

Administratorhandbuch für NSX

Update 12

Geändert am 09. JULI 2020

VMware NSX Data Center for vSphere 6.3



vmware®

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

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

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 © 2010–2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Administratorhandbuch für NSX	12
1 Systemvoraussetzungen für NSX	13
2 Für NSX erforderliche Ports und Protokolle	16
3 Übersicht über NSX	19
NSX-Komponenten	21
Datenebene	21
Steuerungskomponente	22
Managementebene	23
Nutzungsplattform	24
NSX Edge	24
NSX Services	27
4 Übersicht über Cross-vCenter Networking and Security	29
Vorteile von Cross-vCenter NSX	29
Funktionsweise von Cross-vCenter NSX	30
Support-Matrix für NSX-Dienste in Cross-vCenter NSX	32
Globaler Controller-Cluster	33
Globale Transportzone	33
Globale logische Switches	33
Globale logische (Distributed) Router	34
Universelle Firewallregeln	34
Globale Netzwerk- und Sicherheitsobjekte	35
Cross-vCenter NSX-Topologien	36
Cross-vCenter NSX für mehrere und eine einzelne Site	36
Lokaler Ausgang	38
Ändern der NSX Manager-Rollen	39
5 Transportzonen	41
Hinzufügen einer Transportzone	43
Anzeigen und Bearbeiten einer Transportzone	45
Erweitern einer Transportzone	45
Kontrahieren einer Transportzone	46
Modus für den Betrieb mit getrenntem Controller (CDO)	46
Aktivieren des Modus für den Betrieb mit getrenntem Controller (CDO)	47
Deaktivieren des Modus für den Betrieb mit getrenntem Controller (CDO)	48

6 Logische Switches 49

- Hinzufügen eines logischen Switch 51
 - Hinzufügen eines logischen Switch 52
 - Verbinden eines logischen Switch mit einem NSX Edge 54
 - Bereitstellen von Diensten auf einem logischen Switch 55
- Verbinden von virtuellen Maschinen mit einem logischen Switch 55
- Testen der Konnektivität eines logischen Switches 55
- Verhindern von Manipulationen auf einem logischen Switch 56
- Bearbeiten eines logischen Switches 56
- Szenario für einen logischen Switch 57
 - Peter Admin weist NSX Manager einen Segment-ID-Pool und einen Multicast-Adressbereich zu 59
 - Peter Admin konfiguriert VXLAN-Transportparameter 60
 - Peter Admin fügt eine Transportzone hinzu 61
 - Peter Admin erstellt einen logischen Switch 61

7 Konfigurieren von Hardware-Gateways 63

- Szenario: Beispielkonfiguration für ein Hardware-Gateway 64
 - Einrichten des Replizierungsclusters 66
 - Verbinden des Hardware-Gateways mit NSX Controllern 67
 - Hinzufügen eines Hardware-Gateway-Zertifikats 68
 - Binden des logischen Switch an den physischen Switch 69

8 L2-Bridges 71

- Hinzufügen einer L2-Bridge 72
- Hinzufügen einer L2-Bridge zu einer Umgebung mit logischem Routing 73

9 Routing 75

- Hinzufügen eines logischen (verteilten) Router 75
- Hinzufügen eines Edge Services Gateway 89
- Angaben der globalen Konfiguration 101
- Konfiguration von NSX Edge 103
 - Arbeiten mit Zertifikaten 103
 - FIPS-Modus 108
 - Verwalten von Appliances 111
 - Verwalten von Ressourcenreservierungen für die NSX Edge-Appliance 112
 - Arbeiten mit Schnittstellen 115
 - Hinzufügen einer Teilschnittstelle 118
 - Ändern der Konfiguration für die automatische Regel 121
 - Ändern der CLI-Anmeldedaten 122
 - Grundlegendes zu High Availability 122

Erzwingen der Synchronisierung von NSX Edge mit NSX Manager	125
Konfigurieren von Syslog-Servern für NSX Edge	126
Anzeigen des Status eines NSX Edge	126
NSX Edge erneut bereitstellen	127
Herunterladen von Tech-Support-Protokollen für NSX Edge	129
Hinzufügen einer statischen Route	130
Konfigurieren von OSPF auf einem logischen (Distributed) Router	131
Konfigurieren von OSPF in einem Edge Services Gateway	137
Konfigurieren des BGP-Protokolls	143
Konfigurieren der Route Redistribution	148
Anzeigen der Gebietsschema-ID von NSX Manager	149
Konfigurieren der Gebietsschema-ID auf einem globalen (Distributed) Router	150
Konfigurieren der Gebietsschema-ID auf einem Host oder Cluster	151

10 Logische Firewall 152

verteilte Firewall	152
Sitzungs-Timer	155
IP-Erkennung für virtuelle Maschinen	158
Ausschließen von virtuellen Maschinen vom Schutz durch die Firewall	159
Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen	160
Ressourcennutzung der Verteilten Firewall	160
Edge-Firewall	161
Arbeiten mit NSX Edge-Firewallregeln	162
Arbeiten mit Firewallregelabschnitten	173
Hinzufügen eines Firewallregelabschnitts	173
Zusammenführen von Firewallregelabschnitten	174
Löschen eines Firewallregelabschnitts	174
Arbeiten mit Firewallregeln	175
Bearbeiten der standardmäßigen Regel für die verteilte Firewall	176
Hinzufügen einer Regel für die verteilte Firewall	176
Erzwingen der Synchronisierung von verteilten Firewallregeln	182
Hinzufügen einer universellen Firewallregel	182
Firewallregeln mit einem benutzerdefinierten Schicht-3-Protokoll	187
Speichern einer nicht veröffentlichten Konfiguration	188
Laden einer gespeicherten Firewallkonfiguration	189
Filtern der Firewallregeln	190
Ändern der Reihenfolge einer Firewallregel	190
Löschen einer Firewallregel	191
Firewallprotokolle	191

11 Überblick über die identitätsbasierte Firewall (IDFW) 196

Workflow für die identitätsbasierte Firewall 197

12 Arbeiten mit Active Directory-Domänen 199

Registrieren einer Windows-Domäne mit NSX Manager 199

Synchronisieren einer Windows-Domäne mit Active Directory 201

Bearbeiten einer Windows-Domäne 202

Aktivieren des Nur-Lese-Zugriffs auf Sicherheitsprotokolle auf Windows 2008 202

Überprüfen der Verzeichnisrechte 203

13 Verwenden von SpoofGuard 205

Erstellen einer SpoofGuard-Richtlinie 206

Genehmigen von IP-Adressen 207

Bearbeiten einer IP-Adresse 208

Löschen einer IP-Adresse 209

14 Virtual Private Networks (VPN) 210

Überblick über SSL VPN-Plus 210

Konfigurieren von Network Access SSL VPN-Plus 212

Installieren des SSL VPN-Plus Clients 223

Konfigurieren von Proxy-Server-Einstellungen in SSL VPN-Plus-Client 226

SSL VPN-Plus-Protokolle 227

Bearbeiten der Client-Konfiguration 228

Bearbeiten der allgemeinen Einstellungen 229

Bearbeiten des Webportal-Designs 229

Arbeiten mit IP-Pools für SSL VPN 230

Arbeiten mit privaten Netzwerken 231

Arbeiten mit Installationspaketen 233

Arbeiten mit Benutzern 234

Arbeiten mit Anmelde- und Abmeldeskripts 235

Überblick über IPSec-VPN 237

Konfigurieren des IPSec-VPN-Diensts 238

Bearbeiten des IPSec-VPN-Diensts 243

Deaktivieren der IPSec-VPN-Site 243

Löschen einer IPSec-VPN-Site 243

Beispiele für die IPSec-VPN-Konfiguration 244

Überblick über L2 VPN 255

Konfigurieren von L2 VPN 257

Konfigurieren eines L2 VPN-Servers 263

Hinzufügen von Peer-Sites 264

Aktivieren eines L2-VPN-Diensts auf dem Server 265

Konfigurieren eines L2 VPN-Clients 266

- Aktivieren eines L2-VPN-Diensts auf Client 268
- Konfigurieren eines eigenständigen Edge als L2 VPN-Client 268
- Anzeigen von L2 VPN-Statistiken 270
- Entfernen eines ausgeweiteten VLAN 271

15 Logischer Load Balancer 272

- Einrichten des Load Balancing 276
 - Konfigurieren des Load-Balancer-Dienstes 278
 - Erstellen eines Dienstmonitors 279
 - Hinzufügen eines Serverpools 285
 - Erstellen eines Anwendungsprofils 288
 - Hinzufügen einer Anwendungsregel 292
 - Hinzufügen von virtuellen Servern 299
- Verwalten von Anwendungsprofilen 301
 - Bearbeiten eines Anwendungsprofils 301
 - Konfigurieren der SSL-Beendigung für einen Load Balancer 301
 - Löschen eines Anwendungsprofils 302
- Verwalten von Dienstmonitoren 303
 - Bearbeiten eines Dienstmonitors 303
 - Löschen eines Dienstmonitors 303
- Verwalten von Serverpools 304
 - Bearbeiten eines Serverpools 304
 - Konfigurieren eines Load Balancer zur Verwendung des transparenten Modus 304
 - Löschen eines Serverpools 305
 - Anzeigen der Poolstatistik 305
- Verwalten von virtuellen Servern 306
 - Bearbeiten eines virtuellen Servers 306
 - Löschen eines virtuellen Servers 307
- Verwalten von Anwendungsregeln 307
 - Bearbeiten einer Anwendungsregel 307
 - Löschen einer Anwendungsregel 308
- Load-Balancer-Webserver mit NTLM-Authentifizierung 308
- HTTP-Verbindungsmodi des Load Balancer 308
- Szenarien für die NSX-Load-Balancer-Konfiguration 311
 - Konfiguration eines einarmigen Load Balancer 311
 - Szenario: Konfigurieren des NSX-Load-Balancer für den Platform Services Controller 317
 - Szenario: SSL-Offloading 321
 - Szenario: Importieren eines SSL-Zertifikats 326
 - Szenario: SSL-Passthrough 329
 - Szenario: SSL-Client- und -Server-Authentifizierung 331

16 Andere Edge-Dienste 334

- Verwalten des DHCP-Diensts 334
 - Hinzufügen eines DHCP-IP-Pools 334
 - Aktivieren des DHCP-Diensts 336
 - Bearbeiten eines DHCP-IP-Pools 337
 - Hinzufügen einer statischen DHCP-Bindung 338
 - Bearbeiten der DHCP-Bindung 339
- Konfigurieren des DHCP-Relays 339
 - Hinzufügen eines DHCP-Relay-Servers 341
 - Hinzufügen von Relay-Agenten 341
- Konfigurieren eines DNS-Servers 342

17 Service Composer 343

- Verwenden des Service Composer 345
 - Erstellen einer Sicherheitsgruppe in Service Composer 347
 - Erstellen einer Sicherheitsrichtlinie 349
 - Anwenden einer Sicherheitsrichtlinie auf eine Sicherheitsgruppe 354
- Service Composer-Arbeitsfläche 355
- Arbeiten mit Sicherheits-Tags 358
 - Auswahl einer eindeutigen Kennung 358
 - Anzeigen von angewendeten Sicherheits-Tags 359
 - Erstellen eines Sicherheits-Tags 360
 - Zuweisen eines Sicherheits-Tags 360
 - Bearbeiten eines Sicherheits-Tags 361
 - Löschen eines Sicherheits-Tags 361
- Anzeigen von aktiven Diensten 362
 - Anzeigen von aktiven Diensten zu einer Sicherheitsrichtlinie 362
 - Anzeigen von Dienstfehlern für eine Sicherheitsrichtlinie 362
 - Anzeigen von aktiven Diensten auf einer virtuellen Maschine 363
- Arbeiten mit Sicherheitsrichtlinien 363
 - Verwalten der Sicherheitsrichtlinienpriorität 363
 - Bearbeiten einer Sicherheitsrichtlinie 364
 - Löschen einer Sicherheitsrichtlinie 364
- Service Composer-Szenarien 365
 - Szenario zum Sperren von infizierten Maschinen 365
 - Sichern von Sicherheitskonfigurationen 369
- Importieren und Exportieren von Konfigurationen für Sicherheitsrichtlinien 372
 - Exportieren einer Sicherheitsrichtlinien-Konfiguration 372
 - Importieren einer Sicherheitsrichtlinien-Konfiguration 373

18 Guest Introspection 375

Installieren von Guest Introspection auf Hostclustern	376
Installieren von Guest Introspection Thin Agent auf virtuellen Windows-Maschinen	378
Installieren von Guest Introspection Thin Agent auf virtuellen Linux-Maschinen	380
Guest Introspection-Status anzeigen	382
Guest Introspection-Überwachungsmeldungen	382
Erfassen von Daten zur Fehlerbehebung für Guest Introspection	382
Deinstallieren eines Guest Introspection-Moduls	383
Guest Introspection für Linux deinstallieren	383

19 Netzwerk-Erweiterbarkeit 385

Verteilte Service Insertion	386
Edge-basierte Service Insertion	386
Integration von Drittanbieter-Diensten	386
Bereitstellen von Partnerdiensten	387
Anbieter-Dienste durch Service Composer nutzen	389
Umleiten des Datenverkehrs zu einer Anbieterlösung über die logische Firewall	389
Nutzung eines Partner-Load-Balancer	390
Entfernen der Drittanbieterintegration	391

20 Benutzer-Management 392

NSX-Benutzer und -Berechtigungen nach Funktion	392
Konfigurieren von Single Sign-On	397
Verwalten von Benutzerrechten	399
Verwalten des Standardbenutzerkontos	399
Zuweisen einer Rolle zu einem vCenter-Benutzer	400
Erstellen eines Benutzers mit Zugriff auf die Web-Benutzeroberfläche mithilfe der Befehlszeilenschnittstelle	403
Bearbeiten eines Benutzerkontos	406
Ändern einer Benutzerrolle	406
Deaktivieren oder Aktivieren eines Benutzerkontos	407
Löschen eines Benutzerkontos	407

21 Netzwerk- und Sicherheitsobjekte 408

Arbeiten mit IP-Adressgruppen	408
Erstellen einer IP-Adressgruppe	408
Bearbeiten einer IP-Adressgruppe	409
Löschen einer IP-Adressgruppe	410
Arbeiten mit MAC-Adressgruppen	410
Erstellen einer MAC-Adressgruppe	410
Bearbeiten einer MAC-Adressgruppe	411
Löschen einer MAC-Adressgruppe	411
Arbeiten mit IP-Pools	412

Erstellen eines IP-Pools	412
Bearbeiten eines IP-Pools	412
Löschen eines IP-Pools	413
Arbeiten mit Sicherheitsgruppen	413
Erstellen einer Sicherheitsgruppe	414
Bearbeiten einer Sicherheitsgruppe	417
Löschen einer Sicherheitsgruppe	417
Arbeiten mit Diensten und Dienstgruppen	418
Erstellen eines Diensts	418
Erstellen einer Dienstgruppe	419
Bearbeiten eines Diensts oder einer Dienstgruppe	419
Löschen eines Diensts oder einer Dienstgruppe	420

22 Vorgänge und Verwaltung 421

Verwenden des NSX-Dashboard	421
Überprüfen des Kommunikationskanalstatus	425
NSX Controller	426
Ändern des Controller-Kennworts	426
Herunterladen von technischen Support-Protokollen für NSX Controller	427
Konfigurieren eines Syslog-Servers für NSX Controller	427
Ändern des VXLAN-Ports	428
Programm zur Verbesserung der Benutzerfreundlichkeit	430
Bearbeiten der Option „Programm zur Verbesserung der Benutzerfreundlichkeit“ (CEIP)	430
Grundlegendes zu NSX-Protokollen	431
Überwachungsprotokolle	432
Verwendung von NSX Ticket Logger	432
Anzeigen des Überwachungsprotokolls	433
Systemereignisse	434
Anzeigen des Systemereignisberichts	434
Format von Systemereignissen	434
Alarmer	435
Format eines Alarms	436
Arbeiten mit SNMP-Traps	436
Einstellungen für das Managementsystem	441
Anmelden bei der virtuellen NSX Manager-Appliance	441
Bearbeiten des Datums und der Uhrzeit von NSX Manager	442
Konfigurieren eines Syslog-Servers für NSX Manager	442
Ändern des FIPS-Modus und der TLS-Einstellungen für NSX Manager	443
Bearbeiten von DNS-Servern	444
Bearbeiten von Lookup Service-Details	445
Bearbeiten von vCenter Server	445

Herunterladen der Protokolle des technischen Supports für NSX	445
NSX Manager – SSL-Zertifizierung	446
Sichern und Wiederherstellen von NSX	449
Sichern und Wiederherstellen von NSX Manager	450
Sichern von vSphere Distributed Switches	457
Sichern von vCenter	457
Flow Monitoring	458
Anzeigen von Flow Monitoring-Daten	458
Ändern des Datumsbereichs der Flow Monitoring-Diagramme	460
Hinzufügen oder Bearbeiten einer Firewallregel vom Flow Monitoring-Bericht aus	461
Anzeigen von Live-Flow	461
Konfigurieren der Erfassung von Flow Monitoring-Daten	462
Konfigurieren von IPFIX	465
Application Rule Manager	477
Erstellen einer Überwachungssitzung	478
Analysieren von Flows	479
Flow-Konsolidierung und -Anpassung	480
Anpassen von Diensten in Flow-Datensätzen	481
Anpassen von Quelle und Ziel in den Flow-Datensätzen	483
Erstellen von Firewallregeln mit dem Application Rule Manager	485
Veröffentlichen und Verwalten von Firewallregeln mit dem Application Rule Manager	487
Activity Monitoring	488
Einrichten von Activity Monitoring	489
Szenarien zum Activity Monitoring	493
Aktivieren der Datenerfassung	496
Anzeigen des Aktivitätsberichts für virtuelle Maschinen	497
Anzeigen eingehender Aktivität	498
Anzeigen ausgehender Aktivität	499
Anzeigen der Interaktion zwischen Bestandslisten-Containern	501
Anzeigen der ausgehenden AD-Gruppenaktivität	503
Überschreiben der Datenerfassung	504
Datenerfassung für die Endpunktüberwachung	504
Endpunktüberwachung	505
Traceflow	507
Informationen zu Traceflow	507
Fehlerbehebung mithilfe von Traceflow	509

Administratorhandbuch für NSX

Im *Administratorhandbuch für NSX* wird die Konfiguration, Überwachung und Instandhaltung des VMware NSX[®] for vSphere[®]-Systems mithilfe der NSX Manager-Benutzeroberfläche und des vSphere Web Client beschrieben. Zu den bereitgestellten Informationen gehören schrittweise Anleitungen für die Konfiguration sowie empfohlene Vorgehensweisen.

Zielgruppe

Dieses Handbuch ist für alle Benutzer gedacht, die NSX in einer VMware vCenter-Umgebung installieren oder verwenden möchten. Die Informationen in diesem Handbuch sind für erfahrene Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb virtueller Datacenter vertraut sind. Dieses Handbuch setzt voraus, mit VMware vSphere, einschließlich VMware ESXi, vCenter Server und dem vSphere Web Client vertraut zu sein.

VMware Technical Publications – Glossar

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

Systemvoraussetzungen für NSX

1

Bevor Sie NSX installieren oder aktualisieren, prüfen Sie Ihre Netzwerkkonfiguration und -ressourcen. Sie können einen NSX Manager pro vCenter Server, eine Guest Introspection-Instanz pro ESXi™-Host und mehrere NSX Edge-Instanzen pro Datacenter installieren.

Hardware

Diese Tabelle enthält die Hardwareanforderungen für NSX-Appliances.

Tabelle 1-1. Hardwareanforderungen für Appliances

Appliance	Arbeitsspeicher	vCPU	Festplattenspeicher
NSX Manager	16 GB (24 GB für größere NSX-Bereitstellungen)	4 (8 für größere NSX-Bereitstellungen)	60 GB
NSX Controller	4 GB	4	28 GB
NSX Edge	Kompakt: 512 MB Groß: 1 GB Quad Large: 2 GB Sehr groß: 8 GB	Kompakt: 1 Groß: 2 Quad Large: 4 Sehr groß: 6	Kompakt, Groß: 1 Festplatte mit 584 MB + 1 Festplatte mit 512 MB Quad Large: 1 Festplatte mit 584 MB + 2 Festplatten mit 512 MB Sehr groß: 1 Datenträger 584 MB + 1 Datenträger 2 GB + 1 Datenträger 512 MB
Guest Introspection	2 GB	2	5 GB (bereitgestellter Speicherplatz: 6,26 GB)

Als allgemeine Richtlinie gilt: Erhöhen Sie die NSX Manager-Ressourcen auf 8 vCPU und 24 GB RAM, wenn Ihre von NSX verwaltete Umgebung mehr als 256 Hypervisoren oder mehr als 2.000 VMs umfasst.

Um spezifische Details zur Größe zu erhalten, wenden Sie sich an den Support von VMware.

Informationen zur Erhöhung der Arbeitsspeicher- und vCPU-Zuteilung für Ihre virtuellen Appliances finden Sie unter „Zuteilen von Arbeitsspeicherressourcen“ und „Ändern der Anzahl virtueller CPUs“ in der Dokumentation *Verwaltung virtueller vSphere-Maschinen*.

Der bereitgestellte Speicherplatz für eine Guest Introspection-Appliance zeigt 6,26 GB für Guest Introspection an. Dies liegt daran, dass vSphere ESX Agent Manager einen Snapshot von der Dienst-VM erstellt, um schnelle Klone zu erstellen, wenn mehrere Hosts in einem Cluster Speicher gemeinsam nutzen. Weitere Informationen zum Deaktivieren dieser Option über ESX Agent Manager finden Sie in der *ESX Agent Manager*-Dokumentation.

Netzwerklatenz

Stellen Sie sicher, dass die Netzwerklatenz zwischen Komponenten der angegebenen maximalen Latenz entspricht oder niedriger als diese ist.

Tabelle 1-2. Maximale Netzwerklatenz zwischen Komponenten

Komponenten	Maximale Latenz
NSX Manager und NSX Controller	150 ms RTT
NSX Manager und ESXi-Hosts	150 ms RTT
NSX Manager und vCenter Server-System	150 ms RTT
NSX Manager und NSX Manager in einer Cross-vCenter NSX-Umgebung	150 ms RTT
NSX Controller und ESXi-Hosts	150 ms RTT

Software

Die neuesten Interoperabilitätsinformationen finden Sie in den Produkt-Interoperabilitätsmatrizen unter http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Die empfohlenen Versionen von NSX, vCenter Server und ESXi finden Sie in den Versionshinweisen für die Version von NSX, auf die Sie ein Upgrade vornehmen. Die Versionshinweise finden Sie auf der „NSX for vSphere“-Dokumentationsseite: <https://docs.vmware.com/de/VMware-NSX-for-vSphere/index.html>.

Die folgenden Bedingungen müssen erfüllt sein, damit ein NSX Manager in einer Cross-vCenter NSX-Bereitstellung teilnehmen kann:

Komponente	Version
NSX Manager	6.2 oder höher
NSX Controller	6.2 oder höher
vCenter Server	6.0 oder höher
ESXi	<ul style="list-style-type: none"> ■ ESXi 6.0 oder höher ■ Mit NSX 6.2 oder späteren VIBs vorbereitete Hostcluster

Um alle NSX Manager in einer Cross-vCenter NSX-Bereitstellung von einem einzigen vSphere Web Client aus verwalten zu können, müssen Sie Ihre vCenter Server-Instanzen im erweiterten verknüpften Modus verbinden. Erläuterungen dazu finden Sie unter „Verwenden des erweiterten verknüpften Modus“ in der Dokumentation *vCenter Server und Hostverwaltung*.

Informationen zur Überprüfung der Kompatibilität von Partnerlösungen mit NSX finden Sie im „VMware Kompatibilitätshandbuch für Netzwerk und Sicherheit“ unter <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>.

Client- und Benutzerzugriff

Die folgenden Elemente sind zur Verwaltung Ihrer NSX-Umgebung erforderlich:

- Vorwärts- und rückwärtsgerichtete Namensauflösung. Dies ist erforderlich, wenn Sie ESXi-Hosts nach Namen zur vSphere-Bestandsliste hinzugefügt haben. Anderenfalls kann NSX Manager die IP-Adressen nicht auflösen.
- Berechtigungen zum Hinzufügen und Einschalten von virtuellen Maschinen
- Zugriff auf den Datenspeicher, in dem Dateien für virtuelle Maschinen gespeichert werden, sowie Kontoberechtigungen zum Kopieren von Dateien in diesen Datenspeicher
- Cookies müssen in Ihrem Webbrowser aktiviert sein, damit Sie auf die NSX Manager-Benutzeroberfläche zugreifen können.
- Port 443 muss zwischen dem NSX Manager und dem ESXi-Host, dem vCenter Server und den bereitzustellenden NSX-Appliances geöffnet sein. Dieser Port wird zum Herunterladen der OVF-Datei auf dem ESXi-Host für die Bereitstellung benötigt.
- Ein für die von Ihnen verwendete Version von vSphere Web Client unterstützter Webbrowser. Ausführliche Informationen erhalten Sie unter „Verwenden des vSphere Web Client“ in der Dokumentation *vCenter Server und Hostverwaltung*.

Für NSX erforderliche Ports und Protokolle

2

Für einen ordnungsgemäßen Betrieb von NSX müssen die folgenden Ports geöffnet sein.

Hinweis Wenn Sie eine Cross-vCenter NSX-Umgebung haben und sich Ihre vCenter Server-Systeme im erweiterten verknüpften Modus befinden, müssen alle NSX Manager-Appliances die erforderliche Konnektivität mit allen vCenter Server-Systemen in der Umgebung aufweisen, um einen beliebigen NSX Manager über ein beliebiges vCenter Server-System zu verwalten.

Tabelle 2-1. Für NSX for vSphere erforderliche Ports und Protokolle

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
Client-PC	NSX Manager	443	TCP	Verwaltungsschnittstelle von NSX Manager	Nein	Ja	PAM-Authentifizierung
Client-PC	NSX Manager	443	TCP	VIB-Zugang für NSX Manager	Nein	Nein	PAM-Authentifizierung
ESXi-Host	vCenter Server	443	TCP	Vorbereitung des ESXi-Hosts	Nein	Nein	
vCenter Server	ESXi-Host	443	TCP	Vorbereitung des ESXi-Hosts	Nein	Nein	
ESXi-Host	NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort
ESXi-Host	NSX Controller	1234	TCP	UWAC (User World Agent Connection)	Nein	Ja	
NSX Controller	NSX Controller	2878, 2888, 3888	TCP	Controller-Cluster – Statussynchronisierung	Nein	Ja	IPsec
NSX Controller	NSX Controller	7777	TCP	RPC-Port für die Kommunikation zwischen Controllern	Nein	Ja	IPsec
NSX Controller	NSX Controller	30865	TCP	Controller-Cluster – Statussynchronisierung	Nein	Ja	IPsec
NSX Manager	NSX Controller	443	TCP	Kommunikation zwischen Controller und Manager	Nein	Ja	Benutzer/Kennwort

Tabelle 2-1. Für NSX for vSphere erforderliche Ports und Protokolle (Fortsetzung)

Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
NSX Manager	vCenter Server	443	TCP	vSphere Web Access	Nein	Ja	
NSX Manager	vCenter Server	902	TCP	vSphere Web Access	Nein	Ja	
NSX Manager	ESXi-Host	443	TCP	Verwaltungs- und Bereitstellungsverbindung	Nein	Ja	
NSX Manager	ESXi-Host	902	TCP	Verwaltungs- und Bereitstellungsverbindung	Nein	Ja	
NSX Manager	DNS-Server	53	TCP	DNS-Client-Verbindung	Nein	Nein	
NSX Manager	DNS-Server	53	UDP	DNS-Client-Verbindung	Nein	Nein	
NSX Manager	Syslog-Server	514	TCP	Syslog-Verbindung	Nein	Nein	
NSX Manager	Syslog-Server	514	UDP	Syslog-Verbindung	Nein	Nein	
NSX Manager	NTP-Zeitserver	123	TCP	NTP-Client-Verbindung	Nein	Ja	
NSX Manager	NTP-Zeitserver	123	UDP	NTP-Client-Verbindung	Nein	Ja	
vCenter Server	NSX Manager	80	TCP	Hostvorbereitung	Nein	Ja	
REST-Client	NSX Manager	443	TCP	NSX Manager-REST-API	Nein	Ja	Benutzer/Kennwort
VXLAN Tunnel End Point (VTEP)	VXLAN Tunnel End Point (VTEP)	8472 (Standard vor NSX 6.2.3) oder 4789 (Standard in neuen Installationen von NSX 6.2.3 und höher)	UDP	Transportnetzwerk-Kapselung zwischen VTEPs	Nein	Ja	
ESXi-Host	ESXi-Host	6999	UDP	ARP auf VLAN-LIFs	Nein	Ja	
ESXi-Host	NSX Manager	8301, 8302	UDP	DVS-Synchronisierung	Nein	Ja	

Tabelle 2-1. Für NSX for vSphere erforderliche Ports und Protokolle (Fortsetzung)

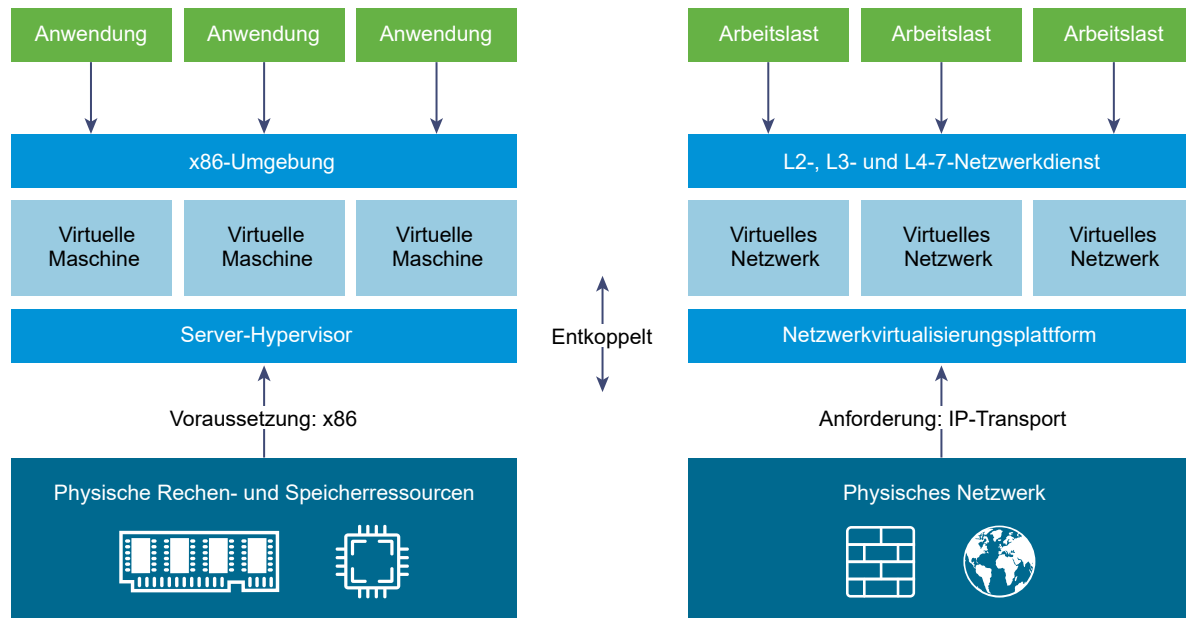
Quelle	Ziel	Port	Protokoll	Zweck	Sensibel	TLS	Authentifizierung
NSX Manager	ESXi-Host	8301, 8302	UDP	DVS-Synchronisierung	Nein	Ja	
Guest Introspection-VM	NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort
Primärer NSX Manager	Sekundärer NSX Manager	443	TCP	Globaler Synchronisierungsdienst für Cross-vCenter NSX	Nein	Ja	
Primärer NSX Manager	vCenter Server	443	TCP	vSphere-API	Nein	Ja	
Sekundärer NSX Manager	vCenter Server	443	TCP	vSphere-API	Nein	Ja	
Primärer NSX Manager	Globaler NSX Controller-Cluster	443	TCP	NSX Controller-REST-API	Nein	Ja	Benutzer/Kennwort
Sekundärer NSX Manager	Globaler NSX Controller-Cluster	443	TCP	NSX Controller-REST-API	Nein	Ja	Benutzer/Kennwort
ESXi-Host	Globaler NSX Controller-Cluster	1234	TCP	Protokoll der NSX-Steuerungskomponente	Nein	Ja	
ESXi-Host	Primärer NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort
ESXi-Host	Sekundärer NSX Manager	5671	TCP	RabbitMQ	Nein	Ja	RabbitMQ-Benutzer/Kennwort

Übersicht über NSX

3

Viele IT-Unternehmen profitieren erheblich von der Servervirtualisierung. Die Serverkonsolidierung reduziert die physische Komplexität und steigert die betriebliche Effizienz sowie die Fähigkeit zur dynamischen Umgestaltung von grundlegenden Ressourcen für eine schnellere und optimale Anpassung an die Anforderungen dynamischer Geschäftsanwendungen.

Die SDDC- (Software-Defined Datacenter) Architektur von VMware erweitert ihre Virtualisierungstechnologien auf die gesamte physische Datacenter-Infrastruktur. Die Netzwerkvirtualisierungsplattform VMware NSX[®] ist ein Schlüsselprodukt in der SDDC-Architektur. Mit NSX liefert die Virtualisierung für die Netzwerke das, was sie bereits für Computing und Speicher geleistet hat. Mithilfe der Servervirtualisierung werden softwarebasierte virtuelle Maschinen programmatisch erstellt, per Snapshot aufgenommen, gelöscht und wiederhergestellt. Mit der NSX-Netzwerkvirtualisierung lassen sich ganze softwarebasierte virtuelle Netzwerke programmatisch erstellen, per Snapshot aufnehmen, löschen und wiederherstellen. Das Ergebnis ist eine absolut innovative Herangehensweise an das Networking, die es Datacenter-Managern ermöglicht, überragende Flexibilität und Wirtschaftlichkeit zu erreichen, und darüber hinaus ein deutlich vereinfachtes Betriebsmodell für das zugrunde liegende physische Netzwerk anbietet. Dank seiner Kompatibilität mit jedem beliebigen IP-Netzwerk, einschließlich sowohl bestehender traditioneller Networking-Modelle und Fabric-Architekturen der nächsten Generation, stellt NSX eine komplett unterbrechungsfreie Lösung dar. Somit ist mit NSX Ihre bestehende physische Netzwerkinfrastruktur alles, was Sie für die Bereitstellung eines Software-Defined Datacenters benötigen.



In der obigen Abbildung wird eine Analogie zwischen Computing und Netzwerkvirtualisierung hergestellt. Bei der Servervirtualisierung reproduziert eine Software-Abstraktionsschicht (Server-Hypervisor) die bekannten Attribute eines physischen x86-Servers (z. B. CPU, RAM, Festplatte, NIC) in Software und ermöglicht so deren programmatische Zusammensetzung in jeder beliebigen Kombination, mit der eine einzigartige VM in Sekundenschnelle erstellt werden kann.

Bei der Netzwerkvirtualisierung reproduziert das funktionale Äquivalent eines Netzwerk-Hypervisors den kompletten Netzwerkdienstsatz von Schicht 2 bis 7 (z. B. Switching, Routing, Zugriffssteuerung, Firewalls, QoS und Load Balancing) in Software. Als Ergebnis können diese Dienste programmatisch in jeder beliebigen Kombination zusammengesetzt werden, um in Sekunden einzigartige, isolierte virtuelle Netzwerke zu erstellen.

Damit lassen sich mit der Netzwerkvirtualisierung ähnliche Vorteile erzielen wie mit der Servervirtualisierung. So wie z. B. die VMs unabhängig von der zugrunde liegenden x86-Plattform sind und es IT-Mitarbeitern ermöglichen, die physischen Hosts als Pool für Computing-Ressourcen zu nutzen, sind die virtuellen Netzwerke unabhängig von der zugrunde liegenden IP-Netzwerk-Hardware und ermöglichen es IT-Mitarbeitern, das physische Netzwerk als Pool für Transportkapazitäten zu nutzen, die auf Anforderung verbraucht und umfunktioniert werden können. Anders als herkömmliche Architekturen können virtuelle Netzwerke bereitgestellt, geändert, gespeichert, gelöscht und programmatisch wiederhergestellt werden, ohne dass die grundlegende physische Hardware oder Topologie neu konfiguriert werden muss. Diese innovative Herangehensweise ans Networking sorgt für die vollständige Entfaltung des Potenzials eines Software-Defined Datacenters, indem sie alle Funktionalitäten, Leistung und Vorteile bekannter Server- und Speichervirtualisierungslösungen bietet.

NSX kann über den vSphere Web Client, eine Befehlszeilenschnittstelle (CLI) und eine REST-API konfiguriert werden.

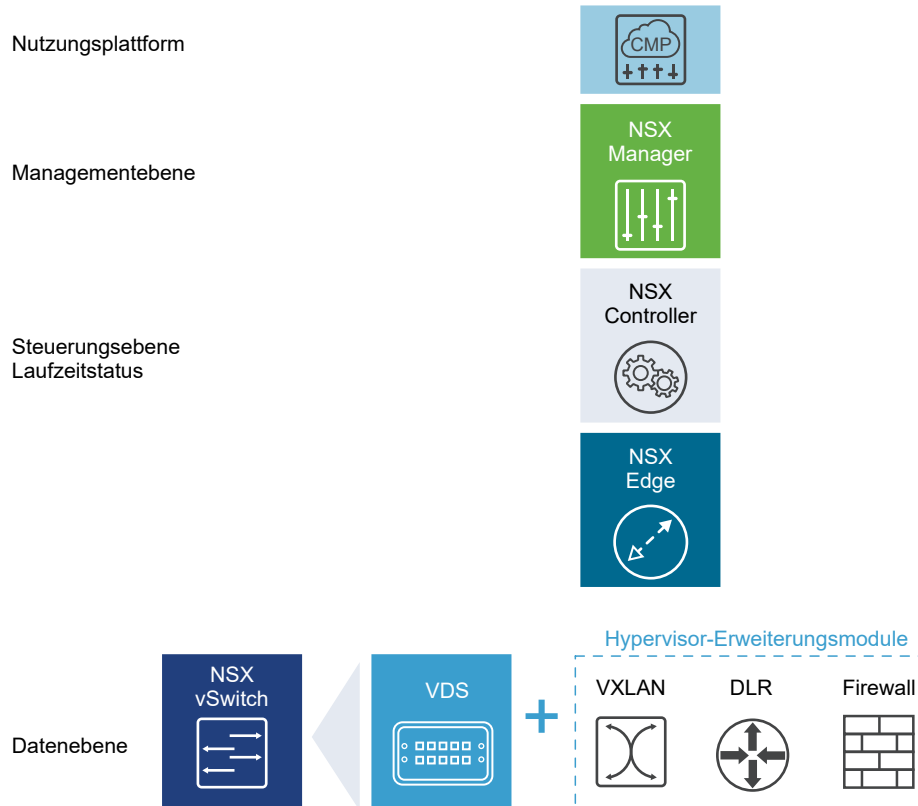
Dieses Kapitel enthält die folgenden Themen:

- **NSX-Komponenten**

- [NSX Edge](#)
- [NSX Services](#)

NSX-Komponenten

In diesem Abschnitt werden die Komponenten der NSX-Lösung beschrieben.



Beachten Sie, dass eine Cloud-Management-Plattform (CMP) keine Komponente von NSX ist, allerdings kann NSX dank REST API und vorgefertigter VMware CMPs in nahezu jede CMP integriert werden.

Datenebene

Die NSX-Datenebene besteht aus einem NSX vSwitch, der auf dem vSphere Distributed Switch (VDS) basiert, sowie aus weiteren Komponenten zur Aktivierung von Diensten. NSX-Kernelmodule, Userspace-Agents, Konfigurationsdateien und Installationsskripts werden in VIBs verpackt und innerhalb des Hypervisorokernels gestartet, um Dienste wie verteiltes Routing und logische Firewall bereitzustellen sowie um VXLAN-Bridging-Funktionalitäten zu aktivieren.

Der (vDS-basierte) NSX vSwitch abstrahiert das physische Netzwerk und bietet Switching auf Zugangsebene im Hypervisor. Diese Funktion ist entscheidend für die Netzwerkvirtualisierung, da sie von physischen Konstruktionen unabhängige logische Netzwerke wie etwa VLAN ermöglicht. Einige der Vorteile von vSwitch:

- Support für Overlay-Netzwerke mit Protokollen (wie VXLAN) und zentralisierte Netzwerk-Konfiguration Overlay-Netzwerke ermöglichen folgende Funktionalitäten:
 - Geringere Nutzung von VLAN-IDs im physischen Netzwerk
 - Erstellung eines flexiblen logischen Schicht 2(L2)-Overlays über vorhandene IP-Netzwerke auf vorhandener physischer Infrastruktur, ohne die Datacenter-Netzwerke umstrukturieren zu müssen
 - Bereitstellung von Kommunikation (ost-west und nord-süd) bei gleichzeitiger Bewahrung der Isolation zwischen Mandanten
 - Vom Overlay-Netzwerk unabhängige Arbeitslasten für Anwendungen und virtuelle Maschinen, die betrieben werden können, als wären sie mit einem physischen L2-Netzwerk verbunden
- Unterstützt eine riesige Anzahl an Hypervisoren
- Mehrere Funktionen wie etwa Port-Spiegelung, NetFlow/IPFIX, Konfigurationssicherung und -wiederherstellung, Netzwerk-Systemstatusprüfung, QoS und LACP stellen ein umfassendes Toolkit für Datenverkehr, Überwachung und Problembehebung innerhalb des virtuellen Netzwerks bereit

Die logischen Router stellen L2-Bridging vom logischen Netzwerkraum (VXLAN) zum physischen Netzwerk (VLAN) her.

Als Gatewaygerät dient üblicherweise eine virtuelle NSX Edge-Appliance. NSX Edge bietet L2, L3, Firewall für den Umgrenzungsbereich, Load Balancing sowie weitere Dienste wie SSL VPN und DHCP.

Steuerungskomponente

Die NSX-Steuerungskomponente wird im NSX Controller-Cluster ausgeführt. NSX Controller ist ein erweitertes, verteiltes Zustandsverwaltungssystem, das Steuerungskomponentenfunktionen für logische Switching- und Routing-Funktionen für NSX bereitstellt. Er ist der zentrale Kontrollpunkt für alle logischen Switches innerhalb eines Netzwerks und enthält Informationen zu allen Hosts, logischen Switches (VXLANs) und verteilten logischen Router.

Der Controller-Cluster ist für die Verwaltung der verteilten Switching- und Routing-Module in den Hypervisoren verantwortlich. Über den Controller wird kein Datenverkehr auf Datenebene übertragen. Controller-Knoten werden in einem Cluster mit drei Mitgliedern bereitgestellt, um High Availability und Skalierung zu aktivieren. Ein Ausfall der Controller-Knoten wirkt sich nicht auf den Datenverkehr auf Datenebene aus.

NSX Controller verteilen die Netzwerkinformationen an Hosts. Um ein hohes Maß an Flexibilität zu erzielen, ist der NSX Controller für Skalierungen und HA geclustert. NSX Controller müssen in einem Cluster mit drei Knoten bereitgestellt werden. Die drei virtuellen Appliances liefern, verwalten und aktualisieren den Zustand aller Netzwerkfunktionen innerhalb der NSX-Domäne. NSX Manager wird zum Bereitstellen der NSX Controller-Knoten verwendet.

Die drei NSX Controller-Knoten bilden einen Controller-Cluster. Der Controller-Cluster benötigt ein Quorum (auch Mehrheit genannt), um ein „Split-Brain-Szenario“ zu vermeiden. In einem Split-Brain-Szenario rühren Dateninkonsistenzen von der Wartung zweier separater Datensätze her, die sich überlappen. Die Inkonsistenzen können durch Ausfälle und Probleme bei der Datensynchronisierung verursacht werden. Da drei Controller-Knoten vorhanden sind, ist bei einem Ausfall einer der NSX Controller-Knoten Datenredundanz sichergestellt.

Ein Controller-Cluster hat mehrere Rollen, darunter:

- API-Anbieter
- Persistenzserver
- Switch-Manager
- Logischer Manager
- Verzeichnisserver

Jede Rolle hat einen Controller-Masterknoten. Wenn ein Controller-Masterknoten für eine Rolle ausfällt, wählt der Cluster aus den verfügbaren NSX Controller-Knoten einen neuen Master für diese Rolle aus. Der neue NSX Controller-Masterknoten für diese Rolle teilt die verlorenen Teile der Arbeit unter den verbliebenen NSX Controller-Knoten neu auf.

NSX unterstützt drei Steuerungskomponenten-Modi von logischen Switches: Multicast, Unicast und Hybrid. Durch die Verwendung eines Controller-Clusters zum Verwalten von VXLAN-basierten logischen Switches wird der Bedarf an Multicast-Support in der physischen Netzwerkinfrastruktur verhindert. Sie müssen keine Multicast-Gruppen-IP-Adressen bereitstellen und auch nicht PIM-Routing oder IGMP-Snooping-Funktionen in physischen Switches oder Routern aktivieren. Somit entkoppeln die Unicast- und Hybrid-Modi NSX aus dem physischen Netzwerk. VXLANs im Unicast-Steuerungskomponentenmodus benötigen das physische Netzwerk nicht, um Multicast für die Verarbeitung von BUM-Datenverkehr (Broadcast, unbekanntes Unicast und Multicast) innerhalb eines logischen Switches zu unterstützen. Der Unicast-Modus repliziert den gesamten BUM-Datenverkehr lokal auf dem Host und benötigt keine physische Netzwerkkonfiguration. Im Hybrid-Modus wird ein Teil der BUM-Datenverkehrsreplizierung zum ersten physischen Hop-Switch ausgelagert, um eine bessere Leistung zu erreichen. Der Hybrid-Modus erfordert IGMP-Snooping auf dem ersten Hop-Switch und Zugriff auf einen IGMP-Abfrager in jedem VTEP-Subnetz.

Managementebene

Die NSX-Managementebene wird vom NSX Manager, der zentralisierten Netzwerk-Managementkomponente von NSX, erstellt. Sie stellt einen zentralen Konfigurationspunkt und REST API-Einstiegspunkte bereit.

Der NSX Manager wird als virtuelle Appliance auf einem beliebigen ESX™-Host in Ihrer vCenter Server-Umgebung eingesetzt. NSX Manager und vCenter haben eine Eins-zu-eins-Beziehung. Für jede NSX Manager-Instanz gibt es einen vCenter Server. Dies gilt selbst für eine Cross-vCenter NSX-Umgebung.

In einer Cross-vCenter NSX-Umgebung finden sich ein primärer NSX Manager und einer oder mehrere sekundäre NSX Manager. Der primäre NSX Manager ermöglicht es Ihnen, globale logische Switches, globale logische (verteilte) Router sowie globale Firewallregeln zu erstellen. Sekundäre NSX Manager werden zur Verwaltung von den für den jeweiligen NSX Manager lokalen Netzwerkdiensten eingesetzt. In einer Cross-vCenter NSX-Umgebung können bis zu sieben sekundäre NSX Manager mit einem primären NSX Manager verknüpft sein.

Nutzungsplattform

Die Nutzung von NSX kann direkt durch die Benutzerschnittstelle von NSX Manager gesteuert werden, die im vSphere Web Client verfügbar ist. Üblicherweise koppeln Endbenutzer die Netzwerkvirtualisierung an ihre Cloud Management Plattform für die Bereitstellung von Anwendungen. NSX stellt eine umfassende Integration in nahezu alle CMPs durch REST-APIs bereit. Eine sofort zu verwendende Integration ist auch durch VMware vCloud Automation Center, vCloud Director und OpenStack mit dem Neutron-Plug-In für NSX verfügbar.

NSX Edge

Sie können NSX Edge als Edge Services Gateway (ESG) oder als verteilten logischen Router (Distributed Logical Router, DLR) installieren.

Edge Services Gateway

Über das ESG können Sie auf alle NSX Edge-Dienste wie Firewall, NAT, DHCP, VPN, Load Balancing und High Availability zugreifen. Sie können mehrere virtuelle ESG-Appliances in einem Datacenter installieren. Jede virtuelle ESG-Appliance kann über insgesamt zehn Uplink- und interne Netzwerkschnittstellen verfügen. Mit einem Trunk kann ein ESG über bis zu 200 Teilschnittstellen verfügen. Die internen Schnittstellen werden mit gesicherten Portgruppen verbunden und dienen als das Gateway für alle geschützten virtuellen Maschinen in der Portgruppe. Das Subnetz, das der internen Schnittstelle zugewiesen ist, kann ein öffentlich gerouteter IP-Bereich, ein gerouteter privater RFC 1918-Adressbereich oder privater RFC 1918-Adressbereich sein, der NAT verwendet. Firewallregeln und andere NSX Edge-Dienste werden beim Datenverkehr zwischen Schnittstellen erzwungen.

Uplink-Schnittstellen von ESG stellen Verbindungen zu Uplink-Portgruppen her, die Zugriff auf ein gemeinsam genutztes Unternehmensnetzwerk oder einen Dienst haben, das bzw. der Zugriffsschichten im Netzwerk bereitstellt. Mehrere externe IP-Adressen können für Load Balancer-, Site-to-Site-VPN- und NAT-Dienste konfiguriert werden.

Verteilter logischer Router

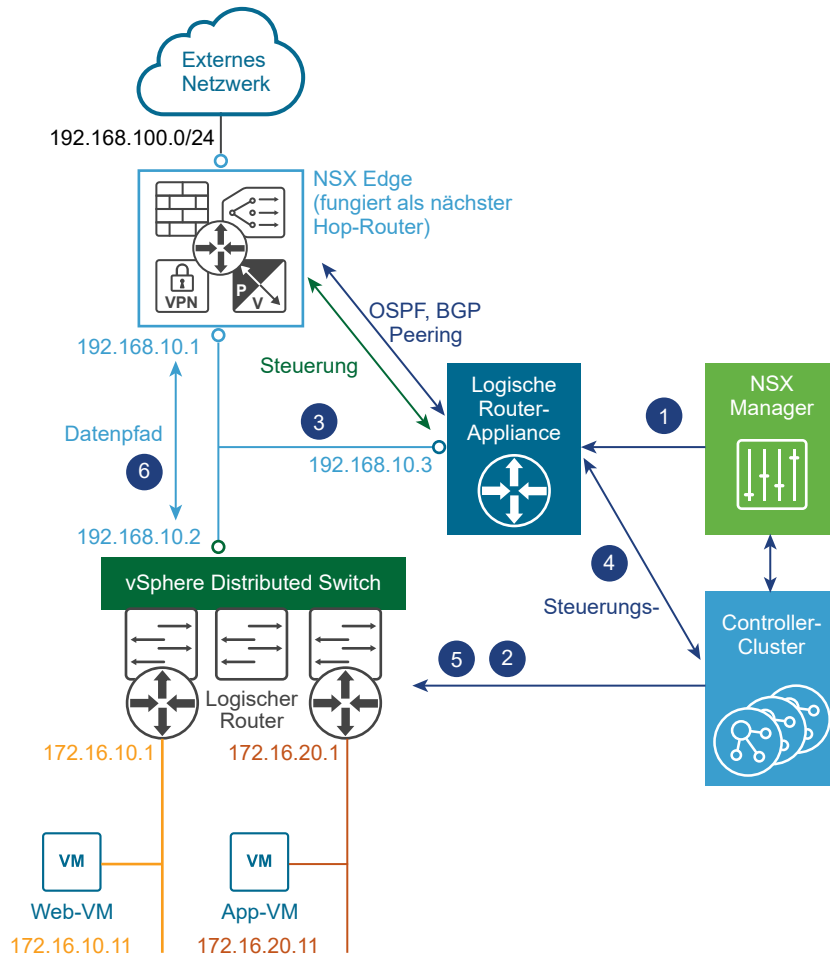
Der DLR stellt horizontal verteiltes Routing mit Mandanten-IP-Adressbereich und Datenpfadisolation bereit. Virtuelle Maschinen oder Arbeitslasten, die auf demselben Host auf verschiedenen Subnetzen vorhanden sind, können miteinander kommunizieren, ohne dass traditionelle Routing-Schnittstellen durchlaufen werden müssen.

Ein logischer Router kann bis zu acht Uplink-Schnittstellen haben und bis zu tausend interne Schnittstellen. Eine Uplink-Schnittstelle auf einem DLR ist in der Regel als Peer eines ESG konfiguriert und nutzt einen intervenierenden logischen Schicht 2-Transit-Switch zwischen dem DLR und dem ESG. Eine interne Schnittstelle auf einem DLR fungiert als Peer einer virtuellen Maschine, die auf einem ESXi-Hypervisor gehostet wird, über einen intervenierenden logischen Switch zwischen der virtuellen Maschine und dem DLR.

Der DLR verfügt über zwei Hauptkomponenten:

- Die DLR-Steuerungskomponente wird von der virtuellen DLR-Appliance bereitgestellt (auch als Kontroll-VM bezeichnet). Diese VM unterstützt dynamische Routing-Protokolle (BGP und OSPF), tauscht Routing-Updates mit dem nächsten Schicht 3-Hop-Gerät aus (normalerweise dem Edge Services Gateway) und kommuniziert mit dem NSX Manager und dem NSX Controller-Cluster. High Availability für die virtuelle DLR-Appliance wird durch Aktiv-Standby-Konfiguration unterstützt: ein Paar virtueller Maschinen in Aktiv-Standby-Modi werden bereitgestellt, wenn Sie den DLR bei aktivierter HA erstellen.
- Auf der Datenebene sind DLR-Kernel-Module (VIBs) vorhanden, die auf den ESXi-Hosts installiert werden, die Teil der NSX-Domäne sind. Die Kernel-Module gleichen den Linecards in einem modularen Gehäuse, das Schicht 3-Routing unterstützt. Die Kernel-Module verfügen über eine Routing-Informationsbasis (Routing Information Base, RIB) – auch als Routing-Tabelle bezeichnet – die per Push vom Controller-Cluster gesendet wird. Die Datenebenenfunktionen von Routensuche und ARP-Eintragssuche werden durch die Kernel-Module ausgeführt. Die Kernel-Module sind mit logischen Schnittstellen (so genannten LIFs) ausgestattet, über die die Verbindung mit den verschiedenen logischen Switches und möglichen VLAN-basierten Portgruppen erfolgt. Jeder LIF ist eine IP-Adresse, die das Standard-IP-Gateway für das logische L2-Segment darstellt, mit dem es verbunden ist, sowie eine vMAC-Adresse zugewiesen. Die IP-Adresse ist für jede LIF eindeutig, allen definierten LIFs hingegen wird dieselbe vMAC zugewiesen.

Abbildung 3-1. Logische Routing-Komponenten



- 1 Eine DLR-Instanz wird über die NSX Manager-Benutzeroberfläche (oder mit API-Aufrufen) erstellt und das Routing wird entweder mittels OSPF oder BGP aktiviert.
- 2 Der NSX Controller nutzt die Steuerungskomponente mit den ESXi-Hosts, um die neue DLR-Konfiguration, einschließlich der LIFs und ihrer zugewiesenen IP- und vMAC-Adressen, per Push zu senden.
- 3 Wenn man davon ausgeht, dass auch ein Routing-Protokoll auf dem nächsten Hop-Gerät (in diesem Beispiel einem NSX Edge [ESG]) aktiviert ist, wird zwischen dem ESG und der DLR-Kontroll-VM OSPF- oder BGP-Peering eingerichtet. Das ESG und der DLR können anschließend Routing-Informationen austauschen:
 - Die DLR-Kontroll-VM kann so konfiguriert werden, dass sie die IP-Präfixe für alle verbundenen logischen Netzwerke (im vorliegenden Beispiel 172.16.10.0/24 und 172.16.20.0/24) in OSPF erneut verteilt. Als Folge davon werden diese Routen-Ankündigungen per Push an das NSX Edge gesendet. Beachten Sie, dass der nächste Hop für diese Präfixe nicht die der Kontroll-VM zugewiesene IP-Adresse (192.168.10.3) ist, sondern die IP-Adresse, die die Datenebenenkomponente des DLR identifiziert (192.168.10.2). Die erste Adresse wird als DLR-„Protokolladresse“ bezeichnet, die zweite ist die „Weiterleitungsadresse“.

- Das NSX Edge sendet die Präfixe per Push an die Kontroll-VM, um IP-Netzwerke im externen Netzwerk zu erreichen. In den meisten Szenarien wird im Normalfall eine einzige Standardroute vom NSX Edge gesendet, weil diese den einzigen Ausgangspunkt zur physischen Netzwerkinfrastruktur darstellt.
- 4 Die DLR-Kontroll-VM sendet die vom NSX Edge erhaltenen IP-Routen per Push an den Controller-Cluster.
 - 5 Der Controller-Cluster ist für die Verteilung der Routen, die ihm von der DLR-Kontroll-VM mitgeteilt wurden, an die Hypervisoren verantwortlich. Jeder Controller-Knoten im Cluster übernimmt die Verantwortung für die Verteilung der Informationen für eine bestimmte logische Router-Instanz. In einer Bereitstellung mit mehreren bereitgestellten logischen Router-Instanzen wird die Last auf die Controller-Knoten verteilt. Normalerweise ist jedem bereitgestellten Mandanten eine separate logische Router-Instanz zugewiesen.
 - 6 Die DLR-Routing-Kernel-Module auf den Hosts verarbeiten den Datenpfad-Datenverkehr für die Kommunikation mit dem externen Netzwerk über das NSX Edge.

NSX Services

Die NSX-Komponenten arbeiten zusammen, um folgende Funktionsdienste zur Verfügung zu stellen.

Logische Switches

Eine Cloud-Bereitstellung oder ein virtuelles Datencenter enthalten diverse Anwendungen für zahlreiche Mandanten. Diese Anwendungen und Mandanten müssen aus Sicherheitsgründen, für Fehlerisolierungszwecke und zur Vermeidung der Überschneidung von IP-Adressen voneinander isoliert werden. NSX ermöglicht die Erstellung von mehreren logischen Switches, die jeweils eine eigene logische Broadcast-Domäne darstellen. Eine Anwendung oder eine Mandanten-VM können logisch an einen logischen Switch gebunden werden. Dies ermöglicht eine schnelle, flexible Bereitstellung bei gleichzeitiger Wahrung aller Vorteile von Broadcast-Domänen eines physischen Netzwerks (VLANs) ohne die Probleme von physischen Schicht-2-Sprawls und ohne Spanning-Tree-Probleme.

Ein logischer Switch wird verteilt und kann alle Hosts in vCenter (oder alle Hosts in einer Cross-vCenter NSX-Umgebung) umspannen. Dies ermöglicht die Mobilität virtueller Maschinen (vMotion) innerhalb des Datencenters ohne Beschränkungen durch die Grenzen der physischen Schicht 2 (VLAN). Die physische Infrastruktur ist nicht durch MAC/FIB-Tabellengrenzen beschränkt, weil die Broadcast-Domäne beim logischen Switch in der Software enthalten ist.

Logische Router

Routing bietet die notwendigen Weiterleitungsinformationen zwischen Schicht 2-Broadcast-Domänen, wodurch Sie die Größe von Schicht 2-Broadcast-Domänen verringern und die Netzwerk-Effizienz und -Größe verbessern können. NSX dehnt diese Informationen auf Orte aus, an denen sich die Arbeitslasten für horizontales Routing befinden. Dies ermöglicht eine direktere Kommunikation zwischen virtuellen Maschinen ohne die kosten- und zeitaufwendige Erweiterung von Hops. Gleichzeitig bieten die logischen NSX-Router auch vertikale Verbindungen, wodurch Mandanten für den Zugriff auf öffentliche Netzwerke aktiviert werden.

Logische Firewall

Die logische Firewall bietet Sicherheitsmechanismen für dynamische virtuelle Datacenter. Mit der Komponente „verteilte Firewall“ der logischen Firewall können Sie virtuelle Datacenterentitäten, z. B. virtuelle Maschinen, anhand der VM-Namen und -Attribute, Benutzeridentitäten und vCenter-Objekte, z. B. Datacenter und Hosts, segmentieren sowie Segmentierungen anhand herkömmlicher Netzwerkattribute wie IP-Adressen, VLANs usw. durchführen. Die Edge-Firewall-Komponente hilft Ihnen dabei, essenzielle Sicherheitsanforderungen für den Umgrenzungsbereich etwa durch den Aufbau von auf IP/VLAN-Konstrukten basierten DMZs und Mandantenisolierung in virtuellen mehrinstanzfähigen Datacentern zu erfüllen.

Die Flow Monitoring-Funktion zeigt Netzwerkaktivitäten zwischen virtuellen Maschinen auf der Anwendungsprotokollebene an. Sie können diese Informationen zum Überprüfen des Netzwerkverkehrs, zum Definieren und zum Verfeinern von Firewallrichtlinien und zum Identifizieren von Netzwerkbedrohungen verwenden.

Logische virtuelle private Netzwerke (VPNs)

Mit SSL VPN-Plus können Remotebenutzer auf private Firmenanwendungen zugreifen. IPSec VPN bietet Interkonnektivität verschiedener Sites zwischen einer NSX Edge-Instanz und Remote-Sites mit NSX oder Hardware-Routern/VPN-Gateways von Drittanbietern. Mit L2 VPN können Sie Ihr Datacenter erweitern, indem Sie zulassen, dass virtuelle Maschinen die Netzwerkkonnektivität über geografische Grenzen hinaus wahren und dabei dieselben IP-Adressen beibehalten.

Logischer Load Balancer

Der Load Balancer von NSX Edge verteilt die Client-Verbindungen, die auf eine einzelne virtuelle IP-Adresse (VIP) ausgerichtet sind, über mehrere Ziele, die als Mitglieder eines Load-Balancing-Pools konfiguriert wurden. Er verteilt eingehende Dienstanforderungen über mehrere Server gleichmäßig auf eine Weise, dass die Lastverteilung für die Benutzer transparent ist. Das Load Balancing hilft deshalb dabei, optimale Ressourcennutzung, maximalen Durchsatz und minimale Reaktionszeit zu erreichen sowie Überlastung zu vermeiden.

Service Composer

Mit Service Composer können Sie Netzwerk- und Sicherheitsdienste für Anwendungen in einer virtuellen Infrastruktur bereitstellen und zuweisen. Sie können diese Dienste einer Sicherheitsgruppe zuweisen. Diese Dienste werden mithilfe einer Sicherheitsrichtlinie auf die virtuellen Maschinen in der Sicherheitsgruppe angewendet.

Erweiterbarkeit von NSX

Drittanbieter von Lösungen können ihre Lösungen mit der NSX-Plattform integrieren. Dadurch können ihre Kunden die VMware-Produkte und die Lösungen unserer Partner in integrierter Weise nutzen. Rechenzentrumsbetreiber können komplexe virtuelle Multi-Tier-Netzwerke in Sekundenschnelle bereitstellen, unabhängig von der zugrunde liegenden Netzwerktopologie oder den zugrunde liegenden Komponenten.

Übersicht über Cross-vCenter Networking and Security

4

NSX 6.2 oder höher ermöglicht Ihnen die Verwaltung mehrerer vCenter NSX-Umgebungen von einem einzelnen primären NSX Manager aus.

Dieses Kapitel enthält die folgenden Themen:

- Vorteile von Cross-vCenter NSX
- Funktionsweise von Cross-vCenter NSX
- Support-Matrix für NSX-Dienste in Cross-vCenter NSX
- Globaler Controller-Cluster
- Globale Transportzone
- Globale logische Switches
- Globale logische (Distributed) Router
- Universelle Firewallregeln
- Globale Netzwerk- und Sicherheitsobjekte
- Cross-vCenter NSX-Topologien
- Ändern der NSX Manager-Rollen

Vorteile von Cross-vCenter NSX

NSX-Umgebungen, die mehr als ein vCenter Server-System enthalten, können zentral verwaltet werden.

Es gibt viele Gründe, warum mehrere vCenter Server-Systeme erforderlich sein können, z. B.:

- Zum Überwinden der Skalierungsgrenzen von vCenter Server
- Zur Aufnahme von Produkten, z. B. Horizon View oder Site Recovery Manager, die dedizierte oder mehrere vCenter Server-Systeme benötigen
- Zum Trennen von Umgebungen, z. B. nach Geschäftseinheit, Mandant, Organisation oder Umgebungstyp

Wenn in NSX 6.1 und früheren Versionen mehrere vCenter NSX-Umgebungen bereitgestellt werden, müssen sie separat verwaltet werden. In NSX 6.2 und höher können Sie auf dem primären NSX Manager universelle Objekte erstellen, die über alle vCenter Server-Systeme in der Umgebung hin synchronisiert werden.

Cross-vCenter NSX enthält diese Funktionen:

- Erhöhte Spanne logischer NSX-Netzwerke. Dieselben logischen Netzwerke stehen in der gesamten vCenter NSX-Umgebung zur Verfügung. Deshalb ist es für virtuelle Maschinen in jedem Cluster auf jedem vCenter Server-System möglich, sich mit demselben logischen Netzwerk zu verbinden.
- Zentrale Verwaltung der Sicherheitsrichtlinien. Firewallregeln werden von einer zentralen Stelle aus verwaltet und gelten für die virtuelle Maschine unabhängig vom Speicherort oder dem vCenter Server-System.
- Unterstützung neuer Mobilitätsgrenzen in vSphere 6, einschließlich Cross-vCenter und vMotion über große Entfernungen zwischen logischen Switches.
- Erweiterte Unterstützung für Multi-Site-Umgebungen, von Metro-Entfernungen bis zu 150 ms RTT. Dies umfasst sowohl Aktiv/Aktiv- als auch Aktiv/Passiv-Datencenter.

Cross-vCenter NSX-Umgebungen haben mehrere Vorteile:

- Zentralisiertes Management von globalen Objekten und eine Reduzierung des Administrationsaufwands.
- Höhere Mobilität der Arbeitslasten – VMs können zwischen vCenter Servern verschoben werden, ohne dass sie neu konfiguriert oder Firewallregeln geändert werden müssen.
- Erweiterte NSX-Multisite- und Notfallplanfunktionen

Hinweis Die Cross-vCenter NSX-Funktionalität wird mit vSphere 6.0 und höher unterstützt.

Funktionsweise von Cross-vCenter NSX

In einer Cross-vCenter NSX-Umgebung haben Sie mehrere vCenter Server, denen jeweils ein eigener NSX Manager zugeordnet werden muss. Einem NSX Manager wird die Rolle des primären NSX Manager zugeteilt, die übrigen erhalten die Rolle eines sekundären NSX Manager.

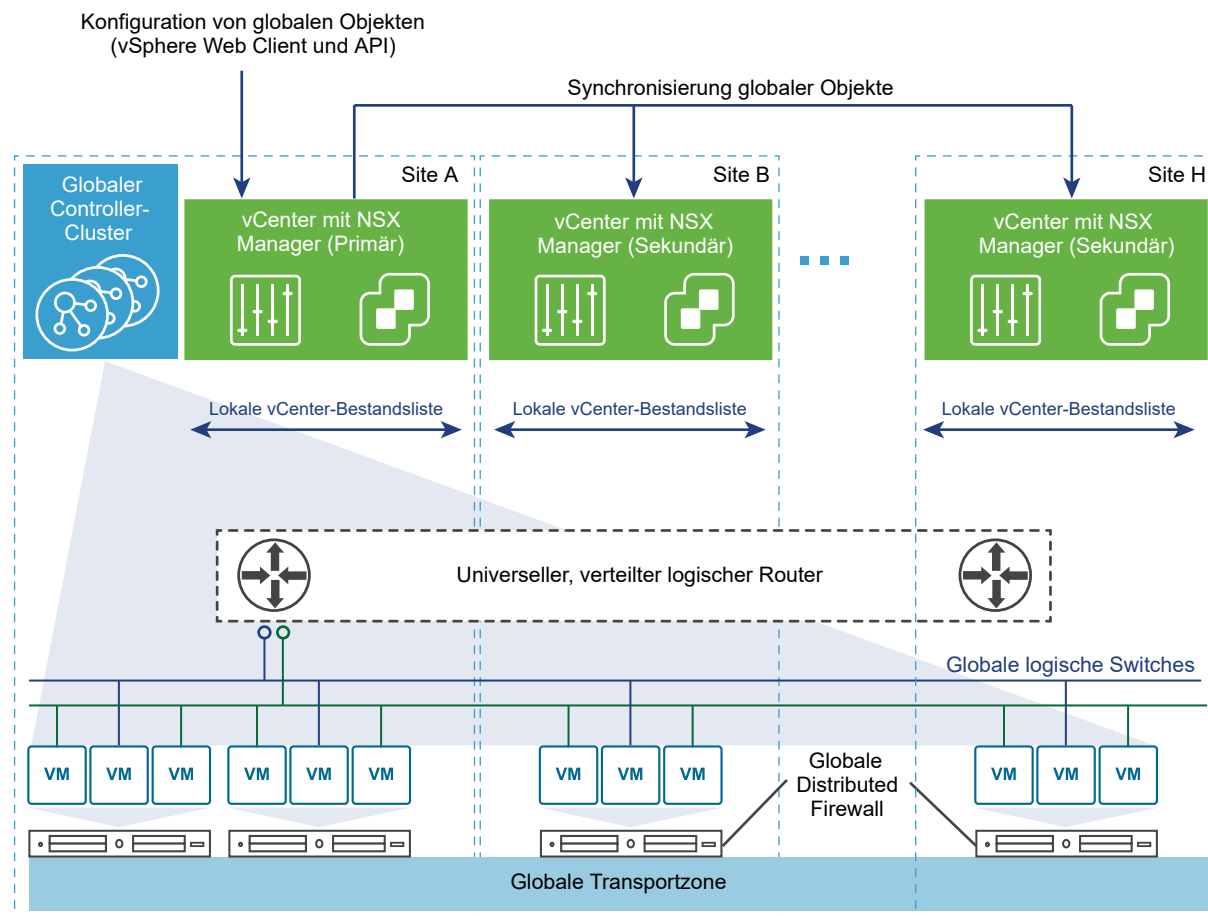
Der primäre NSX Manager wird zur Bereitstellung eines globalen Controller-Clusters genutzt, der die Steuerungsebene für die Cross-vCenter NSX-Umgebung bereitstellt. Die sekundären NSX Manager haben keine eigenen Controller-Cluster.

Der primäre NSX Manager kann globale Objekte wie etwa globale logische Switches erstellen. Diese Objekte werden durch den NSX-Synchronisierungsdienst für alle sekundären NSX Manager synchronisiert. Sie können diese Objekte von einem sekundären NSX Manager anzeigen lassen, können diese dort jedoch nicht bearbeiten. Zur Verwaltung globaler Objekte müssen Sie den primären NSX Manager benutzen. Der primäre NSX Manager kann für die Konfiguration von jedem beliebigen sekundären NSX Manager in der Umgebung verwendet werden.

Sowohl auf dem primären als auch auf jedem sekundären NSX Manager können Objekte wie z. B. logische Switches und logische (verteilte) Router erstellt werden, die für diese spezifische vCenter NSX-Umgebung gelten. Diese existieren nur innerhalb der vCenter NSX-Umgebung, in der sie erstellt wurden. Auf den anderen NSX Managern in der Cross-vCenter NSX-Umgebung werden sie nicht angezeigt.

Einem NSX Manager kann auch eine eigenständige Rolle zugewiesen werden. Diese Zuweisung entspricht Umgebungen vor NSX 6.2 mit einem einzigen NSX Manager und einem vCenter. Ein eigenständiger NSX Manager kann keine globalen Objekte erstellen.

Hinweis Wenn Sie die Rolle einer primären NSX Manager-Instanz in „Eigenständig“ ändern und globale Objekte in der NSX-Umgebung vorhanden sind, wird NSX Manager die Transitrolle zugewiesen. Die globalen Objekte sind weiterhin vorhanden, können aber nicht geändert werden. Zudem können keine neuen globalen Objekte erstellt werden. Sie können globale Objekte aus der Transitrolle löschen. Die Transitrolle darf nur vorübergehend verwendet werden, z. B. wenn der primäre NSX Manager geändert wird.



Support-Matrix für NSX-Dienste in Cross-vCenter NSX

Ein Teil der NSX-Dienste ist für die globale Synchronisierung in Cross-vCenter NSX verfügbar. Dienste, die für die globale Synchronisierung nicht verfügbar sind, können für eine lokale Verwendung mit NSX Manager konfiguriert werden.

Tabelle 4-1. Support-Matrix für NSX-Dienste in Cross-vCenter NSX

NSX-Dienst	Details	Unterstützt Cross-vCenter NSX die Synchronisierung?
Logischer Switch	Transportzone	Ja
	Logischer Switch	Ja
L2-Bridges		Nein
Routing	Logischer (verteilter) Router	Ja
	Logische (verteilte) Router-Appliance	Nein, bedingt durch den Systemaufbau. Wenn mehrere Appliances pro globalem logischen Router erforderlich sind, müssen sie auf jedem NSX Manager erstellt werden. Dies ermöglicht unterschiedliche Konfigurationen pro Appliance, was in einer Umgebung mit konfiguriertem lokalem Ausgang möglicherweise erforderlich ist.
	NSX Edge Services Gateway	Nein
Logische Firewall	verteilte Firewall	Ja
	Ausschlussliste	Nein
	SpoofGuard	Nein
	Flow Monitoring für verbundene Flows	Nein
	Netzwerk Service Insertion	Nein
	Edge-Firewall	Nein
VPN		Nein
Logischer Load Balancer		Nein
Andere Edge-Dienste		Nein
Service Composer		Nein
Netzwerk-Erweiterbarkeit		Nein
Netzwerk- und Sicherheitsobjekte	IP-Adressengruppen (IP Set)	Ja
	MAC-Adressengruppen (MAC Set)	Ja
	IP-Pools	Nein

Tabelle 4-1. Support-Matrix für NSX-Dienste in Cross-vCenter NSX (Fortsetzung)

NSX-Dienst	Details	Unterstützt Cross-vCenter NSX die Synchronisierung?
	Sicherheitsgruppen	Ja, aber die Konfiguration der Mitgliedschaft unterscheidet sich von der Mitgliedschaft nicht globaler Sicherheitsgruppen. Ausführliche Informationen erhalten Sie unter „Erstellen einer Sicherheitsgruppe“ im Dokument <i>Administratorhandbuch für NSX</i> .
	Dienste	Ja
	Dienstgruppen	Ja
Sicherheits-Tags		Ja
Hardware-Gateway (auch bezeichnet als Hardware-VTEP)		Nein. Ausführliche Informationen erhalten Sie unter „Beispielkonfiguration für ein Hardware-Gateway“ im Dokument <i>Administratorhandbuch für NSX</i> .

Globaler Controller-Cluster

Jede Cross-vCenter NSX-Umgebung verfügt über einen globalen Controller-Cluster, der dem primären NSX Manager zugeordnet ist. Sekundäre NSX Manager haben keinen Controller-Cluster.

Da der globale Controller-Cluster der einzige Controller-Cluster für die Cross-vCenter NSX-Umgebung ist, verwaltet er Informationen über globale logische Switches und globale logische Router sowie logische Switches und logische Router, die für ein vCenter NSX-Paar lokal sind.

Um Überlappungen von Objekt-IDs zu vermeiden, werden für globale und lokale Objekte separate ID-Pools verwaltet.

Globale Transportzone

In einer Cross-vCenter NSX-Umgebung darf es nur eine globale Transportzone geben.

Die globale Transportzone wird auf dem primären NSX Manager erstellt und auf die sekundären NSX Manager synchronisiert. Cluster, die an globalen logischen Netzwerken teilnehmen müssen, müssen von ihren NSX Managern zur globalen Transportzone hinzugefügt werden.

Globale logische Switches

Globale logische Switches ermöglichen Schicht 2-Netzwerke, um mehrere Sites einzuschließen.

Wenn Sie in einer globalen Transportzone einen logischen Switch erstellen, erstellen Sie einen globalen logischen Switch. Dieser Switch ist in allen Clustern in der universellen Transportzone verfügbar. Die universelle Transportzone kann Cluster in einem beliebigen vCenter in der Cross-vCenter NSX-Umgebung umfassen.

Der Segment-ID-Pool dient dem Zuweisen von VNIs zu logischen Switches und der globale Segment-ID-Pool dient dem Zuweisen von VNIs zu globalen logischen Switches. Diese Pools dürfen sich nicht überlappen.

Sie müssen einen globalen logischen Router für das Routing zwischen den globalen logischen Switches verwenden. Für ein Routing zwischen einem globalen logischen Switch und einem logischen Switch müssen Sie ein Edge Services Gateway verwenden.

Globale logische (Distributed) Router

Globale logische (Distributed) Router ermöglichen eine zentralisierte Verwaltung und eine Routing-Konfiguration, die im globalen logischen Router, Cluster oder auf Host-Ebene angepasst werden können.

Wenn Sie einen globalen logischen Router erstellen, müssen Sie auswählen, ob Sie den lokalen Ausgang aktivieren, da dies nach der Erstellung nicht mehr geändert werden kann. Mit dem lokalen Ausgang können Sie steuern, welche Routen für ESXi-Hosts basierend auf einem Bezeichner, der Gebietsschema-ID, bereitgestellt werden.

Jedem NSX Manager wird eine Gebietsschema-ID zugewiesen, die standardmäßig auf die NSX Manager-UUID festgelegt ist. Sie können die Gebietsschema-ID auf den folgenden Ebenen umgehen:

- Globaler logischer Router
- Cluster
- ESXi-Host

Wenn Sie den lokalen Ausgang nicht aktivieren, wird die Gebietsschema-ID ignoriert und alle mit dem globalen logischen Router verbundenen ESXi-Hosts erhalten dieselben Routen. Ob Sie den lokalen Ausgang in einer Cross-vCenter NSX-Umgebung aktivieren möchten oder nicht, ist eine Designabwägung, die aber nicht für alle Cross-vCenter NSX-Konfigurationen erforderlich ist.

Universelle Firewallregeln

Mit der verteilten Firewall in einer Cross-vCenter NSX-Umgebung ist eine zentralisierte Verwaltung von Regeln möglich, die auf alle vCenter Server in Ihrer Umgebung angewendet werden. Es unterstützt Cross-vCenter vMotion, wodurch Sie Arbeitslasten oder virtuelle Maschinen aus einem vCenter Server in einen anderen verschieben können, und erweitert die Software-definierte Datensicherheit nahtlos.

Da Ihr Datacenter horizontale Skalierung benötigt, wird der vorhandene vCenter Server möglicherweise nicht auf die gleiche Ebene skaliert. Dadurch müssen Sie möglicherweise einen Satz an Anwendungen auf neuere Hosts verschieben, die von einem anderen vCenter Server verwaltet werden. Alternativ müssen Sie ggf. Anwendungen von Staging bis zur Produktion in eine Umgebung verschieben, in der Staging-Server von einem vCenter-Server und Produktionsserver von einem anderen vCenter-Server verwaltet werden. Die verteilte Firewall unterstützt diese vCenter-übergreifenden vMotion-Szenarien durch sich replizierende Firewall-Richtlinien, die Sie auf bis zu sieben sekundären NSX Manager für den primären NSX Manager definieren können.

Vom primären NSX Manager aus können Sie Regelabschnitte der verteilten Firewall erstellen, die für die globale Synchronisierung markiert sind. Sie können mehrere universelle L2-Regelabschnitte und mehrere universelle L3-Regelabschnitte erstellen. Universelle Abschnitte werden immer am oberen Rand von primären und sekundären NSX Managern aufgeführt. Diese Abschnitte und ihre Regeln werden mit allen sekundären NSX Manager-Instanzen in Ihrer Umgebung synchronisiert. Regeln in anderen Abschnitten bleiben für den entsprechenden NSX Manager lokal.

Die folgenden Funktionen der verteilten Firewall werden in einer Cross-vCenter NSX-Umgebung nicht unterstützt:

- Ausschlussliste
- SpoofGuard
- Flow Monitoring für verbundene Flows
- Netzwerk Service Insertion
- Edge-Firewall

Service Composer unterstützt keine universelle Synchronisierung, daher können Sie damit keine Regeln für die verteilte Firewall im universellen Abschnitt erstellen.

Globale Netzwerk- und Sicherheitsobjekte

Sie können benutzerdefinierte Netzwerk- und Sicherheitsobjekte zur Verwendung in den Regeln für die verteilte Firewall im universellen Abschnitt erstellen.

Universelle Sicherheitsgruppen (USGs) können Folgendes aufweisen:

- Universelle IP Set
- Universelle MAC Set
- Universelle Sicherheitsgruppen
- Universelle Sicherheits-Tags
- Dynamische Kriterien

Universelle Netzwerk- und Sicherheitsobjekte werden ausschließlich auf dem primären NSX Manager erstellt, gelöscht und aktualisiert. Sie können jedoch auf dem sekundären NSX Manager gelesen werden. Der globale Synchronisierungsdienst synchronisiert globale Objekte sofort in vCenter sowie bei Bedarf mit der erzwungenen Synchronisierung.

Universelle Sicherheitsgruppen werden in zwei Bereitstellungstypen verwendet: mehrere live Cross-vCenter-NSX-Umgebungen und aktive Cross-vCenter NSX-Standby-Bereitstellungen, in denen eine Site zu einem bestimmten Zeitpunkt aktiv ist, während sich die anderen Sites in Standby befinden. Es können nur aktive Standby-Bereitstellungen über universelle Sicherheitsgruppen mit dynamischer Mitgliedschaft basierend auf dem VM-Namen oder mit statischer Mitgliedschaft basierend auf einem globalen

Sicherheits-Tag verfügen. Nachdem eine universelle Sicherheitsgruppe erstellt worden ist, kann sie nicht mehr bearbeitet und somit nicht mehr für die aktive Standby-Szenariofunktionalität aktiviert oder deaktiviert werden. Die Mitgliedschaft wird nur durch eingeschlossene Objekte definiert, Sie können keine ausgeschlossenen Objekte verwenden.

Universelle Sicherheitsgruppen können nicht mit dem Service Composer erstellt werden. Mit dem Service Composer erstellte Sicherheitsgruppen sind lokal für den jeweiligen NSX Manager.

Cross-vCenter NSX-Topologien

Sie können Cross-vCenter NSX auf einer einzelnen physischen Site oder auf mehreren Sites bereitstellen.

Cross-vCenter NSX für mehrere und eine einzelne Site

Eine Cross-vCenter NSX-Umgebung ermöglicht Ihnen die Verwendung derselben logischen Switches und weiterer Netzwerkobjekte über mehrere vCenter NSX-Setups hinweg. Die vCenter Server-Systeme können sich auf derselben Site oder auf unterschiedlichen Sites befinden.

Unabhängig davon, ob die Cross-vCenter NSX-Umgebung innerhalb einer einzelnen Site enthalten ist oder mehrere Sites umspannt, kann eine ähnliche Konfiguration verwendet werden. Diese beiden Beispieltopologien bestehen aus:

- Einer globalen Transportzone, die alle Cluster in der Site oder den Sites enthält.
- Globalen logischen Switches, die der globalen Transportzone zugewiesen sind. Zwei globalen logischen Switches zum Verbinden der virtuellen Maschinen und einem Switch als Transit-Netzwerk für den Router-Uplink.
- Virtuellen Maschinen, die zu den globalen logischen Switches hinzugefügt werden
- Einem globalen logischen Router mit einer NSX Edge-Appliance zum Aktivieren des dynamischen Routings. Die globale logische Router-Appliance verfügt über interne Schnittstellen auf den globalen logischen VM-Switches und über eine Uplink-Schnittstelle auf dem globalen logischen Switch des Transit-Netzwerks.
- Edge Services Gateways (ESGs), die mit dem Transit-Netzwerk und dem physischen Ausgangs-Router-Netzwerk verbunden sind.

Weitere Informationen zu Cross-vCenter NSX-Topologien finden Sie im *Cross-vCenter NSX-Design-Handbuch* unter <https://communities.vmware.com/docs/DOC-32552>.

Abbildung 4-1. Cross-vCenter NSX in einer einzelnen Site

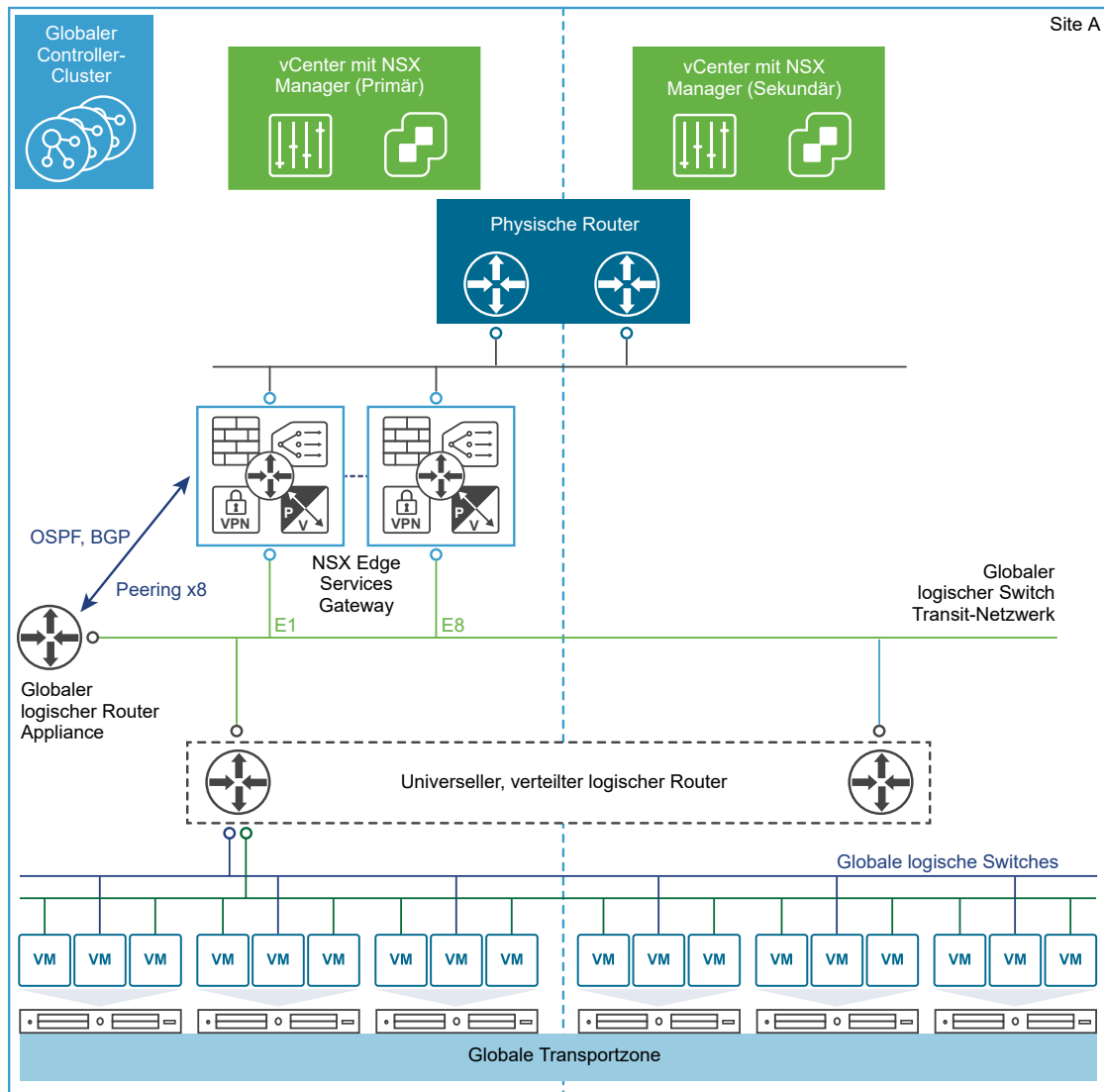
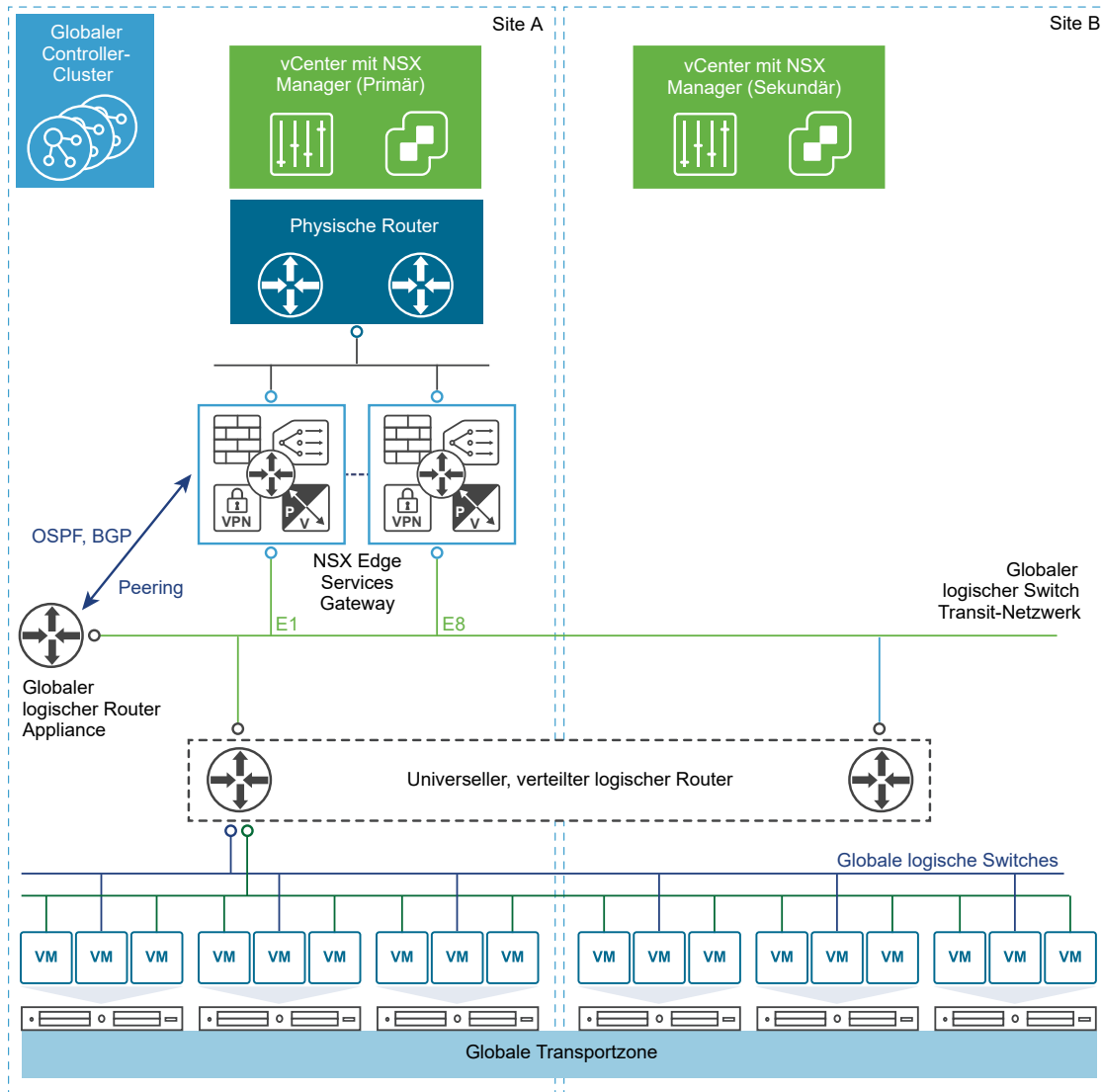


Abbildung 4-2. Cross-vCenter NSX, die zwei Sites umspannt



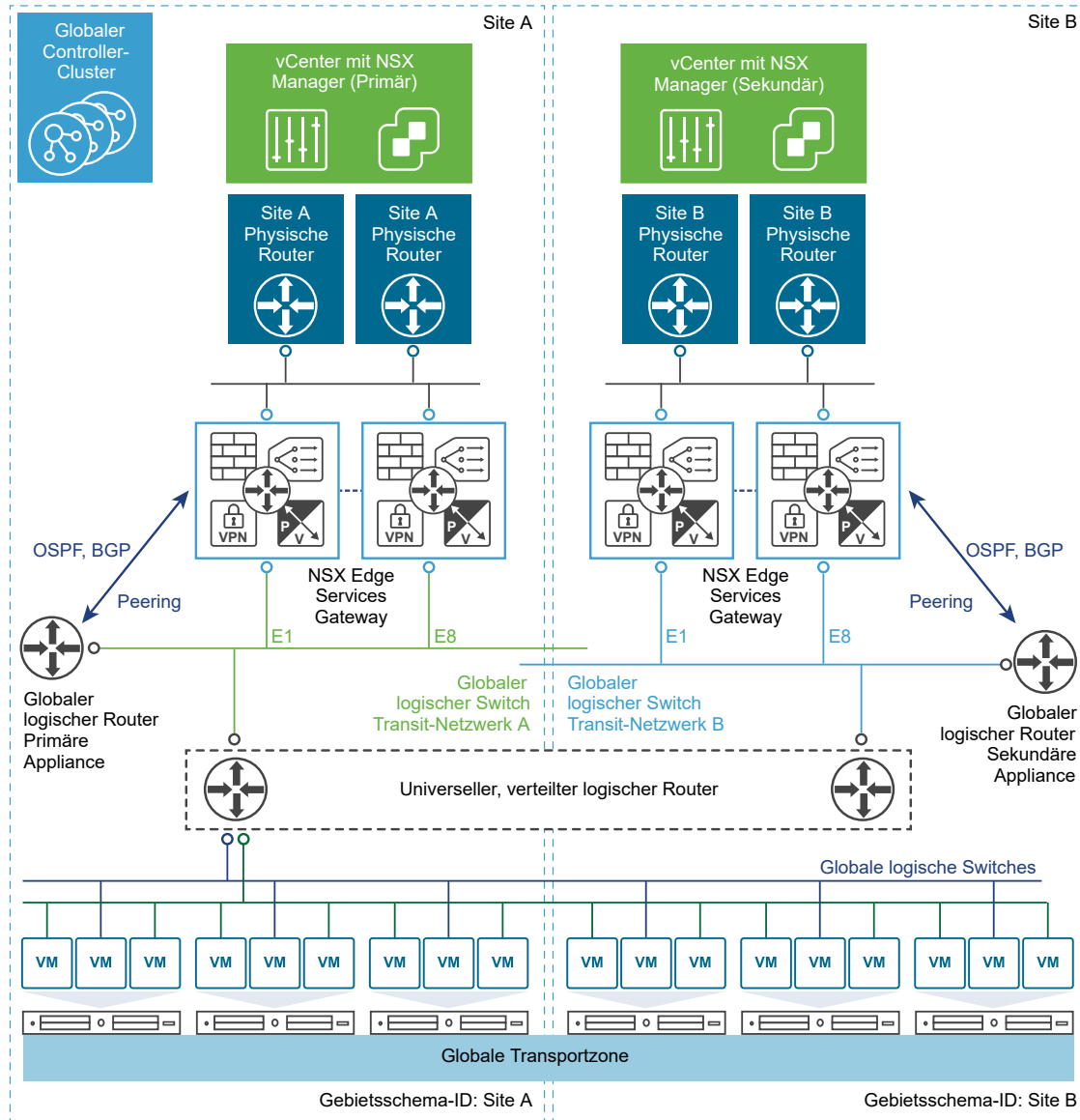
Lokaler Ausgang

Alle Sites einer Multi-Site-Umgebung von Cross-vCenter NSX können für den ausgehenden Datenverkehr dieselben physischen Router verwenden. Wenn die Routen für den ausgehenden Datenverkehr allerdings angepasst werden müssen, muss beim Erstellen des globalen logischen Routers die Funktion „Lokaler Ausgang“ aktiviert werden.

Über einen lokalen Ausgang können Sie Routen am globalen logischen Router, im Cluster oder auf Hostebene anpassen. In diesem Beispiel einer Cross-vCenter NSX-Umgebung mit mehreren Sites ist der lokale Ausgang aktiviert. Die Edge Services Gateways (ESGs) an jeder Site haben eine Standardroute, auf die der Datenverkehr über die physischen Router dieser Site gesendet wird. Der globale logische Router ist mit zwei Appliances konfiguriert, eine für jede Site. Die Appliances erlernen die Routen von den ESGs ihrer Site. Die erlernten Routen werden an den globalen Controller-Cluster gesendet. Da der lokale

Ausgang aktiviert ist, wird diesen Routen die Gebietsschema-ID für diese Site zugewiesen. Der globale Controller-Cluster sendet die Routen mit den passenden Gebietsschema-IDs an die Hosts. Routen, die an der Site A-Appliance erlernt wurden, werden an die Hosts auf Site A gesendet, und die Routen, die an der Site B-Appliance erlernt wurden, werden an die Hosts auf Site B gesendet.

Weitere Informationen zum lokalen Ausgang finden Sie im *Cross-vCenter NSX-Design-Handbuch* unter <https://communities.vmware.com/docs/DOC-32552>.



Ändern der NSX Manager-Rollen

Ein NSX Manager kann über Rollen verfügen, z. B. primär, sekundär, eigenständig oder Transit-Status. Auf dem primären NSX Manager läuft spezielle Synchronisierungssoftware, die alle globalen Objekte auf sekundäre NSX Manager synchronisiert.

Es ist wichtig zu verstehen, was passiert, wenn Sie die Rolle eines NSX Manager ändern.

Als primär festlegen

Mit diesem Vorgang wird die Rolle eines NSX Manager als primär festgelegt und die Synchronisierungssoftware gestartet. Dieser Vorgang schlägt fehl, wenn NSX Manager bereits die primäre oder eine sekundäre Rolle einnimmt.

Als eigenständig festlegen (von sekundär)

Dieser Vorgang legt die Rolle von NSX Manager auf den eigenständigen oder Transitmodus fest. Dieser Vorgang schlägt möglicherweise fehl, wenn NSX Manager bereits die eigenständige Rolle einnimmt.

Als eigenständig festlegen (von primär)

Dieser Vorgang setzt den primären NSX Manager auf den eigenständigen oder Transitmodus zurück, beendet die Synchronisierungssoftware und entfernt alle sekundären NSX Manager aus der Registrierung. Dieser Vorgang schlägt möglicherweise fehl, wenn NSX Manager bereits die eigenständige Rolle einnimmt oder einer der sekundären NSX Manager nicht erreichbar ist.

Verbindung zum primären Manager trennen

Wenn Sie diesen Vorgang auf einem sekundären NSX Manager ausführen, wird der sekundäre NSX Manager einseitig vom primären NSX Manager getrennt. Dieser Vorgang sollte verwendet werden, wenn auf dem primären NSX Manager ein nicht behebbarer Fehler aufgetreten ist und Sie den sekundären NSX Manager bei einem neuen primären Manager registrieren möchten. Wenn der ursprüngliche primäre NSX Manager wieder funktionsfähig ist, führt dessen Datenbank den sekundären NSX Manager weiterhin als registriert auf. Um dieses Problem zu beheben, verwenden Sie die Option **force**, wenn Sie den sekundären Manager vom ursprünglichen primären Manager trennen oder die Registrierung aufheben möchten. Mit der Option **force** wird der sekundäre NSX Manager aus der Datenbank des ursprünglichen primären NSX Manager entfernt.

Transportzonen

5

Eine Transportzone steuert, welche Hosts ein logischer Switch erreichen kann. Sie kann einen oder mehrere vSphere-Cluster umfassen. Transportzonen bestimmen, welche Cluster und damit auch welche VMs bei der Verwendung eines bestimmten Netzwerks teilnehmen können. In einer Cross-vCenter NSX-Umgebung können Sie eine universelle Transportzone erstellen, die Cluster aus beliebigen vCenter-Instanzen in der Umgebung umfassen kann. Sie können nur eine universelle Transportzone erstellen.

Eine NSX-Umgebung kann je nach Ihren Anforderungen mindestens eine Transportzone enthalten. Ein Hostcluster kann zu mehreren Transportzonen gehören. Ein logischer Switch kann jeweils nur zu einer Transportzone gehören.

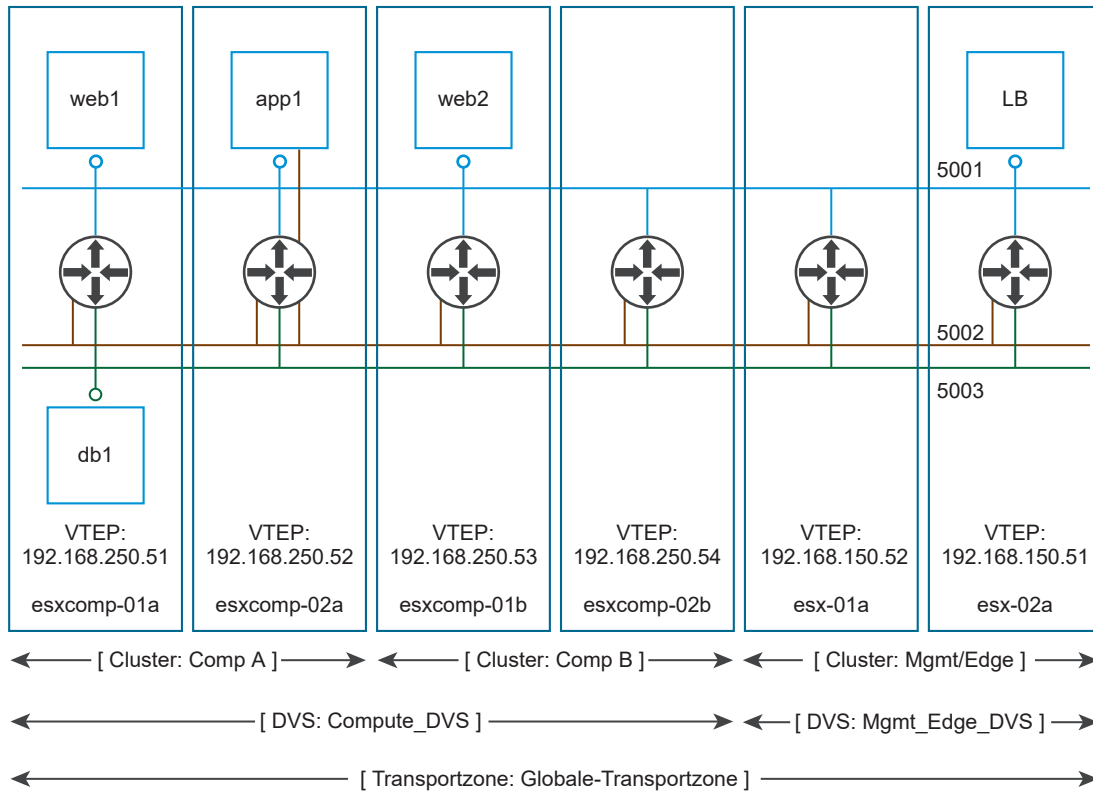
NSX lässt nicht die Verbindung von VMs zu, die sich in unterschiedlichen Transportzonen befinden. Die Spannweite eines logischen Switches ist auf eine Transportzone begrenzt, sodass sich virtuelle Maschinen in unterschiedlichen Transportzonen nicht im selben Schicht 2-Netzwerk befinden können. Ein Distributed Logical Router kann keine Verbindung zu logischen Switches herstellen, die sich in unterschiedlichen Transportzonen befinden. Nachdem Sie den ersten logischen Switch verbunden haben, ist die Auswahl von weiteren logischen Switches auf diejenigen begrenzt, die sich in derselben Transportzone befinden.

Mit den folgenden Richtlinien können Sie die Transportzonen entwerfen.

- Wenn ein Cluster Schicht 3-Konnektivität erfordert, muss sich der Cluster in einer Transportzone befinden, die auch einen Edge-Cluster enthält, d. h. einen Cluster mit Schicht 3-Edge-Geräten (Distributed Logical Router und Edge Services Gateways).
- Angenommen, Sie haben zwei Cluster, einen für Webdienste und einen anderen für Anwendungsdienste. Für VXLAN-Konnektivität zwischen den VMs in diesen zwei Clustern müssen beide Cluster in der Transportzone enthalten sein.
- Beachten Sie, dass alle logischen Switches, die in der Transportzone enthalten sind, für alle VMs innerhalb der Cluster verfügbar und sichtbar sind, die in der Transportzone enthalten sind. Wenn ein Cluster gesicherte Umgebungen enthält, möchten Sie ihn möglicherweise nicht für VMs in anderen Clustern verfügbar machen. Sie können stattdessen den sicheren Cluster in einer isolierteren Transportzone ablegen.

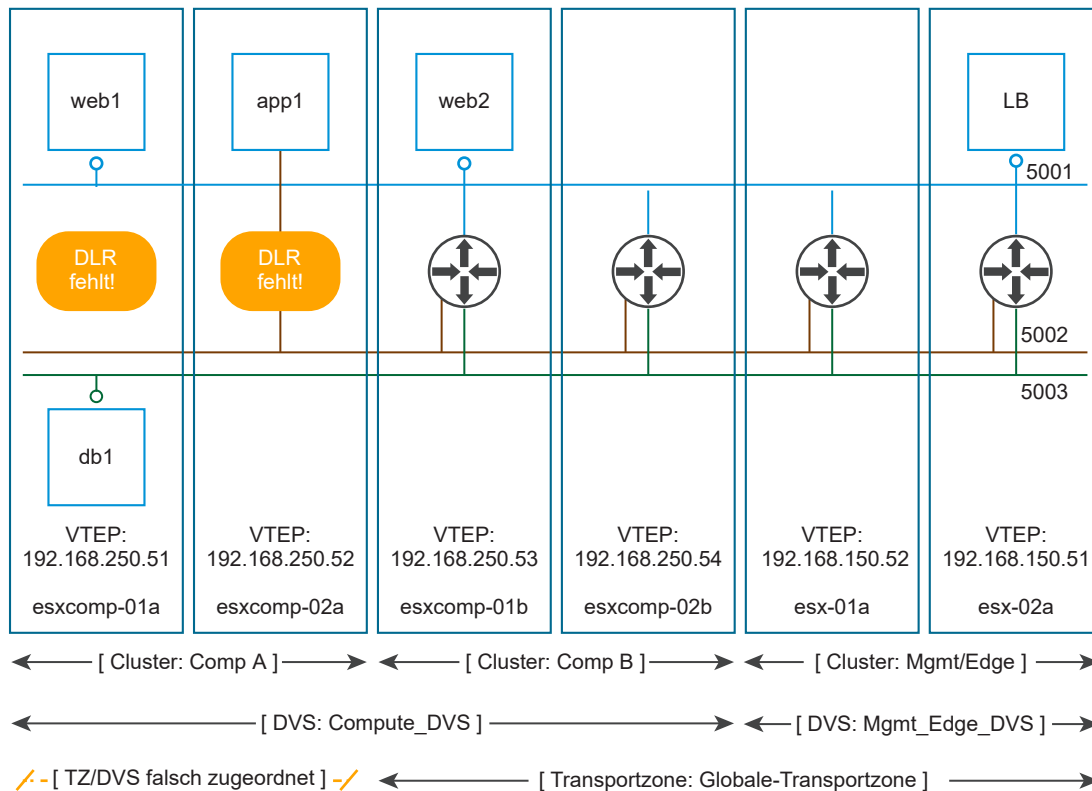
- Die Spannweite des vSphere Distributed Switch (VDS oder DVS) sollte der Spannweite der Transportzone entsprechen. Stellen Sie beim Erstellen von Transportzonen in Multi-Cluster-VDS-Konfigurationen sicher, dass alle Cluster in dem ausgewählten VDS in der Transportzone enthalten sind. Dadurch wird sichergestellt, dass der DLR in allen Clustern verfügbar ist, in denen auch VDS dvPortgroups verfügbar sind.

Das folgende Diagramm zeigt eine Transportzone, die korrekt an der VDS-Begrenzung ausgerichtet ist.



Wenn Sie die bewährte Methode nicht befolgen, sollten Sie Folgendes beachten: Wenn ein VDS mehr als einen Hostcluster umfasst und die Transportzone nur einen (oder eine Teilmenge) dieser Cluster enthält, können alle in dieser Transportzone enthaltenen logischen Switches auf VMs innerhalb aller Cluster zugreifen, die von dem VDS umfasst werden. Mit anderen Worten, die Transportzone kann nicht die Spannweite der logischen Switches auf eine Teilmenge der Cluster beschränken. Wenn dieser logische Switch zu einem späteren Zeitpunkt mit einem DLR verbunden wird, müssen Sie sicherstellen, dass die Router-Instanzen nur in dem Cluster erstellt werden, der in der Transportzone enthalten ist, um Probleme mit Schicht 3 zu vermeiden.

Beispiel: Wenn eine Transportzone nicht an der VDS-Begrenzung ausgerichtet ist, wird der Geltungsbereich der logischen Switches (5001, 5002 und 5003) und die DLR-Instanzen, mit denen diese logischen Switches verbunden sind, getrennt, sodass VMs in Cluster Comp A keinen Zugriff auf die logischen Schnittstellen von DLR (LIFs) haben.



Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen einer Transportzone](#)
- [Anzeigen und Bearbeiten einer Transportzone](#)
- [Erweitern einer Transportzone](#)
- [Kontrahieren einer Transportzone](#)
- [Modus für den Betrieb mit getrenntem Controller \(CDO\)](#)

Hinzufügen einer Transportzone

Eine Transportzone kontrolliert, welche Hosts von einem logischen Switch erreicht werden können, und kann einen oder mehrere vSphere-Cluster umspannen. Transportzonen bestimmen, welche Cluster und damit auch welche VMs bei der Verwendung eines bestimmten Netzwerks teilnehmen können. Globale Transportzonen können sich über vSphere-Cluster in einer Cross-vCenter NSX-Umgebung erstrecken.

Es darf nur eine globale Transportzone in einer Cross-vCenter NSX-Umgebung vorhanden sein.

Voraussetzungen

Legen Sie den entsprechenden NSX Manager fest, bei dem Sie Änderungen durchführen möchten.

- In einer eigenständigen oder einzelnen vCenter NSX-Umgebung gibt es nur einen NSX Manager, sodass Sie keinen auswählen müssen.
- Universelle Objekte müssen vom primären NSX Manager verwaltet werden.

- Lokale Objekte einer NSX Manager-Instanz müssen von diesem NSX Manager aus verwaltet werden.
- In einer Cross-vCenter NSX-Umgebung, in der der erweiterte verknüpfte Modus nicht aktiviert ist, müssen Sie Konfigurationsänderungen von der vCenter-Instanz aus vornehmen, die mit dem NSX Manager verknüpft ist, den Sie ändern möchten.
- In einer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus können Sie Konfigurationsänderungen an beliebigen NSX Manager-Instanzen von jeder verknüpften vCenter-Instanz aus vornehmen. Wählen Sie den geeigneten NSX Manager aus dem Dropdown-Menü „NSX Manager“ aus.

Verfahren

- 1 Wechseln Sie zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** aus.
- 2 Klicken Sie auf **Transportzonen (Transport Zones)** und anschließend auf das Symbol **Neue Transportzone (New Transport Zone) (+)**.
- 3 (Optional) Wählen Sie **Dieses Objekt für globale Synchronisierung markieren (Mark this object for universal synchronization)**, um eine globale Transportzone hinzuzufügen.
- 4 Wählen Sie den Replizierungs-Modus aus:
 - **Multicast:** Multicast-IP-Adressen auf dem physischen Netzwerk werden für die Steuerungskomponente verwendet. Dieser Modus wird nur empfohlen, wenn Sie Upgrades von älteren VXLAN-Bereitstellungen aus durchführen wollen. Erfordert PIM/IGMP im physischen Netzwerk.
 - **Unicast:** Die Steuerungskomponente wird von einem NSX Controller verwendet. Der komplette Unicast-Datenverkehr verwendet die optimierte Kopfendereplikation. Es sind keine Multicast-IP-Adressen oder bestimmte Netzwerkkonfigurationen erforderlich.
 - **Hybrid:** Lagert eine Replizierung des lokalen Datenverkehrs auf das physische Netzwerk aus (L2 Multicast). Erfordert IGMP-Snooping auf dem ersten Hop-Switch und Zugriff auf einen IGMP-Abfrager in jedem VTEP-Subnetz, aber keinen PIM. Der erste Hop-Switch steuert die Datenverkehrsreplizierung für das Subnetz.

Wichtig Wenn Sie eine universelle Transportzone erstellen und als Replizierungsmodus den Hybridmodus auswählen, müssen Sie sicherstellen, dass die verwendete Multicast-Adresse nicht mit einer auf einen NSX Manager in der Umgebung zugewiesenen Multicast-Adresse in Konflikt steht.

- 5 Wählen Sie die Cluster aus, die zur Transportzone hinzugefügt werden sollen.

Ergebnisse

Transport-Zone ist eine Transportzone, die für den NSX Manager, auf dem sie erstellt worden ist, gilt.

Universal-Transport-Zone ist eine globale Transportzone, die auf allen NSX Managern in einer Cross-vCenter NSX-Umgebung verfügbar ist.

Name	1 ▲ Description	Control Plane Mode	Logical Switches
Transport-Zone		Unicast	1
Universal-Transport-Zone		Unicast	4

Nächste Schritte

Wenn Sie eine Transportzone hinzugefügt haben, können Sie logische Switches hinzufügen.

Wenn Sie eine globale Transportzone hinzugefügt haben, können Sie globale logische Switches hinzufügen.

Wenn Sie eine globale Transportzone hinzugefügt haben, können Sie die sekundären NSX Manager auswählen und ihre Cluster zur globalen Transportzone hinzufügen.

Anzeigen und Bearbeiten einer Transportzone

Sie können die logischen Netzwerke in einer ausgewählten Transportzone, die Cluster in dieser Zone und den Steuerungskomponenten-Modus für diese Transportzone anzeigen.

Verfahren

- 1 Doppelklicken Sie in „Transportzonen“ auf eine Transportzone.

Die Registerkarte „Übersicht“ zeigt den Namen und die Beschreibung der Transportzone sowie die Anzahl der damit verbunden logischen Switches an. „Details zur Transportzone“ zeigt die Cluster in der Transportzone an.

- 2 Klicken Sie im Bereich **Details zur Transportzone (Transport Zone Details)** auf das Symbol **Einstellungen bearbeiten (Edit Settings)**, um den Namen, die Beschreibung oder den Steuerungskomponenten-Modus der Transportzone zu bearbeiten.

Wenn Sie den Steuerungskomponenten-Modus der Transportzone ändern, wählen Sie **Vorhandene logische Switches auf neuen Steuerungskomponenten-Modus migrieren (Migrate existing Logical Switches to the new control plane mode)**, um die Steuerungskomponente für weitere vorhandene logische Switches zu ändern, die mit dieser Transportzone verknüpft sind. Wenn Sie dieses Kontrollkästchen nicht aktivieren, haben nur die logischen Switches einen neuen Steuerungskomponenten-Modus, die mit dieser Transportzone verknüpft wurden, nachdem die Bearbeitung abgeschlossen wurde.

- 3 Klicken Sie auf **OK**.


Erweitern einer Transportzone

Sie können Cluster zu einer Transportzone hinzufügen. Alle vorhandenen Transportzonen werden auf den neu hinzugefügten Clustern verfügbar.

Voraussetzungen

Auf den Clustern, die Sie zu einer Transportzone hinzufügen, ist die Netzwerkinfrastruktur installiert, und die Cluster sind für VXLAN konfiguriert. Weitere Informationen finden Sie unter *Installationshandbuch für NSX*.


Verfahren

- 1 Klicken Sie unter „Transportzonen“ auf eine Transportzone.
- 2 Klicken Sie auf das Symbol **Cluster hinzufügen (Add Cluster)** ().
- 3 Wählen Sie die Cluster aus, die Sie zur Transportzone hinzufügen wollen und klicken Sie auf **OK**.

Kontrahieren einer Transportzone

Sie können Cluster aus einer Transportzone entfernen. Die Größe der vorhandenen Transportzonen wird reduziert und an den kleineren Bereich angepasst.

Verfahren

- 1 Doppelklicken Sie in **Transportzonen (Transport Zones)** auf eine Transportzone.
- 2 Klicken Sie in **Details zur Transportzone (Transport Zones Details)** auf das Symbol **Cluster entfernen (Remove Clusters)** ().
- 3 Wählen Sie die Cluster aus, die Sie entfernen möchten.
- 4 Klicken Sie auf **OK**.

Modus für den Betrieb mit getrenntem Controller (CDO)

Mithilfe des CDO-Modus wird sichergestellt, dass die Konnektivität auf Datenebene nicht beeinträchtigt wird, wenn Hosts die Konnektivität mit dem Controller verlieren. Durch Aktivierung des CDO-Modus können Sie vermeiden, dass vorübergehende Konnektivitätsprobleme mit dem Controller auftreten.

Sie können den CDO-Modus für jeden Hostcluster, der mit einer Transportzone verbunden ist, aktivieren. Standardmäßig ist der CDO-Modus deaktiviert.

Hinweis Für die Aktivierung des CDO-Modus müssen alle vorbereiteten Hosts im System auf NSX 6.3.2 oder höher aktualisiert werden.

Bei aktiviertem CDO-Modus erstellt NSX Manager einen speziellen logischen CDO-Switch, und zwar einen für jede Transportzone. Die VXLAN-Netzwerkennung (VNI) des speziellen logischen CDO-Switches unterscheidet sich eindeutig von allen anderen logischen Switches. Bei aktiviertem CDO-Modus ist ein Controller im Cluster für die Erfassung aller VTEP-Informationen zuständig, die von allen Transportknoten gemeldet wurden. Zudem repliziert er die aktualisierten VTEP-Informationen auf alle anderen Transportknoten. Wenn ein Controller fehlschlägt, wird ein neuer Controller als neuer Master gewählt, der diese Zuständigkeit übernimmt. Zudem werden alle mit dem ursprünglichen Master verbundenen Transportknoten auf den neuen Master migriert, und die Daten werden zwischen den Transportknoten und den Controllern synchronisiert.

Wenn Sie einer Transportzone einen neuen Cluster hinzufügen, leitet NSX Manager die Einstellung für den CDO-Modus und die VNI an die neu hinzugefügten Hosts weiter. Wenn Sie den Cluster entfernen, entfernt NSX Manager die VNI-Daten von den Hosts.

Wenn Sie den CDO-Modus in einer Transportzone deaktivieren, entfernt NSX Manager den logischen CDO-Switch vom Controller.

In einer Cross-vCenter NSX-Umgebung können Sie den CDO-Modus nur für die lokalen Transportzonen oder in einer Topologie aktivieren, in der keine lokalen Transportzonen existieren und in der für den primären NSX Manager eine einzelne globale Transportzone vorhanden ist. Der CDO-Modus wird in der globalen Transportzone für alle sekundären NSX Manager repliziert.

Sie können den CDO-Modus in der lokalen Transportzone für sekundäre NSX Manager aktivieren.

Aktivieren des Modus für den Betrieb mit getrenntem Controller (CDO)

Sie können den CDO-Modus für jedes Host-Cluster über die Transportzone aktivieren. Standardmäßig ist der CDO-Modus deaktiviert.

Voraussetzungen

- Stellen Sie sicher, dass für alle vorbereiteten Hosts im System ein Upgrade auf NSX 6.3.2 oder höher durchgeführt wurde.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security > Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und dann auf **Transportzonen (Transport Zones)**.
- 3 Wählen Sie die erforderliche Transportzone aus und klicken Sie auf das Symbol **Aktionen (Actions)**. Sie können auch mit der rechten Maustaste auf die Transportzone klicken.
- 4 Klicken Sie auf **CDO-Modus aktivieren (Enable CDO mode)**.

Ein Dialogfeld zur Bestätigung wird geöffnet.

Hinweis Wenn Sie eine Fehlermeldung in einer Cross-vCenter NSX-Umgebung erhalten, überprüfen Sie die folgenden Zustände:

- Primärer NSX Manager: Sie können den CDO-Modus nur in Transportzonen aktivieren, die nicht denselben verteilten virtuellen Switch verwenden. Wenn die globale Transportzone und die lokalen Transportzonen denselben verteilten virtuellen Switch verwenden, kann der CDO-Modus nur für die globale Transportzone aktiviert werden.
 - Sekundärer NSX Manager: Der CDO-Modus wird für alle sekundären NSX Manager in der globalen Transportzone repliziert. Sie können den CDO-Modus für lokale Transportzonen aktivieren, wenn sie nicht denselben verteilten virtuellen Switch verwenden.
-

- 5 Klicken Sie auf **Ja (Yes)**.

Der CDO-Modus wird für die ausgewählte Transportzone aktiviert.

Ergebnisse

In der Spalte „CDO-Modus“ wird der Status **Aktiviert (Enabled)** angezeigt.

NSX Manager erstellt auf dem Controller einen logischen CDO-Switch.

Deaktivieren des Modus für den Betrieb mit getrenntem Controller (CDO)

Sie können den bereits aktivierten Modus für den Betrieb mit getrenntem Controller (Controller Disconnected Operation, CDO) über die Transportzone deaktivieren, wenn die Verbindungsprobleme mit dem Controller behoben sind. Standardmäßig bleibt der CDO-Modus deaktiviert.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security > Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und dann auf **Transportzonen (Transport Zones)**.
- 3 Wählen Sie die Transportzone aus, in der Sie den CDO-Modus deaktivieren möchten, und klicken Sie auf das Symbol **Aktionen (Actions)**. Sie können auch mit der rechten Maustaste auf die Transportzone klicken.
- 4 Klicken Sie auf **CDO-Modus deaktivieren (Disable CDO mode)**.
Ein Dialogfeld zur Bestätigung wird geöffnet.
- 5 Klicken Sie auf **Ja (Yes)**.
Der CDO-Modus wird für die ausgewählte Transportzone deaktiviert.

Ergebnisse

In der Spalte „CDO-Modus“ wird der Status **Deaktiviert (Disabled)** angezeigt.

NSX Manager entfernt den logischen CDO-Switch vom Controller.

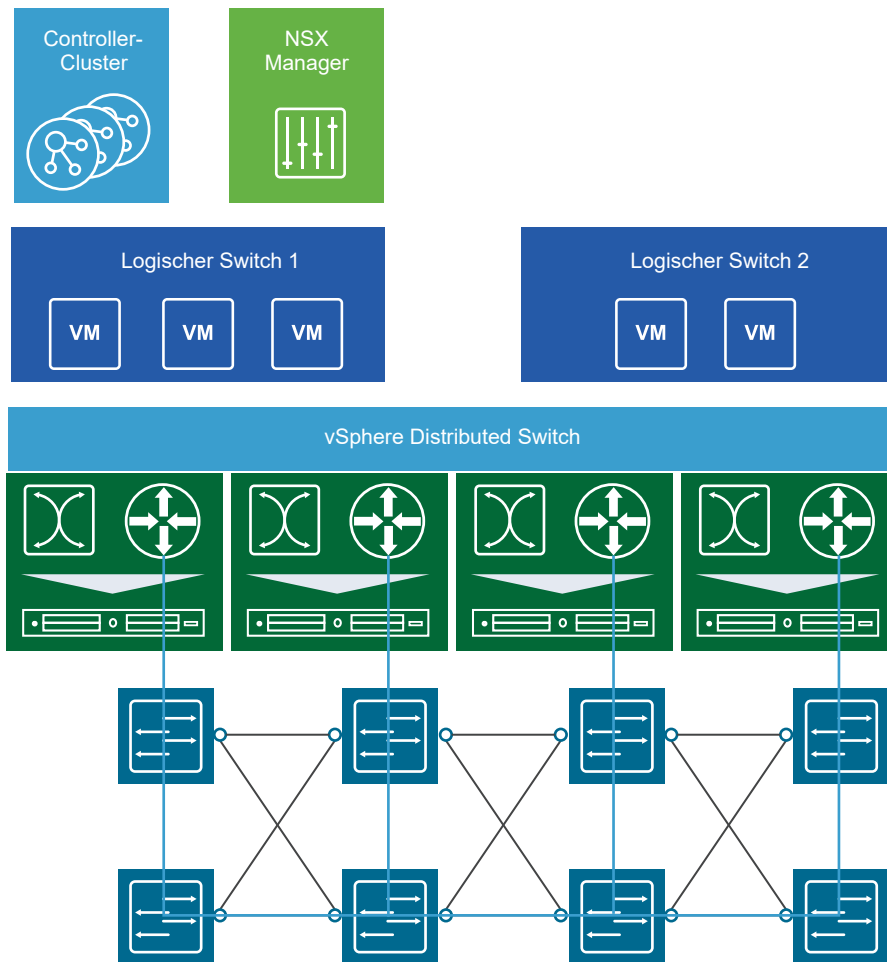
Logische Switches

6

Eine Cloud-Bereitstellung oder ein virtuelles Datencenter enthalten diverse Anwendungen für zahlreiche Mandanten. Diese Anwendungen und Mandanten müssen aus Sicherheitsgründen, für Fehlerisolierungszwecke und zur Vermeidung von Problemen durch sich überschneidende IP-Adressen voneinander isoliert werden. Der logische NSX-Switch erstellt logische Broadcast-Domänen oder Segmente, mit denen die VM einer Anwendung oder eines Mandanten logisch verbunden werden kann. Dies ermöglicht eine schnelle, flexible Bereitstellung bei gleichzeitiger Wahrung aller Vorteile von Broadcast-Domänen eines physischen Netzwerks (VLANs) ohne die Probleme von physischen Schicht-2-Sprawls und ohne Spanning-Tree-Probleme.

Ein logischer Switch wird verteilt und kann sich über beliebig große Rechnercluster erstrecken. Dies ermöglicht die Mobilität virtueller Maschinen (vMotion) innerhalb des Datencenters ohne Beschränkungen durch die Grenzen der physischen Schicht 2 (VLAN). Die physische Infrastruktur ist nicht an MAC/FIB-Tabellengrenzen gebunden, weil die Broadcast-Domäne beim logischen Switch in der Software enthalten ist.

Ein logischer Switch wird einem eindeutigen VXLAN zugeordnet, das den Datenverkehr virtueller Maschinen kapselt und über das physische IP-Netzwerk transportiert.



Der NSX Controller ist der zentrale Kontrollpunkt für alle logischen Switches innerhalb eines Netzwerks und pflegt Informationen von allen virtuellen Maschinen, Hosts, logischen Switches und VXLANs. Der Controller unterstützt zwei neue logische Switch-Steuerungskomponentenmodi, Unicast und Hybrid. Diese Modi koppeln NSX vom physischen Netzwerk ab. VXLANs benötigen das physische Netzwerk nicht mehr, um Multicast für die Verarbeitung von BUM-Datenverkehr (Broadcast, unbekanntes Unicast und Multicast) in einem logischen Switch zu unterstützen. Der Unicast-Modus repliziert den gesamten BUM-Datenverkehr lokal auf dem Host und benötigt keine physische Netzwerkkonfiguration. Im Hybrid-Modus wird ein Teil der BUM-Datenverkehrsreplizierung zum ersten physischen Hop-Switch ausgelagert, um eine bessere Leistung zu erreichen. Für diesen Modus muss IGMP Snooping auf dem physischen Switch des ersten Hop aktiviert sein. Virtuelle Maschinen innerhalb eines logischen Switches können jede Art von Datenverkehr nutzen und senden, einschließlich IPv6 und Multicast.

Sie können einen logischen Switch durch Hinzufügen einer L2-Bridge auf ein physisches Gerät erweitern. Weitere Informationen dazu finden Sie unter [Kapitel 8 L2-Bridges](#).

Für die Verwaltung logischer Switches benötigen Sie die Berechtigungen der Rolle als „Super Administrator“ oder „Enterprise-Administrator“.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen eines logischen Switch](#)

- [Verbinden von virtuellen Maschinen mit einem logischen Switch](#)
- [Testen der Konnektivität eines logischen Switches](#)
- [Verhindern von Manipulationen auf einem logischen Switch](#)
- [Bearbeiten eines logischen Switches](#)
- [Szenario für einen logischen Switch](#)

Hinzufügen eines logischen Switch

Voraussetzungen

- Sie verfügen über die Rollenberechtigung als „Super Administrator“ oder „Enterprise-Administrator“, um logische Switches zu konfigurieren und zu verwalten.
- Der VXLAN UDP-Port ist auf Firewallregeln geöffnet (sofern zutreffend). Der VXLAN UDP-Port kann durch die API konfiguriert werden.
- Die MTU der physischen Infrastruktur beträgt mindestens 50 Bytes mehr als die MTU der vNIC der virtuellen Maschine.
- Die verwaltete IP-Adresse wird für jeden vCenter Server in den Laufzeiteinstellungen von vCenter Server festgelegt. Weitere Informationen hierzu finden Sie unter *vCenter Server und Hostverwaltung*.
- DHCP ist auf Transport-VLANs für VXLAN verfügbar, wenn Sie DHCP für die IP-Zuweisung für VMKNics verwenden.
- Es muss ein konsistenter verteilter virtueller Switch-Typ (Anbieter usw.) über eine bestimmte Transportzone hinweg verwendet werden. Inkonsistente Switch-Typen können ein nicht definiertes Verhalten im logischen Switch verursachen.
- Sie haben eine entsprechende LACP-Gruppierungsrichtlinie konfiguriert und die Verbindung physischer NICs mit den Ports hergestellt. Weitere Informationen zu Gruppierungsmodi finden Sie in der Dokumentation zu VMware vSphere.
- „5-Tuple Hash Distribution“ ist für LACP (Link Aggregation Control Protocol) aktiviert.
- Vergewissern Sie sich, dass für jeden Host, auf dem Sie LACP verwenden, ein separater LACP-Port auf dem verteilten virtuellen Switch vorhanden ist.
- Für den Multicast-Modus ist Multicast-Routing aktiviert, wenn VXLAN-Datenverkehr Router durchläuft. Sie haben einen Multicast-Adressbereich von Ihrem Netzwerkadministrator erhalten.
- Port 1234 (der überwachende Standard-Port des Controllers) ist auf der Firewall für den ESXi-Host für die Kommunikation mit Controllern geöffnet.
- (Empfohlen) Für Multicast- und Hybrid-Modi haben Sie IGMP-Snooping auf den L2-Switches aktiviert, zu denen Hosts, die bei VXLAN teilnehmen, hinzugefügt wurden. Wenn IGMP-Snooping auf L2 aktiviert ist, muss der IGMP-Abfrager auf dem Router oder L3-Switch mit Konnektivität zu Multicast-aktivierten Netzwerken aktiviert sein.

Hinzufügen eines logischen Switch

Ein logischer NSX-Switch bildet die Switching-Funktionalität (Unicast, Multicast, Broadcast) in einer virtuellen Umgebung ab, die vollständig von der zugrunde liegenden physischen Hardware entkoppelt ist. Logische Switches sind mit VLANs insofern vergleichbar, da sie Netzwerkverbindungen bereitstellen, an die virtuelle Maschinen angefügt werden können. Logische Switches sind lokal für eine einzelne vCenter NSX-Bereitstellung. In einer Cross-vCenter NSX-Bereitstellung können Sie globale logische Switches erstellen, die alle vCenter überspannen können. Die Transportzone bestimmt, ob der neue Switch ein logischer oder ein globaler logischer Switch ist.

Wenn Sie einen logischen Switch erstellen, müssen Sie zusätzlich zur Auswahl einer Transportzone und eines Replizierungsmodus zwei Optionen konfigurieren: die IP-Ermittlung und der MAC-Lernvorgang.

Die IP-Ermittlung minimiert das Fluten durch den ARP-Datenverkehr innerhalb einzelner VXLAN-Segmente – mit anderen Worten zwischen VMs, die mit demselben logischen Switch verbunden sind. Die IP-Ermittlung ist standardmäßig aktiviert.

Hinweis Sie können die IP-Ermittlung nicht deaktivieren, wenn Sie einen globalen logischen Switch erstellen. Sie haben aber die Möglichkeit, die IP-Ermittlung nach der Erstellung des globalen logischen Switch über die API zu deaktivieren. Diese Einstellung wird auf jedem NSX Manager gesondert verwaltet. Weitere Informationen finden Sie unter *Handbuch zu NSX-API*.

Der MAC-Lernvorgang erstellt auf jeder vNIC eine VLAN/MAC-Paar-Lerntabelle. Diese Tabelle wird als Teil der dvfilter-Daten gespeichert. Während eines vMotion-Vorgangs speichert dvfilter die Tabelle und stellt sie am neuen Speicherort wieder her. Der Switch gibt anschließend RARPs für alle VLAN/MAC-Einträge in der Tabelle aus. Es kann sinnvoll sein, den MAC-Lernvorgang zu aktivieren, wenn Sie virtuelle Netzwerkkarten verwenden, die VLAN-Trunking vornehmen.

Voraussetzungen

Tabelle 6-1. Voraussetzungen für die Erstellung von logischen oder globalen logischen Switches.

Logischer Switch	Globaler logischer Switch
<ul style="list-style-type: none"> ■ vSphere Distributed Switches müssen konfiguriert werden. ■ NSX Manager muss installiert sein. ■ Controller müssen bereitgestellt werden. ■ Hostcluster müssen für NSX vorbereitet werden. ■ VXLAN muss konfiguriert werden. ■ Ein Segment-ID-Pool muss konfiguriert werden. ■ Eine Transportzone muss erstellt werden. 	<ul style="list-style-type: none"> ■ vSphere Distributed Switches müssen konfiguriert werden. ■ NSX Manager muss installiert sein. ■ Controller müssen bereitgestellt werden. ■ Hostcluster müssen für NSX vorbereitet werden. ■ VXLAN muss konfiguriert werden. ■ Es muss ein primärer NSX Manager zugewiesen sein. ■ Es muss ein globaler Segment-ID-Pool konfiguriert sein. ■ Es muss eine globale Transportzone erstellt sein.

Legen Sie den entsprechenden NSX Manager fest, bei dem Sie Änderungen durchführen möchten.

- In einer eigenständigen oder einzelnen vCenter NSX-Umgebung gibt es nur einen NSX Manager, sodass Sie keinen auswählen müssen.

- Universelle Objekte müssen vom primären NSX Manager verwaltet werden.
- Lokale Objekte einer NSX Manager-Instanz müssen von diesem NSX Manager aus verwaltet werden.
- In einer Cross-vCenter NSX-Umgebung, in der der erweiterte verknüpfte Modus nicht aktiviert ist, müssen Sie Konfigurationsänderungen von der vCenter-Instanz aus vornehmen, die mit dem NSX Manager verknüpft ist, den Sie ändern möchten.
- In einer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus können Sie Konfigurationsänderungen an beliebigen NSX Manager-Instanzen von jeder verknüpften vCenter-Instanz aus vornehmen. Wählen Sie den geeigneten NSX Manager aus dem Dropdown-Menü „NSX Manager“ aus.

Verfahren

- 1 Wechseln Sie zu **Home > Netzwerk und Sicherheit > Logische Switches (Home > Networking & Security > Logical Switches)**:
- 2 Wählen Sie den NSX Manager aus, auf dem Sie den logischen Switch erstellen möchten. Um einen globalen logischen Switch zu erstellen, müssen Sie den primären NSX Manager auswählen.
- 3 Klicken Sie auf **Neuer logischer Switch (New Logical Switch) (+)**.
- 4 Geben Sie einen Namen und eine optionale Beschreibung für den logischen Switch ein.
- 5 Wählen Sie die Transportzone aus, in der Sie den logischen Switch erstellen möchten. Wenn Sie eine globale Transportzone ausgewählt haben, können Sie nur einen globalen logischen Switch erstellen.

Standardmäßig übernimmt der logische Switch den Steuerungskomponenten-Modus der Replikation aus der Transportzone. Sie können auch einen anderen verfügbaren Modus auswählen. Die verfügbaren Modi sind Unicast, Hybrid und Multicast.

Wenn Sie einen universellen logischen Switch erstellen und als Replizierungsmodus den Hybridmodus auswählen, müssen Sie sicherstellen, dass die verwendete Multicast-Adresse nicht mit anderen Multicast-Adressen in Konflikt steht, die auf einem NSX Manager in der Cross-vCenter NSX-Umgebung zugewiesen wurden.
- 6 (Optional) Klicken Sie auf **IP-Erkennung aktivieren (Enable IP Discovery)**, um die ARP-Unterdrückung zu aktivieren.
- 7 (Optional) Klicken Sie auf **MAC-Lernvorgang aktivieren (Enable MAC learning)**.

Beispiel: Logischer Switch und globaler logischer Switch

Die App ist ein logischer Switch, der mit einer Transportzone verbunden ist. Er ist nur auf dem NSX Manager verfügbar, auf dem er erstellt worden ist.

Universal-App ist ein globaler logischer Switch, der mit einer globalen Transportzone verbunden ist. Er ist auf jedem NSX Manager innerhalb der Cross-vCenter NSX-Umgebung verfügbar.

Der logische Switch und der globale logische Switch haben Segment-IDs aus unterschiedlichen Segment-ID-Pools.

Virtual Wire ID	Segment ID	Name	1 ▲	Status	Transport Zone
virtualwire-1	5000	App		✓ Normal	Transport-Zone
universalwire-2	900000	Universal-App		✓ Normal	Universal-Transport-Zone

Nächste Schritte

Fügen Sie VMs zu einem logischen Switch oder einem globalen logischen Switch hinzu.

Erstellen Sie einen logischen Router und fügen Sie ihn an die logischen Switches an, um die Konnektivität zwischen VMs zu aktivieren, die mit verschiedenen logischen Switches verbunden sind.

Erstellen Sie einen universellen logischen Router und fügen Sie ihn an die universellen logischen Switches an, um die Konnektivität zwischen VMs zu aktivieren, die mit verschiedenen universellen logischen Switches verbunden sind.

Verbinden eines logischen Switch mit einem NSX Edge

Das Verbinden eines logischen Switch mit einem NSX Edge Services Gateway oder logischen NSX Edge-Router stellt horizontales Datenverkehrs-Routing (zwischen den logischen Switches) oder vertikales Datenverkehr-Routing zur Außenwelt oder zur Bereitstellung erweiterter Dienste bereit.

Verfahren

Verfahren

- 1 Wählen Sie in „Logische Switches“ den logischen Switch aus, zu dem Sie eine Verbindung mit NSX Edge herstellen möchten.
- 2 Klicken Sie auf das Symbol **Edge verbinden (Connect an Edge)** ().
- 3 Wählen Sie das NSX Edge aus, mit dem Sie den logischen Switch verbinden möchten, und klicken Sie auf **Weiter (Next)**.
- 4 Wählen Sie die Schnittstelle aus, die Sie mit dem logischen Switch verbinden möchten, und klicken Sie auf **Weiter (Next)**.

Ein logisches Netzwerk wird in der Regel mit einer internen Schnittstelle verbunden.

- 5 Geben Sie auf der Seite „NSX Edge-Schnittstelle bearbeiten“ einen Namen für die NSX Edge-Schnittstelle ein.
- 6 Wählen Sie **Intern (Internal)** bzw. **Uplink**, um anzugeben, ob es sich um eine interne oder eine Uplink-Schnittstelle handelt.
- 7 Wählen Sie den Konnektivitätsstatus der Schnittstelle aus.
- 8 Wenn beim NSX Edge, mit dem Sie das logische Netzwerk verbinden, **Manuelle HA-Konfiguration (Manual HA Configuration)** ausgewählt ist, geben Sie zwei Verwaltungs-IP-Adressen im CIDR-Format ein.
- 9 Bearbeiten Sie die standardmäßige MTU, falls erforderlich.

10 Klicken Sie auf **Weiter (Next)**.

11 Überprüfen Sie die NSX Edge-Verbindungsdetails und klicken Sie auf **Beenden (Finish)**.


Bereitstellen von Diensten auf einem logischen Switch

Sie können Dienste von Drittanbietern auf einem logischen Switch bereitstellen.

Voraussetzungen

Eine oder mehrere virtuelle Drittanbieter-Appliances müssen in Ihrer Infrastruktur installiert sein.


Verfahren

- 1 Wählen Sie in **Logische Switches (Logical Switches)** den logischen Switch aus, über den Sie die Dienste bereitstellen möchten.
- 2 Klicken Sie auf das Symbol **Dienstprofil hinzufügen (Add Service Profile)** ().
- 3 Wählen Sie den Dienst und das Dienstprofil aus, die Sie übernehmen möchten.
- 4 Klicken Sie auf **OK**.

Verbinden von virtuellen Maschinen mit einem logischen Switch

Sie können virtuelle Maschinen mit einem logischen oder einem globalen logischen Switch verbinden.

Verfahren

- 1 Wählen Sie in **Logische Switches (Logical Switches)** den logischen Switch, dem Sie die virtuellen Maschinen hinzufügen möchten.
- 2 Klicken Sie auf das Symbol **Virtuelle Maschine hinzufügen (Add Virtual Machine)** ().
- 3 Wählen Sie die virtuellen Maschinen aus, die Sie zum logischen Switch hinzufügen möchten.
- 4 Wählen Sie die vNICs aus, die Sie verbinden möchten.
- 5 Klicken Sie auf **Weiter (Next)**.
- 6 Überprüfen Sie die von Ihnen ausgewählten vNICs.
- 7 Klicken Sie auf **Beenden (Finish)**.

Testen der Konnektivität eines logischen Switches

Ein Ping-Test überprüft, ob sich zwei Hosts in einem VXLAN-Transport-Netzwerk gegenseitig erreichen können.

- 1 Doppelklicken Sie in **Logische Switches (Logical Switches)** in der Spalte **Name** auf den logischen Switch, den Sie testen möchten.

- 2 Klicken Sie auf die Registerkarte **Überwachen (Monitor)**.
- 3 Klicken Sie auf die Registerkarte **Hosts**.
- 4 Klicken Sie im Abschnitt „Quellhost“ auf **Durchsuchen (Browse)**. Wählen Sie im Dialogfeld „Host auswählen“ den Zielhost aus.
- 5 Wählen Sie die Größe des Testpakets aus.

Die Standardgröße bei VXLAN beträgt 1550 Bytes ohne Fragmentierung (sollte mit den MTU der physischen Infrastruktur übereinstimmen). Dies ermöglicht NSX, die Konnektivität zu überprüfen und sicherzustellen, dass die Infrastruktur für den VXLAN-Datenverkehr vorbereitet ist.

Eine minimale Paketgröße führt zu Fragmentierung. Demzufolge kann NSX dank der kleineren Paketgröße die Konnektivität überprüfen, jedoch nicht, ob die Infrastruktur für größere Rahmengrößen eingerichtet ist.

- 6 Klicken Sie im Abschnitt „Zielhost“ auf **Durchsuchen (Browse)**. Wählen Sie im Dialogfeld „Host auswählen“ den Zielhost aus.
- 7 Klicken Sie auf **Test starten (Start Test)**.

Die Ergebnisse des Host-to-Host-Ping-Tests werden angezeigt.

Verhindern von Manipulationen auf einem logischen Switch

Nach der Synchronisierung mit vCenter Server erfasst NSX Manager aus VMware Tools auf jeder virtuellen Maschine oder aus der IP-Erkennung, sofern aktiviert, die IP-Adressen aller virtuellen vCenter-Gastmaschinen. NSX vertraut nicht allen von VMware Tools oder der IP-Erkennung bereitgestellten IP-Adressen. Wenn die Sicherheit einer virtuellen Maschine gefährdet wurde, kann die IP-Adresse manipuliert worden sein. Demzufolge könnten Übertragungen mit böswilligen Absichten Firewallrichtlinien umgehen.

SpoofGuard ermöglicht das Autorisieren der IP-Adressen, die von VMware Tools oder der IP-Erkennung gemeldet werden, und bei Bedarf das Ändern dieser Adressen, um Manipulationen (Spoofing) zu verhindern. SpoofGuard vertraut standardmäßig den MAC-Adressen virtueller Maschinen, die aus VMX-Dateien und dem vSphere SDK erfasst werden. SpoofGuard wird getrennt von den Firewallregeln ausgeführt und kann zum Blockieren von Datenverkehr verwendet werden, der als manipuliert erkannt wurde.

Weitere Informationen finden Sie unter [Kapitel 13 Verwenden von SpoofGuard](#).

Bearbeiten eines logischen Switches

Sie können den Namen, die Beschreibung und den Steuerungskomponenten-Modus eines logischen Switches bearbeiten.

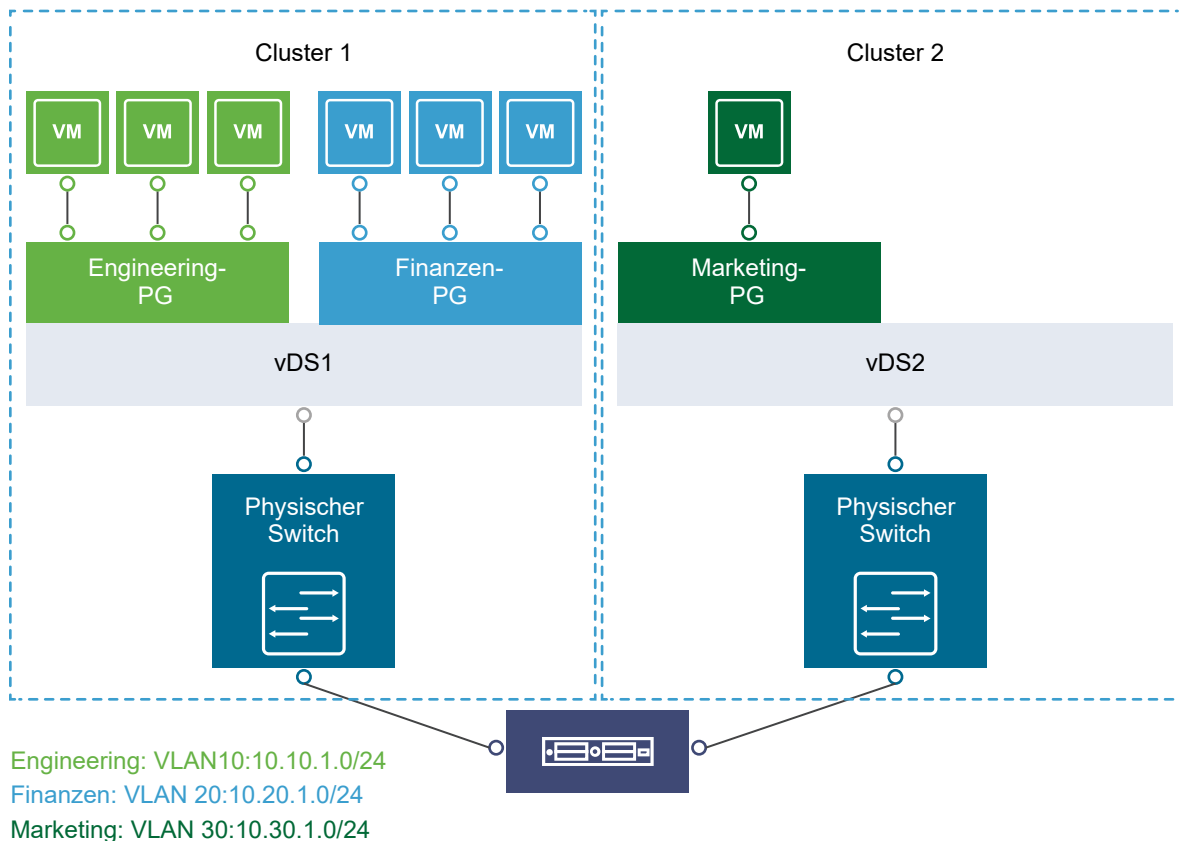
Verfahren

- 1 Wählen Sie unter **Logische Switches (Logical Switches)** den zu bearbeitenden logischen Switch aus.
- 2 Klicken Sie auf das Symbol **Bearbeiten (Edit)**.
- 3 Nehmen Sie die gewünschten Änderungen vor.
- 4 Klicken Sie auf **OK**.

Szenario für einen logischen Switch

Dieses Szenario stellt eine Situation dar, in der das Unternehmen ACME Enterprise im ACME_Datencenter über zwei Cluster mit mehreren ESXi-Hosts verfügt. Die Engineering-Abteilung (mit der Portgruppe „PG-Engineering“) sowie die Finance-Abteilung (mit der Portgruppe „PG-Finance“) befinden sich auf Cluster1. Die Marketing-Abteilung (PG-Marketing) verwendet Cluster2. Beide Cluster werden von einem einzelnen vCenter Server verwaltet.

Abbildung 6-1. Netzwerk von ACME Enterprise vor der Implementierung logischer Switches

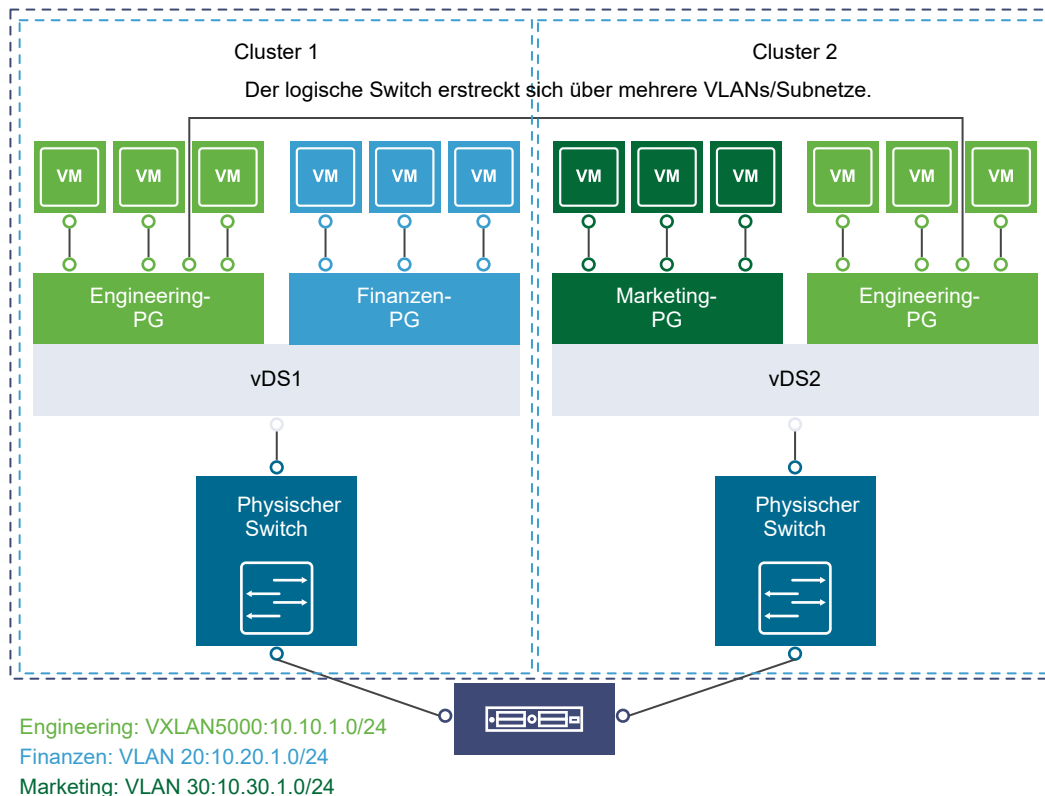


ACME verfügt auf Cluster1 über unzureichende Rechenressourcen, während Cluster2 nicht ausgelastet ist. Der Netzwerk-Supervisor von ACME bittet Peter Admin (Virtualisierungsadministrator bei ACME) zu ermitteln, wie eine Nutzung der Cluster2-Maschinen durch die Engineering-Abteilung aussehen könnte, bei der die virtuellen Maschinen der Engineering-Abteilung auf beiden Clustern miteinander kommunizieren. Dies würde es ACME ermöglichen, durch Ausdehnen der L2-Schicht die Rechenkapazität beider Cluster zu nutzen.

Wenn Peter Admin diese Aufgabenstellung auf eine herkömmliche Weise lösen würde, müsste er die beiden VLANs auf eine besondere Weise verbinden, um beiden Clustern die Zugehörigkeit zur selben L2-Domäne zu ermöglichen. Das würde bedeuten, dass ACME ein neues physisches Gerät für die Trennung des Datenverkehrs anschaffen müsste, und es würde Probleme wie VLAN-Sprawl, Netzwerk-Loops sowie einen Mehraufwand bei Administrations- und Management-Aufgaben nach sich ziehen.

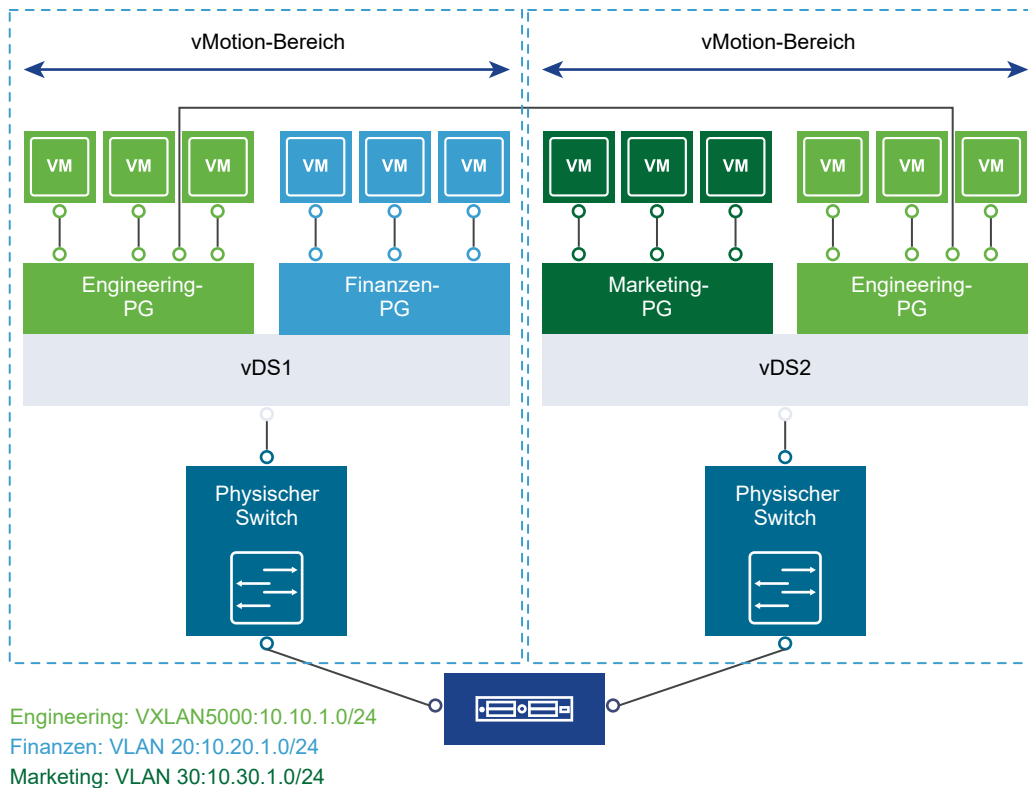
Peter Admin erinnert sich an eine Vorführung eines logischen Netzwerks, die er auf der VMworld gesehen hat, und beschließt, NSX zu testen. Er kommt zu dem Schluss, dass ihm der Aufbau eines virtuellen Switches auf dvSwitch1 und dvSwitch2 ermöglichen wird, die L2-Schicht bei ACME auszuweiten. Da Peter Admin den NSX Controller nutzen kann, braucht er die physische Infrastruktur von ACME nicht anzurühren, denn NSX funktioniert basierend auf bestehenden IP-Netzwerken.

Abbildung 6-2. ACME Enterprise implementiert einen logischen Switch



Nachdem Peter Admin einen logischen Switch auf den beiden Clustern erstellt hat, kann er mithilfe von vMotion virtuelle Maschinen von einem Cluster zu einem anderen verschieben, wobei diese VMs weiterhin mit demselben logischen Switch verbunden bleiben.

Abbildung 6-3. vMotion in einem logischen Netzwerk



Lassen Sie uns nachvollziehen, welche Schritte Peter Admin durchführen muss, um bei ACME Enterprise ein logisches Netzwerk aufzubauen.

Peter Admin weist NSX Manager einen Segment-ID-Pool und einen Multicast-Adressbereich zu

Peter Admin muss den erhaltenen Segment-ID-Pool angeben, um den Netzwerkdatenverkehr von Firma ABC zu isolieren.

Voraussetzungen

- 1 Peter Admin überprüft, ob dvSwitch1 und dvSwitch2 VMware Distributed Switches der Version 5.5 sind.
- 2 Peter Admin legt die verwaltete IP-Adresse für vCenter Server fest.
 - a Wählen Sie **Verwaltung (Administration) > vCenter Server-Einstellungen (vCenter Server Settings) > Laufzeiteinstellungen (Runtime Settings)** aus.
 - b Geben Sie in das Feld „vCenter Server Managed IP“ **10.115.198.165** ein.
 - c Klicken Sie auf **OK**.
- 3 Peter Admin installiert die Netzwerkvirtualisierungskomponenten auf Cluster 1 und Cluster 2. Siehe *Installationshandbuch für NSX*.

- 4 Peter Admin ruft einen Segment-ID-Pool (5000 – 5250) vom NSX Manager-Administrator bei ACME ab. Da er den NSX Controller nutzt, benötigt er kein Multicast in seinem physischen Netzwerk.
- 5 Peter Admin erstellt einen IP-Pool, damit er den VXLAN VTEPs aus diesem IP-Pool eine statische IP-Adresse zuweisen kann. Weitere Informationen dazu finden Sie unter [Hinzufügen eines IP-Pools](#).

Verfahren

- 1 Klicken Sie im vSphere Web Client auf **Networking & Security > Installation**.
- 2 Klicken Sie auf die Registerkarte **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und dann auf **Segment-ID (Segment ID)**.
- 3 Klicken Sie auf **Bearbeiten (Edit)**.
- 4 Geben Sie unter „Segment-ID-Pool“ **5000 – 5250** ein.
- 5 Wählen Sie nicht **Multicast-Adressierung aktivieren (Enable multicast addressing)** aus.
- 6 Klicken Sie auf **OK**.

Peter Admin konfiguriert VXLAN-Transportparameter

Peter Admin konfiguriert VXLAN auf Cluster 1 und Cluster 2. Dabei ordnet er jeden Cluster einem vDS zu. Wenn er einem Switch einen Cluster zuordnet, wird jeder Host in diesem Cluster für logische Switches aktiviert.

Verfahren

- 1 Klicken Sie auf die Registerkarte **Hostvorbereitung (Host Preparation)**.
- 2 Wählen Sie für Cluster 1 die Option **Konfigurieren (Configure)** aus der VXLAN-Spalte.
- 3 Wählen Sie im Dialogfeld zur Konfiguration des VXLAN-Netzwerks dvSwitch1 als virtuellen verteilten Switch für den Cluster.
- 4 Geben Sie **10** für das ACME-Transport-VLAN ein, das von dvSwitch1 verwendet werden soll.
- 5 Behalten Sie unter „Specify Transport Attributes“ für dvSwitch1 den Wert „1600“ als „Maximum Transmission Units (MTU)“ bei.

Unter MTU versteht man die maximale Menge der Daten, die in einem Paket übertragen werden kann, bevor es in kleinere Pakete aufgeteilt wird. Peter Admin weiß, dass Datenverkehr-Frames bei logischen VXLAN-Switches aufgrund der Kapselung etwas größer sind. Demzufolge muss der MTU-Wert für jeden Switch 1550 oder mehr betragen.

- 6 Wählen Sie unter **VMKNic-IP-Adressierung (VMKNic IP Addressing)** die Option **IP-Pool verwenden (Use IP Pool)** aus und wählen Sie einen IP-Pool aus.
- 7 Wählen Sie als **VMKNic-Gruppierungsrichtlinie (VMKNic Teaming Policy)** die Option **Failover**.

Peter Admin möchte die Dienstqualität seines Netzwerks beibehalten, indem er die Leistung der logischen Switches sowohl unter normalen als auch unter fehlerhaften Bedingungen konstant hält. Aus diesem Grund wählt er Failover als Gruppierungsrichtlinie.

- 8 Klicken Sie auf **Hinzufügen (Add)**.
- 9 Wiederholen Sie die Schritte 4 bis 8, um VXLAN auf Cluster 2 zu konfigurieren.

Ergebnisse

Nachdem Peter Admin Cluster 1 und Cluster 2 dem entsprechenden Switch zugeordnet hat, werden die Hosts auf diesen Clustern für logische Switches vorbereitet:

- 1 Jedem Host in Cluster 1 und Cluster 2 wird ein VXLAN-Kernelmodul und eine VMKNic hinzugefügt.
- 2 Auf dem dem logischen Switch zugeordneten vSwitch wird eine spezielle dvPortGroup erstellt, mit der die VMKNic verbunden wird.

Peter Admin fügt eine Transportzone hinzu

Das physische Netzwerk, das ein logisches Netzwerk stützt, wird als transport zone bezeichnet. Bei einer Transportzone handelt es sich um den von einem virtualisierten Netzwerk umfassten Computing-Wirkungsbereich.

Verfahren

- 1 Klicken Sie auf **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und dann auf **Transportzonen (Transport Zones)**.
- 2 Klicken Sie auf das Symbol **Neue Transportzone (New Transport Zone)**.
- 3 Geben Sie im Feld „Name“ **ACME-Zone (ACME Zone)** ein.
- 4 Geben Sie im Feld „Beschreibung“ **Bereich mit ACME-Clustern (Zone containing ACME's clusters)** ein.
- 5 Wählen Sie Cluster 1 und Cluster 2, um diese zur Transportzone hinzuzufügen.
- 6 Wählen Sie unter **Steuerungskomponenten-Modus (Control Plane Mode)** die Option **Unicast** aus.
- 7 Klicken Sie auf **OK**.

Peter Admin erstellt einen logischen Switch

Nachdem Peter Admin die VXLAN-Transportparameter konfiguriert hat, kann er einen logischen Switch erstellen.

Verfahren

- 1 Klicken Sie auf **Logische Switches (Logical Switches)** und anschließend auf das Symbol **Neues logisches Netzwerk (New Logical Network)**.
- 2 Geben Sie im Feld „Name“ **ACME logisches Netzwerk** ein.
- 3 Geben Sie im Feld „Beschreibung“ **Logisches Netzwerk für die Erweiterung des ACME Engineering-Netzwerks auf Cluster 2** ein.
- 4 Wählen Sie unter **Transportzone (Transport Zone)** „ACME-Zone“ aus.

5 Klicken Sie auf **OK**.

NSX erstellt einen logischen Switch, der die L2-Konnektivität zwischen dvSwitch1 und dvSwitch2 herstellt.

Nächste Schritte

Peter Admin kann jetzt die virtuellen Maschinen der Produktionsumgebung von ACME mit dem logischen Switch verbinden und den logischen Switch mit einem NSX Edge Services Gateway oder logischen Router verbinden.

Konfigurieren von Hardware-Gateways

7

Bei der Konfiguration von Hardware-Gateways werden physische Netzwerke logischen Netzwerken zugeordnet. Die Zuordnungskonfiguration soll NSX die Nutzung der Open vSwitch-Datenbank (OVSDB) ermöglichen.

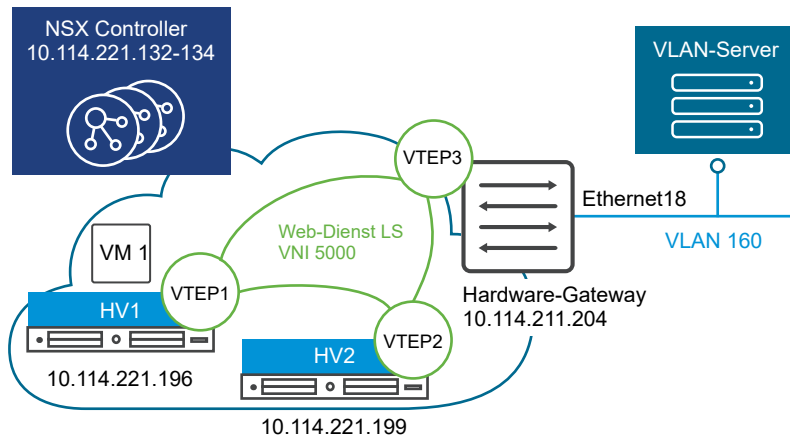
Die OVSDB-Datenbank enthält Informationen über die physische Hardware und das virtuelle Netzwerk. Die Händler-Hardware hostet den Datenbankserver.

Die Hardware-Gateway-Switches in den logischen NSX-Netzwerken beenden die VXLAN-Tunnel. Im virtuellen Netzwerk werden die Hardware-Gateway-Switches als Hardware-VTEP bezeichnet. Weitere Informationen zu VTEPs finden Sie *Installationshandbuch für NSX* und im Handbuch *NSX-Netzwerkvirtualisierungsdesign*.

Eine Basistopologie mit einem Hardware-Gateway muss die folgenden Komponenten enthalten:

- Physischer Server
- Hardware-Gateway-Switch (L2-Port)
- IP-Netzwerk
- Mindestens vier Hypervisoren, inklusive zwei Replizierungscluster mit VMs
- Controller-Cluster mit mindestens drei Knoten

Die Beispieltopologie mit einem Hardware-Gateway enthält die beiden Hypervisoren HV1 und HV2. Die virtuelle Maschine VM1 befindet sich auf HV1. VTEP1 befindet sich auf HV1, VTEP2 auf HV2 und VTEP3 auf dem Hardware-Gateway. Das Hardware-Gateway befindet sich im Subnetz 211, während die beiden Hypervisoren im selben Subnetz 221 enthalten sind.



Die Konfiguration für das Hardware-Gateway kann jede der folgenden Komponenten enthalten:

- Einzelner Switch
- Mehrere physische Bus-Switches mit unterschiedlichen IP-Adressen
- Hardware-Switch-Controller mit mehreren Switches

Der NSX Controller kommuniziert mit dem Hardware-Gateway über seine IP-Adresse an Port 6640. Mit dieser Verbindung werden OVSDB-Transaktionen von Hardware-Gateways gesendet und empfangen.

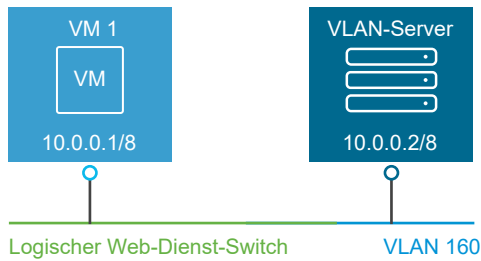
Dieses Kapitel enthält die folgenden Themen:

- [Szenario: Beispielkonfiguration für ein Hardware-Gateway](#)

Szenario: Beispielkonfiguration für ein Hardware-Gateway

Dieses Szenario beschreibt typische Aufgaben für die Konfiguration eines Hardware-Gateway-Switch bei einer NSX-Bereitstellung. Die dargestellten Aufgaben zeigen, wie Sie mithilfe des Hardware-Gateways die virtuelle Maschine VM1 mit dem physischen Server und den logischen Switch des Webdienstes mit dem VLAN-Server VLAN 160 verbinden.

Die Beispieltopologie zeigt, dass die virtuelle Maschine VM1 und der VLAN-Server mit einer IP-Adresse im Subnetz 10 konfiguriert wurden. VM1 wurde dem logischen Switch des Webdienstes angefügt. Der VLAN-Server wurde dem VLAN 160 auf dem physischen Server angefügt.



Wichtig In einer Cross-vCenter NSX-Umgebung werden Hardware-Gateway-Switch-Konfigurationen nur auf dem primären NSX Manager unterstützt. Hardware-Gateway-Switches müssen an nicht universelle logische Switches gebunden sein. Hardware-Gateway-Konfigurationen werden auf sekundären NSX Managern nicht unterstützt.

Voraussetzungen

- In der Händlerdokumentation finden Sie die Anforderungen für das physische Netzwerk.
- Stellen Sie sicher, dass die System- und Hardwareanforderungen von NSX für die Konfiguration des Hardware-Gateways erfüllt sind. Weitere Informationen dazu finden Sie unter [Kapitel 1 Systemvoraussetzungen für NSX](#).
- Stellen Sie sicher, dass die logischen Netzwerke korrekt eingerichtet sind. Informationen dazu finden Sie im *Installationshandbuch für NSX*.
- Stellen Sie sicher, dass die Zuordnungen der Transportparameter im VXLAN korrekt sind. Informationen dazu finden Sie im *Installationshandbuch für NSX*.
- Rufen Sie das Anbieterzertifikat für Ihr Hardware-Gateway ab.
- Stellen Sie sicher, dass für den VXLAN-Port der Wert 4789 eingestellt ist. Weitere Informationen dazu finden Sie unter [Ändern des VXLAN-Ports](#).

Verfahren

1 Einrichten des Replizierungsclusters

Ein Replizierungscluster ist ein Set von Hypervisoren, die für die Weiterleitung von Datenverkehr, der vom Hardware-Gateway gesendet wurde, verantwortlich sind. Der Datenverkehr kann Broadcast-, Unicast- und Multicast-Datenverkehr sein.

2 Verbinden des Hardware-Gateways mit NSX Controllern

Sie müssen die OVSDB-Managertabelle des physischen ToR-Switch für eine Verbindung des Hardware-Gateways mit dem NSX Controller konfigurieren.

3 Hinzufügen eines Hardware-Gateway-Zertifikats

Damit die Konfiguration für ein Hardwaregerät wirksam sein kann, muss diesem ein Hardware-Gateway-Zertifikat hinzugefügt werden.

4 Binden des logischen Switch an den physischen Switch

Der logische Switch des Webdienstes, der der virtuellen Maschine VM1 angefügt wurde, muss mit dem Hardware-Gateway im selben Subnetz kommunizieren.

Einrichten des Replizierungsclusters

Ein Replizierungscluster ist ein Set von Hypervisoren, die für die Weiterleitung von Datenverkehr, der vom Hardware-Gateway gesendet wurde, verantwortlich sind. Der Datenverkehr kann Broadcast-, Unicast- und Multicast-Datenverkehr sein.

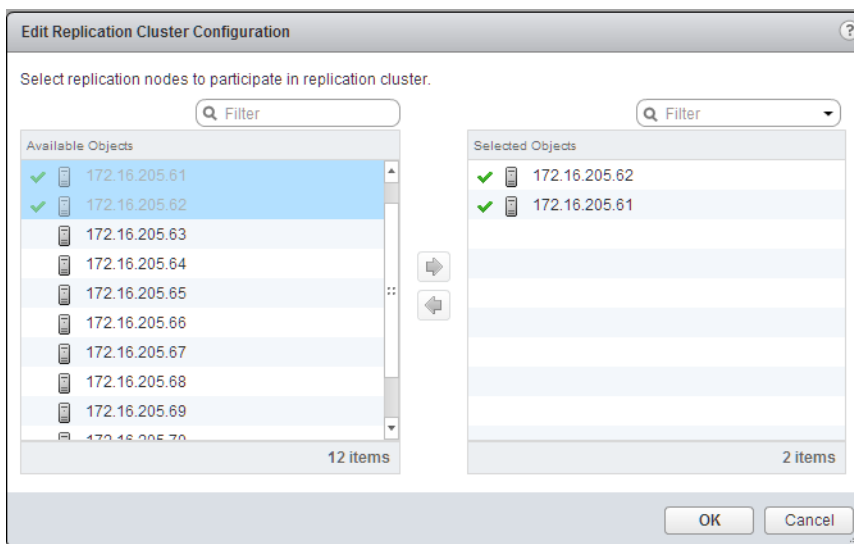
Hinweis Hypervisoren, die die Replizierungsknoten und die Hardware-Gateway-Switches enthalten, dürfen sich nicht im selben IP-Subnetz befinden. Diese Einschränkung ist auf die Beschränkung des Chipsatzes zurückzuführen, der in den meisten Hardware-Gateways verwendet wird. Nahezu alle Hardware-Gateways verwenden den Broadcom Trident II-Chipsatz, für den die Einschränkung gilt, dass zwischen dem Hardware-Gateway und den Hypervisoren ein Layer-3-Underlay-Netzwerk erforderlich ist.

Voraussetzungen

Stellen Sie sicher, dass Sie über Hypervisoren verfügen, die als Replizierungsknoten dienen können.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Networking & Security > Service Definitions** aus.
- 3 Klicken Sie auf die Registerkarte **Hardwaregeräte (Hardware Devices)**.
- 4 Klicken Sie im Abschnitt „Replizierungscluster“ auf **Bearbeiten (Edit)** und wählen Sie die Hypervisoren aus, die als Replizierungsknoten in diesem Replizierungscluster dienen sollen.
- 5 Wählen Sie Hypervisoren aus und klicken Sie auf den blauen Pfeil.



Die ausgewählten Hypervisoren werden in die Spalte „Ausgewählte Objekte“ verschoben.

- 6 Klicken Sie auf **OK**.

Ergebnisse

Die Replizierungsknoten werden dem Replizierungscluster hinzugefügt. Im Replizierungscluster muss mindestens ein Host vorhanden sein.

Verbinden des Hardware-Gateways mit NSX Controllern

Sie müssen die OVSDB-Managertabelle des physischen ToR-Switch für eine Verbindung des Hardware-Gateways mit dem NSX Controller konfigurieren.

Der Controller überwacht passiv den Verbindungsversuch von ToR. Deshalb muss das Hardware-Gateway die Verbindung mithilfe der OVSDB-Managertabelle initiieren.

Voraussetzungen

Die Controller müssen vor der Konfiguration von ToR-Instanzen bereitgestellt werden. Ohne die vorausgehende Bereitstellung von Controllern wird die Fehlermeldung „Der Vorgang konnte auf dem Controller nicht ausgeführt werden“ eingeblendet.

Verfahren

- 1 Mit den für Ihre Umgebung gültigen Befehlen können Sie das Hardware-Gateway mit dem NSX Controller verbinden.

Befehlsbeispiele für die Verbindung von Hardware-Gateway und NSX Controller.

```
prmh-nsx-tor-7050sx-3#enable
prmh-nsx-tor-7050sx-3#configure terminal
prmh-nsx-tor-7050sx-3(config)#cvx
prmh-nsx-tor-7050sx-3(config-cvx)#service hsc
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#manager 172.16.2.95 6640
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#no shutdown
prmh-nsx-tor-7050sx-3(config-cvx-hsc)#end
```

- 2 Legen Sie die OVSDB-Managertabelle auf dem Hardware-Gateway fest.
- 3 Legen Sie für die OVSDB-Portnummer den Wert 6640 fest.
- 4 (Optional) Stellen Sie sicher, dass das Hardware-Gateway mit dem NSX Controller über den OVSDB-Kanal verbunden ist.
 - Prüfen Sie, ob für den Verbindungsstatus UP (Aktiv) gültig ist.
 - Senden Sie an VM1 und VLAN 160 einen Ping-Befehl, um sicherzustellen, dass die Verbindung hergestellt ist.
- 5 (Optional) Stellen Sie sicher, dass das Hardware-Gateway mit dem richtigen NSX Controller verbunden ist.
 - a Melden Sie sich beim vSphere Web Client an.
 - b Wählen Sie **Networking & Security > > Installation > NSX Controller-Knoten (NSX Controller nodes)** aus.

Hinzufügen eines Hardware-Gateway-Zertifikats

Damit die Konfiguration für ein Hardwaregerät wirksam sein kann, muss diesem ein Hardware-Gateway-Zertifikat hinzugefügt werden.

Voraussetzungen

Stellen Sie sicher, dass das Hardware-Gateway-Zertifikat aus Ihrer Umgebung verfügbar ist.

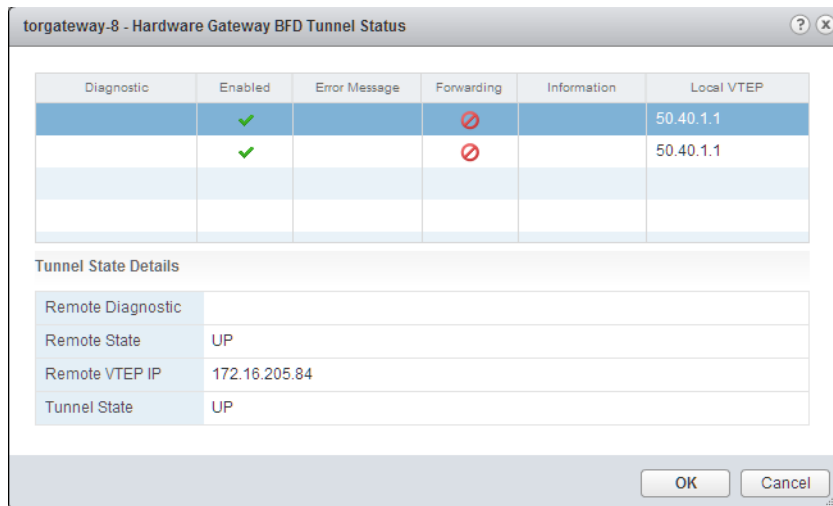
Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Netzwerk und Sicherheit (Networking & Security) > Service Definitions** aus.
- 3 Klicken Sie auf die Registerkarte **Hardwaregeräte (Hardware Devices)**.
- 4 Klicken Sie auf das Symbol „Hinzufügen“ (+), um das Hardware-Gateway-Profil im Detail zu erstellen.

Option	Beschreibung
Name und Beschreibung	Gibt einen Namen für das Hardware-Gateway an. Sie können im Abschnitt „Beschreibung“ Details des Profils hinzufügen.
Zertifikat	Fügt das aus Ihrer Umgebung extrahierte Zertifikat ein.
BFD aktivieren	Das BFD-Protokoll (Bidirectional Forwarding Detection) ist standardmäßig aktiviert. Mit dem Protokoll werden die Konfigurationsinformationen des Hardware-Gateway synchronisiert.

- 5 Klicken Sie auf **OK**.
Es wird ein Profil für das Hardware-Gateway erstellt.
- 6 Aktualisieren Sie den Bildschirm, um sicherzustellen, dass das Hardware-Gateway verfügbar ist und ausgeführt wird.
Für die Konnektivität muss „UP“ gültig sein.

- 7 (Optional) Klicken Sie mit der rechten Maustaste auf das Hardware-Gateway-Profil und wählen Sie aus dem eingeblendeten Kontextmenü **BFD-Tunnelstatus anzeigen (View the BFD Tunnel Status)** aus.



Im Dialogfeld werden Diagnoseinformationen zum Tunnelstatus für die Fehlerbehebung angezeigt.

Binden des logischen Switch an den physischen Switch

Der logische Switch des Webdienstes, der der virtuellen Maschine VM1 angefügt wurde, muss mit dem Hardware-Gateway im selben Subnetz kommunizieren.


Hinweis Wenn Sie mehrere logische Switches an Hardware-Ports binden möchten, müssen Sie die nachfolgend aufgeführten Schritte für jeden logischen Switch durchführen.

Voraussetzungen

- Stellen Sie sicher, dass der logische Switch des Webdienstes verfügbar ist. Weitere Informationen dazu finden Sie unter [Hinzufügen eines logischen Switch](#).
- Stellen Sie sicher, dass ein physischer Switch verfügbar ist.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Netzwerk und Sicherheit (Networking & Security) > Logische Switches (Logical Switches)** aus.
- 3 Wechseln Sie zum logischen Switch des Webdienstes, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Hardware-Bindungen verwalten (Manage Hardware Bindings)** aus dem eingeblendeten Kontextmenü aus.
- 4 Wählen Sie das Hardware-Gateway-Profil aus.

- 5 Klicken Sie auf das Symbol „Hinzufügen“ () und wählen Sie den physischen Switch aus dem Dropdown-Menü aus.




Beispiel: AristaGW.

- 6 Klicken Sie auf **Auswählen (Select)**, um einen physischen Port aus der Liste „Verfügbare Objekte“ auszuwählen.

Beispiel: Ethernet 18.

- 7 Klicken Sie auf **OK**.

- 8 Geben Sie den VLAN-Namen an.

▼ AristaGW (1 Bindings)		
  		
Switch	Port	VLAN
prmh-nsx-tor-7150s-1	Ethernet18	160

Beispiel: 160.

- 9 Klicken Sie auf **OK**.

Ergebnisse

Die Bindung ist abgeschlossen.

Der NSX Controller synchronisiert die physischen und logischen Konfigurationsinformationen mit dem Hardware-Gateway.

L2-Bridges

8

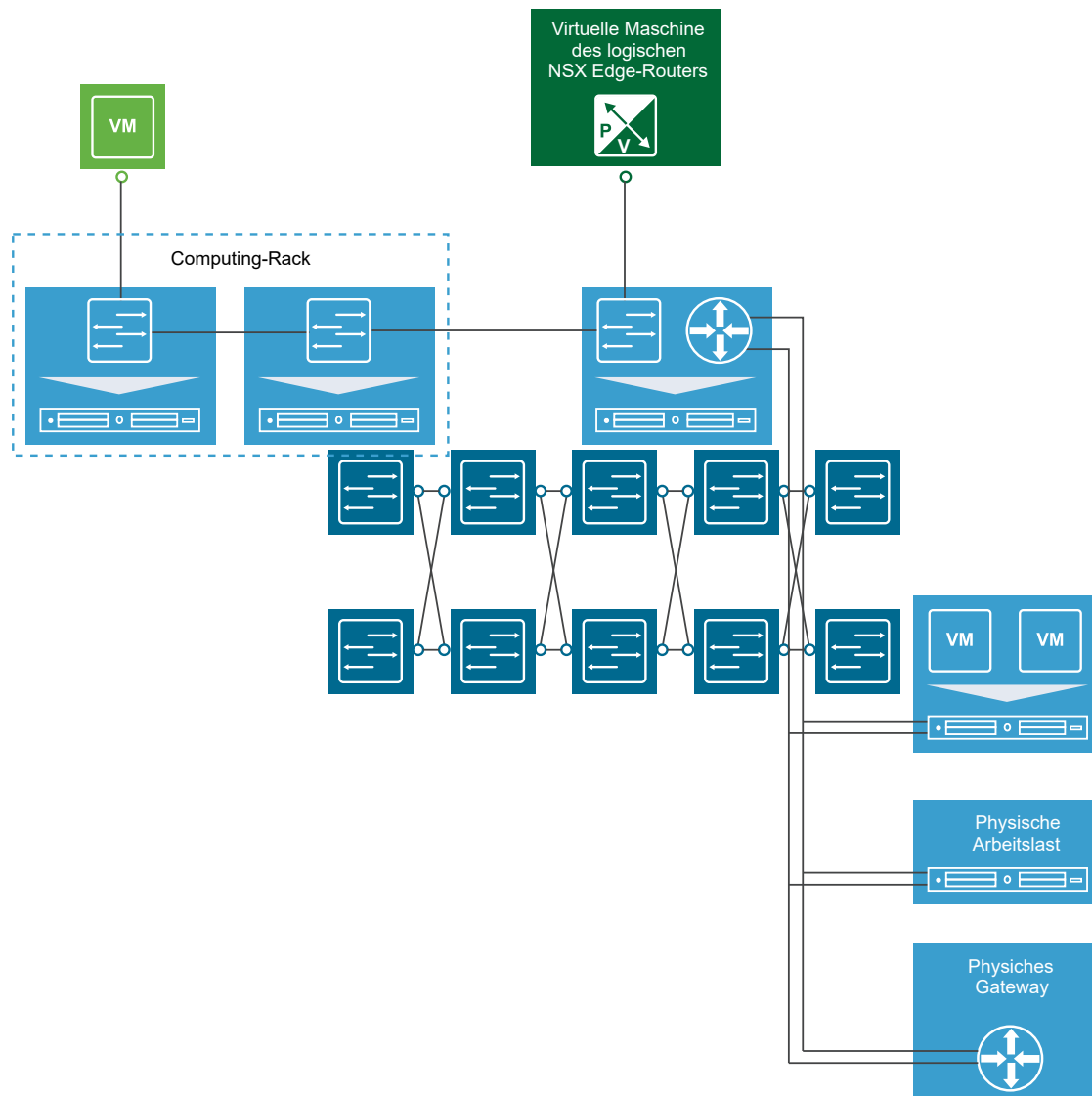
Sie können eine L2-Bridge zwischen einem logischen Switch und einem VLAN erstellen. Damit können Sie virtuelle Arbeitslasten ohne Beeinträchtigung der IP-Adressen auf physische Geräte migrieren.

Eine Schicht-2-Bridge ermöglicht die Konnektivität zwischen dem virtuellen und physischen Netzwerk durch die Aktivierung von virtuellen Maschinen (VMs) für die Verbindung mit einem physischen Server oder Netzwerk. Anwendungsfälle umfassen:

- Migration von physisch zu virtuell oder virtuell zu virtuell. L2-Bridging ermöglicht die Konnektivität zwischen Arbeitslasten in NSX und außerhalb von NSX ohne erneute IP-Adressierung.
- Einfügen einer Appliance in NSX, die nicht virtualisiert werden kann und für die L2-Konnektivität mit den Clients erforderlich ist. Dies ist geläufig bei einigen physischen Datenbankservern.
- Serviceeinfügung Eine L2-Bridge ermöglicht die transparente Integration aller physischen Appliances wie Router, Load Balancer oder Firewall in NSX.

Durch Bridging der Broadcast-Domäne eines logischen Switches zur VLAN-Broadcast-Domäne kann ein logisches Netzwerk ein physisches L3-Gateway nutzen und auf vorhandene physische Netzwerk- und Sicherheitsressourcen zugreifen. Die L2-Bridge wird auf dem Host mit der logischen Router-VM von NSX Edge ausgeführt. Eine L2-Bridgeinstanz wird einem einzelnen VLAN zugeordnet, aber es kann mehrere Bridgeinstanzen geben. Der logische Router kann nicht als Gateway für Geräte verwendet werden, die mit einer Bridge verbunden sind. Die VLAN-Portgruppe und der logische VXLAN-Switch, die eine Bridgeverbindung unterhalten, müssen sich auf demselben VDS (vSphere Distributed Switch) befinden und beide müssen dieselben physischen Netzwerkkarten (NICs) nutzen.

Per VXLAN (VNI)-Netzwerk und VLAN unterstützte Portgruppen müssen sich am selben virtuellen Distributed Switch (VDS) befinden.



Beachten Sie, dass Sie eine L2-Bridge nicht zum Verbinden eines logischen Switches mit einem anderen logischen Switch, eines VLAN-Netzwerks mit einem anderen VLAN-Netzwerk oder zum Verbinden von Datencentern untereinander verwenden sollten. Außerdem können Sie einen globalen logischen Router nicht zum Konfigurieren von Bridging verwenden oder eine Bridge zu einem globalen logischen Switch hinzufügen.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen einer L2-Bridge](#)
- [Hinzufügen einer L2-Bridge zu einer Umgebung mit logischem Routing](#)

Hinzufügen einer L2-Bridge

Sie können eine Bridge von einem logischen Switch zu einer verteilten virtuellen Portgruppe hinzufügen.

Voraussetzungen

Ein konfigurierter logischer Switch und eine VLAN-gestützte, verteilte virtuelle Portgruppe

Der logische Switch und die VLAN-gestützte, verteilte virtuelle Portgruppe, für die das Bridging vorgenommen werden soll, müssen auf demselben Virtual Distributed Switch (VDS) vorhanden sein.

Eine DLR-Kontroll-VM auf einem Hypervisor, auf dem der VDS mit dem logischen Switch und die VLAN-gestützte, verteilte virtuelle Portgruppe instanziiert werden, muss in Ihrer Umgebung bereitgestellt werden.

Sie können zur Konfiguration des Bridging keinen universellen logischen Router verwenden und Sie können keine Bridge zu einem universellen logischen Switch hinzufügen.

Vorsicht Überbrückter Datenverkehr wechselt über den Uplink-Port auf dem dvSwitch, der für den VXLAN-Datenverkehr verwendet wird, in einen ESXi-Host und verlässt diesen. VDS-Gruppierung oder Failover-Richtlinie für VLAN werden nicht auf den überbrückten Datenverkehr angewendet.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf einen logischen Router.
- 4 Klicken Sie auf **Verwalten (Manage)** und anschließend auf **Bridging**.
- 5 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 6 Geben Sie einen Namen für die Bridge ein.

Vorsicht Bridge-Name dürfen maximal 40 Zeichen enthalten. Wenn der Name mehr als 40 Zeichen enthält, schlägt die Bridge-Konfiguration fehl.

- 7 Wählen Sie den logischen Switch aus, für den Sie eine Bridge erstellen möchten.
- 8 Wählen Sie die verteilte virtuelle Portgruppe aus, zu der Sie den logischen Switch überbrücken möchten.
- 9 Klicken Sie auf **OK**.

Hinzufügen einer L2-Bridge zu einer Umgebung mit logischem Routing

Sie können einen bestimmten logischen Switch mit einer aktiven Bridge-Instanz zu einem einzelnen VLAN überbrücken. Ein logischer Router kann über mehrere Bridge-Instanzen verfügen, aber dasselbe VXLAN bzw. VLAN kann nicht mit mehr als einer Bridge-Instanz verbunden sein.

Sie können einen logischen Switch verwenden, um sowohl an der verteilten logischen Weiterleitung als auch am Layer-2-Bridging teilzunehmen. Aus diesem Grund muss der Datenverkehr vom überbrückten logischen Switch nicht über die zentralisierte Edge-VM fließen. Der Datenverkehr vom überbrückten logischen Switch kann über die L2-Bridge-Instanz in das physische VLAN übermittelt werden. Die Bridge-Instanz wird auf dem ESXi-Host aktiviert, auf dem die DLR-Kontroll-VM ausgeführt wird.

Weitere Informationen zum L2-Bridging in NSX finden Sie im Abschnitt „NSX Distributed Routing and Layer 2 Bridging Integration“ im *Design-Handbuch für die NSX-Netzwerkvirtualisierung* unter <https://communities.vmware.com/docs/DOC-27683>.

Voraussetzungen

- Ein logischer NSX-Router muss in Ihrer Umgebung bereitgestellt sein.
- Sie können zur Konfiguration des Bridging keinen universellen logischen Router verwenden und Sie können keine Bridge zu einem universellen logischen Switch hinzufügen.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf den logischen Router, den Sie zum Bridging verwenden möchten.

Hinweis Die Bridge-Instanz muss in derselben Routing-Instanz erstellt werden, mit der das VXLAN verbunden ist. Eine Bridge-Instanz kann über ein VXLAN und ein VLAN verfügen, wobei sich diese nicht überlappen dürfen. Dasselbe VXLAN bzw. VLAN kann nicht mit mehr als einer Bridge-Instanz verbunden sein.

- 4 Klicken Sie auf **Verwalten (Manage)** und anschließend auf **Bridging**.
Bei dem als Router verwendeten logischen Switch wird „Routing aktiviert“ angezeigt.
- 5 Klicken Sie auf das Symbol **Hinzufügen (Add) (+)**.
- 6 Geben Sie einen Namen für die Bridge ein.
- 7 Wählen Sie den logischen Switch aus, für den Sie eine Bridge erstellen möchten.
- 8 Wählen Sie die verteilte virtuelle Portgruppe aus, zu der Sie den logischen Switch überbrücken möchten.
- 9 Klicken Sie auf **OK**.
- 10 Klicken Sie im Fenster „Bridge hinzufügen“ erneut auf **OK**.
- 11 Klicken Sie auf „Veröffentlichen“, damit die Änderungen an der Bridging-Konfiguration wirksam werden.

Für den für das Bridging verwendeten logischen Switch wird **Routing aktiviert (Routing Enabled)** angezeigt. Weitere Informationen finden Sie unter [Hinzufügen eines logischen Switch](#) und [Verbinden von virtuellen Maschinen mit einem logischen Switch](#).

Sie können ein statisches und dynamisches Routing für jedes NSX Edge angeben.

Dynamisches Routing bietet die notwendigen Weiterleitungsinformationen zwischen Schicht 2-Broadcast-Domänen, wodurch Sie Schicht 2-Broadcast-Domänen verringern und die Netzwerk-Effizienz und -Größe verbessern können. NSX dehnt diese Informationen auf Orte aus, an denen sich die Arbeitslasten für horizontales Routing befinden. Dies ermöglicht eine direktere Kommunikation zwischen virtuellen Maschinen ohne die kosten- und zeitaufwendige Erweiterung von Hops. Gleichzeitig bietet NSX auch vertikale Verbindungen, wodurch Mandanten für den Zugriff auf öffentliche Netzwerke aktiviert werden.

Dieses Kapitel enthält die folgenden Themen:

- [Hinzufügen eines logischen \(verteilten\) Router](#)
- [Hinzufügen eines Edge Services Gateway](#)
- [Angaben der globalen Konfiguration](#)
- [Konfiguration von NSX Edge](#)
- [Hinzufügen einer statischen Route](#)
- [Konfigurieren von OSPF auf einem logischen \(Distributed\) Router](#)
- [Konfigurieren von OSPF in einem Edge Services Gateway](#)
- [Konfigurieren des BGP-Protokolls](#)
- [Konfigurieren der Route Redistribution](#)
- [Anzeigen der Gebietsschema-ID von NSX Manager](#)
- [Konfigurieren der Gebietsschema-ID auf einem globalen \(Distributed\) Router](#)
- [Konfigurieren der Gebietsschema-ID auf einem Host oder Cluster](#)

Hinzufügen eines logischen (verteilten) Router

Logische Router-Kernel-Module im Host sind für das Routing zwischen VXLAN-Netzwerken sowie zwischen virtuellen und physischen Netzwerken zuständig. Ein NSX Edge Appliance liefert nach Bedarf eine dynamische Routing-Funktion. Logische Router können auf dem primären und den sekundären NSX Manager-Instanzen in einer Cross-vCenter NSX-Umgebung, universelle logische Router nur auf dem primären NSX Manager erstellt werden.

Beachten Sie beim Bereitstellen eines neuen logischen Routers Folgendes:

- In NSX-Version 6.2 und höher ist es möglich, mit logischen Routern geroutete logische Schnittstellen (LIFs) mit einem VXLAN zu verbinden, das zu einem VLAN überbrückt ist.
- Logische Router- und Bridging-Schnittstellen können nicht mit einer dvPortgroup verbunden werden, wenn die VLAN-ID auf 0 festgelegt ist.
- Eine bestimmte Instanz eines logischen Routers kann nicht mit logischen Switches aus unterschiedlichen Transportzonen verbunden werden. Dadurch soll sichergestellt werden, dass alle logischen Switches und logischen Router-Instanzen aufeinander abgestimmt sind.
- Es kann keine Verbindung zwischen einem logischen Router und VLAN-gestützten Portgruppen hergestellt werden, wenn der logische Router mit logischen Switches verbunden ist, die sich über mehr als einen vSphere Distributed Switch (VDS) erstrecken. Dadurch wird die ordnungsgemäße Ausrichtung logischer Router-Instanzen mit den dvPortgroups logischer Switches über Hosts hinweg sichergestellt.
- Logische Router-Schnittstellen sollten nicht auf zwei unterschiedlichen verteilten Portgruppen (dvPortgroups) mit derselben VLAN-ID erstellt werden, wenn sich die beiden Netzwerke im gleichen vSphere Distributed Switch befinden.
- Logische Router-Schnittstellen sollten nicht auf zwei unterschiedlichen dvPortgroups mit derselben VLAN-ID erstellt werden, wenn sich zwei Netzwerke in unterschiedlichen vSphere Distributed Switches befinden, aber sich die beiden vSphere Distributed Switches dieselben Hosts teilen. In anderen Worten: Logische Router-Schnittstellen können auf zwei unterschiedlichen Netzwerken mit derselben VLAN-ID erstellt werden, wenn sich die beiden dvPortgroups in zwei unterschiedlichen vSphere Distributed Switches befinden, solange sich die vSphere Distributed Switches keinen Host teilen.
- Wenn VXLAN konfiguriert ist, müssen logische Router-Schnittstellen auf dem vSphere Distributed Switch mit verteilten Portgruppen verbunden sein, auf dem VXLAN konfiguriert ist. Verbinden Sie die logischen Router-Schnittstellen nicht mit Portgruppen auf anderen vSphere Distributed Switches.

In der folgenden Liste wird die Unterstützung von Funktionen durch Schnittstellentypen (Uplink und intern) auf dem logischen Router beschrieben:

- Dynamische Routing-Protokolle (BGP und OSPF) werden nur auf Uplink-Schnittstellen unterstützt.
- Firewallregeln gelten nur auf Uplink-Schnittstellen und sind auf Kontrolle und Verwaltung von Datenverkehr beschränkt, der die virtuelle Edge-Appliance zum Ziel hat.
- Weitere Informationen über die DLR-Verwaltungsschnittstelle finden Sie im Knowledgebase-Artikel „Interface Guide: DLR Control VM – NSX“ <http://kb.vmware.com/kb/2122060>.


Wichtig Wenn Sie die Hochverfügbarkeit (High Availability, HA) auf einem NSX Edge in einer Cross-vCenter NSX-Umgebung aktivieren, müssen sich die aktive und die Standby-NSX Edge-Appliance im selben vCenter Server befinden. Wenn Sie ein Mitglied eines NSX Edge-HA-Paares auf ein anderes vCenter Server-System migrieren, können die beiden HA-Appliances nicht mehr als HA-Paar ausgeführt werden. Dies kann zu einer Unterbrechung des Datenverkehrs führen.

Voraussetzungen

- Ihnen muss die Rolle **Enterprise-Administrator** oder **NSX-Administrator** zugewiesen worden sein.
- Sie müssen selbst dann einen lokalen Segment-ID-Pool erstellen, wenn Sie nicht vorhaben, logische NSX-Switches zu erstellen.
- Stellen Sie vor der Erstellung oder Änderung der Konfiguration eines logischen Routers sicher, dass der Controller-Cluster eingerichtet und verfügbar ist. Ein logischer Router kann ohne die Hilfe von NSX Controllern keine Routing-Informationen an Hosts verteilen. Ein logischer Router verlässt sich auf die Funktion von NSX Controllern, was bei Edge Services Gateways (ESGs) nicht der Fall ist.
- Wenn ein logischer Router mit VLAN-dvPortgroups verbunden werden soll, stellen Sie sicher, dass alle Hypervisor-Hosts mit einer installierten logischen Router-Appliance einander auf UDP-Port 6999 erreichen können. Die Kommunikation über diesen Port ist erforderlich, damit der auf dem VLAN des logischen Routers basierende ARP-Proxy funktioniert.
- Legen Sie fest, wo die logische Router-Appliance bereitgestellt werden soll.
 - Der Zielhost muss Teil derselben Transportzone wie die logischen Switches sein, die mit den Schnittstellen des neuen logischen Routers verbunden sind.
 - Vermeiden Sie eine Platzierung auf demselben Host als ein oder mehrere vorgeschaltete ESGs, sofern Sie ESGs in einer ECMP-Einrichtung verwenden. Um dies durchzusetzen, können Sie DRS-Regeln für Anti-Affinität verwenden, wodurch die Auswirkungen eines Hostfehlers auf die Weiterleitung logischer Router reduziert werden. Diese Richtlinie gilt nicht, wenn Sie ein ESG alleine oder im HA-Modus verwenden. Weitere Informationen finden Sie im *Handbuch zum Netzwerkvirtualisierungsdesign für VMware NSX for vSphere* unter <https://communities.vmware.com/docs/DOC-27683>.
- Stellen Sie sicher, dass das Hostcluster, auf dem Sie die logische Router-Appliance installieren möchten, für NSX vorbereitet ist. Informationen dazu erhalten Sie unter „Vorbereiten der Hostcluster für NSX“ in der Dokumentation *Installationshandbuch für NSX*.
- Legen Sie den entsprechenden NSX Manager fest, bei dem Sie Änderungen durchführen möchten.
 - In einer eigenständigen oder einzelnen vCenter NSX-Umgebung gibt es nur einen NSX Manager, sodass Sie keinen auswählen müssen.
 - Universelle Objekte müssen vom primären NSX Manager verwaltet werden.
 - Lokale Objekte einer NSX Manager-Instanz müssen von diesem NSX Manager aus verwaltet werden.
 - In einer Cross-vCenter NSX-Umgebung, in der der erweiterte verknüpfte Modus nicht aktiviert ist, müssen Sie Konfigurationsänderungen von der vCenter-Instanz aus vornehmen, die mit dem NSX Manager verknüpft ist, den Sie ändern möchten.

- In einer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus können Sie Konfigurationsänderungen an beliebigen NSX Manager-Instanzen von jeder verknüpften vCenter-Instanz aus vornehmen. Wählen Sie den geeigneten NSX Manager aus dem Dropdown-Menü „NSX Manager“ aus.
- Ermitteln Sie, welche Art von logischem Router Sie hinzufügen müssen:
 - Wenn Sie einen logischen Switch verbinden müssen, müssen Sie einen logischen Router hinzufügen.
 - Wenn Sie einen globalen logischen Switch verbinden müssen, müssen Sie einen globalen logischen Router hinzufügen.
- Wenn Sie einen globalen logischen Router hinzufügen, ermitteln Sie, ob Sie den lokalen Ausgang aktivieren müssen. Mit dem lokalen Ausgang können Sie selektiv Routen an Hosts senden. Wenn Ihre NSX-Bereitstellung mehrere Sites umfasst, ist diese Option hilfreich. Weitere Informationen hierzu finden Sie unter [Cross-vCenter NSX-Topologien](#). Sie können den lokalen Ausgang nach der Erstellung des globalen logischen Routers nicht mehr aktivieren.

Verfahren

- 1 Navigieren Sie auf vSphere Web Client zu **Start > Networking & Security > NSX Edges (Home > Networking & Security > NSX Edges)**.
- 2 Wählen Sie den entsprechenden NSX Manager aus, auf dem Sie Ihre Änderungen vornehmen. Wenn Sie einen globalen logischen Router erstellen, müssen Sie den primären NSX Manager auswählen.
- 3 Klicken Sie auf das Symbol **Hinzufügen (Add)** (.
- 4 Wählen Sie die Art des logischen Routers aus, den Sie hinzufügen möchten:
 - Wählen Sie **Logischer (verteilter) Router (Logical (Distributed) Router)** aus, um einen logischen Router hinzuzufügen, der für den ausgewählten NSX Manager lokal ist.
 - Wählen Sie **Globaler logischer (Distributed) Router (Universal Logical (Distributed) Router)** aus, um einen logischen Router hinzuzufügen, der sich über die gesamte Cross-vCenter NSX-Umgebung erstrecken kann. Diese Option ist nur dann verfügbar, wenn Sie einen primären NSX Manager zugewiesen haben und Änderungen vom primären NSX Manager aus vornehmen.
 - a Wenn Sie den **Globalen logischen (Distributed) Router (Universal Logical (Distributed) Router)** auswählen, müssen Sie zudem festlegen, ob Sie den lokalen Ausgang aktivieren möchten.
- 5 Geben Sie einen Namen für das Gerät ein.

Dieser Name wird in Ihrer vCenter-Bestandsliste angezeigt. Der Name muss über alle logischen Router eines einzelnen Mandanten hinweg eindeutig sein.

Sie können optional auch einen Hostnamen eingeben. Dieser Name wird in der Befehlszeilenschnittstelle angezeigt. Wenn Sie keinen Hostnamen angeben, wird die automatisch erstellte Edge-ID in CLI angezeigt.

Sie können optional eine Beschreibung und einen Mandanten eingeben.

6 Stellen Sie eine Edge-Appliance bereit.

Edge-Appliance bereitstellen (Deploy Edge Appliance) ist standardmäßig ausgewählt. Eine Edge-Appliance (auch als logische virtuelle Router-Appliance bezeichnet) ist für das dynamische Routing und die Firewall der logischen Router-Appliance erforderlich, die für logische Router-Pings, SSH-Zugriff und dynamisches Routing gilt.

Sie können die Auswahl der Edge-Appliance-Option aufheben, wenn Sie nur statische Routen benötigen und keine Edge-Appliance bereitstellen möchten. Sie können keine Edge-Appliance zum logischen Router hinzufügen, nachdem der logische Router erstellt wurde.

7 (Optional) Aktivieren Sie High Availability.

High Availability aktivieren (Enable High Availability) ist nicht standardmäßig ausgewählt. Wählen Sie **High Availability aktivieren (Enable High Availability)** aus, um High Availability zu aktivieren und zu konfigurieren. High Availability ist erforderlich, wenn Sie dynamisches Routing anwenden möchten.

8 Geben Sie ein Kennwort für den logischen Router ein und bestätigen Sie es durch erneute Eingabe.

Das Kennwort muss zwischen 12 und 255 Zeichen umfassen und Folgendes enthalten:

- Mindestens ein Großbuchstabe
- Mindestens ein Kleinbuchstabe
- mindestens eine Zahl
- Mindestens ein Sonderzeichen

9 (Optional) Aktivieren Sie SSH.

SSH ist standardmäßig deaktiviert. Wenn Sie SSH nicht aktivieren, können Sie auf den logischen Router weiterhin zugreifen, indem Sie die virtuelle Appliance-Konsole öffnen. In diesem Fall führt das Aktivieren von SSH dazu, dass der SSH-Vorgang für die virtuelle Appliance des logischen Routers ausgeführt wird. Sie müssen die Firewallkonfiguration für den logischen Router manuell so anpassen, dass SSH auf die Protokolladresse des logischen Routers zugreifen kann. Die Protokolladresse wird konfiguriert, wenn Sie dynamisches Routing auf dem logischen Router konfigurieren.

10 (Optional) Aktivieren Sie den FIPS-Modus und legen Sie die Protokollierungsebene fest.

Der FIPS-Modus ist standardmäßig deaktiviert. Aktivieren Sie das Kontrollkästchen **FIPS-Modus aktivieren (Enable FIPS mode)**, um den FIPS-Modus zu aktivieren. Wenn Sie den FIPS-Modus aktivieren, werden für die sichere Kommunikation zum oder vom NSX Edge kryptografische Algorithmen oder Protokolle verwendet, die laut FIPS zulässig sind.

Als Protokollierungsebene ist standardmäßig „Notfall“ eingestellt.

Beispiel:

Settings

CLI credentials will be set on the NSX Edge appliance(s). These credentials can be used to login to the read only command line interface of the appliance.

User Name: *

Password: *

Confirm password: *

☐ Enable SSH access

☐ Enable FIPS mode

Edge Control Level Logging ▼

Set the Edge Control Level Logging

11 Konfigurieren Sie die Bereitstellung.

- ◆ Wenn Sie die Option **Edge-Appliance bereitstellen (Deploy Edge Appliance)** nicht ausgewählt haben, wird das Symbol **Hinzufügen (Add)** (➕) ausgeblendet dargestellt. Klicken Sie auf **Weiter (Next)**, um mit der Konfiguration fortzufahren.
- ◆ Wenn Sie **Edge-Appliance bereitstellen (Deploy Edge Appliance)** ausgewählt haben, geben Sie die Einstellungen für die virtuelle Appliance des logischen Routers ein.

Beispiel:

Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

Cluster/Resource Pool: * ▼

Datastore: * ▼

Host: ▼

Folder: ▼

12 Konfigurieren Sie Schnittstellen. Auf logischen Routern wird nur IPv4-Adressierung unterstützt.

- a Konfigurieren Sie die Verbindung der HA-Schnittstelle und optional eine IP-Adresse.

Wenn Sie die Option **Edge-Appliance bereitstellen (Deploy Edge Appliance)** ausgewählt haben, müssen Sie die HA-Schnittstelle mit einer verteilten Portgruppe oder mit einem logischen Switch verbinden. Wenn Sie diese Schnittstelle nur als HA-Schnittstelle nutzen, verwenden Sie einen logischen Switch. Es wird ein /30-Subnetz aus dem lokalen Bereich 169.254.0.0/16 des Links zugewiesen und für die Bereitstellung einer IP-Adresse für jede der beiden NSX Edge-Appliances verwendet.

Wenn Sie diese Schnittstelle für die Herstellung einer Verbindung mit dem NSX Edge verwenden möchten, können Sie optional eine zusätzliche IP-Adresse und ein zusätzliches Präfix für die HA-Schnittstelle angeben.

Hinweis Vor NSX 6.2 wurde die HA-Schnittstelle als „Verwaltungsschnittstelle“ bezeichnet. Eine SSH-Verbindung mit der HA-Schnittstelle ist nur möglich, wenn die Verbindung nicht von außerhalb des IP-Subnetzes aufgebaut wird, in dem sich auch die HA-Schnittstelle befindet. Sie können keine statischen Routen konfigurieren, die aus der HA-Schnittstelle herausführen. Dies bedeutet, dass RPF den eingehenden Datenverkehr ablehnt. Sie könnten RPF theoretisch deaktivieren, was jedoch kontraproduktiv für die Hochverfügbarkeit ist. Für den SSH-Zugriff können Sie auch die Protokolladresse des logischen Routers verwenden. Diese wird später beim Konfigurieren des dynamischen Routing konfiguriert.

In NSX 6.2 und höher wird die HA-Schnittstelle eines logischen Routers automatisch von der Route Redistribution ausgeschlossen.

- b Konfigurieren Sie Schnittstellen dieses NSX Edge.

In **Schnittstellen dieses NSX Edge konfigurieren (Configure interfaces of this NSX Edge)**:

Die internen Schnittstellen dienen Verbindungen zu Switches, die eine Kommunikation zwischen virtuellen Maschinen (manchmal als horizontales Routing bezeichnet) zulässt. Interne Schnittstellen werden auf der logischen virtuellen Router-Appliance als Pseudo-vNICs erstellt. Uplink-Schnittstellen dienen nicht der vertikalen Kommunikation. Die Uplink-Schnittstelle eines logischen Routers kann eine Verbindung zu einem Edge Services Gateway oder einer Drittanbieter-Router-VM herstellen. Sie müssen über mindestens eine Uplink-Schnittstelle verfügen, damit das dynamische Routing funktioniert. Uplink-Schnittstellen werden auf der logischen virtuellen Router-Appliance als vNICs erstellt.

Die Schnittstellen-Konfiguration, die Sie hier eingeben, kann später geändert werden. Sie können nach der Bereitstellung eines logischen Routers Schnittstellen hinzufügen, entfernen und verändern.

Das folgende Beispiel zeigt eine mit der verteilten Verwaltungsportgruppe verbundene HA-Schnittstelle. Das Beispiel zeigt zudem zwei interne Schnittstellen (App und Web) sowie eine Uplink-Schnittstelle (zu ESG).

New NSX Edge

1 Name and description

2 Settings

3 Configure deployment

4 Configure interfaces

5 Default gateway settings

6 Ready to complete

Configure interfaces

HA interface Configuration

Connected To: [Change](#) [Remove](#)

+

x

IP Address	Subnet Prefix Length
192.168.110.60*	24

HA interface is a mandatory special-purpose interface that requires network connectivity and is configured separately from other interfaces in the Logical Router.

Configure interfaces of this NSX Edge

+

x

Name	IP Address	Subnet Prefix Length	Connected To
app	172.16.20.1*	24	app
web	172.16.10.1*	24	web
to-ESG	192.168.10.2*	29	transit

Back

Next

Finish

Cancel

13 Konfigurieren Sie ein Standard-Gateway.

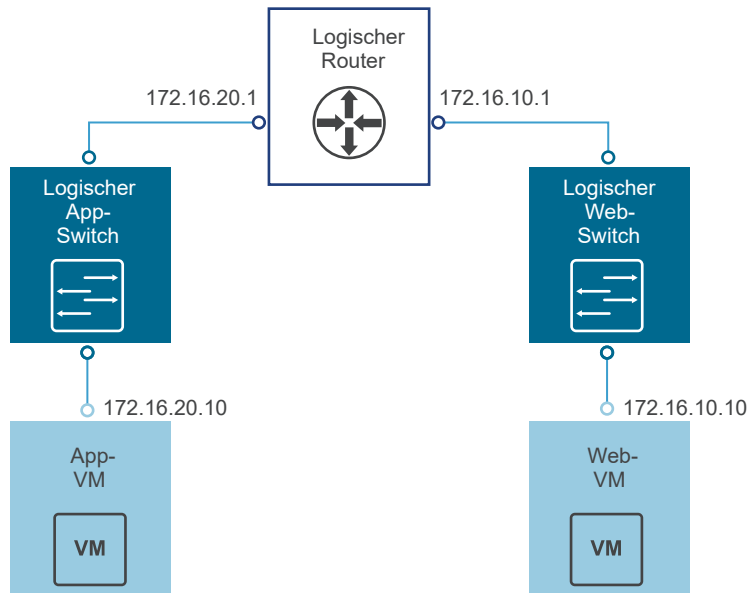
Beispiel:

The screenshot shows the 'New NSX Edge' configuration window. On the left, a progress bar indicates the following steps: 1 Name and description, 2 Settings, 3 Configure deployment, 4 Configure interfaces, 5 Default gateway settings (selected), and 6 Ready to complete. The main configuration area is titled 'Default gateway settings'. It includes a checkbox labeled 'Configure Default Gateway' which is checked. Below this, there are three input fields: 'vNIC' with a dropdown menu showing 'to-ESG', 'Gateway IP' with the text '192.168.10.1', and 'MTU' with the text '1500'. At the bottom of the window, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

- 14 Stellen Sie sicher, dass die Standard-Gateways aller an die logischen Switches angehängten VMs ordnungsgemäß auf die IP-Adressen der logischen Router-Schnittstellen eingestellt sind.

Ergebnisse

In der folgenden Beispiel-Topologie ist das Standard-Gateway der App-VM 172.16.20.1. Das Standard-Gateway der Web-VM ist 172.16.10.1. Stellen Sie sicher, dass die VMs ihre Standard-Gateways und sich gegenseitig pinggen können.



Stellen Sie mit SSH oder über die Konsole eine Verbindung mit dem NSX Manager her und führen Sie die folgenden Befehle aus:

- Führen Sie alle Informationen zur logischen Router-Instanz auf.

```

nsxmgr-l-01a> show logical-router list all
Edge-id      Vdr Name          Vdr id          #Lifs
edge-1       default+edge-1    0x00001388      3
  
```

- Führen Sie die Hosts auf, die vom Controller-Cluster Routing-Informationen für den logischen Router empfangen haben.

```

nsxmgr-l-01a> show logical-router list dlr edge-1 host
ID           HostName
host-25      192.168.210.52
host-26      192.168.210.53
host-24      192.168.110.53
  
```

Die Ausgabe umfasst alle Hosts von allen Hostclustern, die als Mitglieder der Transportzone konfiguriert wurden, welche den mit dem angegebenen logischen Router verbundenen logischen Switch besitzt (in diesem Beispiel edge-1).

- Führen Sie die Routing-Tabelleninformationen auf, die vom logischen Router zu den Hosts übertragen werden. Einträge der Routing-Tabelle sollten über sämtliche Hosts hinweg einheitlich sein.

```

nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 route

VDR default+edge-1 Route Table
Legend: [U: Up], [G: Gateway], [C: Connected], [I: Interface]
Legend: [H: Host], [F: Soft Flush] [!: Reject] [E: ECMP]

Destination  GenMask      Gateway      Flags  Ref Origin  UpTime  Interface
-----
0.0.0.0      0.0.0.0      192.168.10.1  UG     1  AUTO      4101    138800000002
  
```

172.16.10.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10195	13880000000b
172.16.20.0	255.255.255.0	0.0.0.0	UCI	1	MANUAL	10196	13880000000a
192.168.10.0	255.255.255.248	0.0.0.0	UCI	1	MANUAL	10196	138800000002
192.168.100.0	255.255.255.0	192.168.10.1	UG	1	AUTO	3802	138800000002

- Führen Sie zusätzliche Informationen über den Router aus der Sicht eines Hosts auf. Diese Ausgabe ist hilfreich, um festzustellen, welcher Controller mit dem Host kommuniziert.

```
nsx-mgr-l-01a> show logical-router host host-25 dlr edge-1 verbose
```

```
VDR Instance Information :
```

```
-----
Vdr Name:                default+edge-1
Vdr Id:                  0x00001388
Number of Lifs:          3
Number of Routes:        5
State:                   Enabled
Controller IP:           192.168.110.203
Control Plane IP:        192.168.210.52
Control Plane Active:    Yes
Num unique nexthops:     1
Generation Number:       0
Edge Active:             No
```

Überprüfen Sie das Controller-IP-Feld in der Ausgabe des `show logical-router host host-25 dlr edge-1 verbose`-Befehls.

Verschlüsseln Sie SSH zu einem Controller und führen Sie die folgenden Befehle aus, um die erlernten Informationen des Controllers zum VNI-, VTEP-, MAC- und ARP-Tabellenstatus anzuzeigen.

- ```
192.168.110.202 # show control-cluster logical-switches vni 5000
```

| VNI  | Controller      | BUM-Replication | ARP-Proxy | Connections |
|------|-----------------|-----------------|-----------|-------------|
| 5000 | 192.168.110.201 | Enabled         | Enabled   | 0           |

Die Ausgabe für VNI 5000 zeigt null Verbindungen an und führt Controller 192.168.110.201 als Besitzer für VNI 5000 auf. Melden Sie sich bei diesem Controller an, um weitere Informationen über VNI 5000 zu sammeln.

```
192.168.110.201 # show control-cluster logical-switches vni 5000
```

| VNI  | Controller      | BUM-Replication | ARP-Proxy | Connections |
|------|-----------------|-----------------|-----------|-------------|
| 5000 | 192.168.110.201 | Enabled         | Enabled   | 3           |

Die Ausgabe auf 192.168.110.201 zeigt drei Verbindungen an. Überprüfen Sie zusätzliche VNIs.

```
192.168.110.201 # show control-cluster logical-switches vni 5001
```

| VNI  | Controller      | BUM-Replication | ARP-Proxy | Connections |
|------|-----------------|-----------------|-----------|-------------|
| 5001 | 192.168.110.201 | Enabled         | Enabled   | 3           |

```
192.168.110.201 # show control-cluster logical-switches vni 5002
```

| VNI  | Controller      | BUM-Replication | ARP-Proxy | Connections |
|------|-----------------|-----------------|-----------|-------------|
| 5002 | 192.168.110.201 | Enabled         | Enabled   | 3           |

Da 192.168.110.201 alle drei VNI-Verbindungen besitzt, sollten auf dem anderen Controller, 192.168.110.203, erwartungsgemäß null Verbindungen angezeigt werden.

```
192.168.110.203 # show control-cluster logical-switches vni 5000
VNI Controller BUM-Replication ARP-Proxy Connections
5000 192.168.110.201 Enabled Enabled 0
```

- Pingen Sie vor der Überprüfung der MAC- und ARP-Tabellen eine VM durch die andere VM.

Von App-VM zu Web-VM:

```
vmware@app-vm$ ping 172.16.10.10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_req=1 ttl=64 time=2.605 ms
64 bytes from 172.16.10.10: icmp_req=2 ttl=64 time=1.490 ms
64 bytes from 172.16.10.10: icmp_req=3 ttl=64 time=2.422 ms
```

Überprüfen Sie die MAC-Tabellen.

```
192.168.110.201 # show control-cluster logical-switches mac-table 5000
VNI MAC VTEP-IP Connection-ID
5000 00:50:56:a6:23:ae 192.168.250.52 7
```

```
192.168.110.201 # show control-cluster logical-switches mac-table 5001
VNI MAC VTEP-IP Connection-ID
5001 00:50:56:a6:8d:72 192.168.250.51 23
```

Überprüfen Sie die ARP-Tabellen.

```
192.168.110.201 # show control-cluster logical-switches arp-table 5000
VNI IP MAC Connection-ID
5000 172.16.20.10 00:50:56:a6:23:ae 7
```

```
192.168.110.201 # show control-cluster logical-switches arp-table 5001
VNI IP MAC Connection-ID
5001 172.16.10.10 00:50:56:a6:8d:72 23
```

Überprüfen Sie die Informationen zum logischen Router. Jede logische Router-Instanz wird durch einen der Controller-Knoten bedient.

Der `instance`-Unterbefehl des `show control-cluster logical-routers`-Befehls zeigt eine Liste mit logischen Routern an, die mit diesem Controller verbunden sind.

Der `interface-summary`-Unterbefehl zeigt die LIFs an, die der Controller vom NSX Manager abgerufen hat. Diese Informationen werden an die Hosts gesendet, die sich in den unter der Transportzone verwalteten Hostclustern befinden.

Der `routes`-Unterbefehl zeigt die Routing-Tabelle an, die von der virtuellen Appliance des logischen Routers (auch als Kontroll-VM bezeichnet) an diesen Controller gesendet wird. Anders als bei ESXi-Hosts enthält diese Routing-Tabelle keine direkt verbundenen Subnetze, da diese Informationen von der LIF-Konfiguration bereitgestellt werden. Route-Informationen auf den ESXi-Hosts umfassen direkt verbundene Subnetze, da es sich in diesem Fall um eine vom Datenpfad des ESXi-Host verwendete Weiterleitungstabelle handelt.

- Listen Sie alle logischen Router auf, die mit diesem Controller verbunden sind.

```
controller # show control-cluster logical-routers instance all
LR-Id LR-Name Universal Service-Controller Egress-Locale
0x1388 default+edge-1 false 192.168.110.201 local
```

Notieren Sie die LR-ID und verwenden Sie sie im folgenden Befehl.

- `controller # show control-cluster logical-routers interface-summary 0x1388`

| Interface    | Type | Id     | IP[]            |
|--------------|------|--------|-----------------|
| 13880000000b | vxl  | 0x1389 | 172.16.10.1/24  |
| 13880000000a | vxl  | 0x1388 | 172.16.20.1/24  |
| 138800000002 | vxl  | 0x138a | 192.168.10.2/29 |

- `controller # show control-cluster logical-routers routes 0x1388`

| Destination      | Next-Hop[]   | Preference | Locale-Id                            | Source     |
|------------------|--------------|------------|--------------------------------------|------------|
| 192.168.100.0/24 | 192.168.10.1 | 110        | 00000000-0000-0000-0000-000000000000 | CONTROL_VM |
| 0.0.0.0/0        | 192.168.10.1 | 0          | 00000000-0000-0000-0000-000000000000 | CONTROL_VM |

```
[root@comp02a:~] esxcfg-route -l
```

VMkernel Routes:

| Network       | Netmask       | Gateway       | Interface |
|---------------|---------------|---------------|-----------|
| 10.20.20.0    | 255.255.255.0 | Local Subnet  | vmk1      |
| 192.168.210.0 | 255.255.255.0 | Local Subnet  | vmk0      |
| default       | 0.0.0.0       | 192.168.210.1 | vmk0      |

- Zeigen Sie die Verbindungen des Controllers mit dem speziellen VNI an.

```
192.168.110.203 # show control-cluster logical-switches connection-table 5000
```

| Host-IP        | Port  | ID |
|----------------|-------|----|
| 192.168.110.53 | 26167 | 4  |
| 192.168.210.52 | 27645 | 5  |
| 192.168.210.53 | 40895 | 6  |

```
192.168.110.202 # show control-cluster logical-switches connection-table 5001
```

| Host-IP        | Port  | ID |
|----------------|-------|----|
| 192.168.110.53 | 26167 | 4  |
| 192.168.210.52 | 27645 | 5  |
| 192.168.210.53 | 40895 | 6  |

Bei diesen Host-IP-Adressen handelt es sich nicht um VTEPs, sondern um vmk0-Schnittstellen. Verbindungen zwischen ESXi-Hosts und Controllern werden im Verwaltungsnetzwerk erstellt. Bei den Portnummern hier handelt es sich um flüchtige TCP-Ports, die vom ESXi-Host-IP-Stack zugewiesen werden, wenn der Host eine Verbindung zum Controller herstellt.

- Auf dem Host können Sie die mit der Portnummer übereinstimmende Controller-Netzwerkverbindung anzeigen.

```
[root@192.168.110.53:~] #esxcli network ip connection list | grep 26167
tcp 0 0 192.168.110.53:26167 192.168.110.101:1234 ESTABLISHED
96416 newreno netcpa-worker
```

- Zeigen Sie aktive VNIs auf dem Host an. Beobachten Sie, wie die Ausgabe über die Hosts hinweg unterschiedlich ist. Nicht alle VNIs sind auf allen Hosts aktiv. Ein VNI ist auf einem Host aktiv, wenn der Host eine mit dem logischen Switch verbundene VM aufweist.

```
[root@192.168.210.52:~] # esxcli network vswitch dvs vmware vxlan network list --vds-name
Compute_VDS
```

| VXLAN ID   | Multicast IP              | Control Plane                        | Controller Connection |
|------------|---------------------------|--------------------------------------|-----------------------|
| Port Count | MAC Entry Count           | ARP Entry Count                      | VTEP Count            |
| 5000       | N/A (headend replication) | Enabled (multicast proxy, ARP proxy) | 192.168.110.203       |
| (up)       | 1                         | 0                                    | 0                     |
| 5001       | N/A (headend replication) | Enabled (multicast proxy, ARP proxy) | 192.168.110.202       |
| (up)       | 1                         | 0                                    | 0                     |

**Hinweis** Führen Sie zur Aktivierung des VXLAN-Namespace in vSphere 6,0 und höher den `/etc/init.d/hostd restart`-Befehl aus.

Für logische Switches im Hybrid- oder Unicast-Modus enthält der `esxcli network vswitch dvs vmware vxlan network list --vds-name <vds-name>`-Befehl folgende Ausgabe:

- Die Steuerungskomponente ist aktiviert.
- Multicast-Proxy und ARP-Proxy sind aufgeführt. Der AARP-Proxy wird aufgelistet, auch wenn Sie die IP-Ermittlung deaktiviert haben.
- Eine gültige Controller-IP-Adresse ist aufgeführt und die Verbindung ist aktiv.
- Wenn ein logischer Router mit dem ESXi-Host verbunden ist, beträgt die Portanzahl mindestens 1, auch wenn auf dem mit dem logischen Switch verbundenen Host keine VMs vorhanden sind. Dieser eine Port ist der vdrPort, bei welchem es sich um einen speziellen dvPort handelt, der mit dem Kernelmodul des logischen Routers auf dem ESXi-Host verbunden ist.

- Pingen Sie zuerst mit einer VM die andere VM auf einem anderen Subnetz an und zeigen Sie anschließend die MAC-Tabelle an. Beachten Sie, dass „Inner MAC“ der Eintrag der VM ist, während sich „Outer MAC“ und „Outer IP“ auf den VTEP beziehen.

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5000
```

| Inner MAC         | Outer MAC         | Outer IP       | Flags    |
|-------------------|-------------------|----------------|----------|
| 00:50:56:a6:23:ae | 00:50:56:6a:65:c2 | 192.168.250.52 | 00000111 |

```
~ # esxcli network vswitch dvs vmware vxlan network mac list --vds-name=Compute_VDS --vxlan-id=5001
```

| Inner MAC         | Outer MAC         | Outer IP       | Flags    |
|-------------------|-------------------|----------------|----------|
| 02:50:56:56:44:52 | 00:50:56:6a:65:c2 | 192.168.250.52 | 00000101 |
| 00:50:56:f0:d7:e4 | 00:50:56:6a:65:c2 | 192.168.250.52 | 00000111 |

### Nächste Schritte

Wenn Sie eine NSX Edge-Appliance installieren, aktiviert NSX das automatische Starten/Herunterfahren von virtuellen Maschinen auf dem Host, wenn die vSphere HA auf dem Cluster deaktiviert ist. Wenn die Appliance-VMs später auf andere Hosts im Cluster migriert werden, ist auf den neuen Hosts das automatische Starten/Herunterfahren von virtuellen Maschinen möglicherweise nicht aktiviert. Aus diesem Grund wird von VMware empfohlen, bei der Installation von NSX Edge-Appliances auf Clustern, auf denen die vSphere HA deaktiviert ist, alle Hosts im Cluster zu überprüfen, um sicherzustellen, dass das automatische Starten/Herunterfahren aktiviert ist. Weitere Informationen erhalten Sie unter „Bearbeiten der Einstellungen zum Starten/Herunterfahren virtueller Maschinen“ im Dokument *Verwaltung virtueller vSphere-Maschinen*.

Doppelklicken Sie nach der Bereitstellung des Routers auf die ID des logischen Routers, um weitere Einstellungen zu konfigurieren, wie z. B. Schnittstellen, Routing, Firewall, Bridging und DHCP-Relay.

## Hinzufügen eines Edge Services Gateway

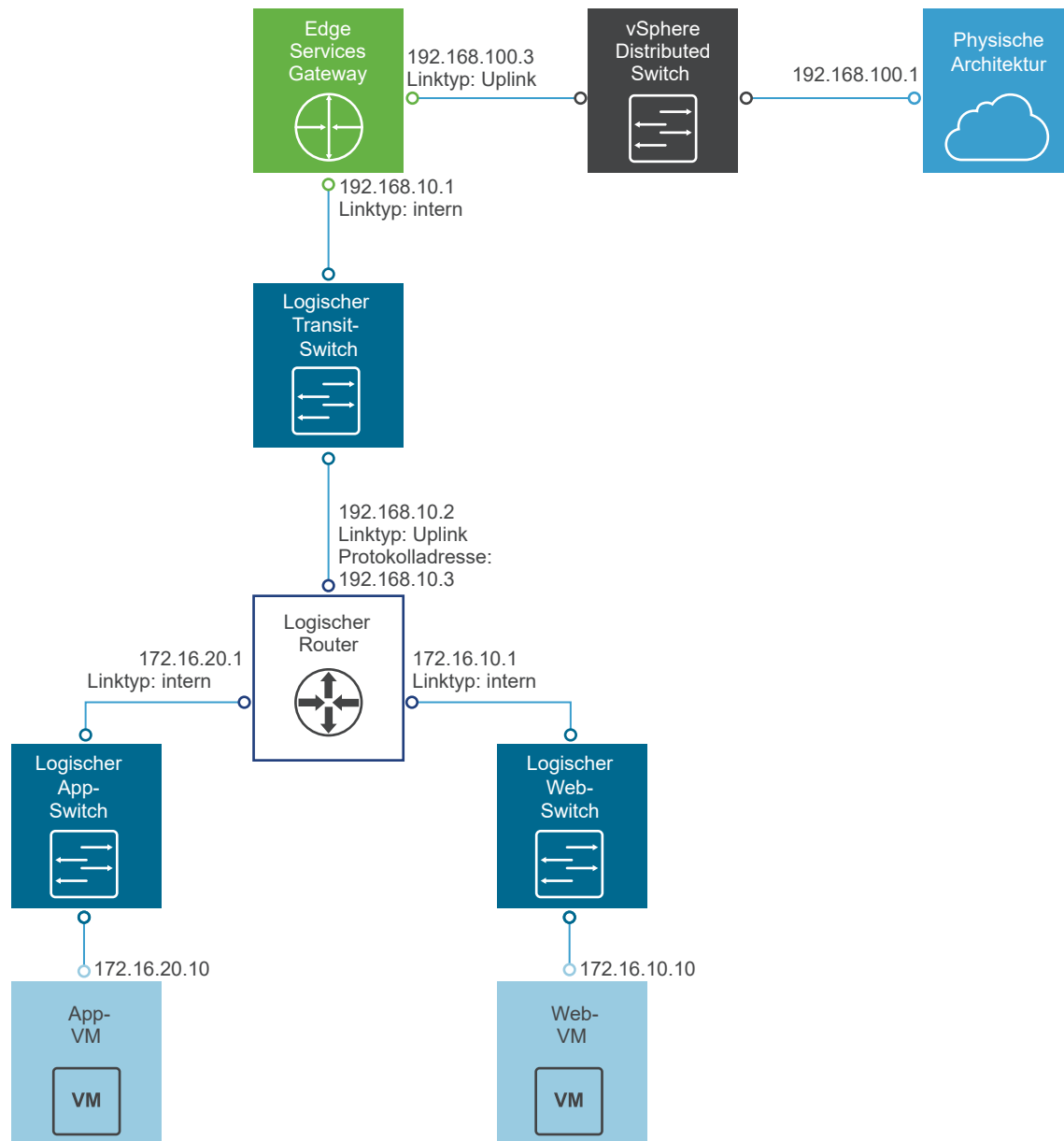
Sie können mehrere virtuelle NSX Edge Services Gateway-Appliances in einem Datacenter installieren. Jede virtuelle NSX Edge-Appliance kann über insgesamt zehn Uplink- und interne Netzwerkschnittstellen verfügen. Die internen Schnittstellen werden mit gesicherten Portgruppen verbunden und dienen als das Gateway für alle geschützten virtuellen Maschinen in der Portgruppe. Das Subnetz, das der internen Schnittstelle zugewiesen ist, kann ein öffentlich gerouteter IP-Adressbereich, ein gerouteter privater RFC 1918-Adressbereich oder privater RFC 1918-Adressbereich sein, der NAT verwendet. Firewallregeln und andere NSX Edge-Dienste werden beim Datenverkehr zwischen Schnittstellen erzwungen.

Uplink-Schnittstellen von ESG stellen Verbindungen zu Uplink-Portgruppen her, die Zugriff auf ein gemeinsam genutztes Unternehmensnetzwerk oder einen Dienst haben, das bzw. der Zugriffsschichten im Netzwerk bereitstellt.

In der folgenden Liste wird die Unterstützung von Funktionen nach Schnittstellenart (intern und Uplink) in einem ESG beschrieben.

- DHCP: wird nicht in einer Uplink-Schnittstelle unterstützt.
- DNS-Weiterleitung: wird nicht in einer Uplink-Schnittstelle unterstützt.
- HA: wird nicht in einer Uplink-Schnittstelle unterstützt, erfordert mindestens eine interne Schnittstelle.
- SSL VPN: Listener-IP muss zur Uplink-Schnittstelle gehören.
- IPSec-VPN: Listener-IP muss zur Uplink-Schnittstelle gehören.
- L2 VPN: Es können nur interne Netzwerke ausgeweitet werden.

Die folgende Abbildung zeigt eine Beispieltopologie mit einer Uplink-Schnittstelle von ESG, die mit der physischen Infrastruktur durch den vSphere Distributed Switch verbunden ist, und der internen Schnittstelle von ESG, die mit einem NSX Logical Router durch einen NSX Logical Transit Switch verbunden ist.



Mehrere externe IP-Adressen können für Load-Balancing-, Site-to-Site-VPN- und NAT-Dienste konfiguriert werden.


**Wichtig** Wenn Sie die Hochverfügbarkeit (High Availability, HA) auf einem NSX Edge in einer Cross-vCenter NSX-Umgebung aktivieren, müssen sich die aktive und die Standby-NSX Edge-Appliance im selben vCenter Server befinden. Wenn Sie ein Mitglied eines NSX Edge-HA-Paares auf ein anderes vCenter Server-System migrieren, können die beiden HA-Appliances nicht mehr als HA-Paar ausgeführt werden. Dies kann zu einer Unterbrechung des Datenverkehrs führen.

#### Voraussetzungen

- Ihnen muss die Rolle „Enterprise-Administrator“ oder „NSX-Administrator“ zugewiesen worden sein.

- Stellen Sie sicher, dass der Ressourcenpool genug Kapazität für die Bereitstellung der virtuellen Edge Services Gateway (ESG)-Appliance aufweist. Weitere Informationen dazu finden Sie unter [Kapitel 1 Systemvoraussetzungen für NSX](#).
- Stellen Sie sicher, dass die Hostcluster, auf denen die NSX Edge-Appliance installiert wird, für NSX vorbereitet ist. Informationen dazu erhalten Sie unter „Vorbereiten der Hostcluster für NSX“ in der Dokumentation *Installationshandbuch für NSX*.

## Verfahren

- 1 Navigieren Sie in vCenter zu **Home > Networking & Security > NSX Edges** und klicken Sie auf das Symbol **Hinzufügen (Add)** (  ).

- 2 Wählen Sie **Edge Services Gateway** aus und geben Sie einen Namen für das Gerät ein.

Dieser Name wird in Ihrer vCenter-Bestandsliste angezeigt. Der Name muss über alle ESGs eines einzelnen Mandanten hinweg eindeutig sein.

Sie können optional auch einen Hostnamen eingeben. Dieser Name wird in der Befehlszeilenschnittstelle angezeigt. Wenn Sie keinen Hostnamen angeben, wird die automatisch erstellte Edge-ID in CLI angezeigt.

Sie können auch eine Beschreibung und einen Mandanten eingeben und „High Availability“ aktivieren.

Beispiel:

**New NSX Edge**

1 Name and description  
 2 Settings  
 3 Configure deployment  
 4 Configure interfaces  
 5 Default gateway settings  
 6 Firewall and HA  
 7 Ready to complete

**Name and description**

Install Type: ☒ Edge Services Gateway  
*Provides common gateway services such as DHCP, Firewall, VPN, NAT, Routing and Load Balancing.*

☐ Logical (Distributed) Router  
*Provides Distributed Routing and Bridging capabilities.*

Name:

Hostname:

Description:

Tenant:

☒ Deploy NSX Edge  
*Select this option to create a new NSX Edge in deployed mode. Appliance and interface configuration is mandatory to deploy the NSX Edge.*

☐ Enable High Availability  
*Enable HA, for enabling and configuring High Availability.*

Back Next Finish Cancel

- 3 Geben Sie ein Kennwort für das ESG ein und bestätigen Sie es.

Das Kennwort muss mindestens 12 Zeichen lang sein und 3 der 4 folgenden Regeln folgen:

- mindestens ein Großbuchstabe
- mindestens ein Kleinbuchstabe
- mindestens eine Zahl
- mindestens ein Sonderzeichen

- 4 (Optional) Aktivieren Sie SSH, hohe Verfügbarkeit, automatische Regelgenerierung und FIPS-Modus, und legen Sie die Protokollierungsebene fest.

Wenn Sie die automatische Regelerstellung nicht aktivieren, müssen Sie die Firewall-, NAT- und Routing-Konfiguration manuell hinzufügen, um den Steuerungsdatenverkehr für bestimmte NSX Edge-Dienste wie beispielsweise Load Balancing, VPN zu ermöglichen. Die Option „Automatische Regelerstellung“ erstellt keine Regeln für Datenkanal-Datenverkehr.

Standardmäßig sind SSH und High Availability deaktiviert und die automatische Regelerstellung ist aktiviert.

Der FIPS-Modus ist standardmäßig deaktiviert.

Als Protokollierungsebene ist standardmäßig „Notfall“ eingestellt.

Beispiel:

- 5 Wählen Sie die Größe der NSX Edge-Instanz basierend auf den Systemressourcen aus.

Das **große (Large)** NSX Edge verfügt über mehr CPU, Arbeitsspeicher und Festplattenspeicher als das **kompakte (Compact)** NSX Edge und unterstützt eine größere Anzahl an gleichzeitigen SSL VPN-Plus-Benutzern. Das **sehr große (X-Large)** NSX Edge eignet sich für Umgebungen, die über einen Load Balancer mit Millionen von gleichzeitig ausgeführten Sitzungen verfügen. Das Quad Large NSX Edge wird bei hohem Durchsatz empfohlen und benötigt eine hohe Verbindungsrate.

Weitere Informationen dazu finden Sie unter [Kapitel 1 Systemvoraussetzungen für NSX](#).

- 6 Erstellen Sie eine Edge-Appliance.

Geben Sie die Einstellungen für die virtuelle ESG-Appliance ein, die zur vCenter-Bestandsliste hinzugefügt wird. Wenn Sie bei der Installation von NSX Edge keine Appliance hinzufügen, bleibt NSX Edge so lange im Offline-Modus, bis Sie eine Appliance hinzugefügt haben.

Wenn HA aktiviert ist, können Sie zwei Appliances hinzufügen. Wenn Sie eine einzelne Appliance hinzufügen, repliziert NSX Edge deren Konfiguration für die Standby-Appliance und stellt sicher, dass sich die zwei virtuellen HA-NSX Edge-Maschinen auch dann nicht auf demselben ESX-Host befinden, wenn Sie DRS und vMotion verwendet haben (es sei denn, Sie migrieren sie per vMotion manuell auf denselben Host). Damit HA ordnungsgemäß funktioniert, müssen Sie beide Appliances in einem gemeinsam verwendeten Datenspeicher bereitstellen.

Beispiel:

Add NSX Edge Appliance

Specify placement parameters for the NSX Edge appliance.

|                        |   |                           |   |
|------------------------|---|---------------------------|---|
| Cluster/Resource Pool: | * | Management & Edge ...     | ▼ |
| Datastore:             | * | ds-1                      | ▼ |
| Host:                  |   | esxmgmt-01a.corp.local    | ▼ |
| Folder:                |   | Discovered virtual mac... | ▼ |

- 7 Wählen Sie **NSX Edge bereitstellen (Deploy NSX Edge)** aus, um den Edge in einem bereitgestellten Modus hinzuzufügen. Sie müssen Appliances und Schnittstellen für die Edge-Instanz konfigurieren, bevor sie bereitgestellt werden kann.

- 8 Konfigurieren Sie Schnittstellen.

Auf ESGs werden sowohl IPv4- als auch IPv6-Adressen unterstützt.

Sie müssen mindestens eine interne Schnittstelle hinzufügen, damit HA funktioniert.

Eine Schnittstelle kann über mehrere nicht überlappende Subnetze verfügen.

Wenn Sie mehr als eine IP-Adresse für eine Schnittstelle eingeben, können Sie die primäre IP-Adresse auswählen. Eine Schnittstelle kann eine primäre und mehrere sekundäre IP-Adressen aufweisen. NSX Edge betrachtet die primäre IP-Adresse als Quelladresse für lokal generierten Datenverkehr, wie z. B. Remote-Syslog- und Operator-initiierte Pings.

Sie müssen der Schnittstelle zuerst eine IP-Adresse hinzufügen, bevor Sie sie für jede beliebige Funktionskonfiguration verwenden können.

Sie können auch die MAC-Adresse für die Schnittstelle hinzufügen.

Wenn Sie die MAC-Adresse später mithilfe des API-Aufrufs ändern, müssen Sie das Edge nach der Änderung der MAC-Adresse erneut bereitstellen.

Wenn HA aktiviert ist, können Sie optional zwei Verwaltungs-IP-Adressen im CIDR-Format eingeben. Die Taktsignale der zwei virtuellen NSX Edge-HA-Maschinen werden über diese Verwaltungs-IP-Adressen übertragen. Die Verwaltungs-IP-Adressen müssen sich in demselben L2/Subnetz befinden und müssen untereinander kommunizieren können.

Sie können auch den MTU-Wert ändern.

Aktivieren Sie Proxy-ARP, wenn das ESG ARP-Anforderungen beantworten soll, die für andere Maschinen bestimmt sind. Dies ist dann zum Beispiel hilfreich, wenn Sie über dasselbe Subnetz auf beiden Seiten einer WAN-Verbindung verfügen.

Aktivieren Sie die ICMP-Umleitung, um Routing-Informationen an Hosts weiterzuleiten.

Aktivieren Sie umgekehrte Pfadfilter, um zu die Erreichbarkeit der Quelladresse in weitergeleiteten Paketen zu überprüfen. Im aktivierten Modus muss das Paket auf der Schnittstelle empfangen werden, die der Router zum Weiterleiten des Rückgabepakets verwenden würde. Im Loose-Modus muss die Quelladresse in der Routing-Tabelle angezeigt werden.

Konfigurieren Sie Fence-Parameter, wenn Sie IP- und MAC-Adressen über verschiedene umgrenzende Umgebungen hinweg wiederverwenden möchten. In einer Cloud-Verwaltungsplattform (Cloud Management Platform, CMP) können Sie mit Fencing mehrere Cloud-Instanzen gleichzeitig mit denselben IP- und MAC-Adressen ausführen, die vollständig isoliert oder „umgrenzt“ sind.

Beispiel:

**Edit NSX Edge Interface**

vNIC#: 1

Name: \* Internal

Type: ☒ Internal ☐ Uplink

Connected To: transit-switch Change Remove

Connectivity Status: ☒ Connected ☐ Disconnected

Configure subnets

| IP Address    | Subnet Prefix Length |
|---------------|----------------------|
| 192.168.10.1* | 29                   |
|               |                      |
|               |                      |
|               |                      |

MAC Addresses:

You can specify a MAC address or leave it blank for auto generation. In case of HA, two different MAC addresses are required.

MTU:

Options: ☐ Enable Proxy ARP ☐ Send ICMP Redirect Reverse Path Filter Disable ▾

Fence Parameters:

Example: ethernet0.filter1.param1=1

OK Cancel

Das folgende Beispiel zeigt zwei Schnittstellen. Eine Schnittstelle, die das ESG mit der Außenwelt durch eine Uplink-Portgroup in einem vSphere Distributed Switch verbindet, und eine zweite Schnittstelle, die das ESG mit einem Logical Transit Switch verbindet, an den auch ein Distributed Logical Router angefügt ist.

**New NSX Edge**

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- ✓ **4 Configure interfaces**
- 5 Default gateway settings
- 6 Firewall and HA
- 7 Ready to complete

**Configure interfaces**

Configure interfaces of this NSX Edge

+ ✎ ✕

| vNIC# | Name     | IP Address    | Subnet Prefix Length | Connected To         |
|-------|----------|---------------|----------------------|----------------------|
| 0     | uplink   | 192.168.100.3 | 24                   | Mgmt_VDS - HQ_Uplink |
| 1     | internal | 192.168.10.1  | 29                   | transit-switch       |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |
|       |          |               |                      |                      |

Back Next Finish Cancel

## 9 Konfigurieren Sie ein Standard-Gateway.

Sie können den MTU-Wert bearbeiten, er darf jedoch nicht höher als der konfigurierte MTU-Wert für die Schnittstelle sein.

Beispiel:

**New NSX Edge**

✓ 1 Name and description  
 ✓ 2 Settings  
 ✓ 3 Configure deployment  
 ✓ 4 Configure interfaces  
**5 Default gateway settings**  
 6 Firewall and HA  
 7 Ready to complete

**Default gateway settings**

☒ Configure Default Gateway

vNIC: \* uplink

Gateway IP: \* 192.168.100.2

MTU: 1500

Back Next Finish Cancel

###### 10 Konfigurieren Sie die Firewallrichtlinie, die Protokollierung und HA-Parameter.

**Vorsicht** Wenn Sie keine Firewallrichtlinie konfigurieren, ist die Standardrichtlinie gesetzt, um jeglichen Datenverkehr zu verweigern.

Standardmäßig sind Protokolle auf allen neuen NSX Edge-Appliances aktiviert. Die Standardprotokollierungsebene ist HINWEIS. Wenn Protokolle lokal im ESG gespeichert sind, werden durch die Protokollierung möglicherweise zu viele Protokolle generiert und die Leistung von NSX Edge wird beeinträchtigt. Aus diesem Grund ist es empfehlenswert, Remote-Syslog-Server zu konfigurieren und alle Protokolle an eine zentrale Stelle zur Analyse und Überwachung weiterzuleiten.

Wenn Sie High Availability aktiviert haben, vervollständigen Sie den HA-Bereich. Standardmäßig wählt HA automatisch eine interne Schnittstelle aus und weist automatisch verbindungslokale IP-Adressen zu. NSX Edge unterstützt zwei virtuelle Maschinen für High Availability und beide Maschinen werden mithilfe von Benutzerkonfigurationen auf dem neuesten Stand gehalten. Falls ein Taktsignalfehler auf der primären virtuellen Maschine auftritt, wird der Zustand der sekundären

virtuellen Maschine in „aktiv“ geändert. Folglich ist immer eine virtuelle NSX Edge-Maschine im Netzwerk aktiv. NSX Edge repliziert die Konfiguration der primären Appliance für die Standby-Appliance und stellt sicher, dass sich die zwei virtuellen HA-NSX Edge-Maschinen auch dann nicht auf demselben ESX-Host befinden, wenn Sie DRS und vMotion verwendet haben. Zwei virtuelle Maschinen werden auf vCenter in demselben Ressourcenpool und Datenspeicher wie die von Ihnen konfigurierte Appliance bereitgestellt. Die IP-Adressen von lokalen Links werden virtuellen HA-Maschinen in der NSX Edge HA zugewiesen, damit sie untereinander kommunizieren können. Wählen Sie die interne Schnittstelle aus, für die HA-Parameter konfiguriert werden sollen. Wenn Sie BELIEBIG für die Schnittstelle auswählen, aber keine internen Schnittstellen konfiguriert sind, wird auf der Benutzeroberfläche ein Fehler angezeigt. Zwei Edge-Appliances werden erstellt, aber da keine interne Schnittstelle konfiguriert ist, bleibt die neue Edge-Appliance im Standby-Modus und HA wird deaktiviert. Sobald eine interne Schnittstelle konfiguriert ist, wird HA in der Edge-Appliance aktiviert. Geben Sie den Zeitraum (in Sekunden) ein, nach dem die primäre Appliance als inaktiv betrachtet wird und die Backup-Appliance die Arbeit übernimmt, falls die Backup-Appliance kein Taktsignal von der primären Appliance erhält. Das Standardintervall beträgt 15 Sekunden. Sie können auch zwei Verwaltungs-IP-Adressen im CIDR-Format eingeben, die die IP-Adressen der lokalen Links überschreiben, die den virtuellen HA-Maschinen zugewiesen sind. Vergewissern Sie sich, dass sich die Verwaltungs-IP-Adressen nicht mit den IP-Adressen überschneiden, die für andere Schnittstellen verwendet wurden, und dass sie das Routing des Netzwerkdatenverkehrs nicht stören. Sie sollten keine IP-Adresse verwenden, die an einer anderen Stelle im Netzwerk existiert, auch wenn das Netzwerk nicht direkt mit dem NSX Edge verbunden ist.

Beispiel:

**New NSX Edge**

- ✓ 1 Name and description
- ✓ 2 Settings
- ✓ 3 Configure deployment
- ✓ 4 Configure interfaces
- ✓ 5 Default gateway settings
- 6 Firewall and HA**
- 7 Ready to complete

### Firewall and HA

☒ **Configure Firewall default policy**

Default Traffic Policy: ☒ Accept ☐ Deny

Logging: ☐ Enable ☒ Disable

#### Configure HA parameters

Configuring HA parameters is mandatory for HA to work.

vNIC: \* internal

Declare Dead Time: 15 (seconds)

Management IPs:

You can specify pair of IPs (in CIDR format) with /30 subnet. Management IPs must not overlap with any vnic subnets.

Back Next Finish Cancel

## Ergebnisse

Nach der Bereitstellung von ESG navigieren Sie zur Ansicht „Hosts und Cluster“ und öffnen Sie die Konsole der virtuellen Edge-Appliance. Stellen Sie in der Konsole sicher, dass Sie die verbundenen Schnittstellen pingen können.

## Nächste Schritte

Wenn Sie eine NSX Edge-Appliance installieren, aktiviert NSX das automatische Starten/Herunterfahren von virtuellen Maschinen auf dem Host, wenn die vSphere HA auf dem Cluster deaktiviert ist. Wenn die Appliance-VMs später auf andere Hosts im Cluster migriert werden, ist auf den neuen Hosts das automatische Starten/Herunterfahren von virtuellen Maschinen möglicherweise nicht aktiviert. Aus diesem Grund wird von VMware empfohlen, bei der Installation von NSX Edge-Appliances auf Clustern, auf denen die vSphere HA deaktiviert ist, alle Hosts im Cluster zu überprüfen, um sicherzustellen, dass das automatische Starten/Herunterfahren aktiviert ist. Weitere Informationen erhalten Sie unter „Bearbeiten der Einstellungen zum Starten/Herunterfahren virtueller Maschinen“ im Dokument *Verwaltung virtueller vSphere-Maschinen*.

Sie können jetzt Routing konfigurieren, um die Konnektivität von externen Geräten zu Ihren VMs zu ermöglichen.

## Angeben der globalen Konfiguration

Sie können das Standard-Gateway für statische Routen konfigurieren und die dynamischen Routing-Details für ein Edge Services Gateway oder einen Distributed Logical Router festlegen.

Sie müssen über eine funktionierende NSX Edge-Instanz verfügen, bevor Sie das Routing darauf konfigurieren können. Weitere Informationen zur Einrichtung von NSX Edge finden Sie unter [Konfiguration von NSX Edge](#).

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Routing** und anschließend auf **Globale Konfiguration (Global Configuration)**.
- 5 Um das ECMP-Routing (Equal-Cost Multi Path) zu aktivieren, klicken Sie neben **ECMP** auf **Start**.

ECMP ist eine Routing-Strategie, die eine Nächster-Hop-Weiterleitung von Paketen zu einem Ziel über mehrere bestmögliche Wege erlaubt. Diese Wege können als statische Routen oder als Ergebnis von metrischen Berechnungen durch dynamische Routing-Protokolle wie OSPF oder BGP hinzugefügt werden. Mehrere Wege für statische Routen lassen sich durch mehrere nächste Hops hinzufügen, die im Dialogfeld „Statische Routen“ durch Komma getrennt angegeben werden können. Weitere Informationen finden Sie unter [Hinzufügen einer statischen Route](#).

Das Edge Services Gateway verwendet die Linux-Netzwerk-Stackimplementierung, einen Round-Robin-Algorithmus mit einer Zufallskomponente. Nachdem ein nächster Hop für ein bestimmtes Quell- und Ziel-IP-Adressenpaar ausgewählt wurde, wird der ausgewählte nächste Hop im Route-Cache gespeichert. Alle Pakete für diesen Flow gehen zum ausgewählten nächsten Hop. Die standardmäßige Zeitüberschreitung für das IPv4-Route-Cache ist 300 Sekunden (gc\_Zeitüberschreitung). Bleibt ein Eintrag für diesen Zeitraum inaktiv, so kann er aus dem Route-Cache entfernt werden. Die tatsächliche Entfernung findet statt, nachdem der Timer für Speicherbereinigung aktiviert wurde (gc\_Intervall = 60 Sekunden).

Der Distributed Logical Router verwendet einen XOR-Algorithmus, um den nächsten Hop aus einer Liste möglicher nächster Hops von ECMP zu ermitteln. Dieser Algorithmus verwendet die Quell- und die Ziel-IP-Adresse auf dem ausgehenden Paket als Entropiequelle.

Statusorientierte Dienste wie Lastausgleich, VPN, NAT und ESG-Firewall funktionieren nicht mit ECMP. Ab Version NSX 6.1.3 können ECMP und die verteilte Firewall jedoch gleichzeitig aktiviert sein.

- 6 (Nur für UDLR): Um die **Gebietsschema-ID (Locale ID)** in einem Universal Distributed Logical Router (UDLR) zu ändern, klicken Sie neben **Routing-Konfiguration (Routing Configuration)** auf **Bearbeiten (Edit)**. Geben Sie eine Gebietsschema-ID ein und klicken Sie auf **Speichern** oder auf **OK**.

Standardmäßig ist die Lokal-ID auf NSX Manager-UUID festgelegt. Sie können die Gebietsschema-ID jedoch überschreiben, indem Sie den lokalen Ausgang zum Zeitpunkt der Erstellung des globalen Distributed Logical Router aktivieren. Die Gebietsschema-ID wird verwendet, um Routen in einer Cross-vCenter NSX- oder Multi-Site-Umgebung selektiv zu konfigurieren. Weitere Informationen hierzu finden Sie unter [Cross-vCenter NSX-Topologien](#).

Die Gebietsschema-ID muss das UUID-Format aufweisen. Zum Beispiel: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, wobei jedes X durch Ziffern des Hexadezimalsystems (0-F) ersetzt wird.

- 7 Um das Standard-Gateway festzulegen, klicken Sie neben **Standard-Gateway (Default Gateway)** auf **Bearbeiten (Edit)**.

- a Wählen Sie die Schnittstelle aus, von der aus der nächste Hop in Richtung des Zielnetzwerks erreicht werden kann.
- b Geben Sie die Gateway-IP ein.
- c (Optional) Geben Sie die Gebietsschema-ID ein. Die Gebietsschema-ID ist nur auf Universal Logical Routern verfügbar.
- d (Optional) Bearbeiten Sie den MTU.
- e Wenn Sie dazu aufgefordert werden, geben Sie den **Admin Distance (Admin Distance)** ein.

Wählen Sie einen Wert zwischen 1 und 255. Der Admin Distance wird zur Auswahl der Route verwendet, wenn mehrere Routen für ein bestimmtes Netzwerk verwendet werden können. Je geringer der Admin Distance, desto höher ist die Präferenz für die Route.

**Tabelle 9-1. Standard-Admin-Abstände**

| Routenquelle             | Standard-Admin Distance |
|--------------------------|-------------------------|
| Verbunden                | 0                       |
| Statisch                 | 1                       |
| Externes BGP             | 20                      |
| Area-internes OSPF       | 30                      |
| Area-übergreifendes OSPF | 110                     |
| Internes BGP             | 200                     |

- f (Optional) Geben Sie eine Beschreibung für das Standard-Gateway ein.
- g Klicken Sie auf **Speichern (Save)**.

- 8 Um das dynamische Routing zu konfigurieren, klicken Sie neben **Konfiguration für dynamisches Routing (Dynamic Routing Configuration)** auf **Bearbeiten (Edit)**.
  - a **Router-ID (Router ID)** zeigt die erste Uplink-IP-Adresse von NSX Edge an, die die Routen zum Kernel für dynamisches Routing überträgt.
  - b Aktivieren Sie hier keine Protokolle.
  - c Wählen Sie **Protokollierung aktivieren (Enable Logging)** aus, um Protokollierungsinformationen zu speichern, und wählen Sie die Protokollierungsebene aus.

---

**Hinweis** Falls Sie in Ihrer Umgebung IPSec-VPN konfiguriert haben, sollten Sie kein dynamisches Routing verwenden.

---

- 9 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

### Nächste Schritte

Klicken Sie zum Löschen der Routing-Konfiguration auf **Zurücksetzen (Reset)**. Dadurch werden alle Routing-Konfigurationen gelöscht (standardmäßige, statische, OSPF- und BGP-Konfigurationen sowie Route Redistribution).

## Konfiguration von NSX Edge

Sobald Sie ein funktionierendes NSX Edge installiert haben (z. B. eine oder mehrere Anwendungen und Schnittstellen hinzugefügt und das Standard-Gateway, die Firewall-Richtlinie und High Availability konfiguriert haben), können Sie NSX Edge-Dienste verwenden.

### Arbeiten mit Zertifikaten

NSX Edge unterstützt selbstsignierte Zertifikate, von einer Zertifizierungsstelle (CA) signierte Zertifikate und Zertifikate, die von einer Zertifizierungsstelle generiert und signiert wurden.

### Konfigurieren eines von einer Zertifizierungsstelle signierten Zertifikats

Sie können eine Signaturanforderung (CSR) generieren und sie von einer Zertifizierungsstelle signieren lassen. Wenn Sie eine CSR auf globaler Ebene generieren, steht sie allen NSX Edges in Ihrer Bestandsliste zur Verfügung.

## Verfahren

- 1 Führen Sie einen der folgenden Schritte aus.

| Option                                           | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Generieren eines globalen Zertifikats</b>     | <ol style="list-style-type: none"> <li>a Melden Sie sich bei der virtuellen NSX Manager-Appliance an.</li> <li>b Klicken Sie auf die Registerkarte „Verwalten“ und anschließend auf „SSL-Zertifikate“.</li> <li>c Klicken Sie auf <b>CSR erzeugen (Generate CSR)</b>.</li> </ol>                                                                                                                                                                                                                                                                                     |
| <b>Generieren eines Zertifikats für NSX Edge</b> | <ol style="list-style-type: none"> <li>a Melden Sie sich beim vSphere Web Client an.</li> <li>b Klicken Sie auf <b>Networking &amp; Security</b> und dann auf <b>Edge Services</b>.</li> <li>c Doppelklicken Sie auf eine NSX Edge-Instanz.</li> <li>d Klicken Sie auf die Registerkarte <b>Verwalten (Manage)</b> und anschließend auf <b>Einstellungen (Settings)</b>.</li> <li>e Klicken Sie auf den Link <b>Zertifikate (Certificates)</b>.</li> <li>f Klicken Sie auf <b>Aktionen (Actions)</b> und wählen Sie <b>CSR generieren (Generate CSR)</b>.</li> </ol> |

- 2 Geben Sie den Namen Ihres Unternehmens und der Organisationseinheit ein.
- 3 Geben Sie Ort, Straße und Land Ihres Unternehmens ein.
- 4 Wählen Sie den Verschlüsselungsalgorithmus für die Kommunikation zwischen den Hosts aus.  
Beachten Sie, dass SSL VPN-Plus nur RSA-Zertifikate unterstützt.

- 5 Ändern Sie bei Bedarf die Standardschlüsselgröße.

- 6 Geben Sie für ein globales Zertifikat eine Beschreibung ein.

- 7 Klicken Sie auf **OK**.

Die Signaturanforderung wird generiert und in der Zertifikatsliste angezeigt.

- 8 Lassen Sie diese CSR von einer Online-Zertifizierungsstelle signieren.

- 9 Importieren Sie das signierte Zertifikat.


- a Kopieren Sie den Inhalt des signierten Zertifikats.
- b Führen Sie einen der folgenden Schritte aus.
  - Um ein signiertes Zertifikat auf der globalen Ebene zu importieren, klicken Sie in der virtuellen NSX Manager Virtual Appliance auf **Importieren (Import)**.
  - Um ein signiertes Zertifikat für eine NSX Edge-Instanz zu importieren, klicken Sie auf **Aktionen (Actions)** und wählen Sie auf der Registerkarte **Zertifikate (Certificates)** die Option **Zertifikat importieren (Import Certificate)** aus.
- c Fügen Sie im Dialogfeld „CSR importieren“ den Inhalt des signierten Zertifikats ein.
- d Klicken Sie auf **OK**.

Das von der Zertifizierungsstelle signierte Zertifikat wird in die Liste der Zertifikate aufgenommen.

## Hinzufügen eines CA-Zertifikats

Durch das Hinzufügen eines CA-Zertifikats werden Sie zur Interim-Zertifizierungsstelle (CA) für Ihr Unternehmen. Sie sind dann berechtigt, Ihre eigenen Zertifikate zu signieren.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und stellen Sie anschließend sicher, dass Sie sich auf der Registerkarte **Einstellungen (Settings)** befinden.
- 5 Klicken Sie auf **Zertifikate (Certificates)**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (  ) und wählen Sie anschließend **CA-Zertifikat (CA Certificate.)** aus.
- 7 Kopieren Sie den Zertifikatsinhalt, und fügen Sie ihn in das Textfeld „Zertifikatsinhalt“ ein.
- 8 Geben Sie eine Beschreibung für das CA-Zertifikat ein.
- 9 Klicken Sie auf **OK**.

Sie können jetzt Ihre eigenen Zertifikate signieren.

## Hinzufügen eines verketteten Zertifikats

Informationen zum Hinzufügen eines Serverzertifikats, das mit Zwischen- und Stamm-CA-Zertifikaten verkettet ist, benötigen Sie ein Serverzertifikat (PEM-Datei), einen privaten Schlüssel für den Servers sowie ein Zwischen- und ein Stammzertifikat.

So importieren Sie das Serverzertifikat als ein Zertifikat, das mit dem Zwischenzertifikat auf dem NSX Edge verkettet wird:

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und stellen Sie anschließend sicher, dass Sie sich auf der Registerkarte **Einstellungen (Settings)** befinden.
- 5 Klicken Sie auf **Zertifikate (Certificates)**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (  ) und wählen Sie anschließend **Zertifikat (Certificate.)** aus.

- 7 Kopieren Sie die Inhalte der cert.pem-Datei des Servers in das Feld **Zertifikatsinhalte (Certificates Contents)** und hängen Sie anschließend den Inhalt der Zwischenzertifikate und des Root-Zertifikats an.

In der Zertifikatskette muss die Reihenfolge der Zertifikate wie folgt lauten:

- Serverzertifikat
- Eine beliebige Anzahl von CA-Zwischenzertifikaten
- CA-Root-Zertifikat

Jedes Zertifikat muss die Zeilen -----BEGIN CERTIFICATE----- und -----END CERTIFICATE----- enthalten, wie im folgenden Beispiel gezeigt:

```
-----BEGIN CERTIFICATE-----
 Server cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 Root cert
-----END CERTIFICATE-----
```

- 8 Fügen Sie im Textfeld **Privater Schlüssel (Private Key)** den Privatschlüsselinhalt des Servers ein.

Es folgt ein Beispiel für den Inhalt des privaten Schlüssels:

```
-----BEGIN RSA PRIVATE KEY-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END RSA PRIVATE KEY-----
```

- 9 Geben Sie das Kennwort für den privaten Schlüssel des Servers ein. Wiederholen Sie es zur Bestätigung.
- 10 (Optional) Geben Sie eine Beschreibung für das verkettete Zertifikat ein.
- 11 Klicken Sie auf **OK**.

## Ergebnisse

Nach dem Import der Zertifikate sollte das Serverzertifikat, das mit den Zwischenzertifikaten verkettet ist, unter **Zertifikatsdetails (Certificate Details)** angezeigt werden.

## Konfigurieren eines selbstsignierten Zertifikats

Sie können selbstsignierte Serverzertifikate erstellen, installieren und verwalten.

### Voraussetzungen

Stellen Sie sicher, dass Sie über ein CA-Zertifikat verfügen, sodass Sie Ihre eigenen Zertifikate signieren können.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und stellen Sie anschließend sicher, dass Sie sich auf der Registerkarte **Einstellungen (Settings)** befinden.
- 5 Klicken Sie auf **Zertifikate (Certificates)**.
- 6 Führen Sie zum Generieren einer Zertifikatsignaturanforderung (CSR) die folgenden Schritte aus.
  - a Klicken Sie auf **Aktionen (Actions)** und wählen Sie **CSR generieren (Generate CSR)**.
  - b Geben Sie im Feld „Allgemeiner Name“ die IP-Adresse oder den vollqualifizierten Domännennamen (FQDN) des NSX Managers ein.
  - c Geben Sie den Namen Ihres Unternehmens und der Organisationseinheit ein.
  - d Geben Sie Ort, Straße und Land Ihres Unternehmens ein.
  - e Wählen Sie den Verschlüsselungsalgorithmus für die Kommunikation zwischen den Hosts aus.  
Beachten Sie, dass SSL VPN-Plus nur RSA-Zertifikate unterstützt. Zwecks Abwärtskompatibilität wird RSA empfohlen.
  - f Ändern Sie bei Bedarf die Standardschlüsselgröße.
  - g Geben Sie eine Beschreibung für das Zertifikat ein.
  - h Klicken Sie auf **OK**.

Die Signaturanforderung wird generiert und in der Zertifikatsliste angezeigt.
- 7 Stellen Sie sicher, dass das von Ihnen angelegte Zertifikat ausgewählt ist.
- 8 Klicken Sie auf **Aktionen (Actions)** und wählen Sie **Selbstsigniertes Zertifikat (Self Sign Certificate)** aus.
- 9 Geben Sie die Anzahl der Tage ein, die das selbstsignierte Zertifikat gültig ist.
- 10 Klicken Sie auf **OK**.

## Verwenden von Zertifikaten

Nach dem Generieren eines Clientzertifikats können Sie dieses an Ihre Remotebenutzer verteilen, damit diese das Zertifikat in ihrem Webbrowser installieren können.

Der Hauptvorteil der Implementierung von Clientzertifikaten ist, dass über den NSX Edge-Load Balancer das Clientzertifikat beim Client angefordert und überprüft werden kann, bevor die Webanfragen an die Backend-Server weitergeleitet werden. Wenn ein Clientzertifikat aufgehoben wird, da es verloren gegangen oder der Client nicht mehr im Unternehmen aktiv ist, validiert NSX Edge, ob das Clientzertifikat nicht in der Zertifikatssperrliste enthalten ist.

NSX Edge-Clientzertifikate werden im Anwendungsprofil konfiguriert.

Weitere Informationen zum Generieren von Clientzertifikaten finden Sie im Dokument [Szenario: SSL-Client- und -Server-Authentifizierung](#).

## Hinzufügen einer Zertifikatswiderrufsliste

Eine CRL (Certificate Revocation List, Zertifikatswiderrufsliste) ist eine Liste von Abonnenten und deren Status, die von Microsoft zur Verfügung gestellt und signiert wird.

Die Liste enthält 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 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und stellen Sie anschließend sicher, dass Sie sich auf der Registerkarte **Einstellungen (Settings)** befinden.
- 5 Klicken Sie auf **Zertifikate (Certificates)**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+) und wählen Sie **CRL** aus.
- 7 Fügen Sie die Liste in **Zertifikatsinhalte (Certificate contents)** ein.
- 8 (Optional) Geben Sie eine Beschreibung ein.
- 9 Klicken Sie auf **OK**.

## FIPS-Modus

Wenn Sie den FIPS-Modus aktivieren, werden für die sichere Kommunikation an oder vom NSX Edge kryptografische Algorithmen oder Protokolle verwendet, die laut der US-Amerikanischen Federal Information Processing Standards (FIPS) zulässig sind. Durch den FIPS-Modus werden die FIPS-konformen Verschlüsselungs-Suiten aktiviert.

Wenn Sie nicht-FIPS-konforme Komponenten auf einem FIPS-fähigen Edge konfigurieren oder wenn Sie FIPS auf einem Edge aktivieren, der nicht-FIPS-konforme Verschlüsselungen oder Authentifizierungsmechanismen aufweist, schlägt der Vorgang in NSX Manager fehl, und es wird eine gültige Fehlermeldung ausgegeben.

## Funktionsunterschied zwischen FIPS-Modus und Nicht-FIPS-Modus

| Komponente    | Funktionalität                            | FIPS-Modus      | Nicht-FIPS-Modus |
|---------------|-------------------------------------------|-----------------|------------------|
| SSL VPN       | RADIUS-Authentifizierung                  | Nicht verfügbar | Verfügbar        |
| SSL VPN       | RSA-Authentifizierung                     | Nicht verfügbar | Verfügbar        |
| TLS-Protokoll | TLSv1.0                                   | Nicht verfügbar | Verfügbar        |
| Routing       | OSPF, BGP – MD5-Kennwortauthentifizierung | Nicht verfügbar | Verfügbar        |
| IPSec-VPN     | PSK-Authentifizierung                     | Nicht verfügbar | Verfügbar        |
| IPSec-VPN     | DH2- und DH5-Gruppen                      | Nicht verfügbar | Verfügbar        |
| IPSec-VPN     | DH14-, DH15- und DH16-Gruppen             | Verfügbar       | Verfügbar        |
| IPSec-VPN     | AES-GCM-Algorithmus                       | Nicht verfügbar | Verfügbar        |

## Ändern des FIPS-Modus in NSX Edge

Durch die Aktivierung des FIPS-Modus werden die FIPS-konformen Verschlüsselungs-Suiten aktiviert. Demzufolge werden für die sichere Kommunikation zum oder vom NSX Edge kryptografische Algorithmen oder Protokolle verwendet, die laut FIPS zulässig sind.

**Vorsicht** Durch eine Änderung des FIPS-Modus wird die NSX Edge-Appliance neu gestartet. Dies führt zu temporären Unterbrechungen des Datenverkehrs. Dies gilt sowohl bei aktivierter als auch bei nicht aktivierter Hochverfügbarkeit.

Je nach Ihren Anforderungen können Sie FIPS auf einigen oder allen NSX Edge-Appliances aktivieren. FIPS-fähige NSX Edge-Appliances können mit NSX Edge-Appliances kommunizieren, für die FIPS nicht aktiviert ist.

Wenn ein logischer (verteilter) Router ohne NSX Edge-Appliance bereitgestellt wird, können Sie den FIPS-Modus nicht ändern. Der logische Router erhält automatisch denselben FIPS-Modus wie das NSX Controller-Cluster. Wenn das NSX Controller-Cluster der Version NSX 6.3.0 oder höher entspricht, ist FIPS aktiviert.

Zum Ändern des FIPS-Modus auf einem universellen logischen (verteilten) Router in einer Cross-vCenter NSX-Umgebung, in der mehrere NSX Edge-Appliances in den primären und sekundären NSX Managern bereitgestellt sind, müssen Sie den FIPS-Modus auf allen NSX Edge-Appliances ändern, die dem universellen logischen (verteilten) Router zugeordnet sind.

Wenn Sie den FIPS-Modus auf NSX Edge-Appliances mit aktivierter Hochverfügbarkeit ändern, wird FIPS auf beiden Appliances aktiviert, und die Appliances werden nacheinander neu gestartet.

Wenn Sie den FIPS-Modus für ein eigenständiges Edge ändern möchten, verwenden Sie den Befehl `fips enable` oder `fips disable`. Weitere Informationen finden Sie unter *Befehlszeilenschnittstellen-Referenz zu NSX*.

## Voraussetzungen

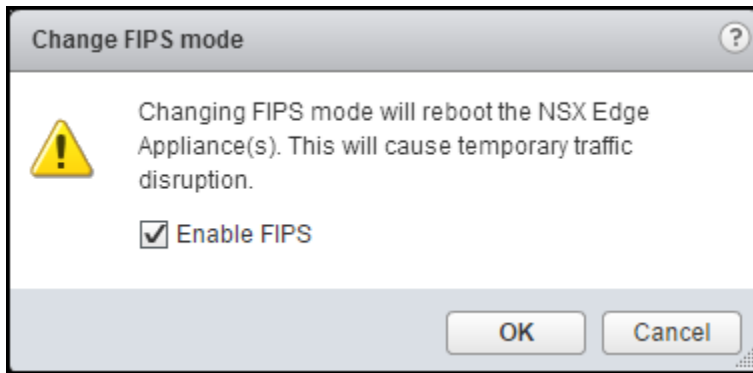
- Stellen Sie sicher, dass Partnerlösungen für den FIPS-Modus zertifiziert sind. Weitere Informationen finden Sie im VMware-Kompatibilitätshandbuch unter <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>.
- Wenn Sie ein Upgrade von einer früheren NSX-Version durchgeführt haben, aktivieren Sie den FIPS-Modus erst nach Abschluss des Upgrades auf NSX 6.3.0. Siehe „Informationen zum Verständnis des FIPS-Modus und NSX-Upgrades“ im *Upgrade-Handbuch für NSX*.
- Stellen Sie sicher, dass NSX Manager der Version NSX 6.3.0 oder höher entspricht.
- Stellen Sie sicher, dass das NSX Controller-Cluster der Version NSX 6.3.0 oder höher entspricht.
- Stellen Sie sicher, dass alle Host-Cluster, auf denen NSX-Arbeitslasten ausgeführt werden, mit NSX 6.3.0 oder höher vorbereitet wurden.
- Stellen Sie sicher, dass alle NSX Edge-Appliances der Version 6.3.0 oder höher entsprechen.
- Stellen Sie sicher, dass die Messaging-Infrastruktur den Status GRÜN hat. Wenden Sie die API-Methode GET `/api/2.0/nwfabric/status?resource={resourceId}` an, wobei „resourceId“ die Host- oder Cluster-Objekt-ID des mit vCenter verwalteten Objekts ist. Suchen Sie im Antworttext nach dem *Status*, der der *featureId* von `com.vmware.vshield.vsm.messagingInfra` entspricht:

```
<nwFabricFeatureStatus>
 <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
 <updateAvailable>>false</updateAvailable>
 <status>GREEN</status>
 <installed>true</installed>
 <enabled>true</enabled>
 <allowConfiguration>>false</allowConfiguration>
</nwFabricFeatureStatus>
```

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Wählen Sie das erforderliche Edge oder den erforderlichen Router aus, klicken Sie auf **Aktionen (Actions)** (⚙️), und wählen Sie **FIPS-Modus ändern (Change FIPS mode)** aus.

Das Dialogfeld **FIPS-Modus ändern (Change FIPS mode)** wird angezeigt.



- 4 Aktivieren oder deaktivieren Sie das Kontrollkästchen **FIPS aktivieren (Enable FIPS)**. Klicken Sie auf **OK**.

Das NSX Edge wird neu gestartet, und der FIPS-Modus ist aktiviert.

#### Nächste Schritte

Optional: [Ändern des FIPS-Modus und der TLS-Einstellungen für NSX Manager](#).

## Verwalten von Appliances

Sie können Appliances hinzufügen, bearbeiten oder löschen. Eine NSX Edge-Instanz bleibt offline, bis ihr wenigstens eine Appliance hinzugefügt wurde.

### Hinzufügen einer Appliance

Sie müssen vor der Bereitstellung mindestens eine Appliance zu NSX Edge hinzufügen.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**.
- 5 Klicken Sie unter **Edge Gateway-Appliances (Edge Gateway Appliances)** auf das Symbol **Hinzufügen (Add) (+)**.
- 6 Wählen Sie den Cluster oder den Ressourcenpool und den Datenspeicher für die Appliance aus.
- 7 (Optional) Wählen Sie den Host aus, auf dem die Appliance hinzugefügt werden soll.
- 8 (Optional) Wählen Sie den vCenter-Ordner aus, in dem die Appliance hinzugefügt werden soll.
- 9 Klicken Sie auf **Hinzufügen (Add)**.

## Bearbeiten einer Appliance

Sie können eine NSX Edge-Appliance bearbeiten.


### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**.
- 5 Wählen Sie unter **Edge Gateway-Appliances (Edge Gateway Appliances)** die zu ändernde Appliance aus.
- 6 Klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- 7 Nehmen Sie im Dialogfeld „Edge-Appliance bearbeiten“ die entsprechenden Änderungen vor.
- 8 Klicken Sie auf **Speichern (Save)**.

## Löschen einer Appliance

Sie können eine NSX Edge-Appliance löschen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**.
- 5 Wählen Sie unter **Edge Gateway-Appliances (Edge Gateway Appliances)** die zu löschende Appliance aus.
- 6 Klicken Sie auf das Symbol **Löschen (Delete)** ().

## Verwalten von Ressourcenreservierungen für die NSX Edge-Appliance

NSX for vSphere verwendet die vSphere-Ressourcenzuteilung, um Ressourcen für NSX Edge-Appliances zu reservieren. Durch das Reservieren von CPU- und Arbeitsspeicherressourcen für NSX Edge wird sichergestellt, dass die Appliance über genügend Ressourcen verfügt, um ordnungsgemäß zu funktionieren.

Sie können die Ressourcenreservierung einer NSX Edge-Appliance über die API festlegen. Sie können die Reservierung konfigurieren, wenn Sie eine NSX Edge mit `POST /api/4.0/edges` erstellen. Sie können die Reservierung auch für eine vorhandene NSX Edge mit `PUT /api/4.0/edges/{edgeId}/appliances` aktualisieren. Die Ressourcenreservierung legen Sie mit `cpuReservation > reservation` und `memoryReservation > reservation` fest. Weitere Informationen finden Sie unter *Handbuch zu NSX-API*.

Ab NSX 6.3.3 können Sie auch die Ressourcenreservierung einer NSX Edge-Appliance mit dem vSphere Web Client festlegen. Beim Erstellen eines NSX Edge werden Sie aufgefordert, eine Reservierungsmethode anzugeben. Sie können auch die Reservierung eines vorhandenen NSX Edge ändern, indem Sie die Appliance bearbeiten. Navigieren Sie zu **Networking & Security > NSX Edges > NSX Edge-Instanz > Verwalten > Einstellungen > Konfiguration** und bearbeiten Sie die Appliance.

Es gibt drei Methoden der Ressourcenreservierung: **Verwaltetes System**, **Benutzerdefiniert** oder **Keine Reservierung**

---

**Wichtig** Wenn Sie **Benutzerdefiniert** oder **Keine Reservierung** als Reservierungsmethode für eine NSX Edge-Appliance auswählen, können Sie nicht zurück zu **Verwaltetes System** wechseln.

---

## Auswahl von „Verwaltetes System“ für die Ressourcenreservierung

Wenn Sie **Verwaltetes System** auswählen, reserviert das System CPU- und Arbeitsspeicherressourcen für die neue NSX Edge-Appliance. Die reservierten Ressourcen entsprechen den Systemvoraussetzungen für die Appliance-Größe. Diese werden anhand der Prozentsätze angepasst, die von der Tuning-Konfigurations-API festgelegt werden.

Wenn Sie eine NSX Edge-Appliance mithilfe der API erstellen und die CPU- oder Arbeitsspeicherreservierungen in der Anforderung explizit festlegen, entspricht dies der Auswahl von **Verwaltetes System** für die Ressourcenreservierung im vSphere Web Client.

Wenn eine NSX Edge-Appliance mit Auswahl von **Verwaltetes System** für die Ressourcenreservierung bereitgestellt wird (während der Installation, der Aktualisierung oder der erneuten Bereitstellung), wird die Reservierung nach dem Einschalten der Appliance auf den Ressourcenpool angewendet. Wenn die verfügbaren Ressourcen nicht ausreichen, schlägt die Reservierung fehl und es wird ein Systemereignis generiert. Die Appliance wird dennoch erfolgreich bereitgestellt. Es wird ein erneuter Versuch für die Reservierung unternommen, wenn die Appliance das nächste Mal bereitgestellt wird (während der Aktualisierung oder der Bereitstellung).

Bei Auswahl von **Verwaltetes System** für die Ressourcenreservierung aktualisiert das System die Ressourcenreservierungen, wenn Sie die Appliance-Größe anpassen, damit die Systemanforderungen der neuen Appliance-Größe entsprechen.

## Auswahl von „Benutzerdefiniert“ für die Ressourcenreservierung

Wenn Sie **Benutzerdefiniert** auswählen, bestimmen Sie die Ressourcenreservierungen für die NSX Edge-Appliance.

Wenn Sie eine NSX Edge-Appliance mithilfe der API erstellen und die CPU- oder Arbeitsspeicherreservierungen in der Anforderung explizit festlegen, entspricht dies der Auswahl von **Benutzerdefiniert** für die Ressourcenreservierung im vSphere Web Client.

Wenn eine NSX Edge-Appliance mit Auswahl von **Benutzerdefiniert** für die Ressourcenreservierung bereitgestellt wird (während der Installation, der Aktualisierung oder der erneuten Bereitstellung), wird die Reservierung vor dem Einschalten der Appliance auf den Ressourcenpool angewendet. Wenn die verfügbaren Ressourcen nicht ausreichen, kann die Appliance nicht eingeschaltet werden und die Bereitstellung der Appliance schlägt fehl.

Sie können Reservierungen mit der Auswahl **Benutzerdefiniert** anwenden, nachdem eine NSX Edge-Appliance bereitgestellt wurde. Die Konfigurationsänderung schlägt fehl, wenn die verfügbaren Ressourcen im Ressourcenpool nicht ausreichen.

Bei der Auswahl von **Benutzerdefiniert** für Ressourcenreservierungen fügt das System keine Ressourcenreservierungen für die Appliance hinzu und passt keine solchen Reservierungen an. Wenn Sie die Appliance-Größe ändern, werden die Systemvoraussetzungen für die Appliance angepasst, die Ressourcenreservierungen werden vom System aber nicht aktualisiert. Sie sollten die Ressourcenreservierung ändern, sodass sie den Systemvoraussetzungen der neuen Appliance-Größe entspricht.

Sie können eine benutzerdefinierte Ressourcenreservierung über den vSphere Web Client oder die API ändern.

## Auswahl von „Keine Reservierung“ für die Ressourcenreservierung

Wenn Sie **Keine Reservierung** auswählen, werden keine Ressourcen für die NSX Edge-Appliance reserviert. Deswegen können Sie trotzdem NSX Edge-Appliances auf Hosts bereitstellen, die nicht über ausreichende Ressourcen verfügen, aber die Appliances funktionieren möglicherweise nicht ordnungsgemäß, wenn es zu Ressourcenkonflikten kommt.

Wenn Sie eine NSX Edge-Appliance mithilfe der API erstellen und die CPU- und Arbeitsspeicherreservierungen explizit auf 0 festlegen, entspricht dies der Einstellung der Ressourcenreservierung auf **Keine Reservierung** im vSphere Web Client.

## Ändern der Ressourcenreservierung bei Auswahl von „Verwaltetes System“ mithilfe der Tuning-Konfiguration

Wenn Sie nicht über ausreichend Ressourcen verfügen, können Sie die Ressourcenreservierungen mit Auswahl von **Verwaltetes System** vorübergehend deaktivieren oder den Standardwert verringern. Sie können die Reservierung ändern, indem Sie Werte für die Parameter `edgeVCpuReservationPercentage` und `edgeMemoryReservationPercentage` in der Tuning-Konfigurations-API `PUT /api/4.0/edgePublish/tuningConfiguration` konfigurieren. Diese Änderung wirkt sich auf neue NSX Edge-Appliance-Bereitstellungen aus, aber nicht auf vorhandene-Appliances. Die Prozentsätze ändern die standardmäßige CPU und den Arbeitsspeicher, der für die entsprechende Größe der NSX Edge-Appliance reserviert wird. Um die Ressourcenreservierung zu deaktivieren, legen Sie die Werte auf 0 fest. Weitere Informationen finden Sie unter *Handbuch zu NSX-API*.

## Systemvoraussetzungen für NSX Edge-Appliance

Die Systemanforderungen für NSX Edge-Appliances hängen von der Appliance-Größe ab: „Kompakt“, „Groß“, „Quad Large“ oder „Sehr groß“. Diese Werte werden für die Ressourcenreservierung mit Auswahl von **Verwaltetes System** verwendet.

**Tabelle 9-2. Systemvoraussetzungen für NSX Edge**

Appliance-Größe	CPU-Reservierung	Arbeitsspeicherreservierung
Kompakt	1000 MHz	512 MB
Groß	2000 MHz	1 GB
Quad Large	4000 MHz	2 GB
Sehr groß	6000 MHz	8 GB

## Arbeiten mit Schnittstellen

Ein NSX Edge Services Gateway kann bis zu zehn interne, Uplink- oder Trunk-Schnittstellen haben. Ein NSX Edge-Router kann acht Uplink-Schnittstellen und bis zu 1.000 interne Schnittstellen haben.

Eine NSX Edge-Instanz muss über mindestens eine interne Schnittstelle verfügen, bevor sie bereitgestellt werden kann.

### Konfigurieren einer Schnittstelle

Interne Schnittstellen sind normalerweise für Ost-West-Datenverkehr bestimmt, während Uplink-Schnittstellen für Nord-Süd-Datenverkehr verwendet werden. Wenn ein logischer Router (DLR) an ein Edge Services Gateway (ESG) angeschlossen ist, handelt es sich bei der Schnittstelle auf dem Router um eine Uplink-Schnittstelle, während die Schnittstelle auf dem ESG eine interne Schnittstelle ist. Eine NSX Trunk-Schnittstelle ist für interne Netzwerke und keine externen Netzwerke bestimmt. Die Trunk-Schnittstelle ermöglicht das Trunking mehrerer interner Netzwerke (entweder VLAN oder VXLAN).

Ein NSX Edge Services Gateway (ESG) kann bis zu zehn interne, Uplink- oder Trunk-Schnittstellen haben. Diese Beschränkungen werden vom NSX Manager durchgesetzt.

Eine NSX-Bereitstellung kann über bis zu 1.000 verteilte logische Router-Instanzen (Distributed Logical Router, DLR) auf einem einzigen ESXi-Host verfügen. Auf einem einzigen logischen Router können bis zu acht Uplink-Schnittstellen und bis zu 991 interne Schnittstellen konfiguriert werden. Diese Beschränkungen werden vom NSX Manager durchgesetzt. Weitere Informationen finden zur Schnittstellenskalierung in einer NSX-Bereitstellung finden Sie im *Handbuch zum Netzwerkvirtualisierungsdesign für VMware® NSX for vSphere* unter <https://communities.vmware.com/docs/DOC-27683>.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Schnittstellen (Interfaces)**.
- 5 Wählen Sie eine Schnittstelle aus und klicken Sie auf das Symbol **Bearbeiten (Edit)** (✎).

- 6 Geben Sie im Dialogfeld „Edge-Schnittstelle bearbeiten“ einen Namen für die Schnittstelle ein.
- 7 Wählen Sie **Intern (Internal)** bzw. **Uplink**, um anzugeben, ob es sich um eine interne oder eine externe Schnittstelle handelt.  
  
Wählen Sie **Trunk**, um eine Teilschnittstelle zu erstellen. Weitere Informationen finden Sie unter [Hinzufügen einer Teilschnittstelle](#).
- 8 Wählen Sie die Portgruppe oder den logischen Switch aus, mit dem diese Schnittstelle verbunden werden soll.
  - a Klicken Sie auf **Auswählen (Select)** neben dem Feld **Verbunden mit (Connected To)**.
  - b Klicken Sie je nachdem, womit die Schnittstelle verbunden werden soll, auf die Registerkarte **logischen Switch (Logical Switch)**, **Standardportgruppe (Standard Portgroup)** oder **Verteilte Portgruppe (Distributed Portgroup)**.
  - c Wählen Sie den entsprechenden logischen Switch oder die Portgruppe aus.
  - d Klicken Sie auf **Auswählen (Select)**.
- 9 Wählen Sie den Konnektivitätsstatus für die Schnittstelle aus.
- 10 Klicken Sie unter **Subnetze konfigurieren (Configure Subnets)** auf das Symbol **Hinzufügen (Add)** (+), um der Schnittstelle ein Subnetz hinzuzufügen.

Eine Schnittstelle kann über mehrere nicht überlappende Subnetze verfügen.

- 11 Klicken Sie unter **Subnetz hinzufügen (Add Subnet)** auf das Symbol **Hinzufügen (Add)** (+), um eine IP-Adresse hinzuzufügen.

Wenn Sie mehr als eine IP-Adresse eingeben, können Sie die primäre IP-Adresse auswählen. Eine Schnittstelle kann eine primäre und mehrere sekundäre IP-Adressen aufweisen. NSX Edge betrachtet die primäre IP-Adresse als die Quelladresse für lokal generierten Datenverkehr.

Sie müssen der Schnittstelle zuerst eine IP-Adresse hinzufügen, bevor Sie sie für jede beliebige Funktionskonfiguration verwenden können.

- 12 Geben Sie die Subnetzmaske für die Schnittstelle ein und klicken Sie auf **Speichern (Save)**.
- 13 Ändern Sie die standardmäßige MTU, falls erforderlich.
- 14 Wählen Sie unter **Optionen (Options)** die erforderlichen Optionen aus.

Option	Beschreibung
<b>Proxy-ARP aktivieren</b>	Unterstützt das Überlappen der Netzwerkweiterleitung zwischen verschiedenen Schnittstellen.
<b>ICMP-Umleitung senden</b>	Leitet Routing-Informationen an Hosts weiter.
<b>Umgekehrter Pfadfilter</b>	Überprüft die Erreichbarkeit der Quelladresse in weitergeleiteten Paketen. Im aktivierten Modus muss das Paket auf der Schnittstelle empfangen werden, die der Router zum Weiterleiten des Rückgabepakets verwenden würde. Im Loose-Modus muss die Quelladresse in der Routing-Tabelle angezeigt werden.

- 15 Geben Sie die Fence-Parameter ein und klicken Sie auf **Hinzufügen (Add)**.

**16** Klicken Sie auf **OK**.

## Löschen einer Schnittstelle

Sie können eine NSX Edge-Schnittstelle löschen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Schnittstellen (Interfaces)**.
- 5 Wählen Sie die zu löschende Schnittstelle.
- 6 Klicken Sie auf das Symbol **Löschen (Delete)** (✖).

## Aktivieren einer Schnittstelle

Eine Schnittstelle muss aktiviert sein, damit NSX Edge die virtuellen Maschinen innerhalb dieser Schnittstelle (Portgruppe oder logischer Switch) isolieren kann.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Schnittstellen (Interfaces)**.
- 5 Wählen Sie die zu aktivierende Schnittstelle aus.
- 6 Klicken Sie auf das Symbol **Aktivieren (Enable)** (✔).

## Deaktivieren einer Schnittstelle

Sie können eine Schnittstelle auf einem NSX Edge deaktivieren.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.

- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Schnittstellen (Interfaces)**.
- 5 Wählen Sie die zu deaktivierende Schnittstelle aus.
- 6 Klicken Sie auf das Symbol **Deaktivieren (Disable)**.

## Ändern der Traffic-Shaping-Richtlinie

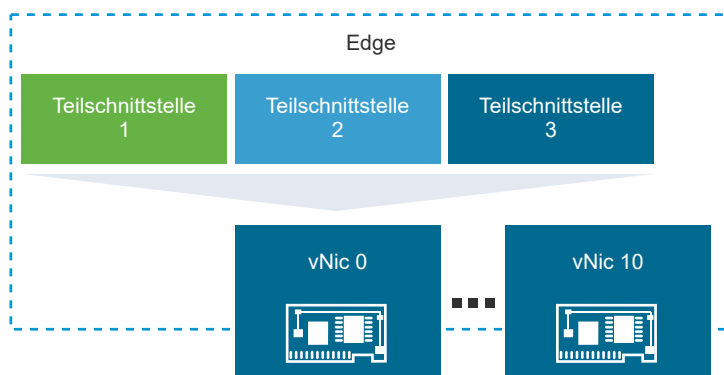
Sie können die Traffic-Shaping-Richtlinie für eine NSX Edge-Schnittstelle auf dem vSphere Distributed Switch ändern.

### Verfahren

- 1 Doppelklicken Sie auf eine NSX Edge-Instanz und navigieren Sie zu **Verwalten (Manage)** > **Einstellungen (Settings)** > **Schnittstellen (Interfaces)**.
- 2 Wählen Sie eine Schnittstelle aus.
- 3 Klicken Sie auf **Aktionen (Actions)** > **Traffic-Shaping-Richtlinie konfigurieren (Configure Traffic Shaping Policy)**.
- 4 Nehmen Sie die entsprechenden Änderungen vor.  
Weitere Informationen zu den Optionen finden Sie unter [Traffic-Shaping-Richtlinie](#).
- 5 Klicken Sie auf **OK**.

## Hinzufügen einer Teilschnittstelle

Sie können eine Teilschnittstelle auf einer Trunk vNIC hinzufügen, welche anschließend von den NSX Edge-Diensten verwendet werden kann.



Trunk-Schnittstellen können zu einem der folgenden Typen zählen:

- VLAN-Trunk ist Standard und funktioniert mit jeder Version von ESXi. Dies wird verwendet, um gekennzeichneten VLAN-Datenverkehr in die Edge-Instanz zu holen.
- VXLAN-Trunk funktioniert mit NSX-Version 6.1 und höher. Dies wird verwendet, um VXLAN-Datenverkehr in die Edge-Instanz zu holen.

Eine Teilschnittstelle kann von den folgenden Edge-Diensten verwendet werden:

- DHCP
- Routing (BGP und OSPF)
- Load Balancer
- IPSec-VPN: IPSec-VPN kann nur als Uplink-Schnittstelle konfiguriert werden. Die Teilschnittstelle kann für den privaten Datenverkehr verwendet werden, der den IPSec-Tunnel durchläuft. Wenn die IPSec-Richtlinie für den privaten-Datenverkehr konfiguriert ist, agiert die Teilschnittstelle als Gateway für das private lokale Subnetz.
- L2 VPN
- NAT

. Eine Teilschnittstelle kann nicht für HA oder Logical Firewall verwendet werden. Sie können jedoch die IP-Adresse der Teilschnittstelle in einer Firewallregel verwenden.

### Verfahren

- 1 Klicken Sie für eine NSX Edge-Instanz auf der Registerkarte **Verwalten (Manage) > Einstellungen (Settings)** auf **Schnittstellen (Interfaces)**.
- 2 Wählen Sie eine Schnittstelle aus und klicken Sie auf das Symbol **Bearbeiten (Edit)** (✎).
- 3 Geben Sie im Dialogfeld „Edge-Schnittstelle bearbeiten“ einen Namen für die Schnittstelle ein.
- 4 Wählen Sie unter „Typ“ die Option **Trunk** aus.
- 5 Wählen Sie die Standardportgruppe oder die verteilte Portgruppe aus, mit der diese Schnittstelle verbunden werden soll.
  - a Klicken Sie neben dem Feld **Verbunden mit (Connected To)** auf **Ändern (Change)**.
  - b Klicken Sie je nachdem, womit die Schnittstelle verbunden werden soll, auf die Registerkarte **Standardportgruppe (Standard Portgroup)** bzw. **Verteilte Portgruppe (Distributed Portgroup)**.
  - c Wählen Sie die entsprechende Portgruppe aus und klicken Sie auf **OK**.
  - d Klicken Sie auf **Auswählen (Select)**.
- 6 Klicken Sie unter „Teilschnittstellen“ auf das Symbol **Hinzufügen (Add)**.
- 7 Klicken Sie auf **Teilschnittstelle aktivieren (Enable Sub interface)** und geben Sie einen Namen für die Teilschnittstelle ein.
- 8 Geben Sie unter **Tunnel-ID (Tunnel Id)** eine Zahl zwischen 1 und 4094 ein.

Die Tunnel-ID wird dazu verwendet, die auszuweitenden Netzwerke zu verbinden. Dieser Wert muss auf dem Client und den Server-Sites übereinstimmen.

- 9 Wählen Sie unter „Backing-Typ“ einen der folgenden Typen aus, um das Netzwerk-Backing für die Teilschnittstelle anzugeben.

- **VLAN** für ein VLAN-Netzwerk

Geben Sie die VLAN-ID des virtuellen LAN ein, das Ihre Teilschnittstelle verwenden soll. VLAN-IDs können zwischen 0 und 4094 liegen.

- **Netzwerk (Network)** für ein VLAN- oder VXLAN-Netzwerk

Klicken Sie auf **Auswählen (Select)** und wählen Sie die verteilte Portgruppe oder den logischen Switch aus. NSX Manager extrahiert die VLAN-ID und verwendet sie in der Trunk-Konfiguration.

- **Keine (None)**, um eine Teilschnittstelle zu erstellen, ohne eine Netzwerk- oder VLAN-ID anzugeben. Diese Teilschnittstelle ist für NSX Edge intern und wird verwendet, um Pakete zwischen einem ausgeweiteten Netzwerk und einem nicht ausgeweiteten (nicht gekennzeichneten) Netzwerk zu routen.

- 10 Um Subnetze zur Teilschnittstelle hinzuzufügen, klicken Sie in der Area „Subnetze konfigurieren“ auf das Symbol **Hinzufügen (Add)**.

- 11 Klicken Sie unter „Subnetze hinzufügen“ auf das Symbol **Hinzufügen (Add)**, um eine IP-Adresse hinzuzufügen. Geben Sie die IP-Adresse ein und klicken Sie auf **OK**.

Wenn Sie mehr als eine IP-Adresse eingeben, können Sie die primäre IP-Adresse auswählen. Eine Schnittstelle kann eine primäre und mehrere sekundäre IP-Adressen aufweisen. NSX Edge betrachtet die primäre IP-Adresse als Quelladresse für lokal generierten Datenverkehr.

- 12 Geben Sie die Länge des Subnetzpräfixes ein und klicken Sie auf **OK**.

- 13 Bearbeiten Sie den standardmäßigen **MTU**-Wert für die Teilschnittstelle, falls erforderlich.

Der Standardwert für MTU für eine Trunk-Schnittstelle beträgt 1600 und der Standardwert für MTU für eine Teilschnittstelle beträgt 1500. Der Wert für MTU für die Teilschnittstelle sollte kleiner oder gleich dem niedrigsten Wert für MTU entlang aller Trunk-Schnittstellen für die NSX Edge-Instanz sein.

- 14 Wählen Sie **Umleitung aktivieren (Enable Send Redirect)** aus, um Routing-Informationen an Hosts weiterzuleiten.

- 15 **Aktivieren (Enable)** oder **deaktivieren (Disable)** Sie den umgekehrten Pfadfilter.

Ein umgekehrter Pfadfilter überprüft die Erreichbarkeit der Quelladresse in weitergeleiteten Paketen. Im aktivierten Modus muss das Paket auf der Schnittstelle empfangen werden, die der Router zum Weiterleiten des Rückgabepakets verwenden würde. Im Loose-Modus muss die Quelladresse in der Routing-Tabelle angezeigt werden.

- 16 Klicken Sie auf **OK**, um zum Fenster „Trunk-Schnittstelle“ zurückzukehren.

- 17 Geben Sie die MAC-Adresse für die Schnittstelle ein, falls erforderlich. Geben Sie zwei MAC-Adressen ein, wenn eine ESG-Hochverfügbarkeit verwendet wird.

Wenn sie nicht erforderlich sind, werden sie automatisch generiert.

- 18** Bearbeiten Sie den standardmäßigen MTU-Wert der Trunk-Schnittstelle, falls erforderlich.

Der MTU-Standardwert beträgt für eine Trunk-Schnittstelle 1600 und für eine Teilschnittstelle 1500. Der MTU-Wert für die Trunk-Schnittstelle muss gleich oder größer als der MTU-Wert der Teilschnittstelle sein.

- 19** Klicken Sie auf **OK**.

### Ergebnisse

Sie können die Teilschnittstelle nun auf Edge-Diensten verwenden.

### Nächste Schritte

Konfigurieren Sie den VLAN-Trunk, wenn die Teilschnittstelle, die einer Trunk-vNIC hinzugefügt wurde, durch eine Standardportgruppe unterstützt wird. Weitere Informationen dazu finden Sie unter [Konfigurieren von VLAN-Trunks](#).

## Konfigurieren von VLAN-Trunks

Wenn Sie Teilschnittstellen auf der Trunk-vNIC eines Edge hinzufügen, der mit einer verteilten Portgruppe verbunden ist, werden sowohl der VLAN- als auch der VXLAN-Trunk unterstützt. Wenn Sie Teilschnittstellen auf der Trunk-vNIC eines Edge hinzufügen, der mit einer Standard-Portgruppe verbunden ist, wird nur der VLAN-Trunk unterstützt.

### Voraussetzungen

Stellen Sie sicher, dass eine Teilschnittstelle mit einer von einer Standardportgruppe unterstützten Trunk-vNIC verfügbar ist. Weitere Informationen dazu finden Sie unter [Hinzufügen einer Teilschnittstelle](#).

### Verfahren

- 1** Melden Sie sich beim vCenter Web Client an.
- 2** Klicken Sie auf **Netzwerk (Networking)**.
- 3** Wählen Sie eine Standardportgruppe aus und klicken Sie auf **Einstellungen bearbeiten (Edit Settings)**.
- 4** Klicken Sie auf die Registerkarte **VLAN**.
- 5** Wählen Sie unter „VLAN-Typ“ die Option „VLAN-Trunking“ aus und geben Sie die VLAN-IDs für das Trunking ein.
- 6** Klicken Sie auf **OK**.

## Ändern der Konfiguration für die automatische Regel

Wenn die automatische Regelerstellung aktiviert ist, fügt NSX Edge Firewall-, NAT- und Routing-Routen hinzu, um den Fluss des Steuerungsdatenverkehrs für diese Dienste zu aktivieren. Wenn die automatische Regelerstellung nicht aktiviert ist, müssen Sie die Firewall-, NAT- und Routing-Konfiguration manuell hinzufügen, um den Steuerungsdatenverkehr für NSX Edge-Dienste wie beispielsweise Load Balancing, VPN, usw. zu ermöglichen.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**. Klicken Sie auf **Konfiguration (Configuration)**.
- 5 Klicken Sie im Detailbereich auf **Aktion (Action)** (⚙️), und wählen Sie **Ändern der Konfiguration für die automatische Regel (Change Auto Rule configuration)**.
- 6 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.

## Ändern der CLI-Anmeldedaten

Sie können die Anmeldedaten ändern, die zum Anmelden bei der Befehlszeilenschnittstelle (CLI) verwendet werden sollen.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**. Klicken Sie auf **Konfiguration (Configuration)**.
- 5 Klicken Sie im Detailbereich auf **Aktion (Action)** (⚙️), und wählen Sie **Ändern der CLI-Anmeldedaten (Change CLI Credentials)**.
- 6 Geben Sie ein neues Kennwort ein, bestätigen Sie es, und klicken Sie auf **OK**.

## Grundlegendes zu High Availability

Die „High Availability“ (HA, Hochverfügbarkeit) stellt sicher, dass die von NSX Edge-Appliances bereitgestellten Dienste auch dann verfügbar sind, wenn eine einzelne Appliance durch einen Hardware- oder Softwarefehler nicht mehr verfügbar ist. Mithilfe der NSX Edge-HA wird die Failover-Ausfallzeit nur minimiert, d. h., sie beträgt nicht null, da wegen des Failover zwischen Appliances eventuell einige Dienste neu gestartet werden müssen.

Beispielsweise synchronisiert die NSX Edge-HA die Verbindungsermittlung der statusorientierten Firewall oder die statusorientierten Informationen des Load Balancer. Für die erneute Aktivierung der gesamten Dienste ist ein bestimmter Zeitaufwand erforderlich. Beispielsweise kann ein Neustart der Dienste zu einer gewissen Ausfallzeit beim dynamischen Routing führen, wenn ein NSX Edge als Router dient.

Manchmal können die beiden NSX Edge-HA-Appliances nicht miteinander kommunizieren und nicht einseitig aktiviert werden. Mit diesem Verhalten soll die Verfügbarkeit der aktiven NSX Edge-Dienste sichergestellt werden, wenn das Standby-NSX Edge nicht verfügbar ist. Ist nach der erneuten Einrichtung der Kommunikation die andere Appliance weiterhin vorhanden, handeln die beiden NSX Edge-HA-Appliances den aktiven und den Standby-Status neu aus. Wird diese Aushandlung nicht abgeschlossen und werden beide Appliances als aktiv erklärt, nachdem die Konnektivität erneut eingerichtet wurde, kommt es zu einem unvorhergesehenen Verhalten. Dieses Szenario, auch als „Split Brain“ bezeichnet, kann bei folgenden Umgebungsbedingungen auftreten:

- Probleme der Konnektivität des physischen Netzwerks, inklusive einer Netzwerkpartition.
- CPU- oder Arbeitsspeicherkonflikt beim NSX Edge.
- Vorübergehende Speicherprobleme, die zum Ausfall von mindestens einer NSX Edge-HA-VM führen können.

Beispielsweise kann es zu einer Verbesserung der NSX Edge-HA-Stabilität und -Leistung kommen, wenn die VMs aus einem überbeanspruchten Speicher entfernt werden. Insbesondere können bei umfangreichen Sicherungen über Nacht große Spitzen der Speicherlatenz die NSX Edge-HA-Stabilität beeinflussen.

- Überlastung des physischen oder virtuellen Netzwerkadapters im Zusammenhang mit dem Austausch von Paketen.

Über Umgebungsprobleme hinaus kommt es zu einem „Split Brain“, wenn sich die HA-Konfigurations-Engine in einem fehlerhaften Zustand befindet oder wenn der HA-Daemon fehlschlägt.

## Statusbehaftete High Availability

Die primäre NSX Edge-Appliance befindet sich im aktiven und die sekundäre Appliance im Standby-Zustand. NSX Manager repliziert die Konfiguration der primären Appliance für die Standby-Appliance. Sie können auch manuell zwei Appliances hinzufügen. Erstellen Sie die primären und sekundären Appliances in getrennten Ressourcenpools und Datenspeichern. Wenn Sie die primäre und sekundäre Appliance im selben Datenspeicher erstellen, muss der Datenspeicher von allen Hosts im Cluster gemeinsam genutzt werden, damit das HA-Appliance-Paar auf verschiedenen ESXi-Hosts bereitgestellt wird. Wenn der Datenspeicher ein lokaler Speicher ist, werden beide virtuelle Maschinen auf demselben Host bereitgestellt.

Alle NSX Edge-Dienste werden auf der aktiven Appliance ausgeführt. Die primäre Appliance hält ein Taktsignal mit der Standby-Appliance aufrecht und sendet Dienst-Updates über eine interne Schnittstelle.

Wenn die Standby-Appliance im festgelegten Zeitintervall (der Standardwert ist 15 Sekunden) kein Taktsignal von der primären Appliance empfängt, gilt die primäre Appliance als ausgefallen. Die Standby-Appliance wechselt in den aktiven Zustand, übernimmt die Schnittstellenkonfiguration der primären Appliance und startet die NSX Edge-Dienste, die auf der primären Appliance ausgeführt wurden. Bei der Durchführung des Wechsels wird auf der Registerkarte **Systemereignisse (System Events)** ein Systemereignis unter „Einstellungen und Berichte“ angezeigt. Der Load Balancer und der VPN-Dienst

müssen die TCP-Verbindung mit NSX Edge wiederherstellen, wodurch der Dienst kurz unterbrochen wird. Dennoch werden Verbindungen logischer Switches und Firewall Sitzungen zwischen primären und Standby-Appliances synchronisiert. Der Dienst wird während des Wechsels unterbrochen, wenn darauf gewartet wird, dass die Standby-Appliance aktiv wird und übernimmt.

Wenn die NSX Edge-Appliance ausfällt und ein fehlerhafter Zustand gemeldet wird, erzwingt HA die Synchronisierung der ausgefallenen Appliance, um sie wiederherzustellen. Nach der Wiederherstellung der Appliance übernimmt diese die Konfiguration der derzeit aktiven Appliance und bleibt im Standby-Modus. Wenn die NSX Edge-Appliance ausgefallen ist, müssen Sie sie löschen und eine neue Appliance hinzufügen.

NSX Edge stellt sicher, dass sich die zwei virtuellen HA NSX Edge-Maschinen auch dann nicht auf demselben ESXi-Host befinden, wenn Sie DRS und vMotion verwendet haben (es sei denn, Sie migrieren sie per vMotion manuell auf denselben Host). Zwei virtuelle Maschinen werden auf vCenter in demselben Ressourcenpool und Datenspeicher wie die von Ihnen konfigurierte Appliance bereitgestellt. Die IP-Adressen von lokalen Links werden virtuellen HA-Maschinen in der NSX Edge-HA zugewiesen, damit sie kommunizieren können. Sie können Verwaltungs-IP-Adressen angeben, um die lokalen Links zu überschreiben.

Wenn Syslog-Server konfiguriert sind, werden die Protokolle auf der aktiven Appliance an die Syslog-Server gesendet.

## **Hochverfügbarkeit (High Availability, HA) in einer Cross-vCenter NSX-Umgebung**

Wenn Sie die Hochverfügbarkeit (High Availability, HA) auf einem NSX Edge in einer Cross-vCenter NSX-Umgebung aktivieren, müssen sich die aktive und die Standby-NSX Edge-Appliance im selben vCenter Server befinden. Wenn Sie ein Mitglied eines NSX Edge-HA-Paares auf ein anderes vCenter Server-System migrieren, können die beiden HA-Appliances nicht mehr als HA-Paar ausgeführt werden. Dies kann zu einer Unterbrechung des Datenverkehrs führen.

### **vSphere High Availability**

NSX Edge HA ist zu vSphere HA kompatibel. Wenn der Host, auf dem die NSX Edge-Instanz ausgeführt wird, ausfällt, wird NSX Edge auf dem Standby-Host neu gestartet. Hierdurch wird sichergestellt, dass das NSX Edge-HA-Paar ein weiteres Failover verarbeiten kann.

Wenn vSphere HA nicht aktiviert ist, übersteht das NSX Edge-HA-Aktiv-Standby-Paar ein Failover. Falls jedoch ein weiteres Failover auftritt, bevor das zweite HA-Paar wiederhergestellt wurde, kann dies die Verfügbarkeit von NSX Edge beeinträchtigen.

Weitere Informationen zu vSphere HA finden Sie unter *vSphere-Verfügbarkeit*.

## Ändern der High Availability-Konfiguration

Sie können die HA-Konfiguration ändern, die Sie bei der Installation von NSX Edge festgelegt haben.

---

**Hinweis** In NSX 6.2.3 und höher scheitert die Aktivierung der Hochverfügbarkeit (High Availability, HA) auf einem vorhandenen Edge, wenn nicht ausreichend Ressourcen für eine zweite Edge-VM-Appliance reserviert werden können. Die Konfiguration wird auf die letzte bekannte brauchbare Konfiguration zurückgesetzt.

---

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**.
- 5 Klicken Sie im Bereich **HA-Konfiguration (HA Configuration)** auf **Ändern (Change)**.
- 6 Führen Sie im Dialogfeld „HA-Konfiguration ändern“ die Änderungen durch, wie im Abschnitt „Hinzufügen eines Edge Services Gateway“ des Installationshandbuch für NSX erläutert.

---

**Hinweis** Wenn L2 VPN auf dieser Edge-Appliance vor der Aktivierung von HA konfiguriert wird, müssen mindestens zwei interne Schnittstellen eingerichtet sein. Falls auf dieser bereits von L2 VPN verwendeten Edge-Instanz eine einzelne Schnittstelle konfiguriert wurde, wird HA auf der Edge-Appliance deaktiviert.

---

- 7 Klicken Sie auf **OK**.

## Erzwingen der Synchronisierung von NSX Edge mit NSX Manager

Sie können eine Synchronisierungsanforderung von NSX Manager an NSX Edge senden.

Das Erzwingen der Synchronisierung wird verwendet, wenn Sie die dem NSX Manager bekannte Edge-Konfiguration auf alle Komponenten synchronisieren müssen.

---

**Hinweis** Für Version 6.2 und höher wird ein Datenverlust beim Ost-West-Datenverkehr durch das Erzwingen der Synchronisierung verhindert, der Nord-Süd-Datenverkehr und das Bridging kann jedoch unterbrochen werden.

---

Das Erzwingen der Synchronisierung führt zu den folgenden Aktionen:

- Edge-Appliances werden neu gestartet und die neueste Konfiguration wird angewendet.
- Die Verbindung zum Host wird geschlossen.


- Wenn es sich um einen primären oder eigenständigen NSX Manager handelt, und das Edge ein logischer verteilter Router (Logical Distributed Router, DLR) ist, wird das Controller-Cluster synchronisiert.
- Eine Meldung wird an alle relevanten Hosts zur Synchronisierung der verteilten Router-Instanz gesendet.

---

**Wichtig** In einer Cross-vCenter NSX-Umgebung ist es erforderlich, dass die Synchronisierung der NSX Edge-Instanz zuerst auf dem primären NSX Manager erzwungen wird. Danach erzwingen Sie die Synchronisierung der NSX Edge-Instanz auf den sekundären NSX Managern.

---

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Wählen Sie eine NSX Edge-Instanz aus.
- 4 Klicken Sie auf **Aktionen (Actions)** ( ) , und wählen Sie **Erzwingen der Synchronisierung (Force Sync)**.

## Konfigurieren von Syslog-Servern für NSX Edge

Sie können einen oder zwei Remote-Syslog-Server konfigurieren. NSX Edge-Ereignisse und -Protokolle im Zusammenhang mit Firewallereignissen, die von NSX Edge-Appliances ausgehen, werden an die Syslog-Server gesendet.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf die Registerkarte **Einstellungen**.
- 5 Klicken Sie im Fenster **Details** neben den Syslog-Servern auf **Ändern**.
- 6 Geben Sie die IP-Adressen beider Remote-Syslog-Server ein und wählen Sie das Protokoll aus.
- 7 Klicken Sie auf **OK**, um die Konfiguration zu speichern.

## Anzeigen des Status eines NSX Edge

Die Statusseite enthält Diagramme für den Datenverkehr, der über die Schnittstellen der ausgewählten NSX Edge-Instanz fließt, sowie Verbindungsstatistiken für die Firewall- und Load-Balancer-Dienste.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.

- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Überwachen (Monitor)**.
- 5 Wählen Sie den Zeitraum aus, für den Sie die Statistik anzeigen möchten.

### Nächste Schritte

Um weitere Informationen zu NSX Edge anzuzeigen, klicken Sie auf **Verwalten (Manage)** und anschließend auf **Einstellungen (Settings)**.

## NSX Edge erneut bereitstellen

Wenn NSX Edge-Dienste nach einer erzwungenen Synchronisierung nicht wie erwartet funktionieren, können Sie die NSX Edge-Instanz erneut bereitstellen.

---

**Hinweis** Das erneute Bereitstellen ist eine Aktion, die den Betrieb unterbricht. Es empfiehlt sich, zuerst eine erzwungene Synchronisierung durchzuführen und erst, wenn sich das Problem dadurch nicht beheben lässt, eine erneute Bereitstellung vorzunehmen.

---

Das erneute Bereitstellen einer NSX Edge-Instanz führt zu den folgenden Aktionen:

- Edge-Appliances werden gelöscht und mit der aktuellsten Konfiguration neu bereitgestellt.
- Logische Router werden vom Controller gelöscht und dann mit der neuesten Konfiguration neu erstellt.
- Distributed Logical Router-Instanzen auf Hosts werden gelöscht und dann mit der neuesten Konfiguration neu erstellt.

OSPF-Nachbarschaften sind von der erneuten Bereitstellung ausgenommen, wenn Graceful Restart nicht aktiviert wurde.

---

**Wichtig** In einer Cross-vCenter-Umgebung müssen Sie die NSX Edge-Instanz zunächst auf dem primären NSX Manager erneut bereitstellen. Danach stellen Sie die NSX Edge-Instanz auf den sekundären NSX Managern erneut bereit. Die NSX Edge-Instanzen müssen sowohl auf dem primären als auch sekundären NSX Manager erneut bereitgestellt werden.

---

### Voraussetzungen

- Überprüfen Sie, ob der Host über ausreichend Ressourcen für die Bereitstellung zusätzlicher NSX Edge Services Gateway-Appliances während der erneuten Bereitstellung verfügt. Unter [Kapitel 1 Systemvoraussetzungen für NSX](#) werden die für jede NSX Edge-Größe erforderlichen Ressourcen dargestellt.
  - Für eine einzelne NSX Edge-Instanz befinden sich während der erneuten Bereitstellung zwei NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status.

- Für eine NSX Edge-Instanz mit Hochverfügbarkeit (HA, High Availability) werden beide Ersetzungs-Appliances bereitgestellt, bevor die alten Appliances ersetzt werden. Das bedeutet, dass sich während des Upgrades einer bestimmten NSX Edge vier NSX Edge-Appliances der geeigneten Größe im eingeschalteten Status befinden. Sobald die NSX Edge-Instanz erneut bereitgestellt wurde, kann eine der HA-Appliances aktiv werden.
- Stellen Sie sicher, dass die Hostcluster, die im konfigurierten und aktuellen Speicherort für die NSX Edge-Appliance aufgeführt sind, für NSX vorbereitet sind und dass für deren Messaging-Infrastruktur der Status GREEN (GRÜN) gilt. Wenn der konfigurierte Speicherort nicht verfügbar ist, etwa weil der Cluster nach der Erstellung der NSX Edge-Appliance entfernt wurde, überprüfen Sie nur den aktuellen Speicherort.
- Suchen Sie die ID des ursprünglich konfigurierten Speicherorts (*configuredResourcePool > Id*) und des aktuellen Speicherorts (*resourcePoolId*) mit der GET `https://NSX-Manager-IP-Address/api/4.0/edges/{edgeId}/appliances-API-Anforderung`.
- Ermitteln Sie mit der GET `https://NSX-Manager-IP-Address/api/2.0/nwfabric/status?resource={resourceId}-API-Anforderung` den Status der Hostvorbereitung und der Messaging-Infrastruktur für diese Cluster, wobei *resourceId* die ID des konfigurierten und des aktuellen Speicherorts der NSX Edge-Appliances darstellt, die zuvor gefunden wurden.
- Suchen Sie im Antworttext nach dem Status, der der *featureId* von `com.vmware.vshield.vsm.nwfabric.hostPrep` entspricht: Der Status muss GREEN (GRÜN) lauten.


```
<nwFabricFeatureStatus>
 <featureId>com.vmware.vshield.vsm.nwfabric.hostPrep</featureId>
 <featureVersion>6.3.1.5124716</featureVersion>
 <updateAvailable>false</updateAvailable>
 <status>GREEN</status>
 <installed>true</installed>
 <enabled>true</enabled>
 <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- Suchen Sie im Antworttext nach dem Status, der der *featureId* von `com.vmware.vshield.vsm.messagingInfra` entspricht: Der Status muss GREEN (GRÜN) lauten.

```
<nwFabricFeatureStatus>
 <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
 <updateAvailable>false</updateAvailable>
 <status>GREEN</status>
 <installed>true</installed>
 <enabled>true</enabled>
 <allowConfiguration>false</allowConfiguration>
</nwFabricFeatureStatus>
```

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.

- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Wählen Sie eine NSX Edge-Instanz aus.
- 4 Klicken Sie auf das Symbol **Aktionen (Actions)** (  ) und wählen Sie **Edge erneut bereitstellen (Redeploy Edge)**.

### Ergebnisse

Die virtuelle NSX Edge-Maschine wird durch eine neue virtuelle Maschine ersetzt und alle Dienste werden wiederhergestellt. Wenn das erneute Bereitstellen nicht funktioniert, schalten Sie die virtuelle NSX Edge-Maschine aus und wiederholen Sie den Vorgang.NSX Edge

---

**Hinweis** Das erneute Bereitstellen gelingt in den folgenden Fällen möglicherweise nicht.

- Der Ressourcenpool, auf dem NSX Edge installiert wurde, befindet sich nicht mehr in der vCenter-Bestandsliste oder seine MO-ID (Managed Objekt-ID) hat sich geändert.
- Der Datenspeicher, auf dem NSX Edge installiert wurde, ist beschädigt, nicht gemountet oder unzugänglich.
- Die dvportGroups, mit denen die NSX Edge-Schnittstellen verbunden waren, befinden sich nicht mehr in der vCenter-Bestandsliste oder ihre MO-ID (Bezeichner in vCenter Server) hat sich geändert.

Wenn eine der oben genannten Bedingungen zutrifft, müssen Sie die MO-ID des Ressourcenpools, des Datenspeichers oder der dvPortGroup mit einem REST API-Aufruf aktualisieren. Weitere Informationen hierzu finden Sie im *NSX API-Programmierhandbuch*.


---

Wenn der FIPS-Modus für NSX Edge aktiviert ist und ein Fehler auftritt, lässt NSX Manager die erneute Edge-Bereitstellung nicht zu. Sie müssen Infrastrukturprobleme bei Kommunikationsfehlern auflösen, anstatt das Edge neu bereitzustellen.

## Herunterladen von Tech-Support-Protokollen für NSX Edge

Sie können Protokolle für den technischen Support für jede NSX Edge-Instanz herunterladen. Wenn High Availability für die NSX Edge-Instanz aktiviert ist, werden die Support-Protokolle von beiden virtuellen NSX Edge-Maschinen heruntergeladen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Wählen Sie eine NSX Edge-Instanz aus.
- 4 Klicken Sie auf **Aktionen** (  ), und wählen Sie **Herunterladen von Tech-Support-Protokollen**.
- 5 Sobald die Protokolle für den technischen Support generiert wurden, klicken Sie auf **Herunterladen**.

# Hinzufügen einer statischen Route

Sie können eine statische Route für ein Ziel-Subnetz oder einen Zielhost hinzufügen.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Routing**.
- 5 Wählen Sie im linken Fensterbereich **Statische Routen (Static Routes)** aus.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 7 Geben Sie unter **Netzwerk (Network)** das Netzwerk in CIDR-Notation ein.
- 8 Geben Sie die IP-Adresse für **Nächster Hop (Next Hop)** ein.  
Der Router muss in der Lage sein, direkt den nächsten Hop zu erreichen.  
Wenn ECMP aktiviert ist, können Sie mehrere nächste Hops eingeben.
- 9 Wählen Sie die **Schnittstelle (Interface)** aus, auf der Sie eine statische Route hinzufügen möchten.
- 10 Bearbeiten Sie unter **MTU** den maximalen Übertragungswert für die Datenpakete, falls erforderlich.  
Der MTU-Wert darf nicht höher als der MTU-Wert sein, der in der NSX Edge-Schnittstelle festgelegt wurde.
- 11 Wenn Sie dazu aufgefordert werden, geben Sie den **Admin Distance (Admin Distance)** ein.  
Wählen Sie einen Wert zwischen 1 und 255. Der Admin Distance wird zur Auswahl der Route verwendet, wenn mehrere Routen für ein bestimmtes Netzwerk verwendet werden können. Je geringer der Admin Distance, desto höher ist die Präferenz für die Route.

**Tabelle 9-3. Standard-Admin-Abstände**

Routenquelle	Standard-Admin Distance
Verbunden	0
Statisch	1
Externes BGP	20
Area-internes OSPF	30
Area-übergreifendes OSPF	110
Internes BGP	200

Ein administrative distance von 255 bewirkt, dass die statische Route von der Routing-Tabelle (RIB) und der Datenebene ausgeschlossen und die Route somit nicht verwendet wird.

**12** (Optional) Geben Sie die **Gebietsschema-ID (Locale ID)** ein.

Routen haben standardmäßig dieselbe Gebietsschema-ID wie der NSX Manager. Wenn Sie hier eine Gebietsschema-ID angeben, wird die Route dieser Gebietsschema-ID zugewiesen. Diese Routen werden nur an Hosts gesendet, die eine übereinstimmende Gebietsschema-ID aufweisen. Weitere Informationen hierzu finden Sie unter [Cross-vCenter NSX-Topologien](#).

**13** (Optional) Geben Sie eine **Beschreibung (Description)** für die statische Route ein.

**14** Klicken Sie auf **OK**.

## Konfigurieren von OSPF auf einem logischen (Distributed) Router

Durch das Konfigurieren von OSPF auf einem logischen Router wird VM-Konnektivität über logische Router hinweg und von logischen Routern zu Edge Services Gateways (ESGs) aktiviert.

OSPF-Routing-Richtlinien bieten einen dynamischen Vorgang des Datenverkehrs-Load-Balancer zwischen Routen mit gleichen Kosten.

Ein OSPF-Netzwerk wird in Routing-Areas unterteilt, um den Datenverkehrsfluss zu optimieren und die Größe der Routing-Tabellen zu begrenzen. Eine Area ist eine logische Sammlung von OSPF-Netzwerken, Routern und Links, die über dieselbe Area-Identifikation verfügen.

Areas werden anhand einer Area-ID identifiziert.

### Voraussetzungen

Es muss eine Router-ID konfiguriert werden, wie unter [OSPF wird im logischen \(verteilten\) Router konfiguriert](#) dargestellt.

Wenn Sie eine Router-ID aktivieren, wird das Feld standardmäßig mit der Uplink-Schnittstelle des logischen Routers ausgefüllt.

### Verfahren

- 1** Melden Sie sich beim vSphere Web Client an.
- 2** Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3** Doppelklicken Sie auf einen logischen Router.
- 4** Klicken Sie auf **Routing** und anschließend auf **OSPF**.

## 5 Aktivieren Sie OSPF.

- a Klicken Sie auf **Bearbeiten (Edit)** in der oberen rechten Ecke des Fensters und dann auf **OSPF aktivieren (Enable OSPF)**.
- b Geben Sie in **Weiterleitungsadresse (Forwarding Address)** eine IP-Adresse ein, die von dem Router-Datenpfad-Modul in den Hosts verwendet wird, um Datenpfadpakete weiterzuleiten.
- c Geben Sie in **Protokolladresse (Protocol Address)** eine eindeutige IP-Adresse innerhalb desselben Subnetzes wie in **Weiterleitungsadresse (Forwarding Address)** ein. Die Protokolladresse wird vom Protokoll zum Gestalten benachbarter Bereiche mit den Peers verwendet.

## 6 Konfigurieren Sie die OSPF-Areas.

- a Sie können auch die „Not-So-Stubby-Area“ (NSSA) 51 löschen, die standardmäßig konfiguriert wird.
- b Klicken Sie in **Area Definition (Area Definitions)** auf das Symbol **Hinzufügen (Add)**.
- c Geben Sie eine Area-ID ein. NSX Edge unterstützt eine Area-ID in Form einer IP-Adresse oder Dezimalzahl.
- d Wählen Sie unter **Typ (Type)** die Option **Normal** oder **NSSA** aus.

NSSAs verhindert das Überfluten von AS-externen Verbindungsstatus-Ankündigungen (LSAs) in NSSAs. Sie verwenden das Standardrouting zu externen Zielen. Daher müssen NSSAs am Rand einer OSPF-Routing-Domäne abgelegt werden. NSSA kann externe Routen in die OSPF-Routing-Domäne importieren, sodass der Transit-Dienst für kleine Routing-Domänen bereitgestellt wird, die nicht Teil der OSPF-Routing-Domäne sind.

## 7 (Optional) Wählen Sie den Typ der **Authentifizierung (Authentication)**. OSPF führt die Authentifizierung auf der Area-Ebene aus.

Daher müssen alle Router innerhalb einer Area über dieselbe Authentifizierung und das entsprechend konfigurierte Kennwort verfügen. Damit die MD5-Authentifizierung funktionieren kann, müssen sowohl der Empfangs- als auch der Übertragungsrouten über denselben MD5-Schlüssel verfügen.

- a **Keine (None)**: Keine Authentifizierung ist erforderlich; dies ist der Standardwert.
- b **Kennwort (Password)**: Bei dieser Authentifizierungsmethode wird ein Kennwort im übertragenen Paket eingeschlossen.

- c **MD5:** Diese Authentifizierungsmethode verwendet die MD5-Verschlüsselung (Message Digest Type 5). Ein MD5-Prüfsummenwert ist im übertragenen Paket eingeschlossen.
- d Geben Sie für den Authentifizierungstyp **Kennwort (Password)** oder **MD5** das Kennwort bzw. den MD5-Schlüssel ein.

---

#### Hinweis

- Bei aktiviertem FIPS-Modus können Sie die **MD5**-Authentifizierung nicht konfigurieren.
  - NSX verwendet immer einen Schlüssel-ID-Wert von 1. Jedes Nicht-NSX-Gerät mit einem Peering mit einem NSX Edge oder einem Distributed Logical Router muss für die Verwendung eines Schlüssel-ID-Werts von 1 konfiguriert sein, wenn die MD5-Authentifizierung verwendet wird. Ansonsten wird keine OSPF-Sitzung eingerichtet.
- 

### 8 Ordnen Sie die Schnittstellen den Areas :zu.

- a Klicken Sie in **Zuordnung von Area zu Schnittstelle (Area to Interface Mapping)** auf das Symbol **Hinzufügen (Add)**, um die Schnittstelle zuzuordnen, die zur OSPF-Area gehört.
- b Wählen Sie die Schnittstelle, die Sie zuordnen möchten, und der OSPF-Area, der sie zugeordnet werden soll.

### 9 (Optional) Bearbeiten Sie bei Bedarf die standardmäßigen OSPF -Einstellungen.

In den meisten Fällen wird empfohlen, die standardmäßigen OSPF-Einstellungen beizubehalten. Wenn Sie Änderungen an den Einstellungen vornehmen, stellen Sie sicher, dass die OSPF-Peers dieselben Einstellungen verwenden.

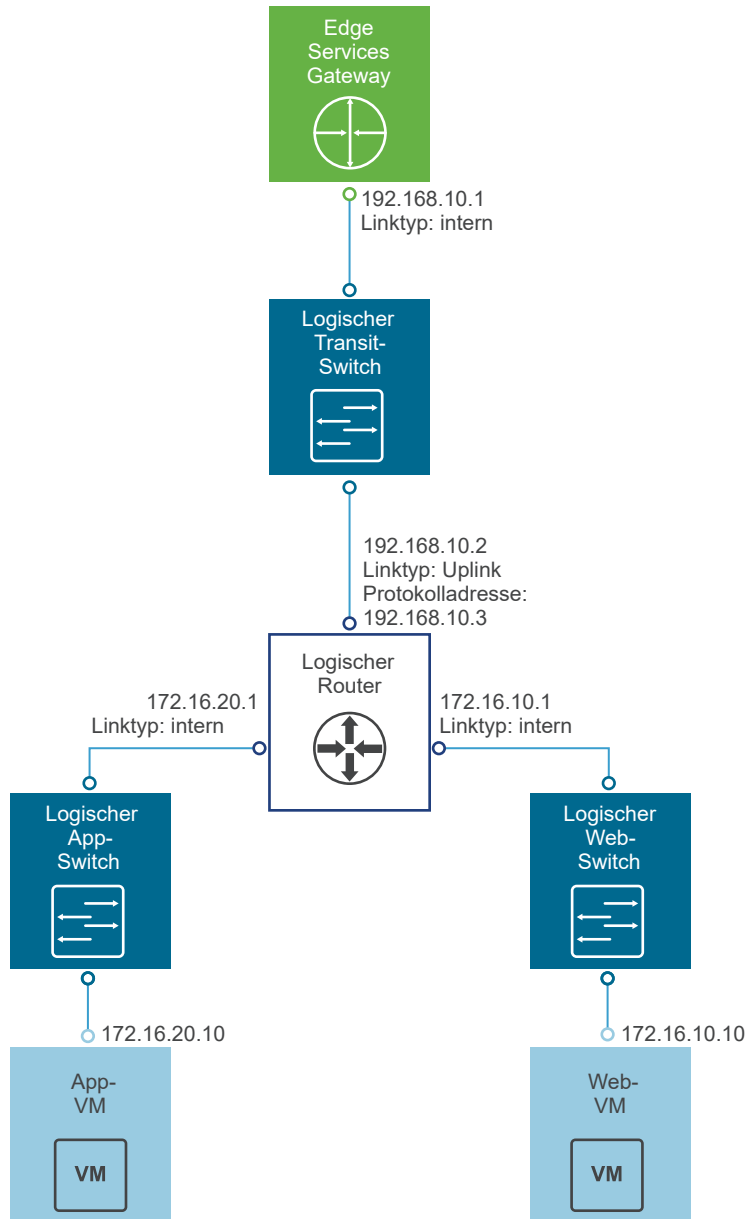
- a **Hallo-Intervall (Hello Interval)** zeigt das Standardintervall zwischen Hallo-Paketen an, die über die Schnittstelle gesendet werden.
- b **Ausfallintervall (Dead Interval)** zeigt das Standardintervall an, während dessen mindestens ein Hallo-Paket von einem Nachbarn empfangen werden muss, bevor der Router den Nachbarn als ausgefallen einstuft.
- c **Priorität (Priority)** zeigt die Standardpriorität der Schnittstelle an. Die Schnittstelle mit der höchsten Priorität ist der festgelegte Router.
- d **Kosten (Cost)** einer Schnittstelle zeigt den Standard-Overhead an, der für das Senden von Paketen über die Schnittstelle erforderlich ist. Die Kosten einer Schnittstelle sind umgekehrt proportional zur Bandbreite dieser Schnittstelle. Je größer die Bandbreite ist, desto geringer sind die Kosten.

### 10 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Beispiel: OSPF wird im logischen (verteilten) Router konfiguriert

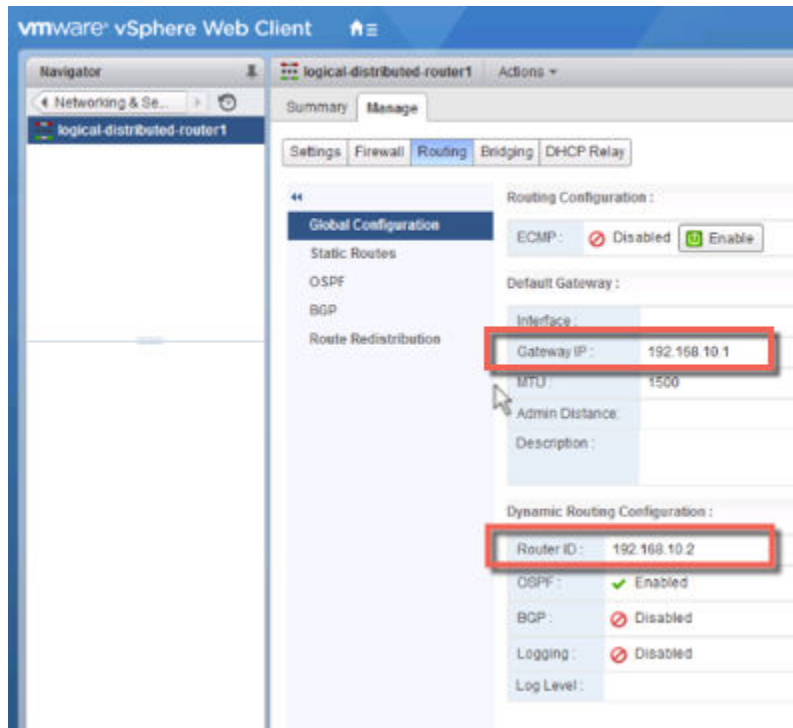
Ein einfaches NSX-Szenario, bei dem OSPF verwendet wird, ist, wenn ein logischer Router (DLR) und ein Edge Services Gateway (ESG) OSPF-Nachbarn sind, wie hier gezeigt.

**Abbildung 9-1. NSX-Topologie**

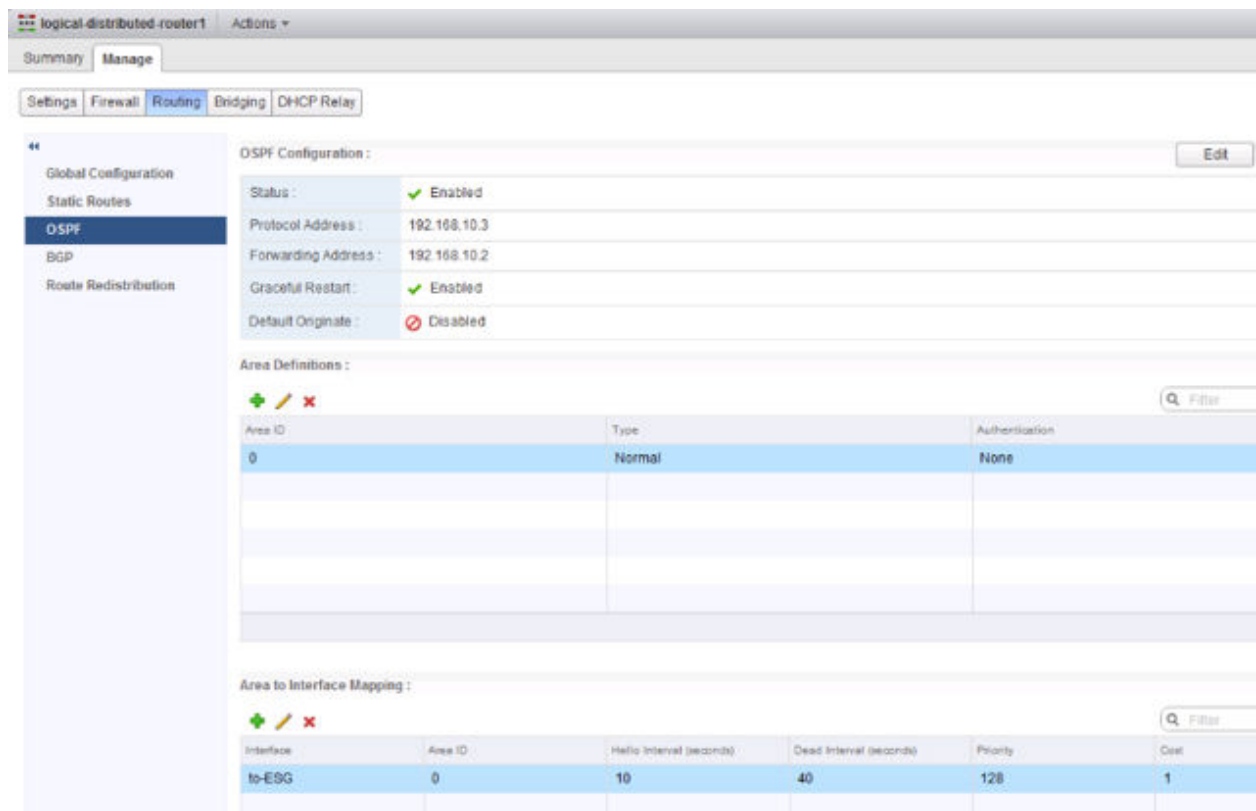


Im folgenden Bildschirm ist das Standard-Gateway des logischen Routers die IP-Adresse der internen Schnittstelle von ESG (192.168.10.1).

Die Router-ID ist die Uplink-Schnittstelle des logischen Routers – in anderen Worten, die IP-Adresse, die ESG gegenüberliegt (192.168.10.2).



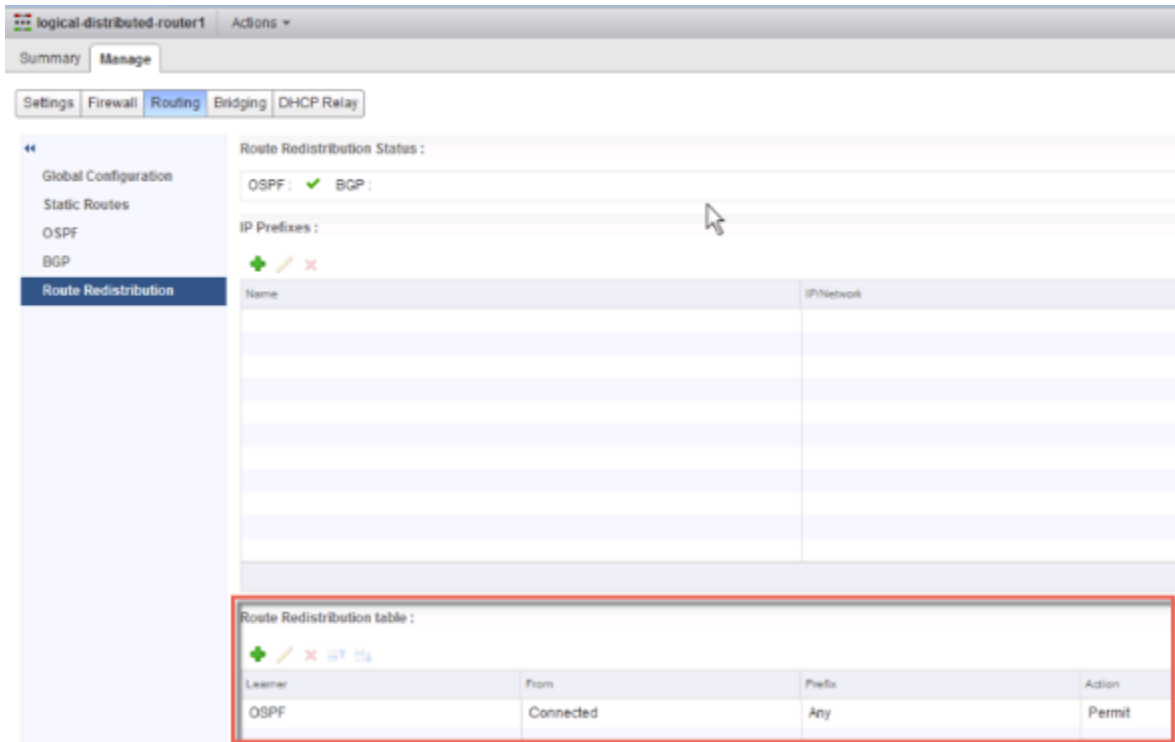
Die Konfiguration des logischen Routers verwendet 192.168.10.2 als Weiterleitungsadresse. Die Protokolladresse kann eine beliebige IP-Adresse sein, die sich im selben Subnetz befindet und an keiner anderen Stelle verwendet wird. In diesem Fall ist 192.168.10.3 konfiguriert. Die konfigurierte Area-ID ist 0, und die Uplink-Schnittstelle (die Schnittstelle, die ESG gegenüberliegt) wird dieser Area zugeordnet.



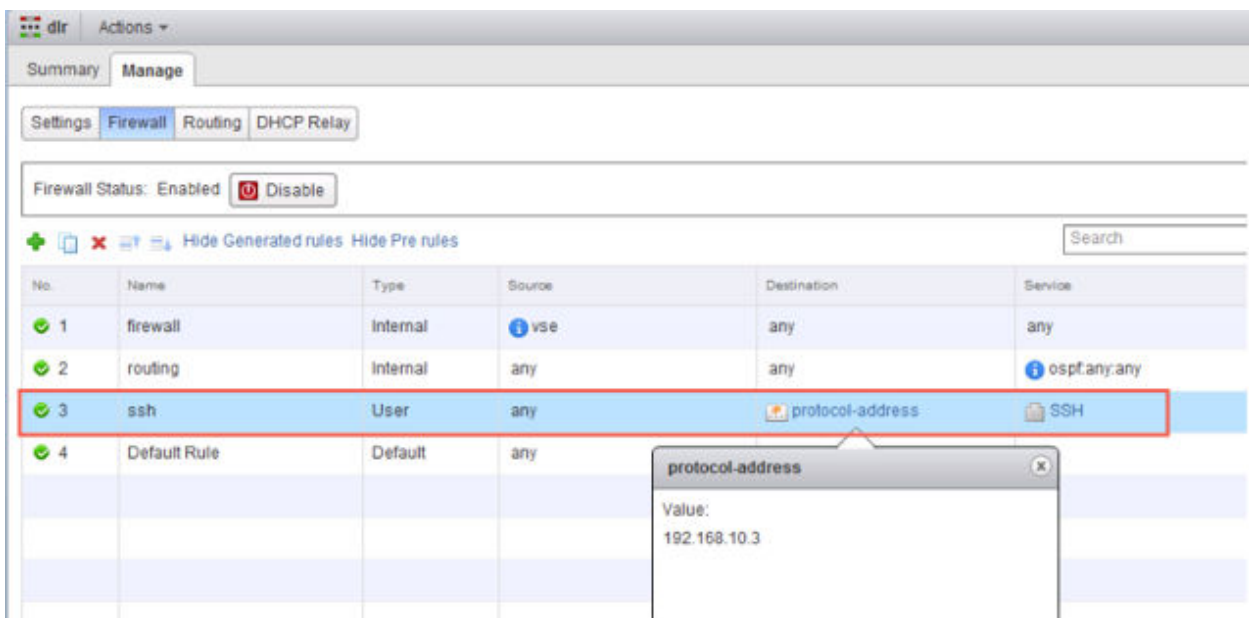
## Nächste Schritte

Stellen Sie sicher, dass durch die Route Redistribution und die Firewallkonfiguration die richtigen Routen angekündigt werden können.

In diesem Beispiel werden die verbundenen Routen (172.16.10.0/24 und 172.16.20.0/24) nach OSPF angekündigt.



Wenn Sie SSH beim Erstellen des logischen Routers aktiviert haben, müssen Sie auch einen Firewallfilter konfigurieren, der SSH zur Protokolladresse des logischen Routers zulässt. Beispiel:



# Konfigurieren von OSPF in einem Edge Services Gateway

Durch das Konfigurieren von OSPF in einem Edge Services Gateway (ESG) kann das ESG lernen und Routen ankündigen. Der gängigste Einsatzbereich von OSPF in einer ESG ist die Verknüpfung zwischen dem ESG und einem logischen (Distributed) Router. Dadurch kann das ESG in Bezug auf die logischen Schnittstellen (LIFs) lernen, die mit dem logischen Router verbunden sind. Dieses Ziel kann mit OSPF, IS-IS, BGP oder statischem Routing erreicht werden.

OSPF-Routing-Richtlinien bieten einen dynamischen Vorgang des Datenverkehrs-Load-Balancer zwischen Routen mit gleichen Kosten.

Ein OSPF-Netzwerk wird in Routing-Areas unterteilt, um den Datenverkehrsfluss zu optimieren und die Größe der Routing-Tabellen zu begrenzen. Eine Area ist eine logische Sammlung von OSPF-Netzwerken, Routern und Links, die über dieselbe Area-Identifikation verfügen.

Areas werden anhand einer Area-ID identifiziert.

## Voraussetzungen

Es muss eine Router-ID konfiguriert werden, wie unter [OSPF wird in einem Edge Services Gateway konfiguriert](#) dargestellt.

Wenn Sie eine Router-ID aktivieren, wird das Feld standardmäßig mit der IP-Adresse der Uplink-Schnittstelle von ESG ausgefüllt.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf ein ESG.
- 4 Klicken Sie auf **Routing** und anschließend auf **OSPF**.
- 5 Aktivieren Sie OSPF.
  - a Klicken Sie auf **Bearbeiten (Edit)** in der oberen rechten Ecke des Fensters und dann auf **OSPF aktivieren (Enable OSPF)**.
  - b (Optional) Klicken Sie auf **Graceful Restart aktiviert (Enable Graceful Restart)**, damit die Paketweiterleitung beim Neustart von OSPF-Diensten nicht unterbrochen wird.
  - c (Optional) Klicken Sie auf **Default Originate aktiviert (Enable Default Originate)**, damit sich ESG selbst als ein Standard-Gateway bei seinen Peers ankündigen kann.
- 6 Konfigurieren Sie die OSPF-Areas.
  - a (Optional) Löschen Sie die „Not-So-Stubby-Area“ (NSSA) 51, die standardmäßig konfiguriert wird.
  - b Klicken Sie in **Area Definition (Area Definitions)** auf das Symbol **Hinzufügen (Add)**.

- c Geben Sie eine Area-ID ein. NSX Edge unterstützt eine Area-ID in Form einer IP-Adresse oder Dezimalzahl.
- d Wählen Sie unter **Typ (Type)** die Option **Normal** oder **NSSA** aus.

NSSAs verhindert das Überfluten von AS-externen Verbindungsstatus-Ankündigungen (LSAs) in NSSAs. Sie verwenden das Standardrouting zu externen Zielen. Daher müssen NSSAs am Rand einer OSPF-Routing-Domäne abgelegt werden. NSSA kann externe Routen in die OSPF-Routing-Domäne importieren, sodass der Transit-Dienst für kleine Routing-Domänen bereitgestellt wird, die nicht Teil der OSPF-Routing-Domäne sind.

- 7 (Optional) Wenn Sie für den Typ **NSSA** auswählen, wird das Feld **NSSA-Konvertierungsrolle (NSSA Translator Role)** angezeigt. Aktivieren Sie das Kontrollkästchen **Immer (Always)**, um Typ-7-LSAs in Typ-5-LSAs zu konvertieren. Alle Typ-7-LSAs werden durch den NSSA-Typ in Typ-5-LSAs konvertiert.

- 8 (Optional) Wählen Sie den Typ der **Authentifizierung (Authentication)**. OSPF führt die Authentifizierung auf der Area-Ebene aus.

Daher müssen alle Router innerhalb einer Area über dieselbe Authentifizierung und das entsprechend konfigurierte Kennwort verfügen. Damit die MD5-Authentifizierung funktionieren kann, müssen sowohl der Empfangs- als auch der Übertragungsrouten über denselben MD5-Schlüssel verfügen.

- a **Keine (None)**: Keine Authentifizierung ist erforderlich; dies ist der Standardwert.
- b **Kennwort (Password)**: Bei dieser Authentifizierungsmethode wird ein Kennwort im übertragenen Paket eingeschlossen.
- c **MD5**: Diese Authentifizierungsmethode verwendet die MD5-Verschlüsselung (Message Digest Type 5). Ein MD5-Prüfsummenwert ist im übertragenen Paket eingeschlossen.
- d Geben Sie für den Authentifizierungstyp **Kennwort (Password)** oder **MD5** das Kennwort bzw. den MD5-Schlüssel ein.

---

#### Hinweis

- Bei aktiviertem FIPS-Modus können Sie die **MD5**-Authentifizierung nicht konfigurieren.
  - NSX verwendet immer einen Schlüssel-ID-Wert von 1. Jedes Nicht-NSX-Gerät mit einem Peering mit einem NSX Edge oder einem Distributed Logical Router muss für die Verwendung eines Schlüssel-ID-Werts von 1 konfiguriert sein, wenn die MD5-Authentifizierung verwendet wird. Ansonsten wird keine OSPF-Sitzung eingerichtet.
- 

- 9 Ordnen Sie die Schnittstellen den Areas :zu.
  - a Klicken Sie in **Zuordnung von Area zu Schnittstelle (Area to Interface Mapping)** auf das Symbol **Hinzufügen (Add)**, um die Schnittstelle zuzuordnen, die zur OSPF-Area gehört.
  - b Wählen Sie die Schnittstelle, die Sie zuordnen möchten, und der OSPF-Area, der sie zugeordnet werden soll.

**10** (Optional) Bearbeiten Sie die standardmäßigen OSPF -Einstellungen.

In den meisten Fällen wird empfohlen, die standardmäßigen OSPF-Einstellungen beizubehalten. Wenn Sie Änderungen an den Einstellungen vornehmen, stellen Sie sicher, dass die OSPF-Peers dieselben Einstellungen verwenden.

- a **Hallo-Intervall (Hello Interval)** zeigt das Standardintervall zwischen Hallo-Paketen an, die über die Schnittstelle gesendet werden.
- b **Ausfallintervall (Dead Interval)** zeigt das Standardintervall an, während dessen mindestens ein Hallo-Paket von einem Nachbarn empfangen werden muss, bevor der Router den Nachbarn als ausgefallen einstuft.
- c **Priorität (Priority)** zeigt die Standardpriorität der Schnittstelle an. Die Schnittstelle mit der höchsten Priorität ist der festgelegte Router.
- d **Kosten (Cost)** einer Schnittstelle zeigt den Standard-Overhead an, der für das Senden von Paketen über die Schnittstelle erforderlich ist. Die Kosten einer Schnittstelle sind umgekehrt proportional zur Bandbreite dieser Schnittstelle. Je größer die Bandbreite ist, desto geringer sind die Kosten.

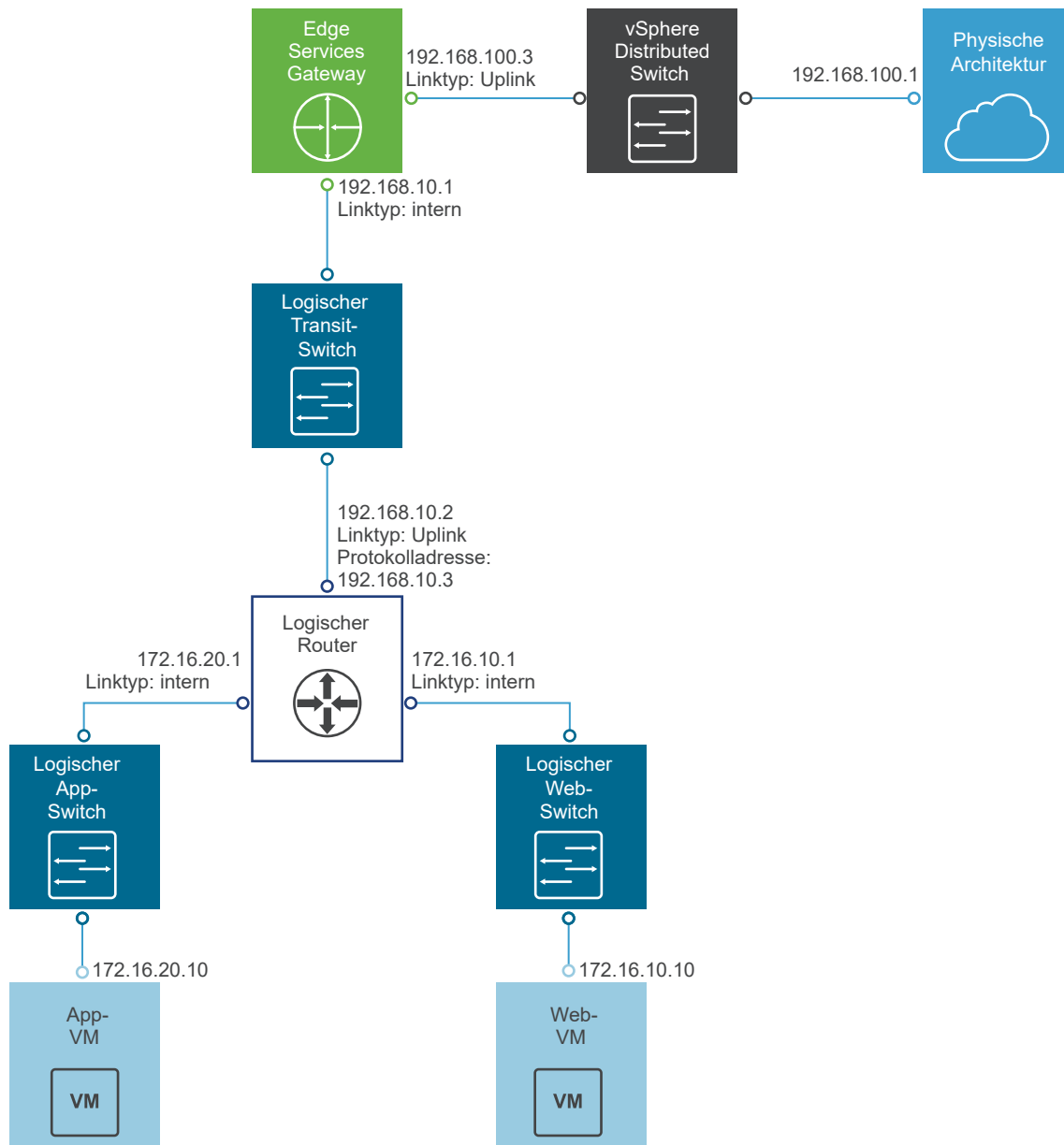
**11** Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.**12** Stellen Sie sicher, dass durch die Route Redistribution und die Firewallkonfiguration die richtigen Routen angekündigt werden können.

## Beispiel: OSPF wird in einem Edge Services Gateway konfiguriert

Ein einfaches NSX-Szenario, bei dem OSPF verwendet wird, liegt vor, wenn wie hier dargestellt ein logischer Router und ein Edge Services Gateway OSPF-Nachbarn sind.

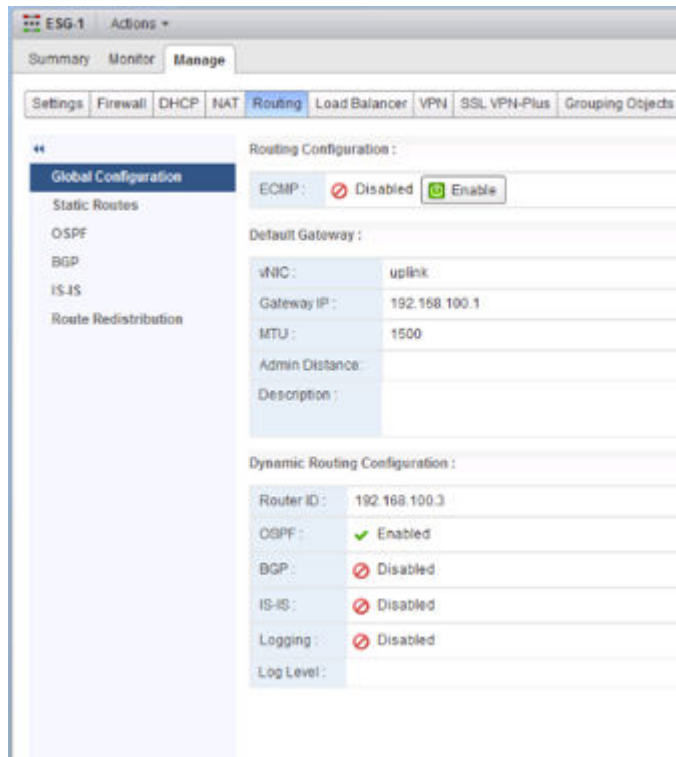
Das ESG kann mit der Außenwelt durch eine Bridge, einen physischen Router (oder wie hier gezeigt) durch eine Uplink-Portgruppe in einem vSphere Distributed Switch verbunden werden.

Abbildung 9-2. NSX-Topologie

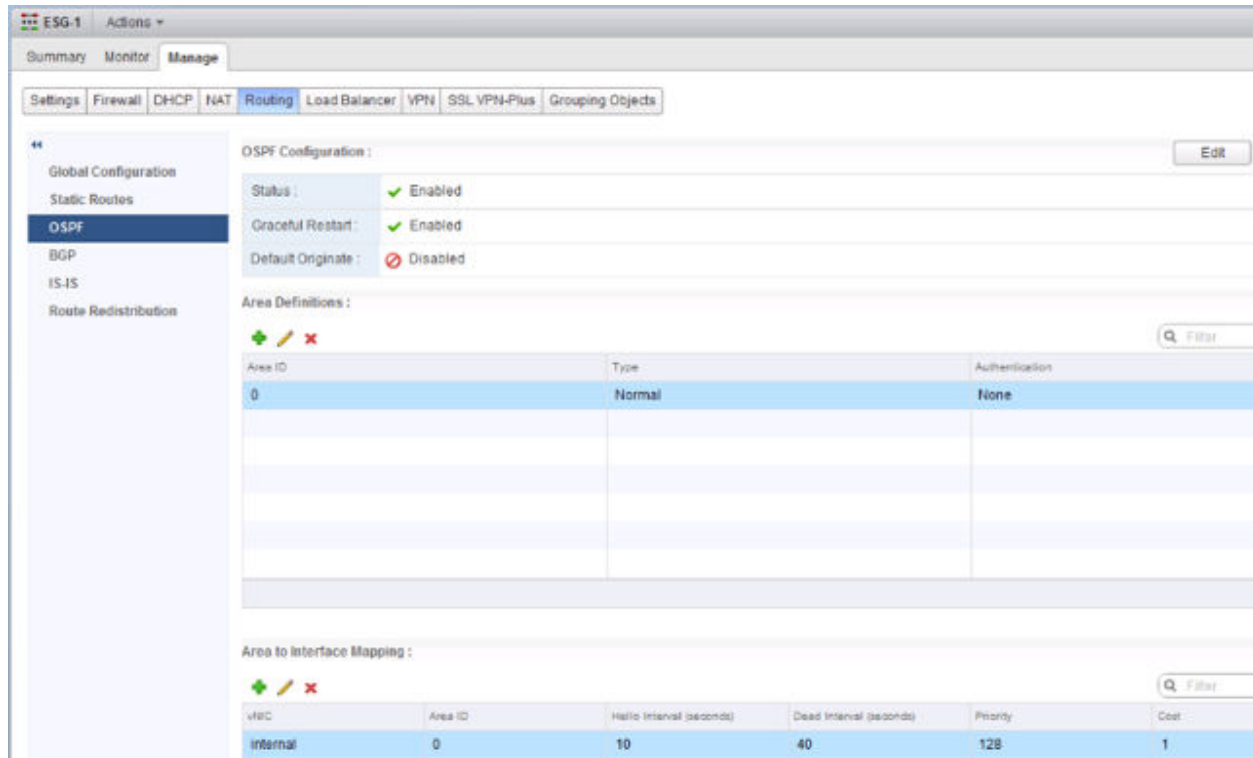


Im folgenden Bildschirm ist das Standard-Gateway von ESG die Uplink-Schnittstelle von ESG zu seinem externen Peer.

Die Router-ID ist die IP-Adresse der Uplink-Schnittstelle von ESG – in anderen Worten, die IP-Adresse, die seinem externen Peer gegenüberliegt.



Die konfigurierte Area-ID ist 0, und die interne Schnittstelle (die Schnittstelle, die dem logischen Router gegenüberliegt) wird der Area zugeordnet.



Die verbundenen Routen werden erneut in OSPF verteilt, sodass der OSPF-Nachbar (der logische Router) Informationen über das Uplink-Netzwerk von ESG abrufen kann.

Summary Monitor Manage

Settings Firewall DHCP NAT **Routing** Load Balancer VPN SSL VPN-Plus Grouping Objects

Global Configuration  
Static Routes  
OSPF  
BGP  
IS-IS  
**Route Redistribution**

Route Redistribution States :

OSPF ☒ ISIS ☐ BGP ☐

IP Prefixes :

+ - ✎ ✖

Name	IP Network

Route Redistribution table :

+ - ✎ ✖

Learned	From	Prefix	Action
OSPF	Connected	Any	Permit

**Hinweis** Zusätzlich kann OSPF zwischen dem ESG und seinem externen Peer-Router konfiguriert werden, aber üblicherweise verwendet dieser Link BGP für die Routen-Ankündigung.

Stellen Sie sicher, dass das ESG die externen Routen von OSPF von dem logischen Router abrufen kann.

```
NSX-edge-7-0> show ip route

Codes: 0 - OSPF derived, i - IS-IS derived, B - BGP derived,
C - connected, S - static, L1 - IS-IS level-1, L2 - IS-IS level-2,
IA - OSPF inter area, E1 - OSPF external type 1, E2 - OSPF external type 2,
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

Total number of routes: 5

S 0.0.0.0/0 [0/0] via 192.168.100.1
0 E2 172.16.10.0/24 [110/1] via 192.168.10.2
0 E2 172.16.20.0/24 [110/1] via 192.168.10.2
C 192.168.10.0/29 [0/0] via 192.168.10.1
C 192.168.100.0/24 [0/0] via 192.168.100.3
```

Um die Konnektivität zu überprüfen, stellen Sie sicher, dass ein externes Gerät in der physischen Architektur die VMs pingen kann.

Beispiel:

```
PS C:\Users\Administrator> ping 172.16.10.10
```

```
Pinging 172.16.10.10 with 32 bytes of data:
Reply from 172.16.10.10: bytes=32 time=5ms TTL=61
Reply from 172.16.10.10: bytes=32 time=1ms TTL=61
```

```
Ping statistics for 172.16.10.10:
 Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 5ms, Average = 3ms
```

```
PS C:\Users\Administrator> ping 172.16.20.10
```

```
Pinging 172.16.20.10 with 32 bytes of data:
Reply from 172.16.20.10: bytes=32 time=2ms TTL=61
Reply from 172.16.20.10: bytes=32 time=1ms TTL=61
```

```
Ping statistics for 172.16.20.10:
 Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

## Konfigurieren des BGP-Protokolls

Border Gateway Protocol (BGP) betrifft wichtige Routing-Entscheidungen. Es beinhaltet eine Tabelle zu IP-Netzwerken oder -Präfixen, die die Erreichbarkeit des Netzwerks zwischen den verschiedenen autonomen Systemen festlegen.

Eine zugrunde liegende Verbindung zwischen zwei BGP-Speakers wird hergestellt, bevor Routing-Informationen ausgetauscht werden. Keepalive-Nachrichten werden von den BGP-Speakers gesendet, um diese Beziehung beizubehalten. Nach dem Herstellen der Verbindung tauschen die BGP-Speakers Routen aus und synchronisieren ihre Tabellen.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Routing** und anschließend auf **BGP**.
- 5 Klicken Sie auf **Bearbeiten (Edit)**.
- 6 Klicken Sie im Dialogfeld „BGP-Konfiguration bearbeiten“ auf **BGP aktivieren (Enable BGP)**.
- 7 Klicken Sie auf **Graceful Restart aktivieren (Enable Graceful Restart)**, damit die Paketweiterleitung beim Neustart von BGP-Diensten nicht unterbrochen wird.
- 8 Klicken Sie auf **Default Originate aktivieren (Enable Default Originate)**, damit sich NSX Edge selbst als ein Standard-Gateway bei seinen Peers ankündigen kann.
- 9 Geben Sie die Router-ID in **Lokales AS (Local AS)** ein. Geben Sie das lokale AS ein. Dies wird angekündigt, wenn BGP-Peers mit Routern in anderen autonomen Systemen (AS) übereinstimmen. Der Pfad von autonomen Systemen, die eine Route durchläuft, wird als eine Metrik verwendet, wenn der beste Pfad zu einem Ziel ausgewählt wird.
- 10 Klicken Sie auf **OK**.
- 11 Klicken Sie unter **Nachbarn (Neighbors)** auf das Symbol **Hinzufügen (Add)**.
- 12 Geben Sie die IP-Adresse des Nachbarn ein.

Wenn Sie BGP-Peering zwischen einem Edge Services Gateway (ESG) und einem logischen Router konfigurieren, verwenden Sie die Protokoll-IP-Adresse des logischen Routers als die BGP-Nachbaradresse von ESG.

- 13 (Nur auf einem logischen Router) Geben Sie die Weiterleitungsadresse ein.

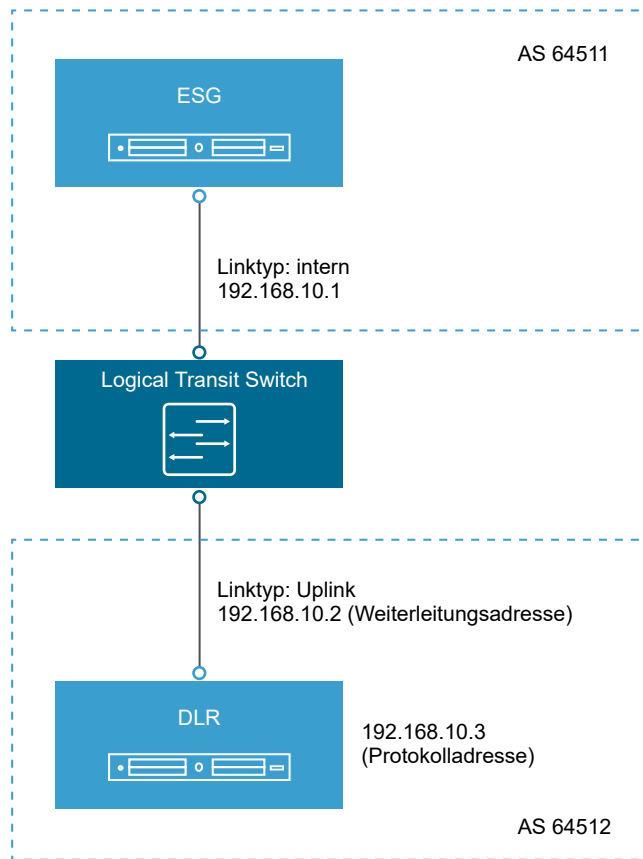
Die Weiterleitungsadresse ist die IP-Adresse, die Sie der Schnittstelle des Distributed Logical Router zugewiesen haben, der seinem BGP-Nachbarn gegenüberliegt (seine Uplink-Schnittstelle).

- 14 (Nur auf einem logischen Router) Geben Sie die Protokolladresse ein.

Die Protokolladresse ist die IP-Adresse, die der logische Router zum Gestalten einer BGP-Nachbar-Beziehung verwendet. Es kann eine beliebige IP-Adresse im selben Subnetz wie die Weiterleitungsadresse sein (solange sie nicht an einer anderen Stelle verwendet wird). Wenn Sie BGP-Peering zwischen einem Edge Services Gateway (ESG) und einem logischen Router konfigurieren, verwenden Sie die Protokoll-IP-Adresse des logischen Routers als die Nachbar-IP-Adresse von ESG.

- 15 Geben Sie das Remote-AS ein.
  - 16 Bearbeiten Sie bei Bedarf die Standardgewichtung für die Nachbarverbindung.
  - 17 **Hold Down-Timer (Hold Down Timer)** zeigt das Intervall (180 Sekunden) an, nachdem Sie keine Keepalive-Nachricht erhalten haben, dass die Software einen Peer als ausgefallen einstuft. Bearbeiten Sie den Eintrag, falls erforderlich.
  - 18 **Keepalive-Timer (Keep Alive Timer)** zeigt die Standardhäufigkeit (60 Sekunden) an, mit der die Software Keepalive-Nachrichten an seinen Peer sendet. Bearbeiten Sie den Eintrag, falls erforderlich.
  - 19 Wenn eine Authentifizierung erforderlich ist, geben Sie das Kennwort für die Authentifizierung ein. Jedes Segment, das über die Verbindung zwischen Nachbarn gesendet wurde, wird überprüft. Die MD5-Authentifizierung muss mit demselben Kennwort auf beiden BGP-Nachbarn konfiguriert werden. Anderenfalls wird keine Verbindung zwischen diesen hergestellt.  
  
Bei aktiviertem FIPS-Modus können Sie kein Kennwort eingeben.
  - 20 Um die Routen-Filterung aus einem Nachbarn festzulegen, klicken Sie in der Area **BGP-Filter (BGP Filters)** auf das Symbol **Hinzufügen (Add)**.
- 
- Vorsicht** Eine Regel „Alle blockieren“ wird am Ende der Filter erzwungen.
- 
- 21 Wählen Sie die Richtung aus, um festzulegen, ob Sie den Datenverkehr zu oder aus einem Nachbarn filtern.
  - 22 Wählen Sie die Aktion aus, um festzulegen, ob Sie den Datenverkehr zulassen oder verweigern.
  - 23 Geben Sie das Netzwerk im CIDR-Format ein, das Sie zum/vom Nachbarn filtern möchten.
  - 24 Geben Sie die zu filternden IP-Präfixe ein und klicken Sie auf **OK**.
  - 25 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

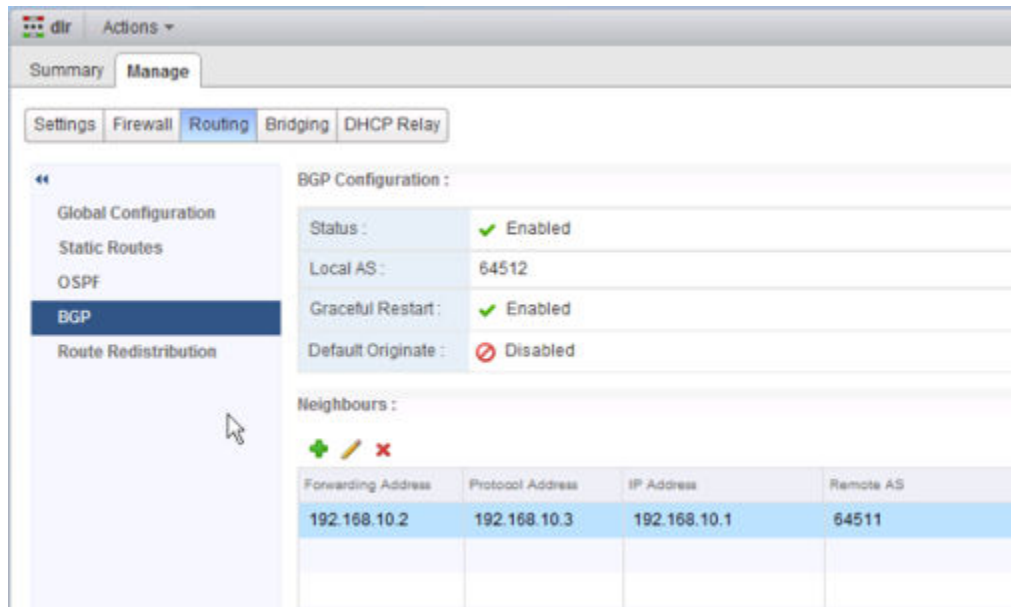
## Beispiel: BGP zwischen ESG und einem logischen Router konfigurieren



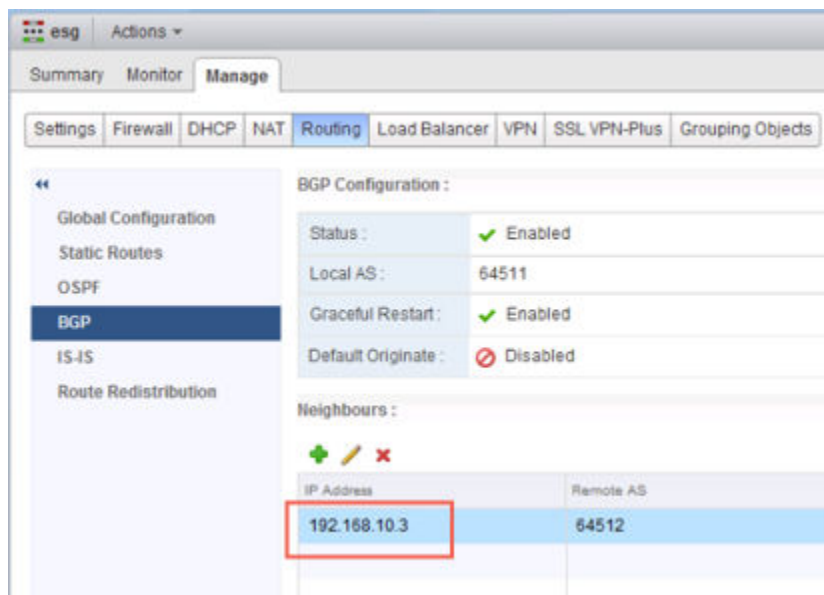
In dieser Topologie befindet sich ESG in AS 64511. Der logische Router (DLR) befindet sich in AS 64512.

Die Weiterleitungsadresse des logischen Routers ist 192.168.10.2. Dies ist die Adresse, die in der Uplink-Schnittstelle des logischen Routers konfiguriert wurde. Die Protokolladresse des logischen Routers ist 192.168.10.3. Dies ist die Adresse, mit der ESG die BGP-Peering-Beziehung mit dem logischen Router gestaltet.

Konfigurieren Sie auf dem logischen Router BGP wie dargestellt:



Konfigurieren Sie ESG BGP wie dargestellt:



Die Nachbaradresse von ESG ist 192.168.10.3, was der Protokolladresse des logischen Routers entspricht.

Führen Sie den `show ip bgp neighbors`-Befehl auf dem logischen Router aus und stellen Sie sicher, dass der BGP-Status „Hergestellt“ ist.

```

NSX-edge-6-0> show ip bgp neighbors

BGP neighbor is 192.168.10.1, remote AS 64511,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
 Route refresh: advertised and received
 Address family IPv4 Unicast:advertised and received
 Graceful restart Capability:advertised and received
 Restart remain time: 0
Received 120 messages, Sent 125 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
 Index 1 Identifier 0x9aa20f3c
 Route refresh request:received 0 sent 0
 Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 5
Local host: 192.168.10.3, Local port: 179
Remote host: 192.168.10.1, Remote port: 43846

```

Führen Sie den `show ip bgp neighbors`-Befehl auf ESG aus und stellen Sie sicher, dass der BGP-Status „Hergestellt“ ist.

```

NSX-edge-7-0> show ip bgp neighbors

BGP neighbor is 192.168.10.3, remote AS 64512,
BGP state = Established, up
Hold time is 180, Keep alive interval is 60 seconds
Neighbor capabilities:
 Route refresh: advertised and received
 Address family IPv4 Unicast:advertised and received
 Graceful restart Capability:advertised and received
 Restart remain time: 0
Received 121 messages, Sent 120 messages
Default minimum time between advertisement runs is 30 seconds
For Address family IPv4 Unicast:advertised and received
 Index 3 Identifier 0x40212c6c
 Route refresh request:received 0 sent 0
 Prefixes received 0 sent 0 advertised 0
Connections established 1, dropped 1
Local host: 192.168.10.1, Local port: 43846
Remote host: 192.168.10.3, Remote port: 179

```

## Konfigurieren der Route Redistribution

Standardmäßig nutzen Router Routen gemeinsam mit anderen Routern, die dasselbe Protokoll ausführen. In einer Umgebung mit mehreren Protokollen müssen Sie die Route Redistribution für die protokollübergreifende gemeinsame Nutzung von Routen konfigurieren.

Durch das Hinzufügen eines Verweigerungskriteriums für ihr Netzwerk können Sie eine Schnittstelle aus der Route Redistribution ausschließen. In NSX 6.2 wird die HA-Schnittstelle (Verwaltung) eines logischen (verteilten) Routers automatisch von der Route Redistribution ausgeschlossen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Routing** und dann auf **Route Redistribution (Route Redistribution)**.
- 5 Klicken Sie auf **Bearbeiten (Edit)** neben **Status der Route Redistribution (Route Redistribution Status)**.
- 6 Wählen Sie die Protokolle aus, für die Sie die Route Redistribution aktivieren, und klicken Sie auf **OK**.
- 7 Fügen Sie ein IP-Präfix hinzu.

Einträge in der IP-Präfix-Liste werden nacheinander verarbeitet.

- a Klicken Sie unter **IP-Präfixe (IP Prefixes)** auf das Symbol **Hinzufügen (Add)**.
- b Geben Sie einen Namen und eine IP-Adresse für das Netzwerk ein.  
  
Es wird nach einer exakten Übereinstimmung des eingegebenen IP-Präfix gesucht, es sei denn, Sie verwenden die Modifizierer „kleiner oder gleich“ bzw. „größer oder gleich“.
- c Klicken Sie auf **OK**.
- 8 Geben Sie Neuverteilungskriterien für das IP-Präfix an.
  - a Klicken Sie unter **Tabelle der Route Redistribution (Route Redistribution table)** auf das Symbol **Hinzufügen (Add)**.
  - b Wählen Sie unter **Protokoll für Lernende (Learner Protocol)** das Protokoll aus, das Routen von anderen Protokollen erlernen soll.
  - c Wählen Sie unter **Lernen zulassen von (Allow Learning from)** die Protokolle aus, von denen Routen erlernt werden sollen.
  - d Klicken Sie auf **OK**.
- 9 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Anzeigen der Gebietsschema-ID von NSX Manager

Jeder NSX Manager verfügt über eine Gebietsschema-ID. Standardmäßig ist sie auf die NSX Manager-UUID festgelegt. Diese Einstellung kann im globalen logischen Router, Cluster oder auf Host-Ebene überschrieben werden.

## Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security** und klicken Sie anschließend unter **Bestandsliste für Netzwerk und Sicherheit (Networking & Security Inventory)** auf einen NSX Manager.
- 2 Klicken Sie auf die Registerkarte **Übersicht (Summary)**. Das Feld **ID** enthält die UUID des NSX Manager.

## Konfigurieren der Gebietsschema-ID auf einem globalen (Distributed) Router

Wenn „Lokaler Ausgang“ beim Erstellen eines globalen logischen Routers aktiviert ist, werden Routen nur dann an Hosts gesendet, wenn die Gebietsschema-ID des Hosts mit der Gebietsschema-ID übereinstimmt, die der Route zugeordnet ist. Sie können die Gebietsschema-ID auf einem Router ändern, und diese aktualisierte Gebietsschema-ID wird allen Routen auf diesem Router zugeordnet (statisch und dynamisch). Die Routen werden an Hosts und Cluster mit übereinstimmenden Gebietsschema-IDs gesendet.

Unter [Cross-vCenter NSX-Topologien](#) finden Sie Informationen zu Routing-Konfigurationen für Cross-vCenter NSX-Umgebungen.

## Voraussetzungen

Der globale logische (Distributed) Router muss mit aktiviertem lokalen Ausgang erstellt worden sein.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf einen globalen logischen (Distributed) Router.
- 4 Klicken Sie auf die Registerkarte **Routing** und anschließend auf **Globale Konfiguration (Global Configuration)**.
- 5 Klicken Sie neben **Routing-Konfiguration (Routing Configuration)** auf **Bearbeiten (Edit)**.
- 6 Geben Sie eine neue Gebietsschema-ID ein.

---

**Wichtig** Die Gebietsschema-ID muss das UUID-Format aufweisen. Zum Beispiel: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, wobei jedes X durch Ziffern des Hexadezimalsystems (0-F) ersetzt wird.

---


# Konfigurieren der Gebietsschema-ID auf einem Host oder Cluster

Wenn „Lokaler Ausgang“ beim Erstellen eines globalen logischen Routers aktiviert ist, werden Routen nur dann an Hosts gesendet, wenn die Gebietsschema-ID des Hosts mit der Gebietsschema-ID übereinstimmt, die der Route zugeordnet ist. Sie können Routen einzeln an Hosts senden, indem Sie die Gebietsschema-ID in einem Cluster von Hosts oder in einem Host konfigurieren.

## Voraussetzungen

Der globale logische (Distributed) Router, der Routing für die Hosts oder Cluster ausführt, muss mit aktiviertem lokalen Ausgang erstellt worden sein.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.
- 3 Klicken Sie auf die Registerkarte **Hostvorbereitung (Host Preparation)**.
- 4 Wählen Sie den NSX Manager aus, der die Hosts oder Cluster verwaltet, die konfiguriert werden müssen.
- 5 Wählen Sie den Host oder Cluster aus, den Sie ändern möchten, und erweitern Sie bei Bedarf die Cluster zum Anzeigen der Hosts.
- 6 Klicken Sie auf das Symbol **Einstellungen (Settings)** () und anschließend auf **Gebietsschema-ID ändern (Change Locale ID)**.
- 7 Geben Sie eine neue Gebietsschema-ID ein und klicken Sie auf **OK (OK.)**.

---

**Hinweis** Die Gebietsschema-ID muss das UUID-Format aufweisen. Zum Beispiel: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, wobei jedes X durch Ziffern des Hexadezimalsystems (0-F) ersetzt wird.

---

## Ergebnisse

Der globale Controller-Cluster sendet nur Routen, die mit dieser neuen Gebietsschema-ID übereinstimmen, an die Hosts.

## Nächste Schritte

Konfigurieren Sie eine statische Route unter Angabe einer angegebenen Gebietsschema-ID.

Die logische Firewall bietet Sicherheitsmechanismen für dynamische virtuelle Datacenter und besteht aus zwei Komponenten für verschiedene Nutzungsszenarien von Bereitstellungen. Die verteilte Firewall konzentriert sich auf die horizontalen Zugriffssteuerungen und Edge Firewall konzentriert sich auf die Erzwingung des vertikalen Datenverkehrs auf der Mandanten- oder Datacenter-Ebene. Zusammen erfüllen diese Komponenten die End-to-End-Firewallanforderungen virtueller Datacenter. Sie können diese Technologien wahlweise entweder einzeln oder zusammen bereitstellen.

Dieses Kapitel enthält die folgenden Themen:

- [verteilte Firewall](#)
- [Edge-Firewall](#)
- [Arbeiten mit Firewallregelabschnitten](#)
- [Arbeiten mit Firewallregeln](#)
- [Firewallprotokolle](#)

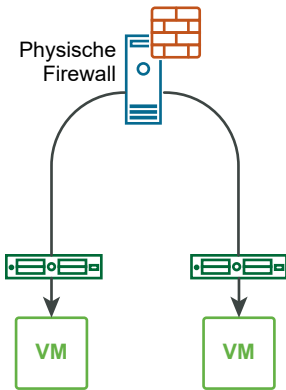
## verteilte Firewall

Eine verteilte Firewall (Distributed Firewall, DFW) wird im Kernel als VIB-Paket auf allen ESXi-Host-Clustern ausgeführt, die für NSX vorbereitet sind. Bei der Host-Vorbereitung wird die DFW automatisch auf den ESXi-Host-Clustern aktiviert.

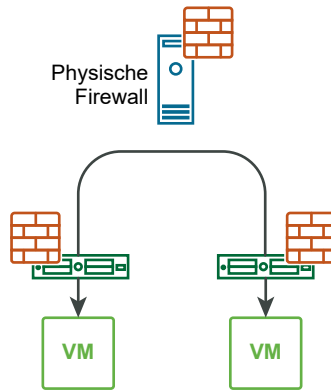
Die grundlegenden Einschränkungen der traditionellen am Perimeter ausgerichteten Sicherheitsarchitektur wirken sich sowohl auf die Sicherheitshaltung als auch auf die Skalierbarkeit der Anwendungen in modernen Datacentern aus. Beispielsweise entsteht bei durch physische Firewalls verursachten Engpässen beim Datenverkehrs im Perimeter des Netzwerks eine zusätzliche Latenz für bestimmte Anwendungen.

Die DFW ergänzt und verbessert Ihre physische Sicherheit, indem unnötige Engpässe aus den physischen Firewalls entfernt werden und die Menge des Datenverkehrs im Netzwerk reduziert wird. Der abgelehnte Datenverkehr wird blockiert, bevor er den ESXi-Host verlässt. Es ist nicht erforderlich, dass der Datenverkehr das Netzwerk durchläuft. Er muss lediglich durch die physische Firewall am Perimeter angehalten werden. Datenverkehr, der für eine andere VM auf demselben Host oder einem anderen Host bestimmt ist, muss das Netzwerk nicht bis zur physischen Firewall durchlaufen und dann wieder zur Ziel-VM zurückkehren. Der Datenverkehr wird auf der ESXi-Ebene überprüft und an die Ziel-VM übermittelt.

Sicherheit ohne NSX DFW



Sicherheit mit NSX DFW



Die NSX-DFW ist eine statusbehaftete Firewall, die den Status der aktiven Verbindungen überwacht und mit diesen Informationen ermittelt, welche Netzwerkpakete die Firewall passieren dürfen. Die DFW wird im Hypervisor implementiert und pro vNIC auf virtuelle Maschinen angewendet. Das heißt, dass die Firewallregeln am vNIC jeder virtuellen Maschine erzwungen werden. Die Überprüfung des Datenverkehrs erfolgt in dem Moment am vNIC einer VM, in dem der Datenverkehr die VM verlässt und den virtuellen Switch (Egress) erreicht. Eine Inspektion erfolgt auch in dem Moment bei der vNIC, in dem der Datenverkehr den Switch verlässt, aber bevor er die VM (Ingress) erreicht.

Virtuelle NSX Manager-Appliance, NSX Controller-VMs und NSX Edge-Dienst-Gateways werden automatisch von der DFW ausgeschlossen. Wenn eine VM keinen DFW-Dienst benötigt, können Sie sie manuell zur Ausschlussliste hinzufügen.

Da die DFW im Kernel eines jeden ESXi-Hosts verteilt wird, wird die Firewall-Kapazität horizontal skaliert, wenn Sie Hosts zu den Clustern hinzufügen. Durch das Hinzufügen weiterer Hosts wird die DFW-Kapazität erhöht. Wenn Ihre Infrastruktur erweitert wird und Sie mehr Server für die Verwaltung Ihrer ständig wachsenden Anzahl von VMs kaufen, steigt die DFW-Kapazität.

## DFW-Richtlinienregeln

Die DFW-Richtlinienregeln werden mithilfe des vSphere Web Client erstellt und in der NSX Manager-Datenbank gespeichert. Mit DFW können Sie Ethernet-Regeln (L2-Regeln) und allgemeine Regeln (L3-bis-L7-Regeln) erstellen. Die Regeln werden von NSX Manager auf ESXi-Cluster und dann von ESXi-Host auf VM-Ebene veröffentlicht. Alle ESXi-Hosts im selben Cluster haben dieselben DFW-Richtlinienregeln.

Eine verteilte Firewall-Instanz auf einem ESXi-Host enthält die folgenden beiden Tabellen:

- Regeltabelle zum Speichern aller Sicherheitsrichtlinienregeln.
- Verbindungs-Tracker-Tabelle für das Zwischenspeichern von Flow-Einträgen für Regeln mit einer Aktion „Zulassen“.

Die DFW-Regeln werden in einer Reihenfolge von oben nach unten ausgeführt. Datenverkehr, der eine Firewall passieren muss, wird als Erstes mit einer Liste von Firewallregeln abgeglichen. Jedes Paket wird anhand der obersten Regel in der Regeltabelle überprüft, bevor zu den nächsten Regeln in der Tabelle nach unten übergegangen wird. Die erste Regel in der Tabelle, die den Datenverkehrsparametern entspricht, wird erzwungen. Die letzte Regel in der Tabelle ist die DFW-Standardregel. Pakete, die keiner Regel über der Standardregel entsprechen, werden durch die Standardregel erzwungen.

Jede VM verfügt über eigene Regeln und einen eigenen Kontext für Firewall-Richtlinien. Während vMotion wird der DFW-Kontext (Regeltabelle, Verbindungs-Tracker-Tabelle) beim Verschieben von VMs von einem ESXi-Host auf einen anderen Host mit der VM verschoben. Darüber hinaus bleiben alle aktiven Verbindungen während vMotion intakt. Mit anderen Worten: die DFW-Sicherheitsrichtlinie ist vom VM-Standort unabhängig.

## Micro-Segmentierung mit DFW

Durch die Mikro-Segmentierung wird die Sicherheit des Datacenter-Netzwerks erhöht, indem jede verwandte Gruppe von virtuellen Maschinen auf ein eindeutiges logisches Netzwerksegment isoliert wird. Die Mikro-Segmentierung ermöglicht es dem Administrator, Datenverkehr von einem logischen Segment des Datacenters zu einem anderen logischen Segment (Ost-West-Datenverkehr) zu durchlaufen. Daher schränkt eine Firewall beim Ost-West-Datenverkehrs die Fähigkeit eines Angreifers ein, sich seitlich im Datacenter zu bewegen.

Die Mikro-Segmentierung wird durch die Distributed Firewall (DFW)-Komponente von NSX ermöglicht. Die Leistung der DFW besteht darin, dass die Netzwerktopologie kein Hindernis mehr für das Erzwingen der Sicherheit darstellt. Derselbe Grad der Zugriffssteuerung für den Datenverkehr kann mit jeder Art von Netzwerktopologie erreicht werden.

Ein detailliertes Beispiel für einen Anwendungsfall für die Mikro-Segmentierung finden Sie im Abschnitt „Micro-Segmentation with NSX DFW and Implementation“ (Mikro-Segmentierung mit NSX DFW und Implementierung) im *NSX Network Virtualization Design Guide (Design-Handbuch für die NSX-Netzwerkvirtualisierung)* unter <https://communities.vmware.com/docs/DOC-27683>.

## DFW-Richtlinienregeln basierend auf der Benutzeridentität

Die verteilte Firewall kann außerdem beim Erstellen identitätsbasierter Regeln helfen. Sicherheits-Administratoren können die Zugriffssteuerung anhand der Benutzeridentität und der Gruppenmitgliedschaften des Benutzers gemäß der Definition im Active Directory des Unternehmens erzwingen. Beispielsweise können identitätsbasierte Distributed Firewall-Regeln in den folgenden Szenarien verwendet werden:

- Benutzer möchten mit einem Laptop oder einem Mobilgerät auf virtuelle Anwendungen zugreifen, wobei die Benutzerauthentifizierung über AD erfolgt
- Benutzer möchten über die VDI-Infrastruktur auf virtuelle Anwendungen zugreifen, auf denen die virtuellen Maschinen ein Microsoft Windows-Betriebssystem verwenden.

Weitere Informationen zu benutzerbasierten DFW-Regeln für Active Directory finden Sie unter [Kapitel 11 Überblick über die identitätsbasierte Firewall \(IDFW\)](#).

## Sitzungs-Timer

Sitzungs-Timer können für TCP-, UDP- und ICMP-Sitzungen konfiguriert werden.

Mithilfe von Sitzungs-Timern wird definiert, wie lange eine Sitzung nach der Inaktivität an der Firewall beibehalten wird. Wenn die Sitzungszeitüberschreitung für das Protokoll abläuft, wird die Sitzung geschlossen.

An der Firewall können verschiedene Zeitüberschreitungen für TCP-, UDP- und ICMP-Sitzungen angegeben werden, die auf eine benutzerdefinierte Teilmenge virtueller Maschinen oder vNICs angewendet werden. Standardmäßig werden virtuelle Maschinen oder vNICs, die nicht im benutzerdefinierten Timer enthalten sind, in den globalen Sitzungs-Timer einbezogen. All diese Zeitüberschreitungen sind global. Das heißt, sie gelten für alle Sitzungen des jeweiligen Typs auf dem Host.

Die Standardwerte für die Sitzung können je nach Netzwerkanforderungen geändert werden. Hinweis: Wenn Sie einen zu niedrigen Wert festlegen, können häufige Zeitüberschreitungen die Folge sein. Die Festlegung zu hoher Werte kann dagegen die Fehlererkennung verzögern.

### Erstellen eines Sitzungs-Timers

Mithilfe von Sitzungs-Timern wird definiert, wie lange eine Sitzung nach Inaktivität in der Sitzung an der Firewall beibehalten wird.

An der Firewall können Sie Zeitüberschreitungen für TCP-, UDP- und ICMP-Sitzungen für einen Satz benutzerdefinierter VMs oder vNICs definieren. Der Standard-Timer ist global, d. h., er gilt für alle Firewall-geschützten virtuellen Maschinen.

#### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Firewall**.
- 2 Vergewissern Sie sich, dass Sie sich auf der Registerkarte **Einstellungen (Settings)** befinden. Wenn mehrere NSX Manager verfügbar sind, wählen Sie einen in der Dropdown-Liste aus.
- 3 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).  
Das Dialogfeld „Zeitüberschreitungskonfiguration hinzufügen“ mit den Standardwerten wird angezeigt.
- 4 Geben Sie einen **Namen (name)** (erforderlich) und eine **Beschreibung (description)** (optional) für den Sitzungs-Timer ein.
- 5 Wählen Sie das Protokoll aus. Übernehmen Sie die Standardwerte, oder geben Sie eigene Werte ein.

TCP-Variablen	Beschreibung
Erstes Paket	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten Pakets. Die Standardeinstellung ist 120 Sekunden.
Geöffnet	Der Zeitüberschreitungswert für die Verbindung nach dem Übertragen des zweiten Pakets. Die Standardeinstellung ist 30 Sekunden.
Hergestellt	Der Zeitüberschreitungswert für die Verbindung, nachdem die Verbindung vollständig hergestellt wurde.

TCP-Variablen	Beschreibung
Wird geschlossen	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten FIN. Die Standardeinstellung ist 120 Sekunden.
Fin Warten	Der Zeitüberschreitungswert für die Verbindung, nachdem beide FINs ausgetauscht wurden und die Verbindung geschlossen ist. Die Standardeinstellung ist 45 Sekunden.
Geschlossen	Der Zeitüberschreitungswert für die Verbindung, nachdem ein Endpoint ein RST gesendet hat. Die Standardeinstellung ist 20 Sekunden.
UDP-Variablen	Beschreibung
Erstes Paket	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten Pakets. Dies ist die initiale Zeitüberschreitung für den neuen UDP-Fluss. Die Standardeinstellung ist 60 Sekunden.
Einzel	Der Zeitüberschreitungswert für die Verbindung, wenn der Quellhost mehrere Pakete sendet und der Zielhost kein Paket zurückgesendet hat. Die Standardeinstellung ist 30 Sekunden.
Mehrere	Der Zeitüberschreitungswert für die Verbindung, wenn beide Hosts Pakete gesendet haben. Die Standardeinstellung ist 60 Sekunden.
ICMP-Variablen	Beschreibung
Erstes Paket	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten Pakets. Dies ist die initiale Zeitüberschreitung für den neuen ICMP-Fluss. Die Standardeinstellung ist 20 Sekunden.
Fehlerantwort	Der Zeitüberschreitungswert für die Verbindung nach dem Zurückgeben eines ICMP-Fehlers in Reaktion auf ein ICMP-Paket. Die Standardeinstellung ist 10 Sekunden.

- Wählen Sie den Objekttyp **vNIC** oder **VM** aus.

Die Liste „Verfügbare Objekte“ wird automatisch gefüllt.

- Wählen Sie ein oder mehrere Objekte aus und klicken Sie auf den Pfeil, um sie in die Spalte **Ausgewählte Objekte (Selected Objects)** zu verschieben.
- Klicken Sie auf **OK**.

## Ergebnisse

Es wurde ein Timer erstellt, der für einen Satz benutzerdefinierter Hosts gilt.

## Bearbeiten eines Sitzungs-Timers

Konfigurieren Sie Zeitüberschreitungsparameter für TCP-, UDP- und ICMP-Protokolle.

Nach dem Erstellen eines Sitzungs-Timers kann dieser bei Bedarf geändert werden. Der Standard-Sitzungs-Timer kann ebenfalls bearbeitet werden.

## Verfahren

- Navigieren Sie in vSphere Web Client zu **Networking & Security > Firewall (Networking & Security --> Firewall)**.
- Vergewissern Sie sich, dass Sie sich auf der Registerkarte **Einstellungen (Settings)** befinden. Wenn mehrere NSX Manager verfügbar sind, wählen Sie einen in der Dropdown-Liste aus.

- 3 Wählen Sie den zu bearbeitenden Timer aus. Beachten Sie, dass die Standard-Timerwerte ebenfalls bearbeitet werden können. Klicken Sie auf das **Stift (pencil)**-Symbol.

Das Dialogfeld „Zeitüberschreitungskonfiguration bearbeiten“ mit den Standardwerten wird angezeigt.

- 4 Geben Sie einen **Namen (name)** (erforderlich) und eine **Beschreibung (description)** (optional) für den Sitzungs-Timer ein.
- 5 Wählen Sie das Protokoll aus. Bearbeiten Sie die Standardwerte, die Sie ändern möchten.

TCP-Variablen	Beschreibung
Erstes Paket	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten Pakets. Die Standardeinstellung ist 120 Sekunden.
Geöffnet	Der Zeitüberschreitungswert für die Verbindung nach dem Übertragen des zweiten Pakets. Die Standardeinstellung ist 30 Sekunden.
Hergestellt	Der Zeitüberschreitungswert für die Verbindung, nachdem die Verbindung vollständig hergestellt wurde.
Wird geschlossen	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten FIN. Die Standardeinstellung ist 120 Sekunden.
Fin Warten	Der Zeitüberschreitungswert für die Verbindung, nachdem beide FINs ausgetauscht wurden und die Verbindung geschlossen ist. Die Standardeinstellung ist 45 Sekunden.
Geschlossen	Der Zeitüberschreitungswert für die Verbindung, nachdem ein Endpoint ein RST gesendet hat. Die Standardeinstellung ist 20 Sekunden.

UDP-Variablen	Beschreibung
Erstes Paket	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten Pakets. Dies ist die initiale Zeitüberschreitung für den neuen UDP-Fluss. Die Standardeinstellung ist 60 Sekunden.
Einzel	Der Zeitüberschreitungswert für die Verbindung, wenn der Quellhost mehrere Pakete sendet und der Zielhost kein Paket zurückgesendet hat. Die Standardeinstellung ist 30 Sekunden.
Mehrere	Der Zeitüberschreitungswert für die Verbindung, wenn beide Hosts Pakete gesendet haben. Die Standardeinstellung ist 60 Sekunden.

ICMP-Variablen	Beschreibung
Erstes Paket	Der Zeitüberschreitungswert für die Verbindung nach dem Senden des ersten Pakets. Dies ist die initiale Zeitüberschreitung für den neuen ICMP-Fluss. Die Standardeinstellung ist 20 Sekunden.
Fehlerantwort	Der Zeitüberschreitungswert für die Verbindung nach dem Zurückgeben eines ICMP-Fehlers in Reaktion auf ein ICMP-Paket. Die Standardeinstellung ist 10 Sekunden.

- 6 Wählen Sie den Objekttyp **vNIC** oder **VM** aus.  
Die Liste „Verfügbare Objekte“ wird automatisch gefüllt.
- 7 Wählen Sie ein oder mehrere Objekte aus und klicken Sie auf den Pfeil, um sie in die Spalte **Ausgewählte Objekte (Selected Objects)** zu verschieben.
- 8 Klicken Sie auf **OK**.

## IP-Erkennung für virtuelle Maschinen

VMware Tools wird auf einer virtuellen Maschine ausgeführt und bietet mehrere Dienste. Ein für die verteilte Firewall maßgeblicher Dienst ist das Zuordnen einer virtuellen Maschine und deren vNICs zu IP-Adressen. Wenn in Versionen vor NSX 6.2 VMware Tools nicht auf einer virtuellen Maschine installiert war, war die IP-Adresse nicht erlernt. Sie können in NSX 6.2 und höher Cluster zum Erkennen von VM-IP-Adressen mittels DHCP-Snooping, ARP-Snooping oder beider Methoden konfigurieren. Somit kann NSX die IP-Adresse erkennen, wenn VMware Tools nicht auf der virtuellen Maschine installiert ist. Wenn VMware Tools installiert ist, funktioniert es in Verbindung mit DHCP- und ARP-Snooping.

VMware empfiehlt, dass Sie VMware Tools auf jeder virtuellen Maschine in Ihrer Umgebung installieren. Zusätzlich zur Bereitstellung der IP-Adresse der virtuellen Maschinen für vCenter bietet VMware Tools viele weitere Funktionen:

- Kopieren und Einfügen zwischen einer virtuellen Maschine und dem Host oder dem Client-Desktop
- Synchronisieren der Uhrzeit mit dem Hostbetriebssystem
- Ermöglichen des Herunterfahrens oder des Neustarts einer VM von vCenter aus
- Erfassen von Netzwerk-, Festplatten- und Arbeitsspeichernutzungsdaten der virtuellen Maschine und Weiterleiten von diesen an den Host
- Ermitteln der Verfügbarkeit einer virtuellen Maschine durch Senden und Erfassen des Taktsignals


Beachten Sie, dass zwei vNICs für eine virtuelle Maschine im selben Netzwerk nicht unterstützt werden. Dies kann zu unerwarteten Ergebnissen bei der Frage führen, welcher Datenverkehr blockiert oder zugelassen wird.

Bei virtuellen Maschinen, auf denen VMware Tools nicht installiert ist, erlernt NSX die IP-Adresse mittels ARP- oder DHCP-Snooping, sofern auf dem Cluster der virtuellen Maschine ARP- und DHCP-Snooping aktiviert sind.

## Ändern des IP-Erkennungstyps

Die IP-Adresse einer virtuellen Maschine kann durch VMware Tools, das auf der VM installiert ist, oder durch DHCP-Snooping und ARP-Snooping, die auf dem Host-Cluster aktiviert sind, erkannt werden. Diese IP-Erkennungsmethoden können zusammen in derselben NSX-Installation verwendet werden.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Installation > Hostvorbereitung (Host Preparation)**.
- 2 Klicken Sie auf den Cluster, den Sie ändern möchten, und dann auf **Aktionen (Actions)** (  ) > **IP-Erkennungstyp ändern (Change IP Detection Type)**.
- 3 Wählen Sie die gewünschten Erkennungstypen aus und klicken Sie auf **OK**.

### Nächste Schritte

Konfigurieren Sie SpoofGuard.

Konfigurieren Sie die Standard-Firewallregel.

## Ausschließen von virtuellen Maschinen vom Schutz durch die Firewall

Sie können virtuelle Maschinen vom Schutz durch die verteilte Firewall von NSX ausschließen.

NSX Manager, NSX Controller und NSX Edge-VMs werden automatisch vom Schutz der Verteilten Firewall von NSX ausgeschlossen. Darüber hinaus wird empfohlen, dass Sie folgende Dienst-VMs in die Ausschlussliste aufnehmen, um freien Datenverkehr zu ermöglichen.

- vCenter Server. vCenter Server kann in einen Cluster verschoben werden, der von der Firewall geschützt wird, er muss jedoch bereits in der Ausschlussliste vorhanden sein, um Verbindungsprobleme zu vermeiden.

---

**Hinweis** vCenter Server muss unbedingt der Ausschlussliste hinzugefügt werden, bevor die Standardregel „allow any any“ von „Zulassen“ in „Blockieren“ geändert wird. Wird dies nicht durchgeführt, wird der Zugriff auf vCenter Server blockiert, wenn eine Regel „Alle verweigern“ erstellt (oder die Standardregel zum Blockieren von Aktionen geändert) wird. Ist dies der Fall, setzen Sie die DFW auf die standardmäßige Firewallregel zurück, indem Sie den folgenden API-Befehl ausführen: `https://NSX_Manager_IP/api/4.0/firewall/globalroot-0/config`. Die Anforderung muss den Status 204 zurückgeben. Mit dieser Option wird die Standardrichtlinie (mit der Standardregel „Zulassen“) für die DFW wiederhergestellt und der Zugriff auf vCenter Server und vSphere Web Client wieder ermöglicht.

---

- Partner-Dienst-VMs.
- Virtuelle Maschinen, die den Promiscuous-Modus erfordern. Werden diese virtuellen Maschinen durch die verteilte Firewall von NSX geschützt, so wirkt sich das nachteilig auf ihre Leistung aus.
- SQL-Server, der von Ihrem Windows-basierten vCenter genutzt wird.
- vCenter-Webserver, wenn Sie diesen getrennt betreiben.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security**.
- 2 Klicken Sie in **Networking & Security (Networking & Security Inventory)** auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und dann auf die Registerkarte **Ausschlussliste (Exclusion List)**.
- 5 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 6 Wählen Sie die auszuschließenden virtuellen Maschinen aus, und klicken Sie auf **Hinzufügen (Add)**.
- 7 Klicken Sie auf **OK**.

## Ergebnisse

Wenn eine virtuelle Maschine über mehrere vNICs verfügt, werden alle vom Schutz ausgeschlossen. Wenn Sie vNICs zu einer virtuellen Maschine hinzufügen möchten, nachdem diese in die Ausschlussliste aufgenommen worden ist, dann wird die Firewall automatisch auf den neu hinzugefügten vNICs bereitgestellt. Um diese vNICs vom Firewallschutz auszuschließen, müssen Sie die virtuelle Maschine aus der Ausschlussliste entfernen und erneut hinzufügen. Eine weitere Umgehung wäre, die virtuelle Maschine ab- und wieder einzuschalten, die erste Option führt allerdings zu weniger Unterbrechungen.

## Anzeigen von Firewall-CPU- und Arbeitsspeicherereignissen

Wenn ein Cluster für die Netzwerkvirtualisierung vorbereitet wird, wird das Firewallmodul auf allen Hosts dieses Clusters installiert. Dieses Modul weist drei Heaps zu, ein Modul-Heap für Modulparameter, ein Regel-Heap für Regeln, Container und Filter sowie ein Zustands-Heap für Datenverkehrsflows. Die Zuweisung der Heap-Größe wird durch den verfügbaren physischen Hostarbeitsspeicher bestimmt. Je nach Anzahl der Regeln, Container-Sätze und den Verbindungen kann sich die Heap-Größe mit der Zeit vergrößern oder verkleinern. Das auf dem Hypervisor ausgeführte Firewallmodul verwendet auch die Host-CPU für die Paketverarbeitung.

Wenn Sie die Hostressourcenauslastung jederzeit feststellen können, können Sie so die Serverauslastung und Netzwerkdesigns besser organisieren.

Der standardmäßige CPU-Schwellenwert beträgt 100 und der Schwellenwert des Arbeitsspeichers 100. Sie können die standardmäßigen Schwellenwerte durch REST-API-Aufrufe ändern. Das Firewallmodul generiert Systemereignisse, wenn die Arbeitsspeicher- und CPU-Auslastung die Schwellenwerte überschreitet. Informationen zum Konfigurieren von standardmäßigen Schwellenwerten finden Sie unter „Arbeiten mit Arbeitsspeicher- und CPU-Schwellenwerten“ im *Handbuch für NSX API*.

## Verfahren

- 1 Klicken Sie im vSphere Web Client auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
- 2 Klicken Sie in der Spalte **Name** auf die IP-Adresse des entsprechenden NSX Manager.
- 3 Klicken Sie auf die Registerkarte **Überwachen (Monitor)** und anschließend auf **Ereignisse (System Events)**.

## Ressourcennutzung der Verteilten Firewall

Arbeitsspeicher wird von den internen Datenstrukturen der Verteilten Firewall in Anspruch genommen und kann für CPU, RAM und Verbindungen pro Sekunde konfiguriert werden.

Jeder ESXi-Host wird mit drei Schwellenwertparametern für die DFW-Ressourcennutzung konfiguriert: CPU, RAM und CPS (Connections per Second = Verbindungen pro Sekunde). Ein Alarm wird ausgelöst, wenn während eines Zeitraums von 200 Sekunden der jeweilige Schwellenwert 20 Mal aufeinanderfolgend überschritten wird. Eine Prüfung erfolgt alle 10 Sekunden.

100 Prozent CPU entspricht der gesamten auf dem Host verfügbaren CPU.

100 Prozent RAM entspricht dem für die verteilte Firewall („Gesamte Maximalgröße“) zugeteilten Arbeitsspeicher, der von der Gesamtmenge des auf dem Host installierten RAM abhängig ist.

**Tabelle 10-1. Gesamte Maximalgröße**

Physischer Arbeitsspeicher	Gesamte Maximalgröße (MB)
0 – 8 GB	160
8 GB – 32 GB	608
32 GB – 64 GB	992
64 GB – 96 GB	1920
96 GB – 128 GB	2944
128 GB	4222

Der Arbeitsspeicher wird von den internen Datenstrukturen der Verteilten Firewall verwendet. Dazu gehören Filter, Regeln, Container, Verbindungsstatus, ermittelte IP-Adressen und Drop Flow-Pakete. Diese Parameter können mithilfe des folgenden API-Aufrufs bearbeitet werden:

```
https://NSX-MGR-IP/api/4.0/firewall/stats/eventthresholds
```

Request body:

```
<eventThresholds>
 <cpu>
 <percentValue>100</percentValue>
 </cpu>
 <memory>
 <percentValue>100</percentValue>
 </memory>
 <connectionsPerSecond>
 <value>100000</value>
 </connectionsPerSecond>
</eventThresholds>
```

## Edge-Firewall

Edge-Firewall überwacht den Nord-Süd-Datenverkehr und bietet Sicherheitsfunktionen im Randbereich, einschließlich Firewall, NAT (Network Address Translation, Netzwerkadressenübersetzung) sowie Site-to-Site-IPSec und SSL VPN-Funktionen. Diese Lösung ist im VM-Formfaktor erhältlich und kann im Hochverfügbarkeitsmodus bereitgestellt werden.

Firewall-Support ist auf den logischen Router begrenzt. Es greifen nur die Regeln für Management- oder Uplink-Schnittstellen, die Regeln für interne Schnittstellen greifen jedoch nicht.

---

**Hinweis** NSX-V Edge ist anfällig für „Syn-Flood“-Angriffe, bei denen ein Angreifer die Tabelle für die Nachverfolgung des Firewallstatus durch massenhaftes Einfügen von SYN-Paketen blockiert. Ein solcher DOS/DDOS-Angriff führt zu einer Dienstunterbrechung für die Originalbenutzer. Edge implementiert zur Verteidigung gegen solche Syn-Flood-Angriffe eine Struktur zur Ermittlung fingierter TCP-Verbindungen und beendet diese ohne Inanspruchnahme von Ressourcen der Nachverfolgung des Firewallstatus. Diese Funktion ist standardmäßig deaktiviert. Zur Aktivierung dieser Funktion in einer risikobehafteten Umgebung legen Sie den REST-API-enableSynFloodProtection-Wert als Teil der globalen Firewallkonfiguration auf true fest.

---

Detaillierte Informationen über das Verhalten bei SynFloodProtection-Aktivierung auf einem NSX Edge finden Sie im VMware-Wissensdatenbankartikel unter <https://kb.vmware.com/s/article/54527>.

## Arbeiten mit NSX Edge-Firewallregeln

Sie können zu einem NSX Edge navigieren, um die auf ihn angewendeten Firewallregeln anzuzeigen.

Auf einen logischen Router angewendete Firewallregeln schützen nur Datenverkehr von Steuerungskomponenten zu und von der Steuerelement-VM des logischen Routers. Sie erzwingen keinen Datenebenenschutz. Um den Datenverkehr der Datenebene zu schützen, erstellen Sie logische Firewallregeln für Ost-West-Schutz oder Regeln auf der Ebene des NSX Edge Services Gateways für Nord-Süd-Schutz.


Die Regeln werden in der folgenden Reihenfolge angezeigt und erzwungen:

- 1 Vordefinierte Regeln für verteilte Firewalls, die auf den Edge angewendet werden.
  - Diese Regeln werden über die Firewall-Benutzeroberfläche definiert (**Netzwerk und Sicherheit > Sicherheit > Firewall**)
  - Diese Regeln werden im **schreibgeschützten** Modus in der Benutzeroberfläche der NSX Edge-Firewall angezeigt.
- 2 Interne Regeln, die den Fluss des Steuerungsdatenverkehrs für Edge-Dienste ermöglichen. Beispielsweise umfassen die internen Regeln die folgenden solcher „Auto-plumbed“-Regeln:
  - a SSL VPN-„Auto-plumbed“-Regel: Die Registerkarte „Edge-Firewall“ zeigt die SSL VPN-„Auto-plumbed“-Regel an, wenn Servereinstellungen konfiguriert sind und der SSL VPN-Dienst aktiviert ist.
  - b DNAT-„Auto-plumbed“-Regel: Die Registerkarte „Edge-NAT“ zeigt die DNAT-„Auto-plumbed“-Regel als Teil der Standard-SSL-VPN-Konfiguration an.
- 3 Benutzerdefinierte Regeln, die über die NSX Edge-Firewall-Benutzeroberfläche hinzugefügt werden.
- 4 Standardregel

## Bearbeiten der NSX Edge Firewall-Standardregel

Die standardmäßigen Firewalleinstellungen gelten für den Datenverkehr, der unter keine der benutzerdefinierten Firewallregeln fällt. Die standardmäßige Edge Firewall-Richtlinie blockiert den gesamten eingehenden Datenverkehr. Sie können die Standardaktion und die Protokolleinstellungen ändern.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > NSX Edges**.
- 2 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 3 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und klicken Sie anschließend auf **Firewall**.
- 4 Wählen Sie die **Standardregel (Default Rule)**, die als letzte Regel in der Firewalltabelle aufgelistet ist.
- 5 Zeigen Sie auf die Zelle **Aktion (Action)** der neuen Regel und klicken Sie auf .
  - a Klicken Sie auf **Akzeptieren (Accept)**, um den Datenverkehr zwischen der angegebenen Quelle und dem Ziel zuzulassen.
  - b Klicken Sie auf **Protokoll (Log)**, um alle Sitzungen, die unter diese Regel fallen, zu protokollieren.  
Das Aktivieren der Protokollierung kann die Leistung beeinträchtigen.
  - c Klicken Sie auf **OK**.
- 6 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Hinzufügen einer NSX Edge-Firewallregel

Die Registerkarte „Edge-Firewall“ zeigt die in der zentralisierten Firewall-Registerkarte erstellten Regeln im Modus „Nur Lesen“ an. Regeln, die Sie hier hinzufügen, werden nicht in der zentralisierten Firewall-Registerkarte angezeigt.

Sie können mehrere NSX Edge-Schnittstellen und/oder IP-Adressgruppen als Quelle und Ziel für Firewallregeln hinzufügen.

**Abbildung 10-1. Firewallregel für den Datenverkehr von einer NSX Edge-Schnittstelle zu einem HTTP-Server**

No.	Name	Type	Source	Destination	Service	Action
1	firewall	Internal	vse	any	any	Accept
2	Traffic to HTTP server	User	vnic-index-0:any	HTTP Address Group	For HTTP server	Accept
3	Default Rule	Default	any			Deny

**HTTP Address Group**

Value:  
10.20.222.34

**For HTTP server**

Value:  
TCP:8080

**Abbildung 10-2. Firewallregel für den ausgehenden Datenverkehr aller internen Schnittstellen (Subnetze auf mit internen Schnittstellen verbundenen Portgruppen) einer NSX Edge-Instanz zu einem HTTP-Server**

No.	Name	Type	Source	Destination	Service	Action
✓ 1	firewall	Internal	vse	any	any	Accept
✓ 2	Traffic to HTTP server	User	internal	HTTP Address Group	For HTTP server	Accept
✓ 3	Default Rule	Default	any			Deny

**HTTP Address Group**  
 Value:  
 10.20.222.34

**For HTTP server**  
 Value:  
 TCP:8080

**Hinweis** Wenn Sie als Quelle **Intern (internal)** auswählen, wird die Regel automatisch aktualisiert, wenn Sie weitere interne Schnittstellen konfigurieren.

**Abbildung 10-3. Firewallregel für den Datenverkehr, die SSH in einem m/c in einem internen Netzwerk zulässt**

No.	Name	Type	Source	Destination	Service	Action
✓ 1	firewall	Internal	vse	any	any	Accept
✓ 2	Traffic to internal network	User	any	VM in internal netw...	Internal VM	Accept
✓ 3	Default Rule	Default	any			Deny





**VM in internal network**  
 Value:  
 192.168.0.10

**Internal VM**  
 Value:  
 TCP:22

#### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > NSX Edges**.
- 2 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 3 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Firewall**.

#### 4 Führen Sie einen der folgenden Schritte aus.

Option	Beschreibung
<b>So fügen Sie eine Regel an einer bestimmten Stelle der Firewalltabelle ein</b>	<p>a Wählen Sie die gewünschte Regel aus.</p> <p>b Klicken Sie in der Spalte „Nr.“ auf  und wählen Sie <b>Oben hinzufügen (Add Above)</b> oder <b>Unten hinzufügen (Add Below)</b>.</p> <p>Die neue Regel wird unter der ausgewählten Regel eingefügt. Wenn die Firewalltabelle nur die systemdefinierte Regel enthält, wird die neue Regel über der Standardregel eingefügt.</p>
<b>So fügen Sie eine Regel durch Kopieren hinzu</b>	<p>a Wählen Sie die gewünschte Regel aus.</p> <p>b Klicken Sie auf das Symbol „Kopieren“ (.</p> <p>c Wählen Sie die gewünschte Regel aus.</p> <p>d Klicken Sie in der Spalte „Nr.“ auf  und wählen Sie <b>Oben einfügen (Paste Above)</b> oder <b>Unten einfügen (Paste Below)</b> aus.</p>
<b>So fügen Sie eine Regel an einer beliebigen Stelle der Firewalltabelle hinzu</b>	<p>a Klicken Sie auf das Symbol <b>Hinzufügen (Add)</b> (.</p> <p>Die neue Regel wird unter der ausgewählten Regel eingefügt. Wenn die Firewalltabelle nur die systemdefinierte Regel enthält, wird die neue Regel über der Standardregel eingefügt.</p>

Diese neue Regel ist standardmäßig aktiviert.

#### 5 Zeigen Sie auf die Zelle **Name** der neuen Regel und klicken Sie auf .

#### 6 Geben Sie einen Namen für die neue Regel ein.

#### 7 Zeigen Sie auf die Zelle **Quelle (Source)** der neuen Regel und klicken Sie auf oder .



Wenn Sie auf  geklickt haben, geben Sie eine IP-Adresse ein.

- a Wählen Sie im Dropdown-Menü ein Objekt aus und nehmen Sie anschließend die entsprechende Auswahl vor.

Wenn Sie **vNIC-Gruppe (vNIC Group)** und dann **VSE** wählen, gilt die Regel für den Datenverkehr, der von der NSX Edge-Instanz generiert wird. Wenn Sie **Intern (internal)** oder **Extern (external)** wählen, gilt die Regel für den Datenverkehr, der von einer internen oder Uplink-Schnittstelle der ausgewählten NSX Edge-Instanz kommt. Die Regel wird automatisch aktualisiert, wenn Sie weitere Schnittstellen konfigurieren. Beachten Sie, dass die Firewallregeln für interne Schnittstellen nicht für einen logischen Router gelten.

Wenn Sie **IP Set (IP Sets)** wählen, können Sie eine neue IP-Adressgruppe erstellen. Sobald Sie die neue Gruppe erstellt haben, wird sie automatisch zur Spalte „Quelle“ hinzugefügt. Weitere Informationen zum Erstellen eines IP Set finden Sie unter [Erstellen einer IP-Adressgruppe](#).





- b Klicken Sie auf **OK**.

- 8 Zeigen Sie auf die Zelle **Ziel (Destination)** der neuen Regel und klicken Sie auf  oder .
- a Wählen Sie im Dropdown-Menü ein Objekt aus und nehmen Sie anschließend die entsprechende Auswahl vor.


Wenn Sie **vNIC-Gruppe (vNIC Group)** und dann **VSE** wählen, gilt die Regel für den Datenverkehr, der von der NSX Edge-Instanz generiert wird. Wenn Sie **Intern (internal)** oder **Extern (external)** wählen, gilt die Regel für den Datenverkehr, der zu einer internen oder Uplink-Schnittstelle der ausgewählten NSX Edge-Instanz kommt. Die Regel wird automatisch aktualisiert, wenn Sie weitere Schnittstellen konfigurieren. Beachten Sie, dass die Firewallregeln für interne Schnittstellen nicht für einen logischen Router gelten.

Wenn Sie **IP Set (IP Sets)** wählen, können Sie eine neue IP-Adressgruppe erstellen. Sobald Sie die neue Gruppe erstellt haben, wird sie automatisch zur Spalte „Quelle“ hinzugefügt. Weitere Informationen zum Erstellen eines IP Set finden Sie unter [Erstellen einer IP-Adressgruppe](#).

- b Klicken Sie auf **OK**.

- 9 Zeigen Sie auf die Zelle **Dienst (Service)** der neuen Regel und klicken Sie auf  oder .
- Wenn Sie auf  geklickt haben, wählen Sie einen Dienst aus. Zum Erstellen eines neuen Dienstes oder einer neuen Dienstgruppe klicken Sie auf **Neu (New)**. Sobald Sie den neuen Dienst erstellt haben, wird er automatisch zur Spalte „Dienst“ hinzugefügt. Weitere Informationen zum Erstellen eines neuen Diensts finden Sie unter [Erstellen eines Diensts](#).
  - Wenn Sie auf  geklickt haben, wählen Sie ein Protokoll aus. Sie können den Quellport angeben, indem Sie neben „Erweiterte Optionen“ auf den Pfeil klicken. Es wird empfohlen, ab Version 5.1 den Quellport nicht anzugeben. Sie können stattdessen einen Dienst für eine Protokoll-Port-Kombination erstellen.

**Hinweis** NSX Edge unterstützt nur Dienste, die mit L3-Protokollen definiert sind.



- 10 Zeigen Sie auf die Zelle **Aktion (Action)** der neuen Regel und klicken Sie auf . Treffen Sie eine entsprechende Auswahl, wie in der nachfolgenden Tabelle beschrieben, und klicken Sie auf **OK**.


Ausgewählte Aktion	Ergebnis
<b>Zulassen</b>	Lässt Datenverkehr zwischen der angegebenen Quelle und dem Ziel zu.
<b>Blockieren</b>	Blockiert den Datenverkehr zwischen der angegebenen Quelle und dem Ziel.
<b>Ablehnen</b>	Versendet Ablehnungsmeldungen für nicht angenommene Pakete. RST-Pakete werden für TCP-Pakete gesendet. ICMP-unerreichbare (administrativ eingeschränkte) Pakete werden für andere Pakete gesendet.
<b>Protokoll</b>	Protokolliert alle Sitzungen, auf die diese Regel zutrifft. Das Aktivieren der Protokollierung kann die Leistung beeinträchtigen.
<b>Nicht protokollieren</b>	Protokolliert keine Sitzungen.
<b>Anmerkungen</b>	Geben Sie bei Bedarf Kommentare ein.

Ausgewählte Aktion	Ergebnis
<b>Erweiterte Optionen &gt; Abgleich mit Übersetzt</b>	Wendet die Regel auf die übersetzten IP-Adressen und Dienste für eine NAT-Regel an
<b>Regelrichtung aktivieren</b>	Gibt an, ob es sich um eine ein- oder ausgehende Regel handelt. Es wird nicht empfohlen, die Richtung für Firewallregeln anzugeben.

- 11 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**, um die neue Regel für die NSX Edge-Instanz zu veröffentlichen.

### Nächste Schritte

- Deaktivieren Sie eine Regel durch Klicken auf  neben der Regelnummer in der Spalte **Nr. (No.)**.
- Blenden Sie erstellte Regeln oder Vorab-Regeln (auf der zentralisierten Firewall-Registerkarte hinzugefügte Regeln) aus, indem Sie auf **Erstellte Regeln ausblenden (Hide Generated rules)** oder auf **Vorab-Regeln ausblenden (Hide Pre rules)** klicken.
- Zeigen Sie weitere Spalten in der Regeltabelle an, indem Sie auf  klicken und die entsprechenden Spalten auswählen.

Spaltenname	Angezeigte Informationen
Regel-Tag	Eindeutige, systemgenerierte ID für jede Regel
Protokoll	Datenverkehr für diese Regel wird protokolliert bzw. nicht protokolliert
Statistik	Durch Klicken auf  wird der von dieser Regel betroffene Datenverkehr angezeigt (Anzahl der Sitzungen, Datenverkehrspakete und Größe)
Anmerkungen	Anmerkungen zur Regel

- Suchen Sie nach Regeln, indem Sie Text in das Feld „Suche“ eingeben.

## Bearbeiten einer NSX Edge-Firewallregel

Sie können nur die benutzerdefinierten Edge-Firewallregeln bearbeiten und nur begrenzte Änderungen an der vom System generierten Standard-Firewallregel vornehmen.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > NSX Edges**.
- 2 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 3 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Firewall**.

- 4 Wählen Sie die zu bearbeitende Regel aus.

---

**Hinweis** Die folgenden Regeltypen können in der Benutzeroberfläche der NSX Edge-Firewall nicht bearbeitet werden:

- Interne Regeln (beispielsweise Auto-plumbed-Regeln, die den Fluss des Steuerungsdatenverkehrs für Edge-Dienste ermöglichen.)
  - Vordefinierte Regeln für verteilte Firewalls, die auf das Edge angewendet werden. Diese Firewallregeln werden in der Firewall-Benutzeroberfläche definiert (**Netzwerk und Sicherheit > Sicherheit > Firewall**).
- 

- 5 Nehmen Sie die Änderungen vor, und klicken Sie auf **OK**.
- 6 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Ändern der Priorität einer NSX Edge-Firewallregel

Sie können die Reihenfolge der auf der Registerkarte „Edge Firewall“ hinzugefügten benutzerdefinierten Firewallregeln ändern, um den über die NSX Edge-Instanz fließenden Datenverkehr anzupassen. Angenommen, Sie haben eine Regel erstellt, die Load-Balancer-Datenverkehr zulässt. Sie können nun eine Regel hinzufügen, die Load-Balancer-Datenverkehr für eine bestimmte IP-Adressengruppe unterbindet, und diese Regel über die Regel für das Zulassen des Load-Balancer-Datenverkehrs stellen.



### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > NSX Edges**.
- 2 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 3 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Firewall**.
- 4 Wählen Sie die Regel aus, für die Sie die Priorität ändern möchten.

---

**Hinweis** Sie können die Priorität weder für automatisch generierte Regeln noch für die Standardregel ändern.

---

- 5 Klicken Sie auf das Symbol **Nach oben verschieben (Move Up)** () oder **Nach unten verschieben (Move Down)** (.
- 6 Klicken Sie auf **OK**.
- 7 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Löschen einer NSX Edge-Firewallregel

Sie können eine benutzerdefinierte Firewallregel, die auf der NSX Edge-Firewall-Registerkarte hinzugefügt worden ist, löschen. Auf der zentralisierten Firewall-Registerkarte hinzugefügte Regeln können hier nicht gelöscht werden.

## Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > NSX Edges**.
- 2 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 3 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Firewall**.
- 4 Wählen Sie die zu löschende Regel aus.

---

**Hinweis** Sie können weder automatisch generierte Regeln noch die Standardregel löschen.

---

- 5 Klicken Sie auf das Symbol **Löschen (Delete)** (✖).

## Verwalten von NAT-Regeln

NSX Edge bietet den Dienst „Network Address Translation“ (NAT), der einem Computer oder einer Gruppe von Computern innerhalb eines privaten Netzwerks eine öffentliche Adresse zuweist. Mithilfe dieser Technologie kann die Anzahl öffentlicher IP-Adressen verringert werden, die eine Organisation oder ein Unternehmen verwenden muss. Dies hat wirtschaftliche Vorteile und dient der Sicherheit. Für den Zugriff auf Dienste, die auf virtuellen Maschinen mit privaten Adressen ausgeführt werden, müssen NAT-Regeln konfiguriert werden.

Die Konfiguration des NAT-Diensts gliedert sich in SNAT- (Source NAT, Quell-NAT) und DNAT-Regeln (Destination NAT, Ziel-NAT).

### Hinzufügen einer SNAT-Regel

Sie können eine Quell-NAT-Regel (SNAT) zum Ändern der Quell-IP-Adresse von einer öffentlichen in eine private IP-Adresse oder umgekehrt erstellen.

## Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > NSX Edges**.
- 2 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 3 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **NAT**.
- 4 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+) und wählen Sie **SNAT-Regel hinzufügen (Add SNAT Rule)**.
- 5 Wählen Sie die Schnittstelle aus, für die die Regel hinzugefügt werden soll.
- 6 Wählen Sie das erforderliche Protokoll aus.

- 7 Geben Sie die ursprüngliche (öffentliche) IP-Quelladresse in einem der folgenden Formate ein.

Format	Beispiel
IP-Adresse	192.0.2.0
IP-Adressbereich	192.0.2.0 – 192.0.2.24
IP-Adresse/-Subnetz	192.0.2.0/24
Beliebig	

- 8 Geben Sie den ursprünglichen Quellport bzw. -portbereich ein.

Format	Beispiel
Portnummer	80
Portbereich	80-85
Beliebig	

- 9 Geben Sie die IP-Zieladresse in einem der folgenden Formate ein.

Format	Beispiel
IP-Adresse	192.0.2.0
IP-Adressbereich	192.0.2.0 – 192.0.2.24
IP-Adresse/-Subnetz	192.0.2.0 /24
Beliebig	

- 10 Geben Sie den Zielport bzw. -portbereich ein.

Format	Beispiel
Portnummer	80
Portbereich	80-85
Beliebig	

- 11 Geben Sie die übersetzten Quell-IP-Adresse in einem der folgenden Formate ein.

Format	Beispiel
IP-Adresse	192.0.2.0
IP-Adressbereich	192.0.2.0 – 192.0.2.24
IP-Adresse/-Subnetz	192.0.2.0/24
Beliebig	

12 Geben Sie den übersetzten Port bzw. Portbereich ein.

Format	Beispiel
Portnummer	80
Portbereich	80-85
Beliebig	

13 Wählen Sie **Aktiviert (Enabled)**, um die Regel zu aktivieren.

14 Klicken Sie auf **Protokollierung aktivieren (Enable logging)**, um die Übersetzung der Adresse zu protokollieren.

15 Klicken Sie auf **OK**, um die Regel hinzuzufügen.

16 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

### Hinzufügen einer DNAT-Regel

Sie können eine Ziel-NAT-Regel (DNAT) zum Ändern der Ziel-IP-Adresse von einer öffentlichen in eine private IP-Adresse oder umgekehrt erstellen.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **NAT**.
- 5 Klicken Sie auf das Symbol **Hinzufügen (Add)** (  ) und wählen Sie **DNAT-Regel hinzufügen (Add DNAT Rule)**.
- 6 Wählen Sie die Schnittstelle aus, für die die DNAT-Regel gelten soll.
- 7 Wählen Sie das erforderliche Protokoll aus.
- 8 Geben Sie die Quell-IP-Adresse in einem der folgenden Formate ein.

Format	Beispiel
IP-Adresse	192.0.2.0
IP-Adressbereich	192.0.2.0 – 192.0.2.24
IP-Adresse/-Subnetz	192.0.2.0 /24
Beliebig	

- 9 Geben Sie den Quellport bzw. -portbereich ein.

Format	Beispiel
Portnummer	80
Portbereich	80-85
Beliebig	

- 10 Geben Sie die ursprüngliche (öffentliche) IP-Adresse in einem der folgenden Formate ein.

Format	Beispiel
IP-Adresse	192.0.2.0
IP-Adressbereich	192.0.2.0 – 192.0.2.24
IP-Adresse/-Subnetz	192.0.2.0 /24
Beliebig	

- 11 Geben Sie den ursprünglichen Port bzw. Portbereich ein.

Format	Beispiel
Portnummer	80
Portbereich	80-85
Beliebig	

- 12 Geben Sie die übersetzte IP-Adresse in einem der folgenden Formate ein.

Format	Beispiel
IP-Adresse	192.0.2.0
IP-Adressbereich	192.0.2.0 – 192.0.2.24
IP-Adresse/-Subnetz	192.0.2.0 /24
Beliebig	

- 13 Geben Sie den übersetzten Port bzw. Portbereich ein.

Format	Beispiel
Portnummer	80
Portbereich	80-85
Beliebig	

- 14 Wählen Sie **Aktiviert (Enabled)**, um die Regel zu aktivieren.

- 15 Wählen Sie **Protokollierung aktivieren (Enable logging)**, um die Übersetzung der Adresse zu protokollieren.

- 16 Klicken Sie auf **OK**, um die Regel hinzuzufügen.

17 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Arbeiten mit Firewallregelabschnitten

Sie können einen Abschnitt hinzufügen, um Firewallregeln zu trennen. Beispiel: Sie möchten möglicherweise die Regeln für den Verkauf und für die Technik in getrennten Abschnitten anordnen.

Sie können mehrere Firewallregelabschnitte für L2- und L3-Regeln erstellen.

Cross-vCenter NSX-Umgebungen können über mehrere universelle Abschnitte für Regeln verfügen. Mit mehreren universellen Abschnitten können Sie Regeln einfacher nach Mandant und Anwendung gliedern. Wenn Regeln innerhalb eines universellen Abschnitts geändert oder bearbeitet werden, erfolgt eine Synchronisierung mit dem sekundären NSX Manager nur für die verteilte Firewall-Regeln dieses Abschnitts. Sie müssen universelle Regeln auf dem primären NSX Manager verwalten, und Sie müssen dort den universellen Bereich erstellen, bevor Sie universelle Regeln hinzufügen können. Universelle Abschnitte werden sowohl auf dem primären wie auf dem sekundären NSX Manager immer oberhalb der lokalen Abschnitte aufgeführt.

Regeln außerhalb der universellen Abschnitte bleiben für die primären oder sekundären NSX Manager lokal, zu denen sie hinzugefügt wurden.

## Hinzufügen eines Firewallregelabschnitts

Sie können in der Firewalltabelle einen neuen Abschnitt hinzufügen, um Ihre Regeln zu organisieren oder um einen universellen Abschnitt zur Verwendung in Cross-vCenter NSX-Umgebungen zu erstellen.


### Voraussetzungen

Legen Sie den entsprechenden NSX Manager fest, bei dem Sie Änderungen durchführen möchten.


- In einer eigenständigen oder einzelnen vCenter NSX-Umgebung gibt es nur einen NSX Manager, sodass Sie keinen auswählen müssen.
- Universelle Objekte müssen vom primären NSX Manager verwaltet werden.
- Lokale Objekte einer NSX Manager-Instanz müssen von diesem NSX Manager aus verwaltet werden.
- In einer Cross-vCenter NSX-Umgebung, in der der erweiterte verknüpfte Modus nicht aktiviert ist, müssen Sie Konfigurationsänderungen von der vCenter-Instanz aus vornehmen, die mit dem NSX Manager verknüpft ist, den Sie ändern möchten.
- In einer Cross-vCenter NSX-Umgebung im erweiterten verknüpften Modus können Sie Konfigurationsänderungen an beliebigen NSX Manager-Instanzen von jeder verknüpften vCenter-Instanz aus vornehmen. Wählen Sie den geeigneten NSX Manager aus dem Dropdown-Menü „NSX Manager“ aus.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Firewall**.

- 2 Sofern mehr als ein NSX Manager verfügbar ist, wählen Sie einen aus. Sie müssen zum Hinzufügen eines universellen Abschnitts den primären NSX Manager auswählen.
- 3 Achten Sie beim Hinzufügen eines Abschnitts für L3-Regeln darauf, dass Sie sich auf der Registerkarte **Allgemein (General)** befinden. Klicken Sie auf die Registerkarte **Ethernet**, um einen Abschnitt für L2-Regeln hinzuzufügen.
- 4 Klicken Sie auf das Symbol **Abschnitt hinzufügen (Add Section)** ().
- 5 Geben Sie einen Namen für den Abschnitt ein und geben Sie die Position für den neuen Abschnitt an. Abschnittsnamen müssen in NSX Manager eindeutig sein.
- 6 (Optional) Wählen Sie zum Erstellen eines universellen Abschnitts **Diesen Abschnitt für globale Synchronisierung markieren (Mark this section for Universal Synchronization)** aus.
- 7 Klicken Sie auf **OK** und anschließend auf **Änderungen veröffentlichen (Publish Changes)**.

#### Nächste Schritte


Fügen Sie Regeln zum Abschnitt hinzu. Sie können den Namen eines Abschnitts bearbeiten. Klicken Sie dazu auf das Symbol **Abschnitt bearbeiten (Edit section)** () für den betreffenden Abschnitt.

## Zusammenführen von Firewallregelabschnitten

Sie können Abschnitte zusammenführen und die Regeln innerhalb dieser Abschnitte konsolidieren. Beachten Sie, dass Sie keine Abschnitte mit Service Composer oder mit Standardabschnitten zusammenführen können. Sie können in einer Cross-vCenter NSX-Umgebung keine Abschnitte mit einem globalen Abschnitt zusammenführen.

Die Zusammenführung und Konsolidierung einer komplexen Firewallkonfiguration vereinfacht die Wartung und Lesbarkeit.

#### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Firewall**.
- 2 Klicken Sie für den Abschnitt, den Sie zusammenführen möchten, auf das Symbol **Zusammenführen (Merge)** () und legen Sie fest, ob Sie diesen Abschnitt mit dem oberen oder unteren Abschnitt zusammenführen möchten.  
  
Die Regeln aus beiden Abschnitten werden zusammengeführt. Der neue Abschnitt behält den Namen des Bereichs bei, mit dem der andere Abschnitt zusammengeführt wurde.
- 3 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Löschen eines Firewallregelabschnitts

Sie können einen Firewallregelabschnitt löschen. Alle Regeln in diesem Abschnitt werden gelöscht.

Sie können einen Abschnitt löschen und zu einem anderen Ort in der Firewalltabelle hinzufügen. Dazu müssen Sie den Abschnitt löschen und die Konfiguration veröffentlichen. Fügen Sie anschließend den gelöschten Abschnitt zur Firewalltabelle hinzu und veröffentlichen Sie die Konfiguration erneut.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Firewall**.
- 2 Stellen Sie sicher, dass Sie sich auf der Registerkarte **Allgemein (General)** befinden, um einen Abschnitt für L3-Regeln zu löschen. Klicken Sie auf die Registerkarte **Ethernet**, um einen Abschnitt für L2-Regeln zu löschen.
- 3 Klicken Sie auf das Symbol **Abschnitt löschen (Delete section)** (✖) für den zu löschenden Abschnitt.
- 4 Klicken Sie auf **OK** und anschließend auf **Änderungen veröffentlichen (Publish Changes)**.

### Ergebnisse

Sowohl der Abschnitt als auch die Regeln in diesem Abschnitt werden gelöscht.

## Arbeiten mit Firewallregeln

Regeln für die verteilte Firewall und die Edge-Firewall können zentral auf der Firewall-Registerkarte verwaltet werden. In einer mehrinstanzenfähigen Umgebung können Anbieter Regeln für Datenverkehrsfluss auf hoher Ebene in der zentralisierten Firewall-Benutzeroberfläche definieren.

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

- 1 Regeln, die in der Firewall-Benutzeroberfläche von Benutzern definiert wurden, haben die höchste Priorität, und werden in absteigender Reihenfolge auf der Ebene der jeweiligen virtuellen Netzwerkkarte erzwungen.
- 2 „Auto-plumbed“-Regeln (Regeln, die den Fluss des Steuerungsdatenverkehrs für Edge-Dienste aktivieren).
- 3 Regeln, die in der NSX Edge-Schnittstelle von Benutzern definiert sind.
- 4 Service Composer-Regeln – ein getrennter Abschnitt für jede Richtlinie. Sie können diese Regeln nicht in der Firewalltabelle bearbeiten, aber Sie können Regeln oben im Bereich für Firewallregeln innerhalb einer Sicherheitsrichtlinie hinzufügen. Dabei müssen Sie die Regeln in Service Composer erneut synchronisieren. Weitere Informationen finden Sie unter [Kapitel 17 Service Composer](#).
- 5 Standardregeln für die verteilte Firewall

Beachten Sie, dass Firewallregeln nur auf Clustern erzwungen werden, auf denen Sie eine Firewall aktiviert haben. Weitere Informationen zum Vorbereiten von Clustern finden Sie unter *Installationshandbuch für NSX*.

## Bearbeiten der standardmäßigen Regel für die verteilte Firewall

Die standardmäßigen Firewallereinstellungen gelten für den Datenverkehr, der unter keine der benutzerdefinierten Firewallregeln fällt. Die Standardregel für die verteilte Firewall wird auf der Benutzer-Schnittstelle der zentralisierten Firewall angezeigt und die Standardregel für jede NSX Edge-Instanz wird auf NSX Edge-Ebene angezeigt.

Die Standardregel für die verteilte Firewall lässt die Durchleitung von L3- und L2-Datenverkehr durch alle Cluster in Ihrer Infrastruktur zu. Die Standardregel befindet sich immer am Ende der Regeltabelle und kann weder gelöscht noch hinzugefügt werden. Sie können jedoch für jede Regel das Element „Aktion“ von „Zulassen“ in „Blockieren“ oder „Ablehnen“ ändern, Anmerkungen zur Regel hinzufügen und festlegen, ob der Datenverkehr zu dieser Regel protokolliert werden soll.

In einer Cross-vCenter NSX-Umgebung ist die Standardregel keine globale Regel. Änderungen der Standardregel müssen in jedem NSX Manager vorgenommen werden.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Firewall**.
- 2 Erweitern Sie den Standardabschnitt und nehmen Sie die erforderlichen Änderungen vor.

Sie können nur **Aktion (Action)** und **Protokoll (Log)** bearbeiten oder Anmerkungen zur Standardregel hinzufügen.

## Hinzufügen einer Regel für die verteilte Firewall

Sie fügen Firewallregeln im Geltungsbereich des NSX Manager hinzu. Wenn Sie das Feld „Angewendet auf“ verwenden, können Sie den Geltungsbereich einschränken, in dem Sie die Regel anwenden möchten. Sie können mehrere Objekte auf Quell- und Zielebene für jede Regel hinzufügen, um so die Gesamtzahl der zu erstellenden Firewallregeln zu verringern.

Die folgenden vCenter-Objekte können als Quelle oder Ziel für eine Firewallregel angegeben werden:

**Tabelle 10-2. Für Firewallregeln unterstützte Objekte**

Quelle oder Ziel	Angewendet auf
■ Cluster	■ Alle Cluster, auf denen die verteilte Firewall installiert wurde (in anderen Worten: alle Cluster, die für Netzwerkvisualisierung vorbereitet wurden)
■ Datacenter	■ Alle auf vorbereiteten Clustern installierte Edge Gateways
■ verteilte Portgruppe	■ Cluster
■ IP Set	■ Datacenter
■ Legacy-Portgruppe	■ verteilte Portgruppe
■ Logischer Switch	■ Edge
■ Ressourcenpool	■ Legacy-Portgruppe
■ Sicherheitsgruppe	■ Logischer Switch
■ vApp	■ Sicherheitsgruppe
■ virtuelle Maschine	■ virtuelle Maschine
■ vNIC	■ vNIC
■ IP-Adresse (IPv4 oder IPv6)	

## Voraussetzungen

Stellen Sie sicher, dass sich die verteilte Firewall von NSX nicht im Abwärtskompatibilitätsmodus befindet. Um den aktuellen Status zu überprüfen, verwenden Sie den REST API-Aufruf „GET https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/status“. Wenn der aktuelle Status der Abwärtskompatibilitätsmodus ist, können Sie den Status durch den REST API-Aufruf „PUT https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state“ ändern. Versuchen Sie nicht, eine Regel für eine verteilte Firewall zu veröffentlichen, während sich die verteilte Firewall im Abwärtskompatibilitätsmodus befindet.

Weitere Informationen zum Hinzufügen von universellen Firewallregeln finden Sie unter [Hinzufügen einer universellen Firewallregel](#).


Wenn Sie eine identitätsbasierte Firewallregel hinzufügen, stellen Sie Folgendes sicher:

- Mindestens eine Domäne wurde bei NSX Manager registriert. NSX Manager ruft Gruppen- und Benutzerinformationen sowie die Beziehung zwischen diesen aus jeder Domäne ab, die bei NSX Manager registriert ist. Weitere Informationen dazu finden Sie unter [Registrieren einer Windows-Domäne mit NSX Manager](#).
- Eine auf Active Directory-Objekten basierte Sicherheitsgruppe wurde erstellt, die als Quelle oder Ziel der Regel verwendet werden kann. Weitere Informationen dazu finden Sie unter [Erstellen einer Sicherheitsgruppe](#).


Wenn Sie eine auf ein VMware vCenter-Objekt basierende Regel hinzufügen, stellen Sie sicher, dass VMware Tools auf den virtuellen Maschinen installiert ist. Weitere Informationen hierzu finden Sie im *Installationshandbuch für NSX*.

VMs, die von 6.1.5 auf 6.2.3 migriert wurden, bieten keine Unterstützung für TFTP ALG. Um die Unterstützung für TFTP ALG nach der Migration zu aktivieren, fügen Sie die VM hinzu und entfernen Sie diese aus der Ausschlussliste oder starten Sie die VM neu. Ein neuer 6.2.3-Filter wird erstellt, der TFTP ALG unterstützt.

## Verfahren




- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Firewall**.
- 2 Achten Sie beim Hinzufügen einer L3-Regel darauf, dass Sie sich auf der Registerkarte **Allgemein (General)** befinden. Klicken Sie auf die Registerkarte **Ethernet**, um eine L2-Regel hinzuzufügen.
- 3 Klicken Sie in dem Abschnitt, in dem Sie eine Regel hinzufügen, auf das Symbol **Regel hinzufügen (Add rule)** (.
- 4 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

Die neue Regel wird an oberster Stelle im Abschnitt eingefügt. Wenn der Abschnitt nur die systemdefinierte Regel enthält, wird die neue Regel über der Standardregel eingefügt.




Wenn Sie eine Regel an einer bestimmten Stelle im Abschnitt einfügen möchten, wählen Sie eine Regel aus. Klicken Sie in der Spalte „Nr.“ auf  und wählen Sie **Oben hinzufügen (Add Above)** oder **Unten hinzufügen (Add Below)** aus.

- 5 Zeigen Sie auf die Zelle **Name** der neuen Regel und klicken Sie auf .




- 6 Geben Sie einen Namen für die neue Regel ein.
- 7 Zeigen Sie auf die Zelle **Quelle (Source)** der neuen Regel. Zusätzliche Symbole werden wie in der Tabelle unten beschrieben angezeigt.

Option	Beschreibung
Klicken Sie auf 	<p>Zur Angabe der Quelle als IP-Adresse.</p> <p>a Wählen Sie das IP-Adressenformat aus.</p> <p>Firewall unterstützt sowohl das IPv4- als auch das IPv6-Format.</p> <p>b Geben Sie die IP-Adresse ein.</p> <p>Sie können mehrere IP-Adressen in einer kommagetrennten Liste eingeben. Die Liste kann bis zu 255 Zeichen lang sein.</p>
Klicken Sie auf 	<p>Zur Angabe der Quelle als Objekt und nicht als bestimmte IP-Adresse.</p> <p>a Wählen Sie unter <b>Ansicht (View)</b> den Container des Ursprungs der Kommunikation aus.</p> <p>Die Objekte des ausgewählten Containers werden angezeigt.</p> <p>b Wählen Sie mindestens ein Objekt aus und klicken Sie auf .</p> <p>Sie können eine neue Sicherheitsgruppe oder ein neues IPSets erstellen. Nachdem Sie das neue Objekt erstellt haben, wird es standardmäßig zur Spalte „Quelle“ hinzugefügt. Weitere Informationen zum Erstellen neuer Sicherheitsgruppen oder IPSets finden Sie unter <a href="#">Kapitel 21 Netzwerk- und Sicherheitsobjekte</a>.</p> <p>c Klicken Sie zum Ausschließen einer Quelle von der Regel auf <b>Erweiterte Optionen (Advanced options)</b>.</p> <p>d Wählen Sie <b>Quelle ablehnen (Negate Source)</b>, um diese Quelle von der Regel auszuschließen.</p> <p>Wenn <b>Quelle ablehnen (Negate Source)</b> ausgewählt ist, gilt die Regel für den Datenverkehr, der aus allen Quellen außer der Quelle stammt, die Sie im vorherigen Schritt angegeben haben.</p> <p>Wenn <b>Quelle ablehnen (Negate Source)</b> nicht ausgewählt ist, gilt die Regel für den Datenverkehr, der aus den Quellen stammt, die Sie im vorherigen Schritt angegeben haben.</p> <p>e Klicken Sie auf <b>OK</b>.</p>


- 8 Zeigen Sie auf die Zelle **Ziel (Destination)** der neuen Regel. Zusätzliche Symbole werden wie in der Tabelle unten beschrieben angezeigt.

Option	Beschreibung
Klicken Sie auf  .	<p>Zur Angabe des Ziels als IP-Adresse.</p> <p>a Wählen Sie das IP-Adressenformat aus.</p> <p>Firewall unterstützt sowohl das IPv4- als auch das IPv6-Format.</p> <p>b Geben Sie die IP-Adresse ein.</p> <p>Sie können mehrere IP-Adressen in einer kommagetrennten Liste eingeben. Die Liste kann bis zu 255 Zeichen lang sein.</p>
Klicken Sie auf  .	<p>Zur Angabe des Ziels als Objekt und nicht als bestimmte IP-Adresse.</p> <p>a Wählen Sie unter <b>Ansicht (View)</b> den Container des Ziels der Kommunikation aus.</p> <p>Die Objekte des ausgewählten Containers werden angezeigt.</p> <p>b Wählen Sie mindestens ein Objekt aus und klicken Sie auf .</p> <p>Sie können eine neue Sicherheitsgruppe oder ein neues IPSet erstellen. Nachdem Sie das neue Objekt erstellt haben, wird es standardmäßig zur Spalte „Ziel“ hinzugefügt. Weitere Informationen zum Erstellen neuer Sicherheitsgruppen oder IPSets finden Sie unter <a href="#">Kapitel 21 Netzwerk- und Sicherheitsobjekte</a>.</p> <p>c Klicken Sie zum Ausschließen eines Zielports auf <b>Erweiterte Einstellungen (Advanced options)</b>.</p> <p>d Wählen Sie <b>Ziel ablehnen (Negate Destination)</b>, um das Ziel von der Regel auszuschließen.</p> <p>Wenn <b>Ziel ablehnen (Negate Destination)</b> ausgewählt ist, gilt die Regel für den Datenverkehr, der zu allen Zielen außer dem Ziel geht, das Sie im vorherigen Schritt angegeben haben.</p> <p>Wenn <b>Ziel ablehnen (Negate Destination)</b> nicht ausgewählt ist, gilt die Regel für den Datenverkehr, der zum Ziel geht, das Sie im vorherigen Schritt angegeben haben.</p> <p>e Klicken Sie auf <b>OK</b>.</p>

- 9 Zeigen Sie auf die Zelle **Dienst (Service)** der neuen Regel. Zusätzliche Symbole werden wie in der Tabelle unten beschrieben angezeigt.


Option	Beschreibung
Klicken Sie auf  .	<p>So geben Sie einen Dienst als Port-Protokoll-Kombination an.</p> <p>a Wählen Sie das Dienstprotokoll aus.</p> <p>Die verteilte Firewall unterstützt ALG (Application Level Gateway) für die folgenden Protokolle: TFTP, FTP, ORACLE, TNS, MS-RPC und SUN-RPC.</p> <p>Edge unterstützt ein ALG für FTP, TFTP und SNMP_BASIC.</p> <p>Hinweis: VMs, die von 6.1.5 auf 6.2.3 migriert wurden, bieten keine Unterstützung für TFTP ALG. Um die Unterstützung für TFTP ALG nach der Migration zu aktivieren, fügen Sie die VM hinzu und entfernen Sie diese aus der Ausschlussliste oder starten Sie die VM neu. Ein neuer 6.2.3-Filter wird erstellt, der TFTP ALG unterstützt.</p> <p>b Geben Sie die Portnummer ein und klicken Sie auf <b>OK</b>.</p>
Klicken Sie auf  .	<p>So wählen Sie einen vordefinierten Dienst/eine vordefinierte Dienstgruppe aus oder definieren einen neuen Dienst bzw. eine neue Dienstgruppe.</p> <p>a Wählen Sie mindestens ein Objekt aus und klicken Sie auf .</p> <p>Sie können einen neuen Dienst oder eine neue Dienstgruppe erstellen. Nachdem Sie das neue Objekt erstellt haben, wird es standardmäßig zur Spalte „Ausgewählte Objekte“ hinzugefügt.</p> <p>b Klicken Sie auf <b>OK</b>.</p>

Zum Schutz Ihres Netzwerks vor ACK- oder SYN-Überflutung können Sie den Dienst auf TCP-all\_ports oder UDP-all\_ports setzen und „Zu blockierende Aktion“ als Standardregel festlegen. Weitere Informationen zum Ändern der Standardregel finden Sie unter [Bearbeiten der standardmäßigen Regel für die verteilte Firewall](#).

- 10 Zeigen Sie auf die Zelle **Aktion (Action)** der neuen Regel und klicken Sie auf . Treffen Sie eine entsprechende Auswahl, wie in der nachfolgenden Tabelle beschrieben, und klicken Sie auf **OK**.

Aktion	Ergebnis
<b>Zulassen</b>	Lässt Datenverkehr von oder zu angegebener/n Quelle/n, Ziel/en und Dienst/en zu.
<b>Blockieren</b>	Blockiert Datenverkehr von oder zu angegebener/n Quelle/n, Ziel/en und Dienst/en.
<b>Ablehnen</b>	<p>Versendet Ablehnungsmeldungen für nicht angenommene Pakete.</p> <p>RST-Pakete werden für TCP-Verbindungen versendet.</p> <p>ICMP-Meldungen mit vom Administrator verbotenen Code werden für UDP-, ICMP- und andere IP-Verbindungen versendet.</p>
<b>Protokoll</b>	Protokolliert alle Sitzungen, auf die diese Regel zutrifft. Das Aktivieren der Protokollierung kann die Leistung beeinträchtigen.
<b>Nicht protokollieren</b>	Protokolliert keine Sitzungen.

- 11 Definieren Sie in **Angewendet auf (Applied To)** die Ebene, auf der diese Regel anwendbar ist. Treffen Sie eine entsprechende Auswahl, wie in der nachfolgenden Tabelle beschrieben, und klicken Sie auf **OK**.

Zum Anwenden einer Regel auf	Führen Sie Folgendes durch
Alle vorbereiteten Cluster in Ihrer Umgebung	Wählen Sie <b>Wenden Sie diese Regel auf alle Cluster an, auf denen die verteilte Firewall aktiviert ist (Apply this rule on all clusters on which Distributed Firewall is enabled)</b> . Nachdem Sie auf „OK“ geklickt haben, wird in der Spalte „Angewendet auf“ die Option <b>verteilte Firewall (Distributed Firewall)</b> angezeigt.
Alle NSX Edge Gateways in Ihrer Umgebung	Wählen Sie <b>Wenden Sie diese Regel auf alle Edge-Gateways an (Apply this rule on all Edge gateways)</b> . Nachdem Sie auf „OK“ geklickt haben, wird in der Spalte „Angewendet auf“ die Option <b>Alle Edges (All Edges)</b> angezeigt.  Wenn beide genannten Optionen ausgewählt sind, wird in der Spalte „Angewendet auf“ die Option <b>Beliebig (Any)</b> angezeigt.
Mindestens ein Cluster, Datacenter, Netzwerk, logischen Switch, eine verteilte virtuelle Portgruppe, NSX Edge, virtuelle Maschine oder vNIC	<ol style="list-style-type: none"> <li>1 Wählen Sie unter <b>Containertyp (Container type)</b> das entsprechende Objekt aus.</li> <li>2 Wählen Sie in der Liste „Verfügbar“ mindestens ein Objekt aus und klicken Sie auf .</li> </ol>

Wenn die Regel virtuelle Maschinen/vNICs in den Feldern „Quelle“ und „Ziel“ enthält, müssen Sie sowohl die Quell-VMs/-vNICs als auch die Ziel-VMs/-vNICs zu **Angewendet auf (Applied To)** hinzufügen, damit die Regel richtig angewandt wird.

- 12 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.


Nach kurzer Zeit wird eine Meldung mit der Angabe angezeigt, ob der Veröffentlichungsvorgang erfolgreich war. Im Falle eines Fehlers werden die Hosts, auf die die Regel nicht angewendet wurde, nicht aufgeführt. Weitere Details zu fehlgeschlagenen Veröffentlichungen finden Sie, wenn Sie zu **NSX Manager (NSX Managers) > NSX\_Manager\_IP\_Address > Überwachen (Monitor) > Systemereignisse (System Events)** navigieren.

Wenn Sie auf **Änderungen veröffentlichen (Publish Changes)** klicken, wird die Konfiguration der Firewall automatisch gespeichert. Informationen zum Wiederherstellen einer früheren Konfiguration finden Sie unter [Laden einer gespeicherten Firewallkonfiguration](#).

### Nächste Schritte

- Deaktivieren Sie eine Regel durch Klicken auf  oder aktivieren Sie eine Regel durch Klicken auf .

- Zeigen Sie weitere Spalten in der Regeltabelle an, indem Sie auf  klicken und die entsprechenden Spalten auswählen.

Spaltenname	Angezeigte Informationen
Regel-ID	Eindeutige, systemgenerierte ID für jede Regel
Protokoll	Datenverkehr für diese Regel wird protokolliert bzw. nicht protokolliert
Statistik	Mit einem Klick auf  wird der auf diese Regel bezogene Datenverkehr angezeigt (Datenverkehrspakete und Größe).
Anmerkungen	Anmerkungen zur Regel


- Suchen Sie nach Regeln, indem Sie Text in das Feld „Suche“ eingeben.
- Verschieben Sie eine Regel in der Firewalltabelle nach oben oder nach unten.
- Führen Sie Abschnitte zusammen, indem Sie auf das Symbol **Abschnitt zusammenführen (Merge section)** klicken und die Option **Mit Abschnitt oben zusammenführen (Merge with above section)** oder **Mit Abschnitt unten zusammenführen (Merge with below section)** auswählen.

## Erzwingen der Synchronisierung von verteilten Firewallregeln

Wenn Firewallregeln nicht für Hosts veröffentlicht werden können, führen Sie eine erzwungene Synchronisierung durch.

Das Erzwingen der Synchronisierung ist erforderlich, wenn die Firewallregeln auf einem einzelnen Host mit NSX Manager synchronisiert werden müssen.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Installation > Hostvorbereitung (Host Preparation)**.
- 2 Wählen Sie den Cluster aus, dessen Synchronisierung erzwungen werden soll, und klicken Sie auf **Aktionen (Actions)** () > **ForceSync-Dienste (Force Sync Services)**.
- 3 Wählen Sie die **Firewall** aus den Diensten für das Erzwingen der Synchronisierung aus. Klicken Sie auf **OK**.

Der Firewallstatus wechselt während der Synchronisierung zu „Belegt“.

## Hinzufügen einer universellen Firewallregel

In einer Cross-vCenter NSX-Umgebung beziehen sich universelle Regeln auf die Regeln für die verteilte Firewall, die auf dem primären NSX Manager im Abschnitt der universellen Regeln definiert wurden. Diese Regeln werden auf allen sekundären NSX Managern in Ihrer Umgebung repliziert, wodurch Sie eine einheitliche Firewallrichtlinie über vCenter-Grenzen hinweg beibehalten können. Edge-Firewallregeln werden für vMotion zwischen mehreren vCenter Servern nicht unterstützt.

Der primäre NSX Manager kann mehrere universelle Abschnitte für universelle L2-Regeln sowie mehrere universelle Abschnitte für universelle L3-Regeln beinhalten. Universelle Abschnitte befinden sich über allen lokalen Abschnitten und Service Composer-Abschnitten. Universelle Abschnitte und universelle Regeln können auf den sekundären NSX Managern angezeigt, aber nicht bearbeitet werden. Die Platzierung des universellen Abschnitts in Bezug auf den lokalen Abschnitt beeinträchtigt nicht die Priorität der Regeln.

**Tabelle 10-3. Für universelle Firewallregeln unterstützte Objekte**



Quelle und Ziel	Angewendet auf	Dienst
<ul style="list-style-type: none"> <li>■ universelles MAC Set</li> <li>■ universelles IP Set</li> <li>■ universelle Sicherheitsgruppe, die ein universelles Sicherheits-Tag, ein IP Set, ein MAC Set oder eine universelle Sicherheitsgruppe enthalten kann</li> </ul>	<ul style="list-style-type: none"> <li>■ universelle Sicherheitsgruppe, die ein universelles Sicherheits-Tag, ein IP Set, ein MAC Set oder eine universelle Sicherheitsgruppe enthalten kann</li> <li>■ Globaler logischer Switch</li> <li>■ verteilte Firewall – wendet Regeln auf allen Clustern an, auf denen die verteilte Firewall installiert ist</li> </ul>	<ul style="list-style-type: none"> <li>■ vorab erstellte universelle Dienste und Dienstgruppen</li> <li>■ vom Benutzer erstellte universelle Dienste und Dienstgruppen</li> </ul>

Beachten Sie, dass andere vCenter-Objekte nicht für universelle Regeln unterstützt werden.




### Voraussetzungen

Sie müssen einen Abschnitt für eine universelle Regel erstellen, bevor Sie universelle Regeln erstellen können. Weitere Informationen dazu finden Sie unter [Hinzufügen eines Firewallregelabschnitts](#).




### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Firewall**.
- 2 Stellen Sie in NSX Manager sicher, dass der primäre NSX Manager ausgewählt ist.  
Universelle Regeln können nur auf dem primären NSX Manager hinzugefügt werden.
- 3 Achten Sie beim Hinzufügen einer universellen L3-Regel darauf, dass Sie sich auf der Registerkarte **Allgemein (General)** befinden. Klicken Sie auf die Registerkarte **Ethernet**, um eine universelle L2-Regel hinzuzufügen.
- 4 Klicken Sie im universellen Abschnitt auf das Symbol **Regel hinzufügen (Add rule)** (  ) und klicken Sie anschließend auf **Änderungen veröffentlichen (Publish Changes)**.  
Die neue Regel wird an oberster Stelle im universellen Abschnitt eingefügt.
- 5 Zeigen Sie auf die Zelle **Name** der neuen Regel und klicken Sie auf  . Geben Sie einen Namen für die Regel ein.




- 6 Zeigen Sie auf die Zelle **Quelle (Source)** der neuen Regel. Zusätzliche Symbole werden wie in der Tabelle unten beschrieben angezeigt.

Option	Beschreibung
Klicken Sie auf  .	<p>Zur Angabe der Quelle als IP-Adresse.</p> <p>a Wählen Sie das IP-Adressenformat aus.</p> <p>Firewall unterstützt sowohl das IPv4- als auch das IPv6-Format.</p> <p>b Geben Sie die IP-Adresse ein.</p>
Klicken Sie auf  .	<p>So geben Sie ein universelles IP Set, ein MAC Set oder eine Sicherheitsgruppe als Quelle an.</p> <p>a Wählen Sie unter <b>Objekttyp (Object Type)</b> den Container des Ursprungs der Kommunikation aus.</p> <p>Die Objekte des ausgewählten Containers werden angezeigt.</p> <p>b Wählen Sie mindestens ein Objekt aus und klicken Sie auf .</p> <p>Sie können eine neue Sicherheitsgruppe oder ein neues IPSets erstellen. Nachdem Sie das neue Objekt erstellt haben, wird es standardmäßig zur Spalte „Quelle“ hinzugefügt. Weitere Informationen zum Erstellen neuer Sicherheitsgruppen oder IPSets finden Sie unter <a href="#">Kapitel 21 Netzwerk- und Sicherheitsobjekte</a>.</p> <p>c Klicken Sie zum Ausschließen einer Quelle von der Regel auf <b>Erweiterte Optionen (Advanced options)</b>.</p> <p>d Wählen Sie <b>Quelle ablehnen (Negate Source)</b>, um diese Quelle von der Regel auszuschließen.</p> <p>Wenn <b>Quelle ablehnen (Negate Source)</b> ausgewählt ist, gilt die Regel für den Datenverkehr, der aus allen Quellen außer der Quelle stammt, die Sie im vorherigen Schritt angegeben haben.</p> <p>Wenn <b>Quelle ablehnen (Negate Source)</b> nicht ausgewählt ist, gilt die Regel für den Datenverkehr, der aus den Quellen stammt, die Sie im vorherigen Schritt angegeben haben.</p> <p>e Klicken Sie auf <b>OK</b>.</p>


- 7 Zeigen Sie auf die Zelle **Ziel (Destination)** der neuen Regel. Zusätzliche Symbole werden wie in der Tabelle unten beschrieben angezeigt.

Option	Beschreibung
Klicken Sie auf  .	<p>Zur Angabe des Ziels als IP-Adresse.</p> <ol style="list-style-type: none"> <li>Wählen Sie das IP-Adressenformat aus.</li> </ol> <p>Firewall unterstützt sowohl das IPv4- als auch das IPv6-Format.</p> <ol style="list-style-type: none"> <li>Geben Sie die IP-Adresse ein.</li> </ol>
Klicken Sie auf  .	<p>So geben Sie ein universelles IP Set, ein MAC Set oder eine Sicherheitsgruppe als Ziel an.</p> <ol style="list-style-type: none"> <li>Wählen Sie unter <b>Objektyp (Object Type)</b> den Container des Ziels der Kommunikation aus.</li> </ol> <p>Die Objekte des ausgewählten Containers werden angezeigt.</p> <ol style="list-style-type: none"> <li>Wählen Sie mindestens ein Objekt aus und klicken Sie auf .</li> </ol> <p>Sie können eine neue Sicherheitsgruppe oder ein neues IPSets erstellen. Nachdem Sie das neue Objekt erstellt haben, wird es standardmäßig zur Spalte „Ziel“ hinzugefügt. Weitere Informationen zum Erstellen neuer Sicherheitsgruppen oder IPSets finden Sie unter <a href="#">Kapitel 21 Netzwerk- und Sicherheitsobjekte</a>.</p> <ol style="list-style-type: none"> <li>Klicken Sie zum Ausschließen eines Ziels von der Regel auf <b>Erweiterte Optionen (Advanced options)</b>.</li> <li>Wählen Sie <b>Ziel ablehnen (Negate Destination)</b>, um das Ziel von der Regel auszuschließen.</li> </ol> <p>Wenn <b>Ziel ablehnen (Negate Destination)</b> ausgewählt ist, gilt die Regel für den Datenverkehr, der zu allen Zielen außer dem Ziel geht, das Sie im vorherigen Schritt angegeben haben.</p> <p>Wenn <b>Ziel ablehnen (Negate Destination)</b> nicht ausgewählt ist, gilt die Regel für den Datenverkehr, der zum Ziel geht, das Sie im vorherigen Schritt angegeben haben.</p> <ol style="list-style-type: none"> <li>Klicken Sie auf <b>OK</b>.</li> </ol>


- 8 Zeigen Sie auf die Zelle **Dienst (Service)** der neuen Regel. Zusätzliche Symbole werden wie in der Tabelle unten beschrieben angezeigt.

Option	Beschreibung
Klicken Sie auf  .	<p>So geben Sie einen Dienst als Port-Protokoll-Kombination an.</p> <p>a Wählen Sie das Dienstprotokoll aus.</p> <p>Die verteilte Firewall unterstützt ALG (Application Level Gateway) für die folgenden Protokolle: FTP, CIFS, ORACLE, TNS, MS-RPC und SUN-RPC.</p> <p>b Geben Sie die Portnummer ein und klicken Sie auf <b>OK</b>.</p>
Klicken Sie auf  .	<p>So wählen Sie einen vordefinierten universellen Dienst/eine vordefinierte universelle Dienstgruppe aus oder definieren einen neuen Dienst bzw. eine neue Dienstgruppe.</p> <p>a Wählen Sie mindestens ein Objekt aus und klicken Sie auf .</p> <p>Sie können einen neuen Dienst oder eine neue Dienstgruppe erstellen. Nachdem Sie das neue Objekt erstellt haben, wird es standardmäßig zur Spalte „Ausgewählte Objekte“ hinzugefügt.</p> <p>b Klicken Sie auf <b>OK</b>.</p>


Zum Schutz Ihres Netzwerks vor ACK- oder SYN-Überflutung können Sie den Dienst auf TCP-all\_ports oder UDP-all\_ports setzen und „Zu blockierende Aktion“ als Standardregel festlegen. Weitere Informationen zum Ändern der Standardregel finden Sie unter [Bearbeiten der standardmäßigen Regel für die verteilte Firewall](#).

- 9 Zeigen Sie auf die Zelle **Action** der neuen Regel und klicken Sie auf . Treffen Sie eine entsprechende Auswahl, wie in der nachfolgenden Tabelle beschrieben, und klicken Sie auf **OK**.

Aktion	Ergebnis
<b>Zulassen</b>	Lässt Datenverkehr von oder zu angegebener/n Quelle/n, Ziel/en und Dienst/en zu.
<b>Blockieren</b>	Blockiert Datenverkehr von oder zu angegebener/n Quelle/n, Ziel/en und Dienst/en.
<b>Ablehnen</b>	<p>Versendet Ablehnungsmeldungen für nicht angenommene Pakete.</p> <p>RST-Pakete werden für TCP-Verbindungen versendet.</p> <p>ICMP-Meldungen mit vom Administrator verbotenen Code werden für UDP-, ICMP- und andere IP-Verbindungen versendet.</p>
<b>Protokoll</b>	Protokolliert alle Sitzungen, auf die diese Regel zutrifft. Das Aktivieren der Protokollierung kann die Leistung beeinträchtigen.
<b>Nicht protokollieren</b>	Protokolliert keine Sitzungen.

- 10 Akzeptieren Sie entweder in der Zelle **Angewendet auf (Applied To)** die Standardeinstellung „verteilte Firewall“, um die Regel auf allen Clustern mit aktivierter Verteilter Firewall anzuwenden, oder klicken Sie auf das Symbol „Bearbeiten“ , um die globalen logischen Switches auszuwählen, auf denen die Regel angewendet werden soll.
- 11 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Ergebnisse




Die universelle Regel wird auf allen sekundären NSX Managern repliziert. Die Regel-ID bleibt über alle NSX-Instanzen hinweg gleich. Um die Regel-ID anzuzeigen, klicken Sie auf  und klicken Sie anschließend auf „Regel-ID“.


Universelle Regeln können auf dem primären NSX Manager bearbeitet werden und sind auf den sekundären NSX Managern schreibgeschützt.

Firewallregeln mit „Universalabschnitt-Schicht 3“ und „Standardabschnitt-Schicht 3“:

No.	Name	Source	Destination	Service	Action	Applied To
Universal Section Layer3 (Rule 1 - 2)						
1	Web Micro-Segmentation	Web USG	Web USG	* any	Block	Distributed Firewall
2	Allow Web Access	* any	Web USG	HTTPS SSH	Allow	Distributed Firewall
Default Section Layer3 (Rule 3 - 7)						
3	Web Micro-Segmentation	Web SG	Web SG	* any	Allow	Distributed Firewall
4	Allow Web Access	* any	Web SG	HTTPS SSH	Allow	Distributed Firewall
5	Default Rule NDP	* any	* any	IPv6-ICMP Neighbor ... IPv6-ICMP Neighbor ...	Allow	Distributed Firewall
6	Default Rule DHCP	* any	* any	DHCP-Client DHCP-Server	Allow	Distributed Firewall
7	Default Rule	* any	* any	* any	Block	Distributed Firewall

## Nächste Schritte

- Deaktivieren Sie eine Regel, indem Sie in der Spalte „Nr.“ auf  klicken, oder aktivieren Sie eine Regel, indem Sie auf  klicken.
- Zeigen Sie weitere Spalten in der Regeltabelle an, indem Sie auf  klicken und die entsprechenden Spalten auswählen.

Spaltenname	Angezeigte Informationen
Regel-ID	Eindeutige, systemgenerierte ID für jede Regel
Protokoll	Datenverkehr für diese Regel wird protokolliert bzw. nicht protokolliert
Statistik	Mit einem Klick auf  wird der auf diese Regel bezogene Datenverkehr angezeigt (Datenverkehrspakete und Größe).
Anmerkungen	Anmerkungen zur Regel





- Suchen Sie nach Regeln, indem Sie Text in das Feld „Suche“ eingeben.
- Verschieben Sie eine Regel in der Firewalltabelle nach oben oder nach unten.

## Firewallregeln mit einem benutzerdefinierten Schicht-3-Protokoll

Firewallregeln können mithilfe einer benutzerdefinierten Protokollnummer erstellt werden, die nicht im Dropdown-Menü „Protokolle“ aufgeführt ist.

Eine Firewallregel mit einer benutzerdefinierten Protokollnummer kann auf der Verteilten Firewall oder auf der NSX Edge-Firewall erstellt werden.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Firewall**.
- 2 Achten Sie beim Hinzufügen einer L3-Regel darauf, dass Sie sich auf der Registerkarte **Allgemein (General)** befinden. Klicken Sie auf das Symbol **Regel hinzufügen (Add rule)** (  ).
- 3 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.  
 Die neue Regel wird an oberster Stelle im Abschnitt eingefügt. Wenn der Abschnitt nur die systemdefinierte Regel enthält, wird die neue Regel über der Standardregel eingefügt.  
 Wenn Sie eine Regel an einer bestimmten Stelle im Abschnitt einfügen möchten, wählen Sie eine Regel aus. Klicken Sie in der Spalte „Nr.“ auf  und wählen Sie **Oben hinzufügen (Add Above)** oder **Unten hinzufügen (Add Below)** aus.
- 4 Zeigen Sie auf die Zelle **Name** der neuen Regel und klicken Sie auf .
- 5 Geben Sie einen Namen für die neue Regel ein.
- 6 Legen Sie unter **Quelle (Source)** die Quelle der neuen Regel fest. Informationen zu Symboldetails finden Sie unter [Hinzufügen einer Regel für die verteilte Firewall](#).
- 7 Legen Sie unter **Ziel (Destination)** das Ziel der neuen Regel fest. Weitere Informationen finden Sie unter [Hinzufügen einer Regel für die verteilte Firewall](#).
- 8 Zeigen Sie auf die Zelle **Dienst (Service)** der neuen Regel. Klicken Sie auf das Symbol **Dienst hinzufügen (Add Service)** (  ).
- 9 Klicken Sie im Fenster **Dienst angeben (Specify Service)** links unten auf **Neuer Dienst (New Service)**.
- 10 Geben Sie unter **Name** den Namen des neuen Protokolls (z. B. OSPF) ein.
- 11 Wählen Sie im Dropdown-Menü „Protokolle“ **L3\_OTHERS** aus.  
 Ein Feld **Protokollnummer (Protocol Number)** wird unter dem Dropdown-Menü angezeigt.
- 12 Geben Sie unter **Protokollnummer (Protocol Number)** die Protokollnummer (z. B. 89 für OSPF) ein.
- 13 Klicken Sie auf **OK**.

### Ergebnisse

Eine Firewallregel wurde mithilfe einer benutzerdefinierten Protokollnummer erstellt.

## Speichern einer nicht veröffentlichten Konfiguration

Sie können eine Regel hinzufügen und die Konfiguration speichern, ohne sie zu veröffentlichen. Sie können die gespeicherte Konfiguration dann später laden und veröffentlichen.

## Verfahren

- 1 Fügen Sie eine Firewallregel hinzu. Weitere Informationen dazu finden Sie unter [Hinzufügen einer Regel für die verteilte Firewall](#).
- 2 Klicken Sie auf **Änderungen speichern (Save Changes)**.
- 3 Geben Sie einen Namen und eine Beschreibung für die Konfiguration ein und klicken Sie auf **OK**.
- 4 Klicken Sie auf **Konfiguration beibehalten (Preserve Configuration)**, um diese Änderung beizubehalten.


NSX kann bis zu 100 Konfigurationen speichern. Wenn dieser Grenzwert überschritten wurde, werden mit **Konfiguration beibehalten (Preserve Configuration)** markierte, gespeicherte Konfigurationen beibehalten, während ältere, nicht beibehaltene Konfigurationen gelöscht werden, um Speicherplatz für beibehaltene Konfigurationen zu schaffen.

- 5 Führen Sie einen der folgenden Schritte aus:
  - Klicken Sie auf **Änderungen rückgängig machen (Revert Changes)**, um die Konfiguration wiederherzustellen, die vor dem Hinzufügen der Regel bestand. Wenn Sie die soeben hinzugefügte Regel veröffentlichen möchten, klicken Sie auf das Symbol **Konfiguration laden (Load Configuration)**, wählen Sie die in Schritt 3 gespeicherte Regel aus und klicken Sie auf **OK**.
  - Klicken Sie auf **Aktualisierungsänderungen (Update Changes)**, um weitere Regeln hinzuzufügen.

## Laden einer gespeicherten Firewallkonfiguration

Sie können eine automatisch gespeicherte oder importierte Firewallkonfiguration laden. Falls Ihre gegenwärtige Konfiguration von Service Composer verwaltete Regeln enthält, werden diese nach dem Import überschrieben.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Firewall**.
- 2 Stellen Sie sicher, dass Sie sich auf der Registerkarte **Allgemein (General)** befinden, um eine L3-Firewallkonfiguration zu laden. Klicken Sie auf die Registerkarte **Ethernet**, um eine L2-Firewallkonfiguration zu laden.
- 3 Klicken Sie auf das Symbol **Konfiguration laden (Load configuration)** ().
- 4 Wählen Sie die zu ladende Konfiguration aus und klicken Sie auf **OK**.

Die aktuelle Konfiguration wird durch die ausgewählte Konfiguration ersetzt.


### Nächste Schritte

Falls Service Composer-Regeln in Ihrer Konfiguration von der geladenen Konfiguration überschrieben werden, klicken Sie in Service Composer auf der Registerkarte „Sicherheitsrichtlinien“ auf **Aktionen (Actions) > Firewallregeln synchronisieren (Synchronize Firewall Rules)**.

## Filtern der Firewallregeln


Ihnen steht eine große Anzahl an Filterkategorien für Ihren Regelsatz zur Verfügung, mit denen sich die Regeln einfach modifizieren lassen. Regeln können nach virtuellen Quell- oder Zielmaschinen, IP-Adresse, Regelaktion, Protokollierung, Regelname, Anmerkungen und Regel-ID gefiltert werden.

### Verfahren

- 1 Klicken Sie auf der Registerkarte „Firewall“ auf das Symbol **Filter anwenden (Apply Filter)** ()
- 2 Geben Sie die Filterkriterien ein bzw. wählen Sie sie aus.
- 3 Klicken Sie auf **Übernehmen (Apply)**.

Regeln, die Ihren Filterkriterien entsprechen, werden angezeigt.

### Nächste Schritte

Um wieder alle Regeln anzuzeigen, klicken Sie auf das Symbol **Angewendeten Filter entfernen (Remove applied filter)** ()

## Ändern der Reihenfolge einer Firewallregel



Firewallregeln werden in der Reihenfolge, in der sie in der Regeltabelle aufgeführt sind, angewendet.

Die Regeln werden in der folgenden Reihenfolge angezeigt (und durchgesetzt):

- 1 Benutzerdefinierte Vorab-Regeln haben die höchste Priorität und werden in absteigender Reihenfolge erzwungen, mit Priorität auf der Ebene der jeweiligen virtuellen Netzwerkkarte.
- 2 Auto Plumbed-Regeln
- 3 Lokale Regeln, die auf einer NSX Edge-Ebene definiert sind
- 4 Service Composer-Regeln – ein getrennter Abschnitt für jede Richtlinie Sie können diese Regeln nicht in der Firewalltabelle bearbeiten, aber Sie können Regeln oben im Bereich für Firewallregeln innerhalb einer Sicherheitsrichtlinie hinzufügen. Dabei müssen Sie die Regeln in Service Composer erneut synchronisieren. Weitere Informationen finden Sie unter [Kapitel 17 Service Composer](#).
- 5 Standardregel für die verteilte Firewall

Sie können eine benutzerdefinierte Regel in der Tabelle nach oben oder nach unten verschieben. Die Standardregel befindet sich immer am Ende der Tabelle und kann nicht verschoben werden.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **Firewall** die zu verschiebende Regel aus.
- 2 Klicken Sie auf das Symbol **Regel nach oben verschieben (Move rule up)** () oder **Regel nach unten verschieben (Move rule down)** ()
- 3 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Löschen einer Firewallregel

Sie können Firewallregeln, die Sie erstellt haben, löschen. Es ist nicht möglich, die Standardregel oder von Service Composer verwaltete Regeln zu löschen.

### Verfahren

- 1 Wählen Sie eine Regel auf der Registerkarte **Firewall** aus.
- 2 Klicken Sie oberhalb der Firewalltabelle auf das Symbol **Ausgewählte Regel löschen (Delete selected rule)** (✖).
- 3 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Firewallprotokolle

Die Firewall generiert und speichert Protokolldateien, wie z. B. das Audit-, Regelmeldungs- und Systemereignisprotokoll. Sie müssen einen Syslog-Server für jedes Cluster konfigurieren, für das eine Firewall aktiviert ist. Der Syslog-Server wird im Attribut `Syslog.global.logHost` angegeben.

Die Firewall generiert Protokolle, wie in der folgenden Tabelle beschrieben.

**Tabelle 10-4. Firewallprotokolle**

Protokolltyp	Beschreibung	Speicherort
Regelmeldungsprotokolle	Schließen alle Zugriffsentscheidungen wie etwa zugelassener oder verweigerter Datenverkehr für jede Regel ein, falls die Protokollierung aktiviert wurde. Enthält die DFW-Paketprotokolle für die Regeln, für die die Protokollierung aktiviert wurde.	<code>/var/log/dfwpktlogs.log</code>
Überwachungsprotokolle	Schließen Verwaltungsprotokolle und Konfigurationsänderungen für die verteilte Firewall ein.	<code>/home/secureall/secureall/logs/vsm.log</code>
Systemereignisprotokolle	Schließen die angewendete Konfiguration der verteilten Firewall, erstellte, gelöschte oder fehlgeschlagene Filter, zu Sicherheitsgruppen hinzugefügte virtuelle Maschinen usw. ein.	<code>/home/secureall/secureall/logs/vsm.log</code>
Datenebene-/VMKernel-Protokolle	Erfassen die Aktivitäten in Verbindung mit einem Firewall-Kernel-Modul (VSIP). Sie enthalten Protokolleinträge für Mails, die vom System generiert werden.	<code>/var/log/vmkernel.log</code>
Nachrichtenbus-Client-/VSFWD-Protokolle	Erfassen die Aktivitäten eines Firewall-Agenten.	<code>/var/log/vsfwd.log</code>

**Hinweis** Um auf die Datei `vsm.log` zuzugreifen, führen Sie den Befehl `show log manager` in der NSX Manager-Befehlszeilenschnittstelle aus und anschließend den Befehl `grep` für das Schlüsselwort `vsm.log`. Diese Datei ist nur für den Benutzer bzw. die Benutzergruppe mit `root`-Rechten zugänglich.

## Regelmeldungsprotokolle

Regelmeldungsprotokolle schließen alle Zugriffsentscheidungen wie etwa zugelassener oder verweigerter Datenverkehr für jede Regel ein, falls die Protokollierung aktiviert wurde. Diese Protokolle werden auf jedem Host unter `/var/log/dfwpktlogs.log` gespeichert.

Hier sind Beispiele für Firewallprotokollmeldungen:

```
more /var/log/dfwpktlogs.log
2015-03-10T03:22:22.671Z INET match DROP domain-c7/1002 IN 242 UDP 192.168.110.10/138-
>192.168.110.255/138

more /var/log/dfwpktlogs.log
2017-04-11T21:09:59.877Z ESXi_FQDN dfwpktlogs: 50047 INET TERM domain-c1/1001 IN TCP RST
10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070
```

Weitere Beispiele:

```
2017-10-19T22:38:05.586Z 58734 INET match PASS domain-c8/1006 OUT 84 ICMP 172.18.8.121->172.18.8.119
RULE_TAG
2017-10-19T22:38:08.723Z 58734 INET match PASS domain-c8/1006 OUT 60 TCP 172.18.8.121/36485-
>172.18.8.119/22 S RULE_TAG
2017-10-19T22:38:18.785Z 58734 INET TERM domain-c8/1006 OUT ICMP 8 0 172.18.8.121->172.18.8.119 2/2
168/168 RULE_TAG
2017-10-19T22:38:20.789Z 58734 INET TERM domain-c8/1006 OUT TCP FIN 172.18.8.121/36484-
>172.18.8.119/22 44/33 4965/5009 RULE_TAG
```

Im nachfolgenden Beispiel:

- 1002 ist die ID der Verteilten Firewall.
- „domain-c7“ ist die Cluster-ID im von vCenter verwalteten Objektbrowser (MOB).
- 192.168.110.10/138 ist die Quell-IP-Adresse.
- 192.168.110.255/138 ist die Ziel-IP-Adresse.
- *RULE\_TAG* ist ein Beispiel für den Text, den Sie im Textfeld **Tag** eingeben, wenn Sie die Firewallregel hinzufügen oder bearbeiten.

Im folgenden Beispiel wird das Ergebnis eines Ping-Befehls von 192.168.110.10 auf 172.16.10.12 angezeigt.

```
tail -f /var/log/dfwpktlogs.log | grep 192.168.110.10

2015-03-10T03:20:31.274Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
2015-03-10T03:20:35.794Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
```

Die folgenden Tabellen erläutern die Textfelder der Firewallprotokollmeldung.

**Tabelle 10-5. Komponenten eines Eintrags in der Protokolldatei**

Komponente	Wert im Beispiel
Zeitstempel	2017-04-11T21:09:59
Firewallspezifischer Teil	877Z ESXi_FQDN dfwpklogs: 50047 INET TERM domain-c1/1001 IN TCP RST 10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070

**Tabelle 10-6. Firewallspezifischer Teil des Eintrags der Protokolldatei**

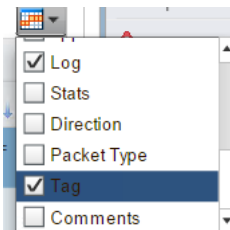
Element	Mögliche Werte
Filter-Hash	Eine Zahl, mit der der Filtername und andere Informationen abgerufen werden können.
AF-Wert	INET, INET6
Grund	<ul style="list-style-type: none"> <li>■ match: Paket stimmt mit einer Regel überein.</li> <li>■ bad-offset: interner Datenpfadfehler beim Erhalt des Pakets.</li> <li>■ fragment: die nicht-ersten Fragmente, nachdem sie zum ersten Fragment zusammengesetzt wurden.</li> <li>■ short: Paket zu kurz (z. B. unvollständig, IP-Header oder TCP/UDP-Header fehlt).</li> <li>■ normalize: falsch formatierte Pakete ohne korrekten Header oder Payload.</li> <li>■ memory: Datenpfad ohne Speicher.</li> <li>■ bad-timestamp: ungültiger TCP-Zeitstempel.</li> <li>■ proto-cksum: falsche Protokollprüfsumme.</li> <li>■ state-mismatch: TCP-Pakete, die die TCP-Status-Maschinenprüfung nicht bestehen.</li> <li>■ state-insert: doppelte Verbindung gefunden.</li> <li>■ state-limit: maximale Anzahl an Status erreicht, die ein Datenpfad nachverfolgen kann.</li> <li>■ SpoofGuard: Paket von SpoofGuard verworfen.</li> <li>■ TERM: Eine Verbindung wird beendet.</li> </ul>
Aktion	<ul style="list-style-type: none"> <li>■ PASS: Paket wird angenommen.</li> <li>■ DROP: Paket wird verworfen.</li> <li>■ NAT: SNAT-Regel.</li> <li>■ NONAT: Stimmt mit SNAT-Regel überein, kann die Adresse aber nicht übersetzen.</li> <li>■ RDR: DNAT-Regel.</li> <li>■ NORDR: Stimmt mit DNAT-Regel überein, kann die Adresse aber nicht übersetzen.</li> <li>■ PUNT: Sendet das Paket zu einer Dienst-VM, die auf demselben Hypervisor der aktuellen virtuellen Maschine ausgeführt wird.</li> <li>■ REDIRECT: Sendet das Paket zu einem Netzwerkdienst, der auf einem anderen Hypervisor als der der aktuellen virtuellen Maschine ausgeführt wird.</li> <li>■ COPY: Nimmt das Paket an und sendet eine Kopie davon zu einer Dienst-VM, die auf demselben Hypervisor der aktuellen virtuellen Maschine ausgeführt wird.</li> <li>■ REJECT: Weist das Paket zurück.</li> </ul>
Regelsatz und Regel-ID	<i>Regelsatz/Regel-ID</i>
Richtung	IN, OUT
Paketlänge	<i>length</i>

**Tabelle 10-6. Firewallspezifischer Teil des Eintrags der Protokolldatei (Fortsetzung)**

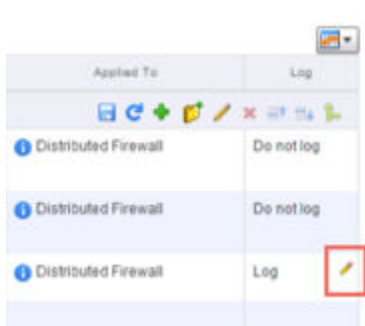
Element	Mögliche Werte
Protokoll	<p>TCP, UDP, ICMP oder PROTO (Protokollnummer)</p> <p>Bei TCP-Verbindungen wird der tatsächliche Grund für das Beenden einer Verbindung nach dem Schlüsselwort TCP angezeigt.</p> <p>Wenn TERM der Grund für eine TCP-Sitzung ist, wird in der Zeile PROTO eine zusätzliche Erläuterung angezeigt. Zu möglichen Gründen für das Beenden einer TCP-Verbindung gehören: RST (TCP-RST-Paket), FIN (TCP-FIN-Paket) und TIMEOUT (zu lange inaktiv).</p> <p>Im o. g. Beispiel ist es <i>RST</i>. Das bedeutet, dass in der Verbindung ein <i>RST</i>-Paket vorhanden ist, das zurückgesetzt werden muss.</p> <p>Bei anderen Verbindungen als TCP-Verbindungen (UDP, ICMP oder andere Protokolle) gibt es als Grund für das Beenden einer Verbindung nur TIMEOUT.</p>
Quell-IP-Adresse und -Port	<i>IP address/port</i>
Ziel-IP-Adresse und -Port	<i>IP address/port</i>
TCP-Flags	S (SYN), SA (SYN-ACK), A (ACK), P (PUSH), U (URGENT), F (FIN), R (RESET)
Anzahl an Paketen	<p>Anzahl an Paketen.</p> <p>22/14 – eingehende Pakete/ausgehende Pakete</p>
Anzahl an Bytes	<p>Anzahl an Bytes.</p> <p>7684/1070 – eingehende Bytes/ausgehende Bytes</p>

Um eine Regelmeldung zu aktivieren, melden Sie sich bei vSphere Web Client an.

- 1 Aktivieren Sie die Spalte **Protokoll** auf der Seite **Networking & Security > Firewall**.



- 2 Sie aktivieren die Protokollierung für eine Regel, indem Sie den Mauszeiger über einer Zelle in der Protokolltabelle halten und auf das Bleistiftsymbol klicken.



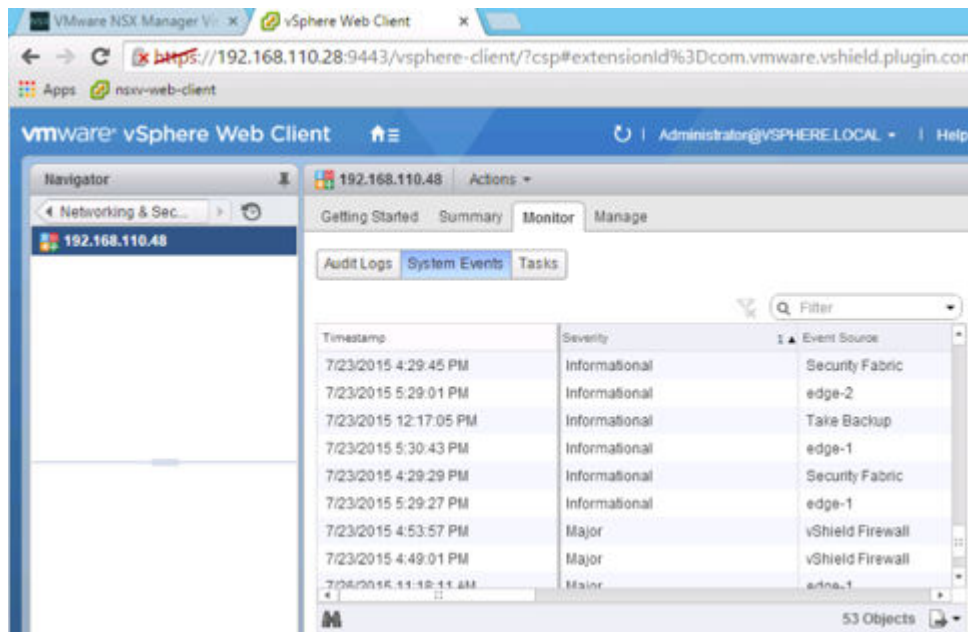
**Hinweis** Um benutzerdefinierten Text in der Firewallprotokollmeldung anzuzeigen, aktivieren Sie die Spalte **Tag** und klicken Sie auf das Stiftsymbol, um den gewünschten Text hinzuzufügen.

## Audit- und Systemereignisprotokolle

Überwachungsprotokolle schließen Verwaltungsprotokolle und Konfigurationsänderungen für die verteilte Firewall ein. Diese werden unter `/home/secureall/secureall/logs/vsm.log` gespeichert.

Systemereignisprotokolle schließen die angewendete Konfiguration der verteilten Firewall, erstellte, gelöschte oder fehlgeschlagene Filter, zu Sicherheitsgruppen hinzugefügte virtuelle Maschinen usw. ein. Diese Protokolle werden unter `/home/secureall/secureall/logs/vsm.log` gespeichert.

Navigieren Sie zum Anzeigen von Audit- und Systemereignisprotokollen in der Benutzeroberfläche zu **Networking & Security > Installation > Verwaltung** und doppelklicken Sie auf die IP-Adresse von NSX Manager. Klicken Sie dann auf die Registerkarte **Überwachen**.



Weitere Informationen finden Sie unter *NSX-Protokollierung und -Systemereignisse*.

# Überblick über die identitätsbasierte Firewall (IDFW)

11

Mit den Funktionen für eine identitätsbasierte Firewall haben NSX-Administratoren die Möglichkeit, benutzerspezifische DFW-Regeln für Active Directory zu erstellen.

Ein Überblick auf oberster Ebene über den Workflow der IDFW-Konfiguration beginnt mit der Vorbereitung der Infrastruktur. Dazu gehört die Installation der Komponenten der Hostvorbereitung in jedem geschützten Cluster durch den Administrator und die Einrichtung der Active Directory-Synchronisierung, damit NSX AD-Benutzer und -Gruppen verwenden kann. Als Nächstes muss IDFW wissen, bei welchem Desktop sich ein Active Directory-Benutzer anmeldet, um die DFW-Regeln zuzuweisen. Für IDFW stehen zwei Methoden zur Erkennung der Anmeldung zur Verfügung: Guest Introspection und/oder der Active Directory Event Log Scraper. Guest Introspection wird für ESXi-Cluster bereitgestellt, auf denen virtuelle IDFW-Maschinen ausgeführt werden. Wenn durch einen Benutzer Netzwerkereignisse generiert werden, leitet ein in der VM installierter Gastagent die Informationen über das Guest Introspection-Framework an den NSX Manager weiter. Die zweite Option ist der Active Directory Event Log Scraper. Konfigurieren Sie den Active Directory Event Log Scraper im NSX Manager so, dass auf eine Instanz in Ihrem Active Directory-Domänen-Controller verwiesen wird. NSX Manager übernimmt dann die Ereignisse aus dem AD-Sicherheitsereignisprotokoll. Sie können beide oder eine von beiden Methoden in Ihrer Umgebung verwenden. Beachten Sie, dass wenn sowohl der AD Event Log Scraper als auch Guest Introspection eingesetzt wird, beide voneinander abhängig sind: Wenn ein Modul nicht mehr funktioniert, stellt das andere kein Backup dafür dar.

Nach der Vorbereitung der Infrastruktur erstellt der Administrator NSX-Sicherheitsgruppen (Security Groups) und fügt die neu verfügbaren AD-Gruppen hinzu (als „Verzeichnisgruppen“ bezeichnet). Der Administrator kann dann Sicherheitsrichtlinien mit zugeordneten Firewallregeln erstellen und diese Richtlinien auf die neu erstellten Sicherheitsgruppen anwenden. Wenn sich jetzt ein Benutzer bei einem Desktop anmeldet, ermittelt das System das Ereignis sowie die verwendete IP-Adresse, sucht die Firewallrichtlinie, die diesem Benutzer zugeordnet ist, und überträgt diese Regeln. Dies gilt für physische wie für virtuelle Desktops. Für physische Desktops wird der AD Event Log Scraper auch für die Ermittlung benötigt, ob ein Benutzer bei einem physischen Desktop angemeldet ist.

## Betriebssystem-unterstützt mit IDFW

AD-unterstützte Server

- Windows 2012

- Windows 2008
- Windows 2008 R2

Gastbetriebssystem-unterstützt

- Windows 2012
- Windows 2008
- Windows 2008 R2
- Windows 10
- Windows 8 32/64
- Windows 7 32/64

Dieses Kapitel enthält die folgenden Themen:

- [Workflow für die identitätsbasierte Firewall](#)

## Workflow für die identitätsbasierte Firewall

Die identitätsbasierte Firewall (IDFW) ermöglicht die Verwendung von benutzerbasierten Regeln für die verteilte Firewall (Distributed Firewall, DFW).

Benutzerbasierte Regeln für die verteilte Firewall werden von der Mitgliedschaft in einer Active Directory-Gruppe bestimmt. IDFW prüft, wo Active Directory-Benutzer angemeldet sind, und ordnet die Anmeldungen jeweils einer IP-Adresse zu, die von der DFW zur Anwendung der Firewallregeln verwendet wird. Die identitätsbasierte Firewall erfordert entweder ein Guest Introspection-Framework oder Active Directory Event Log Scraping.

### Verfahren

- 1 Zur Konfiguration der Active Directory-Synchronisierung in NSX finden Sie Erläuterungen unter [Synchronisieren einer Windows-Domäne mit Active Directory](#). Diese ist für die Verwendung von Active Directory-Gruppen in Service Composer erforderlich.
- 2 Bereiten Sie den ESXi-Cluster für die DFW vor. Informationen dazu erhalten Sie unter „Vorbereiten des Host-Clusters für NSX“ in der Dokumentation *Installationshandbuch für NSX*.
- 3 Konfigurieren Sie die Optionen zur Ermittlung der IDFW-Anmeldung. Eine oder beide der folgenden Optionen müssen konfiguriert werden.

---

**Hinweis** Wenn Sie über eine Active Directory-Architektur mit mehreren Domänen verfügen und Log Scraper aufgrund von Sicherheitsbeschränkungen nicht verfügbar ist, verwenden Sie Guest Introspection für die Erstellung von An- und Abmeldeereignissen.

---

- Konfigurieren Sie den Zugriff auf das Active Directory-Ereignisprotokoll. Weitere Informationen dazu finden Sie unter [Registrieren einer Windows-Domäne mit NSX Manager](#).

- Windows-Gastbetriebssystem mit installiertem Gastagenten. Dieser ist in einer vollständigen Installation von VMware Tools <sup>™</sup> enthalten. Stellen Sie den Guest Introspection-Dienst für geschützte Cluster bereit. Weitere Informationen dazu finden Sie unter [Installieren von Guest Introspection auf Hostclustern](#). Informationen zur Fehlerbehebung für Guest Introspection finden Sie unter [Erfassen von Daten zur Fehlerbehebung für Guest Introspection](#).

# Arbeiten mit Active Directory-Domänen

# 12

Sie können eine oder mehrere Windows-Domänen bei einem NSX Manager und dem zugeordneten vCenter Server registrieren. NSX Manager ruft Gruppen- und Benutzerinformationen sowie die Beziehung zwischen diesen aus jeder Domäne ab, die bei NSX Manager registriert ist. NSX Manager ruft außerdem Active Directory-Anmeldedaten (AD) ab.

Sobald NSX Manager AD-Anmeldedaten abrufen, können Sie auf der Benutzeridentität basierende Sicherheitsgruppen und identitätsbasierte Firewallregeln erstellen sowie Activity Monitoring-Berichte ausführen.

Dieses Kapitel enthält die folgenden Themen:


- [Registrieren einer Windows-Domäne mit NSX Manager](#)
- [Synchronisieren einer Windows-Domäne mit Active Directory](#)
- [Bearbeiten einer Windows-Domäne](#)
- [Aktivieren des Nur-Lese-Zugriffs auf Sicherheitsprotokolle auf Windows 2008](#)
- [Überprüfen der Verzeichnisrechte](#)

## Registrieren einer Windows-Domäne mit NSX Manager

### Voraussetzungen

Das Domänenkonto muss über AD-Leseberechtigung für alle Objekte in der Domänenstruktur verfügen. Das Konto des Ereignisprotokolllesers muss über Leseberechtigungen für Sicherheits-Ereignisprotokolle verfügen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf die Registerkarte **Domäne (Domain)** und anschließend auf das Symbol **Domäne hinzufügen (Add domain)** (  ).

- 5 Geben Sie im Dialogfeld **Domäne hinzufügen (Add Domain)** den vollqualifizierten Domänennamen (z. B. eng.vmware.com) und den netBIOS-Namen für die Domäne ein.

Um den netBIOS-Namen für die Domäne abzurufen, geben Sie `nbtstat -n` in einem Befehlsfenster auf einer Windows-Workstation ein, die Teil einer Domäne ist oder die sich auf einem Domänencontroller befindet. In der lokalen NetBIOS-Namentabelle ist der Eintrag mit einem Präfix <00> und dem Typ „Gruppe“ der netBIOS-Name.

- 6 Wenn Sie eine untergeordnete Domäne hinzufügen, wählen Sie die Funktion **Automatisch zusammenführen (Auto Merge)** aus.
- 7 Klicken Sie während der Synchronisierung zum Herausfiltern von Benutzern, die über kein aktives Konto mehr verfügen, auf **Deaktivierte Benutzer ignorieren (Ignore disabled users)**.
- 8 Klicken Sie auf **Weiter (Next)**.
- 9 Geben Sie auf der Seite „LDAP-Optionen“ den Domänencontroller an, mit dem die Domäne synchronisiert werden soll, und wählen Sie das Protokoll aus.
- 10 Bearbeiten Sie die Portnummer, falls erforderlich.
- 11 Geben Sie die Anmeldedaten für das Domänenkonto ein. Dieser Benutzer muss auf die Verzeichnisstruktur zugreifen können.
- 12 Klicken Sie auf **Weiter (Next)**.
- 13 (Optional) Wählen Sie auf der Seite „Zugriff auf Sicherheits-Ereignisprotokoll“ entweder **CIFS** oder **WMI** als Verbindungsmethode für den Zugriff auf Sicherheits-Ereignisprotokolle auf dem angegebenen AD-Server aus. Ändern Sie die Portnummer, falls erforderlich. Dieser Schritt wird von Active Directory Event Log Scraper verwendet. Weitere Informationen dazu finden Sie unter [Workflow für die identitätsbasierte Firewall](#).

---

**Hinweis** Der Ereignisprotokollleser sucht im AD-Sicherheitseignisprotokoll nach Ereignissen mit den folgenden IDs: Windows 2008/2012: 4624, Windows 2003: 540. Der Ereignisprotokoll-Server ist auf 128 MB beschränkt. Wenn diese Obergrenze erreicht wird, ist eventuell die Ereignis-ID 1104 im Sicherheitsprotokollleser enthalten. Weitere Informationen hierzu finden Sie unter <https://technet.microsoft.com/en-us/library/dd315518>.

---

- 14 Wählen Sie **Anmeldedaten der Domäne verwenden (Use Domain Credentials)** aus, um die Anmeldedaten für den LDAP-Server zu verwenden. Um ein anderes Domänenkonto für den Zugriff auf die Protokolle anzugeben, heben Sie die Auswahl **Anmeldedaten der Domäne verwenden (Use Domain Credentials)** auf und geben Sie den Benutzernamen und das Kennwort an.

Das angegebene Konto muss die Sicherheits-Ereignisprotokolle auf dem Domänencontroller, der in Schritt 10 angegeben wurde, lesen können.

- 15 Klicken Sie auf **Weiter (Next)**.
- 16 Überprüfen Sie die eingegebenen Einstellungen auf der Seite „Bereit zum Abschließen“.

## 17 Klicken Sie auf **Beenden (Finish)**.

### Achtung

- Wenn eine Fehlermeldung anzeigt, dass das Hinzufügen einer Domäne für die Einheit aufgrund eines Domänenkonflikts nicht möglich ist, wählen Sie die Funktion „Automatisch zusammenführen“ aus. Die Domänen werden erstellt, und die Einstellungen werden unterhalb der Domänenliste angezeigt.

### Ergebnisse

Die Domäne wird erstellt und ihre Einstellungen werden unter der Domänenliste angezeigt.

### Nächste Schritte

Vergewissern Sie sich, dass Anmeldeereignisse auf dem Ereignisprotokoll-Server aktiviert sind.

Sie können LDAP-Server hinzufügen, bearbeiten, löschen, aktivieren oder deaktivieren, indem Sie die Registerkarte **LDAP-Server (LDAP Servers)** im Bereich unter der Domänenliste auswählen. Sie können dieselben Aufgaben für Ereignisprotokoll-Server ausführen, indem Sie die Registerkarte **Ereignisprotokoll-Server (Event Log Servers)** im Bereich unter der Domänenliste auswählen. Wenn Sie mehr als einen Windows-Server (Domänencontroller, Exchange Server oder Dateiserver) als Ereignisprotokoll-Server auswählen, wird dadurch die Zuordnung der Benutzeridentität verbessert.

**Hinweis** Wenn Sie IDFW verwenden, werden nur AD-Server unterstützt.

## Synchronisieren einer Windows-Domäne mit Active Directory

Standardmäßig werden alle registrierten Domänen automatisch alle drei Stunden mit Active Directory synchronisiert. Sie können auch bei Bedarf synchronisieren.

Über die vSphere Web Client-Benutzeroberfläche können Sie eine erzwungene Synchronisierung für Active Directory-Domänen durchführen. Es wird regelmäßig einmal wöchentlich eine automatische Synchronisierung durchgeführt. Alle drei Stunden erfolgt außerdem eine Delta-Synchronisierung. Es ist nicht möglich, untergeordnete Strukturen über die Benutzeroberfläche selektiv zu synchronisieren.

Mit NSX 6.4 und höher ist es möglich, untergeordnete Active Directory-Strukturen über API-Aufrufe selektiv zu synchronisieren. Die Rootdomäne darf keine über-/untergeordneten Beziehungen haben und muss einen gültigen definierten Namen (Distinguished Name) für das Verzeichnis aufweisen.



- `/api/1.0/directory/updateDomain` bietet eine Option, den Ordner unter der Rootdomäne anzugeben. Außerdem gibt es eine Möglichkeit, eine erzwungene Aktualisierung `private boolean forceUpdate` durchzuführen.
- `/api/directory/verifyRootDN`. Stellen Sie sicher, dass die RootDN-Liste keine über-/untergeordneten Beziehungen aufweist. Stellen Sie sicher, dass jeder RootDN ein gültiger Active Directory-DN ist.

**Verfahren**

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > System > Benutzer und Domänen (Users and Domains)**.
- 2 Klicken Sie auf die Registerkarte **Domains** und wählen Sie dann die zu synchronisierende Domäne aus.

**Wichtig** Alle Änderungen, die Sie in Active Directory vornehmen, werden in NSX Manager NICHT angezeigt, außer es wurde eine Delta- oder vollständige Synchronisierung durchgeführt.

- 3 Wählen Sie eine der folgenden Optionen aus:

Klicken Sie auf	Zweck
	Durchführen einer Delta-Synchronisierung, bei der lokale AD-Objekte, die sich seit der letzten Synchronisierung geändert haben, aktualisiert werden
	Durchführen einer vollständigen Synchronisierung, bei der der lokale Zustand aller AD-Objekte aktualisiert wird

## Bearbeiten einer Windows-Domäne

Sie können den Namen, den netBIOS-Namen, den primären LDAP-Server und die Kontoanmeldeinformationen einer Domäne bearbeiten.

**Verfahren**

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten (Manage)**.
- 4 Wählen Sie eine Domäne aus und klicken Sie anschließend auf das Symbol **Domäne bearbeiten (Edit domain)**.
- 5 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **Beenden (Finish)**.

## Aktivieren des Nur-Lese-Zugriffs auf Sicherheitsprotokolle auf Windows 2008

Der Nur-Lese-Zugriff auf Sicherheitsprotokolle wird vom Event Log Scraper in IDFW verwendet.

Nach dem Erstellen eines neuen Benutzerkontos müssen Sie den Nur-Lese-Zugriff auf Sicherheitsprotokolle auf einem Domänenabschnitt, der auf Windows 2008 Server basiert, aktivieren, um dem Benutzer einen Nur-Lese-Zugriff erteilen zu können.

---

**Hinweis** Dabei müssen Sie die nachfolgend dargestellten Schritte auf einem Domänen-Controller der Domäne, der Struktur oder der Gesamtstruktur durchführen.

---

### Verfahren

- 1 Wechseln Sie zu **Start > Verwaltungstools > Active Directory-Benutzer und -Computer (Start > Administrative Tools > Active Directory Users and Computers)**.
- 2 In der Navigationsstruktur erweitern Sie den Knoten für die Domäne, für die Sie den Zugriff auf Sicherheitsprotokolle aktivieren möchten.
- 3 Unter dem erweiterten Knoten wählen Sie **Integriert (Builtin)** aus.
- 4 Doppelklicken Sie in der Gruppenliste auf **Ereignisprotokollleser (Event Log Readers)**.
- 5 Wählen Sie die Registerkarte **Mitglieder (Members)** im Dialogfeld „Eigenschaften der Ereignisprotokollleser“ aus.
- 6 Klicken Sie auf die Schaltfläche **Hinzufügen... (Add...)**.  
Das Dialogfeld „Benutzer, Kontakte, Computer oder Gruppen auswählen“ wird angezeigt.
- 7 Wenn Sie zuvor eine Gruppe für den Benutzer „AD-Leser“ erstellt haben, wählen Sie diese Gruppe im Dialogfeld aus. Wenn Sie nur den Benutzer und keine Gruppe erstellt haben, wählen Sie diesen Benutzer im Dialogfeld „Benutzer, Kontakte, Computer oder Gruppen auswählen“ aus.
- 8 Klicken Sie auf **OK**, um das Dialogfeld „Benutzer, Kontakte, Computer oder Gruppen auswählen“ zu schließen.
- 9 Klicken Sie auf **OK**, um das Dialogfenster „Eigenschaften der Ereignisprotokollleser“ zu schließen.
- 10 Schließen Sie das Fenster „Active Directory-Benutzer und -Computer“.

### Nächste Schritte

Nachdem Sie den Zugriff auf Sicherheitsprotokolle aktiviert haben, überprüfen Sie die Verzeichnisrechte mithilfe der in [Überprüfen der Verzeichnisrechte](#) dargestellten Schritte.

## Überprüfen der Verzeichnisrechte

Überprüfen Sie, ob das Benutzerkonto über die erforderlichen Rechte zum Lesen von Sicherheitsprotokollen verfügt.

Nachdem Sie ein neues Benutzerkonto erstellt und den Zugriff auf die Sicherheitsprotokolle aktiviert haben, müssen Sie sicherstellen, dass die Sicherheitsprotokolle gelesen werden können.

## Voraussetzungen

Aktivieren Sie den Zugriff auf die Sicherheitsprotokolle. Weitere Informationen dazu finden Sie unter [Aktivieren des Nur-Lese-Zugriffs auf Sicherheitsprotokolle auf Windows 2008](#).

## Verfahren

- 1 Melden Sie sich von einer beliebigen Workstation in der Domäne bei der Domäne als Administrator an.
- 2 Wechseln Sie zu **Start > Verwaltungstools > Ereignisanzeige (Start > Administrative Tools > Event Viewer)**.
- 3 Wählen Sie die Option **Verbindung mit anderem Computer herstellen... (Connect to Another Computer...)** im Menü **Aktion (Action)**. Das Dialogfeld „Computer auswählen“ wird eingeblendet. (Beachten Sie, dass Sie diesen Schritt auch durchführen müssen, wenn Sie bereits bei dem Computer angemeldet sind, für den Sie das Ereignisprotokoll anzeigen möchten.)
- 4 Aktivieren Sie das Optionsfeld **Anderer Computer (Another computer)**, wenn es noch nicht aktiviert ist.
- 5 In das Textfeld neben dem Optionsfeld **Anderer Computer (Another computer)** geben Sie den Namen des Domänen-Controllers ein. Alternativ klicken Sie auf die Schaltfläche **Durchsuchen... (Browse...)** und wählen Sie dann den Domänen-Controller in der Verzeichnisstruktur aus.
- 6 Aktivieren Sie das Kontrollkästchen **Verbindung unter anderem Benutzerkonto herstellen (Connect as another user)**.
- 7 Klicken Sie auf die Schaltfläche **Benutzer festlegen... (Set User...)**. Das Dialogfeld „Ereignisanzeige“ wird eingeblendet.
- 8 In das Feld **Benutzername (User name)** geben Sie den Benutzernamen für den von Ihnen erstellten Benutzer ein.
- 9 In das Feld **Kennwort (Password)** geben Sie das Kennwort für den von Ihnen erstellten Benutzer ein.
- 10 Klicken Sie auf **OK**.
- 11 Klicken Sie erneut auf **OK**.
- 12 Erweitern Sie den Knoten **Windows-Protokolle (Windows Logs)** in der Navigationsstruktur.
- 13 Wählen Sie unterhalb des Knotens **Windows-Protokolle (Windows Logs)** den Sicherheitsknoten aus. Wenn die Protokollereignisse angezeigt werden, verfügt das Konto über die erforderlichen Rechte.

# Verwenden von SpoofGuard

# 13

Nach der Synchronisierung mit vCenter Server erfasst NSX Manager auf allen virtuellen Maschinen die IP-Adressen aller virtuellen vCenter-Gastmaschinen aus VMware Tools. Wenn die Sicherheit einer virtuellen Maschine gefährdet wurde, kann die IP-Adresse manipuliert worden sein. Demzufolge könnten Übertragungen mit böswilligen Absichten Firewallrichtlinien umgehen.

Erstellen Sie eine SpoofGuard-Richtlinie für bestimmte Netzwerke. Dadurch können Sie die von VMware Tools gemeldeten IP-Adressen autorisieren und diese bei Bedarf ändern, um Manipulationen (Spoofing) zu verhindern. SpoofGuard vertraut standardmäßig den MAC-Adressen virtueller Maschinen, die aus VMX-Dateien und dem vSphere SDK erfasst werden. SpoofGuard wird getrennt von den Firewallregeln ausgeführt und kann zum Blockieren von Datenverkehr verwendet werden, der als manipuliert erkannt wurde.

SpoofGuard unterstützt sowohl IPv4- als auch IPv6-Adressen. Die SpoofGuard-Richtlinie unterstützt mehrere einer vNIC zugewiesenen IP-Adressen, wenn VMware Tools und das DHCP-Snooping verwendet werden. Wenn das ARP-Snooping aktiviert ist, werden mehrere IP-Adressen nicht unterstützt. Die SpoofGuard-Richtlinie überwacht und verwaltet die von Ihren virtuellen Maschinen gemeldeten IP-Adressen in einem der folgenden Modi.

## **IP-Zuweisungen automatisch bei erster Verwendung vertrauen**

Dieser Modus erlaubt die Durchleitung des gesamten, von Ihren virtuellen Maschinen ausgehenden Datenverkehrs. Dabei wird eine Zuweisungstabelle zwischen vNIC- und IP-Adressen erstellt. Sie können diese Tabelle überprüfen und IP-Adressenänderungen vornehmen. In diesem Modus werden automatisch alle IPv4- und IPv6-Adressen, die zuerst auf einer vNIC angezeigt werden, genehmigt.

## **Alle IP-Zuweisungen vor der Verwendung manuell überprüfen und genehmigen**

In diesem Modus wird der gesamte Datenverkehr so lange blockiert, bis Sie die jeweilige vNIC-zu-IP-Adressenzuweisung genehmigen. In diesem Modus können mehrere IPv4-Adressen genehmigt werden.

---

**Hinweis** SpoofGuard lässt standardmäßig DHCP-Anforderungen unabhängig vom aktivierten Modus zu. Im manuellen Prüfmodus wird der Datenverkehr allerdings erst durchgeleitet, nachdem die von DHCP zugewiesene IP-Adresse genehmigt wurde.

---

SpoofGuard beinhaltet eine systemgenerierte Standardrichtlinie, die auf Portgruppen und logische Netzwerke angewendet wird, die nicht anderen SpoofGuard-Richtlinien unterliegen. Ein neu hinzugefügtes Netzwerk wird automatisch zur Standardrichtlinie hinzugefügt, bis Sie das Netzwerk zu einer bestehenden Richtlinie hinzufügen oder eine neue Richtlinie dafür erstellen.

SpoofGuard ist eine der Möglichkeiten, die eine Richtlinie für eine verteilte Firewall von NSX verwenden kann, um die IP-Adresse einer virtuellen Maschine zu ermitteln. Weitere Informationen hierzu finden Sie unter [IP-Erkennung für virtuelle Maschinen](#).

Dieses Kapitel enthält die folgenden Themen:

- [Erstellen einer SpoofGuard-Richtlinie](#)
- [Genehmigen von IP-Adressen](#)
- [Bearbeiten einer IP-Adresse](#)
- [Löschen einer IP-Adresse](#)

## Erstellen einer SpoofGuard-Richtlinie

Sie können eine SpoofGuard-Richtlinie erstellen, um den Betriebsmodus für spezifische Netzwerke anzugeben. Die vom System generierte (Standard)-Richtlinie gilt für Portgruppen und logische Switches, die nicht von den bestehenden SpoofGuard-Richtlinien abgedeckt sind.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > SpoofGuard**.
- 2 Klicken Sie auf das Symbol **Hinzufügen (Add)**.
- 3 Geben Sie einen Namen für die Richtlinie ein.
- 4 Wählen Sie **Aktiviert (Enabled)** bzw. **Deaktiviert (Disabled)**, um anzugeben, ob die Richtlinie aktiviert ist.
- 5 Wählen Sie für **Betriebsmodus (Operation Mode)** eine der folgenden Optionen aus:

Option	Beschreibung
<b>IP-Zuweisungen automatisch bei erster Verwendung vertrauen</b>	Wählen Sie diese Option, um allen IP-Zuweisungen bei der erstmaligen Registrierung bei NSX Manager zu vertrauen.
<b>Alle IP-Zuweisungen vor der Verwendung manuell überprüfen und genehmigen</b>	Wählen Sie diese Option, um eine manuelle Genehmigung aller IP-Adressen anzufordern. Sämtlicher Datenverkehr von und zu nicht genehmigten IP-Adressen wird blockiert.

- 6 Klicken Sie auf **In diesem Namespace lokale Adressen als gültige Adressen zulassen (Allow local address as valid address in this namespace)**, um lokale IP-Adressen für Ihr Setup zuzulassen.

Wenn Sie eine virtuelle Maschine einschalten, die keine Verbindung mit dem DHCP-Server herstellen kann, wird ihr eine lokale IP-Adresse zugewiesen. Diese lokale IP-Adresse wird nur dann als gültig angesehen, wenn der SpoofGuard-Modus auf **In diesem Namespace lokale Adressen als gültige Adressen zulassen (Allow local address as valid address in this namespace)** festgelegt ist. Anderenfalls wird die lokale IP-Adresse ignoriert.

- 7 Klicken Sie auf **Weiter (Next)**.
- 8 Klicken Sie zum Angeben des Geltungsbereichs der Richtlinie auf **Hinzufügen (Add)** und wählen Sie die Netzwerke, verteilten Portgruppen oder logischen Switches aus, auf die diese Richtlinie angewendet werden soll.

Eine Portgruppe oder ein logischer Switch kann jeweils nur zu einer SpoofGuard-Richtlinie gehören.

- 9 Klicken Sie auf **OK** und anschließend auf **Beenden (Finish)**.

#### Nächste Schritte

Sie können eine Richtlinie bearbeiten, indem Sie auf das Symbol **Bearbeiten (Edit)** klicken. Klicken Sie zum Löschen einer Richtlinie auf das Symbol **Löschen (Delete)**.

## Genehmigen von IP-Adressen

Wenn Sie SpoofGuard auf das Anfordern einer manuellen Genehmigung aller IP-Adressenzuweisungen festlegen, müssen Sie IP-Adressenzuweisungen genehmigen, damit die Durchleitung von Datenverkehr von diesen virtuellen Maschinen zugelassen wird.

#### Verfahren

- 1 Wählen Sie auf der Registerkarte **SpoofGuard** eine Richtlinie aus.

Die Richtliniendetails werden unterhalb der Richtlinien-Tabelle angezeigt.

- 2 Klicken Sie in **Ansicht (View)** auf einen der Links für Optionen.

Option	Beschreibung
<b>Aktive virtuelle Netzwerkkarten</b>	Liste aller validierten IP-Adressen
<b>Aktive virtuelle Netzwerkkarten seit letzter Veröffentlichung</b>	Liste mit IP-Adressen, die seit dem letzten Update der Richtlinie validiert wurden.
<b>IP-Adressen virtueller Netzwerkkarten benötigen Genehmigung</b>	IP-Adressenänderung, die genehmigt werden muss, bevor Datenverkehr zu oder von diesen virtuellen Maschinen übertragen werden kann.
<b>Virtuelle Netzwerkkarten mit doppelter IP-Adresse</b>	IP-Adressen, die im ausgewählten Datacenter Duplikate einer vorhandenen zugewiesenen IP-Adresse sind

Option	Beschreibung
Inaktive virtuelle Netzwerkkarten	Liste mit IP-Adressen, bei denen die aktuelle IP-Adresse nicht der veröffentlichten IP-Adresse entspricht.
Nicht veröffentlichte IP-Adresse virtueller Netzwerkkarten	Liste virtueller Maschinen, deren IP-Adressenzuweisung Sie bearbeitet, aber noch nicht veröffentlicht haben.

3 Führen Sie einen der folgenden Schritte aus.

- Um eine einzelne IP-Adresse zu genehmigen, klicken Sie neben der IP-Adresse auf **Genehmigen (Approve)**.
- Um mehrere IP-Adressen zu genehmigen, wählen Sie die entsprechenden vNICs aus und klicken auf **Erkannte IP-Adresse(n) genehmigen (Approve Detected IP(s))**.

## Bearbeiten einer IP-Adresse

Sie können die einer MAC-Adresse zugewiesene IP-Adresse bearbeiten, um diese zu korrigieren.

**Hinweis** SpoofGuard lässt eine eindeutige IP-Adresse von virtuellen Maschinen zu. Sie können eine IP-Adresse jedoch nur einmal zuweisen. Eine genehmigte IP-Adresse ist im gesamten NSX-System eindeutig. Duplizierte genehmigte IP-Adressen sind nicht zulässig.

### Verfahren

1 Wählen Sie auf der Registerkarte **SpoofGuard** eine Richtlinie aus.

Die Richtliniendetails werden unterhalb der Richtlinien-Tabelle angezeigt.

2 Klicken Sie in **Ansicht (View)** auf einen der Links für Optionen.

Option	Beschreibung
Aktive virtuelle Netzwerkkarten	Liste aller validierten IP-Adressen
Aktive virtuelle Netzwerkkarten seit letzter Veröffentlichung	Liste mit IP-Adressen, die seit dem letzten Update der Richtlinie validiert wurden.
IP-Adressen virtueller Netzwerkkarten benötigen Genehmigung	IP-Adressenänderung, die genehmigt werden muss, bevor Datenverkehr zu oder von diesen virtuellen Maschinen übertragen werden kann.
Virtuelle Netzwerkkarten mit doppelter IP-Adresse	IP-Adressen, die im ausgewählten Datacenter Duplikate einer vorhandenen zugewiesenen IP-Adresse sind
Inaktive virtuelle Netzwerkkarten	Liste mit IP-Adressen, bei denen die aktuelle IP-Adresse nicht der veröffentlichten IP-Adresse entspricht.
Nicht veröffentlichte IP-Adresse virtueller Netzwerkkarten	Liste virtueller Maschinen, deren IP-Adressenzuweisung Sie bearbeitet, aber noch nicht veröffentlicht haben.

3 Klicken Sie für die entsprechende vNIC auf das Symbol **Bearbeiten (Edit)** und führen Sie die entsprechenden Änderungen durch.

4 Klicken Sie auf **OK**.

# Löschen einer IP-Adresse

Sie löschen eine genehmigte IP-Adresse von einer SpoofGuard-Richtlinie.

## Verfahren

- 1 Wählen Sie auf der Registerkarte **SpoofGuard** eine Richtlinie aus.

Die Richtliniendetails werden unterhalb der Richtlinien-Tabelle angezeigt.

- 2 Klicken Sie in **Ansicht (View)** auf einen der Links für Optionen.

Option	Beschreibung
<b>Aktive virtuelle Netzwerkkarten</b>	Liste aller validierten IP-Adressen
<b>Aktive virtuelle Netzwerkkarten seit letzter Veröffentlichung</b>	Liste mit IP-Adressen, die seit dem letzten Update der Richtlinie validiert wurden.
<b>IP-Adressen virtueller Netzwerkkarten benötigen Genehmigung</b>	IP-Adressenänderung, die genehmigt werden muss, bevor Datenverkehr zu oder von diesen virtuellen Maschinen übertragen werden kann.
<b>Virtuelle Netzwerkkarten mit doppelter IP-Adresse</b>	IP-Adressen, die im ausgewählten Datacenter Duplikate einer vorhandenen zugewiesenen IP-Adresse sind
<b>Inaktive virtuelle Netzwerkkarten</b>	Liste mit IP-Adressen, bei denen die aktuelle IP-Adresse nicht der veröffentlichten IP-Adresse entspricht.
<b>Nicht veröffentlichte IP-Adresse virtueller Netzwerkkarten</b>	Liste virtueller Maschinen, deren IP-Adressenzuweisung Sie bearbeitet, aber noch nicht veröffentlicht haben.

- 3 Führen Sie einen der folgenden Schritte aus.

- Klicken Sie zum Löschen einer einzelnen IP-Adresse neben der betreffenden IP-Adresse auf **Löschen (Clear)**.
- Wählen Sie zum Löschen mehrerer IP-Adressen die betreffenden vNICs aus und klicken Sie dann auf **Genehmigte IP-Adresse(n) bereinigen (Clear Approved IP(s))**.

# Virtual Private Networks (VPN)

# 14

NSX Edge unterstützt diverse Arten von VPNs. Mit SSL VPN-Plus können Remotebenutzer auf private Firmenanwendungen zugreifen. IPSec VPN bietet die Möglichkeit, durch eine Verbindung zwischen einer NSX Edge-Instanz und Remote-Sites verschiedene Sites miteinander zu verbinden. Mit L2 VPN können Sie Ihr Datacenter erweitern, indem Sie zulassen, dass virtuelle Maschinen die Netzwerkkonnektivität über geografische Grenzen hinaus wahren.

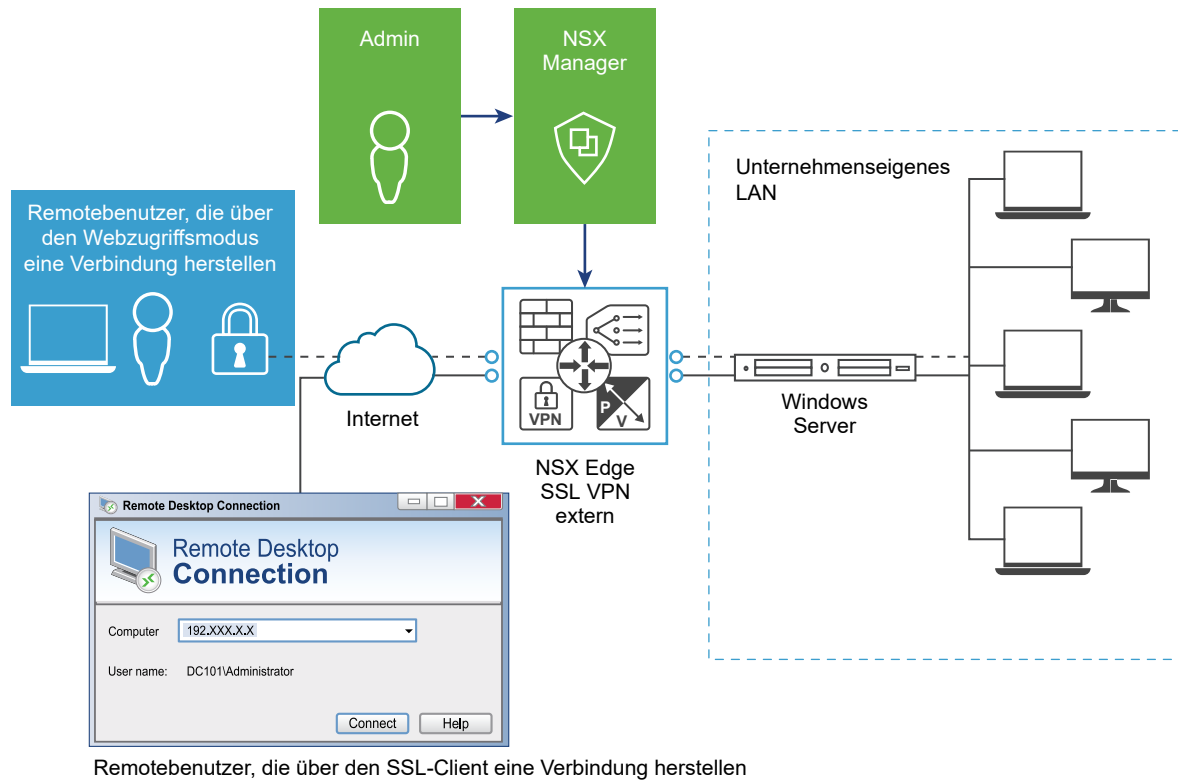
Bevor Sie VPN verwenden können, benötigen Sie eine funktionierende NSX Edge-Instanz. Weitere Informationen zur Einrichtung von NSX Edge finden Sie unter [Konfiguration von NSX Edge](#).

Dieses Kapitel enthält die folgenden Themen:

- [Überblick über SSL VPN-Plus](#)
- [Überblick über IPSec-VPN](#)
- [Überblick über L2 VPN](#)

## Überblick über SSL VPN-Plus

Mit SSL VPN-Plus können Remotebenutzer eine sichere Verbindung mit privaten Netzwerken hinter einem NSX Edge-Gateway herstellen. Remotebenutzer können auf Server und Anwendungen in den privaten Netzwerken zugreifen.



Die folgenden Client-Betriebssysteme werden unterstützt.

Betriebssystem	Unterstützte Versionen
Windows	8, 10 (einschließlich Windows 10 mit aktivierter Option „Sicherer Start“)
Mac OS Sierra	10.12.6
Mac OS High Sierra	10.13.4
Linux Fedora	26, 28
Linux CentOS	6.0, 7.5
Linux Ubuntu	18.04

### Wichtig

- SSL VPN-Plus Client wird auf Computern, die ARM-basierte Prozessoren verwenden, nicht unterstützt.
- Im SSL VPN-Plus Client unter Windows funktioniert die Funktion „automatische Neuverbindung“ nicht wie erwartet, wenn der Npcap-Loopback-Adapter „aktiviert“ ist. Dieser Loopback-Adapter beeinträchtigt die Funktion des Npcap-Treibers auf einem Windows-Computer. Stellen Sie sicher, dass die neueste Version des Npcap-Treibers (0.9983 oder höher) auf Ihrem Windows-Computer installiert ist. Für diese Version des Treibers ist kein Loopback-Adapter für Paketaufnahmen erforderlich.
- Linux TCL-, TK- und Network Security Services(NSS)-Bibliotheken sind erforderlich, damit die Benutzeroberfläche funktioniert.

## Konfigurieren von Network Access SSL VPN-Plus

Im Netzwerkzugriffsmodus kann ein Remotebenutzer auf private Netzwerke zugreifen, sobald er einen SSL-Client heruntergeladen und installiert hat.

### Voraussetzungen

Beim SSL VPN-Gateway muss Port 443 für externe Netzwerke zugänglich sein. Beim SSL VPN-Client müssen die IP-Adresse des NSX Edge-Gateways sowie Port 443 vom Clientsystem aus zugänglich sein.

### Hinzufügen von SSL VPN-Plus-Servereinstellungen

Sie müssen SSL VPN-Servereinstellungen hinzufügen, um auf einer NSX Edge-Schnittstelle SSL aktivieren zu können.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** aus dem linken Fensterbereich **Servereinstellungen (Server Settings)**.
- 2 Klicken Sie auf **Ändern (Change)**.
- 3 Wählen Sie die IPv4- oder IPv6-Adresse aus.
- 4 Bearbeiten Sie die Portnummer, falls erforderlich. Diese Portnummer ist für das Konfigurieren des Installationspakets erforderlich.
- 5 Wählen Sie eine oder mehrere Verschlüsselungsmethoden oder Verschlüsselungen aus.

---

**Hinweis** Wenn eine der folgenden GCM-Verschlüsselungen auf dem SSL-VPN-Server konfiguriert ist, kann bei einigen Browsern ein Problem mit der Abwärtskompatibilität auftreten:

- AES128-GCM-SHA256
  - ECDHE-RSA-AES128-GCM-SHA256
  - ECDHE-RSA-AES256-GCM-SHA38
- 

- 6 (Optional) Verwenden Sie aus der Tabelle „Serverzertifikate“ das Standard-Serverzertifikat oder deaktivieren Sie das Kontrollkästchen **Standardzertifikat verwenden (Use Default Certificate)** und klicken Sie auf das Serverzertifikat, das Sie hinzufügen möchten.
- 

### Einschränkung

- Der SSL VPN-Plus-Dienst unterstützt nur RSA-Zertifikate.
  - Der SSL VPN-Plus-Dienst unterstützt das Serverzertifikat, das nur durch Stamm-CA signiert ist. Serverzertifikate, die durch Zwischen-CA signiert sind, werden nicht unterstützt.
- 

- 7 Klicken Sie auf **OK**.

### Hinzufügen eines IP-Pools

Dem Remotebenutzer wird eine virtuelle IP-Adresse aus dem IP-Pool, den Sie hinzugefügt haben, zugewiesen.

## Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** aus dem linken Fensterbereich **IP-Pools (IP Pools)** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 3 Geben Sie die IP-Startadresse und die IP-Endadresse für den IP-Pool ein.
- 4 Geben Sie die Netzmaske des IP-Pools ein.
- 5 Geben Sie die IP-Adresse für die Routing-Schnittstelle des NSX Edge Gateways ein.
- 6 (Optional) Geben Sie eine Beschreibung für den IP-Pool ein.
- 7 Wählen Sie aus, ob der IP-Pool aktiviert oder deaktiviert werden soll.
- 8 (Optional) Geben Sie im Bereich **Erweitert (Advanced)** den DNS-Namen ein.
- 9 (Optional) Geben Sie den Namen des sekundären DNS ein.
- 10 Geben Sie das verbindungspezifische DNS-Suffix für die domänenbasierte Hostnamenauflösung ein.
- 11 Geben Sie Adresse des WINS-Servers ein.
- 12 Klicken Sie auf **OK**.

## Hinzufügen eines privaten Netzwerks

Fügen Sie das Netzwerk hinzu, auf das der Remotebenutzer zugreifen soll.

## Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Private Netzwerke (Private Networks)** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 3 Geben Sie die IP-Adresse des privaten Netzwerks ein.
- 4 Geben Sie die Netzmaske des privaten Netzwerks ein.
- 5 (Optional) Geben Sie eine Beschreibung für das Netzwerk ein.
- 6 Geben Sie an, ob Sie den privaten Netzwerk- und Internetdatenverkehr über das SSL VPN-Plus-aktivierte NSX Edge übertragen oder NSX Edge übergehen möchten, um den Datenverkehr direkt an den privaten Server zu übertragen.
- 7 Wenn Sie **Datenverkehr über den Tunnel senden (Send traffic over the tunnel)** ausgewählt haben, wählen Sie **TCP-Optimierung aktivieren (Enable TCP Optimization)** aus, um die Geschwindigkeit der Internetverbindung zu optimieren.

Bei einem konventionellen SSL VPNs-Tunnel mit vollem Zugriff werden TCP/IP-Daten in einem zweiten TCP/IP-Stack zwecks Verschlüsselung über das Internet übertragen. Dies führt dazu, dass Anwendungs-Schicht-Daten zweimal in zwei getrennten TCP-Streams gekapselt werden. Wenn Pakete verloren gehen (was auch unter optimalen Internetbedingungen passieren kann), tritt eine

Leistungsbeeinträchtigung mit der Bezeichnung „TCP-over-TCP Meltdown“ ein. Im Wesentlichen korrigieren zwei TCP-Instrumente ein einzelnes Paket von IP-Daten, was den Netzdurchsatz beeinträchtigt und Verbindungszeitüberschreitungen verursacht. Die TCP-Optimierung behebt dieses „TCP-over-TCP“-Problem und sorgt somit für eine optimierte Leistung.

- 8 Wenn die Optimierung aktiviert ist, geben Sie die Portnummern an, für die der Datenverkehr optimiert werden soll.

Der Datenverkehr für die verbleibenden Ports dieses spezifischen Netzwerks wird nicht optimiert.

---

**Hinweis** Wenn keine Portnummern angegeben werden, wird der Datenverkehr für alle Ports optimiert.

---

Wenn der TCP-Datenverkehr optimiert wird, wird die TCP-Verbindung im Namen des Clients vom SSL-VPN-Server geöffnet. Da die TCP-Verbindung vom SSL-VPN-Server geöffnet wird, wird die erste automatisch erstellte Regel angewendet, die das Passieren aller vom Edge geöffneten Verbindungen erlaubt. Auf den nicht optimierten Datenverkehr werden die normalen Edge-Firewall-Regeln angewendet. Die Standardregel ist „allow any any“.

- 9 Geben Sie an, ob Sie das private Netzwerk aktivieren oder deaktivieren möchten.
- 10 Klicken Sie auf **OK**.

### Nächste Schritte

Fügen Sie eine entsprechende Firewallregel hinzu, um den privaten Netzwerkdatenverkehr zuzulassen.

## Hinzufügen der Authentifizierung

Zusätzlich zur lokalen Benutzerauthentifizierung können Sie einen externen Authentifizierungsserver (AD, LDAP, Radius oder RSA) hinzufügen, der an das SSL-Gateway gebunden ist. Alle Benutzer mit Konten auf dem gebundenen Authentifizierungsserver werden authentifiziert.

Die maximale Zeit für die Authentifizierung über SSL VPN beträgt 3 Minuten. Der Grund dafür ist, dass die Zeitüberschreitung ohne Authentifizierung 3 Minuten beträgt und eine Eigenschaft ist, die nicht konfiguriert werden kann. Sie werden also in Szenarien, in denen die Zeitüberschreitung mit AD-Authentifizierung auf mehr als 3 Minuten festgelegt ist, oder wenn es mehrere Authentifizierungsserver in Ketten-Autorisierung gibt und die Zeit für eine Benutzerauthentifizierung mehr als 3 Minuten beträgt, nicht authentifiziert.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** die Option **Authentifizierung (Authentication)** aus dem linken Fensterbereich.
- 2 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 3 Wählen Sie den Typ des Authentifizierungsservers.

#### 4 Füllen Sie je nach ausgewähltem Typ des Authentifizierungsservers die folgenden Felder aus.

##### ◆ AD-Authentifizierungsserver

**Tabelle 14-1. AD-Authentifizierungsserveroptionen**

Option	Beschreibung
<b>SSL aktivieren (Enable SSL)</b>	Durch die Aktivierung von SSL wird ein verschlüsselter Link zwischen einem Webserver und einem Browser hergestellt.  <b>Hinweis</b> Wenn Sie SSL nicht aktivieren und versuchen, das Kennwort mithilfe der Registerkarte „SSL VPN-Plus“ oder vom Clientcomputer später zu ändern, kann es zu Problemen kommen.
<b>IP-Adresse (IP Address)</b>	IP-Adresse des Authentifizierungsservers.
<b>Port</b>	Zeigt den Standard-Portnamen an. Bearbeiten Sie den Eintrag, falls erforderlich.
<b>Zeitüberschreitung (Timeout)</b>	Zeitraum, innerhalb dessen der AD-Server antworten muss (in Sekunden).
<b>Status</b>	Wählen Sie <b>Aktiviert (Enabled)</b> bzw. <b>Deaktiviert (Disabled)</b> , um anzugeben, ob der Server aktiviert ist.
<b>Suchdatenbank (Search base)</b>	Teil der zu durchsuchenden externen Verzeichnisstruktur. Als Suchbasis sind Elemente wie Organisationseinheit (OU), Domänencontroller (DC) oder Domänenname (AD) des externen Verzeichnisses möglich.  Beispiele: <ul style="list-style-type: none"> <li>■ OU=Benutzer, DC=Aslan, DC=lokal</li> <li>■ OU=VPN, DC=Aslan, DC=lokal</li> </ul>
<b>Bind-DN (Bind DN)</b>	Benutzer auf dem externen AD-Server, der das AD-Verzeichnis innerhalb der definierten Suchdatenbank durchsuchen darf. Meistens darf der Bind-DN das gesamte Verzeichnis durchsuchen. Die Rolle des Bind-DN besteht darin, das Verzeichnis unter Verwendung des Abfragefilters und der Suchbasis für den DN (Distinguished Name) für authentifizierte AD-Benutzer abzufragen. Wenn der DN zurückgegeben wird, werden der DN und das Kennwort zum Authentifizieren des AD-Benutzers verwendet.  Beispiel: CN=ldap.edge,OU=Benutzer,OU=Datencenterbenutzer, DC=Aslan, DC=lokal
<b>Bind-Kennwort (Bind Password)</b>	Kennwort zum Authentifizieren des AD-Benutzers.
<b>Bind-Kennwort erneut eingeben (Retype Bind Password)</b>	Geben Sie das Kennwort erneut ein.
<b>Attributname für die Anmeldung (Login Attribute Name)</b>	Name, mit dem die vom Remotebenutzer eingegebene Benutzer-ID abgeglichen wird. Für Active Directory lautet der Attributname für die Anmeldung <b>sAMAccountName</b> .

**Tabelle 14-1. AD-Authentifizierungsserveroptionen (Fortsetzung)**

Option	Beschreibung
<b>Suchfilter (Search Filter)</b>	<p>Filterwerte, mit denen die Suche eingeschränkt werden soll. Das Format für Suchfilter lautet <i>attribute operator value</i>.</p> <p>Wenn Sie die Suchdatenbank auf eine bestimmte Gruppe in AD beschränken müssen und keine Suche im gesamten OU zulassen möchten,</p> <ul style="list-style-type: none"> <li>■ Platzieren Sie keine Gruppennamen innerhalb der Suchdatenbank, nur OU und DC.</li> <li>■ Fügen Sie dem String des Suchfilters <i>objectClass</i> und <i>memberOf</i> nicht gleichzeitig hinzu.</li> </ul> <p>Beispiel für das korrekte Format des Suchfilters: memberOf=CN=VPN_Users,OU=Users,DC=aslan,DC=local</p>
<b>Diesen Server für die sekundäre Authentifizierung verwenden (Use this server for secondary authentication)</b>	Bei Auswahl wird dieser AD-Server als zweite Authentifizierungsebene verwendet.
<b>Sitzung beenden, wenn Authentifizierung fehlschlägt (Terminate Session if authentication fails)</b>	Bei Auswahl wird die Sitzung beendet, falls die Authentifizierung fehlschlägt.

## ◆ LDAP-Authentifizierungsserver

**Tabelle 14-2. LDAP-Authentifizierungsserveroptionen**

Option	Beschreibung
<b>SSL aktivieren (Enable SSL)</b>	Durch die Aktivierung von SSL wird ein verschlüsselter Link zwischen einem Webserver und einem Browser hergestellt.
<b>IP-Adresse (IP Address)</b>	IP-Adresse des externen Servers.
<b>Port</b>	Zeigt den Standard-Portnamen an. Bearbeiten Sie den Eintrag, falls erforderlich.
<b>Zeitüberschreitung (Timeout)</b>	Zeitraum, innerhalb dessen der AD-Server antworten muss (in Sekunden).
<b>Status</b>	Wählen Sie <b>Aktiviert (Enabled)</b> bzw. <b>Deaktiviert (Disabled)</b> , um anzugeben, ob der Server aktiviert ist.
<b>Suchdatenbank (Search base)</b>	Teil der zu durchsuchenden externen Verzeichnisstruktur. Die Suchbasis kann der Organisation, der Gruppe oder dem Domänennamen (AD) des externen Verzeichnisses entsprechen.

Tabelle 14-2. LDAP-Authentifizierungsserveroptionen (Fortsetzung)

Option	Beschreibung
<b>Bind-DN (Bind DN)</b>	Benutzer auf dem externen Server, der das AD-Verzeichnis innerhalb der definierten Suchdatenbank durchsuchen darf. Meistens darf der Bind-DN das gesamte Verzeichnis durchsuchen. Die Rolle des Bind-DN besteht darin, das Verzeichnis unter Verwendung des Abfragefilters und der Suchbasis für den DN (Distinguished Name) für authentifizierte AD-Benutzer abzufragen. Wenn der DN zurückgegeben wird, werden der DN und das Kennwort zum Authentifizieren des AD-Benutzers verwendet.
<b>Bind-Kennwort (Bind Password)</b>	Kennwort zum Authentifizieren des AD-Benutzers.
<b>Bind-Kennwort erneut eingeben (Retype Bind Password)</b>	Geben Sie das Kennwort erneut ein.
<b>Attributname für die Anmeldung (Login Attribute Name)</b>	Name, mit dem die vom Remotebenutzer eingegebene Benutzer-ID abgeglichen wird. Für Active Directory lautet der Attributname für die Anmeldung <b>sAMAccountName</b> .
<b>Suchfilter (Search Filter)</b>	Filterwerte, mit denen die Suche eingeschränkt werden soll. Das Format für Suchfilter lautet <i>attribute operator value</i> .
<b>Diesen Server für die sekundäre Authentifizierung verwenden (Use this server for secondary authentication)</b>	Bei Auswahl wird dieser Server als zweite Authentifizierungsebene verwendet.
<b>Sitzung beenden, wenn Authentifizierung fehlschlägt (Terminate Session if authentication fails)</b>	Bei Auswahl wird die Sitzung beendet, falls die Authentifizierung fehlschlägt.

◆ **RADIUS-Authentifizierungsserver**

Im FIPS-Modus ist die RADIUS-Authentifizierung deaktiviert.

Tabelle 14-3. RADIUS-Authentifizierungsserveroptionen

Option	Beschreibung
<b>IP-Adresse (IP Address)</b>	IP-Adresse des externen Servers.
<b>Port</b>	Zeigt den Standard-Portnamen an. Bearbeiten Sie den Eintrag, falls erforderlich.
<b>Zeitüberschreitung (Timeout)</b>	Zeitraum, innerhalb dessen der AD-Server antworten muss (in Sekunden).
<b>Status</b>	Wählen Sie <b>Aktiviert (Enabled)</b> bzw. <b>Deaktiviert (Disabled)</b> , um anzugeben, ob der Server aktiviert ist.
<b>Schlüssel (Secret)</b>	Gemeinsamer geheimer Schlüssel, den Sie beim Hinzufügen des Authentifizierungsagenten in der RSA-Sicherheitskonsole festgelegt haben.

**Tabelle 14-3. RADIUS-Authentifizierungsserveroptionen (Fortsetzung)**

Option	Beschreibung
<b>Schlüssel erneut eingeben (Retype secret)</b>	Geben Sie den gemeinsamen geheimen Schlüssel erneut ein.
<b>NAS-IP-Adresse (NAS IP Address)</b>	IP-Adresse, die als RADIUS-Attribut 4, NAS-IP-Adresse, konfiguriert und verwendet werden soll, ohne die Quell-IP-Adresse im IP-Header der RADIUS-Pakete zu ändern.
<b>Anzahl Wiederholungen (Retry Count)</b>	Anzahl der Verbindungsversuche, die durchgeführt werden sollen, wenn der RADIUS-Server nicht antwortet.
<b>Diesen Server für die sekundäre Authentifizierung verwenden (Use this server for secondary authentication)</b>	Bei Auswahl wird dieser Server als zweite Authentifizierungsebene verwendet.
<b>Sitzung beenden, wenn Authentifizierung fehlschlägt (Terminate Session if authentication fails)</b>	Bei Auswahl wird die Sitzung beendet, falls die Authentifizierung fehlschlägt.

◆ **RSA-ACE-Authentifizierungsserver**

Im FIPS-Modus ist die RSA-Authentifizierung deaktiviert.

**Tabelle 14-4. RSA-ACE-Authentifizierungsserveroptionen**

Option	Beschreibung
<b>Zeitüberschreitung (Timeout)</b>	Zeitraum, innerhalb dessen der AD-Server antworten muss (in Sekunden).
<b>Konfigurationsdatei (Configuration File)</b>	Klicken Sie auf <b>Durchsuchen (Browse)</b> , um die Datei <code>sdconf.rec</code> auszuwählen, die Sie aus dem RSA Authentication Manager heruntergeladen haben.
<b>Status</b>	Wählen Sie <b>Aktiviert (Enabled)</b> bzw. <b>Deaktiviert (Disabled)</b> , um anzugeben, ob der Server aktiviert ist.
<b>Quell-IP-Adresse (Source IP Address)</b>	IP-Adresse der NSX Edge-Schnittstelle, über die der RSA-Server verfügbar ist.

**Tabelle 14-4. RSA-ACE-Authentifizierungsserveroptionen (Fortsetzung)**

Option	Beschreibung
<b>Diesen Server für die sekundäre Authentifizierung verwenden (Use this server for secondary authentication)</b>	Bei Auswahl wird dieser Server als zweite Authentifizierungsebene verwendet.
<b>Sitzung beenden, wenn Authentifizierung fehlschlägt (Terminate Session if authentication fails)</b>	Bei Auswahl wird die Sitzung beendet, falls die Authentifizierung fehlschlägt.

◆ Lokaler Authentifizierungsserver

**Tabelle 14-5. Lokale Authentifizierungsserveroptionen**

Option	Beschreibung
<b>Kennwortrichtlinie aktivieren (Enable password policy)</b>	Ist diese Option aktiviert, wird eine Kennwortrichtlinie definiert. Geben Sie die erforderlichen Werte an.
<b>Kennwortrichtlinie aktivieren (Enable password policy)</b>	<p>Ist diese Option aktiviert, wird eine Kontosperrrichtlinie definiert. Geben Sie die erforderlichen Werte an.</p> <ol style="list-style-type: none"> <li>1 Geben Sie unter „Anzahl Wiederholungen“ die Anzahl der möglichen Wiederholungsversuche für den Remotebenutzer ein, falls dieser ein falsches Kennwort eingegeben hat.</li> <li>2 Geben Sie unter „Wiederholungszeitraum“ das Zeitintervall ein, nach dessen Ablauf das Konto des Remotebenutzers bei fehlgeschlagenen Anmeldeversuchen gesperrt wird.  Wenn Sie beispielsweise für „Anzahl Wiederholungen“ den Wert 5 und für „Wiederholungszeitraum“ 1 Minute festlegen, wird das Konto des Remotebenutzers nach fünf fehlgeschlagenen Anmeldeversuchen innerhalb einer Minute gesperrt.</li> <li>3 Geben Sie unter „Sperrzeitraum“ die Dauer der Kontosperrung ein. Nach Ablauf dieser Zeitspanne wird die Kontosperrung automatisch aufgehoben.</li> </ol>
<b>Status</b>	Wählen Sie <b>Aktiviert (Enabled)</b> bzw. <b>Deaktiviert (Disabled)</b> , um anzugeben, ob der Server aktiviert ist.

**Tabelle 14-5. Lokale Authentifizierungsserveroptionen (Fortsetzung)**

Option	Beschreibung
<b>Diesen Server für die sekundäre Authentifizierung verwenden (Use this server for secondary authentication)</b>	Bei Auswahl wird dieser Server als zweite Authentifizierungsebene verwendet.
<b>Sitzung beenden, wenn Authentifizierung fehlschlägt (Terminate Session if authentication fails)</b>	Bei Auswahl wird die Sitzung beendet, falls die Authentifizierung fehlschlägt.

- 5 (Optional) Authentifizierung des Clientzertifikats hinzufügen.
  - a Klicken Sie neben **Zertifikatsauthentifizierung (Certificate Authentication)** auf **Ändern (Change)**.
  - b Aktivieren Sie das Kontrollkästchen **Authentifizierung des Clientzertifikats aktivieren (Enable client certificate authentication)**.
  - c Wählen Sie ein Clientzertifikat, das durch die Stamm-CA ausgestellt wurde, und klicken Sie auf **OK**.


#### Einschränkung

- Auf dem SSL VPN-Plus Web Portal und dem SSL VPN-Plus Full Access Client (PHAT Client) wird das Client- oder der Benutzerzertifikat unterstützt, das nur durch Stamm-CA signiert ist. Clientzertifikate, die durch Zwischen-CA signiert sind, werden nicht unterstützt.
- Authentifizierung des Clientzertifikats wird nur auf SSL VPN-Plus Clients unterstützt, die auf einem Windows-Computer installiert sind. Diese Authentifizierung wird nicht auf SSL VPN-Plus Clients unterstützt, die auf Linux- oder Mac-Computern installiert sind.

## Hinzufügen eines Installationspakets

Erstellen Sie ein SSL VPN-Plus Client-Installationspaket für den Remotebenutzer.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Installationspaket (Installation Package)** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen (Add)** (.
- 3 Geben Sie einen Profilnamen für das Installationspaket ein.

- 4 Geben Sie in **Gateway** die IP-Adresse oder den FQDN der öffentlichen NSX Edge-Schnittstelle ein.  
Diese IP-Adresse bzw. der FQDN ist an den SSL-Client gebunden. Wenn der Client installiert wird, können Sie diese IP-Adresse bzw. diesen FQDN auf dem SSL-Client sehen.
- 5 Geben Sie die Portnummer ein, die Sie in den Servereinstellungen für SSL VPN-Plus angegeben haben. Weitere Informationen dazu finden Sie unter [Hinzufügen von SSL VPN-Plus-Servereinstellungen](#).
- 6 (Optional) Um weitere NSX Edge-Uplink-Schnittstellen an den SSL-Client zu binden, führen Sie die folgenden Schritte aus:
  - a Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
  - b Geben Sie die IP-Adresse und die Portnummer ein.
  - c Klicken Sie auf **OK**.
- 7 Das Installationspaket wird standardmäßig für das Windows-Betriebssystem erstellt. Wählen Sie „Linux“ oder „Mac“, um auch ein Installationspaket für das Linux- bzw. Mac-Betriebssystem zu erstellen.
- 8 (Optional) Geben Sie eine Beschreibung für das Installationspaket ein.
- 9 Wählen Sie **Aktivieren (Enable)**, um das Installationspaket auf der Seite „Installationspaket“ anzuzeigen.
- 10 Wählen Sie bei Bedarf die folgenden Optionen aus.


Option	Beschreibung
<b>Client bei Anmeldung starten</b>	Wenn sich der Remotebenutzer beim System anmeldet, wird der SSL VPN-Client gestartet.
<b>Kennwortspeicherung zulassen</b>	Aktiviert die Option zum Speichern des Kennworts.
<b>Installation im unbeaufsichtigten Modus aktivieren</b>	Blendet die Installationsbefehle des Remotebenutzers aus.
<b>SSL-Clientnetzwerkadapter ausblenden</b>	Blendet den VMware SSL VPN-Plus-Adapter aus, der zusammen mit dem SSL VPN-Installationspaket auf dem Computer des Remotebenutzers installiert ist.
<b>Client-Taskleistensymbol ausblenden</b>	Mit dieser Option können Sie das SSL VPN-Taskleistensymbol, das angibt, ob die VPN-Verbindung aktiv ist oder nicht, ausblenden.
<b>Desktopsymbol erstellen</b>	Erstellt auf dem Desktop des Benutzers ein Symbol zum Starten des SSL-Clients.
<b>Betrieb im unbeaufsichtigten Modus aktivieren</b>	Blendet das Popup, das angibt, dass die Installation abgeschlossen ist, aus.
<b>Validierung des Serversicherheitszertifikats</b>	Der SSL VPN-Client prüft das SSL VPN-Serverzertifikat, bevor die sichere Verbindung hergestellt wird.
<b>Benutzer bei Fehlschlagen der Zertifikatvalidierung blockieren</b>	Wenn die Zertifikatvalidierung fehlschlägt, blockieren Sie den SSL VPN-Benutzer.

- 11 Klicken Sie auf **OK (OK.)**.

## Hinzufügen eines Benutzers

Fügen Sie einen Remotebenutzer zur lokalen Datenbank hinzu.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Benutzer (Users)** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen (Add)** (.
- 3 Geben Sie die Benutzer-ID ein.
- 4 Geben Sie das Kennwort ein.
- 5 Geben Sie das Kennwort erneut ein.
- 6 (Optional) Geben Sie den Vor- und Nachnamen des Benutzers ein.
- 7 (Optional) Geben Sie eine Beschreibung für den Benutzer ein.
- 8 Wählen Sie unter „Kennwortdetails“ die Option **Kennwort läuft nie ab (Password never expires)** aus, sodass das Benutzerkennwort immer beibehalten wird.
- 9 Wählen Sie **Kennwortänderung zulassen (Allow change password)** aus, damit der Benutzer das Kennwort ändern kann.
- 10 Wählen Sie **Kennwort bei nächster Anmeldung ändern (Change password on next login)** aus, wenn Sie möchten, dass der Benutzer bei der nächsten Anmeldung das Kennwort ändert.
- 11 Legen Sie den Benutzerstatus fest.
- 12 Klicken Sie auf **OK**.

## Aktivieren des SSL VPN-Plus-Diensts

Nachdem Sie den SSL VPN-Plus-Dienst konfiguriert haben, müssen Sie den Dienst für Remotebenutzer aktivieren, damit sie auf private Netzwerke zugreifen können.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Dashboard** aus.

- 2 Klicken Sie auf das Symbol  **Enable**.

Auf dem Dashboard werden Dienststatus, Anzahl der aktiven SSL VPN-Sitzungen sowie Sitzungsstatistiken und Datenflussinformationen angezeigt. Klicken Sie neben „Anzahl der aktiven Sitzungen“ auf **Details**, um Informationen zu gleichzeitigen Verbindungen zu privaten Netzwerken hinter dem NSX Edge Gateway anzuzeigen.

### Nächste Schritte

- 1 Fügen Sie eine SNAT-Regel hinzu, um die IP-Adresse der NSX Edge-Appliance in die VPN Edge-IP-Adresse zu übersetzen.
- 2 Navigieren Sie mit einem Webbrowser durch Eingabe von **https://NSXEdgeIPAddress** zur IP-Adresse der NSX Edge-Schnittstelle.

- 3 Melden Sie sich unter Verwendung des im Abschnitt [Hinzufügen eines Benutzers](#) erstellten Benutzernamens und des Kennworts an und laden Sie das Installationspaket herunter.
- 4 Aktivieren Sie die Portweiterleitung auf Ihrem Router für die in [Hinzufügen von SSL VPN-Plus-Servereinstellungen](#) verwendete Portnummer.
- 5 Starten Sie den VPN-Client, wählen Sie Ihren VPN-Server aus und melden Sie sich an. Jetzt können Sie zu den Diensten in Ihrem Netzwerk navigieren. SSL VPN-Plus-Gateway-Protokolle werden an den auf der NSX Edge-Appliance konfigurierten Syslog-Server gesendet. SSL VPN-Plus-Client-Protokolle werden im folgenden Verzeichnis auf dem Computer des Remotebenutzers gespeichert: %PROGRAMFILES%/VMWARE/SSLVPN Client/.

## Hinzufügen eines Skripts

Sie können mehrere Anmelde- bzw. Abmeldeskripts hinzufügen. Beispielsweise können Sie ein Anmeldeskript zum Starten von Internet Explorer mit gmail.com binden. Wenn sich der Remotebenutzer beim SSL-Client anmeldet, öffnet Internet Explorer gmail.com.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Anmelde- bzw. Abmeldeskripts (Login/Logoff Scripts)** aus.
- 2 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 3 Klicken Sie unter **Skript (Script)** auf **Durchsuchen (Browse)** und wählen Sie das Skript aus, das Sie an das NSX Edge Gateway binden möchten.
- 4 Wählen Sie unter **Typ (Type)** den Typ des Skripts aus.

Option	Beschreibung
<b>Anmelden</b>	Führt die Skriptaktion durch, wenn sich Remotebenutzer bei SSL VPN anmelden.
<b>Abmelden</b>	Führt die Skriptaktion durch, wenn sich Remotebenutzer bei SSL VPN abmelden.
<b>Beide</b>	Führt die Skriptaktion durch, wenn sich Remotebenutzer bei SSL VPN an- und abmelden.

- 5 Geben Sie eine Beschreibung für das Skript ein.
- 6 Wählen Sie **Aktiviert (Enabled)**, um das Skript zu aktivieren.
- 7 Klicken Sie auf **OK**.

## Installieren des SSL VPN-Plus Clients

Mit dem SSL VPN Full Access (PHAT-)Client können Sie als Remotebenutzer eine Verbindung mit einem konfigurierten privaten Netzwerk herstellen. Der Client wird auf Windows-, Mac- und Linux-Desktops unterstützt.

## Installieren von SSL VPN-Plus Client auf einer Remote-Windows-Site

Verwenden Sie die Schritte in diesem Thema, um den SSL VPN-Plus-Client auf einer Windows-Remote-Site zu installieren.

### Verfahren

- 1 Öffnen Sie auf der Remote-Client-Site ein Browser-Fenster und geben Sie **`https://ExternalEdgeInterfaceIP/sslvpn-plus/`** ein, wobei *ExternalEdgeInterfaceIP* die IP-Adresse der externen Edge-Schnittstelle ist, auf der Sie den SSL VPN-Plus-Dienst aktiviert haben.
- 2 Melden Sie sich mit den Anmeldedaten des Remote-Benutzers beim Portal an.
- 3 Klicken Sie auf die Registerkarte **Vollzugriff (Full Access)**.
- 4 Klicken Sie in der Liste auf den Namen des Installationspakets.
- 5 Klicken Sie auf den Link **Klicken Sie hier (click here)**, um das Paket mit dem Installationsprogramm herunterzuladen.  
  
Der SSL-Client wird heruntergeladen.
- 6 Extrahieren Sie die heruntergeladenen Dateien und führen Sie die Datei `Installer.exe` aus, um den Client zu installieren.

### Nächste Schritte

Melden Sie sich mit den im Abschnitt „Benutzer“ angegebenen Anmeldedaten beim SSL-Client an. Der SSL VPN-Plus-Client validiert das SSL VPN-Serverzertifikat.

Ein Windows-Client wird bei der Erstellung des Installationspakets authentifiziert, da die Option **Validierung des Serversicherheitszertifikats (Server security certificate validation)** standardmäßig ausgewählt ist.

Fügen Sie für Internet Explorer (IE) dem Zertifikatvertrauensspeicher eine vertrauenswürdige Zertifizierungsstelle hinzu. Sollte die Serverzertifikatvalidierung fehlschlagen, werden Sie aufgefordert, sich an Ihren Systemadministrator zu wenden. Bei einer erfolgreichen Serverzertifikatvalidierung wird eine Anmeldeaufforderung angezeigt.

Das Hinzufügen einer vertrauenswürdigen Zertifizierungsstelle (CA) zum Vertrauensspeicher läuft unabhängig vom SSL VPN-Workflow ab.

## Installieren von SSL VPN-Plus Client auf einer Remote-Linux-Site

Verwenden Sie die Schritte in diesem Thema, um den SSL VPN-Plus-Client auf einer Linux-Remote-Site zu installieren.

### Voraussetzungen

Installieren Sie die TCL- und TK-Pakete für Linux auf dem Remote-Computer.

Zum Installieren von SSL VPN-Plus-Client benötigen Sie Root-Berechtigungen.

## Verfahren

- 1 Öffnen Sie auf der Remote-Client-Site ein Browser-Fenster und geben Sie **`https://ExternalEdgeInterfaceIP/sslvpn-plus/`** ein, wobei *ExternalEdgeInterfaceIP* die IP-Adresse der externen Edge-Schnittstelle ist, auf der Sie den SSL VPN-Plus-Dienst aktiviert haben.
- 2 Melden Sie sich mit den Anmeldedaten des Remote-Benutzers beim Portal an.
- 3 Klicken Sie auf die Registerkarte **Vollzugriff (Full Access)**.
- 4 Klicken Sie auf den Namen des Pakets mit dem Installationsprogramm und speichern Sie die komprimierte Datei `linux_phat_client.tgz` auf dem Remote-Computer.
- 5 Extrahieren Sie die komprimierte Datei. Das Verzeichnis `linux_phat_client` wird erstellt.
- 6 Öffnen Sie die Linux-CLI und wechseln Sie zum Verzeichnis `linux_phat_client`.
- 7 Führen Sie den Befehl `$. /install_linux_phat_client.sh` aus.

## Nächste Schritte

Melden Sie sich bei der SSL VPN-GUI mit den im Abschnitt „Benutzer“ angegebenen Anmeldedaten an.

## Achtung

- Die Zwei-Faktor RSA-Authentifizierung wird bei der Anmeldung beim SSL VPN-Client auf Linux-Betriebssystemen nicht unterstützt.
- Die Befehlszeilenschnittstelle (CLI) für den SSL VPN-Linux-Client validiert keine Serverzertifikate. Wenn eine Zertifikatvalidierung des Servers erforderlich ist, verwenden Sie die SSL VPN-GUI zur Herstellung einer Verbindung mit dem Gateway.

Der SSL VPN-Linux-Client validiert standardmäßig das Serverzertifikat anhand des Browser-Zertifikatspeichers. Sollte die Serverzertifikatvalidierung fehlschlagen, werden Sie aufgefordert, sich an Ihren Systemadministrator zu wenden. Bei einer erfolgreichen Serverzertifikatvalidierung wird eine Anmeldeaufforderung angezeigt.

Das Hinzufügen einer vertrauenswürdigen Zertifizierungsstelle (CA) (beispielsweise des Firefox-Zertifikatspeichers) ist unabhängig vom SSL VPN-Workflow.

## Installieren von SSL VPN-Plus Client auf einer Remote-Mac -Site

Verwenden Sie die Schritte in diesem Thema, um den SSL VPN-Plus Client auf einem Remote-Mac-Computer zu installieren.

## Voraussetzungen

Zum Installieren von SSL VPN-Plus-Client benötigen Sie Root-Berechtigungen.

## Verfahren

- 1 Öffnen Sie auf der Remote-Client-Site ein Browser-Fenster und geben Sie **`https://ExternalEdgeInterfaceIP/sslvpn-plus/`** ein, wobei *ExternalEdgeInterfaceIP* die IP-Adresse der externen Edge-Schnittstelle ist, auf der Sie den SSL VPN-Plus-Dienst aktiviert haben.

- 2 Melden Sie sich mit den Anmeldedaten des Remote-Benutzers beim Portal an.
- 3 Klicken Sie auf die Registerkarte **Vollzugriff (Full Access)**.
- 4 Klicken Sie auf den Namen des Installationsprogrammpakets und speichern Sie die komprimierte Datei `mac_phat_client.tgz` auf dem Remote-Computer.
- 5 Extrahieren Sie die komprimierte Datei. Das Verzeichnis `mac_phat_client` wird erstellt.
- 6 Um den SSL VPN-Plus-Client zu installieren, doppelklicken Sie auf die Datei `naclient.pkg`.  
Folgen Sie den Schritten des Assistenten, um die Installation abzuschließen.  
  
Wenn die SSL VPN-Client-Installation fehlschlägt, überprüfen Sie die Protokolldatei der Installation unter `/tmp/naclient_install.log`.  
  
Informationen zur Fehlerbehebung bei der Installation auf Mac OS High Sierra finden Sie unter *Fehlerbehebungshandbuch zu NSX*.

### Nächste Schritte

Melden Sie sich mit den im Abschnitt „Benutzer“ angegebenen Anmeldedaten beim SSL-Client an.

---

**Achtung** Die Zwei-Faktor-RSA-Authentifizierung wird bei der Anmeldung beim SSL VPN-Client auf Mac-Betriebssystemen nicht unterstützt.

---

Der SSL VPN Mac-Client validiert standardmäßig das Serverzertifikat anhand von Keychain. Dies ist eine Datenbank, in der Zertifikate aus Mac OS gespeichert werden. Sollte die Serverzertifikatvalidierung fehlschlagen, werden Sie aufgefordert, sich an Ihren Systemadministrator zu wenden. Bei einer erfolgreichen Serverzertifikatvalidierung wird eine Anmeldeaufforderung angezeigt.

## Konfigurieren von Proxy-Server-Einstellungen in SSL VPN-Plus-Client

Proxy-Server-Konfiguration wird auf einem SSL VPN-Plus-Client auf Windows-Computern unterstützt, auf Mac- und Linux-Computern aber nicht.

### Vorsicht

- Obwohl der SSL VPN-Plus-Client auf Mac OS die Möglichkeit bietet, Proxy-Server-Einstellungen zu konfigurieren, dürfen Remote-Benutzer die Proxy-Server-Einstellungen nicht konfigurieren.
  - Remote-Linux-Betriebssystem-Benutzer müssen es vermeiden, die Proxy-Server-Einstellungen auf dem SSL VPN-Plus-Client über die Linux-CLI zu konfigurieren.
- 

Im folgenden Verfahren werden die Schritte erläutert, um die Proxy-Server-Einstellungen eines SSL VPN-Plus-Clients auf Windows-Computern zu konfigurieren.

### Voraussetzungen

SSL VPN-Plus-Client wird auf dem Remote-Windows-Computer installiert.

## Verfahren

- 1 Doppelklicken Sie auf das Desktopsymbol des SSL VPN-Plus-Clients auf dem Windows-Computer.  
Das Fenster **SSL VPN-Plus Client – Anmeldung** wird geöffnet.
- 2 Klicken Sie auf **Einstellungen (Settings)** und anschließend auf die Registerkarte **Proxy-Einstellungen (Proxy Settings)**.
- 3 Geben Sie die Proxy-Server-Einstellungen an.
  - a Aktivieren Sie das Kontrollkästchen **Proxy verwenden (Use Proxy)**.
  - b Konfigurieren Sie unter **Proxytyp (Type Of Proxy)** einen der Proxyservertypen.

Option	Beschreibung
<b>IE-Einstellungen verwenden</b>	Verwenden Sie die Proxy-Server-Konfiguration, die in Ihrem IE-Browser angegeben ist.
<b>HTTP</b>	Geben Sie die folgenden Einstellungen für einen HTTP-Proxy-Server an: <ul style="list-style-type: none"> <li>■ Proxy-Servernamen oder eine IP-Adresse des Proxy-Servers</li> <li>■ Port des Proxy-Servers Der Standardport ist 80, was Sie bearbeiten können.</li> </ul>
<b>SOCKS Version 4</b>	Geben Sie die folgenden Einstellungen für einen SOCKS 4.0-Proxy-Server an: <ul style="list-style-type: none"> <li>■ Proxy-Servernamen oder eine IP-Adresse des Proxy-Servers</li> <li>■ Port des Proxy-Servers Der Standardport ist 1080, was Sie bearbeiten können.</li> </ul>
<b>SOCKS Version 5</b>	Geben Sie die folgenden Einstellungen für einen SOCKS 5.0-Proxy-Server an: <ul style="list-style-type: none"> <li>■ Proxy-Servernamen oder eine IP-Adresse des Proxy-Servers</li> <li>■ Port des Proxy-Servers Der Standardport ist 1080, was Sie bearbeiten können.</li> <li>■ (Optional) Benutzername und Kennwort für den Zugriff auf den SOCKS 5.0-Server.</li> </ul>

- 4 Um die Proxy-Server-Einstellungen zu speichern, klicken Sie auf **OK**.

## SSL VPN-Plus-Protokolle

SSL VPN-Plus-Gateway-Protokolle werden an den auf der NSX Edge-Appliance konfigurierten Syslog-Server gesendet.

Die folgende Tabelle enthält die Speicherorte auf dem Computer des Remotebenutzers, in dem die SSL VPN-Plus Client-Protokolle gespeichert werden.

Betriebssystem	Speicherort der Protokolldatei
Windows 8	C:\Users\Benutzername\AppData\Local\VMware\vpn\svp_client.log
Windows 10	C:\Users\Benutzername\AppData\Local\VMware\vpn\svp_client.log
Linux	Systemprotokolldateien
Mac	Protokolldatei der Installation unter /tmp/naclient_install.log Systemprotokolldateien

## Ändern der SSL VPN-Plus Client-Protokolle und der Protokollierungsebene

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **Servereinstellungen (Server Settings)**.
- 2 Wechseln Sie zum Abschnitt „Protokollierungsrichtlinie“ und erweitern Sie den Abschnitt, um die aktuellen Einstellungen anzuzeigen.
- 3 Klicken Sie auf **Ändern (Change)**.
- 4 Aktivieren Sie das Kontrollkästchen **Protokollierung aktivieren (Enable logging)**, um die Protokollierung einzuschalten.

ODER

Deaktivieren Sie das Kontrollkästchen **Protokollierung aktivieren (Enable logging)**, um die Protokollierung auszuschalten.

- 5 Wählen Sie die erforderliche Protokollierungsebene aus.

---

**Hinweis** SSL VPN-Plus Client-Protokolle sind standardmäßig aktiviert, und die Protokollierungsebene ist auf „NOTICE“ (HINWEIS) festgelegt.

---

- 6 Klicken Sie auf **OK**.

## Bearbeiten der Client-Konfiguration

Sie können die Art und Weise ändern, wie der SSL VPN-Client-Tunnel reagiert, wenn sich der Remotebenutzer bei SSL VPN anmeldet.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Client-Konfiguration (Client Configuration)** aus.
- 2 Wählen Sie die Option **Tunnelmodus (Tunneling Mode)** aus.  
  
Im Modus „Geteilter Tunnel“ wird nur das VPN über das NSX Edge Gateway übertragen. Im Modus „Vollständiger Tunnel“ wird das NSX Edge Gateway zum Standardgateway des Remotebenutzers und der gesamte Datenverkehr (VPN, lokal und Internet) wird über dieses Gateway übertragen.
- 3 Wenn Sie den Modus „Vollständiger Tunnel“ gewählt haben:
  - a Wählen Sie **Lokale Subnetze ausschließen (Exclude local subnets)**, sodass der lokale Datenverkehr nicht über den VPN-Tunnel gesendet wird.
  - b Geben Sie die IP-Adresse des Standard-Gateways des Remotebenutzersystems ein.
- 4 Wählen Sie **Automatische Wiederherstellung der Verbindung aktivieren (Enable auto reconnect)**, wenn der Remotebenutzer automatisch wieder mit dem SSL VPN-Client verbunden werden soll, nachdem die Verbindung getrennt wurde.
- 5 Wählen Sie **Benachrichtigung bei Client-Upgrade (Client upgrade notification)**, um den Remotebenutzer zu benachrichtigen, wenn ein Upgrade für den Client verfügbar ist. Der Remotebenutzer kann dann entscheiden, ob er das Upgrade installieren möchte.

- 6 Klicken Sie auf **OK**.

## Bearbeiten der allgemeinen Einstellungen

Sie können Standard-VPN-Einstellungen bearbeiten.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Allgemeine Einstellungen (General Settings)** aus.
- 2 Nehmen Sie die gewünschten Änderungen vor.

Option	Zweck
<b>Verwendung desselben Benutzernamens bei Mehrfachanmeldung verhindern</b>	Der Remotebenutzer darf sich mit einem Benutzernamen nur einmal anmelden.
<b>Komprimierung aktivieren</b>	Aktiviert die intelligente TCP-basierte Datenkomprimierung und erhöht die Datenübertragungsgeschwindigkeit.
<b>Protokollierung aktivieren</b>	Protokolliert den Datenverkehr, der über das SSL VPN-Gateway fließt.
<b>Virtuelle Tastatur erzwingen</b>	Die Remotebenutzer dürfen die Web- oder Client-Anmeldeinformationen nur über die virtuelle Tastatur eingeben.
<b>Tasten der virtuellen Tastatur zufällig festlegen</b>	Zufällige Anordnung der Tasten der virtuellen Tastatur.
<b>Erzwungene Zeitüberschreitung aktivieren</b>	Nach Ablauf des festgelegten Zeitlimits wird die Verbindung des Remotebenutzers getrennt. Geben Sie das Zeitlimit in Minuten ein.
<b>Sitzungszeitüberschreitung bei Leerlauf</b>	Falls in der angegebenen Zeitspanne keine Benutzeraktivität stattfindet, wird die Sitzung des Benutzers beendet.  Das SSLVPN-Leerlaufzeitlimit berücksichtigt alle Pakete, einschließlich Kontrolldatenpaketen, die durch beliebige Anwendungs- und Benutzerdaten gesendet werden, bezüglich der Erkennung von Zeitüberschreitungen. Als Folge tritt für die Sitzung keine Zeitüberschreitung auf, wenn eine Anwendung vorhanden ist, die ein periodisches Kontrolldatenpaket (z. B. MDNS) sendet, selbst wenn keine Benutzerdaten vorliegen.
<b>Benutzerbenachrichtigung</b>	Geben Sie die Meldung ein, die bei der Anmeldung des Remotebenutzers angezeigt werden soll.

- 3 Klicken Sie auf **OK**.

## Bearbeiten des Webportal-Designs

Sie können das Client-Banner bearbeiten, das an den SSL VPN-Client gebunden ist.

### Verfahren

- 1 Doppelklicken Sie auf der Registerkarte **NSX Edges** auf eine NSX Edge-Instanz.
- 2 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **SSL VPN-Plus**.

- 3 Wählen Sie im linken Fensterbereich **Portalanpassung (Portal Customization)** aus.
- 4 Geben Sie den Portaltitel ein.
- 5 Geben Sie den Firmennamen des Remotebenutzers ein.
- 6 Klicken Sie in **Logo** auf **Ändern (Change)** und wählen Sie vorzugsweise ein JPEG-Bild für das Firmenlogo aus.

Es gibt keine bevorzugten Abmessungen für die Größe des Logos.

- 7 Klicken Sie unter **Farben (Colors)** auf das Farbfeld neben dem nummerierten Element, für das Sie die Farbe ändern möchten, und wählen Sie die gewünschte Farbe aus.
- 8 Ändern Sie den Client-Banner, falls erforderlich. Wählen Sie ein BMP-Bild für das Banner aus.  
Die bevorzugte Größe für das Client-Banner beträgt 390 x 75 Pixel.
- 9 Klicken Sie auf **OK**.

## Arbeiten mit IP-Pools für SSL VPN


Sie können einen IP-Pool bearbeiten oder löschen.

Weitere Informationen zum Hinzufügen eines IP-Pools finden Sie unter [Konfigurieren von Network Access SSL VPN-Plus](#).

### Bearbeiten eines IP-Pools

Sie können einen IP-Pool bearbeiten.


#### Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **IP-Pool (IP Pool)**.
  - 2 Wählen Sie den zu bearbeitenden IP-Pool aus.
  - 3 Klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- Das Dialogfeld „IP-Pool bearbeiten“ wird geöffnet.
- 4 Nehmen Sie die erforderlichen Änderungen vor.
  - 5 Klicken Sie auf **OK**.

### Löschen eines IP-Pools

Sie können einen IP-Pool löschen.

#### Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **IP-Pool (IP Pool)**.
  - 2 Wählen Sie den zu löschenden IP-Pool aus.
  - 3 Klicken Sie auf das Symbol **Löschen (Delete)** (.
- Der ausgewählte IP-Pool wird gelöscht.

## Aktivieren eines IP-Pools

Sie können einen IP-Pool aktivieren, wenn Sie möchten, dass einem Remotebenutzer eine IP-Adresse aus dem Pool zugewiesen wird.

### Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **IP-Pool (IP Pool)**.
- 2 Wählen Sie den IP-Pool aus, den Sie aktivieren möchten.
- 3 Klicken Sie auf das Symbol **Aktivieren (Enable)** (✓).

## Deaktivieren eines IP-Pools

Sie können einen IP-Pool deaktivieren, wenn Sie nicht möchten, dass einem Remotebenutzer eine IP-Adresse aus dem Pool zugewiesen wird.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** aus dem linken Fensterbereich **IP-Pool (IP Pool)** aus.
- 2 Wählen Sie den IP-Pool aus, den Sie deaktivieren möchten.
- 3 Klicken Sie auf das Symbol **Deaktivieren (Disable)** (⊘).

## Ändern der Reihenfolge eines IP-Pools

SSL VPN weist einem Remotebenutzer basierend auf deren Reihenfolge in der IP-Pool-Tabelle eine IP-Adresse aus einem IP-Pool zu.

### Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **IP-Pool (IP Pool)**.
- 2 Wählen Sie den IP-Pool aus, für den Sie die Reihenfolge ändern möchten.
- 3 Klicken Sie auf das Symbol **Nach oben verschieben (Move Up)** (⇧) oder „Nach unten verschieben“ (⇩).

## Arbeiten mit privaten Netzwerken


Sie können ein privates Netzwerk, auf das ein Remotebenutzer zugreifen kann, bearbeiten oder löschen.

Weitere Informationen zum Hinzufügen eines privaten Netzwerks finden Sie unter [Konfigurieren von Network Access SSL VPN-Plus](#).

## Löschen eines privaten Netzwerks

Sie können ein privates Netzwerk löschen.


## Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Private Netzwerke (Private Networks)** aus.
- 2 Wählen Sie das Netzwerk aus, das Sie löschen möchten, und klicken Sie auf das Symbol **Löschen (Delete)** ().

## Aktivieren eines privaten Netzwerks

Wenn Sie ein privates Netzwerk aktivieren, kann der Remotebenutzer über SSL VPN-Plus darauf zugreifen.


### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Private Netzwerke (Private Networks)** aus.
  - 2 Klicken Sie auf das Netzwerk, das Sie aktivieren möchten.
  - 3 Klicken Sie auf das Symbol **Aktivieren (Enable)** ().
- Das ausgewählte Netzwerk wird aktiviert.

## Deaktivieren eines privaten Netzwerks

Wenn Sie ein privates Netzwerk deaktivieren, kann der Remotebenutzer nicht über SSL VPN-Plus darauf zugreifen.

### Verfahren




- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Private Netzwerke (Private Networks)** aus.
  - 2 Klicken Sie auf das Netzwerk, das Sie deaktivieren möchten.
  - 3 Klicken Sie auf das Symbol **Deaktivieren (Disable)** ().
- Das ausgewählte Netzwerk wird deaktiviert.

## Ändern der Reihenfolge eines privaten Netzwerks

SSL VPN-Plus ermöglicht Remotebenutzern den Zugriff auf private Netzwerke in der Reihenfolge, in der sie im Bereich „Private Netzwerke“ aufgeführt werden.

Wenn Sie für ein privates Netzwerk die Option **TCP-Optimierung aktivieren (Enable TCP Optimization)** auswählen, funktionieren innerhalb dieses Subnetzes möglicherweise einige Anwendungen, z. B. FTP im aktiven Modus, nicht. Zum Hinzufügen eines FTP-Servers im aktiven Modus müssen Sie ein weiteres privates Netzwerk für diesen FTP-Server mit deaktivierter Option „TCP-Optimierung“ hinzufügen. Außerdem muss das aktive private TCP-Netzwerk aktiviert und über dem privaten Subnetz-Netzwerk platziert werden.

## Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Private Netzwerke (Private Networks)** aus.
- 2 Klicken Sie auf das Symbol **Reihenfolge ändern (Change Order)** (.
- 3 Wählen Sie das Netzwerk aus, für das Sie die Reihenfolge ändern möchten.
- 4 Klicken Sie auf das Symbol **Nach oben verschieben (Move Up)** () oder **Nach unten verschieben (Move Down)** (.
- 5 Klicken Sie auf **OK**.

## Nächste Schritte

Erläuterungen zum Hinzufügen eines FTP-Servers im aktiven Modus finden Sie unter [Konfigurieren des privaten Netzwerks für aktive FTP-Server](#).

## Konfigurieren des privaten Netzwerks für aktive FTP-Server

Sie können dem privaten Netzwerk einen FTP-Server im aktiven Modus hinzufügen. Für aktive FTP-Server wird die steuernde Verbindung vom Back-End-FTP-Server mit dem Clientcomputer initiiert, der die TCP-Optimierung nicht unterstützt.

## Voraussetzungen

Der FTP-Server ist im aktiven Modus konfiguriert.

## Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Private Netzwerke (Private Networks)** aus.
- 2 Fügen Sie das private Netzwerk hinzu, das Sie für aktive FTP-Server konfigurieren möchten. Weitere Informationen finden Sie unter [Hinzufügen eines privaten Netzwerks](#).
- 3 Deaktivieren Sie das Kontrollkästchen **TCP-Optimierung aktivieren (Enable TCP Optimization)**.
- 4 Fügen Sie im Feld **Ports** eine Portnummer für das private Netzwerk hinzu.
- 5 Wählen Sie den Status **Aktiviert (Enabled)** aus, um das private Netzwerk zu aktivieren.
- 6 Platzieren Sie das private Netzwerk, das Sie für aktive FTP-Server konfigurieren möchten, über anderen konfigurierten privaten Netzwerken. Weitere Informationen finden Sie unter [Ändern der Reihenfolge eines privaten Netzwerks](#).

## Nächste Schritte

Fügen Sie eine entsprechende Firewallregel hinzu, um den privaten Netzwerkdatenverkehr zuzulassen.

## Arbeiten mit Installationspaketen


Sie können ein Installationspaket für den SSL-Client löschen oder bearbeiten.

Weitere Informationen zum Erstellen eines Installationspakets finden Sie unter [Konfigurieren von Network Access SSL VPN-Plus](#).

## Bearbeiten eines Installationspakets

Sie können ein Installationspaket bearbeiten.


### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Installationspaket (Installation Package)** aus.
  - 2 Wählen Sie das zu bearbeitende Installationspaket aus.
  - 3 Klicken Sie auf das Symbol „Bearbeiten“ ().
- Das Dialogfeld „Installationspaket bearbeiten“ wird geöffnet.
- 4 Nehmen Sie die erforderlichen Änderungen vor.
  - 5 Klicken Sie auf **OK**.

## Löschen eines Installationspakets

Sie können ein Installationspaket löschen.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Installationspaket (Installation Package)** aus.
- 2 Wählen Sie das zu löschende Installationspaket aus.
- 3 Klicken Sie auf das Symbol **Löschen (Delete)** ().

## Arbeiten mit Benutzern


Sie können Benutzer aus der lokalen Datenbank löschen oder sie bearbeiten.

Weitere Informationen zum Hinzufügen eines Benutzers finden Sie unter [Konfigurieren von Network Access SSL VPN-Plus](#).

## Bearbeiten eines Benutzers

Außer der Benutzer-ID können Sie alle Details für einen Benutzer bearbeiten.


### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Benutzer (Users)** aus.
- 2 Klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- 3 Nehmen Sie die erforderlichen Änderungen vor.
- 4 Klicken Sie auf **OK**.

## Löschen eines Benutzers

Sie können einen Benutzer löschen.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Benutzer (Users)** aus.
- 2 **Benutzer (Users)**Klicken Sie im Bereich **Konfigurieren (Configure)** auf **Benutzer (Users)**.
- 3 Wählen Sie den Benutzer aus, den Sie löschen möchten, und klicken Sie auf das Symbol **Löschen (Delete)** ().

## Ändern des Kennworts eines Benutzers

Sie können das Kennwort des Benutzers ändern.

### Verfahren

- 1 Wählen Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich **Benutzer (Users)** aus.
- 2 Klicken Sie auf das Symbol **Kennwort ändern (Change Password)**.
- 3 Geben Sie das neue Kennwort ein. Geben Sie es dann zur Bestätigung noch einmal ein.
- 4 Klicken Sie auf „Kennwort bei nächster Anmeldung ändern“, damit das geänderte Kennwort bei der nächsten Anmeldung des Benutzers verwendet wird.
- 5 Klicken Sie auf **OK**.


## Arbeiten mit Anmelde- und Abmeldeskripts

Sie können ein Anmelde- bzw. Abmeldeskript an das NSX Edge Gateway binden.

## Bearbeiten eines Skripts

Sie können den Typ, die Beschreibung und den Status eines an das NSX Edge Gateway gebundenen Anmelde- oder Abmeldeskripts ändern.


### Verfahren

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **Anmelde- bzw. Abmeldeskripts (Login/Logoff Scripts)**.
- 2 Wählen Sie ein Skript aus und klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- 3 Nehmen Sie die entsprechenden Änderungen vor.
- 4 Klicken Sie auf **OK**.

## Löschen eines Skripts

Sie können Anmelde- bzw. Abmeldeskripts löschen.


**Verfahren**

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **Anmelde- bzw. Abmeldeskripts (Login/Logoff Scripts)**.
- 2 Wählen Sie ein Skript aus und klicken Sie auf das Symbol **Löschen (Delete)** ()

**Aktivieren eines Skripts**

Zur ordnungsgemäßen Funktionsweise müssen Sie ein Skript aktivieren.


**Verfahren**

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **Anmelde- bzw. Abmeldeskripts (Login/Logoff Scripts)**.
- 2 Wählen Sie ein Skript aus und klicken Sie auf das Symbol **Aktivieren (Enable)** ()

**Deaktivieren eines Skripts**

Sie können Anmelde- bzw. Abmeldeskripts deaktivieren.



**Verfahren**

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **Anmelde- bzw. Abmeldeskripts (Login/Logoff Scripts)**.
- 2 Wählen Sie ein Skript aus und klicken Sie auf das Symbol **Deaktivieren (Disable)** ()

**Ändern der Reihenfolge eines Skripts**

Sie können die Reihenfolge eines Skripts ändern. Angenommen, Sie haben ein Anmeldeskript zum Öffnen von gmail.com in Internet Explorer vor ein Anmeldeskript zum Öffnen von yahoo.com gestellt. Wenn der Remotebenutzer sich bei SSL VPN anmeldet, wird gmail.com vor yahoo.com angezeigt. Falls Sie nun die Reihenfolge der Anmeldeskripts umkehren, wird zuerst yahoo.com und anschließend gmail.com geöffnet.

**Verfahren**

- 1 Klicken Sie auf der Registerkarte **SSL VPN-Plus** im linken Fensterbereich auf **Anmelde- bzw. Abmeldeskripts (Login/Logoff Scripts)**.
- 2 Wählen Sie das Skript aus, für das Sie die Reihenfolge ändern möchten, und klicken Sie auf das Symbol **Nach oben verschieben (Move Up)** () oder **Nach unten verschieben (Move Down)** ()
- 3 Klicken Sie auf **OK**.

## Überblick über IPSec-VPN

NSX Edge unterstützt Site-to-Site-IPSec-VPN zwischen einer NSX Edge-Instanz und Remote-Sites. Zertifikatsauthentifizierung, Pre-Shared Key-Modus, IP-Unicast-Datenverkehr und kein dynamisches Routing-Protokoll werden zwischen der NSX Edge-Instanz und Remote-VPN-Routern unterstützt.

Sie können hinter jedem Remote-VPN-Router mehrere Subnetze konfigurieren, um hinter einer NSX Edge-Instanz über IPSec-Tunnel eine Verbindung mit dem internen Netzwerk herzustellen.

**Hinweis** Subnetze und das interne Netzwerk hinter einer NSX Edge-Instanz dürfen keine überlappenden Adressbereiche aufweisen.

Wenn der lokale und der Remote-Peer eines IPSec-VPN sich überlappende IP-Adressen aufweisen, ist der über den Tunnel weitergeleitete Datenverkehr eventuell nicht konsistent, je nachdem, ob lokal verbundene oder Auto-Plumbed-Routen vorhanden sind.

Sie können einen NSX Edge-Agenten hinter einem NAT-Gerät bereitstellen. In dieser Bereitstellung übersetzt das NAT-Gerät die VPN-Adresse einer NSX Edge-Instanz in eine aus dem Internet zugängliche öffentliche Adresse. Remote-VPN-Router verwenden diese öffentliche Adresse für den Zugriff auf die NSX Edge-Instanz.

Sie können Remote-VPN-Router auch hinter einem NAT-Gerät platzieren. Zur Einrichtung des Tunnels müssen Sie sowohl die systemeigene VPN-Adresse als auch die VPN-Gateway-ID angeben. Für die VPN-Adresse ist auf beiden Seiten eine statische 1:1-Netzwerkadressübersetzung erforderlich.

Multiplizieren Sie zum Berechnen der Anzahl der benötigten Tunnel die Anzahl der lokalen Subnetze mit der Anzahl der Peer-Subnetze. Sind z. B. 10 lokale Subnetze und 10 Peer-Subnetze vorhanden, benötigen Sie 100 Tunnel. Die maximale Anzahl der unterstützten Tunnel wird durch die ESG-Größe bestimmt, wie nachfolgend dargestellt.

**Tabelle 14-6. Anzahl der IPSec-Tunnel pro ESG**

ESG	Anzahl der IPSec-Tunnel
Kompakt	512
Groß	1600
Quad Large	4096
Sehr groß	6000

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 Group 2)
- DH-5 (Diffie–Hellman Group 5)
- DH-14 (Diffie–Hellman Group 14)
- DH-15 (Diffie–Hellman Group 15)
- DH-16 (Diffie–Hellman Group 16)

Weitere Informationen zu den Beispielen für die Konfiguration von IPSec-VPN finden Sie unter [Beispiele für die IPSec-VPN-Konfiguration](#).

Erläuterungen zur IPSec-VPN-Fehlerbehebung erhalten Sie unter <https://kb.vmware.com/kb/2123580>.

## Konfigurieren des IPSec-VPN-Diensts

Sie können einen NSX Edge-Tunnel zwischen einem lokalen und einem Peer-Subnetz einrichten.

---

**Hinweis** Wenn Sie eine Verbindung zu einer Remote-Site über IPSec-VPN herstellen, kann die IP-Adresse dieser Site nicht über das dynamische Routing im Edge-Uplink abgerufen werden.

---

### Aktivieren des IPSec-VPN-Diensts

Sie müssen einen IPSec-VPN-Dienst aktivieren, damit der Datenverkehr vom lokalen Subnetz zum Peer-Subnetz übertragen werden kann.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
- 5 Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
- 6 Klicken Sie auf **Aktivieren (Enable)**.

### Verwenden von OpenSSL zum Generieren von Zertifikaten einer Zertifizierungsstelle für IPSec-VPNs

Um die Zertifikatsauthentifizierung für IPSec zu aktivieren, müssen Serverzertifikate und die entsprechenden, von einer Zertifizierungsstelle signierten Zertifikate importiert werden. Optional können Sie ein Open-Source-Befehlszeilen-Tool, wie z. B. OpenSSL, verwenden, um Zertifikate einer Zertifizierungsstelle zu generieren.

#### Voraussetzungen

OpenSSL muss installiert sein.

## Verfahren

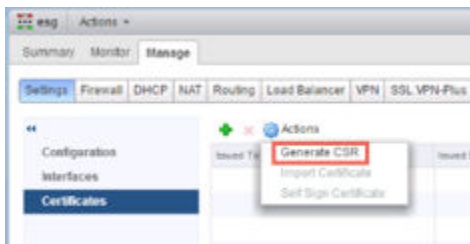
- 1 Öffnen Sie auf einer Linux- oder Mac-Maschine, auf der OpenSSL installiert ist, die Datei: `/opt/local/etc/openssl/openssl.cnf` bzw. `/System/Library/OpenSSL/openssl.cnf`.
- 2 Stellen Sie sicher, dass `dir = .` ausgeführt wird.
- 3 Führen Sie die folgenden Befehle aus:

```
mkdir newcerts
mkdir certs
mkdir req
mkdir private
echo "01" > serial
touch index.txt
```

- 4 Führen Sie den Befehl aus, um ein von einer Zertifizierungsstelle signiertes Zertifikat zu generieren:

```
openssl req -new -x509 -newkey rsa:2048 -keyout private/cakey.pem -out cacert.pem -days 3650
```

- 5 Generieren Sie auf NSX Edge1 eine Zertifikatsignieranforderung (CSR), kopieren Sie den Inhalt der Privacy Enhanced Mail-Datei und speichern Sie ihn in einer Datei in `req/edge1.req`.



Weitere Informationen dazu finden Sie unter [Konfigurieren eines von einer Zertifizierungsstelle signierten Zertifikats](#).

- 6 Führen Sie den Befehl zum Signieren der Zertifikatsignieranforderung aus:

```
sudo openssl ca -policy policy_anything -out certs/edge1.pem -in req/edge1.req
```

- 7 Generieren Sie auf NSX Edge2 eine Zertifikatsignieranforderung (CSR), kopieren Sie den Inhalt der Privacy Enhanced Mail-Datei (PEM) und speichern Sie ihn in einer Datei in `req/edge2.req`.
- 8 Führen Sie den Befehl zum Signieren der Zertifikatsignieranforderung aus:

```
sudo openssl ca -policy policy_anything -out certs/edge2.pem -in req/edge2.req
```

- 9 Laden Sie das PEM-Zertifikat am Ende der Datei `certs/edge1.pem` auf Edge1 hoch.
- 10 Laden Sie das PEM-Zertifikat am Ende der Datei `certs/edge2.pem` auf Edge2 hoch.
- 11 Laden Sie das CA-Zertifikat in der Datei `cacert.pem` auf Edge1 und Edge2 als ein von einer Zertifizierungsstelle signiertes Zertifikat hoch.

- 12 Wählen Sie in der globalen IPSec-Konfiguration für Edge1 und Edge2 das hochgeladene PEM-Zertifikat und das hochgeladene CA-Zertifikat aus und speichern Sie die Konfiguration.
- 13 Klicken Sie auf der Registerkarte **Zertifikat (Certificate)** auf das hochgeladene Zertifikat und notieren Sie die DN-Zeichenfolge.
- 14 Stellen Sie die DN-Zeichenfolge auf das Format  
C=IN, ST=ka, L=b1r, O=bmware, OU=vmware, CN=edge2.eng.vmware.com um und speichern Sie sie für Edge1 und Edge2.
- 15 Erstellen Sie IPsec-VPN-Sites auf Edge1 und Edge2 mit der lokalen ID und der Peer-ID als DN-Zeichenfolge im angegebenen Format.

## Ergebnisse

Überprüfen Sie den Status durch Klicken auf **IPSec-Statistik anzeigen (Show IPsec Statistics)**. Klicken Sie auf den Kanal, um den Tunnelstatus anzuzeigen. Sowohl der Kanal als auch der Tunnelstatus müssten Grün angezeigt werden.

## Angeben der globalen IPSec-VPN-Konfiguration

Dies aktiviert IPSec-VPN auf der NSX Edge-Instanz.

### Voraussetzungen

Um die Zertifikatsauthentifizierung zu aktivieren, müssen Serverzertifikate und die entsprechenden, von einer Zertifizierungsstelle signierten Zertifikate importiert werden. Optional können Sie ein Open-Source-Befehlszeilen-Tool, wie z. B. OpenSSL, verwenden, um Zertifikate einer Zertifizierungsstelle zu generieren.

Selbstsignierte Zertifikate können nicht für IPSec-VPNs verwendet werden. Sie können nur beim Load Balancing und für SSL-VPNs verwendet werden.

### Verfahren


- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
- 5 Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
- 6 Klicken Sie neben dem globalen Konfigurationsstatus auf **Ändern (Change)**.
- 7 Geben Sie einen globalen vorinstallierten Schlüssel für die Sites ein, deren Peer-Endpoint auf „alle“ festgelegt ist, und wählen Sie **Gemeinsam verwendeten Schlüssel anzeigen (Display shared key)** aus, um den Schlüssel anzuzeigen.
- 8 Wählen Sie „Zertifizierungsauthentifizierung aktivieren“ und das entsprechende Zertifikat aus.
- 9 Klicken Sie auf **OK**.

## Aktivieren der Protokollierung für IPSec-VPN

Sie können die Protokollierung des gesamten IPSec-VPN-Datenverkehrs aktivieren.

Standardmäßig ist die Protokollierung aktiviert und dafür die Ebene WARNUNG festgelegt.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
- 5 Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
- 6 Klicken Sie auf  neben **Protokollierungsrichtlinie (Logging Policy)** und klicken Sie dann auf **Protokollierung aktivieren (Enable logging)**, um den Datenverkehrsfluss zwischen dem lokalen Subnetz und dem Peer-Subnetz zu protokollieren und die Protokollierungsebene auszuwählen.
- 7 Wählen Sie die Protokollierungsebene aus und klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Konfigurieren der IPSec-VPN-Parameter

Sie müssen mindestens eine externe IP-Adresse für NSX Edge konfigurieren, um den IPSec-VPN-Dienst bereitstellen zu können.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
- 5 Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (.
- 7 Geben Sie einen Namen für das IPSec-VPN ein.
- 8 Geben Sie die IP-Adresse der NSX Edge-Instanz im Feld **Lokale ID (Local Id)** ein. Diese wird zur Peer-ID auf der Remote-Site.
- 9 Geben Sie die IP-Adresse des lokalen Endpunkts ein.

Wenn Sie unter Verwendung eines vorinstallierten Schlüssels (Pre-Shared Key) eine IP-Adresse zum IP-Tunnel hinzufügen, können die lokale ID und die ID des lokalen Endpunkts identisch sein.

- 10 Geben Sie die Subnetze, die von den Sites gemeinsam genutzt werden sollen, im CIDR-Format ein. Trennen Sie mehrere Subnetze jeweils durch ein Komma.
- 11 Geben Sie die Peer-ID ein, um die Peer-Site eindeutig zu identifizieren. Bei Peers mit Zertifiktsauthentifizierung muss diese ID der allgemeine Name (Common Name) im Peer-Zertifikat sein. Bei PSK-Peers kann diese ID eine beliebige Zeichenfolge sein. VMware empfiehlt, dass Sie die öffentliche IP-Adresse des VPN oder einen FQDN für den VPN-Dienst als Peer-ID verwenden.
- 12 Geben Sie im Feld „Peer-Endpoint“ die IP-Adresse der Peer-Site ein. Falls Sie das Feld leer lassen, wartet NSX Edge auf das Peer-Gerät, um eine Verbindung anzufordern.
- 13 Geben Sie die interne IP-Adresse des Peer-Subnetzes im CIDR-Format ein. Trennen Sie mehrere Subnetze jeweils durch ein Komma.
- 14 Wählen Sie den Verschlüsselungsalgorithmus aus.  
Der AES-GCM-Verschlüsselungsalgorithmus ist nicht FIPS-konform.
- 15 Wählen Sie unter „Authentifizierungsmodell“ eine der folgenden Authentifizierungsmethoden aus:

Option	Beschreibung
<b>PSK (Pre Shared Key)</b>	Gibt an, dass der von NSX Edge und der Peer-Site gemeinsam genutzte geheime Schlüssel für die Authentifizierung verwendet wird. Der geheime Schlüssel kann eine Zeichenfolge mit einer Maximallänge von 128 Byte sein. Im FIPS-Modus ist die PSK-Authentifizierung deaktiviert.
<b>Zertifikat</b>	Gibt an, dass das auf globaler Ebene definierte Zertifikat für die Authentifizierung verwendet wird.

- 16 Geben Sie den Shared Key ein, wenn anonyme Sites eine Verbindung zum VPN-Dienst herstellen sollen.
- 17 Klicken Sie auf **Gemeinsam verwendeten Schlüssel anzeigen (Display Shared Key)**, um den Schlüssel auf der Peer-Site anzuzeigen.
- 18 Wählen Sie unter „Diffie-Hellman (DH)-Gruppe“ das kryptographische Schema aus, das es der Peer-Site und NSX Edge ermöglicht, über einen ungesicherten Kommunikationskanal einen gemeinsamen geheimen Schlüssel einzurichten.  
DH14 ist die Standardauswahl für den FIPS- und Nicht-FIPS-Modus. Bei aktiviertem FIPS-Modus sind DH2 und DH5 nicht verfügbar.
- 19 Geben Sie unter „Erweiterung“ eine der folgenden Optionen ein:
  - `securelocaltrafficbyip=IPAddress` zum Umleiten von lokalem Datenverkehr von der Edge-Instanz über den IPSec-VPN-Tunnel. Dies ist der Standardwert. Weitere Informationen finden Sie unter <http://kb.vmware.com/kb/20080007>.
  - `passthroughSubnets=PeerSubnet/IPAddress` zum Unterstützen überlappender Subnetze.
- 20 Klicken Sie auf **OK**.  
NSX Edge erstellt einen Tunnel vom lokalen Subnetz zum Peer-Subnetz.


## Nächste Schritte

Aktivieren Sie den IPSec-VPN-Dienst.

## Bearbeiten des IPSec-VPN-Diensts

Sie können einen IPSec-VPN-Dienst bearbeiten.


### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
- 5 Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
- 6 Wählen Sie den zu bearbeitenden IPSec-VPN-Dienst aus.
- 7 Klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- 8 Nehmen Sie die gewünschten Änderungen vor.
- 9 Klicken Sie auf **OK**.

## Deaktivieren der IPSec-VPN-Site

Sie können eine IPSec-VPN-Site deaktivieren.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
- 5 Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
- 6 Wählen Sie die IPSec-VPN-Site aus, die Sie deaktivieren möchten.
- 7 Klicken Sie auf das Symbol **Deaktivieren (Disable)** ().

## Löschen einer IPSec-VPN-Site

Sie können eine IPSec-VPN-Site löschen.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
- 5 Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
- 6 Wählen Sie die IPSec-VPN-Site aus, die Sie löschen möchten.
- 7 Klicken Sie auf das Symbol **Löschen (Delete)** (✖).

## Beispiele für die IPSec-VPN-Konfiguration

Dieses Szenario enthält Konfigurationsbeispiele für eine einfache IPSEC-VPN-Punkt-zu-Punkt-Verbindung zwischen einer NSX Edge-Instanz und einem Cisco- oder WatchGuard-VPN am anderen Ende.

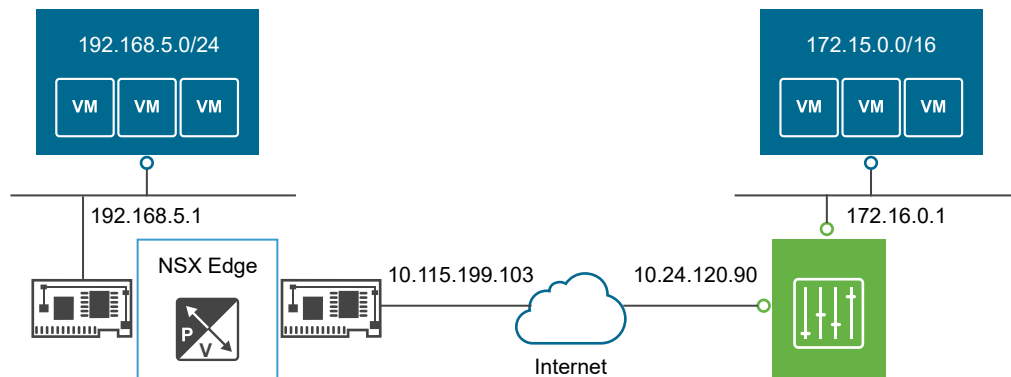
In diesem Szenario verbindet NSX Edge das interne Netzwerk 192.168.5.0/24 mit dem Internet. Die NSX Edge-Schnittstellen sind wie folgt konfiguriert:

- Uplink-Schnittstelle: 192.168.5.1
- Interne Schnittstelle: 10.115.199.103

Das Remote-Gateway verbindet das interne Netzwerk 172.15.0.0/16 mit dem Internet. Die Remote-Gateway-Schnittstellen sind wie folgt konfiguriert:

- Uplink-Schnittstelle: 10.24.120.90
- Interne Schnittstelle: 172.16.0.1

**Abbildung 14-1. NSX Edge stellt die Verbindung mit einem Remote-VPN-Gateway her**



**Hinweis** Für Tunnel zwischen NSX Edge und NSX Edge IPSEC können Sie dasselbe Szenario verwenden, indem Sie die zweite NSX Edge-Instanz als Remote-Gateway einrichten.

## Terminologie

IPSec ist eine Sammlung offener Standards. Die Protokolle der NSX Edge-Instanz und anderer VPN-Appliances, die Sie verwenden können, um Probleme mit IPSEC VPN zu beheben, enthalten viele technische Begriffe.

Dies sind einige der Standardeinträge, die vorkommen können:

- ISAKMP (Internet Security Association and Key Management Protocol), ein Protokoll für den Aufbau von Sicherheitsverbindungen (Security Associations, SA) und den Austausch kryptografischer Schlüssel in einer Internet-Umgebung, ist in RFC 2408 definiert. ISAKMP bietet nur einen Rahmen für die Authentifizierung und den Schlüsselaustausch und ist vom Schlüsselaustausch selbst unabhängig.
- Das Schlüsselvereinbarungsprotokoll Oakley ermöglicht es authentifizierten Parteien, Schlüsselmaterial unter Verwendung des Diffie-Hellman-Schlüsselaustauschalgorithmus über eine unsichere Verbindung auszutauschen.
- IKE (Internet Key Exchange) ist eine Kombination aus ISAKMP und Oakley. NSX Edge stellt IKEv1 bereit.
- Der Diffie-Hellman-Schlüsselaustausch (DH-Schlüsselaustausch) ist ein Protokoll aus dem Bereich der Kryptografie, das zwei Parteien ohne gegenseitige Kenntnisse voneinander ermöglicht, über einen unsicheren Kommunikationskanal einen gemeinsamen sicheren Schlüssel zu erzeugen. VSE unterstützt DH-Gruppe 2 (1024 Bits) und DH-Gruppe 5 (1536 Bits).

## IKE Phase 1 und Phase 2

IKE ist eine Standardmethode für den Aufbau einer sicheren, authentifizierten Kommunikation.

### Parameter der Phase 1

In Phase 1 wird die gegenseitige Authentifizierung der Peers eingerichtet, es werden kryptographische Parameter ausgehandelt und der Sitzungsschlüssel wird generiert. NSX Edge verwendet folgende Parameter der Phase 1:

- Main-Modus
- TripleDES / AES [konfigurierbar]
- SHA-1
- MODP-Gruppe 2 (1024 Bits)
- Pre-Shared Secret [konfigurierbar]
- SA-Lebensdauer von 28800 Sekunden (8 Stunden) ohne neu zugewiesene KB
- Aggressiver ISAKMP-Modus deaktiviert

## Parameter der Phase 2

In der IKE-Phase 2 wird ein IPSec-Tunnel ausgehandelt. Dabei wird das vom IPSec-Tunnel zu verwendende Schlüsselmaterial erstellt (entweder durch das Zugrundelegen der Schlüssel aus IKE-Phase 1 oder mit der Durchführung eines erneuten Schlüsselaustauschs). Folgende Parameter der IKE-Phase 2 werden von NSX Edge unterstützt:

- TripleDES / AES [entspricht der Einstellung in Phase 1]
- SHA-1
- ESP-Tunnelmodus
- MODP-Gruppe 2 (1024 Bits)
- PFS (Perfect Forward Secrecy) für Neuzuweisung
- SA-Lebensdauer von 3600 Sekunden (1 Stunde) ohne neu zugewiesene KB
- Selektoren für alle IP-Protokolle und alle Ports zwischen den beiden Netzen unter Verwendung von IPv4-Subnetzen

## Transaktionsmodus-Proben

NSX Edge unterstützt den Main-Modus für Phase 1 und den Quick-Modus für Phase 2.

NSX Edge schlägt eine Richtlinie vor, die PSK, 3DES/AES128, SHA-1 und die DH-Gruppe 2/5 erfordert. Der Peer muss diese Richtlinie akzeptieren, andernfalls scheitert die Aushandlungsphase.

## Phase 1: Main-Modus-Transaktionen

Dieses Beispiel zeigt den Austausch einer von NSX Edge zu einem Cisco-Gerät initiierten Phase-1-Aushandlung.

Die folgenden Transaktionen werden nacheinander zwischen NSX Edge und einem Cisco VPN-Gerät im Main-Modus durchgeführt.

- 1 NSX Edge an Cisco
  - Vorschlag: Verschlüsselung 3DES-CBC, SHA, PSK, Group5(Group2)
  - DPD aktiviert
- 2 Cisco an NSX Edge
  - enthält den von Cisco gewählten Vorschlag
  - Wenn das Cisco-Gerät keine der Parameter akzeptiert, die NSX Edge in Schritt 1 gesendet hat, sendet das Cisco-Gerät die Meldung mit dem Flag „NO\_PROPOSAL\_CHOSEN“ und beendet die Aushandlung.
- 3 NSX Edge an Cisco
  - DH-Schlüssel und Nonce
- 4 Cisco an NSX Edge
  - DH-Schlüssel und Nonce

## 5 NSX Edge an Cisco (verschlüsselt)

- ID verwenden (PSK)

## 6 Cisco an NSX Edge (verschlüsselt)

- ID verwenden (PSK)
- Wenn das Cisco-Gerät feststellt, dass der PSK nicht übereinstimmt, sendet es eine Nachricht mit dem Flag „INVALID\_ID\_INFORMATION“. Phase 1 schlägt fehl.

### Phase 2: Quick-Modus-Transaktionen

Die folgenden Transaktionen werden nacheinander zwischen NSX Edge und einem Cisco VPN-Gerät im Quick-Modus durchgeführt.

#### 1 NSX Edge an Cisco

NSX Edge schlägt dem Peer die Richtlinie für Phase 2 vor. Beispiel:

```
Aug 26 12:16:09 weiqing-desktop
ipsec[5789]:
"s1-c1" #2: initiating Quick Mode
PSK+ENCRYPT+TUNNEL+PFS+UP+SAREFTRACK
{using isakmp#1 msgid:d20849ac
proposal=3DES(3)_192-SHA1(2)_160
pfsgroup=0AKLEY_GROUP_MODP1024}
```

#### 2 Cisco an NSX Edge

Das Cisco-Gerät sendet NO\_PROPOSAL\_CHOSEN, falls es keine zu dem Vorschlag passende Richtlinie findet. Andernfalls sendet das Cisco-Gerät den Satz der gewählten Parameter.

#### 3 NSX Edge an Cisco

Um das Debuggen zu erleichtern, können Sie in NSX Edge die IPSec-Protokollierung einschalten und auf Cisco das Crypto-Debugging (debug crypto isakmp <Level>) aktivieren.

### Konfigurieren des IPSec-VPN-Diensts – Beispiel

Sie müssen VPN-Parameter konfigurieren und anschließend den IPSEC-Dienst aktivieren.

#### Verfahren

##### 1 Konfigurieren der IPSec-VPN-Parameter – Beispiel

Sie müssen mindestens eine externe IP-Adresse in NSX Edge konfigurieren, um den IPSec-VPN-Dienst bereitstellen zu können.

##### 2 Aktivieren des IPSec-VPN-Diensts – Beispiel

Sie müssen einen IPSec-VPN-Dienst aktivieren, damit der Datenverkehr vom lokalen Subnetz zum Peer-Subnetz übertragen werden kann.

## Konfigurieren der IPSec-VPN-Parameter – Beispiel

Sie müssen mindestens eine externe IP-Adresse in NSX Edge konfigurieren, um den IPSec-VPN-Dienst bereitstellen zu können.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
- 5 Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 7 Geben Sie einen Namen für das IPSec-VPN ein.
- 8 Geben Sie die IP-Adresse der NSX Edge-Instanz im Feld **Lokale ID (Local Id)** ein. Diese wird zur Peer-ID auf der Remote-Site.
- 9 Geben Sie die IP-Adresse des lokalen Endpunkts ein.

Wenn Sie unter Verwendung eines vorinstallierten Schlüssels (Pre-Shared Key) eine IP-Adresse zum IP-Tunnel hinzufügen, können die lokale ID und die ID des lokalen Endpunkts identisch sein.

- 10 Geben Sie die Subnetze, die von den Sites gemeinsam genutzt werden sollen, im CIDR-Format ein. Trennen Sie mehrere Subnetze jeweils durch ein Komma.
- 11 Geben Sie die Peer-ID ein, um die Peer-Site eindeutig zu identifizieren. Bei Peers mit Zertifikatsauthentifizierung muss diese ID der allgemeine Name (Common Name) im Peer-Zertifikat sein. Bei PSK-Peers kann diese ID eine beliebige Zeichenfolge sein. VMware empfiehlt, dass Sie die öffentliche IP-Adresse des VPN oder einen FQDN für den VPN-Dienst als Peer-ID verwenden.
- 12 Geben Sie im Feld „Peer-Endpoint“ die IP-Adresse der Peer-Site ein. Falls Sie das Feld leer lassen, wartet NSX Edge auf das Peer-Gerät, um eine Verbindung anzufordern.
- 13 Geben Sie die interne IP-Adresse des Peer-Subnetzes im CIDR-Format ein. Trennen Sie mehrere Subnetze jeweils durch ein Komma.
- 14 Wählen Sie den Verschlüsselungsalgorithmus aus.
- 15 Wählen Sie unter „Authentifizierungsmodell“ eine der folgenden Authentifizierungsmethoden aus:

Option	Beschreibung
<b>PSK (Pre Shared Key)</b>	Gibt an, dass der von NSX Edge und der Peer-Site gemeinsam genutzte geheime Schlüssel für die Authentifizierung verwendet wird. Der geheime Schlüssel kann eine Zeichenfolge mit einer Maximallänge von 128 Byte sein.
<b>Zertifikat</b>	Gibt an, dass das auf globaler Ebene definierte Zertifikat für die Authentifizierung verwendet wird.

- 16 Geben Sie den Shared Key ein, wenn anonyme Sites eine Verbindung zum VPN-Dienst herstellen sollen.
- 17 Klicken Sie auf **Gemeinsam verwendeten Schlüssel anzeigen (Display Shared Key)**, um den Schlüssel auf der Peer-Site anzuzeigen.
- 18 Wählen Sie unter „Diffie-Hellman (DH)-Gruppe“ das kryptographische Schema aus, das es der Peer-Site und NSX Edge ermöglicht, über einen ungesicherten Kommunikationskanal einen gemeinsamen geheimen Schlüssel einzurichten.
- 19 Ändern Sie den MTU-Schwellenwert, falls erforderlich.
- 20 Wählen Sie aus, ob der Schwellenwert für die perfekte Weiterleitungsgeheimhaltung (Perfect Forward Secrecy, PFS) aktiviert oder deaktiviert werden soll. Bei IPsec-Aushandlungen stellt Perfect Forward Secrecy (PFS) sicher, dass kein neuer kryptographischer Schlüssel eine Beziehung zu einem vorherigen Schlüssel hat.
- 21 Klicken Sie auf **OK**.

NSX Edge erstellt einen Tunnel vom lokalen Subnetz zum Peer-Subnetz.

#### Nächste Schritte

Aktivieren Sie den IPSec-VPN-Dienst.

#### Aktivieren des IPSec-VPN-Diensts – Beispiel

Sie müssen einen IPSec-VPN-Dienst aktivieren, damit der Datenverkehr vom lokalen Subnetz zum Peer-Subnetz übertragen werden kann.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **VPN**.
- 5 Klicken Sie auf **IPSec-VPN (IPSec VPN)**.
- 6 Klicken Sie auf **Aktivieren (Enable)**.

#### Nächste Schritte

Klicken Sie auf **Protokollierung aktivieren (Enable Logging)**, um den Datenverkehr zwischen dem lokalen Subnetz und dem Peer-Subnetz zu protokollieren.

#### Verwenden eines Cisco 2821 Integrated Services-Router

Im Folgenden werden Konfigurationen beschrieben, die unter Verwendung von Cisco IOS durchgeführt wurden.

## Verfahren

### 1 Konfigurieren von Schnittstellen und der Standardroute

```
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 10.24.123.253
```

### 2 Konfigurieren der IKE-Richtlinie

```
Router# config term
Router(config)# crypto isakmp policy 1
Router(config-isakmp)# encryption 3des
Router(config-isakmp)# group 2
Router(config-isakmp)# hash sha
Router(config-isakmp)# lifetime 28800
Router(config-isakmp)# authentication
 pre-share
Router(config-isakmp)# exit
```

### 3 PSS-Zuordnung für jeden Peer

```
Router# config term
Router(config)# crypto isakmp key vshield
 address 10.115.199.103
Router(config-isakmp)# exit
```

### 4 Definieren der IPSEC-Transformation

```
Router# config term
Router(config)# crypto ipsec transform-set
 myset esp-3des esp-sha-hmac
Router(config-isakmp)# exit
```

### 5 Erstellen der IPSEC-Zugriffsliste

```
Router# config term
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# access-list 101 permit ip
 172.16.0.0 0.0.255.255 192.168.5.0 0.0.0.255
Router(config)# exit
```

## 6 Binden der Richtlinie an eine Crypto Map und Bezeichnen der Crypto Map

Im folgenden Beispiel wird die Crypto Map mit „MYVPN“ bezeichnet.

```
Router# config term
Router(config)# crypto map MYVPN 1
 ipsec-isakmp
% NOTE: This new crypto map will remain
 disabled until a peer and a valid
 access list have been configured.
Router(config-crypto-map)# set transform-set
 myset
Router(config-crypto-map)# set pfs group1
Router(config-crypto-map)# set peer
 10.115.199.103
Router(config-crypto-map)# match address 101
Router(config-crypto-map)# exit
```

### Beispiel: Konfiguration

```
router2821#show running-config output
Building configuration...

Current configuration : 1263 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2821
!
boot-start-marker
boot-end-marker
!
! card type command needed for slot 0
! card type command needed for slot 1
enable password cisco
!
no aaa new-model
!
resource policy
!
ip subnet-zero
!
ip cef
!no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
```

```

crypto isakmp key vshield address 10.115.199.103
!
crypto ipsec transform-set myset esp-3des
 esp-sha-hmac
!
crypto map MYVPN 1 ipsec-isakmp
set peer 10.115.199.103
set transform-set myset
set pfs group1
match address 101
!
interface GigabitEthernet0/0
ip address 10.24.120.90 255.255.252.0
duplex auto
speed auto
crypto map MYVPN
!
interface GigabitEthernet0/1
ip address 172.16.0.1 255.255.0.0
duplex auto
speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.24.123.253
!
ip http server
no ip http secure-server
!
access-list 101 permit ip 172.16.0.0
 0.0.255.255 192.168.5.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
scheduler allocate 20000 1000
!
end

```

## Verwenden eines Cisco ASA 5510

Verwenden Sie die folgende Ausgabe für die Konfiguration von Cisco ASA 5510.

```

ciscoasa# show running-config output
: Saved
:
ASA Version 8.2(1)18
!

```

```

hostname ciscoasa
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0/0
nameif untrusted
security-level 100
ip address 10.24.120.90 255.255.252.0
!
interface Ethernet0/1
nameif trusted
security-level 90
ip address 172.16.0.1 255.255.0.0
!
interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
boot system disk0:/asa821-18-k8.bin
ftp mode passive
access-list ACL1 extended permit ip 172.16.0.0 255.255.0.0
 192.168.5.0 255.255.255.0
access-list ACL1 extended permit ip 192.168.5.0 255.255.255.0
 172.16.0.0 255.255.0.0
access-list 101 extended permit icmp any any
pager lines 24
mtu untrusted 1500
mtu trusted 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any untrusted
icmp permit any trusted
no asdm history enable
arp timeout 14400
access-group 101 in interface untrusted
access-group 101 out interface untrusted
access-group 101 in interface trusted
access-group 101 out interface trusted
route untrusted 10.115.0.0 255.255.0.0 10.24.123.253 1
route untrusted 192.168.5.0 255.255.255.0 10.115.199.103 1

```

```

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00
 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
crypto ipsec transform-set MYSET esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
crypto map MYVPN 1 match address ACL1
crypto map MYVPN 1 set pfs
crypto map MYVPN 1 set peer 10.115.199.103
crypto map MYVPN 1 set transform-set MYSET
crypto map MYVPN interface untrusted
crypto isakmp enable untrusted
crypto isakmp policy 1
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400
telnet 10.0.0.0 255.0.0.0 untrusted
telnet timeout 5
ssh timeout 5
console timeout 0
no threat-detection basic-threat
no threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password f3UhLvUj1QsXsuK7 encrypted
tunnel-group 10.115.199.103 type ipsec-l2l
tunnel-group 10.115.199.103 ipsec-attributes
pre-shared-key *
!
!
prompt hostname context
Cryptochecksum:29c3cc49460831ff6c070671098085a9
: end

```

## Konfigurieren einer WatchGuard Firebox X500

Sie können Ihre WatchGuard Firebox X500 als Remote-Gateway konfigurieren.

---

**Hinweis** Genaue Anweisungen finden Sie in Ihrer WatchGuard Firebox-Dokumentation.

---

## Verfahren

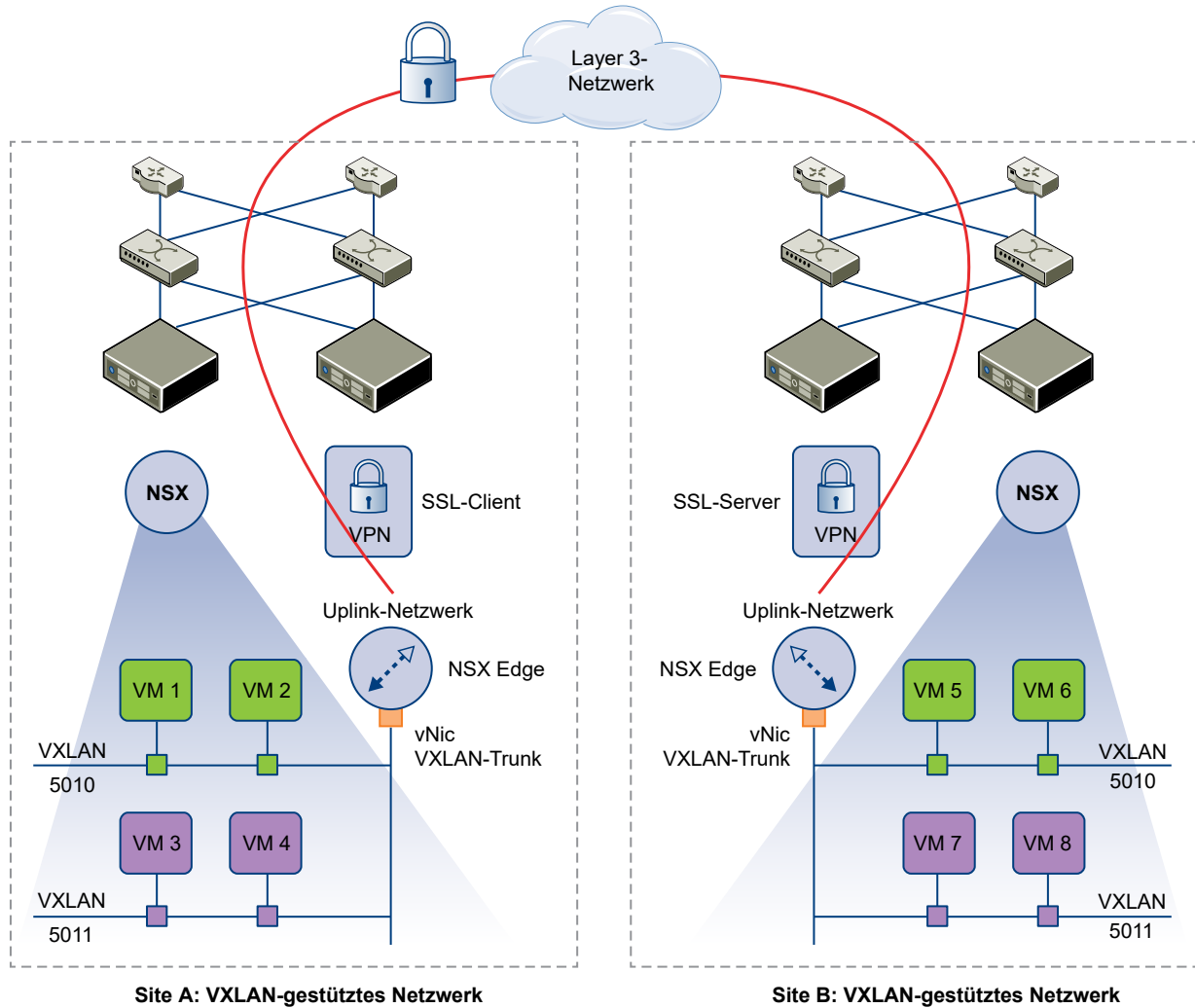
- 1 Wählen Sie in „Firebox System Manager“ **Tools > Policy Manager**.
- 2 Wählen Sie in „Policy Manager“ **Netzwerk (Network) > Konfiguration (Configuration)**.
- 3 Konfigurieren Sie die Schnittstellen und klicken Sie auf **OK**.
- 4 (Optional) Wählen Sie **Netzwerk (Network) > Routen (Routes)**, um eine Standardroute zu konfigurieren.
- 5 Wählen Sie **Netzwerk (Network) > Zweigstelle-VPN (Branch Office VPN) > Manuelle IPSec (Manual IPSec)**, um das Remote-Gateway zu konfigurieren.
- 6 Klicken Sie im Dialogfeld „IPSec-Konfiguration“ auf **Gateways**, um das IPSEC Remote-Gateway zu konfigurieren.
- 7 Klicken Sie im Dialogfeld „IPSec-Konfiguration“ auf **Tunnel (Tunnels)**, um einen Tunnel zu konfigurieren.
- 8 Klicken Sie im Dialogfeld „IPSec-Konfiguration“ auf **Hinzufügen (Add)**, um eine Routing-Richtlinie hinzuzufügen.
- 9 Klicken Sie auf **Schließen (Close)**.
- 10 Bestätigen Sie, dass der Tunnel aktiv ist.

## Überblick über L2 VPN

Mit L2 VPN können Sie mehrere physische logische Netzwerke (sowohl VLAN als auch VXLAN) über geographische Sites ausdehnen. Darüber hinaus können Sie mehrere Sites auf einem L2 VPN-Server konfigurieren. Virtuelle Maschinen verbleiben auf demselben Subnetz, auch wenn sie zwischen diesen Sites verschoben wurden, und ihre IP-Adressen ändern sich nicht. Die Egress-Optimierung ermöglicht es Edge, Pakete, die lokal zur Egress-Optimierungs-IP-Adresse gesendet wurden, zu routen, und alles andere zu bridgen.

Dadurch ermöglicht L2 VPN Unternehmen eine reibungslose und durch VXLAN oder VLAN gesicherte Migration von Arbeitslasten zwischen physisch getrennten Speicherorten. Für Cloud-Anbieter stellt L2 VPN einen Mechanismus zur Verfügung, mit dem Sie Mandanten aufnehmen können, ohne die bestehenden IP-Adressen für Arbeitslasten und Anwendungen ändern zu müssen.

Abbildung 14-2. Ausweitung von VXLAN über mehrere Sites mithilfe von L2 VPN

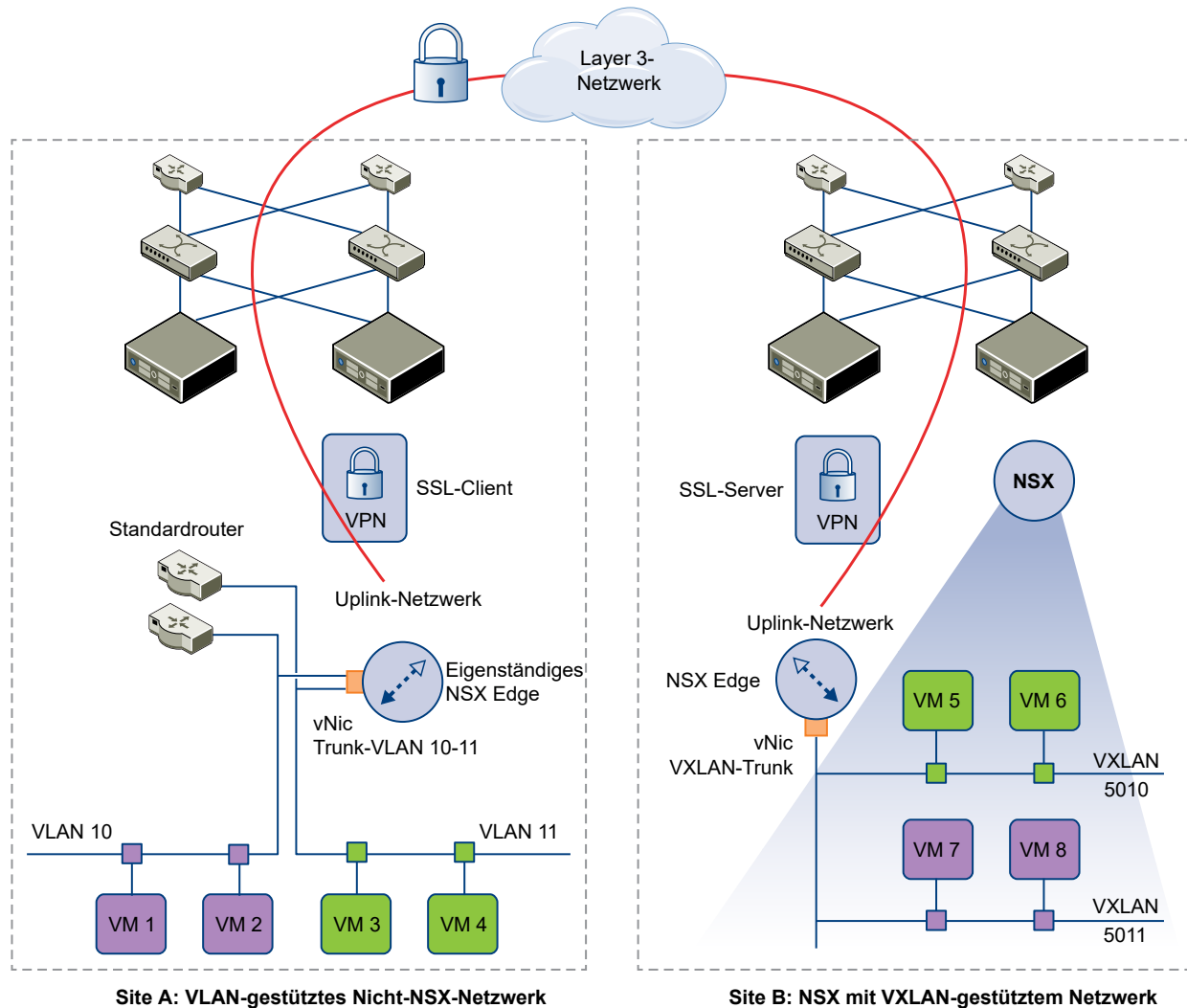


Die L2 VPN-Client und -Server rufen die MAC-Adressen sowohl in lokalen als auch in Remote-Sites auf der Grundlage des über sie übertragenen Datenverkehrs ab. Die Egress-Optimierung behält lokales Routing bei, da das Standard-Gateway für alle virtuellen Maschinen unter Einsatz von Firewallregeln immer in das lokale Gateway aufgelöst wird. Virtuelle Maschinen, die nicht zur Site B migriert wurden, können ebenfalls auf L2-Segmente zugreifen, die auf Site A nicht ausgedehnt wurden.

Wird eine der Sites nicht von NSX gesichert, dann kann auf dieser Site eigenständiges NSX Edge bereitgestellt werden.

In der folgenden Grafik dehnt L2 VPN Netzwerk VLAN 10 zu VXLAN 5010 und VLAN 11 zu VXLAN 5011 aus. So hat eine mit VLAN 10 gebridgete VM 1 Zugriff auf die VMs 2, 5 und 6.

**Abbildung 14-3. Die Ausweitung einer Nicht-NSX-Site mit VLAN-basierten Netzwerken zu einer NSX-Site mit VXLAN-basierten Netzwerken**



## Konfigurieren von L2 VPN

Um Ihr Netzwerk mit L2 VPN auszuweiten, konfigurieren Sie einen L2 VPN-Server (Ziel-Edge) und einen L2 VPN-Client (Quell-Edge). Sie müssen den L2 VPN-Dienst auf dem Server und Client aktivieren.

### Voraussetzungen

Es muss eine Teilschnittstelle in einer Trunk-Schnittstelle von NSX Edge hinzugefügt werden. Weitere Informationen dazu finden Sie unter [Hinzufügen einer Teilschnittstelle](#).

### L2 VPN – Best Practices

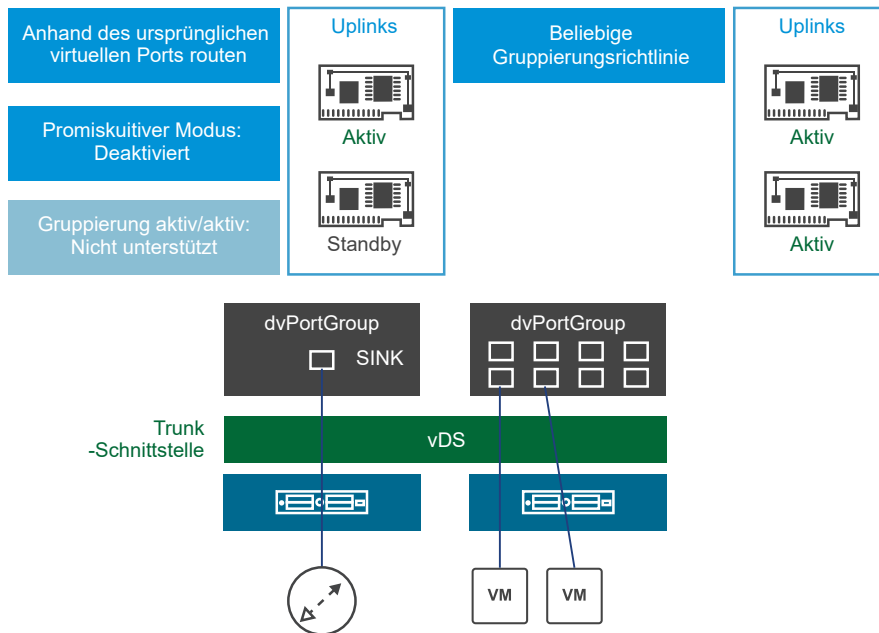
Indem Sie L2 VPN entsprechend den Best Practices konfigurieren, können Sie Problem wie Schleifen sowie doppelte Pings und Antworten vermeiden.

## L2VPN-Optionen zum Verringern des Loopings

Es gibt zwei Optionen, um das Looping zu verringern. Die NSX Edges und virtuellen Maschinen können sich auf unterschiedlichen oder auf demselben ESXi-Host befinden.

### Option 1: Unterschiedliche ESXi-Hosts für die L2VPN Edges und die virtuellen Maschinen

#### 1. Bereitstellen von L2VPN Edges und VMs auf separaten ESXi-Hosts



- 1 Stellen Sie die Edges und die virtuellen Maschinen auf getrennten ESXi-Hosts bereit.
- 2 Konfigurieren Sie die Gruppierungs- und Failover-Richtlinie für die der TRUNK vNic des Edges zugeordnete verteilte Portgruppe wie folgt:
  - a Load Balancing: „Anhand des ursprünglichen virtuellen Ports routen“.
  - b Konfigurieren Sie nur einen Uplink als „Aktiv“ und den anderen Uplink als „Standby“.
- 3 Konfigurieren Sie die Gruppierungs- und Failover-Richtlinie für die den virtuellen Maschinen zugeordnete verteilte Portgruppe wie folgt:
  - a Jede Gruppierungsrichtlinie kann verwendet werden.
  - b Mehrere aktive Uplinks können konfiguriert werden.

- 4 Konfigurieren Sie Edges für die Verwendung des SINK-Portmodus und deaktivieren Sie den Promiscuous-Modus auf der TRUNK vNic.

---

### Hinweis

- Promiskuitiven Modus deaktivieren: Wenn Sie einen vSphere Distributed Switch verwenden.
- Promiskuitiven Modus aktivieren: Wenn Sie den virtuellen Switch verwenden, um die Trunk-Schnittstelle zu konfigurieren.

Wenn für einen virtuellen Switch der promiskuitive Modus aktiviert ist, werden einige Pakete nicht verworfen, die von den Uplinks eingehen, die derzeit nicht vom promiskuitiven Port verwendet werden. Sie sollten ReversePathFwdCheckPromisc aktivieren und dann deaktivieren. Für den promiskuitiven Port werden dann explizit alle Pakete, die von den derzeit nicht verwendeten Uplinks eingehen, verworfen.

Um die duplizierten Pakete zu blockieren, aktivieren Sie die RPF-Überprüfung für den promiskuitiven Modus in der ESXi-CLI, in der NSX Edge vorhanden ist:

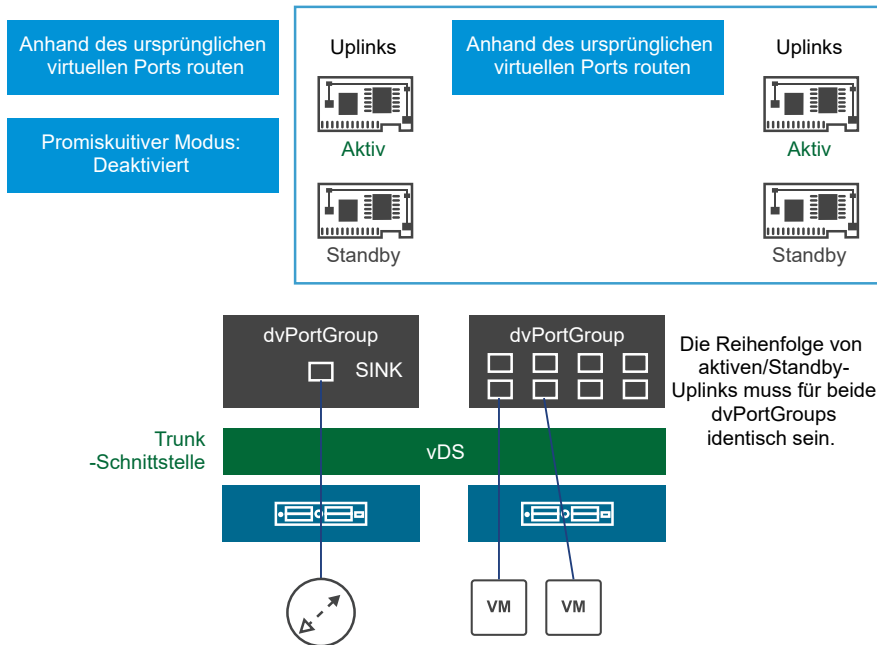
```
esxcli system settings advanced set -o /Net/ReversePathFwdCheckPromisc -i 1
esxcli system settings advanced list -o /Net/ReversePathFwdCheckPromisc
Path: /Net/ReversePathFwdCheckPromisc
Type: integer
Int Value: 1
Default Int Value: 0
Max Value: 1
Min Value: 0
String Value:
Default String Value:
Valid Characters:
Description: Block duplicate packet in a teamed environment when the virtual switch is set to
Promiscuous mode.
```

Ändern Sie in der Sicherheitsrichtlinie **PortGroup** für **PromiscuousMode** den Wert von **Akzeptieren (Accept)** zu **Ablehnen (Reject)** und wieder zu **Akzeptieren (Accept)**, um die konfigurierte Änderung zu aktivieren.

---

- Option 2: Edges und virtuelle Maschinen auf demselben ESXi-Host

## 2. Bereitstellen von L2VPN Edges und VMs auf demselben Host



- a Konfigurieren Sie die Gruppierungs- und Failover-Richtlinie für die der TRUNK vNic des Edges zugeordnete verteilte Portgruppe wie folgt:
  - 1 Load Balancing: „Anhand des ursprünglichen virtuellen Ports routen“.
  - 2 Konfigurieren Sie einen Uplink als „Aktiv“ und den anderen Uplink als „Standby“.
- b Konfigurieren Sie die Gruppierungs- und Failover-Richtlinie für die den virtuellen Maschinen zugeordnete verteilte Portgruppe wie folgt:
  - 1 Jede Gruppierungsrichtlinie kann verwendet werden.
  - 2 Nur ein Uplink kann aktiv sein.
  - 3 Die Reihenfolge der aktiven/Standby-Uplinks muss für die verteilte Portgruppe der virtuellen Maschine und die verteilte Portgruppe der TRUNK vNic des Edges identisch sein.
- c Konfigurieren Sie das clientseitige eigenständige Edge für die Verwendung des SINK-Portmodus und deaktivieren Sie den Promiscuous-Modus auf der TRUNK vNic.

**Konfigurieren eines Sink-Ports**

Wenn ein von NSX verwaltetes NSX Edge als L2 VPN-Client eingerichtet wird, erfolgt ein Teil der Konfiguration automatisch von NSX. Wenn ein eigenständiges NSX Edge als L2 VPN-Client eingerichtet wird, müssen diese Konfigurationsschritte manuell ausgeführt werden.

Wenn auf einem der VPN-Standorte NSX nicht bereitgestellt ist, können Sie ein L2 VPN konfigurieren, indem Sie an diesem Standort ein eigenständiges NSX Edge bereitstellen. Ein eigenständiges Edge wird unter Verwendung einer OVF-Datei auf einem Host bereitgestellt, der nicht von NSX verwaltet wird.

Dadurch wird eine Edge Services Gateway-Appliance bereitgestellt, die als ein L2-VPN-Client funktioniert.

Wenn eine eigenständige Edge Trunk-vNIC mit einem vSphere Distributed Switch verbunden ist, ist entweder der Promiscuous-Modus oder ein Sink-Port erforderlich, damit L2 VPN funktioniert. Die Verwendung des Promiscuous-Modus kann doppelte Pings und doppelte Antworten verursachen. Verwenden Sie aus diesem Grund den Sink-Portmodus bei der Konfiguration des eigenständigen L2 VPN NSX Edge.

## Verfahren

- 1 Rufen Sie die Portnummer für die Trunk-vNIC ab, die Sie als Sink-Port konfigurieren möchten.
  - a Melden Sie sich beim vSphere Web Client an und navigieren Sie zu **Home > Networking**.
  - b Klicken Sie auf die verteilte Portgruppe, mit der die NSX Edge-Trunk-Schnittstelle verbunden ist, und klicken Sie dann auf **Ports**, um die Ports und verbundenen VMs anzuzeigen. Beachten Sie die Portnummer, die der Trunk-Schnittstelle zugeordnet ist.

Verwenden Sie diese Portnummer, wenn Sie Opaque-Daten abrufen und aktualisieren.

- 2 Rufen Sie den dvsUuid-Wert für den vSphere Distributed Switch ab.
  - a Melden Sie sich bei der vCenter Mob-Benutzeroberfläche unter `https://<vc-ip>/mob` an.
  - b Klicken Sie auf **Inhalt (content)**.
  - c Klicken Sie auf den Link für den **rootFolder** (Beispiel: *group-d1 [Datacenter]*).
  - d Klicken Sie auf den Link für das **childEntity** (Beispiel: *Datacenter-1*).
  - e Klicken Sie auf den Link für den **networkFolder** (Beispiel: *Gruppe-n6*).
  - f Klicken Sie auf den DVS-Namens-Link für den vSphere Distributed Switch, der NSX Edges zugeordnet ist (Beispiel: *dvs-1 [Mgmt\_VDS]*).
  - g Kopieren Sie den Wert der UUID-Zeichenfolge.

Verwenden Sie diesen Wert für dvsUuid, wenn Sie Opaque-Daten abrufen und aktualisieren.

- 3 Überprüfen Sie, ob Opaque-Daten für den angegebenen Port vorhanden sind.
  - a Wechseln Sie zu `https://<vc-ip>/mob/?moid=DVSManager&vmodl=1`.
  - b Klicken Sie auf **fetchOpaqueDataEx**.
  - c Fügen Sie die folgende XML-Eingabe in das Feld für den **selectionSet** ein:

```
<selectionSet xsi:type="DVPortSelection">
 <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid -->
 <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

Verwenden Sie die abgerufene Port-Nummer und den dvsUuid-Wert für die NSX Edge-Trunk-Schnittstelle.

- d Legen Sie `isRuntime` auf `false` fest.
- e Klicken Sie auf **Methode aufrufen (Invoke Method)**.

Wenn das Ergebnis Werte für `vim.dvs.OpaqueData.ConfigInfo` anzeigt, ist bereits ein Opaque-Datensatz vorhanden. Verwenden Sie in diesem Fall den Vorgang `edit`, wenn Sie den Sink-Port festlegen. Wenn kein Wert für `vim.dvs.OpaqueData.ConfigInfo` angezeigt wird, verwenden Sie die Operation `add`, wenn Sie den Sink-Port festlegen.

- 4 Konfigurieren Sie den Sink-Port im Browser für verwaltete Objekte (Managed Object Browser, MOB) von vCenter.
  - a Wechseln Sie zu `https://<vc-ip>/mob/?moid=DVSManager&vmodl=1`.
  - b Klicken Sie auf **updateOpaqueDataEx**.
  - c Fügen Sie die folgende XML-Eingabe in das Feld für den **selectionSet** ein:

```
<selectionSet xsi:type="DVPortSelection">
 <dvsUuid>c2 1d 11 50 6a 7c 77 68-e6 ba ce 6a 1d 96 2a 15</dvsUuid> <!-- example dvsUuid --
>
 <portKey>393</portKey> <!-- example port number -->
</selectionSet>
```

Verwenden Sie den `dvsUuid`-Wert, den Sie von vCenter MOB abgerufen haben.

- d Fügen Sie eine der folgenden XML-Eingaben in das Feld für die „opaqueDataSpec“ ein:

Verwenden Sie diese Eingabe, um einen SINK-Port zu aktivieren, wenn keine Opaque-Daten festgelegt sind (wenn operation auf add festgelegt ist):

```
<opaqueDataSpec>
 <operation>add</operation>
 <opaqueData>
 <key>com.vmware.etherswitch.port.extraEthFRP</key>
 <opaqueData
xsi:type="vmodl.Binary">AAABAA
AA
AA
AAAAAAAA=</opaqueData>
 </opaqueData>
</opaqueDataSpec>
```

Verwenden Sie diese Eingabe, um einen SINK-Port zu aktivieren, wenn bereits Opaque-Daten festgelegt sind (wenn operation auf edit festgelegt ist):

```
<opaqueDataSpec>
 <operation>edit</operation>
 <opaqueData>
 <key>com.vmware.etherswitch.port.extraEthFRP</key>
 <opaqueData
xsi:type="vmodl.Binary">AAABAA
AA
AA
AAAAAAAA=</opaqueData>
 </opaqueData>
</opaqueDataSpec>
```

Verwenden Sie diese Eingabe, um einen SINK-Port zu deaktivieren:

```
<opaqueDataSpec>
 <operation>edit</operation>
 <opaqueData>
 <key>com.vmware.etherswitch.port.extraEthFRP</key>
 <opaqueData
xsi:type="vmodl.Binary">AA
AA
AA
AAAAAAAA=</opaqueData>
 </opaqueData>
</opaqueDataSpec>
```

- e Legen Sie isRuntime auf false fest.
- f Klicken Sie auf **Methode aufrufen (Invoke Method)**.

## Konfigurieren eines L2 VPN-Servers

Der L2 VPN-Server ist das Ziel-NSX Edge, mit dem der Client verbunden werden soll.

## Verfahren

- 1 Wählen Sie auf der Registerkarte **L2 VPN** die Option **Server** aus und klicken Sie auf **Ändern (Change)**.
- 2 Geben Sie unter **Listener-IP (Listener IP)** die primäre oder sekundäre IP-Adresse einer externen Schnittstelle des NSX Edge ein.
- 3 Der Standardport für den L2 VPN-Dienst ist 443. Bearbeiten Sie die Portnummer, falls erforderlich.
- 4 Wählen Sie den Verschlüsselungsalgorithmus für die Kommunikation zwischen dem Server und dem Client aus.
- 5 Wählen Sie das Zertifikat aus, das an den SSL VPN-Server gebunden werden soll.

---

**Wichtig** L2-VPN über SSL-Dienst unterstützt nur RSA-Zertifikate.

---

- 6 Klicken Sie auf **OK**.

## Hinzufügen von Peer-Sites

Sie können mehrere Sites zum L2 VPN-Server hinzufügen.

---

**Hinweis** Wenn Sie die Einstellungen für die Site-Konfiguration verändern, werden von NSX Edge alle vorhandenen Verbindungen getrennt und anschließend wiederhergestellt.

---

## Verfahren

- 1 Stellen Sie auf der Registerkarte „L2 VPN“ sicher, dass beim **L2 VPN-Modus (L2 VPN Mode)** die Option **Server** eingestellt ist.
- 2 Klicken Sie unter **Site-Konfigurationsdetails (Site Configuration Details)** auf das Symbol **Hinzufügen (Add)**.
- 3 Geben Sie einen eindeutigen Namen für die Peer-Site ein.
- 4 Geben Sie den Benutzernamen und das Kennwort ein, mit dem die Peer-Site authentifiziert werden soll. Die Anmeldedaten auf der Peer-Site sollten dieselben wie die auf der Client-Site sein.
- 5 Klicken Sie unter **Ausgeweitete Schnittstellen (Stretched Interfaces)** auf **Teilschnittstellen auswählen (Select Sub Interfaces)**, um Teilschnittstellen auszuwählen, die mit dem Client erweitert werden sollen.
  - a Wählen Sie unter „Objekt auswählen“ die Trunk-Schnittstelle für die Edge-Instanz aus.  
Die auf der Trunk vNIC konfigurierten Teilschnittstellen werden angezeigt.
  - b Doppelklicken Sie auf die auszuweitenden Teilschnittstellen.
  - c Klicken Sie auf **OK**.
- 6 Wenn das Standard-Gateway für virtuelle Maschinen für die beiden Sites dasselbe ist, geben Sie die Gateway-IP-Adressen in das Textfeld **Egress-Optimierungs-Gateway-Adresse (Egress Optimization Gateway Address)** ein. Bei diesen IP-Adressen handelt es sich um die Adressen, für die der Datenverkehr lokal weitergeleitet oder über den Tunnel blockiert werden soll.

- 7 (Optional) Aktivieren Sie das Kontrollkästchen **Nicht erweiterte Netzwerke aktivieren (Enable Unstretched Networks)**, wenn die VMs auf den nicht ausgetesteten Netzwerken mit den VMs kommunizieren sollen, die sich hinter dem L2-VPN-Client-Edge auf dem ausgetesteten Netzwerk befinden. Darüber hinaus soll diese Kommunikation über den gleichen L2-VPN-Tunnel geleitet werden. Nicht ausgetestete Subnetze können sich entweder hinter dem L2-VPN-Server-Edge, dem L2-VPN-Client-Edge oder hinter beiden befinden.

Gehen wir beispielsweise davon aus, dass Sie einen L2-VPN-Tunnel erstellt haben, um das 192.168.10.0/24-Subnetzwerk mithilfe des NSX-L2-VPN-Dienstes zwischen zwei Datacenter-Sites auszuweiten.

Hinter dem L2-VPN-Server-Edge befinden sich zwei zusätzliche Subnetze (z. B. 192.168.20.0/24 und 192.168.30.0/24). Wenn nicht ausgetestete Netzwerke aktiviert sind, können die VMs auf den Subnetzen 192.168.20.0/24 und 192.168.30.0/24 mit den VMs kommunizieren, die sich hinter dem L2-VPN-Client-Edge auf dem ausgetesteten Netzwerk (192.168.10.0/24) befinden. Diese Kommunikation wird über denselben L2-VPN-Tunnel geleitet.

- 8 Wenn Sie nicht ausgetestete Netzwerke aktiviert haben, führen Sie diese Schritte aus, je nachdem, wo sich die nicht ausgetesteten Subnetze befinden:
- Wenn sich nicht ausgetestete Subnetze hinter dem L2-VPN-Client-Edge befinden, geben Sie beim Hinzufügen der Peer-Site (Client) die Netzwerkadresse des nicht ausgetesteten Netzwerks im CIDR-Format beim L2-VPN-Server-Edge ein. Um mehrere nicht ausgetestete Netzwerke einzugeben, trennen Sie die Netzwerkadressen durch Kommas.
  - Wenn sich nicht ausgetestete Subnetze hinter dem L2-VPN-Server-Edge befinden, lassen Sie das Textfeld **Nicht ausgetestete Netzwerke (Unstretched Networks)** leer. Geben Sie also die Netzwerkadresse der nicht ausgetesteten Netzwerke beim Hinzufügen der Peer-Site (Client) beim L2-VPN-Server nicht an.

Im Beispiel oben müssen Sie das Textfeld **Nicht ausgetestete Netzwerke (Unstretched Networks)** im Fenster **Hinzufügen der Peer-Site** leer lassen, da sich die nicht ausgetesteten Subnetze hinter dem L2-VPN-Server-Edge befinden.

- 9 Klicken Sie auf **OK** und anschließend auf **Änderungen veröffentlichen (Publish Changes)**.

## Aktivieren eines L2-VPN-Diensts auf dem Server

Aktivieren Sie zunächst den L2 VPN-Dienst auf dem L2 VPN-Server (Ziel-NSX Edge). Ist HA bereits auf dieser Edge-Appliance konfiguriert, dann stellen Sie sicher, dass für die Edge-Instanz mehr als eine interne Schnittstelle konfiguriert ist. Ist nur eine einzige Schnittstelle vorhanden, die bereits von HA verwendet wurde, dann schlägt eine L2 VPN-Konfiguration auf derselben internen Schnittstelle fehl.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.

- 3 Doppelklicken Sie auf ein Ziel-NSX Edge und navigieren Sie zu **Verwalten (Manage) > VPN > L2 VPN**.
- 4 Klicken Sie neben **L2-VPN-Dienststatus (L2 VPN Service Status)** auf **Start**.

#### Nächste Schritte

Erstellen Sie eine NAT- oder Firewall-Regel auf der dem Internet zugewandten Seite der Firewall, um eine Verbindung des Clients mit dem Server zu ermöglichen.

## Konfigurieren eines L2 VPN-Clients

Der L2 VPN-Client ist das Quell-NSX Edge, das die Kommunikation mit dem Ziel-Edge initiiert (L2 VPN-Server).

Sie können auch ein eigenständiges Edge als L2 VPN-Client konfigurieren. Weitere Informationen dazu finden Sie unter [Konfigurieren eines eigenständigen Edge als L2 VPN-Client](#).

#### Verfahren

- 1 Legen Sie auf der Registerkarte „L2 VPN“ den **L2 VPN-Modus (L2 VPN Mode)** auf **Client** fest und klicken Sie auf **Ändern (Change)**.
- 2 Geben Sie die Adresse des L2 VPN-Servers ein, zu dem eine Verbindung dieses Clients hergestellt werden soll. Die Adresse kann der Hostname oder die IP-Adresse sein.
- 3 Bearbeiten Sie, falls nötig, den Standardport, zu dem der L2-VPN-Client eine Verbindung herstellen muss.
- 4 Wählen Sie den Verschlüsselungsalgorithmus für die Kommunikation mit dem Server aus.
- 5 Klicken Sie in **Ausgeweitete Schnittstellen (Stretched Interfaces)** auf **Teilschnittstellen auswählen (Select Sub Interfaces)**, um die Teilschnittstellen auszuwählen, die auf den Server ausgeweitet werden sollen.
  - a Wählen Sie unter **Objekt auswählen (Select Object)** die Trunk-Schnittstelle für die Edge-Instanz aus.  
Die auf der Trunk vNIC konfigurierten Teilschnittstellen werden angezeigt.
  - b Doppelklicken Sie auf die auszuweitenden Teilschnittstellen.
  - c Klicken Sie auf **OK**.
- 6 Geben Sie eine Beschreibung ein.
- 7 Geben Sie in **Egress-Optimierungs-Gateway-Adresse (Egress Optimization Gateway Address)** die Gateway-IP-Adresse der Teilschnittstellen oder die IP-Adressen ein, zu denen kein Datenverkehr über den Tunnel fließen soll.

- 8 (Optional) Aktivieren Sie das Kontrollkästchen **Nicht erweiterte Netzwerke aktivieren (Enable Unstretched Networks)**, wenn die VMs auf den nicht ausgeweiteten Netzwerken mit den VMs kommunizieren sollen, die sich hinter dem L2-VPN-Server-Edge auf dem ausgeweiteten Netzwerk befinden. Darüber hinaus soll diese Kommunikation über den gleichen L2-VPN-Tunnel geleitet werden. Nicht ausgeweitete Subnetze können sich entweder hinter dem L2-VPN-Server-Edge, dem L2-VPN-Client-Edge oder hinter beiden befinden.

Gehen wir beispielsweise davon aus, dass Sie einen L2-VPN-Tunnel erstellt haben, um das 192.168.10.0/24-Subnetzwerk mithilfe des NSX-L2-VPN-Dienstes zwischen zwei Datacenter-Sites auszuweiten.

Hinter dem L2-VPN-Server-Edge befinden sich zwei zusätzliche Subnetze (z. B. 192.168.20.0/24 und 192.168.30.0/24). Wenn nicht ausgeweitete Netzwerke aktiviert sind, können die VMs auf den Subnetzen 192.168.20.0/24 und 192.168.30.0/24 mit den VMs kommunizieren, die sich hinter dem L2-VPN-Server-Edge auf dem ausgeweiteten Netzwerk (192.168.10.0/24) befinden. Diese Kommunikation wird über denselben L2-VPN-Tunnel geleitet.

- 9 Wenn Sie nicht ausgeweitete Netzwerke aktiviert haben, führen Sie diese Schritte aus, je nachdem, wo sich die nicht ausgeweiteten Subnetze befinden:
- Wenn sich nicht ausgeweitete Subnetze hinter dem L2-VPN-Server-Edge befinden, geben Sie beim Konfigurieren des L2-VPN-Client-Edge die Netzwerkadresse des nicht ausgeweiteten Netzwerks im CIDR-Format ein. Um mehrere nicht ausgeweitete Netzwerke einzugeben, trennen Sie die Netzwerkadressen durch Kommas.
  - Wenn sich nicht ausgeweitete Subnetze hinter dem L2-VPN-Client-Edge befinden, lassen Sie das Textfeld **Nicht ausgeweitete Netzwerke (Unstretched Networks)** leer. Geben Sie also die Netzwerkadresse der nicht ausgeweiteten Netzwerke nicht auf dem L2-VPN-Client-Edge ein.
- Im Beispiel oben müssen Sie die nicht ausgeweiteten Netzwerke beim Konfigurieren des L2-VPN-Client-Edge als **192.168.20.0/24, 192.168.30.0/24** eingeben, da sich die nicht ausgeweiteten Subnetze hinter dem L2-VPN-Server-Edge befinden.
- 10 Geben Sie in **Benutzerdetails (User Details)** die Anmeldedaten für die Authentifizierung am Server ein.
- 11 Klicken Sie auf die Registerkarte **Erweitert (Advanced)**.

Wenn das Client-NSX Edge nicht direkt auf das Internet zugreifen kann und das Quell-NSX Edge (Server) über einen Proxy-Server erreichen muss, geben Sie die **Proxy-Einstellungen (Proxy Settings)** an.

- 12 Um nur sichere Proxy-Verbindungen zu aktivieren, wählen Sie **Sicheres Proxy aktivieren (Enable Secure Proxy)** aus.
- 13 Geben Sie die Adresse, den Port, den Benutzernamen und das Kennwort für den Proxy-Server ein.
- 14 Um die Prüfung von Serverzertifikaten zu aktivieren, wählen Sie **Serverzertifikat prüfen (Validate Server Certificate)** und das entsprechende Zertifikat aus.
- 15 Klicken Sie auf **OK** und anschließend auf **Änderungen veröffentlichen (Publish Changes)**.

## Nächste Schritte

Stellen Sie sicher, dass die Internet-Firewall zulässt, dass Datenverkehr von L2 VPN Edge zum Internet fließen kann. Der Zielport lautet 443.

## Aktivieren eines L2-VPN-Diensts auf Client

Aktivieren Sie zunächst den L2 VPN-Dienst auf dem L2 VPN-Client (Quellen-NSX Edge).

### Verfahren

- 1 Navigieren Sie für das Quell-NSX Edge zu **Verwalten (Manage) > VPN > L2 VPN**.
- 2 Klicken Sie neben **L2-VPN-Dienststatus (L2 VPN Service Status)** auf **Start**.

### Nächste Schritte

- Damit sich der Client und der Server miteinander verbinden können, müssen Sie auf der Internetseite der Firewall NAT- oder Firewallregeln erstellen.
- Wird eine von einer Standardportgruppe unterstützte Trunk-vNIC erweitert, dann aktivieren Sie den L2-VPN-Datenverkehr manuell, indem Sie folgende Schritte ausführen:
  - a Setzen Sie den **Promiscuous-Modus (Promiscuous mode)** auf **Akzeptieren (Accept)**.
  - b Setzen Sie **Gefälschte Übertragungen (Forged Transmits)** auf **Akzeptieren (Accept)**.

Weitere Informationen zu Vorgängen im Promiscuous-Modus und gefälschten Übertragungen, finden Sie im Abschnitt zu vSphere Standard-Switches in der *Dokumentation zu VMware vSphere*®.

## Konfigurieren eines eigenständigen Edge als L2 VPN-Client

Wenn eine der Sites, die Sie ausweiten möchten, nicht von NSX gestützt wird, können Sie ein eigenständiges Edge als L2 VPN-Client auf dieser Site bereitstellen.

Wenn Sie den FIPS-Modus für ein eigenständiges Edge ändern möchten, verwenden Sie den Befehl `fips enable` oder `fips disable`. Weitere Informationen finden Sie unter *Befehlszeilenschnittstellen-Referenz zu NSX*.

### Voraussetzungen

Sie haben eine Trunk-Portgruppe erstellt, mit der sich die Trunk-Schnittstelle des eigenständigen Edge verbindet. Für diese Portgruppe ist eine gewisse manuelle Konfiguration erforderlich:

- Wenn sich die Trunk-Portgruppe auf einem vSphere Standard Switch befindet, müssen Sie die folgenden Schritte ausführen:
  - Aktivieren erzwungener Übertragungen
  - Aktivieren des Promiscuous-Modus

Weitere Informationen finden Sie im *vSphere-Netzwerk*.

- Wenn sich die Trunk-Portgruppe auf einem vSphere Distributed Switch befindet, müssen Sie die folgenden Schritte ausführen:
  - Aktivieren erzwungener Übertragungen Weitere Informationen finden Sie im *vSphere-Netzwerk*.
  - Aktivieren Sie den Sink-Port für die Trunk-vNic oder aktivieren Sie den Promiscuous-Modus. Das Aktivieren des Sink-Ports ist die empfohlene Vorgehensweise.

Die Sink-Portkonfiguration muss erfolgen, nachdem das eigenständige Edge bereitgestellt wurde, weil Sie die Konfiguration des mit der Edge-Trunk-vNIC verbundenen Ports ändern müssen.

## Verfahren

- 1 Verwenden Sie den vSphere Web Client zum Anmelden bei dem vCenter Server, der die Nicht-NSX-Umgebung verwaltet.
- 2 Wählen Sie **Hosts und Cluster (Hosts and Clusters)** aus und erweitern Sie die Cluster zum Anzeigen der verfügbaren Hosts.
- 3 Klicken Sie mit der rechten Maustaste auf den Host, auf dem Sie das eigenständige Edge installieren möchten, und wählen Sie **OVF-Vorlage bereitstellen (Deploy OVF Template)** aus.
- 4 Geben Sie die URL ein, um die OVF-Datei aus dem Internet herunterzuladen und zu installieren, oder klicken Sie auf **Durchsuchen (Browse)**, um nach dem Ordner auf Ihrem Computer zu suchen, der die OVF-Datei des eigenständigen Edge enthält, und klicken Sie auf **Weiter (Next)**.
- 5 Überprüfen Sie auf der Seite „Einzelheiten zur OVF-Vorlage“ die Vorlagendetails und klicken Sie auf **Weiter (Next)**.
- 6 Geben Sie auf der Seite „Name und Ordner auswählen“ einen Namen für das eigenständige Edge ein und wählen Sie den Ordner oder das Datacenter für die Bereitstellung aus. Klicken Sie anschließend auf **Weiter (Next)**.
- 7 Wählen Sie auf der Seite „Speicher auswählen“ den Speicherort für die Dateien der bereitgestellten Vorlage aus.
- 8 Konfigurieren Sie auf der Seite „Netzwerke auswählen“ die Netzwerke aus, die die bereitgestellte Vorlage verwenden soll. Klicken Sie auf **Weiter (Next)**.
  - Die öffentliche Schnittstelle ist die Uplink-Schnittstelle.
  - Mit der Trunk-Schnittstelle werden die Teilschnittstellen erstellt, die ausgeweitet werden. Verbinden Sie diese Schnittstelle mit der Trunk-Portgruppe, die Sie erstellt haben.
- 9 Geben Sie auf der Seite „Vorlage anpassen“ die folgenden Werte an.
  - a Geben Sie das CLI-Administrator Kennwort ein und wiederholen Sie es.
  - b Geben Sie das CLI-Aktivierungskennwort ein und wiederholen Sie es.
  - c Geben Sie das CLI-Rootkennwort ein und wiederholen Sie es.
  - d Geben Sie die Uplink-IP-Adresse, die Präfixlänge sowie optional das Standardgateway und die DNS-IP-Adresse ein.

- e Wählen Sie den Schlüssel für die Authentifizierung aus. Dieser sollte der auf dem L2VPN-Server verwendeten Verschlüsselung entsprechen.
- f Um die Egress-Optimierung zu aktivieren, geben Sie die Gateway-IP-Adressen ein, für die Datenverkehr lokal weitergeleitet oder für die Datenverkehr über den Tunnel blockiert werden soll.
- g Geben Sie Adresse und Port des L2 VPN-Servers ein.
- h Geben Sie den Benutzernamen und das Kennwort ein, mit dem die Peer-Site authentifiziert werden soll.
- i Geben Sie unter „Teilschnittstellen, VLAN (Tunnel-ID)“ die VLAN-ID(s) des bzw. der Netzwerke ein, das bzw. die Sie ausweiten möchten. Sie können die VLAN-IDs als eine Liste oder einen Bereich (jeweils durch ein Komma getrennt) auflisten. Beispielsweise 2,3,10-20.

Wenn Sie die VLAN-ID des Netzwerks vor dem Ausweiten auf die Site des eigenständigen Edge ändern möchten, können Sie die VLAN-ID des Netzwerks eingeben und anschließend die Tunnel-ID in Klammern. Beispielsweise 2(100),3(200). Mit der Tunnel-ID werden die Netzwerke, die ausgeweitet werden, zugeordnet. Sie können jedoch nicht die Tunnel-ID mit einem Bereich angeben. Folgendes ist nicht zulässig: 10(100)-14(104). Hierfür ist die folgende Schreibweise erforderlich: 10(100),11(101),12(102),13(103),14(104).

- j Wenn das eigenständige NSX Edge nicht direkt auf das Internet zugreifen kann und das Quell-NSX Edge (Server) über einen Proxy-Server erreichen muss, geben Sie die Proxy-Adresse, Port, Benutzernamen und Kennwort ein.
  - k Wenn eine Root-CA verfügbar ist, können Sie diese im Abschnitt „Zertifikat“ einfügen.
  - l Klicken Sie auf **Weiter (Next)**.
- 10** Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die Einstellungen des eigenständigen Edge und klicken Sie auf **Beenden (Finish)**.

### Nächste Schritte

Schalten Sie die virtuelle Maschine des eigenständigen Edge ein.

Notieren Sie die Portnummer der Trunk-vNIC und konfigurieren Sie einen Sink-Port. Weitere Informationen dazu finden Sie unter [Konfigurieren eines Sink-Ports](#).

Nehmen Sie alle weiteren Konfigurationsänderungen in der Befehlszeilenschnittstelle des eigenständigen Edge vor. Weitere Informationen finden Sie unter *Befehlszeilenschnittstellen-Referenz zu NSX*.

## Anzeigen von L2 VPN-Statistiken

Sie können L2-VPN-Tunnel-Statistiken, wie z. B. Tunnelstatus, gesendete und empfangene Byte und andere Statistiken sowohl auf dem L2-VPN-Server als auch auf Client-Edges anzeigen.

## Verfahren

- 1 Anzeigen von Statistiken auf dem L2-VPN-Client-Edge
  - a Doppelklicken Sie auf das NSX Edge, das Sie im L2-VPN-Clientmodus konfiguriert haben.
  - b Navigieren Sie zu **Verwalten > VPN > L2 VPN**.
  - c Erweitern Sie den Abschnitt **Tunnelstatus** und klicken Sie auf das Symbol **Aktualisieren**, um die Tunnelstatistiken anzuzeigen.
- 2 Anzeigen von Statistiken auf dem L2-VPN-Server-Edge
  - a Doppelklicken Sie auf das NSX Edge, das Sie im L2-VPN-Servermodus konfiguriert haben.
  - b Navigieren Sie zur Seite **L2 VPN**.
  - c Klicken Sie im Abschnitt **Site-Konfigurationsdetails** auf den Link **L2VPN-Statistik anzeigen (Show L2VPN Statistics)**.

Die Statistiken aller auf dem L2-VPN-Server konfigurierten Peer-Sites werden angezeigt.

## Nächste Schritte

Um die in einer Trunk-Schnittstelle konfigurierten Netzwerke anzuzeigen, navigieren Sie zu **Verwalten (Manage) > Einstellungen (Settings) > Schnittstellen (Interfaces)** für die Edge-Instanz und klicken Sie in der Typ-Spalte auf **Trunk**.

## Entfernen eines ausgeweiteten VLAN

Ein L2VPN kann auf mehrere logische Netzwerke und geographische Sites ausgeweitet werden.

Um ein ausgeweitetes VLAN von einem L2 VPN Edge zu entfernen, ohne dass dies Auswirkungen auf andere ausgeweitete VLANS hat, entfernen Sie zuerst das VLAN und dann die Teilschnittstelle vom L2-VPN-Client (Quell-NSX Edge) und vom L2-VPN-Server (Ziel-NSX Edge).

## Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > NSX Edges**.
- 2 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 3 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und navigieren Sie zu **VPN > L2VPN**.
- 4 Entfernen Sie in „Site-Konfigurationsdetails“, „Ausgeweitete Schnittstellen“ das der Teilschnittstelle zugeordnete VLAN.
- 5 Legen Sie den **L2 VPN-Modus (L2 VPN Mode)** auf **Client** fest und entfernen Sie die Teilschnittstelle für dieses VLAN.
- 6 Legen Sie den **L2 VPN-Modus (L2 VPN Mode)** auf **Server** fest und entfernen Sie die Teilschnittstelle für dieses VLAN.
- 7 Veröffentlichen Sie die Änderungen.

# Logischer Load Balancer

# 15

Der NSX Edge-Load Balancer ermöglicht einen High-Availability-Dienst und verteilt die Arbeitslast des Netzwerkdatenverkehrs auf mehrere Server. Er verteilt eingehende Dienstanforderungen über mehrere Server gleichmäßig auf eine Weise, dass die Lastverteilung für die Benutzer transparent ist. Das Load Balancing hilft deshalb dabei, optimale Ressourcennutzung, maximalen Durchsatz und minimale Reaktionszeit zu erreichen sowie Überlastung zu vermeiden. NSX Edge bietet ein Load Balancing bis Schicht 7.

Für den Load Balancer ordnen Sie eine externe oder öffentliche IP-Adresse einer Gruppe interner Server zu. Der Load Balancer akzeptiert TCP-, UDP-, HTTP- oder HTTPS-Anforderungen über die externe IP-Adresse und entscheidet, welcher interne Server verwendet werden soll. Port 80 ist der Standardport für HTTP und Port 443 der Standardport für HTTPS.

Sie müssen über eine gültige NSX Edge-Instanz verfügen, bevor Sie das Load Balancing konfigurieren können. Weitere Informationen zur Einrichtung von NSX Edge finden Sie unter [Konfiguration von NSX Edge](#).

Weitere Informationen zur Konfiguration eines NSX Edge-Zertifikats finden Sie unter [Arbeiten mit Zertifikaten](#).

Das NSX-Load-Balancing beinhaltet folgende Funktionen:

- Protokolle: TCP, UDP, HTTP, HTTPS
- Algorithmen: Weighted Round Robin (WRR), IP Hash, URI, Letzte Verbindung
- SSL-Beendigung mit AES-NI-Beschleunigung
- SSL-Bridging (Client-seitiges SSL + Server-seitiges SSL)
- Verwaltung von SSL-Zertifikaten
- X-Header-Weiterleitung zur Client-Identifizierung
- Transparenter L4/L7-Modus
- Verbindungsdrösselung
- Aktivieren/deaktivieren einzelner Server (Poolmitglieder) für die Wartung
- Methoden zur Systemstatusprüfung (TCP, UDP, HTTP, HTTPS)
- Erweiterte Überwachung des Systemstatus

- Persistenz-/Stickiness-Methoden: SourceIP, MSRP, COOKIE, SSLSESSIONID
- „One-Arm“-Modus (einarmiger Modus)
- Inline-Modus
- Erneutes Schreiben und umleiten der URL
- Anwendungsregeln für die erweiterte Datenverkehrsverwaltung
- Stickiness-Unterstützung für HA-Sitzungen für ein L7-Proxy-Load-Balancing
- IPv6-Unterstützung
- Erweiterte Load-Balancer-Befehlszeilenschnittstelle (CLI) zur Fehlerbehebung
- Verfügbar für alle Varianten eines NSX Edge-Dienstgateways, wobei für den Datenverkehr bei der Produktion die Option „X-Large“ oder „Quad Large“ empfohlen wird

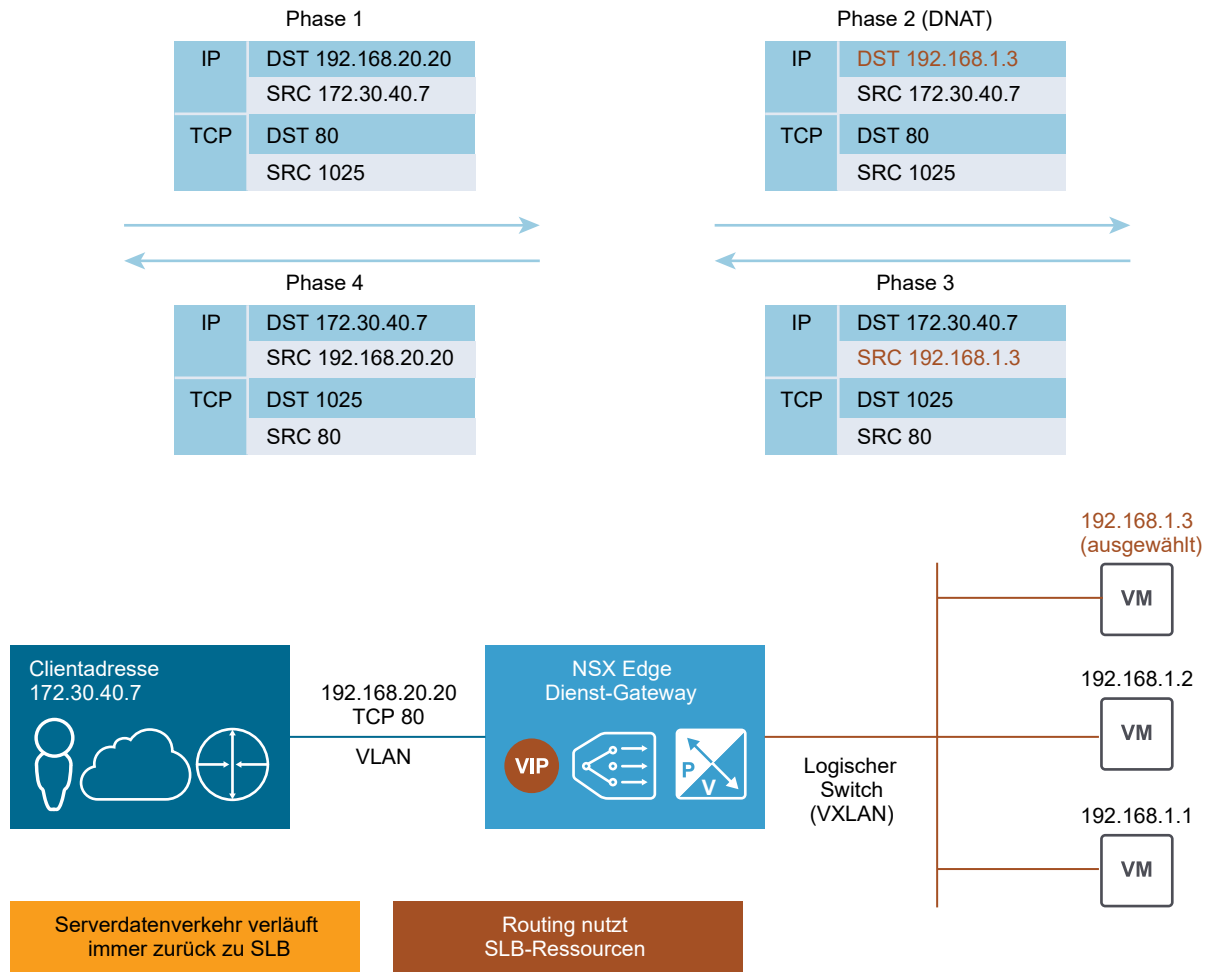
## Topologien

Es stehen zwei Typen von Load-Balancing-Diensten zur Konfiguration in NSX zur Verfügung: ein „Einarmiger“-Modus, auch „Proxy-Modus“ genannt, und der Inline-Modus, auch als „Transparenter Modus“ bezeichnet.

## Logisches NSX Load Balancing: Inline-Topologie

Im Inline-Modus oder transparenten Modus wird das NSX Edge inline für den Datenverkehr bereitgestellt, der für die Serverfarm bestimmt ist. Der Datenverkehrsfluss im transparenten Modus wird wie folgt verarbeitet:

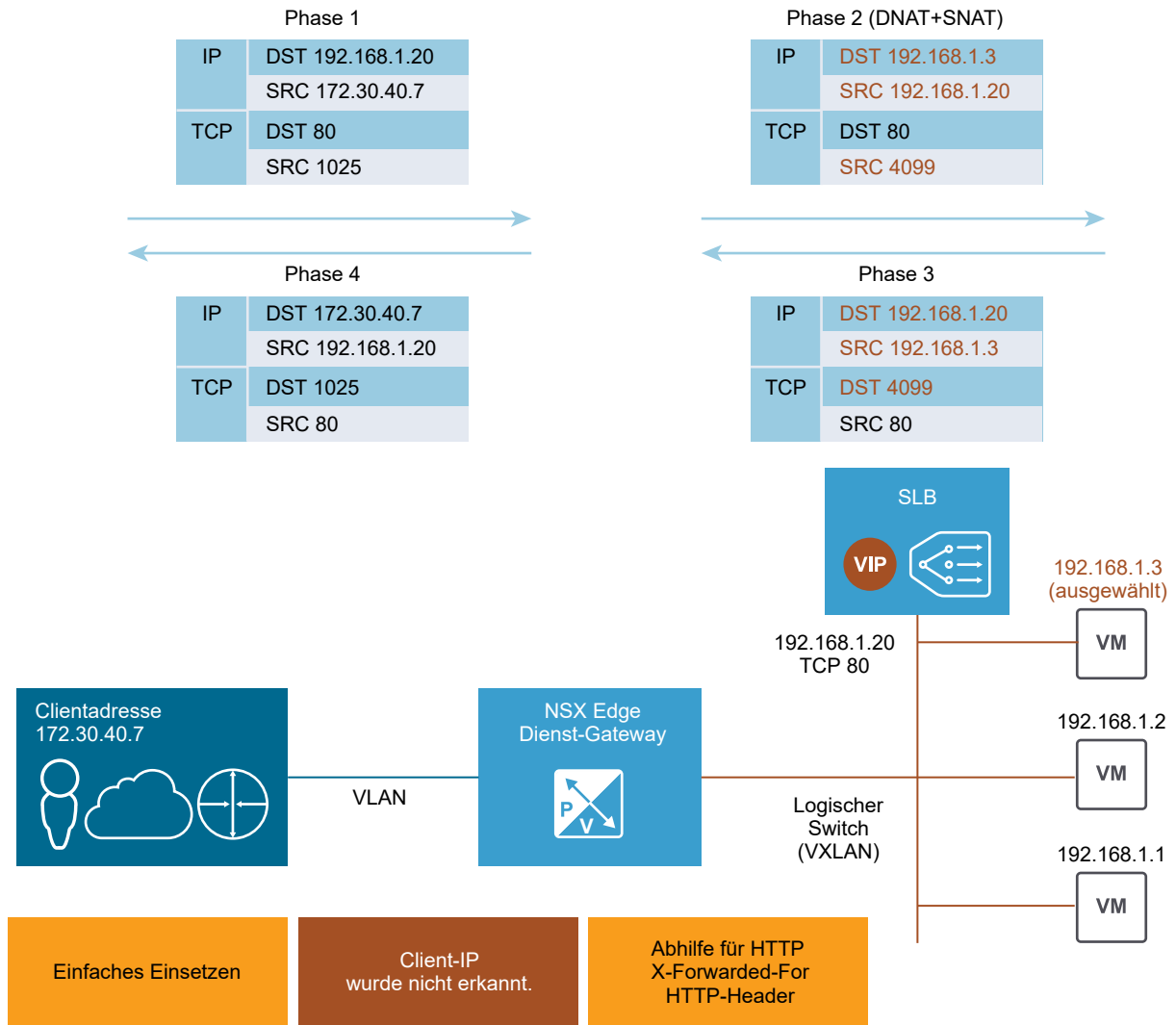
- Der externe Client sendet den Datenverkehr an die virtuelle IP-Adresse (VIP), die vom Load Balancer angegeben wurde.
- Der Load Balancer – ein zentralisiertes NSX Edge – führt nur einen Ziel-NAT-Vorgang (DNAT) durch, um die VIP durch die IP-Adresse eines der in der Serverfarm bereitgestellten Servers zu ersetzen.
- Der Server in der Serverfarm antwortet auf die ursprüngliche Client-IP-Adresse. Der Datenverkehr wird wieder vom Load Balancer empfangen, der er inline bereitgestellt wurde. Dies erfolgt normalerweise in Form des Standard-Gateways für die Serverfarm.
- Der Load Balancer führt einen Quell-NAT-Vorgang aus, um den Datenverkehr an den externen Client zu senden. Dabei nutzt er seine VIP als IP-Quelladresse.



## Logisches NSX Load Balancing: Einarmige Topologie

Der einarmige bzw. Proxy-Modus umfasst die Bereitstellung eines NSX Edges, das direkt mit dem logischen Netzwerk verbunden ist, in dem die Load Balancere benötigt werden.

- Der externe Client sendet den Datenverkehr an die virtuelle IP-Adresse (VIP), die vom Load Balancer angegeben wurde.
- Der Load Balancer führt zwei Adressübersetzungen für die vom Client empfangenen Originalpakete durch: Ziel-NAT (DNAT) zum Ersetzen der VIP durch die IP-Adresse eines Servers, der in der Serverfarm bereitgestellt wurde und Quell-NAT (SNAT) zum Ersetzen der Client-IP-Adresse durch die IP-Adresse, anhand derer der Load Balancer selbst identifiziert wird. SNAT ist erforderlich, um den rückwärtigen Datenverkehr von der Serverfarm an den Client zwangsweise durch den Load Balancer zu leiten.
- Der Server in der Serverfarm antwortet, indem er den Datenverkehr per SNAT-Funktionalität an den Load Balancer sendet.
- Der Load Balancer führt wiederum einen Quell- und Ziel-NAT-Dienst aus, um den Datenverkehr an den externen Client zu senden. Dabei nutzt er seine VIP als IP-Quelladresse.



Dieses Kapitel enthält die folgenden Themen:

- [Einrichten des Load Balancing](#)
- [Verwalten von Anwendungsprofilen](#)

- [Verwalten von Dienstmonitoren](#)
- [Verwalten von Serverpools](#)
- [Verwalten von virtuellen Servern](#)
- [Verwalten von Anwendungsregeln](#)
- [Load-Balancer-Webserver mit NTLM-Authentifizierung](#)
- [HTTP-Verbindungsmodi des Load Balancer](#)
- [Szenarien für die NSX-Load-Balancer-Konfiguration](#)

## Einrichten des Load Balancing

Der NSX Edge-Load Balancer verteilt den Netzwerkdatenverkehr auf mehrere Server, um eine optimale Nutzung der Ressourcen zu erreichen, Redundanz zu bieten und damit die Ressourcennutzung zu verteilen.

Der NSX-Load Balancer unterstützt die Schicht 4- und Schicht 7-Load-Balancer-Engines. Der Load Balancer der Schicht 4 ist paketbasiert und ermöglicht eine schnelle Pfadverarbeitung, während der Load Balancer der Schicht 7 socketbasiert ist und erweiterte Datenverkehrsmanipulationen sowie DDOS-Abschwächungen für Backend-Dienste ermöglicht.

Eine paketbasierte Lastverteilung ist in der TCP- und UDP-Schicht implementiert. Die paketbasierte Lastverteilung beendet die Verbindung nicht und puffert auch nicht die gesamte Anforderung, sondern verarbeitet das Paket und sendet es direkt zum ausgewählten Server. TCP- und UDP-Sitzungen verbleiben im Load Balancer, sodass Pakete für eine einzelne Sitzung zum selben Server gesendet werden. Sie können durch Auswahl von „Beschleunigung aktivieren“ sowohl in der globalen Konfiguration wie in der Konfiguration des betreffenden virtuellen Servers das Paket-basierte Load Balancing aktivieren.

Eine socketbasierte Lastverteilung wird auf der Grundlage der Socketschnittstelle implementiert. Es werden zwei Verbindungen für eine einzelne Anforderung eingerichtet: eine Verbindung mit Client-Kontakt und eine Verbindung mit Server-Kontakt. Die Verbindung mit Server-Kontakt wird nach der Serverauswahl eingerichtet. Bei einer Socket-basierten HTTP-Implementierung wird die gesamte Anforderung vor dem Senden an den ausgewählten Server mit optionaler L7-Verarbeitung empfangen. Bei einer socketbasierten HTTPS-Implementierung werden die Authentifizierungsinformationen über die Verbindung mit Clientkontakt oder über die Verbindung mit Serverkontakt ausgetauscht. Das Socket-basierte Load Balancing ist der Standardmodus für virtuelle Server mit TCP-, HTTP- oder HTTPS-Protokoll.

Wichtige Konzepte des NSX-Load Balancer sind unter anderem:

### Virtueller Server

Zusammenfassender Begriff für einen Anwendungsdienst, der aus einer eindeutigen Kombination aus IP, Port, Protokoll und Anwendungsprofil wie TCP oder UDP besteht.

### Serverpool

Gruppe von Backend-Servern.

### **Serverpoolmitglied**

Stellt den Backend-Server als Mitglied in einem Pool dar.

### **Dienstmonitor**

Definiert die Art und Weise, mit der der Systemzustand eines Backend-Servers überprüft wird.

### **Anwendungsprofil**

Spiegelt die TCP-, UDP-, Persistenz- und Zertifikatkonfiguration für eine bestimmte Anwendung wider.

Sie beginnen mit der Einstellung globaler Optionen für den Load Balancer, erstellen dann einen Serverpool aus Backend-Servermitgliedern und verknüpfen einen Dienstmonitor mit dem Pool zur effizienten Verwaltung und Freigabe der Backend-Server.

Sie können dann ein Anwendungsprofil zur Definition des allgemeinen Anwendungsverhaltens in einem Load Balancer, z. B. in Bezug auf Client-SSL, Server-SSL, „x-forwarded-for“ oder Persistenz, definieren. Durch die Persistenz werden wiederholte Anforderungen mit demselben Merkmal (Quell-IP oder Cookie) gesendet. Diese sind Voraussetzung für das Versenden an dasselbe Poolmitglied, ohne dass der Lastverteilungsalgorithmus ausgeführt wird. Anwendungsprofile können für alle virtuellen Server wiederverwendet werden.

Sie haben dann die Möglichkeit, eine Anwendungsregel zur Konfiguration anwendungsspezifischer Einstellungen für die Verarbeitung des Datenverkehrs zu erstellen, z. B. die notwendige Übereinstimmung mit einer bestimmten URL oder mit einem bestimmten Hostnamen, damit unterschiedliche Anforderungen von unterschiedlichen Pools verarbeitet werden. Im nächsten Schritt können Sie einen Dienstmonitor erstellen, der speziell auf Ihre Anwendung ausgelegt ist, oder einen zuvor erstellten Dienstmonitor verwenden.

Optional können Sie eine Anwendungsregel erstellen, um die erweiterte Funktionalität von virtuellen L7-Servern zu unterstützen. Einige Anwendungsfälle für Anwendungsregeln beinhalten das Wechseln von Inhalten, Kopfzeilenmanipulation, Sicherheitsregeln und DOS-Schutz.

Schlussendlich können Sie einen virtuellen Server erstellen, der Ihren Serverpool, Ihr Anwendungsprofil und potenzielle Anwendungsregeln miteinander verbindet.

Wenn der virtuelle Server eine Anforderung erhält, berücksichtigt der Load-Balancing-Algorithmus die Poolmitgliedskonfiguration und den Laufzeitstatus. Der Algorithmus berechnet dann den entsprechenden Pool für die Verteilung des Datenverkehrs für ein oder mehr 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, Weighted Round-Robin, schwächste Verbindung, Quell-IP-Hash, gewichtete schwächste Verbindungen, URL, URI oder HTTP-Kopfzeile sein.

Jeder Pool wird vom zugehörigen Dienstmonitor überwacht. Wenn der Load Balancer ein Problem bei einem Poolmitglied erkennt, wird das Mitglied als ausgefallen (DOWN) markiert. Es wird nur ein UP-Server bei der Auswahl eines Poolmitglieds aus dem Serverpool ausgewählt. Wenn der Serverpool nicht mit einem Dienstmonitor konfiguriert wurde, werden alle Poolmitglieder als UP behandelt.

---

**Hinweis** Informationen zur Fehlerbehebung für Load Balancer erhalten Sie unter *Fehlerbehebungshandbuch zu NSX*.

---

- [Konfigurieren des Load-Balancer-Dienstes](#)

- [Erstellen eines Dienstmonitors](#)

Sie erstellen einen Dienstmonitor, um Parameter zur Integritätsprüfung für einen bestimmten Typ des Netzwerkdatenverkehrs zu definieren. Wenn Sie einem Pool einen Dienstmonitor zuweisen, werden die Mitglieder des Pools gemäß den Dienstmonitorparametern überwacht.

- [Hinzufügen eines Serverpools](#)

Sie können einen Serverpool hinzufügen, um Backend-Server flexibel und effizient zu verwalten und freizugeben. Ein Serverpool verwaltet Load-Balancer-Verteilungsmethoden und ist mit einem Dienstmonitor für Systemstatusprüfungsparameter verbunden.

- [Erstellen eines Anwendungsprofils](#)

Verwenden Sie Anwendungsprofile, um Ihre Kontrolle über die Verwaltung von Netzwerkverkehr zu verbessern, und gestalten Sie Aufgaben zur Verwaltung des Datenverkehrs einfacher und effizienter.

- [Hinzufügen einer Anwendungsregel](#)

Sie können Anwendungsregeln schreiben, indem Sie die HAProxy-Syntax verwenden, um den Anwendungsdatenverkehr zu bearbeiten und zu verwalten.

- [Hinzufügen von virtuellen Servern](#)

Fügen Sie eine interne Schnittstelle oder eine Uplink-Schnittstelle von NSX Edge als virtuellen Server hinzu.

## Konfigurieren des Load-Balancer-Dienstes

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie auf **Bearbeiten (Edit)**.

- 6 Aktivieren Sie die Kontrollkästchen neben den Optionen, die aktiviert werden sollen. Es können globale Konfigurationsparameter für den Load Balancer festgelegt werden.

Option	Beschreibung
<b>Load Balancer aktivieren</b>	Lässt zu, dass der NSX Edge-Load-Balancer Datenverkehr an interne Server für das Load Balancing verteilt.
<b>Beschleunigung aktivieren</b>	<p>Ist diese Option deaktiviert, verwenden alle virtuelle IP-Adressen (VIPs) die L7-LB-Engine.</p> <p>Ist diese Option aktiviert, verwendet die virtuelle IP-Adresse die schnellere L4-LB-Engine oder L7-LB-Engine (basierend auf der VIP-Konfiguration).</p> <p>Die L4-VIP-Adresse („Beschleunigung aktiviert“ ist in der VIP-Konfiguration ausgewählt und es ist keine L7-Einstellung wie z. B. AppProfile mit Cookie-Persistenz oder SSL-Offload vorhanden) wird vor der Edge-Firewall verarbeitet, und für das Erreichen der VIP-Adresse ist keine Edge-Firewallregel erforderlich. Wenn die VIP-Adresse allerdings einen Pools im nicht-transparenten Modus verwendet, muss die Edge-Firewall aktiviert sein (um die automatisch erstellte SNAT-Regel zuzulassen).</p> <p>Die L7-HTTP/HTTPS-VIP-Adressen („Beschleunigung deaktiviert“ ist in der VIP-Konfiguration ausgewählt oder es ist eine L7-Einstellung wie z. B. AppProfile mit Cookie-Persistenz oder SSL-Offload vorhanden) werden nach der Edge-Firewall verarbeitet und erfordern eine Edge-Firewallregel für das Zulassen, um die VIP-Adresse zu erreichen.</p> <p>Hinweis: Um zu überprüfen, welche LB-Engine für die einzelnen VIP-Adressen durch den NSX-Load-Balancer verwendet wird, führen Sie in der NSX Edge-CLI (ssh oder Konsole) den Befehl „show service loadbalancer virtual“ aus und suchen Sie nach dem Feld „LB PROTOCOL [L4 L7]“.</p>
<b>Protokollierung</b>	<p>Der NSX Edge-Load-Balancer erfasst Datenverkehrsprotokolle.</p> <p>Sie können die Protokollierungsebene aus dem Dropdown-Menü auswählen. Die Protokolle werden zum konfigurierten Syslog-Server exportiert. Sie können die Load-Balancing-Protokolle auch mit dem Befehl <code>show log follow</code> auflisten.</p> <p>Die Optionen „Debuggen“ und „Info“ protokollieren Endbenutzeranforderungen. Die Optionen „Warnung“, „Fehler“ und „Kritisch“ protokollieren keine Endbenutzeranforderungen. Wenn für das NSX Edge-Protokoll auf Steuerungsebene „Debug“ oder „Info“ festgelegt ist, protokolliert der Load Balancer LB-, VIP-, Pool- und Poolmitgliedsstatistiken pro Minute.</p> <p>Beachten Sie, dass mit der Ausführung im Modus „Debug“ oder „Info“ eine hohe Auslastung der CPU und des Partitionsspeicherplatzes für das Edge-Protokoll verbunden ist. Dies reduziert möglicherweise in einem gewissen Umfang die Möglichkeiten, einen maximalen Datenverkehr sicherzustellen.</p>
<b>Service Insertion aktivieren</b>	<p>Lässt zu, dass der Load Balancer mit Drittanbieterdiensten funktioniert.</p> <p>Wenn in Ihrer Umgebung ein Load Balancer eines Drittanbieters bereitgestellt wird, informieren Sie sich unter <a href="#">Nutzung eines Partner-Load-Balancer</a>.</p>

- 7 Klicken Sie auf **OK**.

## Erstellen eines Dienstmonitors

Sie erstellen einen Dienstmonitor, um Parameter zur Integritätsprüfung für einen bestimmten Typ des Netzwerkdatenverkehrs zu definieren. Wenn Sie einem Pool einen Dienstmonitor zuweisen, werden die Mitglieder des Pools gemäß den Dienstmonitorparametern überwacht.

Es werden fünf Überwachungstypen unterstützt: ICMP, TCP, UDP, HTTP und HTTPS.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Dienstüberwachung (Service Monitoring)**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 7 Geben Sie in **Name** einen Namen für den Dienstmonitor ein.  
  
Intervall, Zeitüberschreitung und Max. Wiederholungen sind gängige Parameter für alle Typen von Systemstatusprüfungen.
- 8 Geben Sie in **Intervall (Interval)** die Anzahl der Sekunden für das Intervall ein, in dem ein Server getestet werden soll.  
  
Das Intervall ist die Zeitspanne in Sekunden, in der der Monitor Anforderungen an den Backend-Server sendet.
- 9 Geben Sie unter **Zeitüberschreitung (Timeout)** den Zeitraum für den Empfang einer Antwort ein. Für jede Überprüfung des Systemzustands legt der Wert für die Zeitüberschreitung die maximale Zeit in Sekunden fest, in der eine Antwort vom Server empfangen werden muss.
- 10 Geben Sie unter **Max. Wiederholungen (Max Retries)** die Häufigkeit des Servertests ein. Dieser Wert legt fest, wie oft ein Server getestet wird, bevor er als INAKTIV behandelt wird.  
  
Wenn Sie z. B. **Intervall (Interval)** auf 5 Sekunden, **Zeitüberschreitung (Timeout)** auf 15 Sekunden und für **Max. Wiederholungen (Max Retries)** den Wert 3 festgelegt haben, überprüft der NSX-Load-Balancer alle 5 Sekunden den Backend-Server. Wenn bei einer Überprüfung die vorgesehene Antwort innerhalb von 15 Sekunden vom Server empfangen wird, ist das Ergebnis der Systemstatusprüfung „OK“. Ist dies nicht der Fall, ist das Ergebnis „CRITICAL“. Wenn die letzten drei Systemstatusprüfungen alle „DOWN“ ergeben haben, wird der Server als „DOWN“ gekennzeichnet.
- 11 Wählen Sie im Dropdown-Menü aus, in welcher Weise die Anforderung zur Überprüfung des Systemstatus an den Server gesendet werden soll. Es werden fünf Überwachungstypen unterstützt: ICMP, TCP, UDP, HTTP und HTTPS. Im System sind drei vordefinierte Überwachungen integriert: default\_tcp\_monitor, default\_http\_monitor und default\_https\_monitor.
- 12 Wenn Sie **ICMP** als Überwachungstyp auswählen, werden keine anderen Parameter angewendet. Lassen Sie das Feld für die anderen Parameter leer.

**13** Wenn Sie als Monitortyp **TCP** auswählen, sind drei weitere Parameter verfügbar: Senden, Empfangen und Erweiterung.

- a Senden (optional) – Der String, der an den Back-End-Server gesendet wird, nachdem eine Verbindung hergestellt wurde.
- b Empfangen (optional) – Geben Sie den String ein, der übereinstimmen muss. Dieser String kann sich in der Kopfzeile oder im Text der Antwort befinden. Der Server wird nur dann als AKTIV eingestuft, wenn der empfangene String mit dieser Definition übereinstimmt.
- c Erweiterung – Geben Sie erweiterte Monitorparameter als „Schlüssel=Wert“-Paare im Abschnitt „Erweiterung“ ein.

Zum Beispiel gibt die Erweiterung „Warnung=10“ an, dass der Status eines Servers auf „Warnung“ gesetzt wird, wenn dieser nicht innerhalb von 10 Sekunden antwortet.

Alle Erweiterungselemente sollten mit einem Wagenrücklaufzeichen getrennt werden.

**Tabelle 15-1. Erweiterungen für TCP-Protokoll**

Überwachungserweiterung	Beschreibung
escape	Kann \n, \r, \t oder \ in der send- oder quit-Zeichenfolge verwenden. Muss sich vor der send- oder quit-Option befinden. Standard: nichts hinzugefügt zu send, \r\n hinzugefügt zum Ende von quit.
all	Alle erwarteten Zeichenfolgen müssen in Serverantwort auftreten. Der Standardwert ist „beliebig“.
quit=STRING	Zeichenfolge, die an den Server gesendet wird, um ein ordnungsgemäßes Beenden der Verbindung zu initiieren.
refuse=ok warn crit	Akzeptieren von TCP-Zurückweisungen mit Status „ok“, „warn“ oder „crit“. Standardwert ist „crit“.
mismatch=ok warn crit	Akzeptieren von erwarteten Zeichenfolgenkonflikten mit Status „ok“, „warn“ oder „crit“. Standardwert ist „warn“.
jail	Ausgabe von TCP-Socket ausblenden.
maxbytes=INTEGER	Verbindung schließen, wenn mehr als die angegebene Anzahl an Byte empfangen wurde.
delay=INTEGER	Sekunden beim Warten zwischen dem Senden der Zeichenfolge und dem Abrufen der Antwort.
certificate=INTEGER[,INTEGER]	Mindestanzahl der Tage, die ein Zertifikat gültig sein muss. Der erste Wert ist die Anzahl der Tage bis zur Warnung und der zweite Wert ist „Kritisch“ (wenn nicht angegeben – 0).
warning=DOUBLE	Antwortzeit in Sekunden, nach der ein Warnstatus gemeldet wird.
critical=DOUBLE	Antwortzeit in Sekunden, nach der ein kritischer Status gemeldet wird.

**14** Wenn Sie als Monitortyp **HTTP** oder **HTTPS** auswählen, führen Sie die im Folgenden aufgeführten Schritte aus.

- a Erwartet – Geben Sie den String ein, mit dem der Monitor in der Statuszeile der HTTP-Antwort im Abschnitt „Erwartet“ übereinstimmen muss. Es handelt sich hier um eine kommagetrennte Liste.  
Beispiel: 200,301,302,401.
- b Methode (optional) – Wählen Sie aus dem Dropdown-Menü die Methode zur Ermittlung des Serverstatus aus: GET, OPTIONS oder POST.
- c URL (optional) – Legen Sie für die URL GET oder POST fest (Standard: „/“).
- d Geben Sie bei Auswahl der POST-Methode im Abschnitt **Fett (Bold)** die Daten ein, die gesendet werden sollen.

- e Geben Sie im Abschnitt „Erwartet“ den String ein, der im Antwortinhalt im Abschnitt **Empfangen (Receive)** übereinstimmen muss. Dieser String kann sich in der Kopfzeile oder im Text der Antwort befinden.

Besteht keine Übereinstimmung mit dem String im Abschnitt „Erwartet“, prüft der Monitor nicht die Übereinstimmung des Inhalts von „Empfangen“.

- f Erweiterung – Geben Sie erweiterte Monitorparameter als „Schlüssel=Wert“-Paare im Abschnitt „Erweiterung“ ein.

Zum Beispiel gibt die Erweiterung „Warnung=10“ an, dass der Status eines Servers auf „Warnung“ gesetzt wird, wenn dieser nicht innerhalb von 10 Sekunden antwortet.

Alle Erweiterungselemente sollten mit einem Wagenrücklaufzeichen getrennt werden.

**Tabelle 15-2. Erweiterungen für HTTP/HTTPS-Protokoll**

Überwachungserweiterung	Beschreibung
no-body	Nicht auf Dokumenthauptteil warten: Lesen nach Kopfzeilen beenden. Beachten Sie, dass dies immer noch einen HTTP GET oder POST, nicht einen HEAD erstellt.
ssl-version=3	Erzwingt den SSL-Handshake mithilfe von sslv3. sslv3 und tlsv1 sind standardmäßig in der Option für die Systemstatusprüfung deaktiviert.
ssl-version=10	Erzwingt den SSL-Handshake mithilfe von tls 1.0.
ssl-version=11	Erzwingt den SSL-Handshake mithilfe von tls 1.1.
ssl-version=12	Erzwingt den SSL-Handshake mithilfe von tls 1.2.
max-age=SECONDS	Warnen, wenn das Dokument mehr als SEKUNDEN alt ist. Die Zahl kann auch in der Form 10m für Minuten, 10h für Stunden oder 10d für Tage angegeben werden.
content-type=STRING	Gibt den Medientyp „Content-Type-Kopfzeile“ in POST-Aufrufen an.
linespan	regex darf Zeilenvorschübe umfassen (-r oder -R muss vorausgehen).
regex=STRING oder ereg=STRING	Seite nach regex-ZEICHENFOLGE durchsuchen.
eregi=STRING	Seite nach regex-ZEICHENFOLGE (Groß-/Kleinschreibung nicht beachten) durchsuchen.
invert-regex	KRITISCH zurückgeben, wenn gefunden, andernfalls OK.
proxy-authorization=AUTH_PAIR	Benutzername:Kennwort auf Proxyservern mit Standardauthentifizierung.
useragent=STRING	Zu sendende Zeichenfolge in HTTP-Kopfzeile als User Agent.
header=STRING	Alle anderen in HTTP-Kopfzeile zu sendenden Tags. Für zusätzliche Kopfzeilen mehrmals verwenden.

**Tabelle 15-2. Erweiterungen für HTTP/HTTPS-Protokoll (Fortsetzung)**

Überwachungserweiterung	Beschreibung
onredirect=ok warning critical follow sticky stickyport	Informationen zur Verarbeitung von weitergeleiteten Seiten. sticky ist wie „follow“, aber an der angegebenen IP-Adresse festhalten. stickyport stellt auch sicher, dass sich der Port nicht ändert.
pagesize=INTEGER:INTEGER	Erforderliche Mindestseitengröße (Byte) : Erforderliche maximale Seitengröße (Byte).
warning=DOUBLE	Antwortzeit in Sekunden, nach der ein Warnstatus gemeldet wird.
critical=DOUBLE	Antwortzeit in Sekunden, nach der ein kritischer Status gemeldet wird.
expect = STRING	Liste mit durch Kommas getrennten Strings, von denen mindestens einer in der ersten Zeile (Statuszeile) der Serverantwort enthalten sein muss (Standard: HTTP/1). Bei Angabe dieses Werts werden alle anderen Statuszeilenstrukturen (z. B. 3xx-, 4xx-, 5xx-Verarbeitung) übersprungen.
string = STRING	Zeichenfolge, die im Inhalt erwartet wird.
url = PATH	URL mit GET oder POST (Standard: /).
post = STRING	URL zur Codierung der HTTP-POST-Daten.
method = STRING	Legt die HTTP-Methode fest (z. B. HEAD, OPTIONS, TRACE, PUT, DELETE).
timeout = INTEGER	Anzahl der Sekunden, nach denen die Zeit für eine Verbindung überschritten ist (Standard: 10 Sekunden).
header=Host:host_name -H host_name --sni	<p>host_name ist ein gültiger Hostname oder ein FQDN des Hosts.</p> <p>Erstellen Sie für jeden virtuellen Host einen separaten Dienstmonitor und fügen Sie in jedem Dienstmonitor eine SNI-Erweiterung (Servernamensanzeige) hinzu.</p>

**Tabelle 15-3. Erweiterungen für HTTPS-Protokoll**

Überwachungserweiterung	Beschreibung
certificate=INTEGER	Mindestanzahl der Tage, die ein Zertifikat gültig sein muss. Port standardmäßig 443. Bei Verwendung dieser Option wird die URL nicht überprüft.
authorization=AUTH_PAIR	Benutzername:Kennwort auf Sites mit Standardauthentifizierung.
ciphers='ECDHE-RSA-AES256-GCM-SHA384'	Stellt die bei der HTTPS-Systemstatusprüfung verwendeten Verschlüsselungen dar.

**15** Wenn Sie **UDP** als Überwachungstyp auswählen, führen Sie die folgenden Schritte aus:

- a Senden (erforderlich): Geben Sie den String ein, der an den Backend-Server nach dem Verbindungsaufbau gesendet werden soll.
- b Empfangen (erforderlich): Geben Sie den String ein, der vom Backend-Server empfangen werden soll. Der Server wird nur dann als **AKTIV** eingestuft, wenn der empfangene String mit dieser Definition übereinstimmt.

---

**Hinweis** Für die UDP-Überwachung wird keine Erweiterung unterstützt.

---

**16** Klicken Sie auf **OK**.

### Nächste Schritte

Weisen Sie einem Pool einen Dienstmonitor zu.

## Hinzufügen eines Serverpools

Sie können einen Serverpool hinzufügen, um Backend-Server flexibel und effizient zu verwalten und freizugeben. Ein Serverpool verwaltet Load-Balancer-Verteilungsmethoden und ist mit einem Dienstmonitor für Systemstatusprüfungsparameter verbunden.

### Verfahren


- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Pools**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 7 Geben Sie einen Namen und eine Beschreibung für den Load-Balancer-Pool ein.
- 8 Wählen Sie für jeden aktivierten Dienst die algorithmische Ausgleichsmethode aus.

Option	Beschreibung
<b>IP-HASH</b>	Wählt einen Server auf der Basis eines Hash der Quell-IP-Adresse und der gesamten Gewichtung aller ausgeführten Server aus. Algorithmusparameter sind für diese Option deaktiviert.
<b>LEASTCONN</b>	Verteilt basierend auf der Anzahl der bereits auf den Servern aktiven Verbindungen die Client-Anforderungen an mehrere Server. Neue Verbindungen werden an den Server mit den wenigsten Verbindungen gesendet. Algorithmusparameter sind für diese Option deaktiviert.

Option	Beschreibung
<b>ROUND_ROBIN</b>	<p>Dabei wird die jedem Server zugeordnete Gewichtung berücksichtigt.</p> <p>Dies ist der geeignetste Algorithmus bei gleichmäßig verteilter Prozessorzeit auf dem Server.</p> <p>Algorithmusparameter sind für diese Option deaktiviert.</p>
<b>URI</b>	<p>Der linke Teil des URI (vor dem Fragezeichen) wird zerlegt und durch die Gesamtgewichtung der laufenden Server geteilt.</p> <p>Aus dem Ergebnis wird ersichtlich, welcher Server die Anforderung erhält. Dies gewährleistet, dass ein URI immer auf denselben Server gerichtet ist, solange kein Server heruntergefahren oder gestartet wird.</p> <p>Der URI-Algorithmusparameter verfügt über zwei Optionen: <code>uriLength=&lt;len&gt;</code> und <code>uriDepth=&lt;dep&gt;</code>. Der Bereich für den Längenparameter lautet <code>1&lt;=len&lt;256</code>. Der Bereich für den Tiefenparameter lautet <code>1&lt;=dep&lt;10</code>.</p> <p>Den Parametern für Länge und Tiefe folgt eine positive Ganzzahl. Mit diesen Optionen können Server nur auf der Basis des Anfangs des URI ausgeglichen werden. Der Längenparameter gibt an, dass der Algorithmus nur die definierten Zeichen am Anfang des URI zur Berechnung des Hash verwenden soll.</p> <p>Der Tiefenparameter legt die maximale Verzeichnistiefe zur Berechnung des Hash fest. Jeder Schrägstrich in der Anforderung wird als ein Level behandelt. Wenn beide Parameter angegeben wurden, wird die Evaluierung beendet, wenn der Wert eines der beiden erreicht ist.</p>
<b>HTTPHEADER</b>	<p>Der Name des HTTP-Header, der in jeder HTTP-Anforderung gesucht wird.</p> <p>Für den Header-Namen in Klammern wird wie bei der Funktion ACL 'hdr()' zwischen Groß- und Kleinschreibung nicht unterschieden. Wenn der Header nicht vorhanden ist oder keinen Wert enthält, wird der Round-Robin-Algorithmus angewendet.</p> <p>Der HTTPHEADER-Algorithmusparameter verfügt über eine Option: <code>headerName=&lt;name&gt;</code>. Beispielsweise können Sie als HTTPHEADER-Algorithmusparameter <b>host</b> verwenden.</p>
<b>URL</b>	<p>Der im Argument angegebene URL-Parameter wird im Abfrage-String jeder HTTP GET-Anforderung gesucht.</p> <p>Stehen nach dem Parameter ein Gleichheitszeichen (=) und ein Wert, erhält der Wert einen Hash und wird durch die gesamte Gewichtung der ausgeführten Server geteilt. Aus dem Ergebnis wird ersichtlich, welcher Server die Anforderung erhält. Mit diesen Vorgang werden Benutzerbezeichner in Anforderungen ermittelt und es wird damit sichergestellt, dass eine bestimmte Benutzer-ID immer zum selben Server gesendet wird, solange kein Server aktiviert oder deaktiviert wird.</p> <p>Wenn kein Wert oder kein Parameter gefunden wurde, wird ein Round-Robin-Algorithmus angewendet.</p> <p>Der URL-Algorithmusparameter verfügt über eine Option: <code>urlParam=&lt;url&gt;</code>.</p>

- 9 (Optional) Wählen Sie eine vorhandene Standard- oder eine benutzerdefinierte Überwachung aus dem Dropdown-Menü **Überwachen (Monitors)** aus.

## 10 Fügen Sie dem Pool Mitglieder hinzu.

- a Klicken Sie auf das Symbol **Hinzufügen (Add)** (.
- b Geben Sie den Namen und die IP-Adresse des Servermitglieds ein oder klicken Sie auf **Auswählen (Select)**, um gruppierte Objekte zuzuweisen.

---

**Hinweis** VMware Tools muss auf jeder virtuellen Maschine installiert sein oder es muss eine aktivierte IP-Erkennungsmethode (DHCP-Snooping und/oder ARP-Snooping) eingerichtet sein, wenn gruppierte Objekte anstelle von IP-Adressen verwendet werden. Weitere Informationen finden Sie unter [IP-Erkennung für virtuelle Maschinen](#).

---

Bei den gruppierten Objekten kann es sich entweder um vCenter oder NSX handeln.

- c Wählen Sie für den Mitgliedsstatus **Aktivieren (Enable)**, **Deaktivieren (Disable)** oder **Ausgleichen (Drain)** aus.
  - **Ausgleichen (Drain)** – Erzwingt ein ordnungsgemäßes Herunterfahren des Servers für die Wartung. Durch Festlegen von „Ausgleichen“ für das Poolmitglied wird der Back-End-Server aus dem Load Balancer entfernt, während er für das Beenden von vorhandenen Verbindungen und für neue Verbindungen von Clients mit einer Persistenz für diesen Server verwendet werden kann. Als Persistenzmethoden können im Status „Ausgleichen“ Persistenz der Quell-IP-Adresse, Einfügen von Cookies und Cookie-Präfix verwendet werden.

---

**Hinweis** Das Aktivieren und Deaktivieren der Hochverfügbarkeitskonfiguration auf dem NSX Edge kann die Persistenz und den Ausgleichsstatus mit der Methode der Persistenz der Quell-IP-Adresse unterbrechen.

---

- **Aktivieren (Enable)** – Beendet den Wartungsmodus für den Server und setzt diesen wieder in Betrieb. Der Pool-Mitgliedsstatus sollte **Ausgleichen (Drain)** oder **Deaktiviert (Disabled)** lauten.
- **Deaktivieren (Disable)** – Der Server verbleibt im Wartungsmodus.

---

**Hinweis** Eine Änderung des Pool-Mitgliedsstatus von **Deaktiviert (Disabled)** in **Ausgleichen (Drain)** ist nicht möglich.

---

- d Geben Sie den Port ein, über den das Poolmitglied Datenverkehr empfangen soll, und den Überwachungsport, über den das Mitglied Statusüberwachungs-Pings empfangen soll.

Der Wert für den Port muss null sein, wenn der zugehörige virtuelle Server mit einem Portbereich konfiguriert wurde.

- e Geben Sie den Anteil des Datenverkehrs für dieses Mitglied im Abschnitt „Gewichtung“ ein.
- f Geben Sie die maximale Zahl der gleichzeitigen Verbindungen ein, die das Mitglied verarbeiten kann.

Wenn die eingehenden Anforderungen das Maximum überschreiten, werden sie in die Warteschlange eingereiht und warten auf die Freigabe einer Verbindung.

- g Geben Sie die Mindestanzahl der gleichzeitigen Verbindungen ein, die ein Mitglied immer akzeptieren muss.
  - h Klicken Sie auf **OK**.
- 11** Aktivieren Sie **Transparent**, um die Client-IP-Adressen für die Backend-Server sichtbar zu machen. Weitere Informationen finden Sie unter [Kapitel 15 Logischer Load Balancer](#).
- Ist die Option „Transparent“ nicht ausgewählt (Standardwert), sehen die Backend-Server als IP-Adresse der Datenverkehrsquelle die interne Load-Balancer-IP-Adresse. Ist die Option „Transparent“ ausgewählt, ist die Quell-IP-Adresse die reale Client-IP-Adresse, und NSX Edge muss als Standard-Gateway festgelegt werden, damit Rückpakete über das NSX Edge-Gerät geleitet werden.
- 12** Klicken Sie auf **OK**.

## Erstellen eines Anwendungsprofils

Verwenden Sie Anwendungsprofile, um Ihre Kontrolle über die Verwaltung von Netzwerkverkehr zu verbessern, und gestalten Sie Aufgaben zur Verwaltung des Datenverkehrs einfacher und effizienter.

Erstellen Sie ein Anwendungsprofil, um das Verhalten eines bestimmten Netzwerkverkehrstyps zu definieren. Ordnen Sie das Profil nach der Konfiguration des Profils einem virtuellen Server zu. Der virtuelle Server verarbeitet den Datenverkehr anschließend gemäß den im Profil angegebenen Werten.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Anwendungsprofile (Application Profiles)**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 7 Geben Sie einen Namen für das Profil ein und wählen Sie aus dem Dropdown-Menü den Datenverkehrstyp aus, für den Sie das Profil erstellen.

Datenverkehrstyp	Unterstützte Persistenzmethode
TCP	Quell-IP, MSRP
HTTP	Cookie, Quell-IP
HTTPS	Cookie, SSL-Sitzungs-ID (mit SSL-Passthrough aktiviert), Quell-IP
UDP	Quell-IP-Adresse

- 8 Geben Sie die URL ein, zu der Sie den HTTP-Datenverkehr umleiten möchten.
- Sie können den Datenverkehr beispielsweise von `http://myweb.com` zu `https://myweb.com` zuweisen.

## 9 Legen Sie den Persistenztyp für das Profil im Dropdown-Menü fest.

Die Persistenz verfolgt und speichert Sitzungsdaten wie das spezifische Poolmitglied, das eine Client-Anforderung verarbeitet hat. Die Persistenz stellt sicher, dass die Client-Anforderungen in einer gesamten Sitzung oder während nachfolgender Sitzungen demselben Poolmitglied zugeordnet werden.

- Wählen Sie die Persistenz **Cookie**, um ein eindeutiges Cookie zur Identifizierung der Sitzung beim ersten Zugriff eines Client auf die Site einzufügen.

Auf das Cookie wird in den folgenden Anforderungen zur Aufrechterhaltung der Verbindung mit dem jeweiligen Server Bezug genommen.

- Wählen Sie die Persistenz **Quell-IP (Source IP)** aus, um Sitzungen auf der Basis der Quell-IP-Adresse nachzuverfolgen.

Wenn ein Client eine Verbindung zu einem virtuellen Server anfordert, der die Affinitätspersistenz der Quelladresse unterstützt, überprüft der Load Balancer, ob der Client sich zuvor verbunden hat, und wenn dies der Fall ist, gibt er den Client zu demselben Poolmitglied zurück.

- Wählen Sie die Microsoft Remote Desktop Protocol (**MSRDP**)-Persistenz aus, um die persistenten Sitzungen zwischen Windows-Clients und -Servern, die in dem Microsoft Remote Desktop Protocol (RDP)-Dienst ausgeführt werden, beizubehalten.

Das empfohlene Szenario für die Aktivierung der MSRDP-Persistenz ist das Erstellen eines Load-Balancing-Pools, der aus Mitgliedern besteht, die Windows Server 2003 oder Windows Server 2008 ausführen, wobei alle Mitglieder zu einem Windows-Cluster gehören und an einem Windows-Sitzungsverzeichnis teilnehmen.

- 10 Geben Sie einen Cookie-Namen ein und wählen Sie den Modus aus, nach dem das Cookie eingefügt werden soll.

Option	Beschreibung
<b>Einfügen</b>	NSX Edge sendet ein Cookie. Sendet der Server eines oder mehrere Cookies, dann erhält der Client ein zusätzliches Cookie (Server-Cookie(s) + Edge-Cookie). Sendet der Server keine Cookies, dann erhält der Client nur das Edge-Cookie.
<b>Präfix</b>	Diese Option wird ausgewählt, wenn Ihr Client nur ein Cookie unterstützt.  <b>Hinweis</b> Alle Browser akzeptieren mehrere Cookies. Bei Ihrer Anwendung kann es sich auch um eine proprietäre Anwendung mit einem proprietären Client handeln, der nur ein Cookie unterstützt. Der Webserver sendet wie üblich sein Cookie. NSX Edge fügt seine Cookie-Information (als Präfix) in den Server-Cookiewert ein. Diese hinzugefügte Cookie-Information wird entfernt, wenn NSX Edge dieses an den Server sendet.
<b>App-Sitzung</b>	Der Server sendet kein Cookie. Stattdessen sendet er die Informationen zur Benutzersitzung als eine URL. Beispiel: <code>http://mysite.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD</code> , wobei <code>jsessionid</code> die Informationen zur Benutzersitzung darstellen und für die Persistenz verwendet werden. Die Persistenztabelle für die App-Sitzung kann zwecks Problembehebung nicht eingesehen werden.

- 11 Geben Sie den Zeitraum für die Persistenz bis zum Ablauf in Sekunden ein. Der Standardwert für die Persistenz beträgt 300 Sekunden (fünf Minuten). Beachten Sie, dass die Größe der Persistenztabelle begrenzt ist. Ein hoher Wert für die Zeitüberschreitung führt möglicherweise dazu, dass die Persistenztabelle sich schnell füllt, wenn der Datenverkehr hoch ist. Wenn die Persistenztabelle voll ist, wird für den aktuellen Eintrag der älteste Eintrag gelöscht.

Die Persistenztabelle des Load Balancer enthält Einträge, die die Weiterleitung von Clientanforderungen zum selben Poolmitglied aufzeichnen.

- Wenn vom selben Client keine neuen Verbindungsanforderungen innerhalb des festgelegten Zeitraums empfangen werden, verfällt der Persistenzeintrag und wird gelöscht.
- Wenn vom selben Client eine neue Verbindungsanforderung innerhalb des festgelegten Zeitraums eingeht, wird der Timer zurückgesetzt und die Clientanforderung an ein verfügbares Poolmitglied gesendet.
- Nach Ablauf des festgelegten Zeitraums wird eine Verbindungsanforderung an ein über den Load-Balancing-Algorithmus bestimmtes Poolmitglied gesendet.

Für den Fall einer TCP-Quell-IP-Persistenz mit dem L7-Load-Balancer legt der Persistenzeintrag den Zeitpunkt fest, ab dem keine neuen TCP-Verbindungen für einen bestimmten Zeitraum erstellt werden, auch wenn die vorhandenen Verbindungen weiterhin aktiv sind.

## 12 (Optional) Erstellen Sie ein Anwendungsprofil für den HTTPS-Datenverkehr.

Unterstützte HTTPS-Datenverkehrsmuster:

- SSL-Offloading – Client -> HTTPS -> LB (mit SSL-Beendigung) -> HTTP -> Server
  - SSL-Proxy – Client -> HTTPS -> LB (mit SSL-Beendigung) -> HTTPS -> Server
  - SSL-Passthrough – Client -> HTTPS-> LB (mit SSL-Passthrough) -> HTTPS -> Server
  - Client -> HTTP-> LB -> HTTP -> Server
- a (Optional) Aktivieren Sie **HTTP-Header 'X-Forwarded-For' einfügen (Insert X-Forwarded-For HTTP header)** für das Identifizieren der Ursprungs-IP-Adresse eines Clients aus, der über den Load Balancer eine Verbindung zu einem Webserver herstellt.
- b Aktivieren Sie **Dienstzertifikat konfigurieren (Configure Service Certificate)** in der Registerkarte **Zertifikate für den virtuellen Server (Virtual Server Certificates)** für die Auswahl des anwendbaren Serverzertifikats, der CA-Zertifikate und CRLs zur Beendigung des HTTPS-Datenverkehrs vom Client zum Load Balancer.

Dies ist nur dann erforderlich, wenn zwischen Client und LB eine HTTPS-Verbindung verwendet wird.

- c (Optional) Aktivieren Sie **Pool Side SSL aktivieren (Enable Pool Side SSL)** zur Aktivierung der HTTPS-Kommunikation zwischen dem Load Balancer und den Backend-Servern.

Sie können mit dem Pool-seitigen SSL ein End-to-End-SSL konfigurieren.

- d (Optional) Aktivieren Sie **Dienstzertifikat konfigurieren (Configure Service Certificate)** in der Registerkarte **Poolzertifikate (Pool Certificates)** für die Auswahl des anwendbaren Serverzertifikats, der CA-Zertifikate und CRLs zur Authentifizierung des Load Balancer auf der Serverseite.

Dies ist nur für das Muster Client -> HTTPS -> LB -> HTTPS -> Server erforderlich.

Sie können ein Dienstzertifikat konfigurieren, wenn der NSX Edge-Load Balancer über ein CA-Zertifikat verfügt und CRL bereits konfiguriert ist, und der Load Balancer ein Dienstzertifikat von Backend-Servern verifizieren muss. Diese Option kann auch für die Bereitstellung eines Load-Balancer-Zertifikats für Backend-Server verwendet werden, wenn der Backend-Server das Dienstzertifikat auf der Load-Balancer-Seite verifizieren muss.

- 13 Geben Sie die Verschlüsselungsalgorithmen oder die Verschlüsselungssammlung ein, die während des SSL/TLS-Handshakes ausgehandelt wurden. Mehrere Verschlüsselungen können durch Doppelpunkt (:) getrennt hinzugefügt werden. Stellen Sie sicher, dass die genehmigte Verschlüsselungs-Suite DH-Schlüssellängen von mindestens 1024 Bit enthält.

Sie können die genehmigte Verschlüsselungs-Suite verwenden, siehe unten:

Verschlüsselungswert	Verschlüsselungsname
DEFAULT	DEFAULT
ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ECDHE-RSA-AES256-GCM-SHA384	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Verschlüsselungswert	Verschlüsselungsname
ECDHE-RSA-AES256-SHA	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
ECDHE-ECDSA-AES256-SHA	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
ECDH-ECDSA-AES256-SHA	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
ECDH-RSA-AES256-SHA	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA
AES128-SHA	TLS_RSA_WITH_AES_128_CBC_SHA
DES-CBC3-SHA	TLS_RSA_WITH_3DES_EDE_CBC_SHA

- 14** Geben Sie im Dropdown-Menü an, ob die Client-Authentifizierung ignoriert werden soll oder erforderlich ist.

Wenn Sie „Erforderlich“ auswählen, muss der Client nach der Anforderung ein Zertifikat liefern oder der Handshake wird abgebrochen.

- 15** Klicken Sie auf **OK**.

## Hinzufügen einer Anwendungsregel

Sie können Anwendungsregeln schreiben, indem Sie die HAProxy-Syntax verwenden, um den Anwendungsdatenverkehr zu bearbeiten und zu verwalten.

Weitere Informationen zur Anwendungsregelsyntax finden Sie in der HAProxy-Dokumentation unter <http://cbonte.github.io/haproxy-dconv/>.

Beispiele für häufig verwendete Anwendungsregeln finden Sie unter [Beispiele für Anwendungsregeln](#).

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Anwendungsregeln (Application Rules)**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 7 Geben Sie den Namen und das Skript für die Regel ein.
- 8 Klicken Sie auf **OK**.

## Beispiele für Anwendungsregeln

Häufig verwendete Anwendungsregeln.

## HTTP/HTTPS-Umleitung nach Bedingung

Mit einem Anwendungsprofil können Sie eine HTTP/HTTPS-Umleitung angeben, die den Datenverkehr immer umleitet, unabhängig von den angeforderten URLs. Sie haben außerdem die Flexibilität, die Bedingungen anzugeben, unter denen der HTTP/HTTPS-Datenverkehr umgeleitet werden soll.

```
move the login URL only to HTTPS.
acl clear dst_port 80
acl secure dst_port 8080
acl login_page url_beg /login
acl logout url_beg /logout
acl uid_given url_reg /login?userid=[^&]+
acl cookie_set hdr_sub(cookie) SEEN=1
redirect prefix https://mysite.com set-cookie SEEN=1 if !cookie_set
redirect prefix https://mysite.com if login_page !secure
redirect prefix http://mysite.com drop-query if login_page !uid_given
redirect location http://mysite.com/ if !login_page secure
redirect location / clear-cookie USERID= if logout
```

## Routing nach Domänenname

Sie können eine Anwendungsregel erstellen, mit der Anforderungen je nach dem Domännennamen an einen spezifischen Load-Balancer-Pool geleitet werden. Die folgende Regel leitet Anforderungen an foo.com an pool\_1 und Anforderungen an bar.com an pool\_2.

```
acl is_foo hdr_dom(host) -i foo
acl is_bar hdr_dom(host) -i bar
use_backend pool_1 if is_foo
use_backend pool_2 if is_bar
```

## Microsoft RDP-Load-Balancing und Schutz

In dem folgenden Beispielszenario verteilt der Load Balancer einen neuen Nutzer auf den weniger ausgelasteten Server und nimmt eine unterbrochene Sitzung wieder auf. Die IP-Adresse der internen NSX Edge-Schnittstelle für dieses Szenario lautet 10.0.0.18, die interne Schnittstellen-IP-Adresse lautet 192.168.1.1 und die virtuellen Server haben die Adressen 192.168.1.100, 192.168.1.101 und 192.168.1.102.

- 1 Erstellen Sie ein Anwendungsprofil für den TCP-Verkehr mit MSRDP-Persistenz.
- 2 Erstellen Sie eine TCP-Statusüberwachung (tcp\_monitor).
- 3 Erstellen Sie einen Pool (namens rdp-pool) mit den Mitgliedern 192.168.1.100:3389, 192.168.1.101:3389 und 192.168.1.102:3389.
- 4 Ordnen Sie tcp\_monitor to rdp-pool zu.
- 5 Erstellen Sie die folgende Anwendungsregel.

```
tcp-request content track-sc1 rdp_cookie(msthash) table rdp-pool
tcp-request content track-sc2 src table ipv4_ip_table

each single IP can have up to 2 connections on the VDI infrastructure
tcp-request content reject if { sc2_conn_cur ge 2 }
```

```
each single IP can try up to 5 connections in a single minute
tcp-request content reject if { sc2_conn_rate ge 10 }

Each user is supposed to get a single active connection at a time, block the second one
tcp-request content reject if { sc1_conn_cur ge 2 }

if a user tried to get connected at least 10 times over the last minute,
it could be a brute force
tcp-request content reject if { sc1_conn_rate ge 10 }
```

- 6 Erstellen Sie einen virtuellen Server (namens rdp-vs).
- 7 Ordnen Sie das Anwendungsprofil diesem virtuellen Server zu und fügen Sie die in Schritt 4 erstellte Anwendungsregel hinzu.

Die neu zugewiesene Anwendungsregel auf dem virtuellen Server stellt einen Schutz für RDP-Server dar.

### Erweiterte Protokollierung

Der NSX-Load-Balancer unterstützt standardmäßig die allgemeine Protokollierung. Sie können wie folgt eine Anwendungsregel erstellen, um detailliertere Protokollierungsmeldungen für die Fehlersuche und -behebung anzuzeigen.

```
log the name of the virtual server
capture request header Host len 32

log the amount of data uploaded during a POST
capture request header Content-Length len 10
log the beginning of the referrer
capture request header Referer len 20

server name (useful for outgoing proxies only)
capture response header Server len 20

logging the content-length is useful with "option logasap"
capture response header Content-Length len 10

log the expected cache behaviour on the response
capture response header Cache-Control len 8

the Via header will report the next proxy's name
capture response header Via len 20

log the URL location during a redirection
capture response header Location len 20
```

Nachdem Sie die Anwendungsregel dem virtuellen Server zugeordnet haben, enthalten die Protokolle detaillierte Meldungen, wie zum Beispiel die folgende.

```
2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 -- [25/Apr/
2013:09:18:16 +0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51656 856 "vip-http-complete"
"pool-http-complete" "m2" 145 0 1 26 172 --NI 1 1 0 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux" ""

2013-04-25T09:18:17+00:00 edge-187 loadbalancer[18498]: [org1]: 10.117.7.117 -- [25/Apr/
2013:09:18:16 +0000] "GET /favicon.ico HTTP/1.1" 404 1440 "" "" 51657 856 "vip-http-complete"
"pool-http-complete" "m2" 412 0 0 2 414 --NI 0 0 0 0 0 0 0 "" "" "10.117.35.187" "Mozilla/5.0
(Windows NT 6.1; WOW64) AppleWebKit/537.31
(KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31" "Apache/2.2.15 (Linux" ""
```

Zur Fehlersuche und -behebung beim HTTPS-Datenverkehr müssen Sie möglicherweise weitere Regeln hinzufügen. Die meisten Webanwendungen verwenden 301/302-Antworten mit einem Adressheader, um den Client zu einer Seite umzuleiten (meistens nach einer Anmeldung oder einem POST-Aufruf) und erfordern außerdem ein Anwendungsscookie. Ihr Anwendungsserver könnte daher Schwierigkeiten bei der Ermittlung der Client-Verbindungsinformationen haben und kann möglicherweise nicht die richtigen Antworten geben: Er kann die Anwendung sogar anhalten.

Damit die Webanwendung die SSL-Verschiebung zulässt, müssen Sie die folgende Regel hinzufügen.

```
See clearly in the log if the application is setting up response for HTTP or HTTPS
capture response header Location len 32
capture response header Set-Cookie len 32

Provide client side connection info to application server over HTTP header
http-request set-header X-Forwarded-Proto https if { ssl_fc }
http-request set-header X-Forwarded-Proto http if !{ ssl_fc }
```

Der Load Balancer fügt den folgenden Header ein, wenn die Verbindung über SSL hergestellt wird.

```
X-Forwarded-Proto: https
```

Der Load Balancer fügt den folgenden Header ein, wenn die Verbindung über HTTP hergestellt wird.

```
X-Forwarded-Proto: http
```

## Sperrern spezifischer URLs

Sie können Anforderungen mit bestimmten Schlüsselwörtern in der URL sperren. Die nachfolgend aufgeführte Beispielregel überprüft, ob Anforderungen mit /private oder /finance beginnt und blockiert jede Anforderung mit solchen Begriffen.

```
Check if the request starts with "/private" or "/finance" (case insensitive)
acl block_url_list path_beg -i /private /finance

If the request is part of the list forbidden urls,reply "Forbidden"(HTTP response code
403)
block if block_url_list
```

## HTTP-Umleitung zur Authentifizierung ohne Cookies

Sie können eine Client-Anforderung, die über kein Cookie verfügt, für eine Authentifizierung umleiten. Die nachfolgend aufgeführte Beispielregel überprüft die Authentizität der HTTP-Anforderung und das Vorhandensein von Cookies in der Kopfzeile. Wenn die Anforderung über keine Cookies verfügt, leitet die Regel sie zu /authentic.php zur Authentifizierung um.

```
acl authentic_url url /authentic.php
acl cookie_present hdr_sub(cookie) cookie1=
redirect prefix /authentic.php if !authentic_url !cookie_present
```

## Umleitung zur Standardseite

Sie können die Client-Anforderung / zu einer Standardseite umleiten. Die nachfolgend aufgeführte Beispielregel überprüft, ob die HTTP-Anforderung / lautet, und leitet diese dann gegebenenfalls zu einer Standardanmeldeseite um.

```
acl default_url url /
redirect location /login.php if default_url
```

## Umleitung zur Wartungs-Site

Wenn der primäre Pool inaktiv ist, können Sie einen Wartungsserverpool verwenden und die URL zur Wartungs-Website umleiten.

```
redirect location http://maintenance.xyz.com/maintenance.htm
```

## NT LAN Manager- (NTLM-)Authentifizierung

Standardmäßig schließt NSX auf der Serverseite die TCP-Verbindung nach jeder Anforderung. Wenn Sie die Serversitzung nach einer Anforderung nicht schließen möchten, kann die Serversitzung aktiv und durch das NTLM-Protokoll gesichert bleiben.

```
no option http-server-close
```

Standardmäßig behält NSX auf dem Client die TCP-Verbindung bei, die zwischen Anforderungen eingerichtet wurde. Mit der Option „X-Forwarded-For“ wird die Sitzung jedoch nach jeder Anforderung geschlossen. Mit der im Folgenden dargestellten Option bleibt die Clientverbindung zwischen Anforderungen geöffnet, auch wenn XFF konfiguriert ist.

```
no option httpclose
```

## Ersetzen der Serverkopfzeile

Sie können die vorhandenen Antwortserverkopfzeilen löschen und diese durch einen anderen Server ersetzen. Die im Folgenden aufgeführte Beispielregel löscht die Serverkopfzeile und ersetzt diese mit dem NGINX-Webserver, der als Reverseproxyserver für HTTP-, HTTPS-, SMTP-, POP3- und IMAP-Protokolle sowie für den HTTP-Cache und als Load Balancer dienen kann.

```
rspidel Server
rspadd Server:\ nginx
```

## Ändern der Umleitung

Sie können den Adressheader von HTTP in HTTPS ändern. Die nachfolgend dargestellte Beispielregel ermittelt den Adressheader und ersetzt HTTP mit HTTPS.

```
rspirep ^Location:\ http://(.*) Location:\ https://\1
```

## Auswählen bestimmter Pools auf der Basis eines Hosts

Sie können Anforderungen mit einem bestimmten Host zu definierten Pools umleiten. Das nachfolgend aufgeführte Beispiel überprüft die Anforderungen auf bestimmte Hosts wie app1.xyz.com, app2.xyz.com und host\_any\_app3 und leitet diese Anforderungen jeweils zu den definierten Pools pool\_app1 oder pool\_app2 und pool\_app3 um. Alle anderen Anforderungen werden zu vorhandenen, im virtuellen Server definierten Pools umgeleitet.

```
acl host_app1 hdr(Host) -i app1.xyz.com
acl host_app2 hdr(Host) -i app2.xyz.com
acl host_any_app3 hdr_beg(host) -i app3
```

Verwenden Sie einen bestimmten Pool für jeden einzelnen Hostnamen.

```
use_backend pool_app1 if host_app1
use_backend pool_app2 if host_app2
use_backend pool_app3 if host_any_app3
```

## Auswählen bestimmter Pools auf der Basis von URLs

Sie können Anforderungen mit URL-Schlüsselwörtern zu bestimmten Pools umleiten. Die nachfolgend aufgeführte Beispielregel überprüft, ob die Anforderungen mit /private oder /finance beginnen und leitet diese Anforderungen dann zu den definierten Pools pool\_private oder pool\_finance um. Alle anderen Anforderungen werden zu vorhandenen, im virtuellen Server definierten Pools umgeleitet.

```
acl site_private path_beg -i /private
acl site_finance path_beg -i /finance
use_backend pool_private if site_private
use_backend pool_finance if site_finance
```

## Umleitung bei inaktivem primären Pool

Wenn Ihre Server im primären Pool inaktiv sind, können Sie Benutzer zu den Servern im sekundären Pool umleiten. Die nachfolgend aufgeführte Beispielregel überprüft, ob `pool_production` inaktiv ist und überträgt die Benutzer dann in diesem Fall zu `pool_sorry_server`.

```
acl pool_production_down nbsrv(pool_production) eq 0
use_backend pool_sorry_server if pool_production_down
```

## Positivliste für die TCP-Verbindung

Sie können Client-IP-Adressen für den Zugriff auf Ihren Server sperren. Die im Folgenden dargestellte Beispielregel blockiert die definierte IP-Adresse und setzt die Verbindung zurück, wenn die Client-IP-Adresse nicht in der Positivliste enthalten ist.

```
acl whitelist src 10.10.10.0 20.20.20.0
tcp-request connection reject if !whitelist
```

## Aktivieren von sslv3 und tlsv1

Standardmäßig sind die Dienstmonitorerweiterungen `sslv3` und `tlsv1` deaktiviert. Sie können diese mit der nachfolgend dargestellten Anwendungsregel aktivieren.

```
sslv3 enable
tlsv1 enable
```

## Konfigurieren des Zeitlimits für die Clientsitzung

Der Wert für das Sitzungszeitlimit stellt die maximal zulässige Dauer der Verbindungsinaktivität auf der Clientseite dar. Dieses Zeitlimit für die Inaktivität gilt in den Fällen, in denen Daten vom Client bestätigt oder gesendet werden sollen. Im HTTP-Modus wird dieses Zeitlimit insbesondere sowohl in der ersten Phase berücksichtigt, wenn der Client die Anforderung sendet, als auch während der Antwort, wenn der Client die vom Server gesendeten Daten liest. Das Standardzeitlimit beträgt fünf Minuten.

Die nachfolgende Beispielregel legt den Zeitraum auf 100 Sekunden fest.

```
timeout client 100s
```

Der Zeitwert kann als Ganzzahl in Millisekunden, Sekunden, Minuten, Stunden oder Tagen festgelegt werden.

## Umleitung zur HTTPS-Site

Sie können die Clients, die HTTP nutzen, zu derselben Seite mit HTTPS umleiten.

```
Redirect all HTTP requests to same URI but HTTPS redirect scheme
https if ![ssl_fc]
```

Eine andere Möglichkeit lautet wie folgt:

```
rsprep ^Location:\ http://(.*) Location:\ https://\1
```

## Nicht authentische Clients umleiten

Leiten Sie die Client-Anforderungen an „/authent.php“ um, wenn sie kein Cookie haben.

```
Check the HTTP request if request is "/authent.php"
acl authent_url url /authent.php
Check the cookie "cookie1" is present
acl cookie_present hdr_sub(cookie) cookie1=
If the request is NOT "/authent.php" and there is no cookie, then redirect to "/authent.php"
redirect prefix /authent.php if !authent_url !cookie_present
```

## HTTP-Antwortkopfzeile umschreiben

Ersetzen Sie die Antwortserverkopfzeile „Server“ durch den Wert „nginx“.

```
Delete the existing Response Server header "Server"
rspidel Server
Add the Response Server header "Server" with the value "nginx"
rspadd Server:\ nginx
```

## Sorry Server

Falls die Server im primären Pool alle ausgefallen sind, verwenden Sie Server aus dem sekundären Pool.

```
detect if pool "pool_production" is still up
acl pool_production_down nbsrv(pool_production) eq 0
use pool "pool_sorry_server" if "pool_production" is dead
use_backend pool_sorry_server if pool_production_down
Option 1: # Redirect everything to maintenance site
redirect location http://maintenance.xyz.com/maintenance.htm
Option 2: #Use a specific maintenance server pool and rewrite all URLs to maintenance.php
acl match_all always_true
use_backend maint_pool if match_all
reqirep ^GET\(.*)\HTTP\(.*) GET\ /maintenance.php\ HTTP/\2
```

## Hinzufügen von virtuellen Servern

Fügen Sie eine interne Schnittstelle oder eine Uplink-Schnittstelle von NSX Edge als virtuellen Server hinzu.

### Voraussetzungen

- Stellen Sie sicher, dass ein Anwendungsprofil verfügbar ist. Weitere Informationen dazu finden Sie unter [Erstellen eines Anwendungsprofils](#).
- Erläuterungen zum Zuordnen einer Anwendungsregel zu einem virtuellen Server erhalten Sie unter [Erstellen eines Anwendungsprofils](#).
- Die Aktivierung der Beschleunigung für die Verwendung eines schnelleren Load Balancer muss bei der Konfiguration des Load Balancer durchgeführt werden. Weitere Informationen dazu finden Sie unter [Konfigurieren des Load-Balancer-Dienstes](#).

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Virtuelle Server (Virtual Servers)**.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 7 Aktivieren Sie **Virtuellen Server aktivieren (Enable Virtual Server)**, damit dieser virtuelle Server für die Verwendung zur Verfügung steht.
- 8 (Optional) Aktivieren Sie **Beschleunigung aktivieren (Enable Acceleration)** für den NSX Edge-Load Balancer zur Verwendung der schnelleren L4-Load-Balancer-Engine anstelle der L7-Load-Balancer-Engine.

---

**Hinweis** Für diese Konfiguration muss die Firewall am Edge aktiviert sein.

---

Wenn die Konfiguration eines virtuellen Servers, z. B. für Anwendungsregeln, HTTP-Typ oder Cookie-Persistenz die L7-Load-Balancer-Engine verwendet, gilt dies unabhängig von der Aktivierung der Beschleunigung. Die Option **Beschleunigung aktiviert (Acceleration Enabled)** unter „Globale Konfiguration“ muss ausgewählt sein.

Mit dem CLI-Befehl **show service loadbalancer virt** können Sie die verwendete Load-Balancer-Engine überprüfen.

- 9 Wählen Sie das Anwendungsprofil aus, das dem virtuellen Server zugewiesen werden soll.  
Das Anwendungsprofil muss dasselbe Protokoll verwenden wie der virtuelle Server, den Sie hinzufügen. Die vom ausgewählten Pool unterstützten Dienste werden angezeigt.
- 10 Geben Sie einen Namen und eine Beschreibung für den virtuellen Server ein.
- 11 Klicken Sie auf **IP-Adresse auswählen (Select IP Address)**, um die IP-Adresse festzulegen, die der Load Balancer überwacht, und um das Protokoll einzugeben, das der virtuelle Server verarbeiten wird.  
Das Dialogfeld „IP-Adresse auswählen“ zeigt nur die primäre IP-Adresse an. Wenn Sie ein VIP erstellen, das eine sekundäre IP-Adresse verwendet, geben Sie sie manuell ein.
- 12 Wählen Sie das Protokoll für den virtuellen Server aus dem Dropdown-Menü aus.
- 13 Geben Sie die Portnummer ein, die der Load Balancer überwacht.  
Sie können für Ports auch einen Bereich festlegen, z. B. 80,8001-8004,443, um die Konfiguration des virtuellen Servers etwa für Serverpool, Anwendungsprofil und Anwendungsregel freizugeben.  
Für die Verwendung von FTP muss dem TCP-Protokoll der Port 21 zugewiesen werden.
- 14 Wählen Sie die Anwendungsregel aus.

- 15 Geben Sie im Abschnitt „Grenzwert für Verbindungen“ die maximale Anzahl an Verbindungen ein, die der virtuelle Server gleichzeitig verarbeiten kann.
- 16 Geben Sie im Abschnitt „Grenzwert für Verbindungsrate“ die maximale Anzahl an eingehenden neuen Verbindungsanforderungen pro Sekunde ein.
- 17 (Optional) Klicken Sie auf die Registerkarte **Erweitert (Advanced)** und fügen Sie die Anwendungsregel hinzu, die dem virtuellen Server zugeordnet werden soll.
- 18 Klicken Sie auf **OK**.

## Verwalten von Anwendungsprofilen

Nach dem Erstellen eines Anwendungsprofils und dessen Zuordnung zu einem virtuellen Server können Sie das vorhandene Profil aktualisieren oder zur Erhöhung der verfügbaren Systemressourcen löschen.

### Bearbeiten eines Anwendungsprofils

Sie können ein Anwendungsprofil bearbeiten.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Anwendungsprofile (Application Profiles)**.
- 6 Wählen Sie ein Profil aus und klicken Sie auf das Symbol **Bearbeiten (Edit)** (✎).
- 7 Führen Sie die entsprechenden Änderungen für den Datenverkehr, die Persistenz, das Zertifikat oder die Verschlüsselungskonfiguration durch und klicken Sie auf **Beenden (Finish)**.

### Konfigurieren der SSL-Beendigung für einen Load Balancer

Ohne konfigurierte SSL-Beendigung werden HTTP-Anforderungen nicht überprüft. Der Load Balancer sieht die Quell- und Ziel-IP-Adressen und verschlüsselte Daten. Wenn Sie die HTTP-Anforderungen überprüfen möchten, können Sie die SSL-Sitzung auf dem Load Balancer beenden und dann eine neue SSL-Sitzung für den Zellpool erstellen.

#### Voraussetzungen

Wechseln Sie zu **Verwalten > Einstellungen > Zertifikate (Manage > Settings > Certificates)**, um sicherzustellen, dass ein gültiges Zertifikat vorhanden ist. Sie können ein Zertifikat für Load Balancer wie folgt hochladen:

- Im PEM-Format oder

- Per CSR-Generierung oder
- Per Erstellung eines selbstsignierten Zertifikats

### Verfahren

- 1 Erstellen Sie ein Anwendungsprofil durch Auswahl von **Verwalten > Load Balancer > Anwendungsprofile (Manage > Load Balancer > Application Profiles)**.
- 2 Wählen Sie als Typ **HTTPS** aus dem Dropdown-Menü aus.
- 3 Stellen Sie sicher, dass **SSL-Passthrough aktivieren (Enable SSL Passthrough)** nicht ausgewählt ist.
- 4 Stellen Sie sicher, dass **Dienstzertifikat konfigurieren (Configure Service Certificate)** aktiviert ist.
- 5 Wählen Sie das geeignete Zertifikat aus der Liste aus.

**Edit Profile** ?

Name:

Type:

☐ Enable SSL Passthrough

HTTP Redirect URL:

Persistence:

Cookie Name:

Mode:

Expires in (Seconds):

☐ Insert X-Forwarded-For HTTP header

☐ Enable Pool Side SSL

**Virtual Server Certificates** Pool Certificates

Service Certificates CA Certificates CRL

☒ Configure Service Certificate

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

## Löschen eines Anwendungsprofils

Sie können ein Anwendungsprofil löschen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.

- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Anwendungsprofile (Application Profiles)**.
- 6 Wählen Sie ein Profil aus und klicken Sie auf das Symbol **Löschen (Delete)**.

## Verwalten von Dienstmonitoren

Ein Dienstmonitor definiert Parameter für die Systemstatusprüfung des Lastausgleichsdiensts.

Wenn Sie die Überwachung für den Lastausgleichsdienst mit High Availability (HA) verwenden, muss diese auf einer eigenen Schnittstelle aktiviert sein.

Nach dem Erstellen eines Dienstmonitors und dessen Zuordnung zu einem Pool können Sie den vorhandenen Dienstmonitor aktualisieren oder löschen, um weniger Systemressourcen in Anspruch zu nehmen.

Weitere Informationen zu Dienstmonitoren finden Sie unter [Erstellen eines Dienstmonitors](#).

## Bearbeiten eines Dienstmonitors

Sie können einen Dienstmonitor bearbeiten.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Dienstüberwachung (Service Monitoring)**.
- 6 Wählen Sie einen Dienstmonitor aus und klicken Sie auf das Symbol **Bearbeiten (Edit)**.
- 7 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.

## Löschen eines Dienstmonitors

Sie können einen Dienstmonitor löschen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.

- 5 Klicken Sie im linken Navigationsfenster auf **Dienstüberwachung (Service Monitoring)**.
- 6 Wählen Sie einen Dienstmonitor aus und klicken Sie auf das Symbol **Löschen (Delete)**.

## Verwalten von Serverpools

Nachdem Sie einen Serverpool zur Verwaltung der Load-Balancer-Verteilung hinzugefügt haben, können Sie den vorhandenen Pool aktualisieren oder zur Erhöhung der verfügbaren Systemressourcen löschen.

### Bearbeiten eines Serverpools

Sie können einen Serverpool bearbeiten.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Vergewissern Sie sich, dass Sie sich auf der Registerkarte „Pool“ befinden.
- 6 Wählen Sie den zu bearbeitenden Pool aus.
- 7 Klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- 8 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.

### Konfigurieren eines Load Balancer zur Verwendung des transparenten Modus

„Transparent“ gibt an, ob Client-IP-Adressen für die Backend-Server sichtbar sind. Ist die Option „Transparent“ nicht ausgewählt (Standardwert), sehen die Backend-Server als IP der Datenverkehrsquelle die interne Load-Balancer-IP. Wurde die Option „Transparent“ ausgewählt, stellt die Quell-IP-Adresse die reale Client-IP-Adresse dar und NSX Edge muss sich auf dem Pfad der Serverantwort befinden. Ein typisches Konzept ist die Verwendung des NSX Edge als Server-Standard-Gateway.

Weitere Informationen finden Sie unter [Kapitel 15 Logischer Load Balancer](#).

## Verfahren

- ◆ In der Konfiguration der Serverpools aktivieren Sie unter **Verwalten > Load Balancer > Pools** (Manage > Load Balancer > Pools) den transparenten Modus.

**Edit Pool**

Name: \* Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default\_https\_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	web-01a	172.16.1...	1	443	443	0	0
✓	web-02a	172.16.1...	1	443	443	0	0

☒ Transparent

OK Cancel

## Löschen eines Serverpools

Sie können einen Serverpool löschen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Vergewissern Sie sich, dass Sie sich auf der Registerkarte „Pool“ befinden.
- 6 Wählen Sie den zu löschenden Pool aus.
- 7 Klicken Sie auf das Symbol **Löschen (Delete)** (✗).

## Anzeigen der Poolstatistik

Sie können den aktuellen Systemzustand des Pools und der zugeordneten Poolmitglieder anzeigen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.

- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Pools**.
- 6 Wählen Sie den erforderlichen Pool aus, und klicken Sie dann auf den Link **Poolstatistik anzeigen (Show Pool Statistics)**.

Der Poolstatus kann UP (Aktiv) oder DOWN (Inaktiv) lauten. Ein Pool ist als DOWN (Inaktiv) markiert, wenn alle Mitglieder im Pool inaktiv sind. Andernfalls lautet der Poolstatus UP (Aktiv).

Der Mitgliedsstatus kann wie folgt lauten:

- UP (Aktiv): Das Mitglied ist aktiviert, und der Systemzustand des Mitglieds lautet UP (Aktiv). Oder für den Pool ist keine Überwachung definiert.
- DOWN (Inaktiv): Das Mitglied ist aktiviert, und der Systemzustand des Mitglieds lautet DOWN (Inaktiv).
- MAINT (Wartung): Das Mitglied ist deaktiviert.
- DRAIN: Das Mitglied befindet sich im Drain-Status.

## Verwalten von virtuellen Servern

Nach dem Hinzufügen von virtuellen Servern können Sie die vorhandene Konfiguration für virtuelle Server aktualisieren oder löschen.

### Bearbeiten eines virtuellen Servers

Sie können einen virtuellen Server bearbeiten.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie auf die Registerkarte **Virtuelle Server (Virtual Servers)**.
- 6 Wählen Sie den zu bearbeitenden virtuellen Server aus.
- 7 Klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- 8 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **Beenden (Finish)**.

## Löschen eines virtuellen Servers

Sie können einen virtuellen Server löschen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie auf die Registerkarte **Virtuelle Server (Virtual Servers)**.
- 6 Wählen Sie den zu löschenden virtuellen Server aus.
- 7 Klicken Sie auf das Symbol **Löschen (Delete)** (✖).

## Verwalten von Anwendungsregeln

Nach dem Erstellen von Anwendungsregeln zur Konfiguration des Anwendungsdatenverkehrs können Sie die vorhandene Regel bearbeiten oder entfernen.

### Bearbeiten einer Anwendungsregel

Verwenden Sie die HAProxy-Syntax, um Anwendungsregeln zum Steuern des Anwendungsdatenverkehrs hinzuzufügen oder zu bearbeiten.

Weitere Informationen zur Anwendungsregelsyntax finden Sie in der HAProxy-Dokumentation unter <http://cbonte.github.io/haproxy-dconv/>.

Beispiele für häufig verwendete Anwendungsregeln finden Sie unter [Beispiele für Anwendungsregeln](#).

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Anwendungsregeln (Application Rules)**.
- 6 Wählen Sie eine Regel aus und klicken Sie auf das Symbol **Bearbeiten (Edit)**.
- 7 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.

## Löschen einer Anwendungsregel

Sie können eine Anwendungsregel löschen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 5 Klicken Sie im linken Navigationsfenster auf **Anwendungsprofile (Application Profiles)**.
- 6 Wählen Sie ein Profil aus und klicken Sie auf das Symbol **Löschen (Delete)**.

## Load-Balancer-Webserver mit NTLM-Authentifizierung

Für den NSX-Load Balancer und die NTLM-Authentifizierung muss die Serververbindung aufrechterhalten werden.

Standardmäßig schließt der NSX-Load Balancer die Server-TCP-Verbindung nach jeder Clientanforderung, jedoch ist für die Windows NT LAN Manager (NTLM)-Authentifizierung diese Verbindung für die Lebensdauer der authentifizierten Anfrage erforderlich. Daher werden Verbindungen für die Dauer der Anfragen aufrechterhalten.

Damit die Serververbindung zwischen Anforderungen offen bleibt, fügen Sie die folgende Anwendungsregel zur virtuellen IP für die Lastverteilung der Webserver mithilfe der NTLM-Authentifizierung hinzu:

```
add # NTLM authentication and keep the server connection open between requests
no option http-server-close
```

## HTTP-Verbindungsmodi des Load Balancer

Bei NSX 6.1.5 und höher ändert sich beim Aktivieren von „x-forwarded-for“ der HTTP-Verbindungsmodus von „Passiv schließen“ (Option „httpclose“) in den Standard-HTTP-Modus „Server schließen“ (http-server-close). Dadurch bleibt die Clientverbindung offen, während die Verbindung mit Serverkontakt nach dem Empfang einer Antwort vom Server geschlossen wird. Vor NSX 6.1.5 beendete der NSX-Load Balancer die Verbindung nicht proaktiv, sondern fügte die Kopfzeile „Connection:close“ in beide Richtungen ein, um die Verbindung durch den Client oder Server zu schließen. Wenn eine HTTP/HTTPS-Transaktion beim NSX-Load Balancer nach dem Upgrade auf NSX 6.1.5 oder später fehlschlägt, fügen Sie eine Anwendungsregel mit der Skriptoption „httpclose“ hinzu und ordnen Sie sie dem virtuellen Server zu, der nicht mehr ausgeführt wird.

**HTTP-Server schließen (Standard)** – Die Verbindung mit Serverkontakt wird beendet, nachdem das Ende der Antwort empfangen wurde, und die Verbindung mit Clientkontakt bleibt offen. „HTTP-Server schließen“ bietet Latenz auf Clientseite (langsames Netzwerk) und Wiederverwendung der schnellsten Sitzung auf Serverseite, um weniger Serverressourcen in Anspruch zu nehmen. Sie ermöglicht außerdem, dass nicht-keep-alive-fähige Server mit Hinblick auf den Client im Keep-alive-Modus bedient werden. Dieser Modus eignet sich für die am häufigsten auftretenden Anwendungsfälle, insbesondere für langsame Netzwerke mit Clientkontakt und schnelle Netzwerke mit Serverkontakt.

**HTTP-Keep-alive** – Alle Anforderungen und Antworten werden verarbeitet und Verbindungen bleiben offen, aber zwischen Antworten und neuen Anfragen im Leerlauf. Reduzierte Latenz zwischen Transaktionen und weniger erforderliche Verarbeitungsleistung auf Serverseite sind die Vorteile. Beachten Sie, dass die Anforderungen an den Arbeitsspeicher erhöht werden, um die Anzahl der aktiven Sitzungen aufzunehmen, die steigt, da Verbindungen nicht mehr nach jeder Anforderung geschlossen werden. Zeitüberschreitung bei Leerlauf mit Clientkontakt kann über die Anwendungsregel „timeout http-keep-alive [time]“ konfiguriert werden. Standardmäßig beträgt die Leerlaufzeitüberschreitung 1 Sekunde. Dieser Modus ist zwingend erforderlich, wenn für eine Anwendung NTLM-Authentifizierung erforderlich ist.

**HTTP-Tunnel** – Nur die erste Anforderung und Antwort werden verarbeitet und es wird ein Tunnel zwischen Client und Server hergestellt, um die Kommunikation ohne weitere Analyse des HTTP-Protokolls zu ermöglichen. Sobald die Verbindung eingerichtet ist, ist sie sowohl auf Client- als auch Serverseite persistent. Zum Aktivieren dieses Modus sollte keine der folgenden Optionen festgelegt werden: „Passiv schließen“, „Server schließen“, „Schließen erzwingen“.

Der HTTP-Tunnelmodus hat Auswirkungen auf die folgenden Funktionen und betrifft nur die erste Anforderung und Antwort in einer Sitzung:

- Keine Protokollerstellung
- HTTP-Kopfzeilenanalyse
- HTTP-Kopfzeilenmanipulation
- Cookieverarbeitung
- Inhaltswechsel
- Einfügen der Kopfzeile „X-Forwarded-For“

**HTTP passiv schließen** – Wie Tunnelmodus, aber mit Kopfzeile „Connection: close“ sowohl in der Client- als auch der Serverrichtung. Beide Enden werden geschlossen, nachdem die erste Anforderung und Antwort ausgetauscht wurden. Wenn „option httpclose“ festgelegt ist, wird der NSX-Load Balancer im HTTP-Tunnelmodus ausgeführt und überprüft, ob die Kopfzeile „Connection: close“ in beiden Richtungen vorhanden ist. Wenn die Kopfzeile nicht vorhanden ist, wird eine „Connection: close“-Kopfzeile hinzugefügt. An beiden Enden wird dann aktiv die TCP-Verbindung nach jeder Übertragung geschlossen, sodass in den HTTP-Schließen-Modus gewechselt wird. Kopfzeilen von Verbindungen, die nicht „Schließen“ lauten, werden entfernt. Anwendungen, die die zweite sowie nachfolgende Anforderungen nicht ordnungsgemäß verarbeiten können (z. B. ein eingefügtes Cookie durch den NSX-Load Balancer, das dann durch die folgenden Clientanfragen zurückübertragen wird), können den Tunnel- oder Passiv-schließen-Modus verwenden.

Einige HTTP-Server schließen nicht notwendigerweise die Verbindungen, wenn sie „Connection: close“ wie durch „option httpclose“ festgelegt erhalten. Wenn der Client auch nicht geschlossen wird, bleibt die Verbindung offen, bis die Zeitüberschreitung eintritt. Dies führt zu einer großen Anzahl simultaner Verbindungen auf den Servern und langen globalen Sitzungszeiten in den Protokollen. Aus diesem Grund sind sie nicht mit älteren HTTP-1.0-Browsern kompatibel. Falls dies passiert, verwenden Sie „option forceclose“, wodurch die Anforderungsverbindung aktiv geschlossen wird, nachdem der Server antwortet. Durch die Option „forceclose“ wird außerdem die Serververbindung früher geschlossen, da nicht auf die Bestätigung des Clients gewartet werden muss.

HTTP-schließen erzwingen – Sowohl Client als auch Serververbindungen werden am Ende einer Antwort aktiv vom NSX-Load Balancer geschlossen. Einige HTTP-Server schließen nicht notwendigerweise die Verbindungen, wenn sie „Connection: close“ wie durch „option httpclose“ festgelegt erhalten. Wenn der Client auch nicht geschlossen wird, bleibt die Verbindung offen, bis die Zeitüberschreitung eintritt. Dies führt zu einer großen Anzahl simultaner Verbindungen auf den Servern und langen globalen Sitzungszeiten in den Protokollen. In diesem Fall schließt „option forceclose“ aktiv den ausgehenden Serverkanal, sobald der Server die Antwort abgeschlossen hat. So werden einige Ressourcen früher freigegeben als mit „option httpclose“.

<b>NSX</b>	<b>Standardverbindungsmodus</b>	<b>Verbindungsmodus bei aktiviertem „X-Forwarded-For“</b>	<b>Verfügbare Anwendungsregeln zum Wechsel des Verbindungsmodus</b>
6.0.x, 6.1.0, 6.1.1	HTTP-Server schließen	„option httpclose“ wird dem virtuellen Server automatisch hinzugefügt, um das Hinzufügen von XFF zu jeder Anforderung wie im HAProxy-Dokument angegeben zu erzwingen. Die XFF-Kopfzeile wird jeder Anforderung vom Client bei der Übergabe an einen Backendserver hinzugefügt.	Nein
6.1.2–6.1.4	HTTP-Server schließen	HTTP passiv schließen („option httpclose“ wird dem virtuellen Server automatisch hinzugefügt)	„no option http-server-close“ „option httpclose“ „no option httpclose“
6.1.5–6.1.x, 6.2.0–6.2.2	HTTP-Server schließen	Die XFF-Kopfzeile „HTTP-Server schließen“ wird jeder Anforderung vom Client bei der Übergabe an einen Backendserver hinzugefügt.	„no option http-server-close“ „option httpclose“ „no option httpclose“
6.2.3–6.2.5	HTTP-Server schließen	Die XFF-Kopfzeile „HTTP-Server schließen“ wird jeder Anforderung vom Client bei der Übergabe an einen Backendserver hinzugefügt.	„no option http-server-close“ „option httpclose“ „no option httpclose“

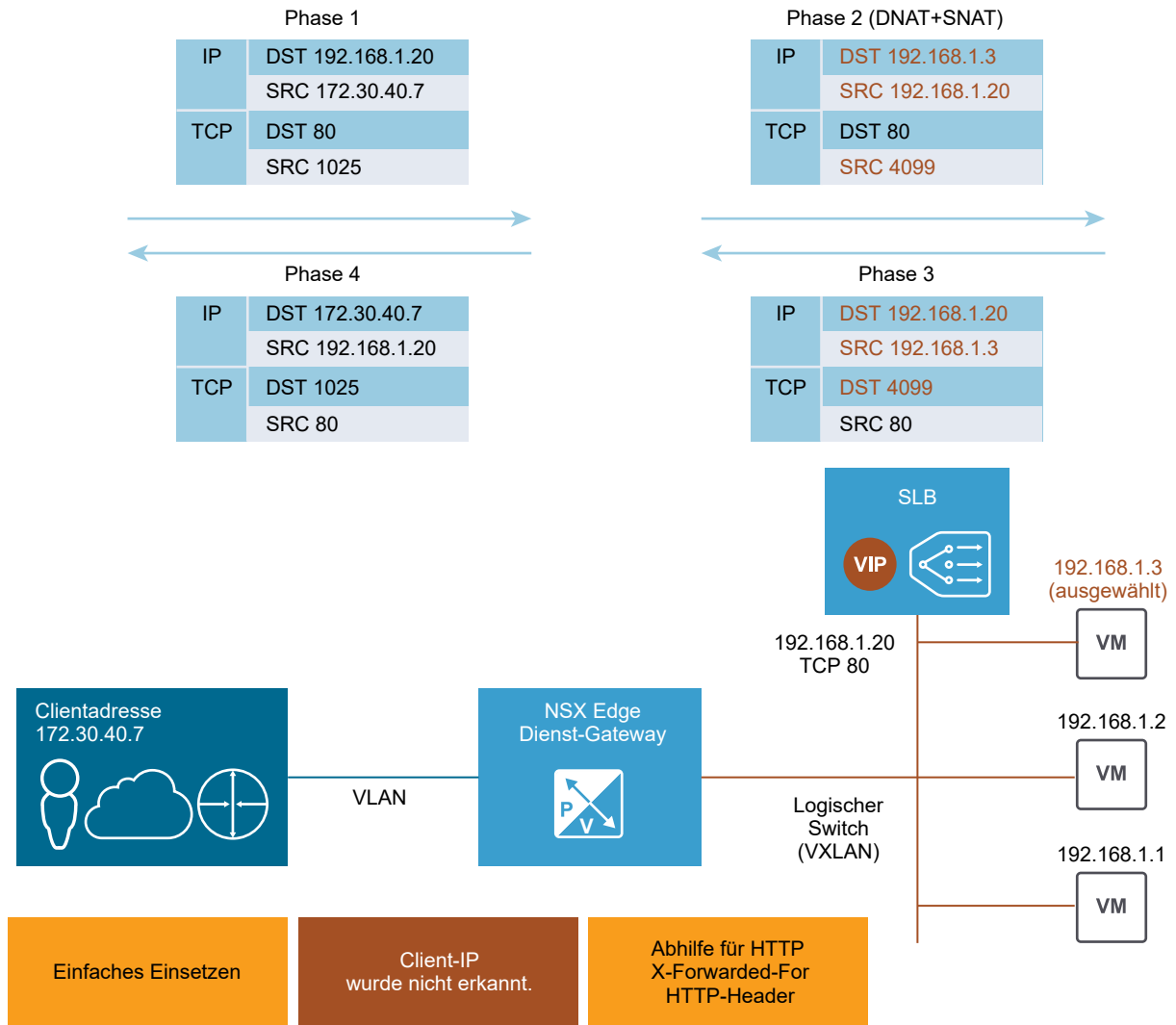
<b>NSX</b>	<b>Standardverbindungsmodus</b>	<b>Verbindungsmodus bei aktiviertem „X-Forwarded-For“</b>	<b>Verfügbare Anwendungsregeln zum Wechsel des Verbindungsmodus</b>
6.2.3–6.2.5	HTTP-Server schließen	Die XFF-Kopfzeile „HTTP-Server schließen“ wird jeder Anforderung vom Client bei der Übergabe an einen Backendserver hinzugefügt.	„no option http-server-close“ „no option httpclose“ „option httpclose“
6.2.5–6.2.x	HTTP-Server schließen	Die XFF-Kopfzeile „HTTP-Server schließen“ wird jeder Anforderung vom Client bei der Übergabe an einen Backendserver hinzugefügt.	„no option http-server-close“ „option http-keep-alive“ „option http-tunnel“ „option httpclose“ „option forceclose“

## Szenarien für die NSX-Load-Balancer-Konfiguration

Die Szenarien für die NSX-Load-Balancer-Konfiguration bieten eine erläuternde Darstellung des erforderlichen End-to-End-Workflows.

### Konfiguration eines einarmigen Load Balancer

Das Edge Services Gateway (ESG) kann als Proxy für den eingehenden Benutzerdatenverkehr angesehen werden.



Im Proxymodus verwendet der Load Balancer seine eigene IP-Adresse als Quelladresse, um Anforderungen an einen Backend-Server zu senden. Der Backend-Server interpretiert jeden Datenverkehr so, als würde er vom Load Balancer gesendet und antwortet dem Load Balancer direkt. Dieser Modus wird auch als SNAT-Modus oder nicht-transparenter Modus bezeichnet. Weitere Informationen finden Sie unter *Administratorhandbuch für NSX*.

Ein typischer einarmiger NSX-Load-Balancer wird in demselben Subnetz wie seine Backend-Server bereitgestellt, getrennt vom logischen Router. Der virtuelle Server des NSX-Load-Balancer hört eine virtuelle IP auf eingehende Anforderungen ab und verteilt die Anforderungen an die Backend-Server. Für den Datenverkehr in der Gegenrichtung ist eine umgekehrte NAT erforderlich, um die Quell-IP-Adresse vom Backend-Server in eine virtuelle IP- (VIP-)Adresse umzuwandeln und dann die VIP-Adresse an den Client zu senden. Ohne diesen Vorgang wird die Verbindung zum Client unterbrochen.

Nachdem das ESG den Datenverkehr empfangen hat, werden zwei Operationen durchgeführt: Mit der „Destination Network Address Translation“ (DNAT) wird die VIP-Adresse in die IP-Adresse einer Load-Balancer-Maschine umgewandelt. Mit der „Source Network Address Translation“ (SNAT) wird die Client-IP-Adresse durch die ESG-IP-Adresse ersetzt.

Dann sendet der ESG-Server den Datenverkehr an den Load-Balancer-Server und der Load-Balancer-Server sendet die Antwort zurück an das ESG und weiter an den Client. Diese Option ist sehr viel einfacher zu konfigurieren als der Inline-Modus. Es sind aber zwei potenzielle Einschränkungen vorhanden. Erstens erfordert dieser Modus einen dedizierten ESG-Server, zweitens kennen die Load-Balancer-Server die Original-IP-Adresse des Client nicht. Eine Problemumgehung für HTTP/HTTPS-Anwendungen besteht in der Aktivierung von „X-Forwarded-For“ einfügen“ im HTTP-Anwendungsprofil, damit die Client-IP-Adresse in den X-Forwarded-For-HTTP-Header der Anforderung übertragen wird, die zum Backend-Server gesendet wird.

Wenn der Backend-Server die Client-IP-Adresse für andere Anwendungen als HTTP/HTTPS kennen muss, können Sie den IP-Pool so konfigurieren, dass er transparent ist. Wenn sich die Clients nicht in demselben Subnetz befinden wie die Backend-Server, sollte der Inline-Modus verwendet werden. Andernfalls müssen Sie die IP-Adresse des Load Balancer als Standard-Gateway des Backend-Servers verwenden.

---

**Hinweis** In der Regel gibt es drei Methoden, um die Verbindungsintegrität zu gewährleisten:

- Inline-/Transparent-Modus
- SNAT-/Proxy-/nicht-transparenter Modus (siehe Erläuterungen weiter oben)
- Direct Server Return (SDR) – derzeit nicht unterstützt

Im DSR-Modus sendet der Backend-Server die Antwort direkt an den Client. Aktuell unterstützt der NSX-Load-Balancer DSR nicht.

---

## Verfahren

- 1 Lassen Sie uns als Beispiel einen einarmigen virtuellen Server mit SSL-Offloading konfigurieren. Erstellen Sie ein Zertifikat durch Doppelklicken auf das Edge und durch anschließende Auswahl von **Verwalten > Einstellungen > Zertifikat (Manage > Settings > Certificate)**.

- 2 Aktivieren Sie den Dienst des Load Balancer durch Auswahl von **Verwalten > Load Balancer > Globale Konfiguration > Bearbeiten (Manage > Load Balancer > Global Configuration > Edit)**.

- 3 Erstellen Sie ein HTTPS-Anwendungsprofil durch Auswahl von **Verwalten > Load Balancer > Anwendungsprofile (Manage > Load Balancer > Application Profiles)**.

	Common Name	Issuer	Validity
<input checked="" type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu
<input type="radio"/>	VSM_SOLUTION_71	VSM_SOLUTION_71	Tue Sep 8 2015 - Thu

**Hinweis** Die in der obigen Abbildung verwendeten selbstsignierten Zertifikate dienen nur der Veranschaulichung.

- 4 Optional klicken Sie auf **Verwalten > Load Balancer > Dienstüberwachung (Manage > Load Balancer > Service Monitoring)** und ändern Sie die Standarddienstüberwachung vom Basis-HTTP/HTTPS-Protokoll in spezifische URL/URIs je nach Anforderung.

- 5 Erstellen Sie Serverpools durch Auswahl von **Verwalten > Load Balancer > Pools (Manage > Load Balancer > Pools)**.

Wenn Sie den SNAT-Modus verwenden möchten, lassen Sie das Kontrollkästchen **Transparent** in der Poolkonfiguration deaktiviert.

**Edit Pool**

Name: \* Web-Tier-Pool-01

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default\_https\_monitor

Members:

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
✓	web-01a	172.16.10.11	1	443	443	0	0
✓	web-02a	172.16.10.12	1	443	443	0	0

☒ Transparent

OK Cancel

Stellen Sie sicher, dass die VMs aufgelistet und aktiviert sind.

- 6 Optional klicken Sie auf **Verwalten > Load Balancer > Pools > Poolstatistik anzeigen (Manage > Load Balancer > Pools > Show Pool Statistics)**, um den Status zu überprüfen.

Stellen Sie sicher, dass der Mitgliedsstatus „UP“ ist.

- 7 Erstellen Sie einen virtuellen Server durch Auswahl von **Verwalten > Load Balancer > Virtueller Server (Manage > Load Balancer > Virtual Servers)**.

Wenn Sie den L4-Load-Balancer für UDP oder ein leistungsstärkeres TCP verwenden möchten, aktivieren Sie **Beschleunigung aktivieren (Enable Acceleration)**. Wenn Sie **Beschleunigung aktivieren (Enable Acceleration)** aktiviert haben, stellen Sie sicher, dass der Firewallstatus auf dem Load-Balancer-NSX Edge auf **Aktiviert (Enabled)** festgelegt ist, da für L4 SNAT eine Firewall erforderlich ist.

**General** | Advanced

☒ Enable Virtual Server  
☐ Enable Acceleration

Application Profile: \* OneArmWeb-01 ▼

Name: \* Web-Tier-VIP-01

Description:

IP Address: \* 172.16.10.10 [X] Select IP Address

Protocol: HTTPS ▼

Port: \* 443

Default Pool: Web-Tier-Pool-01 ▼

Connection Limit: 0

Connection Rate Limit: 0 (CPS)

Stellen Sie sicher, dass die IP-Adresse an den Serverpool gebunden ist.

- 8 Optional können Sie, wenn Sie eine Anwendungsregel verwenden, die Konfiguration unter **Verwalten > Load Balancer > Anwendungsregeln (Manage > Load Balancer > Application Rules)** überprüfen.

**Add Application Rule** ?

Name: App-Rule-1

Script: # A sample application rule to log the name of the virtual server  
capture request header Host len 32

- 9 Bei der Verwendung einer Anwendungsregel müssen Sie sicherstellen, dass die Anwendungsregel mit dem virtuellen Server verbunden ist. Dies können Sie unter **Verwalten > Load Balancer > Virtueller Server > Erweitert (Manage > Load Balancer > Virtual Servers > Advanced)**überprüfen.

Weitere unterstützte Beispiele finden Sie unter <https://communities.vmware.com/docs/DOC-31772>.

**Edit Virtual Server** ?

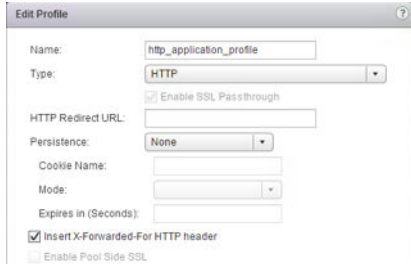
General | **Advanced**

Application Rules:

+ × ≡ ↕ Filter

Rule Id	Name	Script
applicationRule-1	App-rule-1	capture request he...

Im nicht-transparenten Modus kann der Backend-Server nicht die Client-IP, aber die interne IP-Adresse des Load Balancer erkennen. Als Problemumgehung für den HTTP/HTTPS-Datenverkehr aktivieren Sie **HTTP-Header 'X-Forwarded-For' einfügen (Insert X-Forwarded-For HTTP header)**. Wenn diese Option aktiviert ist, fügt der Edge Load Balancer den Header „X-Forwarded-For“ mit dem Wert der Client-Quell-IP-Adresse hinzu.



## Szenario: Konfigurieren des NSX-Load-Balancer für den Platform Services Controller

Der Platform Services Controller (PSC) bietet Sicherheitsfunktionen für die Infrastruktur wie z. B. vCenter Single Sign-On (einmalige Anmeldung), Lizenzierung, Zertifikatverwaltung und Serverreservierung.

Nach der Konfiguration des NSX-Load-Balancer können Sie die Uplink-Schnittstellen-IP-Adresse des NSX Edge-Geräts für ein vCenter Single Sign-On bereitstellen.

### Voraussetzungen

- Führen Sie die in der Knowledgebase aufgeführten Vorbereitungsaufgaben für die PSC-Hochverfügbarkeit (High Availability) durch. Weitere Informationen dazu finden Sie unter <http://kb.vmware.com/kb/2113315>.
- Speichern Sie /ha/lb.crt und /ha/lb\_rsa.key vom ersten PSC-Knoten zur Konfiguration der Zertifikate.
- Stellen Sie sicher, dass ein NSX Edge-Gerät konfiguriert ist.
- Stellen Sie sicher, dass mindestens ein Uplink für die VIP-Konfiguration vorhanden ist und eine Schnittstelle dem internen logischen Switch angefügt wurde.

### Verfahren

- 1 Fügen Sie dem NSX Edge PSC-CA-Zertifikate hinzu.
  - a Speichern Sie die PSC-Datei root.cer und das Zertifikat sowie RSA und die mit dem Befehl OpenSSL generierte Passphrase.
  - b Doppelklicken Sie auf das Edge, und wählen Sie **Verwalten (Manage) > Einstellungen (Settings) > Zertifikat (Certificate)** aus.
  - c Fügen Sie die gespeicherte Inhaltsdatei root.cer dem CA-Zertifikat-Inhalt hinzu.
  - d Fügen Sie die gespeicherte Passphrase dem Abschnitt für den privaten Schlüssel hinzu.

**2** Aktivieren Sie den Load-Balancer-Dienst.

- a Wählen Sie **Verwalten (Manage) > Load Balancer > Bearbeiten (Edit)** aus.
- b Aktivieren Sie die Optionen **Load Balancer aktivieren (Enable Load Balancing)** und **Protokollierung (Logging)**.

- 3 Erstellen Sie mit den TCP- und HTTPS-Protokollen Anwendungsprofile.
  - a Wählen Sie **Verwalten (Manage) > Load Balancer > Anwendungsprofile (Application Profiles)** aus.
  - b Erstellen Sie ein TCP-Anwendungsprofil.

The 'New Profile' dialog box is shown with the following configuration:

- Name:** sso\_tcp\_profile
- Type:** TCP
- ☐ Enable SSL Passthrough
- HTTP Redirect URL:** (empty)
- Persistence:** Source IP
- Cookie Name:** (empty)
- Mode:** (empty)
- Expires in (Seconds):** (empty)
- ☐ Insert X-Forwarded-For HTTP header
- ☐ Enable Pool Side SSL
- Virtual Server Certificates:** Pool Certificates
- Service Certificates:** CA Certificates
- ☐ Configure Service Certificate
- | Common Name        | Issuer | Validity              |
|--------------------|--------|-----------------------|
| NSX-ESG-1-0.system | CA     | Thu Jul 30 2015 - Thu |
- Cipher:** (empty)
- Client Authentication:** Ignore

Buttons: OK, Cancel

- c Erstellen Sie ein HTTPS-Anwendungsprofil.

The 'New Profile' dialog box is shown with the following configuration:

- Name:** sso\_https\_profile
- Type:** HTTPS
- ☐ Enable SSL Passthrough
- HTTP Redirect URL:** (empty)
- Persistence:** Source IP
- Cookie Name:** (empty)
- Mode:** (empty)
- Expires in (Seconds):** (empty)
- ☐ Insert X-Forwarded-For HTTP header
- ☒ Enable Pool Side SSL
- Virtual Server Certificates:** Pool Certificates
- Service Certificates:** CA Certificates
- ☒ Configure Service Certificate
- | Common Name        | Issuer | Validity              |
|--------------------|--------|-----------------------|
| NSX-ESG-1-0.system | CA     | Thu Jul 30 2015 - Thu |
- Cipher:** (empty)
- Client Authentication:** Ignore

Buttons: OK, Cancel

- 4 Erstellen Sie Anwendungspools zum Hinzufügen von Mitglieds-PSC-Knoten.
- Wählen Sie **Verwalten (Manage) > Load Balancer > Pools** aus.
  - Erstellen Sie zwei Anwendungspools mit dem Überwachungsport 443.  
Verwenden Sie die IP-Adresse des PSC-Knotens.

**Edit Pool** ?

Name: \* sso\_tcp\_pool1

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default\_tcp\_monitor

Members:

+ ✎ ✕

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	PSC01	192.168....	1	443		0	0
✓	PSC02	192.168....	1	443		0	0

☐ Transparent

OK Cancel

- Erstellen Sie zwei Anwendungspools mit dem Überwachungsport 389.  
Verwenden Sie die IP-Adresse des PSC-Knotens.

**New Pool** ?

Name: \* sso\_tcp\_pool2

Description:

Algorithm: ROUND-ROBIN

Algorithm Parameters:

Monitors: default\_tcp\_monitor

Members:

+ ✎ ✕

Enabled	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connection.
✓	PSC01	192.168....	1	389		0	0
✓	PSC02	192.168....	1	389		0	0

☐ Transparent

OK Cancel

- 5 Erstellen Sie virtuelle Server für die TCP- und HTTPS-Protokolle.
  - a Wählen Sie **Verwalten (Manage) > Load Balancer > Virtuelle Server (Virtual Servers)** aus.
  - b Erstellen Sie einen virtuellen Server für TCP VIP.

The screenshot shows the 'New Virtual Server' dialog box with the 'General' tab selected. The configuration is as follows:

- ☒ Enable Virtual Server
- ☐ Enable Acceleration
- Application Profile: \* sso\_tcp\_profile
- Name: \* sso\_tcp\_vip
- Description: (empty)
- IP Address: \* 10.156.209.158 [Select IP Address](#)
- Protocol: TCP
- Port: \* 389,636,2012,2014,2020
- Default Pool: sso\_tcp\_pool2
- Connection Limit: (empty)
- Connection Rate Limit: (empty) (CPS)

Buttons: OK, Cancel

- c Erstellen Sie einen virtuellen Server für HTTPS VIP.

The screenshot shows the 'New Virtual Server' dialog box with the 'General' tab selected. The configuration is as follows:


- ☒ Enable Virtual Server
- ☐ Enable Acceleration
- Application Profile: \* sso\_https\_profile
- Name: \* sso\_https\_vip
- Description: (empty)
- IP Address: \* 10.156.209.158 [Select IP Address](#)
- Protocol: HTTPS
- Port: \* 443
- Default Pool: sso\_tcp\_pool1
- Connection Limit: (empty)
- Connection Rate Limit: (empty) (CPS)

Buttons: OK, Cancel

## Szenario: SSL-Offloading

Edge beendet Client-HTTPS (SSL-Sitzungen). Edge führt ein Load Balancing für die Clients auf HTTP auf den Servern durch. Es können L7-Anwendungsregeln angewendet werden.

## Verfahren

- 1 Importieren Sie das Webserverzertifikat.
  - a Melden Sie sich beim vSphere Web Client an.
  - b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
  - c Doppelklicken Sie auf eine NSX Edge-Instanz.
  - d Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**.
  - e Klicken Sie im linken Navigationsfenster auf **Zertifikate (Certificates)**.
  - f Klicken Sie auf das Symbol **Hinzufügen (Add)** () und wählen Sie anschließend **Zertifikat (Certificate)** aus. Weitere Informationen finden Sie unter [Arbeiten mit Zertifikaten](#).

- g Kopieren Sie den Zertifikatsinhalt und fügen Sie ihn in das Textfeld **Zertifikatsinhalt (Certificate Contents)** ein. Der Text sollte die Ausdrücke „-----BEGIN xxx-----“ und „-----END xxx-----“ beinhalten.

Wählen Sie für verkettete Zertifikate (Serverzertifikat und Root-CA-Zertifikat) die Option **Zertifikat (Certificate)** aus. Es folgt ein Beispiel für den Inhalt verketteter Zertifikate:

```
-----BEGIN CERTIFICATE-----
 Server cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 Root cert
-----END CERTIFICATE-----
```

- h Kopieren Sie den Inhalt des privaten Schlüssels und fügen Sie ihn in das Textfeld **Privater Schlüssel (Private Key)** ein.

Es folgt ein Beispiel für den Inhalt des privaten Schlüssels:

```
-----BEGIN RSA PRIVATE KEY-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END RSA PRIVATE KEY-----
```

Dem Zertifikatsinhalt (PEM für Zertifikat oder privaten Schlüssel) sollte eine der folgenden Zeichenfolgen vorangestellt sein:

```
-----BEGIN PUBLIC KEY-----
-----BEGIN RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE REQUEST-----
-----BEGIN NEW CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE-----
-----BEGIN PKCS7-----
-----BEGIN X509 CERTIFICATE-----
-----BEGIN X509 CRL-----
-----BEGIN ATTRIBUTE CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
-----BEGIN DSA PRIVATE KEY-----
-----BEGIN EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
```

Vollständige Beispiele für Zertifikate und private Schlüssel finden Sie unter dem Thema [Beispiel: Zertifikat und privater Schlüssel](#).

**Hinweis** Das folgende Präfix wird in NSX Manager nicht unterstützt:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

## 2 Erstellen Sie das HTTPS-Anwendungsprofil.

- a Melden Sie sich beim vSphere Web Client an.
- b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- c Doppelklicken Sie auf eine NSX Edge-Instanz.
- d Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Load Balancer**.
- e Klicken Sie im linken Navigationsfenster auf **Anwendungsprofil (Application Profile)**. Weitere Informationen finden Sie unter [Verwalten von Anwendungsprofilen](#).
- f Erstellen Sie ein neues Anwendungsprofil mit den folgenden Parametern:
  - Wählen Sie unter „Typ“ in der Liste den Eintrag **HTTPS** aus.
  - Aktivieren Sie das Kontrollkästchen **Dienstzertifikate konfigurieren (Configure Service Certificates)**.
  - Wählen Sie das in Schritt 1 konfigurierte Serverzertifikat aus.

## 3 Erstellen Sie einen virtuellen Server.

- a Melden Sie sich beim vSphere Web Client an.
- b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- c Doppelklicken Sie auf eine NSX Edge-Instanz.
- d Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Load Balancer**.
- e Klicken Sie im linken Navigationsfenster auf **Virtuelle Server (Virtual Servers)**. Weitere Informationen finden Sie unter [Verwalten von virtuellen Servern](#).
- f Erstellen Sie einen neuen virtuellen Server mit den folgenden Parametern:
  - Aktivieren Sie das Kontrollkästchen **Virtuellen Server aktivieren (Enable Virtual Server)**, um den virtuellen Server für die Verwendung zur Verfügung zu stellen.
  - Wählen Sie unter „Protokoll“ die Option **HTTPS** aus.
  - Wählen Sie den aus HTTP-Servern (nicht aus HTTPS-Servern) bestehenden Standardpool aus.
  - Wählen Sie das in Schritt 2 konfigurierte Anwendungsprofil aus.

## Beispiel: Zertifikat und privater Schlüssel

Nachfolgend finden Sie Beispiele für Zertifikate und den privaten Schlüssel.

### Webserver-Zertifikat

```
-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEWJGUjET
MBEGA1UECAwKU29tZS1TdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDALBgNVBAoMBERp
bWkxDALBgNVBAsMBE5TQlUxEDA0BgNVBAMMB0RpbWkgQ0ExGzAZBgkqhkiG9w0B
```

```

CQEWdGRpbWlAZGltA5SmcjAeFw0xNDAMjgyMDM2NTVaFw0yNDAMjYyMDM2NTVa
MFsxZAJBgNVBAYTAkZSMRMwEQYDVQIDApTb211LVN0YXRIMSEwHwYDVQQKBHJ
bnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxFDASBgNVBAMMC3d3dy5kaW1pLmZyMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvpnaPKLIKdvx98KW681z8pGa
RRcYersNGqPjpi fMVjJE8LuCoXgPU0HePnNTUjPShBnynKCvrtWhN+haKbSp+QWX
SxiTrW99HBfAl1MDQYwCukoEb9Cw6INctVUN4iRvkn9T8E6q174RbcnwA/7yTc7p
1NCvw+6B/aAN9l1G2pQXgRdYC/+G6o1IZEHtWhqzE97nY5QKNUVD0V09dc5CDYB
aKjgetwvw6DFk/GRd0SEd/6bW+20z0qSHpa3YNW6qSp+x5pyYmDrzRIR03os6Dau
ZkChSRyc/Whvurx6o85D6qpzywo8xwNaLZHxTQPgcIA5su9ZIyTv9LH2E+lSwwID
AQABO3sweTAJBgNVHRMEAIAAMCwGCWGSAGG+EIBDQqFFh1PcGVuU1NMIEdlbmVy
YXR1ZCBBDXJ0aWZpY2F0ZTAuBgNVHQ4EFgQU+tugFtyN+cXe1wxUqeA7X+yS3bgw
HwYDVROjBBgwFoAUhMwqkbBrGp87HxfvvgPn1GgVR64wDQYJKoZIhvcNAQEFBQAD
ggEBAIEEmqghEzeXZ4CKhE5UM9vCKzkj5Iv9TFs/a9CcQuepzplT7YVmevBFN0c0
+1ZyR4tXgi4+5MHGzhYCIvHo4hKqYm+J+o5mwQInflqoAHu07CLD3WNa1sKcVUV
vepIxc/1aHzRG+dPeEHt0MDF0w13YdUc2FH6AqEdcEL4aV5PXq2eYR8hR4zKbc1
fBtuqUsvA8NWSIyzQ16fyGve+ANf6vXvUizyvwDrPRv/kfvLNa3ZPnLMMxU98Mvh
PXy3PkB8++6U4Y3vdk2Ni2WYYLIls8yqbM4327IKmDc2TimS8u60CT47mKU7aDY
cbTV5RDkrLaYwm5yqlTIgLvCv7o=
-----END CERTIFICATE-----

```

## Webserver-Zertifikat mit Verkettung (einschließlich Stamm-CA)

```

-----BEGIN CERTIFICATE-----
MIID0DCCArigAwIBAgIBATANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjET
MBEGA1UECAwKU29tZS1tdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERp
bWkxDTALBgNVBASMBE5TQlUxEDA0BgNVBAMMB0RpbWkgQ0ExGzAZBgkqhkiG9w0B
CQEWdGRpbWlAZGltA5SmcjAeFw0xNDAMjgyMDM2NTVaFw0yNDAMjYyMDM2NTVa
MFsxZAJBgNVBAYTAkZSMRMwEQYDVQIDApTb211LVN0YXRIMSEwHwYDVQQKBHJ
bnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxFDASBgNVBAMMC3d3dy5kaW1pLmZyMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvpnaPKLIKdvx98KW681z8pGa
RRcYersNGqPjpi fMVjJE8LuCoXgPU0HePnNTUjPShBnynKCvrtWhN+haKbSp+QWX
SxiTrW99HBfAl1MDQYwCukoEb9Cw6INctVUN4iRvkn9T8E6q174RbcnwA/7yTc7p
1NCvw+6B/aAN9l1G2pQXgRdYC/+G6o1IZEHtWhqzE97nY5QKNUVD0V09dc5CDYB
aKjgetwvw6DFk/GRd0SEd/6bW+20z0qSHpa3YNW6qSp+x5pyYmDrzRIR03os6Dau
ZkChSRyc/Whvurx6o85D6qpzywo8xwNaLZHxTQPgcIA5su9ZIyTv9LH2E+lSwwID
AQABO3sweTAJBgNVHRMEAIAAMCwGCWGSAGG+EIBDQqFFh1PcGVuU1NMIEdlbmVy
YXR1ZCBBDXJ0aWZpY2F0ZTAuBgNVHQ4EFgQU+tugFtyN+cXe1wxUqeA7X+yS3bgw
HwYDVROjBBgwFoAUhMwqkbBrGp87HxfvvgPn1GgVR64wDQYJKoZIhvcNAQEFBQAD
ggEBAIEEmqghEzeXZ4CKhE5UM9vCKzkj5Iv9TFs/a9CcQuepzplT7YVmevBFN0c0
+1ZyR4tXgi4+5MHGzhYCIvHo4hKqYm+J+o5mwQInflqoAHu07CLD3WNa1sKcVUV
vepIxc/1aHzRG+dPeEHt0MDF0w13YdUc2FH6AqEdcEL4aV5PXq2eYR8hR4zKbc1
fBtuqUsvA8NWSIyzQ16fyGve+ANf6vXvUizyvwDrPRv/kfvLNa3ZPnLMMxU98Mvh
PXy3PkB8++6U4Y3vdk2Ni2WYYLIls8yqbM4327IKmDc2TimS8u60CT47mKU7aDY
cbTV5RDkrLaYwm5yqlTIgLvCv7o=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDyTCCArGgAwIBAgIBADANBgkqhkiG9w0BAQUFADB/MQswCQYDVQQGEwJGUjET
MBEGA1UECAwKU29tZS1tdGF0ZTEOMAwGA1UEBwwFUGFyaXMxDTALBgNVBAoMBERp
bWkxDTALBgNVBASMBE5TQlUxEDA0BgNVBAMMB0RpbWkgQ0ExGzAZBgkqhkiG9w0B
CQEWdGRpbWlAZGltA5SmcjAeFw0xNDAMjgyMDI2NDRaFw0yNDAMjYyMDI2NDRa
MH8xCzAJBgNVBAYTAkZSMRMwEQYDVQIDApTb211LVN0YXRIMQ4wDAYDVQQHDAVQ
YXJpczENMAsGA1UECgwERGRltaTENMASGA1UECwwETlNCVTEQMA4GA1UEAwwHRGlt
aSBDOQTEbMBkGCSqGSIb3DQEJARYMZGltAUBkaW1pLmZyMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEauxuG4QeBIGXj/AB/YRLLtpgpTpGnDntVlgsycZrL
3qqyQdBNlwnvCB9etfY5iWzjeq7YZRr6i0dIV4sFNBR2NoK+YvdD9j1TRi7njZg0

```

```
d6zth0x1s0hCsDlV/YCL1CTcYDlKA/QiKeIQa7GU3RhF0t/KnAkr6mwoDbdKBQX1
D5HgQuXJiFdH5XRebxF1ZB3gH+0kCEaEZPrjFDApk0XNxEARZdpBLpbvQljtVXtj
HMsvrIOc7QqUSOU3GcbBMSHJT8cgg8ssf492Go3bDQkIzTROz9QgDHaqDqTC9Hoe
vLIpTS+q/3BCY5AGWKL3CCR6dDyK6honn0R/8srezaN4PwIDAQABo1AwTjAdBgNV
HQ4EFgQUHmWqkbBrGp87HxfvvgPnLGgVR64wHwYDVR0jBBgwFoAUhMwqkbBrGp87
HxfvvgPnLGgVR64wDAYDVR0TBAlUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAQYq
vhm5wAEKmvRKRjeb5kiEIP7oZAFkYp6sKODuZ1VdkjMDD4wv46iqAe1QIIIsfGwd
Dmv0oqSl+iPPy24ATMSZQBPL05K64Hw7Q8KPos0yD8gHSg2d4S0ukj+FD2IjAH17
a8auMw7TTHu6976JprQKtPADRcfodGd5UFiz/6ZgLzUE23cktJMc2Bt18B90ZII
J9ef2PZxZirJg10qF2KsDLJP5EC09K3EmovC5M5Aly++s8ayjBnNivtklYL1V0T
ZrpPgcndTHUA5KS/Duf40dXm0snCxLAKNP28pMowDLSYc6IjVrD4+qqw3f1b7yGb
bJcFgxKDeg5YecQOSg==
-----END CERTIFICATE-----
```


## Privater Schlüssel (keine Passphrase)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAwpnaPKLIKdvx98KW68lz8pGaRRcYersNGqPjpi fMVjjE8LuC
oXgPU0HePnNTUjpShBnynKCvrtWhN+haKbSp+QWXSxiTrW99HBfAl1MDQyWcukoE
b9Cw6INctVUN4iRvkn9T8E6q174RbcnW/7yTc7p1NCvw+6B/aAN9l1G2pQXgRdY
C/+G6o1IIEHtWhqzE97nY5QKNUVD0V09dc5CDYBaKjgetwvw6DFk/GRd0SEd/6b
W+20z0qSHpa3YNW6qSp+x5pyYmDrZRIR03os6DauZkChSRyc/Whvurx6o85D6qpz
ywo8xwNaLZXhTQPgcIA5su9ZIyvtv9LH2E+lSwwIDAQABaoIBAFm18cD9a5pMqlW3
f9btTQz1sRL4Fvp7CmHSXhvsjeHwhHckEe0ObkWTRsgkTsm1XLu5W8IITnhn0+1
iNr+78eB+rRGngdAXh8di0dkEy+8/Cee8tFI3jyutKdRlXmbwiKsouVviumoq3fx
OGQYwQ0Z2l/PvCwy/Y82Ffq3ysC5gAJsbBYsCrg14bQo44ulrELE4SDWs5HCjKYb
EI2b8c0MucqZS0txg9niLN/je2bo/I2HGSawibgc0dBms8k6TvsSrZMr3kJ506J+
77LGwKH37brVgbVYvbq6nWPL0xLG7dUv+7LWEo5qQaPy6aXb/zbcqkLqu6/Ej0Ve
ydG5JQECgYEA9kKFTZD/WEVAreA0dzfeJRu8vlnwoagL7cJaoDxqXos4mcr5mPDT
kbWgFkLFFH/AyUnPB1K6BcJp1XK67B13ETUa3i9Q5t1WuZEobiKKBLFm9DDQJt43
uKZWJxBKFGSvFrYPtGZst719mZVcPct2CzPjEgN3Hlpt6fyw3e0rnoECgYEAxiOu
jwXC0muGaB7+0W2tR0PGEzbvVLEGdKAJ6TC/HoKM1A8r2u4hLTEJJCrLLTfw++4I
ddHE2dLeR4Q7058SfLphwgPmLDezN7WRLGr7Vyfuv7VmaHjGuC3Gv9aghnWD1A2Q
gBG9/R9oVFL0Dc7CgJgLeUtItCYC31bGT3yhV0McgYEA4k3DG4L+RN4PXDpHvK9I
pA1jXAJHEifeHnaW1d3vWkbSkvJmgVf+9U5VeV+OwRHN1qzPZV4suRI6M/8lK8rA
Gr4UnM4aqK4K/qkY4G05LKrik9Ev2CgqSLQDRA7CJQ+Jn3Nb50qq6hFnFPafN+J7
7juWln08wFYV4Atpd+9XQECgYBxizkZFL+9Iqkf0cONvWAZGo+Dq1N0L3J4iTIk
w56CKWxyj88d4qB4eUU3yJ4uB4S9miaW/eLEwKZIBWpUPFAn0db7i6h3ZmP5ZL8Q
qS3nQCb9DULmU2/tU641eRUKAmIoka1g9sndKAZuWo+o6fdkIb1Rg0bk9XNn8R4r
psv+aQKBgB+CICExR30vycv5bnZN9EFLIXNkaeMJUrYCXcRQNvrnUIUBvA08+jAe
CdLygS5RtgOLZib0IVERqWsp3EI1ACGuLts0vQ9GFLQGaN1SaMS40C9kvns1mLDu
LhIhYpJ8UsCVt5snWo2N+M+6ANh5tpWdQnEK6zILh4tRbuzaiHgb
-----END RSA PRIVATE KEY-----
```

## Szenario: Importieren eines SSL-Zertifikats

SSL-End-to-End: Das NSX Edge beendet Client-HTTPS (SSL-Sitzungen). Edge führt einen Lastausgleich des Clients für neue HTTPS-Verbindungen mit den Servern durch. Es können L7-Anwendungsregeln angewendet werden.

## Verfahren

- 1 Importieren Sie das Webserverzertifikat.
  - a Melden Sie sich beim vSphere Web Client an.
  - b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
  - c Doppelklicken Sie auf eine NSX Edge-Instanz.
  - d Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**.
  - e Klicken Sie im linken Navigationsfenster auf **Zertifikate (Certificates)**.
  - f Klicken Sie auf das Symbol **Hinzufügen (Add)** () und wählen Sie anschließend **Zertifikat (Certificate)** aus. Weitere Informationen finden Sie unter [Arbeiten mit Zertifikaten](#).

- g Kopieren Sie den Zertifikatsinhalt und fügen Sie ihn in das Textfeld **Zertifikatsinhalt (Certificate Contents)** ein. Der Text sollte die Ausdrücke „-----BEGIN xxx-----“ und „-----END xxx-----“ beinhalten.

Wählen Sie für verkettete Zertifikate (Serverzertifikat und Root-CA-Zertifikat) die Option **Zertifikat (Certificate)** aus. Es folgt ein Beispiel für den Inhalt verketteter Zertifikate:

```
-----BEGIN CERTIFICATE-----
 Server cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 Intermediate cert
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 Root cert
-----END CERTIFICATE-----
```

- h Kopieren Sie den Inhalt des privaten Schlüssels und fügen Sie ihn in das Textfeld **Privater Schlüssel (Private Key)** ein.

Es folgt ein Beispiel für den Inhalt des privaten Schlüssels:

```
-----BEGIN RSA PRIVATE KEY-----
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-----END RSA PRIVATE KEY-----
```

Dem Zertifikatsinhalt (PEM für Zertifikat oder privaten Schlüssel) sollte eine der folgenden Zeichenfolgen vorangestellt sein:

```
-----BEGIN PUBLIC KEY-----
-----BEGIN RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE REQUEST-----
-----BEGIN NEW CERTIFICATE REQUEST-----
-----BEGIN CERTIFICATE-----
-----BEGIN PKCS7-----
-----BEGIN X509 CERTIFICATE-----
-----BEGIN X509 CRL-----
-----BEGIN ATTRIBUTE CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
-----BEGIN DSA PRIVATE KEY-----
-----BEGIN EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
```

Vollständige Beispiele für Zertifikate und private Schlüssel finden Sie unter dem Thema [Beispiel: Zertifikat und privater Schlüssel](#).

**Hinweis** Das folgende Präfix wird in NSX Manager nicht unterstützt:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
```

## 2 Erstellen Sie das HTTPS-Anwendungsprofil.

- a Melden Sie sich beim vSphere Web Client an.
- b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- c Doppelklicken Sie auf eine NSX Edge-Instanz.
- d Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Load Balancer**.
- e Klicken Sie im linken Navigationsfenster auf **Anwendungsprofil (Application Profile)**. Weitere Informationen finden Sie unter [Verwalten von Anwendungsprofilen](#).
- f Erstellen Sie ein neues Anwendungsprofil mit den folgenden Parametern:
  - Wählen Sie unter „Typ“ in der Liste den Eintrag **HTTPS** aus.
  - Aktivieren Sie das Kontrollkästchen **Pool Side SSL aktivieren (Enable Pool Side SSL)**.
  - Aktivieren Sie das Kontrollkästchen **Dienstzertifikate konfigurieren (Configure Service Certificates)**.
  - Wählen Sie das in Schritt 1 konfigurierte Serverzertifikat aus.

## 3 Erstellen Sie einen virtuellen Server.

- a Melden Sie sich beim vSphere Web Client an.
- b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- c Doppelklicken Sie auf eine NSX Edge-Instanz.
- d Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Load Balancer**.
- e Klicken Sie im linken Navigationsfenster auf **Virtuelle Server (Virtual Servers)**. Weitere Informationen finden Sie unter [Verwalten von virtuellen Servern](#).
- f Erstellen Sie einen neuen virtuellen Server mit den folgenden Parametern:
  - Aktivieren Sie das Kontrollkästchen **Virtuellen Server aktivieren (Enable Virtual Server)**, um den virtuellen Server für die Verwendung zur Verfügung zu stellen.
  - Wählen Sie unter „Protokoll“ die Option **HTTPS** aus.
  - Wählen Sie den Standardpool aus, der sich aus HTTPS-Servern zusammensetzt.
  - Wählen Sie das in Schritt 2 konfigurierte Anwendungsprofil aus.

## Szenario: SSL-Passthrough

Edge beendet keine Client-HTTPS (SSL-Sitzungen). Edge führt einen Lastausgleich der TCP-Sitzungen mit den Servern durch. Client-SSL-Sitzungen werden für die Server beendet (nicht für Edge). L7-Anwendungsregeln können nicht angewendet werden.

## Voraussetzungen

---

**Hinweis** Für das HTTPS-Passthrough-Szenario sind keine Zertifikate erforderlich.

---

## Verfahren

- 1 Erstellen Sie das HTTPS-Anwendungsprofil.
  - a Melden Sie sich beim vSphere Web Client an.
  - b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
  - c Doppelklicken Sie auf eine NSX Edge-Instanz.
  - d Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Load Balancer**.
  - e Klicken Sie im linken Navigationsfenster auf **Anwendungsprofil (Application Profile)**. Weitere Informationen finden Sie unter [Verwalten von Anwendungsprofilen](#).
  - f Erstellen Sie ein neues Anwendungsprofil mit den folgenden Parametern:
    - Wählen Sie unter „Typ“ in der Liste den Eintrag **HTTPS** aus.
    - Aktivieren Sie das Kontrollkästchen **SSL-Passthrough aktivieren (Enable SSL Passthrough)**.
    - Wählen Sie unter „Persistenz“ die Option **Keine (None)** aus.

---

**Hinweis** Für das HTTPS-Passthrough-Szenario sind keine Zertifikate erforderlich.

---

- 2 Erstellen Sie einen virtuellen Server.
  - a Melden Sie sich beim vSphere Web Client an.
  - b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
  - c Doppelklicken Sie auf eine NSX Edge-Instanz.
  - d Klicken Sie auf **Verwalten (Manage)** und anschließend auf die Registerkarte **Load Balancer**.
  - e Klicken Sie im linken Navigationsfenster auf **Virtuelle Server (Virtual Servers)**. Weitere Informationen finden Sie unter [Verwalten von virtuellen Servern](#).
  - f Erstellen Sie einen neuen virtuellen Server mit den folgenden Parametern:
    - Aktivieren Sie das Kontrollkästchen **Virtuellen Server aktivieren (Enable Virtual Server)**, um den virtuellen Server für die Verwendung zur Verfügung zu stellen.
    - Wählen Sie unter „Protokoll“ die Option **HTTPS** aus.
    - Wählen Sie den Standardpool aus, der sich aus HTTPS-Servern zusammensetzt.

- Wählen Sie das in Schritt 1 konfigurierte Anwendungsprofil aus.

---

**Hinweis** Wenn das Kontrollkästchen **Beschleunigung aktivieren (Enable Acceleration)** aktiviert ist und keine L7-bezogenen Konfigurationen vorhanden sind, wird die Sitzung vom Edge NICHT beendet.

Ist das Kontrollkästchen **Beschleunigung aktivieren (Enable Acceleration)** nicht aktiviert, wird die Sitzung als L7-TCP-Modus behandelt und von Edge beendet und in zwei Sitzungen aufgeteilt.

---

## Szenario: SSL-Client- und -Server-Authentifizierung

SSL-Client- und -Server-Authentifizierung.

### Client-Authentifizierung

Clients greifen über HTTPS auf die Webanwendung zu. HTTPS wird am Edge-VIP beendet und fordert ein Client-Zertifikat an.

- 1 Importieren Sie das Webserverzertifikat zusammen mit der Stamm-CA. Einzelheiten dazu finden Sie unter [Szenario: Importieren eines SSL-Zertifikats](#).
- 2 Erstellen Sie das HTTPS-Anwendungsprofil mit den folgenden Parametern:
  - a Wählen Sie unter „Typ“ in der Liste den Eintrag **HTTPS** aus.
  - b Wählen Sie die Registerkarte **Virtuelle Serverzertifikate (Virtual Server Certificates)** aus, und wählen Sie dann die Registerkarte **CA-Zertifikate (CA Certificates)** aus. CA wird zum Überprüfen des Client-Zertifikats verwendet.
  - c Wählen Sie das in Schritt 1 konfigurierte Serverzertifikat aus.
  - d Wählen Sie für die „Client-Authentifizierung“ in der Liste die Einstellung **Erforderlich (Required)** aus.

---

**Hinweis** Wenn die Option **Client-Authentifizierung (Client Authentication)** auf **Ignorieren (Ignore)** festgelegt ist, ignoriert der Lastausgleich die Authentifizierung des Client-Zertifikats.

---

- 3 Erstellen Sie einen virtuellen Server. Einzelheiten dazu finden Sie unter [Szenario: Importieren eines SSL-Zertifikats](#).

---

**Hinweis** Wenn die Option **Pool Side SSL aktivieren (Enable Pool Side SSL)** im Anwendungsprofil deaktiviert ist, setzt sich der ausgewählte Pool aus HTTP-Servern zusammen. Wenn die Option **Pool Side SSL aktivieren (Enable Pool Side SSL)** im Anwendungsprofil aktiviert ist, setzt sich der ausgewählte Pool aus HTTPS-Servern zusammen.

---

- 4 Importieren Sie ein Client-Zertifikat, das von der Stamm-CA signiert ist, in den Browser.
- 5 a Rufen Sie die Website <https://www.sslshopper.com/ssl-converter.html> auf.

- b Konvertieren Sie das Zertifikat und den privaten Schlüssel in die *pfx*-Datei. Vollständige Beispiele für Zertifikate und private Schlüssel finden Sie unter dem Thema [Beispiel: Zertifikat und privater Schlüssel](#).

Certificate File to Convert:  client.crt

Private Key File:  client.key

Chain Certificate File (optional):  Dimi-CA.crt

Chain Certificate File 2 (optional):  No file chosen

Type of Current Certificate:  Detected type from file extension

Type To Convert To:

PFX Password:

- c Importieren Sie die *pfx*-Datei in den Browser.

## Server-Authentifizierung

Clients greifen über HTTPS auf die Webanwendung zu. HTTPS wird am Edge-VIP beendet. Edge stellt neue HTTPS-Verbindungen mit den Servern her. Das Serverzertifikat wird angefordert und überprüft.

Vom Edge werden nur spezifische Verschlüsselungen akzeptiert.

- 1 Importieren Sie das Webserverzertifikat und Stamm-CA-Zertifikat für die Server-Zertifikatauthentifizierung. Einzelheiten dazu finden Sie unter [Szenario: Importieren eines SSL-Zertifikats](#).
- 2 Erstellen Sie das HTTPS-Anwendungsprofil mit den folgenden Parametern:
  - a Wählen Sie unter „Typ“ in der Liste den Eintrag **HTTPS** aus.
  - b Aktivieren Sie das Kontrollkästchen **Pool Side SSL aktivieren (Enable Pool Side SSL)**.
  - c Wählen Sie die Registerkarte **Poolzertifikate (Pool Certificates)** und wählen Sie dann die Registerkarte **CA-Zertifikate (CA Certificates)** aus. CA wird zum Überprüfen des Client-Zertifikats vom HTTPS-Backend-Server verwendet.
  - d Aktivieren Sie das Kontrollkästchen **Server-Authentifizierung (Server Authentication)**.
  - e Wählen Sie das in Schritt 1 konfigurierte CA-Zertifikat aus.
  - f Wählen Sie die erforderliche Verschlüsselung in der Liste **Verschlüsselungen (Ciphers)** aus.

---

**Hinweis** Wenn die Verschlüsselung nicht in der genehmigten Verschlüsselungs-Suite enthalten ist, wird sie auf Standard zurückgesetzt.

Wenn die Verschlüsselung nach einem Upgrade von einer alten Version null/leer oder nicht in der genehmigten Verschlüsselungs-Suite enthalten ist, wird sie auf Standard zurückgesetzt.

---

- 3 Erstellen Sie einen virtuellen Server. Einzelheiten dazu finden Sie unter [Szenario: Importieren eines SSL-Zertifikats](#).

---

**Hinweis** Wenn die Option **Pool Side SSL aktivieren (Enable Pool Side SSL)** im Anwendungsprofil deaktiviert ist, setzt sich der ausgewählte Pool aus HTTP-Servern zusammen. Wenn die Option **Pool Side SSL aktivieren (Enable Pool Side SSL)** im Anwendungsprofil aktiviert ist, setzt sich der ausgewählte Pool aus HTTPS-Servern zusammen.

---

Ein NSX Services Gateway bietet IP-Adresspools und die 1:1-Zuordnung statischer IP-Adressen und eine externe DNS-Server-Konfiguration.

Sie müssen über eine funktionierende NSX Edge-Instanz verfügen, bevor Sie einen der obigen Dienste verwenden können. Weitere Informationen zur Einrichtung von NSX Edge finden Sie unter [Konfiguration von NSX Edge](#).

Dieses Kapitel enthält die folgenden Themen:

- [Verwalten des DHCP-Diensts](#)
- [Konfigurieren des DHCP-Relays](#)
- [Konfigurieren eines DNS-Servers](#)

## Verwalten des DHCP-Diensts

NSX Edge unterstützt IP-Adresspools und die 1:1-Zuordnung statischer IP-Adressen. Die Bindung statischer IP-Adressen basiert auf der von vCenter verwalteten Objekt- und Schnittstellen-ID des anfordernden Clients.

Der NSX Edge-DHCP-Dienst beachtet folgende Richtlinien:

- Die interne NSX Edge-Schnittstelle wird für die DHCP-Suche überwacht.
- Die IP-Adresse der internen NSX Edge-Schnittstelle wird als standardmäßige Gateway-Adresse für alle Clients verwendet (mit Ausnahme nicht direkt verbundener Pools), und die Broadcast- und Subnetzmaskenwerte der internen Schnittstelle werden für das Containernetzwerk verwendet.

In folgenden Fällen müssen Sie den DHCP-Dienst auf virtuellen Client-Maschinen neu starten:

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

## Hinzufügen eines DHCP-IP-Pools

Der DHCP-Dienst benötigt einen Pool von IP-Adressen.

Ein IP-Pool ist ein sequenzieller Bereich von IP-Adressen innerhalb des Netzwerks. Virtuellen Maschinen, die von NSX Edge geschützt werden und keiner Adresse zugeordnet sind, wird eine IP-Adresse aus diesem Pool zugewiesen. Die IP-Pool-Bereiche dürfen sich nicht überschneiden, d. h., eine IP-Adresse darf nur einem IP-Pool angehören.

## Verfahren


- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf **DHCP**.
- 5 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 6 Konfigurieren Sie auf der Registerkarte „Allgemein“ den Pool.

Option	Aktion
<b>DNS automatisch konfigurieren (Auto Configure DNS)</b>	Wählen Sie diese Option aus, wenn Sie die DNS-Dienst-Konfiguration für die DHCP-Bindung verwenden möchten.
<b>Lease läuft nie ab (Lease never expires)</b>	Wählen Sie diese Option aus, um die Adresse dauerhaft an die MAC-Adresse der virtuellen Maschine zu binden. Wenn Sie diese Option auswählen, wird die Option <b>Lease-Dauer (Lease Time)</b> deaktiviert.
<b>Start-IP (Start IP)</b>	Geben Sie die IP-Startadresse für den Pool ein.
<b>End-IP (End IP)</b>	Geben Sie die IP-Endadresse für den Pool ein.
<b>Domänenname (Domain Name)</b>	Geben Sie den Domännennamen des DNS-Servers ein. Die Auswahl dieser Option ist optional.
<b>Primärer Namensserver (Primary Name Server)</b>	Wenn Sie die Option <b>DNS automatisch konfigurieren (Auto Configure DNS)</b> nicht aktiviert haben, geben Sie den <b>Primären Namensserver (Primary Nameserver)</b> für den DNS-Dienst ein. Sie müssen die IP-Adresse eines DNS-Servers für die Auflösung von Hostnamen in IP-Adressen eingeben. Die Auswahl dieser Option ist optional.
<b>Sekundärer Namensserver (Secondary Name Server)</b>	Wenn Sie die Option <b>DNS automatisch konfigurieren (Auto Configure DNS)</b> nicht aktiviert haben, geben Sie den <b>Sekundären Namensserver (Secondary Nameserver)</b> für den DNS-Dienst ein. Sie müssen die IP-Adresse eines DNS-Servers für die Auflösung von Hostnamen in IP-Adressen eingeben. Die Auswahl dieser Option ist optional.
<b>Standard-Gateway (Default Gateway)</b>	Geben Sie die Adresse des Standard-Gateways ein. Falls Sie die IP-Adresse des Standard-Gateways nicht angeben, wird die interne Schnittstelle der NSX Edge-Instanz als Standard-Gateway verwendet. Die Auswahl dieser Option ist optional.

Option	Aktion
<b>Subnetzmaske (Subnet Mask)</b>	Geben Sie die Subnetzmaske an. Die Subnetzmaske muss mit der Subnetzmaske der Edge-Schnittstelle bzw. im Falle eines verteilten Routers mit der Subnetzmaske des DHCP-Relays identisch sein.
<b>Lease-Dauer (Lease Time)</b>	Legen Sie fest, ob Sie die Adresse für den standardmäßigen Zeitraum (1 Tag) für den Client leasen möchten, oder geben Sie für den Zeitraum einen Wert in Sekunden an. Die Option „Lease-Dauer“ steht nicht zur Verfügung, wenn Sie <b>Lease läuft nie ab (Lease never expires)</b> ausgewählt haben. Die Auswahl dieser Option ist optional.

## 7 (Optional) Konfigurieren Sie auf der Registerkarte „DHCP-Optionen“ die DHCP-Optionen.

Wenn bei NSX 6.2.5 oder höher ein DHCP-Pool auf einem Edge Services Gateway sowohl mit klassenlosen statischen Routen als auch mit einem Standard-Gateway konfiguriert wird, wird das Standard-Gateway als klassenlose statische Route hinzugefügt.

Option	Aktion
<b>Nächster Server (Next Server)</b>	Nächster Boot-TFTP-Server, der von PXE boot oder bootp verwendet wird
<b>TFTP-Servername (Option 66) (TFTP server name (option 66))</b>	Geben Sie eine Unicast-IPv4-Adresse oder einen Hostnamen ein, die bzw. den das Gerät verwenden soll, um die Datei herunterzuladen, die im Namen der Startdatei (Option 67) angegeben ist.
<b>TFTP-Serveradresse (Option 150) (TFTP server address (option 150))</b>	Geben Sie mindestens eine TFTP-Server-IPv4-Adresse ein.
<b>Name der Startdatei (Option 67) (Bootfile name (option 67))</b>	Geben Sie den Namen der Startdatei ein, die vom Server heruntergeladen werden soll, der im TFTP-Servernamen (Option 66) angegeben ist.
<b>Schnittstellen-MTU (Option 26) (Interface MTU (option 26))</b>	Die maximale Übertragungseinheit (Maximum Transmission Unit; MTU) ist die maximale Framegröße, die zwischen zwei Hosts ohne Fragmentierung gesendet werden kann. Diese Option bestimmt die MTU-Größe, die auf der Schnittstelle verwendet werden soll. Für jeden Pool und jede statische Bindung kann eine MTU-Größe (in Byte) festgelegt werden. Der minimale MTU-Wert ist 68 Byte und der Maximalwert ist 65.535 Byte. Wenn der Schnittstellen-MTU-Wert nicht auf dem DHCP-Server festgelegt ist, behalten DHCP-Clients die Standard-Betriebseinstellung der Schnittstellen-MTU bei.
<b>Klassenlose statische Route (Option 121) (Classless static route (option 121))</b>	Jede klassenlose statische Routenoption hat möglicherweise mehrere Routen mit demselben Ziel. Jede Route enthält ein Zielsubnetz, eine Subnetzmaske und einen Router für den nächsten Hop. Beachten Sie, dass 0.0.0.0/0 ein ungültiges Subnetz für eine statische Route ist. Informationen zu klassenlosen statischen Routen und Option 121 finden Sie in RFC 3442. <ul style="list-style-type: none"> <li>a Klicken Sie auf das Symbol <b>Hinzufügen (Add)</b> (  ).</li> <li>b Geben Sie das Ziel und die IP-Adresse des Routers für den nächsten Hop ein.</li> </ul>

## 8 Klicken Sie auf **OK**.

## Aktivieren des DHCP-Diensts

Aktivieren Sie den DHCP-Dienst, damit NSX Edge einer virtuellen Maschine automatisch eine IP-Adresse aus einem definierten IP-Pool zuweisen kann.

## Voraussetzungen

Ein DHCP-IP-Pool muss hinzugefügt worden sein.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **DHCP**.
- 5 Klicken Sie auf **Aktivieren (Enable)**.
- 6 Wählen Sie **Protokollierung aktivieren (Enable logging)** (falls erforderlich) und die Protokollierungsebene aus.
- 7 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Ergebnisse

---

**Hinweis** VMware empfiehlt dringend die Erstellung einer Firewallregel, um zu verhindern, dass Benutzer mit boshaften Absichten nicht autorisierte DHCP-Server erstellen. Fügen Sie dazu eine Firewallregel hinzu, die den UDP-Datenverkehr nur an den Ports 67 und 68 zulässt, wenn der Datenverkehr zu einer gültigen IP-Adresse eines DHCP-Servers läuft oder davon stammt. Einzelheiten dazu finden Sie unter [Arbeiten mit Firewallregeln](#).

---

## Nächste Schritte

Erstellen Sie einen IP-Pool und Bindungen.

## Bearbeiten eines DHCP-IP-Pools

Sie können den DHCP-IP-Pool bearbeiten und IP-Adressen hinzufügen oder daraus entfernen.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **DHCP**.
- 5 Wählen Sie einen DHCP-Pool aus und klicken Sie auf das Symbol **Bearbeiten (Edit)**.
- 6 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.

## Hinzufügen einer statischen DHCP-Bindung

Wenn auf einer virtuellen Maschine Dienste ausgeführt werden und Sie nicht möchten, dass die IP-Adresse geändert wird, können Sie eine IP-Adresse an die MAC-Adresse einer virtuellen Maschine binden. Die IP-Adresse, die Sie binden, darf keinen IP-Pool überlappen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **DHCP**.
- 5 Wählen Sie im linken Fensterbereich **Bindungen (Bindings)** aus.
- 6 Klicken Sie auf das Symbol **Hinzufügen (Add)** (+).
- 7 Konfigurieren Sie die Bindung.

Option	Aktion
<b>DNS automatisch konfigurieren (Auto Configure DNS)</b>	Wählen Sie diese Option aus, wenn Sie die DNS-Dienst-Konfiguration für die DHCP-Bindung verwenden möchten.
<b>Lease läuft nie ab (Lease never expires)</b>	Wählen Sie diese Option aus, um die Adresse dauerhaft an die MAC-Adresse der virtuellen Maschine zu binden.
<b>Schnittstelle (Interface)</b>	Wählen Sie die zu bindende NSX Edge-Schnittstelle aus.
<b>VM-Name (VM Name)</b>	Wählen Sie die zu bindende virtuelle Maschine aus.
<b>VM-vNIC-Index (VM vNIC Index)</b>	Wählen Sie die Netzwerkkarte der virtuellen Maschine aus, die an die IP-Adresse gebunden werden soll.
<b>Hostname (Host Name)</b>	Geben Sie den Hostnamen der virtuellen DHCP-Clientmaschine ein.
<b>IP-Adresse (IP Address)</b>	Geben Sie die Adresse ein, an die Sie die MAC-Adresse der ausgewählten virtuellen Maschine binden möchten.
<b>Subnetzmaske (Subnet Mask)</b>	Geben Sie die Subnetzmaske an. Die Subnetzmaske sollte mit der Subnetzmaske der Edge-Schnittstelle bzw. im Falle eines verteilten Routers mit der Subnetzmaske des DHCP-Relays identisch sein.
<b>Domänenname (Domain Name)</b>	Geben Sie den Domännennamen des DNS-Servers ein.
<b>Primärer Namensserver (Primary Name Server)</b>	Wenn Sie die Option <b>DNS automatisch konfigurieren (Auto Configure DNS)</b> nicht aktiviert haben, geben Sie den <b>Primären Namensserver (Primary Nameserver)</b> für den DNS-Dienst ein. Sie müssen die IP-Adresse eines DNS-Servers für die Auflösung von Hostnamen in IP-Adressen eingeben.
<b>Sekundärer Namensserver (Secondary Name Server)</b>	Wenn Sie die Option <b>DNS automatisch konfigurieren (Auto Configure DNS)</b> nicht aktiviert haben, geben Sie den <b>Sekundären Namensserver (Secondary Nameserver)</b> für den DNS-Dienst ein. Sie müssen die IP-Adresse eines DNS-Servers für die Auflösung von Hostnamen in IP-Adressen eingeben.

Option	Aktion
<b>Standard-Gateway (Default Gateway)</b>	Geben Sie die Adresse des Standard-Gateways ein. Falls Sie die IP-Adresse des Standard-Gateways nicht angeben, wird die interne Schnittstelle der NSX Edge-Instanz als Standard-Gateway verwendet.
<b>Lease-Dauer (Lease Time)</b>	Falls Sie <b>Lease läuft nie ab (Lease never expires)</b> nicht ausgewählt haben, geben Sie an, ob Sie die Adresse für den standardmäßigen Zeitraum (1 Tag) für den Client leasen möchten, oder geben Sie für den Zeitraum einen Wert in Sekunden an.

- 8 Klicken Sie auf **Hinzufügen (Add)**.
- 9 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Bearbeiten der DHCP-Bindung

Sie können eine andere statische IP-Adresse zuweisen, die an eine MAC-Adresse einer virtuellen Maschine gebunden ist.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **DHCP**.
- 5 Wählen Sie im linken Fensterbereich **Bindungen (Bindings)** aus und klicken Sie auf die zu bearbeitende Bindung.
- 6 Klicken Sie auf das Symbol „Bearbeiten“.
- 7 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.

## Konfigurieren des DHCP-Relays

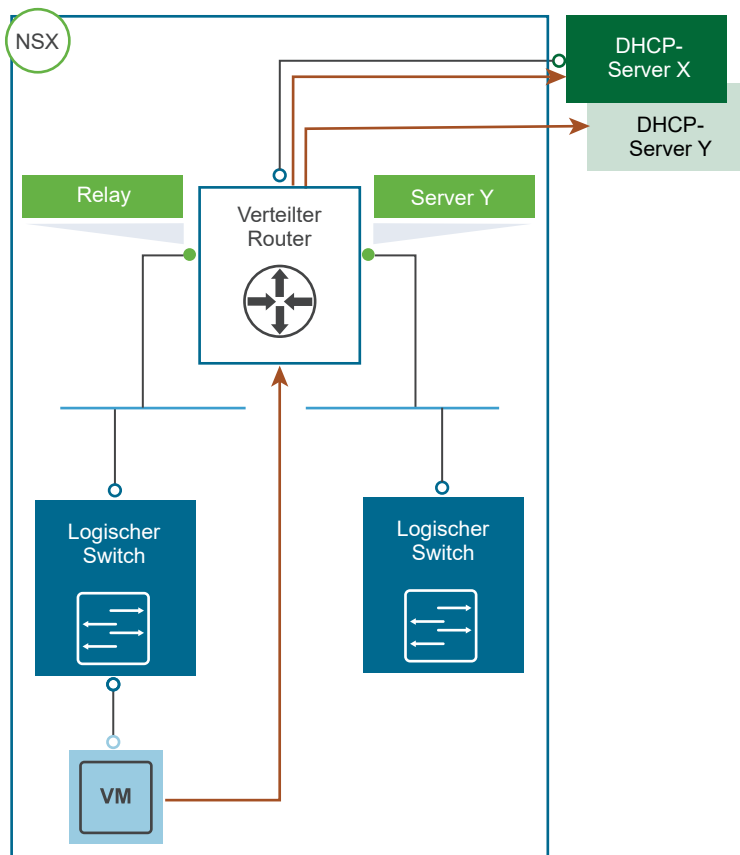
DHCP- (Dynamic Host Configuration Protocol) Relay ermöglicht den Einsatz Ihrer vorhandenen DHCP-Infrastruktur von NSX aus, ohne die Verwaltung der IP-Adressen in Ihrer Umgebung zu beeinträchtigen. DHCP-Mitteilungen werden von virtuellen Maschinen zu dedizierten DHCP-Servern in der physischen Welt gesendet. Dadurch bleiben die IP-Adressen innerhalb von NSX weiterhin mit den IP-Adressen in den anderen Umgebungen synchronisiert.

DHCP-Konfiguration wird auf den logischen Routerport angewandt und kann mehrere DHCP-Server enthalten. Die Anforderungen werden an alle gelisteten Server gesendet. Während der Übertragung der DHCP-Anforderung vom Client fügt das Relay der Anforderung eine Gateway-IP-Adresse hinzu. Der externe DHCP-Server nutzt diese Gateway-Adresse, um eine Übereinstimmung mit einem Pool und zu finden und eine IP-Adresse für die Anforderung zuzuteilen. Die Gateway-Adresse muss zu einem Subnetz des NSX-Ports gehören, auf dem das Relay läuft.

Sie können für jeden logischen Switch einen anderen DHCP-Server angeben und mehrere DHCP-Server auf jedem logischen Router konfigurieren, um Support für mehrere IP-Domänen bereitzustellen.

**Hinweis** Wenn das DHCP-Angebot eine IP-Adresse enthält, die nicht mit einer logischen Schnittstelle (LIF) übereinstimmt, wird es von DLR nicht wieder an die VM zurückgeleitet. Das Paket wird verworfen.

Stellen Sie bei der Konfiguration des Pools und der Bindungen am DHCP-Server sicher, dass die Teilnetzmaske des Pools/der Bindungen für die weitergeleiteten Anfragen identisch mit der Schnittstelle des DHCP-Relays ist. Informationen zur Subnetzmaske müssen in der API zur Verfügung gestellt werden, während DLR als DHCP-Relay zwischen virtuellen Maschinen und dem Edge fungiert, das den DHCP-Dienst bereitstellt. Diese Subnetzmaske muss mit der Maske identisch sein, die auf der Gateway-Schnittstelle für virtuelle Maschinen auf DLR konfiguriert ist.



## Hinweis

- Das DHCP-Relay unterstützt keine überlappenden IP-Adressbereiche (Option 82).
- DHCP-Relay und DHCP-Dienst können nicht gleichzeitig auf einem Port/vNIC laufen. Wird ein Relay-Agent auf einem Port konfiguriert, dann kann auf dem Subnetz dieses Ports kein DHCP-Pool konfiguriert werden.


## Hinzufügen eines DHCP-Relay-Servers

Fügen Sie den bzw. die externen Relay-Server hinzu, an die die DHCP-Nachrichten vermittelt werden sollen. Der Relay-Server kann ein IP Set, ein IP-Adressenblock, eine Domäne oder eine Kombination aus allen sein. Nachrichten werden an jeden aufgeführten DHCP-Server vermittelt.

### Voraussetzungen

- Das DHCP-Relay unterstützt keine überlappenden IP-Adressbereiche (Option 82).
- DHCP-Relay und DHCP-Dienst können nicht gleichzeitig auf einem Port/vNIC laufen. Wird ein Relay-Agent auf einem Port konfiguriert, dann kann auf dem Subnetz dieses Ports kein DHCP-Pool konfiguriert werden.
- Wenn das DHCP-Angebot eine IP-Adresse enthält, die nicht mit einer logischen Schnittstelle (LIF) übereinstimmt, wird es von DLR nicht wieder an die VM zurückgeleitet. Das Paket wird verworfen.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > NSX Edges**.
- 2 Doppelklicken Sie auf die entsprechende Edge-Instanz und stellen Sie sicher, dass Sie sich auf der Registerkarte **Verwalten (Manage) > DHCP** befinden.
- 3 Klicken Sie neben **Globale Konfiguration des DHCP-Relays (DHCP Relay Global Configuration)** auf **Bearbeiten (Edit)**.
- 4 So fügen Sie ein IP Set als Server hinzu:
  - a Klicken Sie auf das Symbol **Hinzufügen (Add)** und wählen Sie das IP Set.
  - b Verschieben Sie das ausgewählte IP Set in die Liste „Ausgewählte Objekte“, indem Sie auf das Symbol  klicken.
  - c Klicken Sie auf **OK**.
- 5 Um IP-Adressen oder Domännennamen hinzuzufügen, geben Sie die Adresse oder den Namen in die entsprechende Area ein.
- 6 Klicken Sie auf **OK**.

## Hinzufügen von Relay-Agenten

Fügen Sie die Edge-Schnittstellen hinzu, von denen aus DHCP-Nachrichten an den bzw. die externen DHCP-Relay-Server weitergeleitet werden sollen.

### Verfahren

- 1 Klicken Sie in der Area **DHCP-Relay-Agenten (DHCP Relay Agents)** auf das Symbol **Hinzufügen (Add)**.

- 2 Stellen Sie unter **vNIC** sicher, dass eine interne vNIC ausgewählt ist.

Die **Gateway-IP-Adresse (Gateway IP Address)** zeigt die primäre IP-Adresse der ausgewählten vNIC an.

- 3 Klicken Sie auf **OK**.

## Konfigurieren eines DNS-Servers

Sie können externe DNS-Server auf einem NSX Edge konfigurieren. Das Edge leitet DNS-Anforderungen von Clientanwendungen an die DNS-Server zur Auflösung eines Netzwerknamens weiter. Das Edge kann auch die Antwort zwischenspeichern, die von den DNS-Servern eingeht. Der DNS-Dienst wird auf einem Edge Services Gateway, DLR und UDLR in einer Cross-vCenter NSX-Umgebung unterstützt.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und anschließend auf **NSX Edges**.
- 3 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**.
- 5 Klicken Sie im Bereich **DNS-Konfiguration (DNS Configuration)** auf **Ändern (Change)**.
- 6 Klicken Sie auf **DNS-Dienst aktivieren (Enable DNS Service)**, um den DNS-Dienst zu aktivieren.
- 7 Geben Sie IP-Adressen für beide DNS-Server ein.
- 8 Ändern Sie bei Bedarf die Cachegröße.
- 9 Klicken Sie auf **Protokollierung aktivieren (Enable Logging)**, um DNS-Datenverkehr zu protokollieren und die Protokollierungsebene auszuwählen.  
Generierte Protokolle werden an den Syslog-Server gesendet.
- 10 Klicken Sie auf **OK**.

Mit Service Composer können Sie Netzwerk- und Sicherheitsdienste für Anwendungen in einer virtuellen Infrastruktur bereitstellen und zuweisen. Sie können diese Dienste einer Sicherheitsgruppe (Security Group) zuweisen. Diese Dienste werden auf die virtuellen Maschinen in der Sicherheitsgruppe angewendet.

## Security Group

Zuerst erstellen Sie eine Sicherheitsgruppe, um die Assets zu definieren, die geschützt werden sollen. Sicherheitsgruppen können statisch (dazu gehören bestimmte virtuelle Maschinen) oder dynamisch sein, wobei die Mitgliedschaft auf eine der folgenden Weisen definiert werden kann:

- vCenter-Container (Cluster, Portgruppen oder Datacenter)
- Sicherheits-Tags, IPset, MACset oder sogar andere Sicherheitsgruppen. Beispielsweise können Sie ein Kriterium hinzufügen, nach dem alle Mitglieder mit einem bestimmten Sicherheits-Tag (wie AntiVirus.virusFound) zu der Sicherheitsgruppe hinzugefügt werden.
- Verzeichnisgruppen (wenn NSX Manager bei Active Directory registriert ist)
- Reguläre Ausdrücke, wie beispielsweise virtuelle Maschinen mit dem Namen *VM1*

Beachten Sie, dass sich die Mitgliedschaft der Sicherheitsgruppe ständig ändert. Beispielsweise wird eine virtuelle Maschine, die mit dem Tag AntiVirus.virusFound versehen ist, in die Sicherheitsgruppe „Quarantäne“ verschoben. Wenn der Virus gelöscht und das Tag aus der virtuellen Maschine entfernt wurde, wird die virtuelle Maschine wieder aus der Sicherheitsgruppe „Quarantäne“ verschoben.

## Sicherheitsrichtlinie

Eine Sicherheitsrichtlinie besteht aus den folgenden Dienstkonfigurationen:

**Tabelle 17-1. In einer Sicherheitsrichtlinie enthaltene Sicherheitsdienste**

Dienst	Beschreibung	Geltungsbereich
Firewallregeln	Diese Regeln legen den Datenverkehr fest, der von, zu oder innerhalb der Sicherheitsgruppe zulässig ist.	vNIC
Endpoint-Dienst	Dienste von Drittanbietern, wie beispielsweise Virenschutz- oder Vulnerability Management-Dienste.	virtuelle Maschinen
Netzwerk-Introspektionsdienste	Diese Dienste überwachen Ihr Netzwerk, wie beispielsweise IPS.	virtuelle Maschinen

Während einer Dienstbereitstellung in NSX wählt der Drittanbieter die Kategorie des bereitgestellten Dienstes aus. Für jede Anbietervorlage wird ein voreingestelltes Dienstprofil erstellt.

Bei der Aktualisierung der Drittanbieter-Dienste auf NSX 6.1 werden voreingestellte Dienstprofile für die aktualisierten Anbietervorlagen erstellt. Vorhandene Dienstrichtlinien, die Regeln für Guest Introspection beinhalten, werden aktualisiert, um auf die während der Aktualisierung erstellten Dienstprofile zu verweisen.

### Zuweisen einer Sicherheitsrichtlinie zu einer Sicherheitsgruppe

Sie können eine Sicherheitsrichtlinie (beispielsweise SP1) zu einer Sicherheitsgruppe (beispielsweise SG1) zuweisen. Die für SP1 konfigurierten Dienste werden auf alle virtuellen Maschinen angewendet, die Mitglieder von SG1 sind.

---

**Hinweis** Angenommen, mehrere Sicherheitsgruppen müssen mit derselben Sicherheitsrichtlinie verknüpft werden. In diesem Fall erstellen Sie eine übergeordnete Sicherheitsgruppe, die alle untergeordneten Sicherheitsgruppen beinhaltet, und wenden Sie die Sicherheitsrichtlinie auf diese übergeordnete Sicherheitsgruppe an. Dadurch wird eine effiziente Nutzung des ESXi Host-Arbeitsspeichers durch die verteilte Firewall von NSX sichergestellt.

---

### Abbildung 17-1. Übersicht über Service Composer



Wenn eine virtuelle Maschine zu mehr als einer Sicherheitsgruppe gehört, dann sind die auf die virtuelle Maschine angewendeten Dienste abhängig vom Vorrang der Sicherheitsrichtlinie, die den Sicherheitsgruppen zugewiesen ist.

Die Service Composer-Profile können als Sicherungen oder zur Verwendung in anderen Umgebungen exportiert und importiert werden. Diese Methode zum Verwalten von Netzwerk- und Sicherheitsdiensten bietet Ihnen eine detaillierte und reproduzierbare Verwaltung von Sicherheitsrichtlinien.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden des Service Composer](#)
- [Service Composer-Arbeitsfläche](#)
- [Arbeiten mit Sicherheits-Tags](#)

- [Anzeigen von aktiven Diensten](#)
- [Arbeiten mit Sicherheitsrichtlinien](#)
- [Service Composer-Szenarien](#)
- [Importieren und Exportieren von Konfigurationen für Sicherheitsrichtlinien](#)

## Verwenden des Service Composer

Service Composer unterstützt Sie bei der einfachen Nutzung von Sicherheitsdiensten.

Das folgende Beispiel zeigt, wie Sie mithilfe von Service Composer Ihr Netzwerk umfassend schützen können. Angenommen, Sie haben die folgenden Sicherheitsrichtlinien für Ihre Umgebung definiert:

- Eine Sicherheitsrichtlinie für den Originalzustand, die einen Dienst zum Suchen nach Schwachstellen umfasst (InitStatePolicy)
- Eine Sicherheitsrichtlinie für die Wartung, die einen Dienst für die Verhinderung von Eindringversuchen in das Netzwerk, Firewallregeln und einen Antivirus-Dienst umfasst (RemPolicy)

Stellen Sie sicher, dass RemPolicy eine höhere Gewichtung (Vorrang) hat als InitStatePolicy.

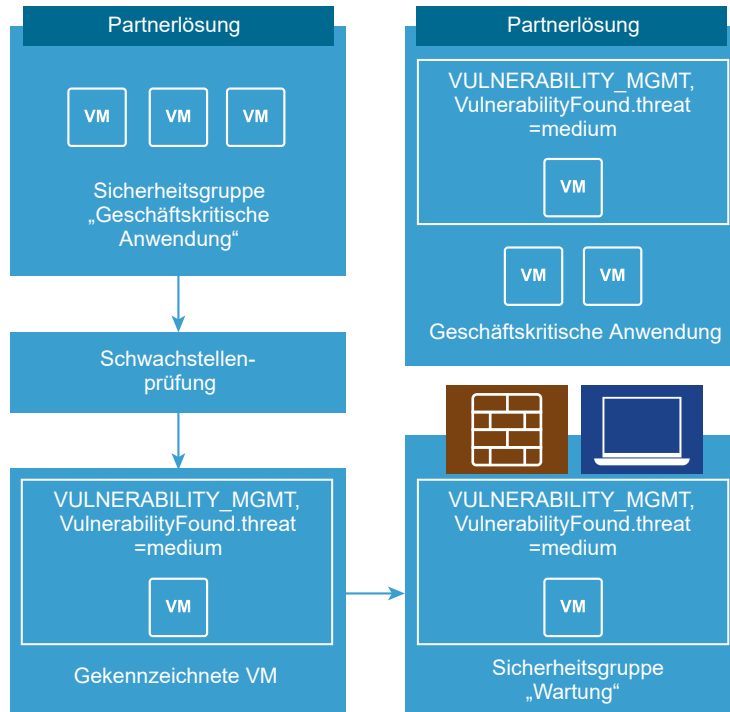
Außerdem sind die folgenden Sicherheitsgruppen vorhanden:

- Eine Gruppe mit Anwendungs-Assets, die die geschäftskritischen Anwendungen Ihrer Umgebung enthält (AssetGroup)
- Eine Sicherheitsgruppe für die Wartung, die von einem Tag definiert wird, das darauf hinweist, dass die virtuelle Maschine anfällig ist (`VULNERABILITY_MGMT.VulnerabilityFound.threat=medium`) (RemGroup)

Nun ordnen Sie die InitStatePolicy-Richtlinie der AssetGroup-Gruppe zu, um alle geschäftskritischen Anwendungen in Ihrer Umgebung zu schützen. Außerdem ordnen Sie die RemPolicy-Richtlinie der RemGroup-Gruppe zu, um anfällige virtuelle Maschinen zu schützen.

Wenn Sie eine Suche nach Schwachstellen einleiten, werden alle virtuellen Maschinen in der AssetGroup-Gruppe überprüft. Wenn die Prüfung eine virtuelle Maschine mit einer Schwachstelle identifiziert, wird das Tag `VULNERABILITY_MGMT.VulnerabilityFound.threat=medium` auf die virtuelle Maschine angewendet.

Service Composer fügt diese gekennzeichnete virtuelle Maschine sofort der RemGroup-Gruppe hinzu, die bereits eine Lösung für die Verhinderung von Eindringversuchen in das Netzwerk vorsieht. So wird diese anfällige virtuelle Maschine geschützt.

**Abbildung 17-2. Funktionsweise von Service Composer**

In diesem Thema werden nun die Schritte zur Nutzung der von Service Composer angebotenen Sicherheitsdienste beschrieben.

## Verfahren

### 1 Erstellen einer Sicherheitsgruppe in Service Composer

Sie erstellen eine Sicherheitsgruppe (Security Group) auf der NSX Manager-Ebene.

### 2 Erstellen einer Sicherheitsrichtlinie

Eine Sicherheitsrichtlinie ist ein Satz von Guest Introspection-, Firewall- und Netzwerk-Introspektionsdiensten, die auf eine Sicherheitsgruppe angewendet werden können. Die Anzeigereihenfolge der Sicherheitsrichtlinien richtet sich nach ihrer Gewichtung. Standardmäßig wird einer neuen Richtlinie die höchste Gewichtung zugewiesen, sodass die Richtlinie sich ganz oben in der Tabelle befindet. Sie können die standardmäßig zugewiesene Gewichtung jedoch ändern und so die Reihenfolge der neuen Richtlinie ändern.

### 3 Anwenden einer Sicherheitsrichtlinie auf eine Sicherheitsgruppe

Sie können eine Sicherheitsrichtlinie auf eine Sicherheitsgruppe (Security Group) anwenden, um Ihre virtuellen Desktops, geschäftskritischen Anwendungen und die Verbindungen dazwischen zu sichern. Außerdem können Sie eine Liste der Dienste anzeigen, die nicht angewendet wurden. Dabei wird auch der jeweilige Grund angezeigt.

## Erstellen einer Sicherheitsgruppe in Service Composer

Sie erstellen eine Sicherheitsgruppe (Security Group) auf der NSX Manager-Ebene.

### Verfahren

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Security Groups** und anschließend auf das Symbol **Security Group hinzufügen (Add Security Group)**.
- 4 Geben Sie einen Namen und eine Beschreibung für die Sicherheitsgruppe (Security Group) ein und klicken Sie auf **Weiter (Next)**.
- 5 Definieren Sie auf der Seite „Dynamische Mitgliedschaft“ die Kriterien, die ein Objekt erfüllen muss, bevor es zur von Ihnen erstellten Sicherheitsgruppe hinzugefügt werden kann.

Beispielsweise können Sie ein Kriterium hinzufügen, nach dem alle Mitglieder mit einem bestimmten Sicherheits-Tag (wie AntiVirus.virusFound) zu der Sicherheitsgruppe hinzugefügt werden.

Sie können aber auch alle virtuellen Maschinen zur Sicherheitsgruppe hinzufügen, die den Namen W2008 enthalten, SOWIE virtuelle Maschinen, die sich im logischen Switch global\_wire befinden.

Bei Sicherheits-Tags wird die Groß- und Kleinschreibung berücksichtigt.

---

**Hinweis** Wenn Sie eine Sicherheitsgruppe für virtuelle Maschinen definieren, auf die ein bestimmtes Sicherheits-Tag angewendet wird, können Sie einen dynamischen oder bedingten Workflow erstellen. In dem Moment, in dem das Tag auf eine virtuelle Maschine angewendet wird, wird die virtuelle Maschine automatisch zu dieser Sicherheitsgruppe hinzugefügt.

---

- 6 Klicken Sie auf **Weiter (Next)**.
- 7 Wählen Sie auf der Seite „Einzubeziehende Objekte auswählen“ den Objekttyp aus dem Dropdown-Menü aus.
- 8 Doppelklicken Sie auf das Objekt, das Sie zur Einschlussliste hinzufügen möchten. Sie können die folgenden Objekte zu einer Sicherheitsgruppe hinzufügen:
  - Andere Sicherheitsgruppen, die innerhalb der von Ihnen erstellten Sicherheitsgruppe verschachtelt werden sollen.
  - Cluster
  - Logischer Switch
  - Netzwerk
  - Virtuelle App
  - Datencenter

- IP Set
- AD-Gruppen

---

**Hinweis** Die AD-Konfiguration für NSX-Sicherheitsgruppen unterscheidet sich von der AD-Konfiguration für vSphere SSO. Die AD-Gruppenkonfiguration für NSX ist für Endbenutzer bestimmt, die auf virtuelle Gastmaschinen zugreifen, während vSphere SSO für Administratoren bestimmt ist, die vSphere und NSX verwenden.

---

- MAC Set

---

**Hinweis** Service Composer ermöglicht die Verwendung von Sicherheitsgruppen, die MAC Sets in Richtlinienkonfigurationen enthalten. Allerdings kann Service Composer keine Regeln für diese speziellen MAC Sets erzwingen. Service Composer arbeitet auf Schicht 3 und unterstützt keine Schicht2-Konstrukte.

---

- Sicherheits-Tag
- vNIC
- Virtuelle Maschine
- Ressourcenpool
- Verteilte virtuelle Portgruppe

Die hier ausgewählten Objekte sind immer in der Sicherheitsgruppe eingeschlossen, unabhängig davon, ob die Kriterien für die dynamische Mitgliedschaft erfüllt werden.

Wenn Sie einer Sicherheitsgruppe eine Ressource hinzufügen, werden automatisch auch alle zugewiesenen Ressourcen hinzugefügt. Wenn Sie beispielsweise eine virtuelle Maschine auswählen, wird die zugewiesene vNIC automatisch zur Sicherheitsgruppe hinzugefügt.

- 9 Klicken Sie auf **Weiter (Next)** und doppelklicken Sie auf die Objekte, die Sie aus der Sicherheitsgruppe ausschließen möchten.

Die hier ausgewählten Objekte werden immer aus der Sicherheitsgruppe ausgeschlossen, sogar wenn sie den dynamischen Kriterien entsprechen oder in der Einschlussliste ausgewählt wurden.

- 10 Klicken Sie auf **Beenden (Finish)**.

### Beispiel

Die Mitgliedschaft in einer Sicherheitsgruppe richtet sich nach Folgendem:

{Ergebnis des Ausdrucks (abgeleitet aus [Schritt Schritt 4](#)) + Einschlüsse (angegeben in [Schritt Schritt 7](#)) – Ausschluss (angegeben in [Schritt Schritt 8](#)),

Dies bedeutet, dass Einschlüsselemente zuerst zum Ergebnis des Ausdrucks hinzugefügt werden. Ausschlussobjekte werden dann vom kombinierten Ergebnis subtrahiert.

## Erstellen einer Sicherheitsrichtlinie


Eine Sicherheitsrichtlinie ist ein Satz von Guest Introspection-, Firewall- und Netzwerk-Introspektionsdiensten, die auf eine Sicherheitsgruppe angewendet werden können. Die Anzeigereihenfolge der Sicherheitsrichtlinien richtet sich nach ihrer Gewichtung. Standardmäßig wird einer neuen Richtlinie die höchste Gewichtung zugewiesen, sodass die Richtlinie sich ganz oben in der Tabelle befindet. Sie können die standardmäßig zugewiesene Gewichtung jedoch ändern und so die Reihenfolge der neuen Richtlinie ändern.

### Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Die erforderlichen integrierten VMware-Dienste müssen installiert sein (beispielsweise verteilte Firewall und Guest Introspection).
- Die erforderlichen Partnerdienste müssen bei NSX Manager registriert worden sein.
- Der gewünschte Standardwert für „Angewendet auf“ wurde für Service Composer-Firewallregeln festgelegt. Weitere Informationen dazu finden Sie unter [Bearbeiten der Einstellung „Angewendet auf“ für die Service Composer-Firewall](#).

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)**.
- 4 Klicken Sie auf das Symbol **Sicherheitsrichtlinie erstellen (Create Security Policy)** ().
- 5 Geben Sie im Dialogfeld „Sicherheitsrichtlinie hinzufügen“ einen Namen für die Sicherheitsrichtlinie ein.
- 6 Geben Sie eine Beschreibung für die Sicherheitsrichtlinie ein.

NSX weist der Richtlinie eine Standardgewichtung zu (höchste Gewichtung +1000). Wenn die höchste Gewichtung der vorhandenen Richtlinien beispielsweise 1200 ist, wird der neuen Richtlinie die Gewichtung 2200 zugewiesen.

Sicherheitsrichtlinien werden anhand ihrer Gewichtung angewendet. Richtlinien mit höherer Gewichtung haben Vorrang vor Richtlinien mit niedrigerer Gewichtung.

- 7 Wählen Sie **Sicherheitsrichtlinie von angegebener Richtlinie übernehmen (Inherit security policy from specified policy)**, wenn die neu erstellte Richtlinie Dienste von einer anderen Sicherheitsrichtlinie übernehmen soll. Wählen Sie die übergeordnete Richtlinie aus.

Die neue Richtlinie übernimmt alle Dienste der übergeordneten Richtlinie.

- 8 Klicken Sie auf **Weiter (Next)**.

9 Klicken Sie auf der Seite für Guest Introspection-Dienste auf das Symbol **Guest Introspection-Dienst hinzufügen (Add Guest Introspection Service)** (+).

- a Geben Sie im Dialogfeld „Guest Introspection-Dienst hinzufügen“ einen Namen und eine Beschreibung für den Dienst ein.
- b Geben Sie an, ob Sie den Dienst anwenden oder blockieren möchten.

Wenn Sie eine Sicherheitsrichtlinie übernehmen, können Sie festlegen, dass ein Dienst der übergeordneten Richtlinie blockiert werden soll.

Falls Sie einen Dienst übernehmen möchten, wählen Sie einen Dienst und ein Dienstprofil aus. Falls Sie einen Dienst blockieren möchten, wählen Sie den Dienstyp aus, der blockiert werden soll.

- c Falls Sie sich dafür entschieden haben, einen Dienst zu blockieren, wählen Sie den Dienstyp aus.
- d Falls Sie einen Guest Introspection-Dienst übernehmen möchten, wählen Sie den Dienstnamen aus.

Das voreingestellte Dienstprofil für den ausgewählten Dienst wird angezeigt. Darin finden Sie Informationen zu Dienstfunktionstypen, die von der entsprechenden Anbietervorlage unterstützt werden.

- e Geben Sie unter **Zustand (State)** an, ob der ausgewählte Guest Introspection-Dienst aktiviert oder deaktiviert sein soll.


Sie können Guest Introspection-Dienste als Platzhalter für Dienste hinzufügen, die zu einem späteren Zeitpunkt aktiviert werden sollen. Dies ist besonders nützlich, wenn Dienste bei Bedarf angewendet werden müssen (beispielsweise neue Anwendungen).

- f Geben Sie an, ob der Guest Introspection-Dienst erzwungen werden soll (in diesem Fall kann er nicht außer Kraft gesetzt werden). Falls das ausgewählte Dienstprofil mehrere Dienstfunktionstypen unterstützt, dann ist standardmäßig **Erzwingen (Enforce)** eingestellt. Diese Einstellung kann nicht geändert werden.


Wenn Sie einen Guest Introspection-Dienst in einer Sicherheitsrichtlinie erzwingen, erfordern andere Richtlinien, die diese Sicherheitsrichtlinie übernehmen, dass diese Richtlinie vor den anderen untergeordneten Richtlinien angewendet wird. Wenn dieser Dienst nicht erzwungen wird, würde bei Auswahl der Vererbung die übergeordnete Richtlinie hinzugefügt, nachdem die untergeordneten Richtlinien angewendet wurden.

- g Klicken Sie auf **OK**.

Sie können weitere Guest Introspection-Dienste hinzufügen, indem Sie die oben beschriebenen Schritte ausführen. Die Guest Introspection-Dienste können mithilfe der Symbole oberhalb der Dienstabelle verwaltet werden.

Sie können die Dienste auf dieser Seite exportieren oder kopieren, indem Sie unten rechts auf der Seite „Guest Introspection-Dienste“ auf das Symbol  klicken.

10 Klicken Sie auf **Weiter (Next)**.

11 Klicken Sie auf der Seite „Firewall“ auf das Symbol **Firewallregel hinzufügen (Add Firewall Rule)** ()

Hier definieren Sie die Firewallregeln für die Sicherheitsgruppe(n), auf die diese Sicherheitsrichtlinie angewendet wird.

- a Geben Sie einen Namen und eine Beschreibung für die Firewallregel ein, die Sie hinzufügen.
- b Wählen Sie **Zulassen (Allow)** oder **Blockieren (Block)**, um festzulegen, ob die Regel den Datenverkehr zum ausgewählten Ziel zulassen oder blockieren soll.
- c Wählen Sie die Quelle für die Regel aus. Standardmäßig gilt die Regel für den Datenverkehr, der von den Sicherheitsgruppen stammt, auf die diese Richtlinie angewendet wird. Zum Ändern der Standardquelle klicken Sie auf **Ändern (Change)** und wählen die entsprechenden Sicherheitsgruppen aus.
- d Wählen Sie das Ziel für die Regel aus.

---


**Hinweis** Entweder das Ziel oder die Quelle (oder beide) müssen Sicherheitsgruppen sein, auf die diese Richtlinie angewendet wird.

---

Angenommen, Sie erstellen eine Regel mit der Standardquelle, geben als Ziel „Gehaltsabrechnung“ an und wählen **Ziel ablehnen (Negate Destination)** aus. Dann wenden Sie diese Sicherheitsrichtlinie auf die Sicherheitsgruppe „Technik“ an. Dies würde bewirken, dass „Technik“ auf alles zugreifen kann, mit Ausnahme des Servers „Gehaltsabrechnung“.

- e Wählen Sie die Dienste und/oder Dienstgruppen aus, für die die Regel gilt.
- f Wählen Sie **Aktiviert (Enabled)** oder **Deaktiviert (Disabled)**, um den Status der Regel anzugeben.
- g Klicken Sie auf **Protokoll (Log)**, um die Sitzungen, die unter diese Regel fallen, zu protokollieren. Das Aktivieren der Protokollierung kann die Leistung beeinträchtigen.
- h Klicken Sie auf **OK**.

Sie können weitere Firewallregeln hinzufügen, indem Sie die oben beschriebenen Schritte ausführen. Die Firewallregeln können mithilfe der Symbole oberhalb der Firewalltabelle verwaltet werden.

Sie können die Regeln auf dieser Seite exportieren oder kopieren, indem Sie unten rechts auf der Seite „Firewall“ auf das Symbol  klicken.

Die Firewallregeln, die Sie hier hinzufügen, werden in der Firewalltabelle angezeigt. VMware empfiehlt, die Service Composer-Regeln in der Firewalltabelle nicht zu bearbeiten. Wenn dies zur Fehlerbehebung im Notfall erforderlich ist, müssen Sie die Service Composer-Regeln mit den Firewallregeln neu synchronisieren, indem Sie auf der Registerkarte „Sicherheitsrichtlinien“ im Menü **Aktionen (Synchronize Firewall Rules)** die Option **Firewallregeln synchronisieren (Actions)** auswählen.

**12** Klicken Sie auf **Weiter (Next)**.

Auf der Seite „Netzwerk-Introspektionsdienste“ werden NetX-Dienste angezeigt, die Sie in Ihre virtuelle VMware-Umgebung integriert haben.


**13** Klicken Sie auf das Symbol **Netzwerk-Introspektionsdienst hinzufügen (Add Network Introspection Service)** (.

- a Geben Sie im Dialogfeld „Netzwerk-Introspektionsdienst hinzufügen“ einen Namen und eine Beschreibung für den Dienst ein, den Sie hinzufügen.
- b Geben Sie an, ob der Dienst umgeleitet werden soll oder nicht.
- c Wählen Sie den Dienstnamen und das Dienstprofil aus.
- d Wählen Sie die Quelle und das Ziel aus.
- e Wählen Sie den gewünschten Netzwerkdienst zum Hinzufügen aus.

Je nach ausgewähltem Dienst stehen Ihnen weitere Auswahloptionen zur Verfügung.

- f Wählen Sie aus, ob der Dienst aktiviert oder deaktiviert sein soll.
- g Klicken Sie auf „Protokoll“, um die Sitzungen, die unter diese Regel fallen, zu protokollieren.
- h Klicken Sie auf **OK**.

Sie können weitere Netzwerk-Introspektionsdienste hinzufügen, indem Sie die oben beschriebenen Schritte ausführen. Die Netzwerk-Introspektionsdienste können mithilfe der Symbole oberhalb der Dienstabelle verwaltet werden.

Sie können die Dienste auf dieser Seite exportieren oder kopieren, indem Sie unten rechts auf der Seite „Netzwerk-Introspektionsdienste“ auf das Symbol  klicken.

---

**Hinweis** In den Richtlinien für Service Composer verwendete manuell erstellte Bindungen für die Dienstprofile werden überschrieben.

---

**14** Klicken Sie auf **Beenden (Finish)**.

Die Sicherheitsrichtlinie wird der Richtlinien-tabelle hinzugefügt. Durch Klicken auf den Namen der Richtlinie und Auswahl der entsprechenden Registerkarte können Sie eine Übersicht der der Richtlinie zugeordneten Dienste anzeigen, Dienstfehler anzeigen oder einen Dienst bearbeiten.

**Nächste Schritte**

Weisen Sie die Sicherheitsrichtlinie einer Sicherheitsgruppe zu.

**Bearbeiten der Einstellung „Angewendet auf“ für die Service Composer-Firewall**

Sie können die Einstellung „Angewendet auf“ für alle Firewallregeln, die über Service Composer erstellt wurden, entweder auf die verteilte Firewall oder auf die Sicherheitsgruppen der Richtlinie festlegen. Standardmäßig für „Angewendet auf“ die verteilte Firewall eingestellt.

Wenn für Firewallregeln des Service Composer die Einstellung „Angewendet auf“ auf die verteilte Firewall festgelegt ist, werden die Regeln auf alle Cluster angewendet, auf denen die verteilte Firewall installiert ist. Wenn die Firewallregeln auf die Sicherheitsgruppen der Richtlinie angewendet werden, können Sie die Firewallregeln präziser festlegen, benötigen aber eventuell mehrere Sicherheitsrichtlinien oder Firewallregeln für das gewünschte Ergebnis.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security**, anschließend auf **Service Composer** und dann auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)**.
- 3 Klicken Sie auf **Aktionen (Actions) > Richtlinien-Firewalleinstellungen bearbeiten (Edit Firewall Policy Settings)**. Wählen Sie eine Standardeinstellung für „Angewendet auf“ aus und klicken Sie auf „OK“.

Option	Beschreibung
<b>verteilte Firewall</b>	Die Firewallregeln werden auf alle Cluster angewendet, auf denen die verteilte Firewall installiert ist.
<b>Sicherheitsgruppen der Richtlinie</b>	Die Firewallregeln werden auf alle Sicherheitsgruppen angewendet, für die die Sicherheitsrichtlinie gilt.

Die Standardeinstellung für „Angewendet auf“ kann über die API angezeigt und geändert werden. Weitere Informationen finden Sie unter *Handbuch zu NSX-API*.

## Beispiel: Verhalten von „Angewendet auf“

Im folgenden Beispielszenario wurde als Standardaktion der Firewallregel „Blockieren“ festgelegt. Sie verfügen über zwei Sicherheitsgruppen: web-servers (Webserver) und app-servers (App-Server), die VMs enthalten. Sie erstellen eine Sicherheitsrichtlinie (allow-ssh-from-web), die die im Folgenden aufgeführte Firewallregel enthält und diese auf die App-Server der Sicherheitsgruppe anwendet.

- Name: allow-ssh-from-web
- Quelle: web-servers
- Ziel: Sicherheitsgruppe der Richtlinie
- Dienst: ssh
- Aktion: Zulassen

Wenn die Firewallregel auf die verteilte Firewall angewendet wird, können Sie eine SSH-Verbindung von einer VM in der Sicherheitsgruppe „web-servers“ mit einer VM in der Sicherheitsgruppe „app-servers“ herstellen.


Wenn die Firewallregel auf die Sicherheitsgruppe der Richtlinie angewendet wird, können Sie keine SSH-Verbindung herstellen, da der Datenverkehr zu den App-Servern blockiert ist. Um eine SSH-Verbindung mit den App-Servern zu ermöglichen, müssen Sie eine zusätzliche Sicherheitsrichtlinie erstellen und diese auf die Sicherheitsgruppe „web-servers“ anwenden.

- Name: allow-ssh-to-app
- Quelle: Sicherheitsgruppe der Richtlinie
- Ziel: app-servers
- Dienst: ssh
- Aktion: Zulassen

## Anwenden einer Sicherheitsrichtlinie auf eine Sicherheitsgruppe

Sie können eine Sicherheitsrichtlinie auf eine Sicherheitsgruppe (Security Group) anwenden, um Ihre virtuellen Desktops, geschäftskritischen Anwendungen und die Verbindungen dazwischen zu sichern. Außerdem können Sie eine Liste der Dienste anzeigen, die nicht angewendet wurden. Dabei wird auch der jeweilige Grund angezeigt.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinie (Security Policy)**.
- 4 Wählen Sie eine Sicherheitsrichtlinie aus und klicken Sie auf das Symbol **Sicherheitsrichtlinie anwenden (Apply Security Policy)** ().

- 5 Wählen Sie die Sicherheitsgruppe aus, auf die Sie die Richtlinie anwenden möchten.

Wenn Sie eine Sicherheitsgruppe auswählen, die von virtuellen Maschinen definiert ist, denen ein bestimmtes Sicherheits-Tag zugewiesen ist, können Sie einen dynamischen oder bedingten Workflow erstellen. In dem Moment, in dem das Tag auf eine virtuelle Maschine angewendet wird, wird die virtuelle Maschine automatisch zu dieser Sicherheitsgruppe hinzugefügt.

Die Regeln für Network Introspection und für Endpoint sind mit der Richtlinie verknüpft und gelten nicht für Sicherheitsgruppen mit IPSet- und/oder MacSet-Mitgliedern.

- 6 Klicken Sie auf das Symbol **Vorschau des Dienststatus (Preview Service Status)**, um die Dienste, die nicht auf die ausgewählte Sicherheitsgruppe angewendet werden können, und den Grund für den Fehler anzuzeigen.

Beispielsweise enthält die Sicherheitsgruppe eine virtuelle Maschine, die zu einem Cluster gehört, auf dem einer der Richtliniendienste nicht installiert wurde. Sie müssen diesen Dienst auf dem jeweiligen Cluster installieren, damit die Sicherheitsrichtlinie wie beabsichtigt funktioniert.

- 7 Klicken Sie auf **OK**.

## Service Composer-Arbeitsfläche

Die Registerkarte „Service Composer-Arbeitsfläche“ bietet eine grafische Ansicht, in der alle Sicherheitsgruppen im ausgewählten NSX Manager angezeigt werden. Die Ansicht zeigt auch Einzelheiten wie die Mitglieder der einzelnen Sicherheitsgruppen sowie die jeweils angewendete Sicherheitsrichtlinie.

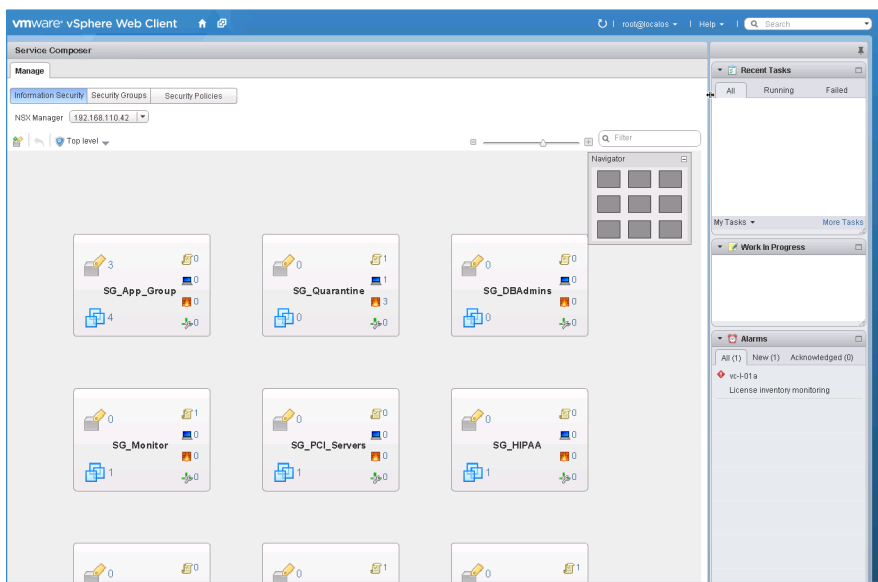
In diesem Thema wird Service Composer mithilfe eines teilweise konfigurierten Systems vorgestellt. Dabei werden die Zuordnungen zwischen Sicherheitsgruppen und Sicherheitsrichtlinienobjekten übersichtlich in der Arbeitsflächen-Ansicht dargestellt.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Arbeitsfläche (Canvas)**.

Alle Sicherheitsgruppen im ausgewählten NSX Manager (die nicht in einer anderen Sicherheitsgruppe enthalten sind) werden zusammen mit den Richtlinien angezeigt, die auf sie angewendet wurden. In der Dropdown-Liste **NSX Manager** werden alle NSX Manager aufgeführt, für die dem derzeit angemeldeten Benutzer eine Rolle zugewiesen ist.

**Abbildung 17-3. Arbeitsflächen-Ansicht auf oberster Ebene von Service Composer**











### Ergebnisse

Jedes Rechteck in der Arbeitsfläche steht für eine Sicherheitsgruppe. Die Symbole innerhalb der Rechtecke zeigen die Mitglieder der Sicherheitsgruppen sowie Einzelheiten zu der Sicherheitsrichtlinie, die der Sicherheitsgruppe zugeordnet ist.

## Abbildung 17-4. Sicherheitsgruppe

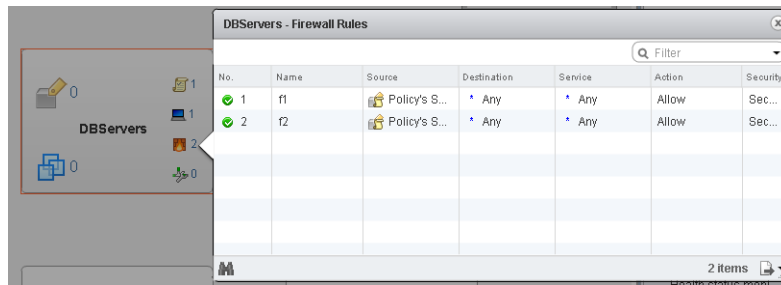


Die Zahlen neben den Symbolen geben die Anzahl der Instanzen an. Beispielsweise bedeutet , dass dieser Sicherheitsgruppe 1 Sicherheitsrichtlinie zugeordnet ist.

Symbol	Durch Klicken auf dieses Symbol wird Folgendes angezeigt
	Sicherheitsgruppen, die in der Hauptsicherheitsgruppe verschachtelt sind
	Virtuelle Maschinen, die derzeit zu der Hauptsicherheitsgruppe sowie zu verschachtelten Sicherheitsgruppen gehören. Klicken Sie auf die Registerkarte „Fehler“, um virtuelle Maschinen mit Dienstfehlern anzuzeigen.
	Aktive Sicherheitsrichtlinien, die der Sicherheitsgruppe zugeordnet sind <ul style="list-style-type: none"> <li>Sie können eine neue Sicherheitsrichtlinie erstellen, indem Sie auf das Symbol <b>Sicherheitsrichtlinie erstellen (Security Policy)</b> () klicken. Das neu erstellte Sicherheitsrichtlinienobjekt wird der Sicherheitsgruppe automatisch zugeordnet.</li> <li>Ordnen Sie zusätzliche Sicherheitsrichtlinien der Sicherheitsgruppe zu, indem Sie auf das Symbol <b>Sicherheitsrichtlinie anwenden (Apply Security Policy)</b> () klicken.</li> </ul>
	Aktive Endpoint-Dienste, die zu der Sicherheitsrichtlinie gehören, die der Sicherheitsgruppe zugeordnet ist. Angenommen, auf eine Sicherheitsgruppe wurden zwei Richtlinien angewendet, für die beide ein Endpoint-Dienst derselben Kategorie konfiguriert ist. In diesem Fall ist der aktive Dienst der Dienst mit der Nummer 1 (er hat Vorrang vor dem zweiten Dienst, der eine niedrigere Priorität hat). Endpoint-Dienstfehler werden, falls vorhanden, durch das Alarmsymbol gekennzeichnet. Durch Klicken auf das Symbol wird der Fehler angezeigt.
	Aktive Firewallregeln, die zu der Sicherheitsrichtlinie gehören, die der Sicherheitsgruppe zugeordnet ist. Eventuell vorliegende Dienstfehler werden durch ein Warnsymbol gekennzeichnet. Durch Klicken auf das Symbol wird der Fehler angezeigt.
	Aktive Netzwerk-Introspektionsdienste, die zu der Sicherheitsrichtlinie gehören, die der Sicherheitsgruppe zugeordnet ist. Eventuell vorliegende Dienstfehler werden durch ein Warnsymbol gekennzeichnet. Durch Klicken auf das Symbol wird der Fehler angezeigt.

Durch Klicken auf ein Symbol wird ein Dialogfeld mit weiteren Einzelheiten angezeigt.

**Abbildung 17-5. Details, die durch Klicken auf ein Symbol in der Sicherheitsgruppe angezeigt werden**



Sie können Sicherheitsgruppen anhand des Namens suchen. Wenn Sie beispielsweise PCI in das Suchfeld oben rechts in der Arbeitsflächen-Ansicht eingeben, werden nur die Sicherheitsgruppen angezeigt, deren Namen die Buchstabenfolge PCI enthält.

Um die Hierarchie der Sicherheitsgruppen anzuzeigen, klicken Sie auf das Symbol **Oberste Ebene (Top Level)** (▼) im oberen linken Bereich des Fensters und wählen Sie die Sicherheitsgruppe, die Sie anzeigen möchten. Wenn eine Sicherheitsgruppe verschachtelte Sicherheitsgruppen enthält, klicken Sie auf ►, um die verschachtelten Gruppen anzuzeigen. Die Leiste ganz oben zeigt den Namen der übergeordneten Sicherheitsgruppe, und die Symbole in der Leiste zeigen die Gesamtanzahl der Sicherheitsrichtlinien, Endpoint-Dienste, Firewalldienste und Netzwerk-Introspektionsdienste, die für die übergeordnete Gruppe gelten. Sie können zurück zur obersten Ebene navigieren, indem Sie auf das

Symbol **Eine Ebene höher (Go up one level)** (↶) im oberen linken Bereich des Fensters klicken.

Sie können die Arbeitsflächen-Ansicht nach Bedarf vergrößern oder verkleinern, indem Sie den Schieberegler in der oberen rechten Ecke des Fensters ziehen. Das Navigator-Feld zeigt eine verkleinerte Ansicht der gesamten Arbeitsfläche. Wenn die Arbeitsfläche wesentlich größer als der verfügbare Platz auf dem Bildschirm ist, wird die derzeit angezeigte Area durch ein Feld gekennzeichnet. Sie können dieses Feld verschieben, um eine andere Area der Arbeitsfläche auf dem Bildschirm anzuzeigen.

### Nächste Schritte

Sie haben nun die Funktionsweise der Zuordnung zwischen Sicherheitsgruppen und Sicherheitsrichtlinien kennengelernt. Nun können Sie Sicherheitsrichtlinien erstellen, um die Sicherheitsdienste zu definieren, die Sie auf Ihre Sicherheitsgruppen anwenden möchten.

## Zuordnen einer Sicherheitsgruppe zu einer Sicherheitsrichtlinie

Sie können die ausgewählte Sicherheitsgruppe (Security Group) einer Sicherheitsrichtlinie zuordnen.

### Verfahren

- 1 Wählen Sie die Sicherheitsrichtlinie aus, die Sie auf die Sicherheitsgruppe anwenden möchten.
- 2 Zum Erstellen einer neuen Richtlinie wählen Sie „Neue Sicherheitsgruppe“ aus.

Weitere Informationen dazu finden Sie unter [Erstellen einer Sicherheitsrichtlinie](#).

- 3 Klicken Sie auf **Speichern (Save)**.

## Arbeiten mit Sicherheits-Tags

Sie können die auf eine virtuelle Maschine angewendeten Sicherheits-Tags anzeigen oder ein benutzerdefiniertes Sicherheits-Tag erstellen.

Sicherheits-Tags sind Beschriftungen, die einer virtuellen Maschine (VM) zugeordnet werden können. Zur Identifizierung einer spezifischen Arbeitslast können zahlreiche Sicherheits-Tags erstellt werden. Bei den Übereinstimmungskriterien einer Sicherheitsgruppe kann es sich um eine Sicherheitsgruppe handeln. Zudem kann eine mit Tags versehene Arbeitslast automatisch in eine Sicherheitsgruppe eingefügt werden.

Das Hinzufügen oder Entfernen von Sicherheits-Tags zu bzw. von einer VM kann bedingt durch verschiedene Kriterien wie Antivirus- oder Schwachstellenprüfungen und Intrusion Prevention-Systemen dynamisch erfolgen. Tags können auch manuell durch einen Administrator hinzugefügt oder entfernt werden.

In einer Cross-vCenter NSX-Umgebung werden auf dem primären NSX Manager universelle Sicherheits-Tags erstellt, die für die globale Synchronisierung mit sekundären NSX Managern markiert werden. Universelle Sicherheits-Tags können VMs statisch und auf Grundlage der eindeutigen ID-Auswahl zugewiesen werden.

## Auswahl einer eindeutigen Kennung

Die Auswahlkriterien für die eindeutige Kennung werden beim Zuweisen von Tags zu virtuellen Maschinen in aktiven Standby-Bereitstellungen verwendet.

Die eindeutige Kennung wird vom NSX Manager verwendet, wenn eine virtuelle Maschine (VM) von der Standby-Bereitstellung in die aktive Bereitstellung wechselt. Die eindeutige Kennung kann auf der VM-Instanz-UUID, der VM-BIOS-UUID, dem VM-Namen oder auf einer Kombination dieser Optionen basieren. Beachten Sie, dass das Sicherheits-Tag gelöst und erneut an die VMs angehängt werden muss, wenn sich nach der Erstellung universeller Sicherheits-Tags und deren Anhängen an VMs die Kriterien ändern (beispielsweise bei einer Änderung des VM-Namens).

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Start > Networking & Security > Installation (Home > Networking & Security > Installation)** und wählen Sie die Registerkarte „Management“ aus.
- 2 Klicken Sie auf den primären NSX Manager. Wählen Sie dann **Aktionen > Auswahlkriterien für eindeutige Kennung (Actions > Unique ID Selection Criteria.)** aus.

### 3 Wählen Sie eine oder mehrere Optionen für die eindeutige Kennung aus:

- Instanz-UUID der virtuellen Maschine verwenden (empfohlen) – Die Instanz-UUID der virtuellen Maschine ist im Allgemeinen in einer VC-Domäne eindeutig. Es gibt jedoch Ausnahmen, beispielsweise, wenn Bereitstellungen über Snapshots generiert werden. Wenn die VM-Instanz-UUID nicht eindeutig ist, wird empfohlen, die VM-BIOS-UUID in Kombination mit dem VM-Namen zu verwenden.
- BIOS-UUID der virtuellen Maschine verwenden – Die BIOS-UUID ist innerhalb einer VC-Domäne nicht zwingend eindeutig. Sie wird für den Notfall jedoch immer beibehalten. Es wird empfohlen, die BIOS-UUID in Kombination mit dem VM-Namen zu verwenden.
- Virtuellen Maschinennamen verwenden – Wenn alle VM-Namen in einer Umgebung eindeutig sind, kann ein VM mithilfe des VM-Namens vCenter-übergreifend identifiziert werden. Es wird empfohlen, den VM-Namen in Kombination mit der VM-BIOS-UUID zu verwenden.

### 4 Klicken Sie auf **OK**.

#### Nächste Schritte

Im nächsten Schritt erstellen Sie Sicherheits-Tags.

## Anzeigen von angewendeten Sicherheits-Tags

Sie können die Sicherheits-Tags anzeigen, die auf virtuelle Maschinen in Ihrer Umgebung angewendet wurden.

#### Voraussetzungen

Eine Antiviren-Prüfung muss durchgeführt und auf die entsprechende virtuelle Maschine muss ein Tag angewendet worden sein.

---

**Hinweis** Einzelheiten zu den Tags, die von Drittanbieterlösungen angewendet werden, finden Sie in der entsprechenden Dokumentation.

---

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf die Registerkarte **Sicherheits-Tags (Security Tags)**.

Daraufhin wird eine Liste der Tags angezeigt, die in Ihrer Umgebung angewendet wurden. Außerdem werden Einzelheiten zu den virtuellen Maschinen angezeigt, auf die diese Tags angewendet wurden. Notieren Sie sich den genauen Tag-Namen, wenn Sie eine Sicherheitsgruppe hinzufügen möchten, die virtuelle Maschinen mit einem bestimmten Tag enthält.

- 5 Klicken Sie auf die Zahl in der Spalte **Anzahl an VMs (VM Count)**, um die virtuellen Maschinen anzuzeigen, auf die das Tag in dieser Reihe angewendet wurde.

## Erstellen eines Sicherheits-Tags

Sie können ein Sicherheits-Tag erstellen und auf eine virtuelle Maschine anwenden. In einer Cross-vCenter-Umgebung werden Sicherheits-Tags zwischen primären und sekundären NSX Managern synchronisiert.

### Voraussetzungen

Wenn Sie ein globales Sicherheits-Tag in einem Szenario einer aktiven Standby-Bereitstellung erstellen, müssen Sie zuerst die Auswahlkriterien für die eindeutige ID auf dem primären NSX Manager festlegen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf die Registerkarte **Sicherheits-Tags (Security Tags)**.
- 5 Klicken Sie auf das Symbol **Neues Sicherheits-Tag (New Security Tag)**.
- 6 (Optional) Wählen Sie zum Erstellen eines globalen Sicherheits-Tags für Cross-vCenter NSX-Umgebungen die Option **Dieses Objekt für globale Synchronisierung markieren (Mark this object for universal synchronization)** aus.
- 7 Geben Sie einen Namen und eine Beschreibung für das neue Tag ein und klicken Sie auf **OK**.

### Nächste Schritte

Weisen Sie dem Sicherheits-Tag virtuelle Maschinen zu.

## Zuweisen eines Sicherheits-Tags

Zusätzlich zum Erstellen eines bedingten Workflows mit einem dynamischen, mitgliedschaftsbasierten Sicherheits-Tag können Sie virtuellen Maschinen manuell ein Sicherheits-Tag zuweisen.

Sicherheits-Tags können als Übereinstimmungskriterien in Sicherheitsgruppen verwendet werden. In einer Cross-vCenter-Umgebung werden Sicherheits-Tags zwischen primären und sekundären NSX Managern synchronisiert.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten (Manage)**.

- 4 Klicken Sie auf die Registerkarte **Sicherheits-Tags (Security Tags)**.
- 5 Klicken Sie mit der rechten Maustaste auf ein Sicherheits-Tag und wählen Sie **Sicherheits-Tag zuweisen (Assign Security Tag)** aus.

Das mit den verfügbaren VMs gefüllte Fenster **Sicherheits-Tag zu virtueller Maschine zuweisen (Assign Security Tag to Virtual Machine)** wird angezeigt.

- 6 Doppelklicken Sie auf eine oder mehrere virtuelle Maschinen, um sie in die Spalte **Ausgewählte Objekte (Selected Objects)** zu verschieben. Klicken Sie auf **OK**.

Die Registerkarte **Sicherheits-Tags (Security Tags)** wird angezeigt. Sie enthält eine aktualisierte VM-Anzahl für das Sicherheits-Tag.

## Bearbeiten eines Sicherheits-Tags

Sie können ein benutzerdefiniertes Sicherheits-Tag bearbeiten. Wenn eine Sicherheitsgruppe auf dem gerade bearbeiteten Tag basiert, haben Änderungen des Tags möglicherweise Auswirkungen auf die Mitgliedschaft der Sicherheitsgruppe.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf die Registerkarte **Sicherheits-Tags (Security Tags)**.
- 5 Klicken Sie mit der rechten Maustaste auf ein Sicherheits-Tag und wählen Sie **Sicherheits-Tag bearbeiten (Edit Security Tag)** aus.
- 6 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.

## Löschen eines Sicherheits-Tags

Sie können ein benutzerdefiniertes Sicherheits-Tag löschen. Wenn eine Sicherheitsgruppe auf dem Tag basiert, das Sie löschen, haben Änderungen des Tags möglicherweise Auswirkungen auf die Mitgliedschaft der Sicherheitsgruppe.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf die Registerkarte **Sicherheits-Tags (Security Tags)**.

- 5 Wählen Sie ein Sicherheits-Tag aus und klicken Sie auf das Symbol **Sicherheits-Tag löschen** (Delete Security Tag) (✖).

## Anzeigen von aktiven Diensten

Sie können die Dienste anzeigen, die auf einem Sicherheitsrichtlinienobjekt oder auf einer virtuellen Maschine gerade aktiv sind.

### Anzeigen von aktiven Diensten zu einer Sicherheitsrichtlinie

Sie können die Dienste anzeigen, die bei einer Sicherheitsrichtlinie aktiv sind. Dies schließt auch Dienste ein, die von einer übergeordneten Richtlinie übernommen werden.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)**.
- 4 Klicken Sie in der Spalte **Name** auf eine Sicherheitsrichtlinie.
- 5 Vergewissern Sie sich, dass Sie sich auf der Registerkarte **Verwalten (Manage) > Informationssicherheit (Information Security)** befinden.

#### Ergebnisse

Auf den drei Registerkarten (**Endpoint-Dienste (Endpoint Services)**, **Firewall**, **Netzwerk-Introspektionsdienste (Network Introspection Services)**) werden jeweils die entsprechenden Dienste für die Sicherheitsrichtlinie angezeigt.

Dienste, die nicht wirksam sind, werden abgeblendet dargestellt. In der Spalte **Außer Kraft gesetzt (Overridden)** werden die Dienste angezeigt, die aktuell auf die Sicherheitsrichtlinie angewendet werden, und in der Spalte **Geerbt von (Inherited from)** wird die Sicherheitsrichtlinie angezeigt, von der die Dienste übernommen werden.

### Anzeigen von Dienstfehlern für eine Sicherheitsrichtlinie

Sie können die einer Sicherheitsrichtlinie zugewiesenen Dienste anzeigen, die nicht auf die Sicherheitsgruppe(n) für die Richtlinie angewendet werden konnten.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)**.
- 4 Klicken Sie in der Spalte **Name** auf eine Sicherheitsrichtlinie.

- 5 Vergewissern Sie sich, dass Sie sich auf der Registerkarte **Überwachen (Monitor) > Dienstfehler (Service Errors)** befinden.

Mit einem Klick auf den Link in der Spalte **Status** gelangen Sie zur Seite „Dienstbereitstellung“, auf der Sie Dienstfehler beheben können.

## Anzeigen von aktiven Diensten auf einer virtuellen Maschine

Sie können die Dienste anzeigen, die auf einer virtuellen Maschine gerade aktiv sind. Wenn mehrere Sicherheitsrichtlinien auf eine virtuelle Maschine angewendet werden (z. B. wenn eine virtuelle Maschine zu mehreren Sicherheitsgruppen mit Richtlinien gehört), dann werden in dieser Ansicht alle aktiven Dienste aus all diesen Richtlinien in der Reihenfolge ihrer Anwendung aufgelistet. In der Spalte „Dienststatus“ wird für jeden Dienst der Status angezeigt.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **vCenter** und anschließend auf **Virtuelle Maschinen (Virtual Machines)**.
- 3 Klicken Sie auf eine virtuelle Maschine in der Spalte **Name**.
- 4 Stellen Sie sicher, dass Sie sich auf der Registerkarte **Überwachen (Monitor) > Service Composer** befinden.

## Arbeiten mit Sicherheitsrichtlinien

Eine Sicherheitsrichtlinie ist eine Gruppe aus Netzwerk- und Sicherheitsdiensten.

Die folgenden Netzwerk- und Sicherheitsdienste können in einer Sicherheitsrichtlinie gruppiert werden:

- Endpoint-Dienste – Virenschutz und Vulnerability Management
- Regeln für die verteilte Firewall
- Netzwerk-Introspektionsdienste – Netzwerk-IPS und Netzwerk-Diagnose




## Verwalten der Sicherheitsrichtlinienpriorität

Sicherheitsrichtlinien werden ihrer Gewichtung entsprechend angewendet – eine Sicherheitsrichtlinie mit höherer Gewichtung hat höhere Priorität. Wenn Sie eine Richtlinie in der Tabelle nach oben oder nach unten verschieben, wird ihre Gewichtung entsprechend angepasst.

Mehrere Sicherheitsrichtlinien können auf eine virtuelle Maschine angewendet werden, entweder weil die Sicherheitsgruppe (Security Group), die die virtuelle Maschine enthält, mit mehreren Richtlinien verknüpft ist, oder weil die virtuelle Maschine zu mehreren Sicherheitsgruppen gehört, die mit verschiedenen Sicherheitsrichtlinien verknüpft sind. Besteht ein Konflikt zwischen den unter den einzelnen Richtlinien gruppierten Diensten, so bestimmt die Gewichtung der Richtlinie darüber, welche Dienste auf die virtuelle

Maschine angewendet werden. Beispiel: Richtlinie 1 blockiert den Internetzugriff und hat einen Gewichtungswert von 1000, während Richtlinie 2 den Internetzugriff zulässt und einen Gewichtungswert von 2000 hat. In diesem speziellen Fall hat Richtlinie 2 eine höhere Gewichtung, sodass der Zugriff der virtuellen Maschine auf das Internet zugelassen wird.


#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)**.
- 4 Klicken Sie auf das Symbol **Vorrang verwalten (Manage Precedence)** ().
- 5 Wählen Sie im Dialogfeld „Vorrang verwalten“ die Sicherheitsrichtlinie aus, für die Sie den Vorrang ändern möchten, und klicken Sie auf das Symbol **Nach oben verschieben (Move Up)** () oder **Nach unten verschieben (Move Down)** ().
- 6 Klicken Sie auf **OK**.

## Bearbeiten einer Sicherheitsrichtlinie

Sie können den Namen oder die Beschreibung einer Sicherheitsrichtlinie sowie die zugehörigen Dienste und Regeln bearbeiten.


#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)**.
- 4 Wählen Sie die Sicherheitsrichtlinie aus, die Sie bearbeiten möchten, und klicken Sie auf das Symbol **Sicherheitsrichtlinie bearbeiten (Edit Security Policy)** ().
- 5 Nehmen Sie im Dialogfeld „Sicherheitsrichtlinie bearbeiten“ die gewünschten Änderungen vor und klicken Sie auf **Beenden (Finish)**.

## Löschen einer Sicherheitsrichtlinie

Sie können eine Sicherheitsrichtlinie löschen.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)**.
- 4 Wählen Sie die Sicherheitsrichtlinie aus, die Sie löschen möchten, und klicken Sie auf das Symbol **Sicherheitsrichtlinie löschen (Delete Security Policy)** ().

## Service Composer-Szenarien

In diesem Abschnitt werden einige theoretische Szenarien für Service Composer veranschaulicht. In jedem Anwendungsfall wird vorausgesetzt, dass die Rolle des Sicherheitsadministrators erstellt und dem Administrator zugewiesen wurde.

### Szenario zum Sperren von infizierten Maschinen

Service Composer kann mithilfe von Antivirusbefehlen von Drittanbietern infizierte Systeme auf Ihrem Netzwerk identifizieren und sperren, um spätere Angriffe zu verhindern.

Unser Beispielszenario zeigt, wie Sie Ihre Desktops vollständig schützen können.

Abbildung 17-6. Konfigurieren des Service Composer

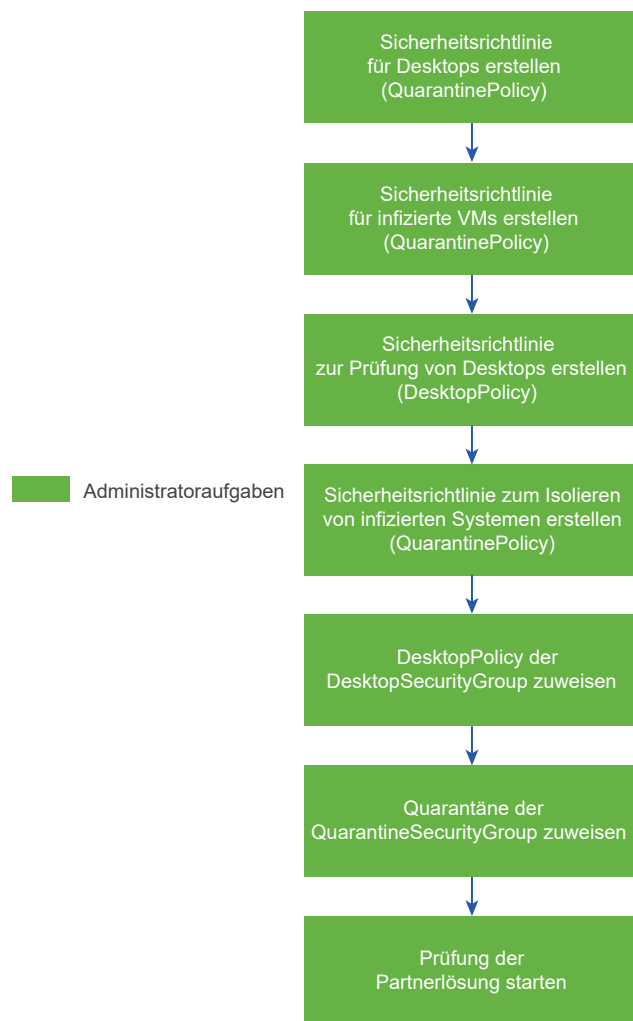
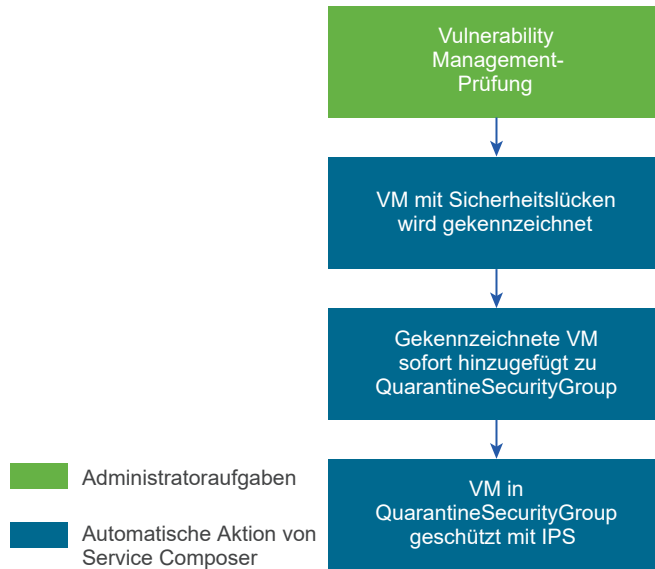


Abbildung 17-7. Bedingter Workflow des Service Composer




### Voraussetzungen

Wir stellen fest, dass Symantec-Tags die virtuelle Maschine mit dem Tag **AntiVirus.virusFound** infiziert haben.


### Verfahren

- 1 Installieren und registrieren Sie die Antimalware-Lösung von Symantec und stellen Sie sie bereit.
- 2 Erstellen Sie eine Sicherheitsrichtlinie für Ihre Desktops.
  - a Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)** und anschließend auf das Symbol **Sicherheitsrichtlinie hinzufügen (Add Security Policy)**.
  - b Geben Sie unter **Name** den Namen **DesktopPolicy** ein.
  - c Geben Sie unter **Beschreibung (Description)** die Beschreibung **Antivirus-Prüfung für alle Desktops** ein.
  - d Ändern Sie den Gewichtungswert auf 51000. Für den Richtlinienvorrang ist ein sehr hoher Wert festgelegt, um sicherzustellen, dass sie gegenüber allen anderen Richtlinien durchgesetzt wird.
  - e Klicken Sie auf **Weiter (Next)**.

- f Klicken Sie auf der Seite „Endpoint-Dienst hinzufügen“ auf  und geben Sie die folgenden Werte ein:

Option	Wert
Aktion (Action)	Standardwert nicht ändern
Diensttyp (Service Type)	Anti Virus
Dienstname (Service Name)	Symantec Antimalware
Dienstkonfiguration (Service Configuration)	Silver
Zustand (State)	Standardwert nicht ändern
Erzwingen (Enforce)	Standardwert nicht ändern
Name	Desktop-AV
Beschreibung (Description)	Obligatorische Richtlinie zur Anwendung auf allen Desktops


- g Klicken Sie auf **OK**.
- h Fügen Sie keine Firewalldienste oder Netzwerk-Introspektionsdienste hinzu. Klicken Sie auf **Beenden (Finish)**.
- 3** Erstellen Sie eine Sicherheitsrichtlinie für infizierte virtuelle Maschinen.
- a Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)** und anschließend auf das Symbol **Sicherheitsrichtlinie hinzufügen (Add Security Policy)**.
- b Geben Sie unter „Name“ den Namen **QuarantinePolicy** ein.
- c Geben Sie unter „Beschreibung“ die Beschreibung **Richtlinie zur Anwendung auf alle infizierten Systeme** ein.
- d Ändern Sie die Standardgewichtung nicht.
- e Klicken Sie auf **Weiter (Next)**.
- f Nehmen Sie auf der Seite „Endpoint-Dienst hinzufügen“ keine Einstellungen vor und klicken Sie auf **Weiter (Next)**.
- g Fügen Sie unter „Firewall“ drei Regeln hinzu: eine Regel zum Blockieren des ausgehenden Datenverkehrs, eine zweite Regel zum Blockieren des gesamten Datenverkehrs mit Gruppen und die letzte Regel zum Zulassen des eingehenden Datenverkehrs nur von Wartungstools.
- h Fügen Sie keine Netzwerk-Introspektionsdienste hinzu und klicken Sie auf **Beenden (Finish)**.
- 4** Verschieben Sie **QuarantinePolicy** nach ganz oben in der Sicherheitsrichtlinientabelle, um sicherzustellen, dass sie gegenüber allen anderen Richtlinien durchgesetzt wird.
- a Klicken Sie auf das Symbol **Priorität verwalten (Manage Priority)**.
- b Wählen Sie **QuarantinePolicy** und klicken Sie auf das Symbol **Nach oben verschieben (Move Up)**.

- 5 Erstellen Sie eine Sicherheitsgruppe für alle Desktops in Ihrer Umgebung.
  - a Melden Sie sich beim vSphere Web Client an.
  - b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und dann auf **Service Composer**.
  - c Klicken Sie auf die Registerkarte **Security Groups** und dann auf das Symbol **Security Group hinzufügen (Add Security Group)**.
  - d Geben Sie unter „Name“ den Namen **DesktopSecurityGroup** ein.
  - e Geben Sie unter „Beschreibung“ die Beschreibung **Alle Desktops** ein.
  - f Klicken Sie auf den nächsten paar Seiten auf **Weiter (Next)**.
  - g Überprüfen Sie Ihre Auswahl auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Beenden (Finish)**.
  
- 6 Erstellen Sie eine Sicherheitsgruppe mit dem Namen „Quarantäne“, in der die infizierten virtuellen Maschinen abgelegt werden.
  - a Klicken Sie auf die Registerkarte **Security Groups** und dann auf das Symbol **Security Group hinzufügen (Add Security Group)**.
  - b Geben Sie unter **Name** den Namen **QuarantineSecurityGroup** ein.
  - c Geben Sie unter **Beschreibung (Description)** die Beschreibung **Dynamische Gruppenmitgliedschaft, die auf durch die Antivirus-Prüfung identifizierten infizierten VMs basiert** ein.
  - d Klicken Sie auf der Seite „Kriterien für Mitgliedschaft definieren“ auf  und fügen Sie das folgende Kriterium hinzu:



- e Nehmen Sie keine Einstellungen auf den Seiten „Einzubeziehende Objekte auswählen“ oder „Auszuschließende Objekte auswählen“ vor und klicken Sie auf **Weiter (Next)**.
- f Überprüfen Sie Ihre Auswahl auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Beenden (Finish)**.

7 Weisen Sie die Richtlinie **DesktopPolicy** der Sicherheitsgruppe **DesktopSecurityGroup** zu.

- a Vergewissern Sie sich, dass auf der Registerkarte „Sicherheitsrichtlinien“ die Richtlinie **DesktopPolicy** ausgewählt ist.
- b Klicken Sie auf das Symbol **Sicherheitsrichtlinie anwenden (Apply Security Policy)** () und wählen Sie die Gruppe SG\_Desktops aus.
- c Klicken Sie auf **OK**.

Durch diese Zuweisung wird sichergestellt, dass alle Desktops (zugehörig zur **DesktopSecurityGroup**) geprüft werden, wenn eine Antivirus-Prüfung gestartet wird.

8 Navigieren Sie zur Arbeitsflächenansicht, um zu überprüfen, dass in **QuarantineSecurityGroup** noch keine virtuellen Maschinen eingeschlossen sind.

- a Klicken Sie auf die Registerkarte **Informationssicherheit (Information Security)**.

- b Stellen Sie sicher, dass in der Gruppe () 0 virtuelle Maschinen enthalten sind.

9 Weisen Sie die **QuarantinePolicy** der **QuarantineSecurityGroup** zu.

Durch diese Zuweisung wird sichergestellt, dass kein Datenverkehr in die infizierten Systeme übertragen wird.

10 Starten Sie auf der Symantec Antimalware-Konsole eine Prüfung für Ihr Netzwerk.


Die Prüfung identifiziert infizierte virtuelle Maschinen und versieht sie mit dem Sicherheits-Tag **AntiVirus.virusFound**. Die mit einem Tag versehenen virtuellen Maschinen werden sofort zu der **QuarantineSecurityGroup** hinzugefügt. Die **QuarantinePolicy** lässt keinen Datenverkehr von und zu den infizierten Systemen zu.

## Sichern von Sicherheitskonfigurationen

Mithilfe von Service Composer können Sie Ihre Sicherheitskonfigurationen auf effiziente Weise sichern und zu einem späteren Zeitpunkt wiederherstellen.


### Verfahren

- 1 Zunächst müssen Sie die Rapid 7-Lösung für das Schwachstellen-Management installieren, registrieren und bereitstellen.
- 2 Erstellen Sie eine Sicherheitsgruppe für die erste Schicht der SharePoint-Anwendung – Webserver.
  - a Melden Sie sich beim vSphere Web Client an.
  - b Klicken Sie auf **Netzwerk und Sicherheit (Networking & Security)** und dann auf **Service Composer**.
  - c Klicken Sie auf die Registerkarte **Security Groups** und dann auf das Symbol **Security Group hinzufügen (Add Security Group)**.
  - d Geben Sie in das Feld **Name** den Text **SG\_Web** ein.

- e Geben Sie in das Feld **Beschreibung (Description)** den Text **Sicherheitsgruppe für Anwendungsschicht** ein.
  - f Nehmen Sie keine Aktionen auf der Seite „Regeln der Mitgliedschaft definieren“ vor. Klicken Sie auf **Weiter (Next)**.
  - g Wählen Sie auf der Seite „Einzubeziehende Objekte auswählen“ die virtuellen Maschinen der Webserver aus.
  - h Nehmen Sie keine Aktionen auf der Seite „Auszuschließende Objekte auswählen“ vor. Klicken Sie auf **Weiter (Next)**.
  - i Überprüfen Sie Ihre Auswahl auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Beenden (Finish)**.
- 3** Erstellen Sie nun je eine Sicherheitsgruppe für Ihre Datenbank- und SharePoint-Server und nennen Sie sie **SG\_Database** bzw. **SG\_Server\_SharePoint**. Schließen Sie die entsprechenden Objekte in die einzelnen Gruppen ein.
- 4** Erstellen Sie eine Sicherheitsgruppe auf oberster Ebene für die Anwendungsschichten und nennen Sie sie **SG\_App\_Group**. Fügen Sie dieser Gruppe SG\_Web, SG\_Database und SG\_Server\_SharePoint hinzu.
- 5** Erstellen Sie eine Sicherheitsrichtlinie für Ihre Webserver.
- a Klicken Sie auf die Registerkarte „Sicherheitsrichtlinien“ und dann auf das Symbol „Sicherheitsrichtlinie hinzufügen“.
  - b Geben Sie in das Feld „Name“ **SP\_App** ein.
  - c Geben Sie in das Feld „Beschreibung“ den Text **SP für Anwendungs-Webserver** ein.
  - d Ändern Sie die Gewichtung in 50000. Der Vorrang der Richtlinie wird sehr hoch eingestellt, um zu gewährleisten, dass die Richtlinie vor den meisten anderen Richtlinien angewendet wird (mit Ausnahme der Quarantäne).
  - e Klicken Sie auf „Weiter“.
  - f Klicken Sie auf der Seite „Endpoint-Dienste“ auf  und geben Sie die folgenden Werte an.

Option	Wert
Aktion (Action)	Standardwert nicht ändern
Diensttyp (Service Type)	Vulnerability Management
Dienstname (Service Name)	Rapid 7
Dienstkonfiguration (Service Configuration)	Silver
Zustand (State)	Standardwert nicht ändern
Erzwingen (Enforce)	Standardwert nicht ändern

- g Fügen Sie keine Firewalldienste oder Netzwerk-Introspektionsdienste hinzu. Klicken Sie auf **Beenden (Finish)**.

- 6 Ordnen Sie SP\_App der Gruppe SG\_App\_Group zu.
- 7 Navigieren Sie zur Arbeitsflächen-Ansicht, um zu bestätigen, dass SP\_App der Gruppe SG\_App\_Group zugeordnet wurde.
  - a Klicken Sie auf die Registerkarte „Informationssicherheit“.
  - b Klicken Sie auf die Zahl neben dem Symbol , um zu sehen, dass SP\_App zugeordnet ist.
- 8 Exportieren Sie die SP\_App-Richtlinie.
  - a Klicken Sie auf die Registerkarte „Sicherheitsrichtlinien“ und dann auf das Symbol **Blueprint exportieren (Export Blueprint)** ().
  - b Geben Sie im Feld **Name** den Text **Template\_ App\_** und im Feld **Präfix (Prefix)** den Text **FromAppArchitect** ein.
  - c Klicken Sie auf „Weiter“.
  - d Wählen Sie die SP\_App-Richtlinie aus und klicken Sie auf „Weiter“.
  - e Überprüfen Sie Ihre Auswahl und klicken Sie auf „Beenden“.
  - f Wählen Sie das Verzeichnis auf Ihrem Computer aus, in das Sie die exportierte Datei herunterladen möchten, und klicken Sie auf „Speichern“.

Die Sicherheitsrichtlinie wird zusammen mit allen Sicherheitsgruppen exportiert, auf die diese Richtlinie angewendet wurde (in unserem Beispiel die Anwendungssicherheitsgruppe sowie die drei darin verschachtelten Sicherheitsgruppen).

- 9 Um die Funktionsweise der exportierten Richtlinie zu veranschaulichen, löschen Sie die SP\_App-Richtlinie.
- 10 Wir werden nun die in Schritt 7 exportierte Template\_ App\_ DevTest-Richtlinie wiederherstellen.
  - a Klicken Sie auf **Aktionen (Actions)** und anschließend auf das Symbol **Dienstkonfiguration importieren (Import Service Configuration)**.
  - b Wählen Sie die Datei **FromAppArchitect\_Template\_App** auf Ihrem Desktop aus (dies ist die Datei, die Sie in Schritt 7 gespeichert haben).
  - c Klicken Sie auf **Weiter (Next)**.
  - d Die Seite „Bereit zum Abschließen“ zeigt die zu importierenden Sicherheitsrichtlinien mit verknüpften Objekten (Sicherheitsgruppen, auf denen diese angewendet wurden, sowie Endpoint-Dienste, Firewallregeln und Netzwerk-Introspektionsdienste) an.
  - e Klicken Sie auf **Beenden (Finish)**.

Die Konfiguration und die zugehörigen Objekte werden in die vCenter-Bestandsliste importiert und in der Arbeitsflächen-Ansicht angezeigt.

## Importieren und Exportieren von Konfigurationen für Sicherheitsrichtlinien

Sie können den Service Composer verwenden, um die Konfiguration der Sicherheitsrichtlinie aus einem NSX Manager in ein bestimmtes Dateiformat zu exportieren und die exportierte Konfiguration in einen anderen NSX Manager zu importieren.

Im Service Composer können Sie Sicherheitsgruppen nicht direkt exportieren. Sie müssen zuerst sicherstellen, dass eine Sicherheitsrichtlinie einer Sicherheitsgruppe zugewiesen ist, und dann diese Sicherheitsrichtlinie exportieren. Alle Inhalte der Sicherheitsrichtlinie, wie z. B. DFW-Regeln, Regeln für die Guest Introspection, Regeln für die Netzwerk-Introspektion und die Sicherheitsgruppen, die an die Sicherheitsrichtlinie gebunden sind, werden exportiert.

Wenn eine Container-Sicherheitsgruppe geschachtelte Sicherheitsgruppen enthält, werden die verschachtelten Sicherheitsgruppen nicht exportiert. Beim Exportieren können Sie der Richtlinie ein Präfix hinzufügen. Das Präfix wird auf den Richtliniennamen, den Namen der Richtlinienaktionen und den Namen der Sicherheitsgruppe angewendet.

Wenn Sie die Konfiguration auf einen anderen NSX Manager importieren, können Sie ein Suffix angeben. Das Suffix wird auf den Richtliniennamen, den Namen der Richtlinienaktionen und den Namen der Sicherheitsgruppe angewendet. Wenn auf dem NSX Manager, in dem der Import erfolgt, eine Sicherheitsgruppe oder Sicherheitsrichtlinie mit demselben Namen vorhanden ist, schlägt der Import der Sicherheitsrichtlinienkonfiguration fehl.

### Exportieren einer Sicherheitsrichtlinien-Konfiguration

Sie können eine Sicherheitsrichtlinien-Konfiguration exportieren und auf Ihrem Desktop speichern. Die gespeicherte Konfiguration kann als Sicherung für Situationen verwendet werden, in denen Sie möglicherweise versehentlich eine Richtlinienkonfiguration löschen, oder sie kann für die Verwendung in einer anderen NSX Manager-Umgebung exportiert werden.

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)**.
- 4 Wählen Sie die Sicherheitsrichtlinie aus, die Sie exportieren möchten.
- 5 Klicken Sie auf **Aktionen (Actions)** und dann auf **Konfiguration exportieren (Export Configuration)**.
- 6 Geben Sie einen Namen und eine Beschreibung für die Konfiguration ein, die Sie exportieren.
- 7 Geben Sie, falls erforderlich, das Präfix ein, das zu den Sicherheitsrichtlinien und Sicherheitsgruppen, die importiert wurden, hinzugefügt werden soll.

Wenn Sie ein Präfix angeben, wird es zu den Namen der Zielsicherheitsrichtlinie hinzugefügt. Folglich wird sichergestellt, dass sie über eindeutige Namen verfügen.

- 8 Klicken Sie auf **Weiter (Next)**.
- 9 Wählen Sie auf der Seite **Sicherheitsrichtlinien auswählen** die zu exportierende Sicherheitsrichtlinie aus und klicken Sie auf **Weiter (Next)**.
- 10 Auf der Seite **Bereit zum Abschließen** werden die Sicherheitsrichtlinien, EndPoint-Dienste, Firewallregeln und die zu exportierenden Netzwerk-Introspektionsdienste angezeigt.  
Auf dieser Seite werden auch die Sicherheitsgruppen angezeigt, auf die die Sicherheitsrichtlinien angewendet werden.
- 11 Klicken Sie auf **Beenden (Finish)**.
- 12 Wählen Sie auf Ihrem Computer das Verzeichnis aus, in das Sie den Blueprint herunterladen möchten, und klicken Sie auf **Speichern (Save)**.  
Die Sicherheitsrichtlinien-Konfigurationsdatei wird im angegebenen Verzeichnis gespeichert.

## Importieren einer Sicherheitsrichtlinien-Konfiguration

Sie können eine gespeicherte Sicherheitsrichtlinien-Konfiguration entweder als Sicherung oder zum Wiederherstellen einer ähnlichen Konfiguration auf einem anderen NSX Manager importieren.

Wenn Sie die Konfiguration importieren, wird eine leere Sicherheitsgruppe erstellt. Alle Dienste, Dienstprofile, Anwendungen und Anwendungsgruppen müssen in der Zielumgebung vorhanden sein. Ansonsten schlägt der Import fehl.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.
- 3 Klicken Sie auf die Registerkarte **Sicherheitsrichtlinien (Security Policies)**.
- 4 Klicken Sie auf **Aktionen (Actions)** und anschließend auf das Symbol **Dienstkonfiguration importieren (Import Service Configuration)**.
- 5 Wählen Sie die zu importierende Konfigurationsdatei aus.
- 6 Geben Sie, falls erforderlich, das Suffix ein, das zu den Sicherheitsrichtlinien und Sicherheitsgruppen, die importiert werden, hinzugefügt werden soll.

Wenn Sie ein Suffix angeben, wird es zu den Namen der Sicherheitsrichtlinie hinzugefügt, die importiert wird. Somit wird sichergestellt, dass sie über eindeutige Namen verfügen.

- 7 Klicken Sie auf **Weiter (Next)**.

Service Composer stellt sicher, dass alle Dienste, auf die in der Konfiguration verwiesen wird, in der Zielumgebung verfügbar sind. Falls nicht, wird die Seite **Fehlende Dienste verwalten** angezeigt, auf der Sie die fehlenden Dienste verfügbaren Zieldiensten zuordnen können.

Auf der Seite **Bereit zum Abschließen** werden die Sicherheitsrichtlinien, EndPoint-Dienste, Firewallregeln und die zu importierenden Netzwerk-Introspektionsdienste angezeigt. Auf dieser Seite werden auch die Sicherheitsgruppen angezeigt, auf die die Sicherheitsrichtlinien angewendet werden.

**8** Klicken Sie auf **Beenden (Finish)**.

Die importierte Sicherheitsrichtlinien-Konfiguration wird zum oberen Bereich der Sicherheitsrichtlinien-Tabelle (über den bestehenden Richtlinien) in der NSX Manager-Zielinstanz hinzugefügt. Die ursprüngliche Reihenfolge der importierten Regeln und Sicherheitsdienste in der Sicherheitsrichtlinie wird beibehalten.

Guest Introspection lagert die Verarbeitung von Antivirus- und Anti-Malware-Agenten auf eine dedizierte sichere virtuelle Appliance aus, die von VMware-Partnern bereitgestellt wird. Da die sichere virtuelle Appliance (im Unterschied zu einer virtuellen Gastmaschine) nicht offline geschaltet wird, kann sie kontinuierlich Antivirus-Signaturen aktualisieren und dabei den virtuellen Maschinen auf dem Host unterbrechungsfreien Schutz bieten. Zudem werden neue virtuelle Maschinen (oder vorhandene virtuelle Offline-Maschinen) sofort durch die aktuellen Antivirus-Signaturen geschützt, wenn sie wieder online geschaltet werden.

Der Guest Introspection-Integritätsstatus wird mithilfe von Alarmen überwacht, die in der vCenter Server-Konsole mit roten Symbolen angezeigt werden. Zusätzlich können weitere Statusinformationen anhand der Ereignisprotokolle gesammelt werden.

---

**Wichtig** Ihre Umgebung muss für die Guest Introspection-Sicherheit ordnungsgemäß konfiguriert werden:

- Alle Hosts in einem Ressourcenpool, die geschützte virtuelle Maschinen enthalten, müssen für Guest Introspection vorbereitet sein, damit virtuelle Maschinen weiterhin geschützt bleiben, wenn sie mit vMotioned von einem auf einen anderen ESXi-Host innerhalb des Ressourcenpools migriert werden.
- Auf virtuellen Maschinen muss für den Schutz durch die Guest Introspection-Sicherheitslösung der Guest Introspection Thin Agent installiert sein. Nicht alle Gastbetriebssysteme werden unterstützt. Virtuelle Maschinen mit nicht unterstützten Gastbetriebssystemen werden nicht von der Sicherheitslösung geschützt.

---

Dieses Kapitel enthält die folgenden Themen:

- [Installieren von Guest Introspection auf Hostclustern](#)
- [Installieren von Guest Introspection Thin Agent auf virtuellen Windows-Maschinen](#)
- [Installieren von Guest Introspection Thin Agent auf virtuellen Linux-Maschinen](#)
- [Guest Introspection-Status anzeigen](#)
- [Guest Introspection-Überwachungsmeldungen](#)
- [Erfassen von Daten zur Fehlerbehebung für Guest Introspection](#)
- [Deinstallieren eines Guest Introspection-Moduls](#)

# Installieren von Guest Introspection auf Hostclustern

Durch die automatische Installation von Guest Introspection werden auf jedem Host im Cluster ein neuer VIB und eine neue Dienst-VM installiert. Guest Introspection ist für Activity Monitoring und verschiedene Drittanbieter-Sicherheitslösungen erforderlich.

**Hinweis** Sie können eine Dienst-VM (Service VM, SVM) nicht mithilfe von vMotion/SvMotion migrieren. Die Dienst-VMs müssen für eine korrekte Ausführung auf dem Host verbleiben, auf dem sie bereitgestellt wurden.

## Voraussetzungen

Die folgenden Installationsanweisungen setzen voraus, dass Sie über folgendes System verfügen:


- Ein Datacenter mit unterstützten Versionen von vCenter Server und ESXi, die auf jedem Host im Cluster installiert sein müssen.
- Falls die Hosts in Ihren Clustern von der vCenter Server-Version 5.0 auf 5.5 aktualisiert wurden, dann müssen Sie auf diesen Hosts die Ports 80 und 443 öffnen.
- Die Hosts in dem Cluster, in dem Sie Guest Introspection installieren möchten, wurden für NSX vorbereitet. Informationen dazu erhalten Sie unter „Vorbereiten der Hostcluster für NSX“ in der Dokumentation *Installationshandbuch für NSX*. Guest Introspection kann nicht auf eigenständigen Hosts installiert werden. Wenn Sie NSX für das Bereitstellen und Verwalten von Guest Introspection nur für die Antivirenfunktion verwenden, müssen Sie die Hosts nicht für NSX vorbereiten. Mit der NSX für vShield Endpoint-Lizenz ist dies nicht möglich.
- NSX Manager ist installiert und wird ausgeführt.
- Stellen Sie sicher, dass die NSX Manager und die vorbereiteten Hosts, auf denen die Guest Introspection-Dienste ausgeführt werden, mit demselben NTP-Server verknüpft sind und dass die Zeit synchronisiert ist. Andernfalls sind VMs möglicherweise nicht durch Antivirendienste geschützt, auch wenn der Status des Clusters für Guest Introspection und alle Drittanbieterdienste grün angezeigt wird.

Wird ein NTP-Server hinzugefügt, empfiehlt VMware, Guest Introspection und alle Drittanbieterdienste anschließend erneut bereitzustellen.

Wenn Sie der VM des NSX Guest Introspection-Dienstes eine IP-Adresse aus einem IP-Pool zuweisen möchten, erstellen Sie den IP-Pool, bevor Sie NSX Guest Introspection installieren. Informationen dazu finden unter „Arbeiten mit IP-Pools“ im Dokument *Administratorhandbuch für NSX*.

vSphere Fault Tolerance kann nicht zusammen mit Guest Introspection verwendet werden.

## Verfahren

- 1 Klicken Sie auf der Registerkarte **Installation** auf **Dienstbereitstellungen (Service Deployments)**.
- 2 Klicken Sie auf das Symbol **Neue Dienstbereitstellung (New Service Deployment)** (  ).

- 3 Wählen Sie im Dialogfeld „Netzwerk- und Sicherheitsdienste bereitstellen“ die Option **Guest Introspection** aus.
- 4 Wählen Sie unter **Zeitplan angeben (Specify schedule)** (am unteren Rand des Dialogfelds) die Option **Jetzt bereitstellen (Deploy now)** aus, um Guest Introspection sofort nach der Installation bereitzustellen, oder wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- 5 Klicken Sie auf **Weiter (Next)**.
- 6 Wählen Sie das Datacenter und die Cluster aus, in denen Sie Guest Introspection installieren möchten, und klicken Sie auf **Weiter (Next)**.
- 7 Wählen Sie auf der Seite „Speicher- und Verwaltungsnetzwerk auswählen“ den Datenspeicher aus, auf dem Sie den VM-Speicher für den Dienst hinzufügen möchten, oder wählen Sie die Option **Angegeben auf dem Host (Specified on host)** aus. Es wird empfohlen, dass Sie gemeinsame Datenspeicher und Netzwerke anstatt „Angegeben auf dem Host“ verwenden, damit die bereitgestellten Workflows automatisiert werden.

Der ausgewählte Datenspeicher muss auf allen Hosts im ausgewählten Cluster verfügbar sein.

Wenn Sie **Angegeben auf dem Host (Specified on host)** ausgewählt haben, führen Sie die unten genannten Schritte für jeden Host im Cluster aus.

- a Klicken Sie auf der Startseite von vSphere Web Client auf **vCenter** und dann auf **Hosts**.
  - b Klicken Sie in der Spalte **Name** auf einen Host und dann auf die Registerkarte **Verwalten (Manage)**.
  - c Klicken Sie auf **Agent-VMs (Agent VMs)** und anschließend auf **Bearbeiten (Edit)**.
  - d Wählen Sie den Datenspeicher aus und klicken Sie auf **OK**.
- 8 Wählen Sie die verteilte virtuelle Portgruppe aus, in der die Verwaltungsschnittstelle gehostet werden soll. Wenn der Datenspeicher auf **Angegeben auf dem Host (Specified on host)** gesetzt ist, muss das Netzwerk auch auf **Angegeben auf dem Host (Specified on host)** gesetzt sein.

Die ausgewählte Portgruppe muss die Portgruppe des NSX Manager erreichen können und auf allen Hosts im ausgewählten Cluster verfügbar sein.

Wenn Sie **Angegeben auf dem Host (Specified on host)** ausgewählt haben, führen Sie die Teilschritte unter Schritt 7 aus, um ein Netzwerk auf dem Host auszuwählen. Wenn Sie dem Cluster einen (oder mehrere) Hosts hinzufügen, muss vor dem Hinzufügen der Datenspeicher und das Netzwerk für jeden Host festgelegt werden.

- 9 Wählen Sie unter „IP-Zuweisungen“ eine der folgenden Optionen aus:

Option	Zweck
<b>DHCP</b>	Weisen Sie der VM des NSX Guest Introspection-Dienstes eine IP-Adresse über Dynamic Host Configuration Protocol (DHCP) zu. Wählen Sie diese Option aus, wenn Ihre Hosts auf unterschiedlichen Subnetzen untergebracht sind.
<b>Einen IP-Pool</b>	Weisen Sie der VM des NSX Guest Introspection-Diensts eine IP-Adresse aus dem ausgewählten IP-Pool zu.

- 10 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Weiter (Next)** und anschließend auf **Beenden (Finish)**.
- 11 Überwachen Sie die Bereitstellung, bis **Erfolg (Succeeded)** für die Spalte **Installationsstatus (Installation Status)** angezeigt wird.
- 12 Wenn **Fehlgeschlagen (Failed)** für die Spalte **Installationsstatus (Installation Status)** angezeigt wird, klicken Sie auf das Symbol neben „Fehlgeschlagen“. Es werden alle Bereitstellungsfehler angezeigt. Klicken Sie auf **Auflösen (Resolve)**, um die Fehler zu beheben. In einigen Fällen werden beim Auflösen der Fehler zusätzliche Fehlermeldungen angezeigt. Führen Sie die nötige(n) Aktion(en) aus und klicken Sie wieder auf **Auflösen (Resolve)**.

## Installieren von Guest Introspection Thin Agent auf virtuellen Windows-Maschinen

Zum Schutz von VMs, die eine Guest Introspection-Sicherheitslösung verwenden, müssen Sie den Guest Introspection Thin Agent, auch Guest Introspection-Treiber genannt, auf den virtuellen Maschinen installieren. Guest Introspection-Treiber sind im Lieferumfang der VMware Tools für Windows enthalten, aber sie sind nicht Teil der Standardinstallation. Um Guest Introspection auf einer Windows-VM zu installieren, müssen Sie eine benutzerdefinierte Installation vornehmen und die Treiber auswählen.

- Wenn Sie vSphere 5.5 oder 6.0 verwenden, beziehen Sie sich auf diese Anweisungen zum Installieren von VMware Tools: [http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm\\_admin.doc%2FGUID-391BE4BF-89A9-4DC3-85E7-3D45F5124BC7.html](http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.vm_admin.doc%2FGUID-391BE4BF-89A9-4DC3-85E7-3D45F5124BC7.html).
- Wenn Sie vSphere 6.5 verwenden, beziehen Sie sich auf diese Anweisungen zum Installieren von VMware Tools: <https://www.vmware.com/support/pubs/vmware-tools-pubs.html>.

Virtuelle Windows-Maschinen, auf denen die Guest Introspection-Treiber installiert sind, werden automatisch geschützt, wenn sie auf einem ESXi-Host gestartet werden, auf dem die Sicherheitslösung installiert ist. Geschützte virtuelle Maschinen behalten den Sicherheitsschutz auch nach dem Herunterfahren und Neustarten und sogar nach einer vMotion-Verschiebung auf einen anderen ESXi-Host, auf dem die Sicherheitslösung installiert ist.

Linux-Anweisungen finden Sie unter [Installieren von Guest Introspection Thin Agent auf virtuellen Linux-Maschinen](#).

### Voraussetzungen

Stellen Sie sicher, dass auf der virtuellen Gastmaschine eine unterstützte Version von Windows installiert ist. Die folgenden Windows-Betriebssysteme werden für NSX Guest Introspection unterstützt:

- Windows XP SP3 und höher (32-Bit)
- Windows Vista (32-Bit)
- Windows 7 (32/64-Bit)
- Windows 8 (32/64-Bit) – nur vSphere 5.5

- Windows 8.1 (32/64) – ab vSphere 5.5 Patch 2 und höher
- Windows 10
- Windows 2003 SP2 und höher (32/64-Bit)
- Windows 2003 R2 (32/64-Bit)
- Windows 2008 (32/64-Bit)
- Windows 2008 R2 (64-Bit)
- Win2012 (64) – nur vSphere 5.5
- Win2012 R2 (64) – ab vSphere 5.5 Patch 2 und höher

## Verfahren

- 1 Starten Sie die Installation von VMware Tools gemäß den Anweisungen für Ihre Version von vSphere. Wählen Sie die **Benutzerdefinierte (Custom)** Installation.
- 2 Erweitern Sie den Abschnitt **VMCI-Treiber (VMCI Driver)**.

Die verfügbaren Optionen variieren je nach Version von VMware Tools.

Treiber	Beschreibung
vShield Endpoint-Treiber	File Introspection (vsepfilt)- und Network Introspection (vnetflt)-Treiber werden installiert.
Guest Introspection-Treiber	File Introspection (vsepfilt)- und Network Introspection (vnetflt)-Treiber werden installiert.
NSX File Introspection- und NSX Network Introspection-Treiber	<p>Wählen Sie „NSX File Introspection-Treiber“, um vsepfilt zu installieren.</p> <p>Wählen Sie optional „NSX Network Introspection-Treiber“, um vnetflt (vnetWFP für Windows 10) zu installieren.</p> <p><b>Hinweis</b> Wählen Sie NSX Network Introspection-Treiber nur, wenn Sie die identitätsbasierte Firewall oder Funktionen zur Endpunktüberwachung verwenden.</p>

- 3 Wählen Sie im Dropdown-Menü neben den Treibern, die Sie hinzufügen möchten, **Diese Funktion wird auf der lokalen Festplatte installiert (This feature will be installed on the local hard drive)**.
- 4 Führen Sie die restlichen Schritte dieses Vorgangs aus.

## Nächste Schritte

Überprüfen Sie, ob der Thin Agent ausgeführt wird. Verwenden Sie dazu den `fltmc`-Befehl mit Administratorrechten. In der Spalte „Filtername“ in der Ausgabe wird der Thin Agent mit dem Eintrag `vsepfilt` aufgelistet.

# Installieren von Guest Introspection Thin Agent auf virtuellen Linux-Maschinen

Guest Introspection unterstützt File Introspection in Linux nur für den Virenschutz. Um Linux-VMs mit einer Guest Introspection-Sicherheitslösung zu schützen, müssen Sie den Guest Introspection Thin Agent installieren.

Der GI Thin Agent ist als Bestandteil der betriebssystemspezifischen Pakete (OSP, Operating System Specific Packages) für die VMware Tools verfügbar. Das Installieren von VMware Tools ist nicht erforderlich. Die Installation und das Upgrade von GI Thin Agent sind nicht mit der Installation und dem Upgrade von NSX verknüpft. Zudem kann der Administrator des Unternehmens oder der Sicherheitsadministrator (Nicht-NSX-Administrator) den Agent auf Gast-VMs außerhalb von NSX installieren.

Verwenden Sie zum Installieren von GI Thin Agent auf RHEL- oder SLES-Linux-Systemen das *RPM*-Paket. Verwenden Sie zum Installieren von GI Thin Agent auf Ubuntu Linux-Systemen das *DEB*-Paket.

Windows-Anweisungen finden Sie unter [Installieren von Guest Introspection Thin Agent auf virtuellen Windows-Maschinen](#).

## Voraussetzungen

- Stellen Sie sicher, dass auf der virtuellen Gastmaschine eine unterstützte Version von Linux installiert ist:
  - Red Hat Enterprise Linux (RHEL) 7 GA (64 Bit)
  - SUSE Linux Enterprise Server (SLES) 12 GA (64 Bit)
  - Ubuntu 14.04 LTS (64 Bit)
- Stellen Sie sicher, dass GLib 2.0 auf der Linux-VM installiert ist.
- Laden Sie das GI Thin Agent-Paket (`vmware-nsx-gi-file`) herunter, indem Sie das VMware-Paket-Repository unter <https://packages.vmware.com/packages/index.html> besuchen.

## Verfahren

- ◆ Führen Sie basierend auf Ihrem Linux-Betriebssystem die folgenden Schritte mit Stammrecht aus:
  - Für Ubuntu-Systeme:
    - a Rufen Sie die öffentlichen VMware-Paketschlüssel mithilfe der folgenden Befehle ab, und importieren Sie sie:

```
curl -O https://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub
apt-key add VMWARE-PACKAGING-GPG-RSA-KEY.pub
```

- b Erstellen Sie eine neue Datei mit dem Namen `vm.list` unter `/etc/apt/sources.list.d`.

- c Bearbeiten Sie die Datei mit folgendem Inhalt:

```
vi /etc/apt/sources.list.d/vm.list
deb https://packages.vmware.com/packages/ubuntu/ trusty main
```

- d Installieren Sie nun das Paket wie folgt:

```
apt-get update
apt-get install vmware-nsx-gi-file
```

- Für RHEL7-Systeme:

- a Rufen Sie die öffentlichen VMware-Paketschlüssel mithilfe der folgenden Befehle ab, und importieren Sie sie:

```
curl -O https://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-GPG-RSA-KEY.pub
```

- b Erstellen Sie eine neue Datei mit dem Namen *vm.repo* unter */etc/yum.repos.d*.

- c Bearbeiten Sie die Datei mit folgendem Inhalt:

```
vi /etc/yum.repos.d/vm.repo
[vm]
name = VMware
baseurl = https://packages.vmware.com/packages/rhel7/x86_64
enabled = 1
gpgcheck = 1
metadata_expire = 86400
ui_repoid_vars = basearch
```

- d Installieren Sie nun das Paket wie folgt:

```
yum install vmware-nsx-gi-file
```

- ◆ Für SLES-Systeme:

- a Rufen Sie die öffentlichen VMware-Paketschlüssel mithilfe der folgenden Befehle ab, und importieren Sie sie:

```
curl -O https://packages.vmware.com/tools/keys/VMWARE-PACKAGING-GPG-RSA-KEY.pub
rpm --import VMWARE-PACKAGING-GPG-RSA-KEY.pub
```

- b Fügen Sie das folgende Repository hinzu:

```
zypper ar -f "https://packages.vmware.com/packages/sle12/x86_64/" VMware
```

- c Installieren Sie nun das Paket wie folgt:

```
zypper install vmware-nsx-gi-file
```

## Nächste Schritte

Überprüfen Sie, ob der Thin Agent ausgeführt wird. Verwenden Sie dazu den `service vsep status-` Befehl mit Administratorrechten. Der Status sollte Ausführung lauten.

## Guest Introspection-Status anzeigen

Die Überwachung einer Guest Introspection-Instanz umfasst die Überprüfung von Statusinformationen von den Guest Introspection-Komponenten: die sichere virtuelle Maschine (SVM), Guest Introspection-Modul auf dem ESXi-Host und Thin Agent auf der geschützten virtuellen Maschine.

### Verfahren

- 1 Klicken Sie im vSphere Web Client auf **vCenter-Bestandslisten (vCenter Inventory Lists)** und anschließend auf **Datencenter (Datacenters)**.
- 2 Klicken Sie in der Spalte **Name** auf ein Datencenter.
- 3 Klicken Sie auf **Überwachen (Monitor)**, und klicken Sie dann auf **Guest Introspection**.

Die Guest Introspection-Seite „Health and Alarms“ zeigt den Systemstatus der Objekte unter dem ausgewählten Datencenter sowie die aktiven Alarme an. Systemzustandsänderungen werden innerhalb einer Minute nach dem tatsächlichen Eintreten des Ereignisses wiedergegeben, das die Änderung ausgelöst hat.

## Guest Introspection-Überwachungsmeldungen

Überwachungsmeldungen umfassen schwerwiegende Fehler und andere wichtige Überwachungsinformationen. Überwachungsmeldungen werden in der Datei `vmware.log` protokolliert.

Die folgenden Bedingungen werden als AUDIT-Meldungen protokolliert:

- Erfolgreiche Thin-Agent-Initialisierung (und Versionsnummer)
- Fehler bei der Thin-Agent-Initialisierung
- Erste Einrichtung einer Kommunikation mit SVM
- Fehler beim Einrichten der Kommunikation mit SVM (bei erstem Fehler)

Generierte Protokollmeldungen weisen die folgenden Teilzeichenfolgen im Anfangsabschnitt jeder Protokollmeldung auf: `vf-AUDIT`, `vf-ERROR`, `vf-WARN`, `vf-INFO`, `vf-DEBUG`.

## Erfassen von Daten zur Fehlerbehebung für Guest Introspection

Der Technische Support von VMware fordert bei einer Supportanfrage routinemäßig Diagnoseinformationen oder ein Supportpaket an. Diese Diagnoseinformationen enthalten Protokoll- und Konfigurationsdateien für Ihre virtuellen Maschinen.

## Daten zur Fehlerbehebung bei einer identitätsbasierten Firewall

Wenn Ihre identitätsbasierte Firewall-Umgebung Guest Introspection verwendet, finden Sie die Diagnosedaten unter *Fehlerbehebungshandbuch zu NSX und NSX-Protokollierung und -Systemereignisse*.

## Deinstallieren eines Guest Introspection-Moduls

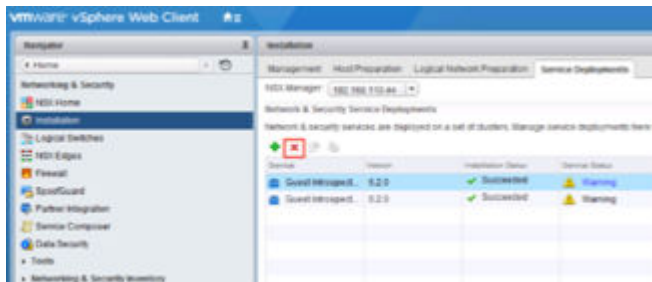
Durch das Deinstallieren von Guest Introspection wird ein VIB aus den Hosts im Cluster und die Dienst-VM aus jedem Host im Cluster entfernt. Guest Introspection ist für die Identitäts-Firewall, die Endpoint-Überwachung und verschiedene Drittanbieter-Sicherheitslösungen erforderlich. Das Deinstallieren von Guest Introspection kann weitreichende Auswirkungen haben.

**Vorsicht** Bevor Sie ein Guest Introspection-Modul aus einem Cluster deinstallieren, müssen Sie alle Drittanbieter-Produkte, die Guest Introspection verwenden, auf den Hosts in diesem Cluster deinstallieren. Halten Sie sich dabei an die Anweisungen des Anbieters.

Es gibt weniger Schutz für VMs im NSX-Cluster. Sie müssen mit vMotion die virtuellen Maschinen aus dem Cluster verschieben, bevor Sie die Deinstallation durchführen.

So wird Guest Introspection deinstalliert:

- 1 Navigieren Sie in vCenter zu **Home > Networking & Security > Installation** und wählen Sie die Registerkarte **Dienstbereitstellungen (Service Deployments)** aus.
- 2 Wählen Sie die Guest Introspection-Instanz aus und klicken Sie auf das Symbol „Löschen“.
- 3 Löschen Sie sie entweder jetzt oder planen Sie das Löschen für einen späteren Zeitpunkt.



## Guest Introspection für Linux deinstallieren

Sie können Linux Thin Agent für Guest Introspection von der virtuellen Gast-Maschine deinstallieren.

### Voraussetzungen

Guest Introspection für Linux ist installiert. Sie haben Stammrechte für das Linux-System.

### Verfahren

- ◆ Führen Sie zum Deinstallieren des Pakets von einem Ubuntu-System den Befehl `apt-get remove vmware-nsx-gi-file` aus.

- ◆ Führen Sie zum Deinstallieren des Pakets von einem RHEL7-System den Befehl `yum remove vmware-nsx-gi-file` aus.
- ◆ Führen Sie zum Deinstallieren des Pakets von einem SLES-System den Befehl `zypper remove vmware-nsx-gi-file` aus.

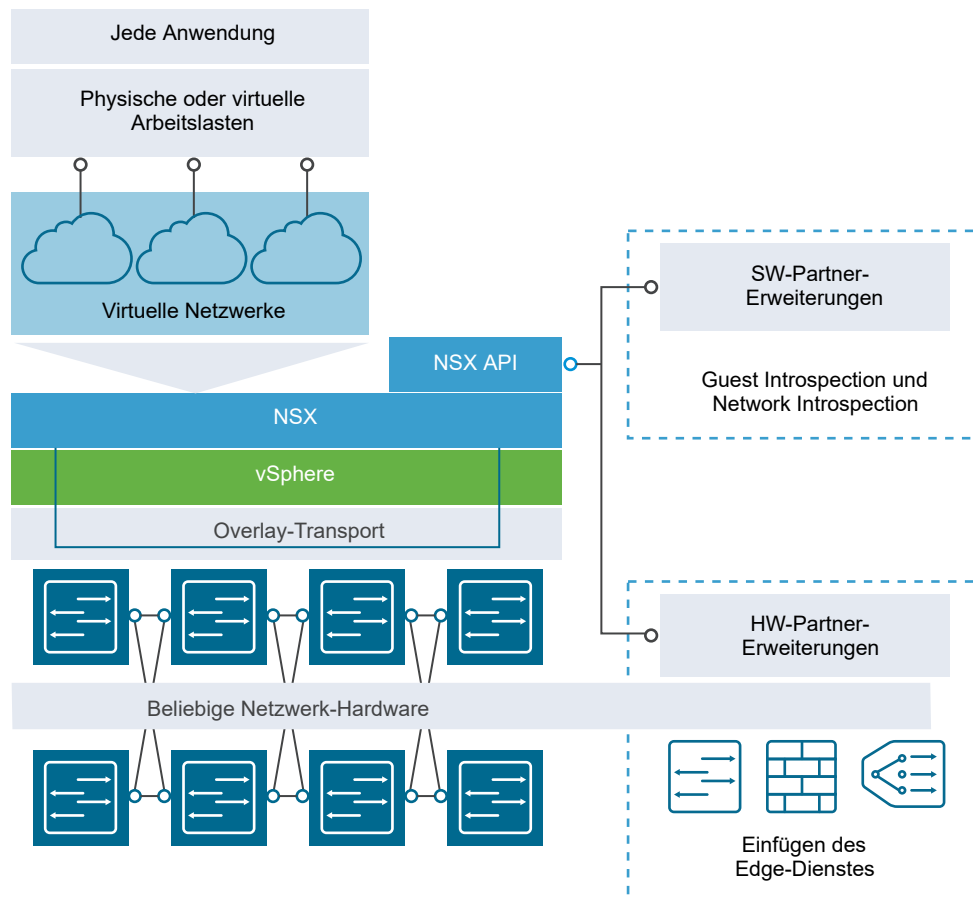
### Ergebnisse

Der auf der virtuellen Linux-Maschine installierte Thin Agent wird deinstalliert.

# Netzwerk-Erweiterbarkeit

# 19

Datencenter-Netzwerke umfassen für gewöhnlich eine Reihe von Netzwerkdiensten wie Switching, Routing, Firewalls, Load Balancing usw. In den meisten Fällen werden diese Dienste von unterschiedlichen Anbietern bereitgestellt. In der physischen Welt stellt die Verbindung dieser Dienste in einem Netzwerk eine komplizierte Aufgabe dar, bei der physische Netzwerkgeräte gestackt und aufgebaut werden müssen, um eine physische Verbindung herzustellen. Diese Geräte müssen außerdem getrennt verwaltet werden. NSX vereinfacht die Verbindung der richtigen Dienste zu den richtigen Datenverkehrswegen und hilft Ihnen so dabei, komplexe Netzwerke innerhalb eines einzigen ESX-Serverhosts oder über mehrere ESX-Serverhosts zu Produktions-, Test- oder Entwicklungszwecken aufzubauen.



Für die Einfügung von Drittanbieterdiensten in NSX stehen mehrere Bereitstellungsmethoden zur Verfügung.

Dieses Kapitel enthält die folgenden Themen:

- [Verteilte Service Insertion](#)
- [Edge-basierte Service Insertion](#)
- [Integration von Drittanbieter-Diensten](#)
- [Bereitstellen von Partnerdiensten](#)
- [Anbieter-Dienste durch Service Composer nutzen](#)
- [Umleiten des Datenverkehrs zu einer Anbieterlösung über die logische Firewall](#)
- [Nutzung eines Partner-Load-Balancer](#)
- [Entfernen der Drittanbieterintegration](#)

## Verteilte Service Insertion

Bei einer verteilten Service Insertion verfügt ein Host über alle Dienstmodule, Kernmodule und virtuellen Maschinen auf einer einzigen physischen Maschine. Alle Systemkomponenten interagieren mit Komponenten innerhalb des physischen Hosts. Dadurch werden eine schnellere Kommunikation zwischen Modulen und kompakte Bereitstellungsmodelle ermöglicht. Die gleiche Konfiguration kann zwecks Skalierbarkeit auch auf physische Systeme im Netzwerk repliziert werden, während Steuerungs- und Datenebenenverkehr zwischen den Dienstmodulen und VMkernel im dem gleichen physischen System bleiben. Wenn vMotion für geschützte virtuelle Maschinen ausgeführt wird, ändert die Partner-Sicherheitsmaschine den Zustand der virtuellen Maschine vom Quell- zum Zielhost.

Anbieterlösungen, die diese Art von Dienstinserion nutzen, sind unter anderem Intrusion Prevention Service (IPS)/Intrusion Detection Service (IDS), Firewall, Anti Virus, File Identity Monitoring (FIM) und Vulnerability Management.

## Edge-basierte Service Insertion

NSX Edge wird im Edge-Dienste-Cluster neben weiteren Netzwerkdiensten als eine virtuelle Maschine bereitgestellt. Mit NSX Edge können Sie bestimmten Datenverkehr zu Drittanbieter-Netzwerkdiensten umleiten.

Zu Anbieterlösungen, die diese Art von Dienstinserion nutzen, gehören unter anderem ADC- und Load-Balancing-Einrichtungen.

## Integration von Drittanbieter-Diensten

Dies ist ein allgemeiner umfassender Workflow zum Einfügen von Drittanbieterdiensten in die NSX-Plattform.

## Verfahren

- 1 Registrieren Sie den Drittanbieterdienst im NSX Manager auf der Anbieterkonsole.

Für die Registrierung des Dienstes benötigen Sie NSX-Anmeldedaten. Weitere Informationen dazu finden Sie in der Anbieter-Dokumentation.

- 2 Stellen Sie den Dienst in NSX bereit. Weitere Informationen dazu finden Sie unter [Bereitstellen von Partnerdiensten](#).

Nach der Bereitstellung wird der Drittanbieterdienst im Fenster mit den NSX-Dienstdefinitionen angezeigt und kann sofort genutzt werden. Welches Verfahren Sie zur Nutzung des Dienstes in NSX wählen, hängt vom Typ des eingefügten Dienstes ab.

So können Sie zum Beispiel einen hostbasierten Firewalldienst aktivieren, indem Sie eine Sicherheitsrichtlinie in Service Composer oder eine Firewallregel zum Umleiten von Datenverkehr an den Dienst erstellen. Siehe [Anbieter-Dienste durch Service Composer nutzen](#) oder [Umleiten des Datenverkehrs zu einer Anbieterlösung über die logische Firewall](#). Weitere Informationen zur Nutzung eines Edge-basierten Dienstes finden Sie unter [Nutzung eines Partner-Load-Balancer](#).

## Bereitstellen von Partnerdiensten

Enthält die Partnerlösung eine virtuelle Appliance auf einem Host, können Sie den Dienst installieren, nachdem die Lösung in NSX Manager registriert worden ist.

### Voraussetzungen

Stellen Sie sicher, dass folgende Voraussetzungen erfüllt sind:

- Die Partnerlösung wurde in NSX Manager registriert.
- NSX Manager kann auf die Verwaltungskonsole der Partnerlösung zugreifen.
- Die erforderliche Lizenzedition wurde zugewiesen. Weitere Informationen dazu finden Sie unter <https://kb.vmware.com/kb/2145269>.

### Verfahren

- 1 Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.
- 2 Klicken Sie auf die Registerkarte **Dienstbereitstellungen (Service Deployments)** und auf das Symbol **Neue Dienstbereitstellung (New Service Deployment)** (+).
- 3 Wählen Sie im Dialogfeld „Netzwerk- und Sicherheitsdienste bereitstellen“ die entsprechende(n) Lösung(en) aus.
- 4 Wählen Sie (unten im Dialogfeld) unter **Zeitplan angeben (Specify schedule)** die Option **Jetzt bereitstellen (Deploy now)**, um die Lösung sofort bereitzustellen, oder wählen Sie Datum und Uhrzeit für die Bereitstellung aus.
- 5 Klicken Sie auf **Weiter (Next)**.

- 6 Wählen Sie das Datacenter und den bzw. die Cluster aus, in denen Sie die Lösung bereitstellen möchten, und klicken Sie auf **Weiter (Next)**.

- 7 Wählen Sie den Datenspeicher aus, auf dem Sie den VM-Speicher für den Dienst hinzufügen möchten, oder wählen Sie **Angegeben auf dem Host (Specified on host)** aus.

Der ausgewählte Datenspeicher muss auf allen Hosts im ausgewählten Cluster verfügbar sein.

Wenn Sie **Angegeben auf dem Host (Specified on host)** ausgewählt haben, muss der Datenspeicher für den ESX-Host in den **Agent-VM-Einstellungen (AgentVM Settings)** des Hosts angegeben werden, bevor dieser zum Cluster hinzugefügt wird. Weitere Informationen hierzu finden Sie in der *vSphere-API/SDK-Dokumentation*.

- 8 Wählen Sie die verteilte virtuelle Portgruppe aus, in der die Verwaltungsschnittstelle gehostet werden soll. Diese Portgruppe muss in der Lage sein, die Portgruppe des NSX Managers zu erreichen.

Wenn für das Netzwerk die Einstellung **Angegeben auf dem Host (Specified on host)** gewählt wurde, muss das zu verwendende Netzwerk für jeden Host im Cluster in der Eigenschaft **Agent-VM-Einstellungen > Netzwerk (Agent VM Settings > Network)** angegeben werden. Weitere Informationen hierzu finden Sie in der *vSphere-API/SDK-Dokumentation*.

Sie müssen die Agent-VM-Netzwerkeigenschaft auf einem Host festlegen, bevor Sie ihn zu einem Cluster hinzufügen. Navigieren Sie zu **Verwalten (Manage) > Einstellungen (Settings) > Agent-VM-Einstellungen (Agent VM Settings) > Netzwerk (Network)** und klicken Sie auf **Bearbeiten (Edit)**, um das Agent-VM-Netzwerk einzustellen.

Die ausgewählte Portgruppe muss auf allen Hosts im ausgewählten Cluster verfügbar sein.

- 9 Wählen Sie unter „IP-Zuweisungen“ eine der folgenden Optionen aus:

Option	Zweck
DHCP	Weisen Sie der Dienst-VM eine IP-Adresse über Dynamic Host Configuration Protocol (DHCP) zu.
Einen IP-Pool	Weisen Sie der Dienst-VM eine IP-Adresse aus dem ausgewählten IP-Pool zu.

- 10 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Weiter (Next)** und anschließend auf **Beenden (Finish)**.

- 11 Überwachen Sie die Bereitstellung, bis „Erfolgreich“ für **Installationsstatus (Installation Status)** angezeigt wird. Wenn als Status „Fehlgeschlagen“ angezeigt wird, klicken Sie auf das Symbol neben „Fehlgeschlagen“ und führen Sie die nötigen Schritte aus, um den Fehler zu beheben.

### Nächste Schritte

Sie können den Partnerdienst jetzt über die NSX-Benutzeroberfläche oder die NSX API belegen.

## Anbieter-Dienste durch Service Composer nutzen

Drittanbieter-Dienste umfassen die Umleitung des Datenverkehrs, Load Balancer und Gastsicherheitsdienste wie beispielsweise Vermeiden von Datenverlust, Anti Virus usw. Mit Service Composer können Sie diese Dienste auf einen Satz an vCenter-Objekten anwenden.

Eine Sicherheitsgruppe ist ein Satz an vCenter-Objekten wie beispielsweise Cluster, virtuelle Maschinen, vNICs und logische Switches. Eine Sicherheitsrichtlinie ist ein Satz an Guest Introspection-Diensten, Firewallregeln und Introspektionsdiensten.

Wenn Sie eine Sicherheitsrichtlinie einer Sicherheitsgruppe zuordnen, werden Umleitungsregeln im entsprechenden Dienstprofil des Drittanbieters erstellt. Wenn Datenverkehr aus virtuellen Maschinen fließt, die zu dieser Sicherheitsgruppe gehören, wird er an registrierte Drittanbieterdienste weitergeleitet, die bestimmen, wie dieser Datenverkehr verarbeitet wird. Weitere Informationen zu Service Composer finden Sie unter [Verwenden des Service Composer](#).


## Umleiten des Datenverkehrs zu einer Anbieterlösung über die logische Firewall

Sie können Firewallregeln hinzufügen, um den Datenverkehr zu registrierten Anbieterlösungen umzuleiten. Umgeleiteter Datenverkehr wird dann von dem Anbieterdienst verarbeitet.


### Voraussetzungen


- Der Drittanbieterdienst muss in NSX Manager registriert und der Dienst in NSX bereitgestellt werden.
- Falls durch die voreingestellte Firewallregel „Blockieren“ als Aktion eingestellt wurde, müssen Sie eine neue Regel hinzufügen, damit der Datenverkehr umgeleitet werden kann.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > Firewall**.
- 2 Klicken Sie auf die Registerkarte **Partnersicherheitsdienste (Partner security services)**.
- 3 Klicken Sie in dem Abschnitt, zu dem Sie eine Regel hinzufügen möchten, auf das Symbol **Regel hinzufügen (Add rule)** (.

Die neue Regel wird an oberster Stelle im Abschnitt eingefügt.

- 4 Zeigen Sie auf die Zelle **Name** in der neuen Regel, klicken Sie auf  und geben Sie einen Namen für die Regel ein.
- 5 Geben Sie **Quelle (Source)**, **Ziel (Destination)** und **Dienst (Service)** für die Regel an. Weitere Informationen finden Sie unter [Hinzufügen einer Regel für die verteilte Firewall](#).

- 6 Zeigen Sie auf die Zelle **Aktion (Action)** der neuen Regel und klicken Sie auf .
  - a Unter **Aktion (Action)** wählen Sie **Umleiten (Redirect.)**.
  - b Wählen Sie unter **Umleiten zu (Redirect To)** das Dienstprofil sowie den logischen Switch oder die Sicherheitsgruppe aus, an die Sie das Dienstprofil binden möchten.  
  
Das Dienstprofil wird auf virtuelle Maschinen angewandt, die mit dem ausgewählten logischen Switch verbunden oder in der ausgewählten Sicherheitsgruppe enthalten sind.
  - c Geben Sie an, ob der umgeleitete Datenverkehr protokolliert werden soll und geben Sie ggf. Anmerkungen ein.
  - d Klicken Sie auf **OK**.  
  
Das ausgewählte Dienstprofil wird als Link in der Spalte **Aktion (Action)** angezeigt. Durch Anklicken des Dienstprofil-Links werden die Dienstprofil-Bindungen angezeigt.
- 7 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

## Nutzung eines Partner-Load-Balancer

Sie können einen Drittanbieter-Load-Balancer verwenden, um den Datenverkehr für einen bestimmten NSX Edge auszugleichen.

### Voraussetzungen

Der Drittanbieter-Load-Balancer muss bei NSX Manager registriert und in NSX bereitgestellt werden.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerk und Sicherheit (Networking & Security) > NSX Edges**.
- 2 Doppelklicken Sie auf eine NSX Edge-Instanz.
- 3 Klicken Sie auf **Verwalten (Manage)** und dann auf die Registerkarte **Load Balancer**.
- 4 Klicken Sie neben der globalen Konfiguration des Load Balancer auf **Bearbeiten (Edit)**.
- 5 Wählen Sie **Load Balancer aktivieren (Enable Load Balancer)** und **Service Insertion aktivieren (Enable Service Insertion)**.
- 6 Wählen Sie in **Dienstdefinition (Service Definition)** den entsprechenden Load Balancer aus.
- 7 Wählen Sie in **Dienstkonfiguration (Service Configuration)** die entsprechende Dienstkonfiguration aus.
- 8 Vervollständigen Sie die übrigen Felder und richten Sie einen Load Balancer ein, indem Sie eine Dienstüberwachung, einen Server-Pool, ein Anwendungsprofil, Anwendungsregeln und einen virtuellen Server hinzufügen. Wenn Sie einen virtuellen Server hinzufügen, wählen Sie die vom Anbieter bereitgestellte Vorlage aus. Weitere Informationen finden Sie unter [Einrichten des Load Balancing](#).

## Ergebnisse

Der Load Balancer für Datenverkehr für die angegebene Edge-Instanz wird durch die Verwaltungskonsole des Drittanbieters ausgeführt.

## Entfernen der Drittanbieterintegration

Dieses Beispiel beschreibt, wie aus NSX eine Drittanbieter-Integrationslösung entfernt wird.

Beim Entfernen einer Drittanbieter-Softwarelösung muss die Software in einer bestimmten Reihenfolge entfernt werden. Wird diese Reihenfolge nicht eingehalten, insbesondere beim Deinstallieren oder Löschen der Drittanbieterlösung vor dem Aufheben der Registrierung bei NSX Manager, schlägt das Entfernen fehl. Anweisungen für eine entsprechende Lösung finden Sie unter <https://kb.vmware.com/kb/2126678>.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Networking & Security > Service Composer** und löschen Sie die Regeln (oder die Sicherheitsrichtlinien), die den Datenverkehr auf die Drittanbieterlösung umleiten.
- 2 Navigieren Sie zu **Dienstdefinitionen (Service Definitions)** und doppelklicken Sie auf den Namen der Drittanbieterlösung.
- 3 Klicken Sie auf **Verwandte Objekte (Related Objects)** und löschen Sie die verwandten Objekte.
- 4 Navigieren Sie zu **Installation > Dienstbereitstellungen (Installation > Service Deployments)** und löschen Sie die Drittanbieterbereitstellung.

Mit dieser Aktion werden die zugewiesenen virtuellen Maschinen deinstalliert.

- 5 Kehren Sie zu **Dienstdefinitionen (Service Definitions)** zurück und löschen Sie alle Unterkomponenten der Definition.
- 6 Löschen Sie in der Dienstinstanz das Dienstprofil.
- 7 Löschen Sie die Dienstinstanz.
- 8 Löschen Sie die Dienstdefinition.

### Ergebnisse

Die Drittanbieter-Integrationslösung wird von NSX entfernt.

### Nächste Schritte

Notieren Sie die Konfigurationseinstellungen und entfernen Sie dann NSX aus der Drittanbieterlösung. Möglicherweise müssen Sie Regeln löschen, die auf andere Objekte verweisen, und dann diese Objekte löschen.

In vielen Organisationen sind verschiedene Teams oder Mitarbeiter für den Netzwerk- und den Sicherheitsbetrieb zuständig. Diese Organisationen benötigen unter Umständen eine Möglichkeit, bestimmte Vorgänge auf spezifische Benutzer zu begrenzen. In diesem Thema werden die Möglichkeiten beschrieben, die NSX für die Konfiguration einer entsprechenden Zugriffssteuerung bietet.

NSX unterstützt außerdem Single Sign On (SSO), sodass NSX Benutzer anderer Identitätsdienste, wie z. B. Active Directory, NIS und LDAP, authentifizieren kann.

Die Benutzerverwaltung in vSphere Web Client und die Benutzerverwaltung über die Befehlszeilenschnittstelle einer NSX-Komponente sind separat implementiert.

Dieses Kapitel enthält die folgenden Themen:

- [NSX-Benutzer und -Berechtigungen nach Funktion](#)
- [Konfigurieren von Single Sign-On](#)
- [Verwalten von Benutzerrechten](#)
- [Verwalten des Standardbenutzerkontos](#)
- [Zuweisen einer Rolle zu einem vCenter-Benutzer](#)
- [Erstellen eines Benutzers mit Zugriff auf die Web-Benutzeroberfläche mithilfe der Befehlszeilenschnittstelle](#)
- [Bearbeiten eines Benutzerkontos](#)
- [Ändern einer Benutzerrolle](#)
- [Deaktivieren oder Aktivieren eines Benutzerkontos](#)
- [Löschen eines Benutzerkontos](#)

## NSX-Benutzer und -Berechtigungen nach Funktion

Zur Bereitstellung und Verwaltung von NSX sind bestimmte vCenter-Berechtigungen erforderlich. NSX bietet umfangreiche Lese- und Schreibberechtigungen für unterschiedliche Benutzer und Rollen.

## Funktionsliste mit Rollen und Berechtigungen

Funktion	Beschreibung	Rollen			
		Auditor	Sicherheits admin	NSX-Admin	Unternehmens admin
Administrator					
Konfiguration	vCenter - und SSO-Konfiguration mit NSX	L	L	L, S	L, S
Aktualisieren		Kein Zugriff	Kein Zugriff	L, S	L, S
Systemereignisse	Systemereignisse	L	L, S	L, S	L, S
Überwachungsprotokolle	Überwachungsprotokolle	L	L	L	L
Benutzerkonto-Management (URM) (User Account Management (URM))					
Benutzerkonto-Management	Benutzer-Management	Kein Zugriff	Kein Zugriff	L	L, S
Objektzugriffssteuerung		Kein Zugriff	Kein Zugriff	L	L
Funktionszugriffssteuerung		Kein Zugriff	Kein Zugriff	L	L
Edge					
System	System bezieht sich auf allgemeine Systemparameter	L	L	L, S	L, S
Appliance	Verschiedene Formfaktoren von NSX Edge (kompakt/groß/extra-groß/QuadLarge)	L	L	L, S	L, S
High Availability		L	L	L, S	L, S
vNic	Schnittstellenkonfiguration in NSX Edge	L	L, S	L, S	L, S
DNS		L	L, S	L	L, S
SSH	SSH-Konfiguration in NSX Edge	L	L, S	L, S	L, S
Auto-Plumbing		L	L, S	L	L, S
Statistik		L	L	L	L, S
NAT	NAT-Konfiguration in NSX Edge	L	L, S	L	L, S
DHCP		L	L, S	L	L, S
Lastausgleich		L	L, S	L	L, S
VPN		L	L, S	L	L, S
Syslog	Syslog-Konfiguration in NSX Edge	L	L, S	L, S	L, S
Support		Kein Zugriff	L, S	L, S	L, S
Routing	Gesamtes statisches und dynamisches Routing (BGP/OSPF) in NSX Edge	L	L, S	L	L, S

Funktion	Beschreibung	Rollen			
		Auditor	Sicherheits admin	NSX-Admin	Unternehmens admin
Firewall	Firewall-Konfiguration in NSX Edge	L	L, S	L	L, S
Bridging		L	L, S	L	L, S
Zertifikat		L	L, S	L	L, S
Systemsteuerung	Die Systemsteuerung bezieht sich auf System-Kernel-Parameter wie Maximalgrenzen, IP-Weiterleitung, Netzwerk und Systemeinstellungen. Beispiel: ysctl.net.ipv4.conf.vNic_1.rp_filter sysctl.net.netfilter.nf_conntrack_tcp_timeout_established	L	L, S	L, S	L, S
<b>verteilte Firewall (Distributed Firewall)</b>					
Firewall-Konfiguration	Firewall-Regeln für Schicht3 (allgemein) und Schicht2 (Ethernet)	L	L, S	Kein Zugriff	L, S
Flows	Die Flow-Überwachung dient der Überwachung der Datenverkehr-Flows im System. Live-Flows können ebenfalls überwacht werden.	L	L, S	Kein Zugriff	L, S
IPFix-Konfiguration	IPFix-Aktivierung/-Deaktivierung und Zuweisung von Collectors	L	L, S	Kein Zugriff	L, S
ForceSync	ForceSync führt eine vollständige Synchronisierung auf der Seite <b>Installation &gt; Hostvorbereitung (Installation &gt; Host Preparation)</b> durch	L	L	Kein Zugriff	L, S
DFW installieren (Hostvorbereitung)	VIBS auf Clustern installieren	L	L	L, S	L, S
Gespeicherte Konfigurationen (Entwürfe)	Bei jeder Veröffentlichung wird die vorhandene DFW-Konfiguration automatisch als Entwurf gespeichert	L	L, S	Kein Zugriff	L, S
Ausschlussliste	Hinzufügen von VMs zur Ausschlussliste, die NICHT durch DFW geschützt oder die entfernt werden sollen	L	L, S	Kein Zugriff	L, S
Technischer DFW-Support	Abrufen des technischen DFW-Support-Pakets von einem Host (nur NSX-Konfigurations-Shell)	Kein Zugriff	L, S	Kein Zugriff	L, S
DFW-Sitzungs-Timer	TCP/UDP konfigurieren/Andere Zeitüberschreitungskonfiguration für Protokollverbindungen	L	L, S	Kein Zugriff	L, S

Funktion	Beschreibung	Rollen			
		Auditor	Sicherheits admin	NSX-Admin	Unternehmens admin
IP-Erkennung (DHCP/ ARP-Snooping)	IP-Erkennung, wenn VMware Tools nicht auf Gast-VMs ausgeführt werden	L	L, S	Kein Zugriff	L, S
Application Rule Manager	Flows werden für die ausgewählte Gruppe von Anwendungen erfasst. Basierend auf den erfassten Flows werden dann Firewallregeln erstellt.	L	L, S	Kein Zugriff	L, S
<b>NameSpace</b>					
Konfiguration		L	L	L, S	L, S
<b>SpoofGuard</b>					
Konfiguration	SpoofGuard-Veröffentlichung im TOFU- oder manuellen Mode	L	L, S	Kein Zugriff	L, S
<b>Endpoint-Sicherheit (EPSEC) (Endpoint Security (EPSEC))</b>					
Berichte		L	L	L, S	L, S
Registrierung	Lösungen verwalten [registrieren, Registrierung aufheben, registrierte Lösungen abfragen, aktivieren]	L	Kein Zugriff	L, S	L, S
Statusüberwachung	Systemzustand von VM, SVM in NSX Manager abrufen	Kein Zugriff	L	L	L
Richtlinie	Sicherheitsrichtlinien verwalten [erstellen, lesen, aktualisieren, löschen]	L	L, S	L, S	L, S
Zeitplan prüfen		L	Kein Zugriff	L, S	L, S
<b>Bibliothek (Library)</b>					
Hostvorbereitung	Hostvorbereitungsaktion auf Cluster	Kein Zugriff	Kein Zugriff	L, S	L, S
Gruppieren	IP Set, MAC Set, Sicherheitsgruppe, Dienst, Dienstgruppe	L	L, S	L	L, S
Tagging	Sicherheits-Tag (beispielsweise VMs anhängen oder trennen)	L	L, S	L	L, S
<b>Installieren (Install)</b>					
App		Kein Zugriff	L	L, S	L, S
EPSEC		Kein Zugriff	L	L, S	L, S
DLP		Kein Zugriff	L	L, S	L, S
<b>VDN</b>					
NSM konfigurieren	Network Security Manager konfigurieren	L	L	L, S	L, S
Bereitstellen		L	L	L, S	L, S

Funktion	Beschreibung	Rollen			
		Auditor	Sicherheits admin	NSX-Admin	Unternehmens admin
ESX Agent Manager (EAM)					
Installieren	ESX Agent Manager	Kein Zugriff	L	L, S	L, S
Service Insertion					
Dienst		L	L, S	L, S	L, S
Dienstprofil		L	L	L, S	L, S
Trust Store					
trustentity_management	Verwaltung von NSX-Zertifikaten	L	L, S	L, S	L, S
IP-Adressverwaltung (IPAM) (IP Address Management (IPAM))					
Konfiguration	Konfiguration des IP-Pools	L	L, S	L, S	L, S
IP-Zuteilung	IP-Zuteilung und -Freigabe	L	L, S	L, S	L, S
Sicherheits-Fabric (Security Fabric)					
Bereitstellen	Dienst- oder Sicherheits-VM auf dem Cluster mithilfe der <b>Dienstbereitstellung (Service Deployment)</b> bereitstellen	L	L	L, S	L, S
Alarmer	Verwalten Sie auf der Seite <b>Dienstbereitstellung (Service Deployment)</b> Alarmer, die von der Sicherheits-VM generiert werden	L	L	L, S	L, S
Agent-Systemzustand	Verwalten des Alarms für den Agent-Systemzustand per REST-Aufruf, wird hauptsächlich von Partner-VMs genutzt	L	L, S	L, S	L, S
Messaging					
Messaging	Von NSX Edge und Guest Introspection für die Kommunikation mit NSX Manager verwendetes Messaging-Framework	L	L, S	L, S	L, S
Replikator (Multi vCenter-Einrichtung mit sekundärem NSX Manager) (Replicator (Multi vCenter setup with secondary NSX Manager))					
Konfiguration	Wählen Sie die primäre Rolle für NSX Manager aus oder heben Sie die entsprechende Auswahl auf, und fügen Sie den sekundären NSX Manager hinzu, oder entfernen Sie ihn.	L	L	L, S	L, S
Sicherheitsrichtlinie (Security Policy)					

Funktion	Beschreibung	Rollen			
		Auditor	Sicherheits admin	NSX-Admin	Unternehmens admin
Konfiguration	Konfigurieren Sie die Sicherheitsrichtlinie zum Erstellen, Aktualisieren, Bearbeiten oder Löschen	L	L, S	Kein Zugriff	L, S
Sicherheitsgruppenbindung	Ordnen Sie die Sicherheitsgruppe einer Sicherheitsrichtlinie zu	L	L, S	Kein Zugriff	L, S

## Konfigurieren von Single Sign-On

SSO macht vSphere und NSX sicherer, da es die Kommunikation der verschiedenen Komponenten untereinander über einen sicheren Token-Austauschmechanismus ermöglicht. Dadurch ist es nicht mehr nötig, dass jede Komponente einen Benutzer separat authentifizieren muss.

Sie können Lookup Service im NSX Manager konfigurieren und die SSO-Administratoranmeldedaten zum Registrieren von NSX Management Service als SSO-Benutzer bereitstellen. Durch das Integrieren des Single Sign On-Diensts (SSO) in NSX wird die Sicherheit der Benutzerauthentifizierung für vCenter-Benutzer erhöht und NSX ermöglicht, Benutzer aus anderen Identitätsdiensten, wie z. B. AD, NIS und LDAP, zu authentifizieren. Mit SSO unterstützt NSX die Authentifizierung mithilfe authentifizierter SAML-Token (Security Assertion Markup Language) einer vertrauenswürdigen Quelle über REST-API-Aufrufe. NSX Manager kann auch Authentifizierungs-SAML-Token für die Verwendung mit anderen VMware-Lösungen erwerben.

NSX speichert Gruppeninformationen für SSO-Benutzer zwischen. Die Weitergabe von Änderungen an Gruppenmitgliedschaften vom Identitätsanbieter (z. B. Active Directory) an NSX kann bis zu 60 Minuten dauern.

### Voraussetzungen

- Sie benötigen zum Verwenden von SSO auf NSX Manager vCenter Server 5.5 oder höher und der Single Sign On-Dienst (SSO-Dienst) muss auf dem vCenter Server installiert sein. Beachten Sie, dass dies für eingebettetes SSO gilt. Ihre Bereitstellung verwendet möglicherweise stattdessen einen externen, zentralisierten SSO-Server.

Informationen zu den von vSphere bereitgestellten SSO-Diensten finden Sie unter <http://kb.vmware.com/kb/2072435> und <http://kb.vmware.com/kb/2113115>.

- Der NTP-Server muss angegeben werden, um sicherzugehen, dass die Zeit des SSO-Servers und von NSX Manager synchron sind.

Beispiel:

Time Settings		Unconfigure NTP Servers	Edit
Specify NTP server below. For SSO configuration to work correctly it is required that the time on this virtual appliance and NTP server should be in sync. It is recommended to use the same NTP server used by the SSO server.			
NTP Server	192.168.110.10		
Timezone	UTC		
Date/Time	12/28/2016 21:31:49		

## Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.

Navigieren Sie in einem Web-Browser zur NSX Manager Appliance-GUI unter <https://<nsx-manager-ip>> oder <https://<nsx-manager-hostname>> und melden Sie sich als Administrator mit dem Kennwort an, das Sie bei der Installation von NSX Manager konfiguriert haben.

- 2 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 3 Klicken Sie auf der Startseite auf **Appliance-Einstellungen verwalten (Manage Appliance Settings) > NSX-Verwaltungsdienst (NSX Management Service)**.

- 4 Klicken Sie im Bereich „Lookup Service-URL“ auf **Bearbeiten (Edit)**.

- 5 Geben Sie die IP-Adresse oder den Namen des Hosts mit dem Lookup Service ein.

- 6 Geben Sie die Portnummer ein.

Geben Sie Port 443 ein, wenn Sie vSphere 6.0 verwenden. Für vSphere 5.5 verwenden Sie die Portnummer 7444.

Die URL des Lookup Service wird basierend auf dem angegebenen Host und Port angezeigt.

- 7 Geben Sie den Benutzernamen und das Kennwort des SSO-Administrators ein und klicken Sie auf **OK**.



Der Fingerabdruck des Zertifikats für den SSO-Server wird angezeigt.

- 8 Überprüfen Sie, ob der Fingerabdruck des Zertifikats mit dem des SSO-Serverzertifikats übereinstimmt.

Wenn Sie auf dem Server der Zertifizierungsstelle ein von der Zertifizierungsstelle signiertes Zertifikat installiert haben, erhalten Sie den Fingerabdruck des von der Zertifizierungsstelle signierten Zertifikats. Anderenfalls erhalten Sie ein selbstsigniertes Zertifikat.

- 9 Vergewissern Sie sich, dass der Status von Lookup Service **Verbunden (Connected)** lautet.

Beispiel:

Lookup Service URL:	https://psc-01a.corp.local:443/lookupservice/sdk
SSO Administrator User Name:	administrator@vsphere.local
Status:	 Connected 

### Nächste Schritte

Siehe „Zuweisen einer Rolle zu einem vCenter-Benutzer“ im *Administratorhandbuch für NSX*.

## Verwalten von Benutzerrechten

Die Rolle eines Benutzers definiert die Aktionen, die der Benutzer für eine bestimmte Ressource ausführen kann. Die Rolle legt fest, welche Rechte der Benutzer an der Ressource hat, wodurch sichergestellt wird, dass ein Benutzer nur auf die Funktionen Zugriff hat, die zum Ausführen notwendiger Vorgänge erforderlich sind. So kann der Zugriff auf bestimmte Ressourcen auf Domänenebene oder systemweit gesteuert werden, wenn Ihre Rechte nicht eingeschränkt sind.

Die folgenden Regeln werden erzwungen:

- Ein Benutzer kann jeweils nur eine Rolle haben.
- Sie können einem Benutzer eine Rolle hinzufügen oder eine dem Benutzer zugewiesene Rolle entfernen. Sie können allerdings auch die einem Benutzer zugewiesene Rolle ändern.

**Tabelle 20-1. NSX Manager-Benutzerrollen**

Recht	Berechtigungen
Enterprise-Administrator	NSX-Vorgänge und -Sicherheit.
NSX-Administrator	Nur NSX-Vorgänge: z. B. Installieren von virtuellen Appliances, Konfigurieren von Portgruppen.
Security Administrator	Nur NSX-Sicherheit: z. B. Definieren von Regeln für die verteilte Firewall, Konfigurieren von NAT und Load-Balancer-Diensten.
Auditor	Nur Lesen.

Die Rollen „Enterprise-Administrator“ und „NSX-Administrator“ können nur vCenter-Benutzern zugewiesen werden.

## Verwalten des Standardbenutzerkontos

Zur NSX Manager-Benutzeroberfläche gehört auch ein Benutzerkonto, das Zugriffsrechte auf alle Ressourcen hat. Die Rechte dieses Benutzers können nicht bearbeitet und der Benutzer kann nicht gelöscht werden. Der Standardbenutzername lautet **admin**, und das Standardkennwort lautet **default** oder entspricht dem Kennwort, das Sie während der Installation von NSX Manager angegeben haben.

Sie können den **admin**-Benutzer der NSX Manager-Appliance nur über CLI-Befehle verwalten.

## Zuweisen einer Rolle zu einem vCenter-Benutzer

Wenn Sie einem SSO-Benutzer eine Rolle zuweisen, authentifiziert vCenter den Benutzer anhand des Identitätsdiensts, der auf dem SSO-Server konfiguriert ist. Wenn der SSO-Server nicht konfiguriert oder nicht verfügbar ist, wird der Benutzer basierend auf der vCenter-Konfiguration entweder lokal oder mit Active Directory authentifiziert.

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
- 3 Klicken Sie in der Spalte „Name“ auf einen NSX Manager und anschließend auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf **Benutzer (Users)**.
- 5 Klicken Sie auf **Hinzufügen (Add)**.

Das Fenster „Rolle zuweisen“ wird geöffnet.

- 6 Klicken Sie auf **vCenter-Benutzer festlegen (Specify a vCenter user)** oder **vCenter-Gruppe festlegen (Specify a vCenter group)**.
- 7 Geben Sie den vCenter-**Benutzer (User)**- oder **Gruppen (Group)**-Namen für den Benutzer ein.

Weitere Informationen finden Sie im nachfolgenden Beispiel.

Domänenname: corp.vmware.com

Alias: corp

Gruppenname: group1@corp.vmware.com

Benutzername: user1@corp.vmware.com

Wenn einer Gruppe eine Rolle des NSX Manager zugewiesen wurde, kann sich jeder Benutzer dieser Gruppe bei der Benutzeroberfläche des NSX Manager anmelden.

Wenn Sie einem Benutzer eine Rolle zuweisen, geben Sie den Alias des Benutzers ein. Beispiel: user1@corp.

- 8 Klicken Sie auf **Weiter (Next)**.
- 9 Wählen Sie die Rolle für den Benutzer aus und klicken Sie auf **Weiter (Next)**. Weitere Informationen zu den verfügbaren Rollen finden Sie unter [Verwalten von Benutzerrechten](#).
- 10 Klicken Sie auf **Beenden (Finish)**.

Das Benutzerkonto wird in der Benutzertabelle angezeigt.

## Grundlegendes zu gruppenbasierten Rollenzuweisungen

Organisationen erstellen Benutzergruppen, um Benutzer ordnungsgemäß zu verwalten. Nach der Integration in SSO kann NSX Manager Details zu den Gruppen abrufen, denen ein Benutzer angehört. Statt einzelnen derselben Gruppe angehörenden Benutzern Rollen zuzuweisen, weist NSX Manager Rollen zu Gruppen zu. In den folgenden Szenarien werden Szenarien dargestellt, wie NSX Manager Rollen zuweist.

### Beispiel: Rollenbasiertes Zugriffssteuerungsszenario

In diesem Szenario wird einer IT-Netzwerk-Ingenieurin (Sarah Maier) in der folgenden Umgebung Zugriff auf NSX-Komponenten eingeräumt.

AD-Domäne: corp.local, vCenter-Gruppe: neteng@corp.local, Benutzername: smaier@corp.local

Voraussetzungen: vCenter Server wurde bei NSX Manager registriert und SSO wurde konfiguriert.

Beachten Sie, dass SSO nur für Gruppen erforderlich ist.

- 1 Weisen Sie Sarah eine Rolle zu.
  - a Melden Sie sich beim vSphere Web Client an.
  - b Klicken Sie auf **Networking & Security** und anschließend auf **NSX Manager (NSX Managers)**.
  - c Klicken Sie in der Spalte „Name“ auf einen NSX Manager und anschließend auf die Registerkarte **Verwalten (Manage)**.
  - d Klicken Sie auf **Benutzer (Users)** und anschließend auf **Hinzufügen (Add)**.  
Das Fenster „Rolle zuweisen“ wird geöffnet.
  - e Klicken Sie auf **vCenter-Gruppe festlegen (Specify a vCenter group)** und geben Sie unter **Gruppe (Group)** den Gruppennamen neteng@corp.local ein.
  - f Klicken Sie auf **Weiter (Next)**.
  - g Klicken Sie unter „Rollen auswählen“ auf **NSX Administrator** und klicken Sie anschließend auf **Weiter (Next)**.
- 2 Gewähren Sie Sarah Zugriffsrechte auf das Datacenter.
  - a Klicken Sie auf das Startseiten-Symbol und klicken Sie anschließend auf **vCenter-Home (vCenter Home) > Datacenter (Datacenters)**.
  - b Wählen Sie ein Datacenter aus und klicken Sie auf **Aktionen (Actions) > Alle vCenter-Aktionen (All vCenter Actions) > Berechtigung hinzufügen (Add Permission)**.
  - c Klicken Sie auf **Hinzufügen (Add)** und wählen Sie die Domäne CORP aus.
  - d Wählen Sie unter **Benutzer und Gruppen (Users and Groups)** die Option **Gruppen zuerst anzeigen (Show Groups First)** aus.
  - e Wählen Sie „NetEng“ aus, und klicken Sie auf **OK**.

- f Wählen Sie unter **Zugewiesene Rolle (Assigned Role)** die Option **Nur Lesen (Read-only)** aus, deaktivieren Sie **An untergeordnete Objekte weitergeben (Propagate to children)** und klicken Sie anschließend auf **OK**.
- 3 Melden Sie sich beim vSphere Web Client ab und als „smaier@corp.local“ wieder an.

Sarah kann nur NSX-Vorgänge ausführen. Beispiele hierfür sind das Installieren von virtuellen Appliances, das Erstellen von logischen Switches usw.

## Beispiel: Berechtigungen durch eine Mitgliedschaft in einer Benutzergruppe vererben

Gruppenoption	Wert
Name	G1
Zugewiesene Rolle	Auditor (schreibgeschützt)
Ressourcen	Global Root

Benutzeroption	Wert
Name	Peter
Gehört zur Gruppe	G1
Zugewiesene Rolle	Keine

Peter gehört der Gruppe G1 an, der die Rolle „Auditor“ zugewiesen wurde. Peter übernimmt die Gruppenrolle und die Ressourcenberechtigungen.

## Beispiel: Szenario eines Benutzers, der Mitglied von mehreren Gruppen ist

Gruppenoption	Wert
Name	G1
Zugewiesene Rolle	Auditor (schreibgeschützt)
Ressourcen	Global Root

Gruppenoption	Wert
Name	G2
Zugewiesene Rolle	Sicherheitsadministrator (Lesen und Schreiben)
Ressourcen	Datacenter1

Benutzeroption	Wert
Name	Paul
Gehört zur Gruppe	G1, G2
Zugewiesene Rolle	Keine

Paul gehört den Gruppen G1 und G2 an und übernimmt eine Kombination von Rechten und Berechtigungen der Rollen „Auditor“ und „Sicherheitsadministrator“. Peter verfügt beispielsweise über folgende Berechtigungen:

- Lesen, Schreiben (Rolle „Sicherheitsadministrator“) für Datacenter1
- Nur Lesen (Auditor) für Global Root

## Beispiel: Szenario eines Benutzers, der Mitglied von mehreren Rollen ist

Gruppenoption	Wert
Name	G1
Zugewiesene Rolle	Enterprise-Administrator
Ressourcen	Global Root

Benutzeroption	Wert
Name	Florian
Gehört zur Gruppe	G1
Zugewiesene Rolle	Sicherheitsadministrator (Lesen und Schreiben)
Ressourcen	Datacenter1

Florian wurde die Rolle „Sicherheitsadministrator“ zugewiesen, sodass er die Rollenberechtigungen der Gruppe nicht übernimmt. Florian verfügt über folgende Berechtigungen

- Lesen, Schreiben (Rolle „Sicherheitsadministrator“) für Datacenter1 und dessen untergeordnete Ressourcen
- Die Rolle „Enterprise-Administrator“ für Datacenter1

## Erstellen eines Benutzers mit Zugriff auf die Web-Benutzeroberfläche mithilfe der Befehlszeilenschnittstelle

Sie können mithilfe der Befehlszeilenschnittstelle (CLI) einen NSX-Benutzer erstellen, der über einen Zugriff auf die Web-Benutzeroberfläche verfügt. Sie haben die Möglichkeit, dieses Benutzerkonto für den Zugriff auf unterschiedliche Plug-Ins und für deren Anwendung oder für Überwachungszwecke zu verwenden.

### Verfahren

- 1 Erstellen Sie ein CLI-Benutzerkonto. Sie können ein CLI-Benutzerkonto für jede virtuelle NSX-Appliance erstellen. Für die Erstellung eines CLI-Benutzerkontos führen Sie die folgenden Schritte aus:
  - a Melden Sie sich bei vSphere Web Client an und wählen Sie eine virtuelle NSX Manager-Appliance aus.
  - b Klicken Sie auf die Registerkarte **Konsole (Console)**, um eine CLI-Sitzung zu öffnen.

- c Melden Sie sich bei der CLI-Sitzung mit dem Administratorkonto und dem Kennwort an, das Sie bei der Installation von NSX Manager angegeben haben. Beispiel:

```
nsx-mgr> enable
Password:
nsx-mgr>
```

- d Wechseln Sie mithilfe des Befehls `enable` vom Basismodus in den privilegierten Modus wie im Folgenden dargestellt:

```
nsx-mgr> enable
Password:
nsx-mgr#
```

- e Wechseln Sie mithilfe des Befehls `configure terminal` vom privilegierten Modus in den Konfigurationsmodus wie im Folgenden dargestellt:

```
nsx-mgr# configure terminal
nsx-mgr(config)#
```

- f Fügen Sie mithilfe des Befehls `user username password (hash | plaintext) password` ein CLI-Benutzerkonto hinzu. Beispiel:

```
nsx-mgr(config)# user cliuser password plaintext abcd1234
```

---

**Hinweis** Benutzernamen mit Großbuchstaben sind nicht zulässig.

---

- g Speichern Sie die Konfiguration wie folgt:

```
nsx-mgr(config)# write memory
Configuration saved
[OK]
```

- 2** Erteilen Sie jetzt eine Berechtigung für die Web-Benutzeroberfläche, die dem Benutzer die Möglichkeit gibt, sich bei der virtuellen NSX Manager-Appliance anzumelden und REST-APIs zur Appliance-Verwaltung wie folgt auszuführen:

- a Stellen Sie mit folgendem Befehl sicher, dass Sie sich im Konfigurationsmodus befinden:

```
nsx-mgr# configure terminal
nsx-mgr(config)#
```

- b Ermöglichen Sie dem erstellten CLI-Benutzer die Ausführung von REST-API-Aufrufen mithilfe des Befehls `user username privilege web-interface`. Beispiel:

```
nsx-mgr(config)# user userName privilege web-interface

nsx-mgr(config)# user cliuser privilege web-interface
```

### 3 (Optional) Sie können die ausgeführte Konfiguration wie folgt überprüfen:

```
nsx-mgr# show running-config
Building configuration...

Current configuration:
!
user cliuser
!
ntp server 192.168.110.1
!
ip name server 192.168.110.10
!
hostname nsxmgr-01a
!
interface mgmt
 ip address 192.168.110.15/24
!
 ip route 0.0.0.0/0 192.168.110.1
!
web-manager
```

### 4 Beenden Sie die CLI-Sitzung.

```
nsx-mgr#(config)# exit
nsx-mgr# exit
```

Der erstellte Benutzer ist nicht auf der Registerkarte unter **Networking & Security > NSX-Manager (NSX Managers)**, „**NSX Manager auswählen**“ (**“Select your NSX Manager”**) > **Verwalten (Manage)** > **Benutzer (Users)** aufgeführt. Dem Benutzer wurde auch keine Rolle zugewiesen.

### 5 Weisen Sie dem Benutzer mithilfe der REST-API die erforderliche Rolle zu. Sie können die Rollen auditor (Prüfer), security\_admin (Sicherheitsadministrator) oder super\_user (Systemadministrator) wie folgt zuweisen:

```
POST - https://<NSX-IP>/api/2.0/services/usermgmt/role/<username>?isCli=true
<accessControlEntry>
<role>auditor</role> # Enter the required role #
<resource>
<resourceId>globalroot-0</resourceId>
</resource>
</accessControlEntry>
```

#### Ergebnisse

Der NSX-CLI-Benutzer wird mit der Möglichkeit des Zugriffs auf die Web-Benutzerschnittstelle erstellt.

#### Nächste Schritte

Sie können sich bei vSphere Web Client mithilfe der beim Erstellen des Benutzers eingegebenen Anmeldedaten anmelden.

Weitere Informationen zur Befehlszeilenschnittstelle CLI finden Sie im Dokument *Befehlszeilenschnittstellen-Referenz zu NSX*.

Weitere Informationen zur API finden Sie im Dokument *Handbuch zu NSX-API*.

## Bearbeiten eines Benutzerkontos

Sie können ein Benutzerkonto bearbeiten, um das Kennwort oder den Gültigkeitsbereich zu ändern. Das **admin**-Konto kann nicht bearbeitet werden.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte „Name“ auf einen NSX Manager und anschließend auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf **Benutzer (Users)**.
- 5 Wählen Sie den Benutzer aus, den Sie bearbeiten möchten.
- 6 Klicken Sie auf **Bearbeiten (Edit)**.
- 7 Nehmen Sie die gewünschten Änderungen vor.
- 8 Klicken Sie auf **Beenden (Finish)**, um Ihre Änderungen zu speichern.

## Ändern einer Benutzerrolle

Sie können die Rollenzuweisung für alle Benutzer ändern mit Ausnahme des **admin**-Benutzers.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte „Name“ auf einen NSX Manager und anschließend auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf **Benutzer (Users)**.
- 5 Wählen Sie den Benutzer aus, für den Sie die Rolle ändern möchten.
- 6 Klicken Sie auf **Rolle ändern (Change Role)**.
- 7 Nehmen Sie die gewünschten Änderungen vor.
- 8 Klicken Sie auf **Beenden (Finish)**, um Ihre Änderungen zu speichern.

## Deaktivieren oder Aktivieren eines Benutzerkontos

Sie können ein Benutzerkonto deaktivieren, um den entsprechenden Benutzer daran zu hindern, sich bei NSX Manager anzumelden. Den Benutzer **admin** oder einen Benutzer, der aktuell bei NSX Manager angemeldet ist, können Sie nicht deaktivieren.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte „Name“ auf einen NSX Manager und anschließend auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf **Benutzer (Users)**.
- 5 Wählen Sie ein Benutzerkonto aus.
- 6 Klicken Sie auf eines der Symbole **Aktivieren (Enable)** oder **Deaktivieren (Disable)**.

## Löschen eines Benutzerkontos

Sie können jedes erstellte Benutzerkonto löschen. Das **admin**-Konto kann nicht gelöscht werden. Überwachungsdatensätze für gelöschte Benutzer werden in der Datenbank verwaltet und können in einem Überwachungsprotokollbericht referenziert werden.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte „Name“ auf einen NSX Manager und anschließend auf die Registerkarte **Verwalten (Manage)**.
- 4 Klicken Sie auf **Benutzer (Users)**.
- 5 Wählen Sie ein Benutzerkonto aus.
- 6 Klicken Sie auf **Löschen (Delete)**.
- 7 Klicken Sie auf **OK**, um den Löschvorgang zu bestätigen.

Wenn Sie ein vCenter-Benutzerkonto löschen, wird nur die Rollenzuweisung für NSX Manager gelöscht. Das Benutzerkonto auf vCenter wird nicht gelöscht.

# Netzwerk- und Sicherheitsobjekte

# 21

In diesem Abschnitt werden benutzerdefinierte Netzwerk- und Sicherheits-Container beschrieben. Diese Container können in der verteilten Firewall und in Service Composer genutzt werden. In einer Cross-vCenter NSX-Umgebung können Sie universelle Netzwerk- und Sicherheits-Container erstellen, die in den universellen Regeln für die verteilte Firewall verwendet werden. In Service Composer können Sie keine universellen Netzwerk- und Sicherheitsobjekte verwenden.

---

**Hinweis** Doppelte Namen sind zulässig, wenn Sie eine Gruppe mit universellem Geltungsbereich erstellen. Sie können doppelte Namen angeben, wenn Sie die Option **Dieses Objekt für globale Synchronisierung markieren (Mark this object for Universal Synchronization)** beim Erstellen der folgenden Gruppen auswählen:

- IP-Adressgruppe
- MAC-Adressgruppe
- Sicherheitsgruppe
- Dienste und Dienstgruppe

---

Dieses Kapitel enthält die folgenden Themen:

- [Arbeiten mit IP-Adressgruppen](#)
- [Arbeiten mit MAC-Adressgruppen](#)
- [Arbeiten mit IP-Pools](#)
- [Arbeiten mit Sicherheitsgruppen](#)
- [Arbeiten mit Diensten und Dienstgruppen](#)

## Arbeiten mit IP-Adressgruppen

### Erstellen einer IP-Adressgruppe

Sie können eine IP-Adressgruppe erstellen und anschließend diese Gruppe als Quelle oder Ziel zu einer Firewallregel hinzufügen. Eine solche Regel kann physische Maschinen vor virtuellen Maschinen schützen oder umgekehrt.

## Voraussetzungen

VMware Tools muss auf jeder virtuellen Maschine installiert sein oder es muss eine aktivierte IP-Erkennungsmethode (DHCP-Snooping und/oder ARP-Snooping) eingerichtet sein, wenn gruppierte Objekte anstelle von IP-Adressen verwendet werden. Weitere Informationen finden Sie unter [IP-Erkennung für virtuelle Maschinen](#).

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler IP-Adressengruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und dann auf **IP Set (IP Sets)**.
- 5 Klicken Sie auf das Symbol **Hinzufügen** (+).
- 6 Geben Sie einen Namen für die Adressgruppe ein.
- 7 (Optional) Geben Sie eine Beschreibung für die Adressgruppe ein.
- 8 Geben Sie die IP-Adressen oder einen Bereich von IP-Adressen ein, die zur Gruppe hinzugefügt werden sollen.

---

**Vorsicht** Stellen Sie bei der Eingabe von IPv6-Adressbereichen in den IP-Sätzen sicher, dass die Adressbereiche in /64 unterteilt sind. Andernfalls schlägt die Veröffentlichung der Firewallregeln fehl.

---


- 9 (Optional) Wählen Sie **Vererbung aktivieren, um die Sichtbarkeit auf zugrunde liegenden Geltungsbereichen zuzulassen**.
- 10 (Optional) Wählen Sie **Dieses Objekt für globale Synchronisierung markieren**, um eine globale IP-Adressengruppe zu erstellen.
- 11 Klicken Sie auf **OK**.

## Bearbeiten einer IP-Adressgruppe

### Voraussetzungen


### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.

- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler IP-Adressengruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten** und dann auf **IP-Sätze**.
- 5 Wählen Sie die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- 6 Nehmen Sie im Dialogfeld „IP Set bearbeiten“ die entsprechenden Änderungen vor.
- 7 Klicken Sie auf **OK**.

## Löschen einer IP-Adressgruppe

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler IP-Adressengruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und dann auf **IP Set (IP Sets)**.
- 5 Wählen Sie die Gruppe aus, die Sie löschen möchten, und klicken Sie auf das Symbol **Löschen (Delete)** ().

## Arbeiten mit MAC-Adressgruppen

### Erstellen einer MAC-Adressgruppe

Sie können eine MAC-Adressgruppe mit einem Bereich von MAC-Adressen erstellen und diese Gruppe als Quelle oder Ziel einer Regel für die verteilte Firewall hinzufügen. Eine solche Regel kann physische Maschinen vor virtuellen Maschinen schützen oder umgekehrt.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.

- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler MAC-Adressengruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und anschließend auf **MAC Set (MAC Sets)**.
- 5 Klicken Sie auf das Symbol **Hinzufügen (+)**.
- 6 Geben Sie einen Namen für die Adressgruppe ein.
- 7 (Optional) Geben Sie eine Beschreibung für die Adressgruppe ein.
- 8 Geben Sie die MAC-Adressen ein, die zur Gruppe hinzugefügt werden sollen.
- 9 (Optional) Wählen Sie **Vererbung aktivieren, um die Sichtbarkeit auf zugrunde liegenden Geltungsbereichen zuzulassen**.
- 10 (Optional) Wählen Sie **Dieses Objekt für globale Synchronisierung markieren**, um eine globale MAC-Adressengruppe zu erstellen.
- 11 Klicken Sie auf **OK**.

## Bearbeiten einer MAC-Adressgruppe

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler MAC-Adressengruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und anschließend auf **MAC Set (MAC Sets)**.
- 5 Wählen Sie die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie auf das Symbol **Bearbeiten (Edit) (✎)**.
- 6 Nehmen Sie im Dialogfeld „MAC Set bearbeiten“ die entsprechenden Änderungen vor.
- 7 Klicken Sie auf **OK**.

## Löschen einer MAC-Adressgruppe

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler MAC-Adressengruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und anschließend auf **MAC Set (MAC Sets)**.
- 5 Wählen Sie die Gruppe aus, die Sie löschen möchten, und klicken Sie auf das Symbol **Löschen (Delete)** (✖).

## Arbeiten mit IP-Pools

Sie können einen IP-Pool für die Angabe eines Bereichs von IP-Adressen erstellen.

### Erstellen eines IP-Pools

#### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und klicken Sie auf **IP-Pool (IP Pool)**.
- 5 Klicken Sie auf das Symbol **Neuen IP-Pool hinzufügen (Add New IP Pool)**.
- 6 Geben Sie einen Namen für den IP-Pool ein und geben Sie das Standard-Gateway sowie die Präfixlänge an.
- 7 (Optional) Geben Sie den primären und den sekundären DNS sowie das DNS-Suffix ein.
- 8 Geben Sie die IP-Adressbereiche ein, die in den Pool eingeschlossen werden sollen, und klicken Sie auf **OK**.

### Bearbeiten eines IP-Pools

Sie können einen IP-Pool, jedoch nicht CIDR oder das Gateway bearbeiten.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und anschließend auf **IP-Pools (IP Pools)**.
- 5 Wählen Sie einen IP-Pool aus und klicken Sie auf das Symbol **Bearbeiten (Edit)**.
- 6 Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **OK**.

## Löschen eines IP-Pools

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und klicken Sie auf **IP-Pool (IP Pool)**.
- 5 Wählen Sie den IP-Pool aus, den Sie löschen möchten, und klicken Sie auf das Symbol **Löschen (Delete)**.

## Arbeiten mit Sicherheitsgruppen

Eine Sicherheitsgruppe ist eine Sammlung von Assets oder Gruppierungsobjekten aus Ihrer vSphere-Bestandsliste.

Sicherheitsgruppen sind Container, die mehrere Objekttypen enthalten können, einschließlich logischer Switches, vNICs, IPsets und virtueller Maschinen (VM). Sicherheitsgruppen können dynamische Mitgliedschaftskriterien aufweisen, die auf Sicherheits-Tags, dem VM-Namen oder dem Namen logischer Switches basieren. Beispielsweise werden alle VMs mit dem Sicherheits-Tag „web“ automatisch einer speziellen Sicherheitsgruppe für Webserver hinzugefügt. Nach dem Erstellen einer Sicherheitsgruppe wird auf diese Gruppe eine Sicherheitsrichtlinie angewendet.

In einer Cross-vCenter NSX-Umgebung sind auf dem primären NSX Manager universelle Sicherheitsgruppen definiert, die für die globale Synchronisierung mit sekundären NSX Managern markiert werden. Für universelle Sicherheitsgruppen können keine dynamischen Mitgliedschaftskriterien definiert werden, sofern sie nicht für die Verwendung in einem aktiven Standby-Bereitstellungsszenario markiert sind.

In einer Cross-vCenter NSX-Umgebung mit aktivem Standby-Bereitstellungsszenario erstellt der SRM für jede geschützte VM auf der aktiven Site eine Platzhalter-VM auf der Wiederherstellungs-Site. Die Platzhalter-VMs sind nicht aktiv und bleiben im Standby-Modus. Wenn die geschützte VM deaktiviert wird, werden die Platzhalter-VMs auf der Wiederherstellungs-Site hochgefahren, und sie übernehmen dann die Aufgaben der geschützten VM. Benutzer erstellen Regeln für die verteilte Firewall mit universellen Sicherheitsgruppen, die universelle Sicherheits-Tags auf der aktiven Site enthalten. Der NSX Manager repliziert die Regel für die verteilte Firewall mit den universellen Sicherheitsgruppen, in denen die universellen Sicherheits-Tags enthalten sind, auf den Platzhalter-VMs. Beim Hochfahren der Platzhalter-VMs werden die replizierten Firewallregeln mit den universellen Sicherheitsgruppen und den universellen Sicherheits-Tags korrekt durchgesetzt.

---

### Hinweis

- Vor Version 6.3 erstellte universelle Sicherheitsgruppen können nicht für die Verwendung in aktiven Standby-Bereitstellungen bearbeitet werden.
- 

## Erstellen einer Sicherheitsgruppe

Sie erstellen eine Sicherheitsgruppe (Security Group) auf der NSX Manager-Ebene.

Globale Sicherheitsgruppen werden in zwei Bereitstellungstypen verwendet: Aktiv/Aktiv-Cross-vCenter-NSX-Umgebungen und Aktiv/Standby-Cross-vCenter NSX-Umgebungen, in denen eine Site zu einem bestimmten Zeitpunkt aktiv ist, während sich die anderen Sites in Standby befinden.

- Globale Sicherheitsgruppen in einer Aktiv/Aktiv-Umgebung können nur die folgenden eingeschlossenen Objekte enthalten: Sicherheitsgruppen, IP Sets, MAC Sets. Sie können keine dynamische Mitgliedschaft oder ausgeschlossene Objekte konfigurieren.
- Globale Sicherheitsgruppen in einer Aktiv/Standby-Umgebung können die folgenden eingeschlossenen Objekte enthalten: Sicherheitsgruppen, IP Sets, MAC Sets, globalen Sicherheits-Tags. Sie können auch eine dynamische Mitgliedschaft mithilfe des VM-Namens konfigurieren. Ausgeschlossene Objekte können nicht konfiguriert werden.

---

**Hinweis** Vor Version 6.3 erstellte universelle Sicherheitsgruppen können nicht für die Verwendung in aktiven Standby-Bereitstellungen bearbeitet werden.

---

### Voraussetzungen

Wenn Sie eine auf Active Directory-Gruppenobjekten basierende Sicherheitsgruppe erstellen, stellen Sie sicher, dass mindestens eine Domäne bei NSX Manager registriert ist. NSX Manager ruft Gruppen- und Benutzerinformationen sowie die Beziehung zwischen diesen aus jeder Domäne ab, die bei NSX Manager registriert ist. Weitere Informationen dazu finden Sie unter [Registrieren einer Windows-Domäne mit NSX Manager](#).

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.

- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler Sicherheitsgruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** auf **Sicherheitsgruppe (Security Group)** und dann auf das Symbol **Security Group hinzufügen (Add Security Group)**.
- 5 Geben Sie einen Namen und optional eine Beschreibung für die Sicherheitsgruppe ein.
- 6 (Optional) Wenn Sie eine universelle Sicherheitsgruppe erstellen, wählen Sie **Dieses Objekt für globale Synchronisierung markieren (Mark this object for universal synchronization)** aus.
- 7 (Optional) Wenn Sie eine universelle Sicherheitsgruppe für eine aktive Standby-Bereitstellung erstellen, wählen Sie **Dieses Objekt für globale Synchronisierung markieren (Mark this object for universal synchronization)** und **Für aktive Standby-Bereitstellungen verwenden (Use for active standby deployments)** aus. Die dynamische Mitgliedschaft für universelle Sicherheitsgruppen mit aktiver Standby-Bereitstellung basiert auf dem Namen der virtuellen Maschine.
- 8 Klicken Sie auf **Weiter (Next)**.
- 9 Definieren Sie auf der Seite „Dynamische Mitgliedschaft“ die Kriterien, die ein Objekt erfüllen muss, bevor es zur von Ihnen erstellten Sicherheitsgruppe hinzugefügt werden kann. Dies hilft Ihnen dabei, virtuelle Maschinen aufzunehmen, indem Sie die Filterkriterien mit einer Anzahl an unterstützen Parametern zur Übereinstimmung mit den Suchkriterien definieren.

**Hinweis** Wenn Sie eine globale Sicherheitsgruppe erstellen, ist der Schritt **Dynamische Mitgliedschaft definieren (Define dynamic membership)** in Aktiv/Aktiv-Umgebungen nicht verfügbar. Er steht nur in Aktiv/Standby-Bereitstellungen auf der Basis des Namens der virtuellen Maschine zur Verfügung.

Beispielsweise können Sie ein Kriterium definieren, nach dem alle virtuellen Maschinen mit einem bestimmten Sicherheits-Tag (wie AntiVirus.virusFound) zu der Sicherheitsgruppe hinzugefügt werden. Bei Sicherheits-Tags wird die Groß- und Kleinschreibung berücksichtigt.

Sie können aber auch alle virtuellen Maschinen zur Sicherheitsgruppe hinzufügen, die den Namen W2008 enthalten, sowie virtuelle Maschinen, die sich im logischen Switch global\_wire befinden.

- 10 Klicken Sie auf **Weiter (Next)**.

- 11 Wählen Sie auf der Seite „Einzubeziehende Objekte auswählen“ die Registerkarte der Ressource, die Sie hinzufügen möchten, und wählen Sie eine oder mehrere Ressourcen aus, die zur Sicherheitsgruppe hinzugefügt werden sollen. Sie können die folgenden Objekte zu einer Sicherheitsgruppe hinzufügen:

**Tabelle 21-1. Objekte, die in Sicherheitsgruppen und universellen Sicherheitsgruppen hinzugefügt werden können.**

Sicherheitsgruppe	Universelle Sicherheitsgruppe
<ul style="list-style-type: none"> <li>■ Andere Sicherheitsgruppen, die innerhalb der von Ihnen erstellten Sicherheitsgruppe verschachtelt werden sollen.</li> <li>■ Cluster</li> <li>■ Logischer Switch</li> <li>■ Netzwerk</li> <li>■ Virtuelle App</li> <li>■ Datencenter</li> <li>■ IP Set</li> <li>■ Verzeichnisgruppen</li> </ul>	<ul style="list-style-type: none"> <li>■ Andere universelle Sicherheitsgruppen, die innerhalb der von Ihnen erstellten universellen Sicherheitsgruppe verschachtelt werden sollen.</li> <li>■ Universelle IP Set</li> <li>■ Universelle MAC Set</li> <li>■ Globaler Sicherheits-Tag (nur Aktiv/Standby-Bereitstellungen)</li> </ul>
<p><b>Hinweis</b> Die Active Directory-Konfiguration für NSX-Sicherheitsgruppen unterscheidet sich von der AD-Konfiguration für vSphere SSO. Die AD-Gruppenkonfiguration für NSX ist für Endbenutzer bestimmt, die auf virtuelle Gastmaschinen zugreifen, während die Konfiguration für vSphere SSO für Administratoren bestimmt ist, die vSphere und NSX verwenden. Damit diese Verzeichnisgruppen verwendet werden können, müssen sie mit Active Directory synchronisiert werden. Weitere Informationen dazu finden Sie unter <a href="#">Kapitel 11 Überblick über die identitätsbasierte Firewall (IDFW)</a>.</p>	
<ul style="list-style-type: none"> <li>■ MAC Set</li> <li>■ Sicherheits-Tag</li> <li>■ vNIC</li> <li>■ Virtuelle Maschine</li> <li>■ Ressourcenpool</li> <li>■ Verteilte virtuelle Portgruppe</li> </ul>	

Die hier ausgewählten Objekte sind immer in der Sicherheitsgruppe eingeschlossen, unabhängig davon, ob die Kriterien in [Schritt 8](#) erfüllt werden.

Wenn Sie einer Sicherheitsgruppe eine Ressource hinzufügen, werden automatisch auch alle zugewiesenen Ressourcen hinzugefügt. Wenn Sie beispielsweise eine virtuelle Maschine auswählen, wird die zugewiesene vNIC automatisch zur Sicherheitsgruppe hinzugefügt.

- 12 Klicken Sie auf **Weiter (Next)** und wählen Sie die Objekte aus, die Sie aus der Sicherheitsgruppe ausschließen möchten.

**Hinweis** Wenn Sie eine universelle Sicherheitsgruppe erstellen, ist der Schritt **Auszuschließende Objekte auswählen** nicht verfügbar.

Die hier ausgewählten Objekte sind immer aus der Sicherheitsgruppe ausgeschlossen, unabhängig davon, ob die Kriterien für die dynamische Mitgliedschaft erfüllt werden.

**13** Klicken Sie auf **Weiter (Next)**.

Das Fenster **Bereit zum Abschließen (Ready to Complete)** mit einer Übersicht über die Sicherheitsgruppe wird angezeigt.

**14** Klicken Sie auf **Beenden (Finish)**.

### Beispiel

Die Mitgliedschaft in einer Sicherheitsgruppe richtet sich nach Folgendem:

{Ergebnis des Ausdrucks (abgeleitet von **Dynamische Mitgliedschaft definieren (Define dynamic membership)**) + Einschlüsse (angegeben in **Einzubeziehende Objekte auswählen (Select objects to include)**) – Ausschluss (angegeben in **Auszuschließende Objekte auswählen (Select objects to exclude)**)}

Dies bedeutet, dass die Einbeziehungsobjekte zuerst zum Ergebnis des Ausdrucks hinzugefügt werden. Ausschlussobjekte werden dann vom kombinierten Ergebnis subtrahiert.

## Bearbeiten einer Sicherheitsgruppe

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler Sicherheitsgruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und dann auf **Security Group**.
 

Beachten Sie, dass vor Version 6.3 erstellte universelle Sicherheitsgruppen nicht für die Verwendung in aktiven Standby-Bereitstellungen bearbeitet werden können.
- 5 Wählen Sie die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie auf das Symbol **Bearbeiten (Edit)** (✎).
- 6 Nehmen Sie im Dialogfeld „Security Group bearbeiten“ die entsprechenden Änderungen vor.
- 7 Klicken Sie auf **OK**.

## Löschen einer Sicherheitsgruppe

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler Sicherheitsgruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und dann auf **Security Group**.
- 5 Wählen Sie die Gruppe aus, die Sie löschen möchten, und klicken Sie auf das Symbol **Löschen (Delete)** (✖).

## Arbeiten mit Diensten und Dienstgruppen

Bei einem Dienst handelt es sich um die Kombination aus Protokoll und Port; eine Dienstgruppe ist eine Gruppe von Diensten oder von anderen Dienstgruppen.

### Erstellen eines Diensts

Sie können einen Dienst erstellen und anschließend Regeln für diesen Dienst definieren.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler Dienste müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und anschließend auf **Dienst (Service)**.
- 5 Klicken Sie auf das Symbol **Hinzufügen** (+).
- 6 Geben Sie im Feld **Name** einen Namen ein, um den Dienst zu identifizieren.
- 7 (Optional) Geben Sie im Feld **Beschreibung (Description)** eine Beschreibung für den Dienst ein.
- 8 Wählen Sie ein **Protokoll (Protocol)** aus.
  - a Je nach ausgewähltem Protokoll werden Sie möglicherweise aufgefordert, weitere Informationen wie beispielsweise einen Zielport einzugeben.
- 9 (Optional) Wählen Sie **Vererbung aktivieren, um die Sichtbarkeit auf zugrunde liegenden Geltungsbereichen zuzulassen**.

- 10 (Optional) Wählen Sie **Dieses Objekt für globale Synchronisierung markieren**, um einen globalen Dienst zu erstellen.
- 11 Klicken Sie auf **OK**.

### Ergebnisse

Der Dienst wird in der Tabelle „Dienste“ angezeigt.

## Erstellen einer Dienstgruppe

Sie können eine Dienstgruppe erstellen und dann Regeln für diese Dienstgruppe definieren.

### Verfahren


- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler Dienstgruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und dann auf **Dienstgruppen (Service Groups)**.
- 5 Klicken Sie auf das Symbol **Hinzufügen (Add)**.
- 6 Geben Sie im Feld **Name** einen Namen ein, um die Dienstgruppe zu identifizieren.
- 7 (Optional) Geben Sie im Feld **Beschreibung (Description)** eine Beschreibung für die Dienstgruppe ein.
- 8 (Optional) Wählen Sie **Dieses Objekt für globale Synchronisierung markieren**, um eine globale Dienstgruppe zu erstellen.
- 9 Wählen Sie unter „Mitglieder“ die Dienste oder Dienstgruppen aus, die Sie der Gruppe hinzufügen möchten.
- 10 (Optional) Wählen Sie **Vererbung aktivieren, um die Sichtbarkeit auf zugrunde liegenden Geltungsbereichen zuzulassen**.
- 11 Klicken Sie auf **OK**.

## Bearbeiten eines Diensts oder einer Dienstgruppe

Sie können Dienste und Dienstgruppen bearbeiten.

### Verfahren


- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.

- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler Dienste oder Dienstgruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und dann auf **Dienst (Service)** oder **Dienstgruppen (Service Groups)**.
- 5 Wählen Sie einen benutzerdefinierten Dienst oder eine benutzerdefinierte Dienstgruppe aus und klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- 6 Nehmen Sie die entsprechenden Änderungen vor.
- 7 Klicken Sie auf **OK**.

## Löschen eines Diensts oder einer Dienstgruppe

Sie können Dienste und Dienstgruppen löschen.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Manager und klicken Sie dann auf die Registerkarte **Verwalten**.
  - ◆ Zur Verwaltung globaler Dienste oder Dienstgruppen müssen Sie den primären NSX Manager auswählen.
- 4 Klicken Sie auf die Registerkarte **Gruppieren von Objekten (Grouping Objects)** und dann auf **Dienst (Service)** oder **Dienstgruppen (Service Groups)**.
- 5 Wählen Sie einen benutzerdefinierten Dienst oder eine benutzerdefinierte Dienstgruppe aus und klicken Sie auf das Symbol **Löschen (Delete)** ().
- 6 Klicken Sie auf **Ja (Yes)**.

Der Dienst bzw. die Dienstgruppe wird gelöscht.

Dieses Kapitel enthält die folgenden Themen:

- [Verwenden des NSX-Dashboard](#)
- [Überprüfen des Kommunikationskanalstatus](#)
- [NSX Controller](#)
- [Ändern des VXLAN-Ports](#)
- [Programm zur Verbesserung der Benutzerfreundlichkeit](#)
- [Grundlegendes zu NSX-Protokollen](#)
- [Überwachungsprotokolle](#)
- [Systemereignisse](#)
- [Einstellungen für das Managementsystem](#)
- [Sichern und Wiederherstellen von NSX](#)
- [Flow Monitoring](#)
- [Application Rule Manager](#)
- [Activity Monitoring](#)
- [Datenerfassung für die Endpunktüberwachung](#)
- [Traceflow](#)

## Verwenden des NSX-Dashboard

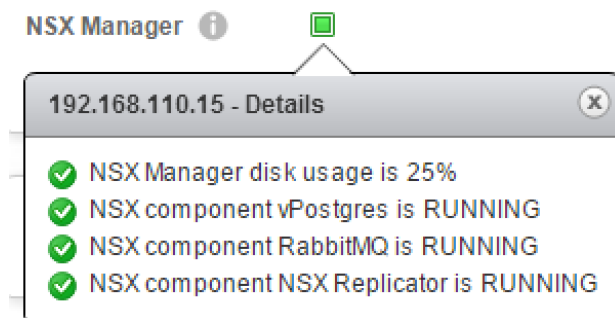
Das NSX-Dashboard bietet Transparenz des allgemeinen Systemzustands von NSX-Komponenten in einer zentralen Ansicht. Das NSX-Dashboard vereinfacht die Fehlerbehebung, weil es den Status der unterschiedlichen NSX-Komponenten anzeigt, z. B. von NSX Manager-Controllern, logischen Switches, der Hostvorbereitung, Dienstbereitstellung, von Sicherungen und Edge-Benachrichtigungen.

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Dashboard**. Die Dashboard-Seite wird angezeigt.

- 3 Wählen Sie in einer Cross-vCenter NSX-Umgebung NSX Manager mit primärer oder sekundärer Rolle aus.

Dashboard stellt folgende Informationen bereit:

- NSX-Infrastruktur – Der NSX Manager-Komponentenstatus für die folgenden Dienste wird überwacht:
  - Datenbank-Dienst (vPostgres).
  - Nachrichtenbus-Dienst (RabbitMQ).
  - Replikator-Dienst – auch für die Überwachung im Hinblick auf Replizierungsfehler zuständig (falls Cross-vCenter NSX aktiviert ist).
  - NSX Manager-Festplattennutzung:
    - Gelb zeigt eine Festplattennutzung von > 80 % an.
    - Rot zeigt eine Festplattennutzung von > 90 % an.



- NSX-Infrastruktur – NSX Controller-Status:
  - Status des Controller-Knotens (verfügbar/nicht verfügbar/wird ausgeführt/wird bereitgestellt/wird entfernt/ausgefallen/unbekannt).
  - Der Konnektivitätsstatus vom Controller-Peer wird angezeigt. Wenn der Controller nicht verfügbar ist und in roter Farbe angezeigt wird, werden die Peer-Controller in gelber Farbe angezeigt.
  - Controller-VM-Status: ausgeschaltet/gelöscht.
  - Controller-Warnung für Festplattenlatenz.



- NSX Manager-Sicherungsstatus:
  - Sicherungszeitplan.
  - Letzter Sicherungsstatus (fehlgeschlagen/erfolgreich/nicht geplant mit Datum und Uhrzeit).

- Letzter Sicherungsversuch (Datum und Uhrzeit mit Details).
- Letzte erfolgreiche Sicherung (Datum und Uhrzeit mit Details).

**Backup Status** ⓘ
 

Backup schedule:	✓	Daily at 14:50 hrs
Last backup status:	✗	Failed
Last backup attempt:	✗	10/18/2016 10:53:48 PM
Latest successful backup:	✓	10/18/2016 8:24:23 AM

**Backup Status** ⓘ
 

Backup schedule:	⚠	Not scheduled
Last backup status:	✓	Successful
Last backup attempt:	✓	10/18/2016 2:19:40 AM

- NSX-Infrastruktur – Der Hoststatus für die folgenden Dienste wird überwacht:
  - Zugehörige Bereitstellung:
    - Anzahl der Cluster mit gescheiterter Installation.
    - Anzahl der Cluster mit erforderlichem Upgrade.
    - Anzahl der Cluster mit aktuell durchgeführter Installation.
    - Anzahl der nicht vorbereiteten Cluster.
  - Firewall:
    - Anzahl der Cluster mit deaktivierter Firewall.
    - Anzahl der Cluster, bei denen der Firewallstatus gelb/rot ist:
      - Gelb bedeutet, dass die verteilte Firewall auf allen Clustern deaktiviert ist.
      - Rot bedeutet, dass die verteilte Firewall auf allen Hosts/Clustern nicht installiert werden konnte.
  - VXLAN:
    - Anzahl der Cluster mit nicht konfiguriertem VXLAN.
    - Anzahl der Cluster, bei denen der VXLAN-Status grün/gelb/rot ist:
      - Grün bedeutet, dass die Funktion erfolgreich konfiguriert wurde.
      - Gelb steht für beschäftigt, wenn die VXLAN-Konfiguration gerade durchgeführt wird.

- Rot (Fehler) weist darauf hin, dass die VTEP-Erstellung fehlgeschlagen ist, VTEP die IP-Adresse nicht finden konnte, VTEP eine *LinkLocal*-IP-Adresse zugewiesen bekam usw.
- NSX-Infrastruktur – Status der Dienstbereitstellung
  - Bereitstellungsfehler – Installationsstatus für fehlgeschlagene Bereitstellungen.
  - Dienststatus – für alle fehlgeschlagenen Dienste.

- NSX-Infrastruktur – NSX Edge-Benachrichtigungen:

Das Dashboard für Edge-Benachrichtigungen zeigt aktive Warnungen für bestimmte Dienste an. Es überwacht die Liste der unten aufgeführten kritischen Ereignisse und verfolgt sie nach, bis das Problem behoben ist. Die Warnungen werden automatisch aufgehoben, wenn ein Wiederherstellungsereignis gemeldet wird oder eine erzwungene Edge-Synchronisierung stattfindet oder das Edge erneut bereitgestellt oder aktualisiert wird.

- Load Balancer (Edge-Load-Balancer-Serverstatus):
  - Der Backend-Server des Edge-Load-Balancers ist nicht verfügbar.
  - Warnstatus des Backend-Servers des Edge-Load-Balancers.
- VPN (IPsec-Tunnel/IPsec-Kanalstatus):
  - Edge-IPsec-Kanal ist nicht verfügbar.
  - Edge-IPsec-Tunnel ist nicht verfügbar.
- Appliance (Edge-VM, Edge-Gateway, Edge-Dateisystem, NSX Manager und Berichtsstatus des Edge Services Gateway):
  - Beim Edge-Dienst-Gateway fehlt das Signal für die Prüfung des Systemzustands.
  - Die Edge-VM wurde ausgeschaltet.
  - Bei der Edge-VM fehlt das Signal für die Prüfung des Systemzustands.
  - NSX Edge meldet einen fehlerhaften Status.
  - NSX Manager meldet einen fehlerhaften Status für dieses Edge Services Gateway.
  - Edge-VM ist nicht in VC-Bestand vorhanden.

- Split-Brain-Situation bei Hochverfügbarkeit entdeckt.

**Hinweis** Load-Balancer- und VPN-Warnungen werden bei Konfigurationsaktualisierungen nicht automatisch aufgehoben. Wenn das Problem behoben ist, müssen Sie die Warnungen manuell aufheben. Nutzen Sie dafür die API mit dem Befehl `alarm-id`. Hier ist das Beispiel der API, die Sie zum Aufheben der Warnungen verwenden können. Genauere Informationen finden Sie unter *Handbuch zu NSX-API*.

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{source-Id}
POST https://<<NSX-IP>>/api/2.0/services/alarms?action=resolve

GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

- NSX-Dienste – Firewallveröffentlichungsstatus:
  - Anzahl an Hosts, bei denen der Veröffentlichungsstatus der Firewall „fehlgeschlagen“ lautet. Der Status wird in Rot angezeigt, wenn ein Host die veröffentlichte verteilte Firewallkonfiguration nicht erfolgreich anwendet.
- NSX-Dienste – Status des logischen Netzwerks:
  - Anzahl an logischen Switches mit dem Status Fehler oder Warnung.
  - Wird gekennzeichnet, wenn die gesicherte verteilte virtuelle Portgruppe vom vCenter Server entfernt wird.

## Überprüfen des Kommunikationskanalstatus

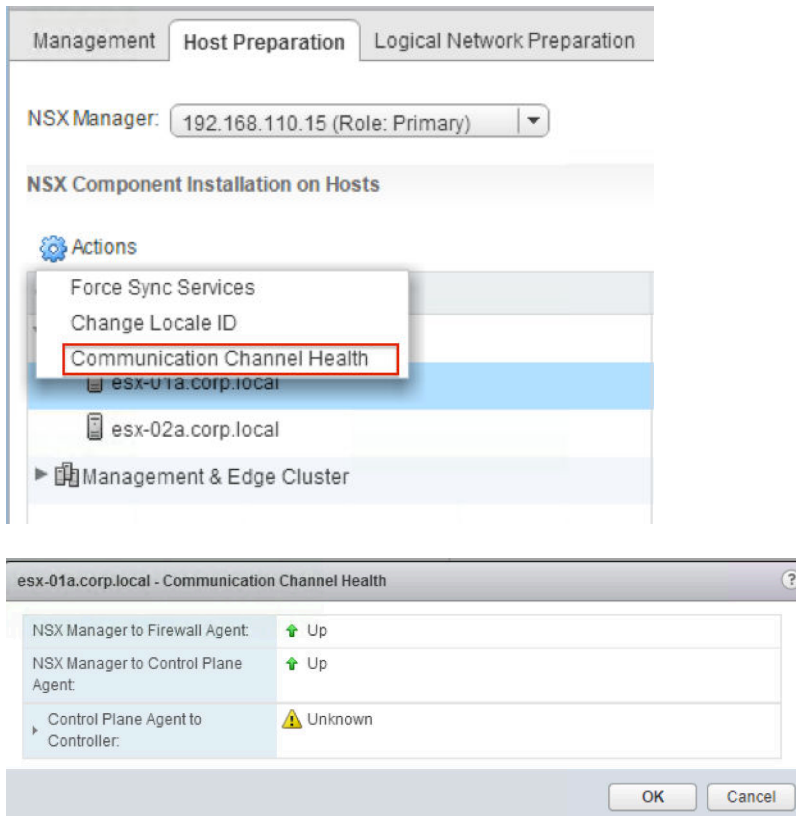
NSX überprüft den Status der Kommunikation zwischen NSX Manager und Firewallagent, NSX Manager und Steuerungskomponenten-Agent sowie Steuerungskomponenten-Agent und Controllern.

### Verfahren

- 1 Navigieren Sie im vSphere Web Client zu **Netzwerke & Sicherheit (Networking & Security) > Installation > Hostvorbereitung (Host Preparation)**.

- Wählen Sie einen Cluster aus oder erweitern Sie die Cluster und wählen Sie einen Host aus. Klicken Sie auf **Aktionen (Actions)** (⚙️) und dann auf **Kommunikationskanalstatus (Communication Channel Health)**.

Die Informationen zum Kommunikationskanalstatus werden angezeigt.



## NSX Controller

Sie können NSX Controller-Instanzen verwalten.

Informationen zur Behebung von Problemen mit dem Controller-Cluster, einschließlich zum sicheren Löschen von Controllern, finden Sie unter dem Abschnitt zu NSX Controller im *Fehlerbehebungshandbuch zu NSX*.

## Ändern des Controller-Kennworts

Um die Sicherheit zu gewährleisten, können Sie die Kennwörter für NSX Controller ändern.

### Verfahren

- Melden Sie sich beim vSphere Web Client an.
- Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.
- Wählen Sie unter „Verwaltung“ den Controller aus, dessen Kennwort Sie ändern möchten.

- 4 Klicken Sie auf **Aktionen (Actions)** und anschließend auf **Kennwort des Controller-Clusters ändern (Change Controller Cluster Password)**.
- 5 Geben Sie ein neues Kennwort ein und klicken Sie auf **OK**.

Das Controller-Kennwort wurde geändert.

## Herunterladen von technischen Support-Protokollen für NSX Controller

Sie können Protokolle für den technischen Support für jede NSX Controller-Instanz herunterladen. Diese produktspezifischen Protokolle enthalten Diagnoseinformationen für die Analyse.

So erfassen Sie NSX Controller-Protokolle:

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Installation**.
- 3 Wählen Sie unter **Management** den Controller aus, von dem Sie Protokolle herunterladen möchten.
- 4 Klicken Sie auf **Tech-Support-Protokolle herunterladen**.
- 5 Klicken Sie auf **Herunterladen**.

NSX Manager startet den Download des NSX Controller-Protokolls und erhält die Sperre.

---

**Hinweis** Laden Sie die NSX Controller einzeln herunter. Wenn der erste Download abgeschlossen ist, starten Sie mit den nächsten. Wenn Sie Protokolle von mehreren Controllern gleichzeitig herunterladen, kann ein Fehler auftreten.

---

- 6 Wenn das Protokoll fertig gestellt wurde, klicken Sie auf **Speichern**, um das Protokoll auf Ihren Desktop herunterzuladen.

Das Protokoll ist komprimiert und hat die Dateierweiterung **.gz**.

### Ergebnisse

Sie können die heruntergeladenen Protokolle nun analysieren.

### Nächste Schritte

Wenn Sie Diagnosedaten für den technischen Support von VMware hochladen möchten, schlagen Sie im [Knowledgebase-Artikel 2070100](#) nach.

## Konfigurieren eines Syslog-Servers für NSX Controller

Wenn Sie einen Syslog-Server für NSX Controller konfigurieren, sendet NSX Manager alle Überwachungsprotokolle und Systemereignisse an den Syslog-Server. Syslog-Daten sind hilfreich bei der Problembehebung und bei der Überprüfung von Daten, die während der Installation und Konfiguration protokolliert worden sind. Die Konfiguration des Syslog-Servers auf den NSX Controllern kann nur über die NSX-API durchgeführt werden. VMware empfiehlt die Verwendung des UDP-Protokolls für Syslog.

## Verfahren

- 1 Um Syslog auf dem NSX Controller zu aktivieren, verwenden Sie die im Folgenden dargestellte NSX-API. Damit wird der Controller-Syslog-Exporter hinzugefügt und ein Syslog-Exporter auf dem angegebenen Controller-Knoten konfiguriert.

```
Request
POST https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Request Body:
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

- 2 Sie können den Controller-Syslog-Exporter abfragen und Details zum konfigurierten Syslog-Exporter auf dem angegebenen Controller-Knoten mithilfe der nachfolgend dargestellten NSX-API abrufen.

```
Request
GET https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Response Body:
<?xml version="1.0" encoding="UTF-8"?>
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

- 3 Wenn er nicht erforderlich ist, können Sie den Syslog-Exporter auf dem angegebenen Controller-Knoten mithilfe der im Folgenden dargestellten NSX-API löschen.

```
Request
DELETE https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
```

## Nächste Schritte

Weitere Informationen zur API erhalten Sie unter *Handbuch zu NSX-API*.

## Ändern des VXLAN-Ports

Sie können den für den VXLAN-Datenverkehr verwendeten Port ändern.

In NSX 6.2.3 und höher lautet der von IANA zugewiesene Standard-VXLAN-Port 4789. Vor NSX 6.2.3 lautete die Standard-VXLAN-UDP-Portnummer 8472.

Alle neuen NSX-Installationen verwenden jetzt den UDP-Port 4789 für VXLAN.

Wenn Sie von NSX 6.2.2 oder früher ein Upgrade auf NSX 6.2.3 oder höher durchführen und für Ihre Installation vor dem Upgrade die alte Standardnummer (8472) oder eine benutzerdefinierte Portnummer verwendet wurde (z. B. 8888), wird dieser Port so lange nach dem Upgrade weiter benutzt, bis Sie diesen ändern.

Wenn die Installation, für die ein Upgrade durchgeführt wurde, Hardware-VTEP-Gateways („ToR-Gateways“) verwendet oder verwenden soll, müssen Sie zum VXLAN-Port 4789 wechseln.

Cross-vCenter NSX erfordert nicht die Verwendung von 4789 für den VXLAN-Port. Allerdings muss für alle Hosts in einer Cross-vCenter NSX-Umgebung die Verwendung desselben VXLAN-Ports konfiguriert werden. Dadurch wird bei einem Wechsel zu Port 4789 sichergestellt, dass neue der Cross-vCenter NSX-Umgebung hinzugefügte NSX-Installationen denselben Port wie vorhandene NSX-Bereitstellungen verwenden.

Die Änderung des VXLAN-Ports erfolgt in drei Stufen und führt nicht zur Unterbrechung des VXLAN-Datenverkehrs.

- 1 NSX Manager konfiguriert alle Hosts, die auf VXLAN-Datenverkehr sowohl auf den alten wie auf den neuen Ports überwacht werden sollen. Hosts senden weiterhin VXLAN-Datenverkehr auf den alten Port.
- 2 NSX Manager konfiguriert alle Hosts für das Senden des Datenverkehrs auf den neuen Port.
- 3 NSX Manager konfiguriert alle Hosts für das Beenden der Überwachung auf dem alten Port. Der gesamte Datenverkehr wird auf dem neuen Port gesendet und empfangen.

In einer Cross-vCenter NSX-Umgebung müssen Sie die Änderung des Ports auf dem primären NSX Manager initiieren. In jeder Phase werden die Konfigurationsänderungen auf allen Hosts in der Cross-vCenter NSX-Umgebung durchgeführt, bevor mit der nächsten Phase fortgesetzt wird.

### Voraussetzungen

- Stellen Sie sicher, dass der Port, den Sie für VXLAN verwenden möchten, nicht durch eine Firewall blockiert ist.
- Stellen Sie sicher, dass die Hostvorbereitung nicht zur gleichen Zeit ausgeführt wird wie die Änderung des VXLAN-Ports.

### Verfahren

- 1 Klicken Sie auf die Registerkarte **Vorbereitung des logischen Netzwerks (Logical Network Preparation)** und dann auf **VXLAN-Transport (VXLAN Transport)**.
- 2 Klicken Sie im VXLAN-Portbereich auf die Schaltfläche **Ändern (Change)**. Geben Sie den Port ein, zu dem Sie wechseln möchten. 4789 ist der Port, der von IANA für VXLAN zugewiesen wurde.

Es dauert einen Moment, bis die Portänderung an alle Hosts übermittelt wird.

- 3 (Optional) Sie können den Fortschritt der Portänderung mit der API-Anforderung `GET /api/2.0/vdn/config/vxlan/udp/port/taskStatus` überprüfen.

```
GET https://nsxmgr-01a/api/2.0/vdn/config/vxlan/udp/port/taskStatus
```

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
 <prevPort>8472</prevPort>
 <targetPort>4789</targetPort>
 <taskPhase>PHASE_TWO</taskPhase>
 <taskStatus>PAUSED</taskStatus>
</vxlanPortUpdatingStatus>
```

...

```
<?xml version="1.0" encoding="UTF-8"?>
<vxlanPortUpdatingStatus>
 <prevPort>8472</prevPort>
 <targetPort>4789</targetPort>
 <taskPhase>FINISHED</taskPhase>
 <taskStatus>SUCCEED</taskStatus>
</vxlanPortUpdatingStatus>
```

## Programm zur Verbesserung der Benutzerfreundlichkeit

NSX nimmt am VMware-Programm zur Verbesserung der Benutzerfreundlichkeit (Customer Experience Improvement Program, CEIP) teil.

Einzelheiten zu den im Rahmen des CEIP erfassten Daten sowie zum Zweck der Verwendung durch VMware können im Trust & Assurance Center unter <https://www.vmware.com/solutions/trustvmware/ceip.html> eingesehen werden.

Informationen zur Teilnahme am CEIP für NSX bzw. zum Abmelden davon und zum Bearbeiten von Programmeinstellungen finden Sie unter [Bearbeiten der Option „Programm zur Verbesserung der Benutzerfreundlichkeit“ \(CEIP\)](#).

## Bearbeiten der Option „Programm zur Verbesserung der Benutzerfreundlichkeit“ (CEIP)

Wenn Sie NSX Manager installieren oder ein Upgrade dafür durchführen, können Sie wählen, ob Sie sich am CEIP (Customer Experience Improvement Program) beteiligen. Sie können auch zu einem späteren Zeitpunkt am CEIP teilnehmen bzw. sich jederzeit daraus abmelden. Darüber hinaus haben Sie die Möglichkeit, die Häufigkeit der Erfassung der Informationen und die Tage dafür festzulegen.

### Voraussetzungen

- Stellen Sie sicher, dass mit dem NSX Manager eine Verbindung hergestellt wurde und eine Synchronisierung mit vCenter Server möglich ist.
- Stellen Sie sicher, dass DNS auf dem NSX Manager konfiguriert ist.

- Stellen Sie sicher, dass NSX mit einem öffentlichen Netzwerk für das Hochladen von Daten verbunden ist.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Networking & Security** aus.
- 3 Unter „Bestandsliste für Netzwerk und Sicherheit“ wählen Sie **NSX Managers** aus.
- 4 Doppelklicken Sie auf den NSX Manager, den Sie verändern möchten.
- 5 Klicken Sie auf die Registerkarte **Übersicht (Summary)**.
- 6 Klicken Sie im Dialogfeld „Programm zur Verbesserung der Benutzerfreundlichkeit“ auf **Bearbeiten (Edit)**.
- 7 Aktivieren oder deaktivieren Sie die Option **Am VMware Customer Experience Improvement Program teilnehmen (Join the VMware Customer Experience Improvement Program)**.
- 8 (Optional) Konfigurieren Sie die Serieneinstellungen.
- 9 Klicken Sie auf **OK**.

## Grundlegendes zu NSX-Protokollen

Sie können den Syslog-Server konfigurieren und Protokolle des technischen Supports für die einzelnen NSX-Komponenten anzeigen. Protokolle der Verwaltungsebene sind über NSX Manager verfügbar, Protokolle der Datenebene hingegen über vCenter Server. Daher ist es ratsam, denselben Syslog-Server für die NSX-Komponente und vCenter Server anzugeben, um beim Betrachten von Protokollen auf dem Syslog-Server ein vollständiges Bild zu erhalten.

Informationen zum Konfigurieren eines Syslog-Servers für durch einen vCenter Server verwaltete Hosts finden Sie in der entsprechenden Version der vSphere-Dokumentation unter <https://docs.vmware.com>.

**Hinweis** Syslog- oder Jump-Server, die zur Erfassung von Protokollen und zum Zugriff auf eine NSX-DLR-Kontroll-VM (Distributed Logical Router) verwendet werden, können sich nicht auf dem logischen Switch befinden, der direkt den logischen Schnittstellen (LIFs) dieses DLR angefügt wurde.

**Tabelle 22-1. NSX-Protokolle**

Komponente	Beschreibung
ESXi-Protokolle	<p>Diese Protokolle werden als Teil des VM-Support-Pakets erfasst, das von vCenter Server generiert wird.</p> <p>Weitere Informationen zu ESXi-Protokolldateien finden Sie in der vSphere-Dokumentation.</p>
NSX Edge-Protokolle	<p>Verwenden Sie den Befehl <code>show log [follow   reverse]</code> in der Befehlszeilenschnittstelle von NSX Edge.</p> <p>Laden Sie das Protokollpaket für den technischen Support über die Benutzeroberfläche von NSX Edge herunter.</p>

**Tabelle 22-1. NSX-Protokolle (Fortsetzung)**

Komponente	Beschreibung
NSX Manager-Protokolle	Verwenden Sie den Befehl <code>show log</code> in der Befehlszeilenschnittstelle von NSX Manager. Laden Sie das Protokollpaket für den technischen Support über die Benutzeroberfläche der virtuellen NSX Manager-Appliance herunter.
Routing-Protokolle	Siehe Handbuch <i>NSX-Protokollierung und -Systemereignisse</i> .
Firewallprotokolle	Siehe Handbuch <i>NSX-Protokollierung und -Systemereignisse</i> .
Guest Introspection-Protokolle	Siehe Handbuch <i>NSX-Protokollierung und -Systemereignisse</i> .

## NSX Manager

Informationen zum Angeben eines Syslog-Servers erhalten Sie unter [Konfigurieren eines Syslog-Servers für NSX Manager](#).

Informationen zum Herunterladen der Protokolle des technischen Supports erhalten Sie unter [Herunterladen der Protokolle des technischen Supports für NSX](#).

## NSX Edge

Informationen zum Angeben eines Syslog-Servers erhalten Sie unter [Konfigurieren von Syslog-Servern für NSX Edge](#).

Informationen zum Herunterladen der Protokolle des technischen Supports erhalten Sie unter [Herunterladen von Tech-Support-Protokollen für NSX Edge](#).

## NSX Controller

Informationen zum Angeben eines Syslog-Servers erhalten Sie unter [Konfigurieren eines Syslog-Servers für NSX Controller](#).

Informationen zum Herunterladen der Protokolle des technischen Supports erhalten Sie unter [Herunterladen von technischen Support-Protokollen für NSX Controller](#).

## Firewall

Weitere Informationen finden Sie unter [Firewallprotokolle](#).

## Überwachungsprotokolle

Überwachungsprotokolle für Vorgänge, die durch ein Ticket verfolgt werden, enthalten die Ticket-ID. Mit der NSX Ticket Logger-Funktion können Sie die Änderungen verfolgen, die Sie mit einer Ticket-ID vornehmen.

## Verwendung von NSX Ticket Logger

Der NSX Ticket Logger ermöglicht Ihnen, die vorgenommenen Infrastrukturänderungen zu verfolgen. Alle Vorgänge werden mit der angegebenen Ticket-ID gekennzeichnet, und die Überwachungsprotokolle für

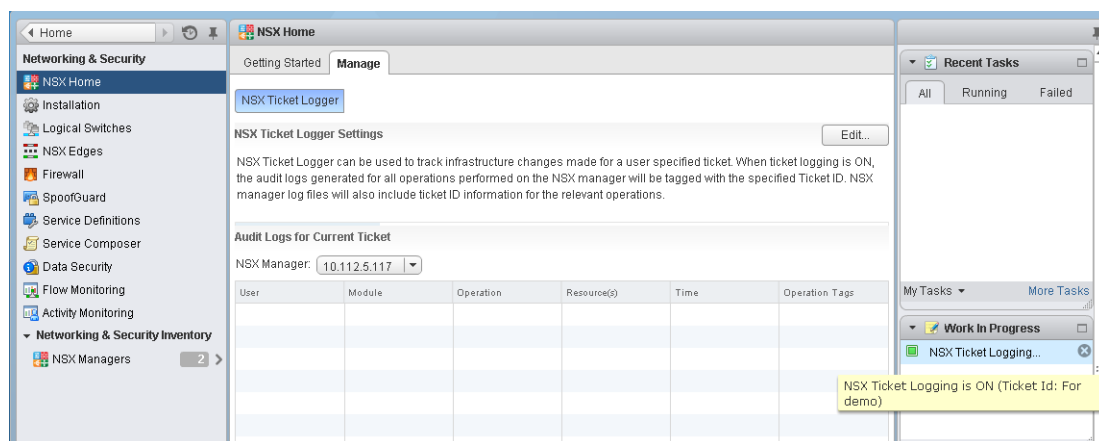
diese Vorgänge beinhalten die Ticket-ID. Protokolldateien für diese Vorgänge werden mit derselben Ticket-ID gekennzeichnet.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf die Registerkarte **Verwalten (Manage)**.
- 3 Klicken Sie neben **NSX Ticket Logger-Einstellungen (NSX Ticket Logger Settings)** auf **Bearbeiten (Edit)**.
- 4 Geben Sie eine Ticket-ID ein und klicken Sie auf **Einschalten (Turn On)**.

Der Bereich „NSX Ticket Logging“ wird auf der rechten Seite des vSphere Web Client-Fensters angezeigt. Überwachungsprotokolle für die Vorgänge, die Sie in der aktuellen Benutzeroberflächensitzung durchführen, beinhalten die Ticket-ID in der Spalte **Vorgangs-Tags (Operation Tags)**.

Abbildung 22-1. Bereich „NSX Ticket Logger“



Wenn mehrere vCenter Server durch vSphere Web Client verwaltet werden, wird die Ticket-ID für die Protokollierung bei allen zutreffenden NSX Managern verwendet.

## Nächste Schritte

Die Ticket-Protokollierung ist sitzungsbasiert. Wenn die Ticket-Protokollierung aktiviert ist und Sie sich abmelden oder die Sitzung abgebrochen wird, wird die Ticket-Protokollierung standardmäßig deaktiviert, wenn Sie sich erneut bei der Benutzeroberfläche anmelden. Wenn Sie die Vorgänge für ein Ticket abschließen, deaktivieren Sie die Protokollierung, indem Sie die Schritte 2 und 3 wiederholen und auf **Ausschalten (Turn Off)** klicken.

## Anzeigen des Überwachungsprotokolls

Auf der Registerkarte **Überwachungsprotokolle** wird eine Ansicht der von allen NSX Manager-Benutzern durchgeführten Aktionen bereitgestellt. NSX Manager behält bis zu 100.000 Überwachungsprotokolle bei.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie in der Spalte **Name** auf einen NSX Server und anschließend auf die Registerkarte **Überwachen**.
- 4 Klicken Sie auf die Registerkarte **Überwachungsprotokolle**.
- 5 Sobald Details des Überwachungsprotokolls zur Verfügung stehen, ist der Text in der Spalte **Vorgang** anklickbar. Klicken Sie auf den Text in der Spalte **Vorgang**, um die Details des Überwachungsprotokolls anzuzeigen.
- 6 Wählen Sie in **Änderungsdetails – Überwachungsprotokoll** den Eintrag **Geänderte Zeilen** aus, wenn nur Eigenschaften angezeigt werden sollen, deren Werte sich für diesen Überwachungsprotokollvorgang geändert haben.

## Systemereignisse

Systemereignisse sind Ereignisse, die sich auf NSX-Vorgänge beziehen. Sie werden generiert, um Detailinformationen zu Ereignissen bereitzustellen. Ereignisse können sich auf den allgemeinen Betrieb (Informational) oder auf einen kritischen Fehler (Critical) beziehen.

## Anzeigen des Systemereignisberichts

In vSphere Web Client können Sie alle Systemereignisse für die von NSX Manager verwalteten Komponenten anzeigen lassen.

## Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend unter **Bestandsliste für Netzwerk und Sicherheit** auf **NSX Manager**.
- 3 Klicken Sie auf einen NSX Manager in der Spalte **Name** und anschließend auf die Registerkarte **Überwachen**.
- 4 Klicken Sie auf die Registerkarte **Systemereignisse**.

Sie können die Ereignisse durch Klicken auf die Pfeile in der Spaltenüberschrift sortieren oder mithilfe des Textfeldes **Filter** filtern.

## Format von Systemereignissen

Wenn Sie einen Syslog-Server angeben, sendet NSX Manager alle Systemereignisse an den Syslog-Server.

Das Format dieser Meldungen ähnelt dem folgenden:

```
Jan 8 04:35:00 NSXMGR 2017-01-08 04:35:00.422 GMT+00:00
INFO TaskFrameworkExecutor-18 SystemEventDaoImpl:133 -
[SystemEvent] Time:'Tue Nov 08 04:35:00.410 GMT+00:00 2016',
Severity:'High', Event Source:'Security Fabric', Code:'250024',
Event Message:'The backing EAM agency for this deployment could not be found.
It is possible that the VC services may still be initializing.
Please try to resolve the alarm to check existence of the agency.
In case you have deleted the agency manually, please delete the deployment
entry from NSX.', Module:'Security Fabric', Universal Object:'false'
```

Das Systemereignis enthält die folgenden Informationen.

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Event Message: Text containing detailed information about the event.
Module: Event component. May be the same as event source.
Universal Object: Value displayed is True or False.
```

## Alarme

Alarme sind Benachrichtigungen, die als Reaktion auf ein Ereignis, einen Satz von Bedingungen oder den Status eines Objekts aktiviert werden. Alarme werden zusammen mit anderen Warnungen im NSX-Dashboard und auf anderen Bildschirmen in der vSphere Web Client-Benutzeroberfläche angezeigt.

Sie können die GET `api/2.0/services/systemalarms-API` verwenden, um Alarme für NSX-Objekte anzuzeigen.

NSX unterstützt zwei Methoden für einen Alarm:

- Der Alarm generiert ein Systemereignis und verfügt über einen zugeordneten Lösungsmechanismus, mit dem versucht wird, das Problem zu lösen, das den Alarm ausgelöst hat. Dieser Ansatz ist auf die Fabric-Bereitstellung für Netzwerk und Sicherheit (z. B. EAM, Nachrichtenbus, Bereitstellungs-Plugin) ausgelegt und wird von Service Composer unterstützt. Für diese Alarme wird der Ereigniscode als Alarmcode verwendet. Weitere Informationen finden Sie im Dokument *NSX-Protokollierung und -Systemereignisse*.
- Edge-Benachrichtigungen/Alarme sind als Alarmpaar zum Auslösen und Beheben strukturiert. Diese Methode wird durch mehrere Edge-Funktionen unterstützt, einschließlich IPSec-VPN, Lastausgleichsdienst, Hochverfügbarkeit, Funktionstest, Edge-Dateisystem und Ressourcenreservierung. Für diese Alarme wird ein eindeutiger Alarmcode verwendet, der nicht mit dem Ereigniscode identisch ist. Weitere Informationen finden Sie im Dokument *NSX-Protokollierung und -Systemereignisse*.

In der Regel wird ein Alarm vom System automatisch gelöscht, wenn der Fehler behoben ist. Einige Alarme werden nicht automatisch bei einer Aktualisierung der Konfiguration gelöscht. Sobald das Problem behoben wurde, müssen Sie die Alarme manuell löschen.

Hier ist ein Beispiel der API, die Sie zum Aufheben der Warnungen verwenden können.

Sie können Alarmer für eine bestimmte Quelle abrufen, beispielsweise Cluster, Host, Ressourcenpool, Sicherheitsgruppe oder NSX Edge. Anzeigen von Alarmen für eine Quelle von *sourceId*:

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}
```

Beheben aller Alarmer für eine Quelle von *sourceId*:

```
POST https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}?action=resolve
```

Sie können NSX-Alarmer anzeigen, einschließlich Nachrichtenbus-, Bereitstellungs-Plugin-, Service Composer- und Edge-Alarmen:

```
GET https://<<NSX-IP>>/api/2.0/services/systemalarms
```

Sie können einen bestimmten NSX-Alarm durch *alarmId* anzeigen:

```
GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
```

Sie können einen bestimmten NSX-Alarm durch *alarmId* beheben:

```
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

Weitere Informationen zur API finden Sie im Dokument *Handbuch zu NSX-API*.

## Format eines Alarms

Sie können das Format eines Alarms über die API anzeigen.

Das Format eines Alarms enthält die folgenden Informationen.

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Message: Text containing detailed information about the event.
Alarm ID: ID of an alarm.
Alarm Code: Event code which uniquely identifies the system alarm.
Alarm Source: Source where you should look to resolve the reported event.
```

## Arbeiten mit SNMP-Traps

Der NSX Manager erhält Systemereignisse mit dem Schweregrad „Zur Information“, „Warnung“ oder „Kritisch“, z. B. vom NSX Edge und von Hypervisor. Der SNMP-Agent leitet die SNMP-Traps mit OIDs an den SNMP-Empfänger weiter.

Für SNMP-Traps muss die Version SNMPv2c vorhanden sein. Die Traps müssen einer Management Information Base (MIB) zugeordnet sein, damit der SNMP-Empfänger die Traps mit Objektkennungen (Object Identifier, OID) verarbeiten kann.

Standardmäßig ist die Verwendung von SNMP-Traps deaktiviert. Die Aktivierung von SNMP-Traps aktiviert nur Benachrichtigungen vom Schweregrad „Kritisch“ und „Hoch“, sodass der SNMP-Manager nicht mit einer zu hohen Anzahl an Benachrichtigungen konfrontiert wird. Eine IP-Adresse oder ein Hostname definiert das Trap-Ziel. Damit der Hostname als Trap-Ziel dienen kann, muss das Gerät für die Abfrage des DNS-Servers (Domain-Name-System-Server) eingerichtet sein.

Wenn Sie den SNMP-Dienst aktivieren, wird als Erstes ein coldStart-Trap (Kaltstart-Trap) mit der OID 1.3.6.1.6.3.1.1.5.1 gesendet. Ein warmStart-Trap (Warmstart-Trap) mit der OID 1.3.6.1.6.3.1.1.5.2 wird später bei jedem Stopp-Start-Vorgang an die konfigurierten SNMP-Empfänger gesendet.

Bei dauerhafter Aktivierung des SNMP-Dienstes wird ein vmwHbHeartbeat-Trap (Taktsignal-Trap) mit der OID 1.3.6.1.4.1.6876.4.190.0.401 alle fünf Minuten gesendet. Wenn Sie den Dienst deaktivieren, wird ein vmwNsxMSnmpDisabled-Trap (Deaktiviert-Trap) mit der OID 1.3.6.1.4.1.6876.90.1.2.1.0.1 gesendet. Dieser Vorgang beendet die Ausführung des vmwHbHeartbeat-Trap und deaktiviert den Dienst.

Wenn Sie einen SNMP-Empfänger-Wert hinzufügen, ändern oder löschen, wird ein warmStart-Trap mit der OID 1.3.6.1.6.3.1.1.5.2 und ein vmwNsxMSnmpManagerConfigUpdated-Trap mit der OID 1.3.6.1.4.1.6876.90.1.2.1.0.2 zur neuen oder aktualisierten Gruppe von SNMP-Empfängern gesendet.

---

**Hinweis** Der SNMP-Abruf wird nicht unterstützt.

---

## Konfigurieren von SNMP-Einstellungen

Sie können mit den SNMP-Einstellungen die Zielempfänger zum Senden von Traps mit dem Schweregrad „Kritisch“, „Hoch“ oder „Zur Information“ konfigurieren.

### Voraussetzungen

- Machen Sie sich mit dem Mechanismus von SNMP-Traps vertraut. Weitere Informationen dazu finden Sie unter [Arbeiten mit SNMP-Traps](#).
- Stellen Sie sicher, dass ein SNMP-Empfänger konfiguriert ist.
- Laden Sie das MIB-Modul herunter und installieren Sie es für den NSX Manager, damit der SNMP-Empfänger die Traps mit OID (Object Identifier, Objektkennung) verarbeiten kann. Weitere Informationen dazu finden Sie unter <http://kb.vmware.com/kb/1013445>.

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Networking & Security > Bestandsliste für Netzwerk und Sicherheit (Networking & Security Inventory) > NSX Manager** aus.
- 3 Wählen Sie eine NSX Manager-IP-Adresse aus.
- 4 Wählen Sie die Registerkarten **Verwalten (Manage) > Systemereignisse (System Events)** aus.

- 5 Klicken Sie auf **Bearbeiten (Edit)**, um die SNMP-Einstellungen zu konfigurieren.

Option	Beschreibung
<b>Dienst</b>	Sendet einen SNMP-Trap. Standardmäßig ist diese Option deaktiviert.
<b>Gruppenbenachrichtigung</b>	Vordefiniertes Set von Gruppen für einige Systemereignisse, die zur Zusammenfassung der generierten Ereignisse verwendet werden. Standardmäßig ist diese Option aktiviert.  Wenn z. B. zu einer Gruppe ein Systemereignis gehört, wird der Trap für diese gruppierten Ereignisse zurückgehalten. Alle fünf Minuten wird ein Trap gesendet, der die Anzahl der Systemereignisse spezifiziert, die vom NSX Manager empfangen wurden. Je weniger Traps gesendet werden, desto weniger SNMP-Empfänger-Ressourcen werden in Anspruch genommen.
<b>Empfänger</b>	Konfiguriert bis zu vier Empfänger, an die Traps gesendet werden können. Für die nachfolgend aufgeführten Abschnitte müssen Festlegungen für das Hinzufügen eines SNMP-Empfängers getroffen werden. Empfängeradresse – IP-Adresse oder vollqualifizierter Domänenname (FQDN) des Empfängerhosts. Empfängerport – Der Standard-UDP-Port für SNMP-Empfänger ist 162. Community-String – Als Teil des Benachrichtigungs-Trap gesendete Informationen. Aktiviert – Anzeige, ob dieser Empfänger einen Trap sendet.

- 6 Klicken Sie auf **OK**.

### Ergebnisse

Der SNMP-Dienst ist aktiviert und die Traps werden an die Empfänger gesendet.

### Nächste Schritte

Überprüfen Sie das Funktionieren der SNMP-Konfiguration. Weitere Informationen dazu finden Sie unter [Überprüfen der SNMP-Trap-Konfiguration](#).

## Überprüfen der SNMP-Trap-Konfiguration

Bevor Sie mit der Bearbeitung eines vorhandenen System-Trap beginnen, müssen Sie prüfen, ob der neu aktivierte oder aktualisierte SNMP-Dienst korrekt arbeitet.

### Voraussetzungen

Stellen Sie sicher, dass das SNMP konfiguriert wurde. Weitere Informationen dazu finden Sie unter [Konfigurieren von SNMP-Einstellungen](#).

## Verfahren

- 1 Überprüfen Sie die SNMP-Konfiguration und die Empfänger Verbindung.
  - a Wählen Sie die Registerkarten **Verwalten (Manage) > Systemereignisse (System Events)** aus.
  - b Klicken Sie auf **Bearbeiten (Edit)**, um die SNMP-Einstellungen zu konfigurieren.  
Die Einstellungen im Dialogfeld dürfen nicht geändert werden.
  - c Klicken Sie auf **OK**.

Ein warmStart-Trap (Warmstart-Trap) mit der OID 1.3.6.1.6.3.1.1.5.2 wird an alle SNMP-Empfänger gesendet.
- 2 Beheben Sie eventuelle SNMP-Konfigurations- oder Empfängerfehler.
  - a Wenn der SNMP-Empfänger die Traps nicht erhält, müssen Sie prüfen, ob der SNMP-Empfänger auf einem konfigurierten Port ausgeführt wird.
  - b Überprüfen Sie im Abschnitt „SNMP-Einstellungen“, ob die Details des Empfängers korrekt sind.
  - c Wenn der SNMP-Empfänger den Empfang eines vmwHbHeartbeat-Trap (Taktsignal-Trap) mit der OID 1.3.6.1.4.1.6876.4.190.0.401 beendet, der alle fünf Minuten gesendet wird, überprüfen Sie, ob die NSX Manager-Appliance oder der NSX Manager-SNMP-Agent aktiv ist.
  - d Wenn der Taktsignal-Trap stoppt, überprüfen Sie, ob der SNMP-Dienst deaktiviert ist oder ob keine Netzwerkkonnektivität zwischen dem NSX Manager und dem SNMP-Empfänger besteht.

## Bearbeiten von System-Traps

Sie können einen System-Trap bearbeiten, um den Schweregrad und die Aktivierung eines Trap zu erhöhen oder zu verringern, um festzulegen, wann Traps entweder an Empfänger gesendet oder zurückgehalten werden.

Wenn für das Modul SNMP OID oder für die Spalte „SNMP-Trap aktiviert“ -- angezeigt wird, ist diesen Ereignissen keine Trap-OID zugeteilt worden. Deshalb wird für diese Ereignisse kein Trap gesendet.

Ein System-Trap verfügt über verschiedene Spalten mit den unterschiedlichen Merkmalen eines Systemereignisses.





Option	Beschreibung
Ereigniscode	Der statische Ereigniscode, der einem Ereignis zugeordnet ist.
Beschreibung	Zusammenfassende Beschreibung des Ereignisses.
Modul	Teilkomponente, die ein Ereignis auslöst.
Schweregrad	Level eines Ereignisses mit folgenden möglichen Werten: Zur Information, Niedrig, Mittel, Wesentlich, Kritisch und Hoch.  Standardmäßig werden Traps bei aktiviertem SNMP-Dienst nur für Ereignisse mit dem Schweregrad „Kritisch“ und „Hoch“ gesendet, um den Fokus auf jene Traps zu richten, die eine sofortige Behandlung erfordern.

Option	Beschreibung
SNMP OID	<p>Gibt die einzelne OID (Object Identifier, Objektkennung) an, die gesendet wird, wenn ein Systemereignis generiert wird.</p> <p>Die Gruppenbenachrichtigung ist standardmäßig aktiviert. Wenn Gruppenbenachrichtigungen aktiviert sind, wird für die Ereignisse oder Traps unter dieser Gruppe die OID der Gruppe angezeigt, zu der das Ereignis oder der Trap gehört.</p> <p>Beispielsweise lautet die OID der Gruppenbenachrichtigung in der Konfigurationsgruppe 1.3.6.1.4.1.6876.90.1.2.0.1.0.1.</p>
SNMP-Trap aktiviert	<p>Zeigt an, ob das Senden des Trap für dieses Ereignis aktiviert ist.</p> <p>Sie können mit dem Symbol die Ereignis- oder Trap-Aktivierung individuell umschalten. Wenn die Gruppenbenachrichtigung aktiviert ist, lässt sich die Trap-Aktivierung nicht umschalten.</p>
Filter	Suchbegriffe zum Filtern der System-Traps.

### Voraussetzungen

Stellen Sie sicher, dass die SNMP-Einstellungen verfügbar sind. Weitere Informationen dazu finden Sie unter [Konfigurieren von SNMP-Einstellungen](#).

### Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Networking & Security > Bestandsliste für Netzwerk und Sicherheit (Networking & Security Inventory) > NSX Manager (NSX Managers)** aus.
- 3 Wählen Sie eine NSX Manager-IP-Adresse aus.
- 4 Wählen Sie die Registerkarten **Verwalten (Manage) > Systemereignisse (System Events)** aus.
- 5 Wählen Sie ein Systemereignis im Abschnitt „System-Traps“ aus.
- 6 Klicken Sie auf das Symbol **Bearbeiten (Edit)** ().  
Das Bearbeiten einer Trap-Aktivierung ist nicht möglich, wenn die Gruppenbenachrichtigung aktiviert ist. Sie können aber die Aktivierung von Traps ändern, die zu keiner Gruppe gehören.
- 7 Ändern Sie den Schweregrad des Systemereignisses im Dropdown-Menü.
- 8 Wenn Sie den Schweregrad von „Zur Information“ auf „Kritisch“ ändern, aktivieren Sie das Kontrollkästchen **Als SNMP-Trap aktivieren (Enable as SNMP Trap)**.
- 9 Klicken Sie auf **OK**.
- 10 (Optional) Klicken Sie auf das Symbol **Aktivieren (Enable)** () oder auf das Symbol **Deaktivieren (Disable)** () in der Kopfzeile, um das Senden eines System-Trap zu aktivieren oder zu deaktivieren.
- 11 (Optional) Klicken Sie auf das Symbol **Kopieren (Copy)** () , um eine oder mehrere Ereigniszeilen in Ihre Zwischenablage zu kopieren.

## Einstellungen für das Managementsystem

Sie können die bei der ersten Anmeldung angegebenen Definitionen für vCenter Server, für den DNS- und NTP-Server sowie für den Lookup-Server bearbeiten. NSX Manager muss mit vCenter Server und Diensten wie beispielsweise DNS und NTP kommunizieren können, um Details zur VMware Infrastructure-Bestandsliste bereitzustellen.

## Anmelden bei der virtuellen NSX Manager-Appliance

Nachdem Sie die NSX Manager-VM installiert und konfiguriert haben, melden Sie sich bei der virtuellen NSX Manager-Appliance an, um die bei der Installation angegebenen Einstellungen zu überprüfen.

### Verfahren

- 1 Öffnen Sie ein Webbrowser-Fenster und geben Sie die IP-Adresse an, die dem NSX Manager zugewiesen ist. Beispiel: **https://192.168.110.42**.

Die NSX Manager-Benutzeroberfläche wird mithilfe von SSL in einem Webbrowser-Fenster geöffnet.

- 2 Akzeptieren Sie das Sicherheitszertifikat.

---

**Hinweis** Sie können das SSL-Zertifikat zur Authentifizierung verwenden.

---

Der Anmeldebildschirm von NSX Manager wird angezeigt.

- 3 Melden Sie sich mit dem Benutzernamen **admin** und dem bei der Installation eingerichteten Kennwort bei der virtuellen NSX Manager-Appliance an.
- 4 Klicken Sie auf **Anmelden (Log In)**.

## Ereignisse für virtuelle NSX Manager-Appliance

Die folgenden Ereignisse sind spezifisch für die virtuelle NSX Manager-Appliance.

**Tabelle 22-2. Ereignisse für virtuelle NSX Manager-Appliance**

	Ausschalten	Einschalten	Schnittstelle nicht verfügbar	Schnittstelle verfügbar
Lokale CLI	show log follow-Befehl ausführen	show log follow-Befehl ausführen	show log follow-Befehl ausführen	show log follow-Befehl ausführen
GUI	–	–	–	–

**Tabelle 22-3. Ereignisse für virtuelle NSX Manager-Appliance**

	CPU	Arbeitsspeicher	Speicher
Lokale CLI	show process monitor-Befehl ausführen	show system memory-Befehl ausführen	show filesystem-Befehl ausführen
GUI	–	–	–

## Bearbeiten des Datums und der Uhrzeit von NSX Manager

Sie können den während der anfänglichen Anmeldung angegebenen NTP-Server ändern.

### Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 2 Klicken Sie unter **Appliance-Verwaltung (Appliance Management)** auf **Appliance-Einstellungen verwalten (Manage Appliance Settings)**.
- 3 Klicken Sie neben **Uhrzeiteinstellungen (Time Settings)** auf **Bearbeiten (Edit)**.
- 4 Nehmen Sie die entsprechenden Änderungen vor.
- 5 Klicken Sie auf **OK**.
- 6 Starten Sie NSX Manager neu.

## Konfigurieren eines Syslog-Servers für NSX Manager

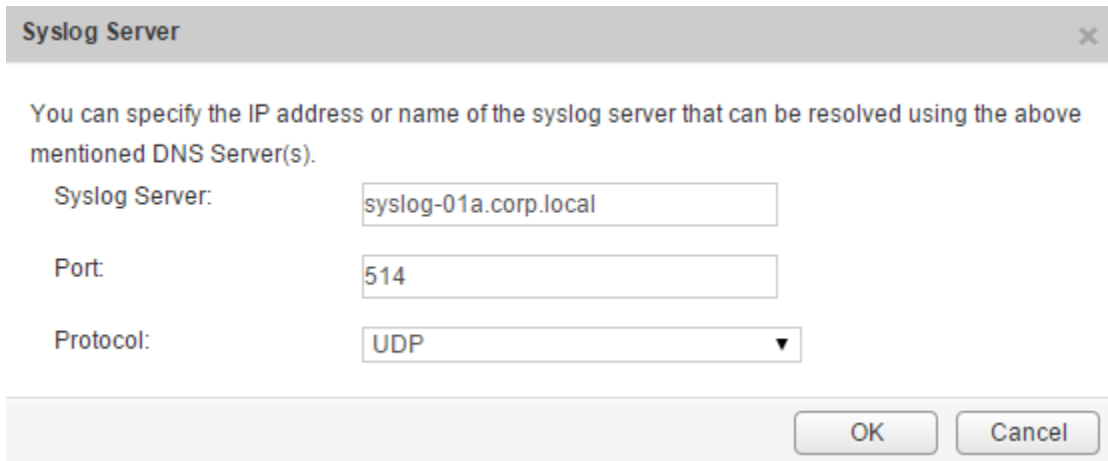
Wenn Sie einen Syslog-Server angeben, sendet NSX Manager alle Überwachungsprotokolle und Systemereignisse an den Syslog-Server.

Syslog-Daten sind hilfreich bei der Problembehebung und bei der Überprüfung von Daten, die während der Installation und Konfiguration protokolliert worden sind.

NSX Edge unterstützt zwei Syslog-Server. NSX Manager und NSX Controller unterstützen einen Syslog-Server.

### Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.  
  
Navigieren Sie in einem Web-Browser zur NSX Manager Appliance-GUI unter <https://<nsx-manager-ip>> oder <https://<nsx-manager-hostname>> und melden Sie sich als Administrator mit dem Kennwort an, das Sie bei der Installation von NSX Manager konfiguriert haben.
- 2 Klicken Sie auf der Startseite auf **Appliance-Einstellungen verwalten (Manage Appliance Settings) > Allgemein (General)**.
- 3 Klicken Sie neben **Syslog-Server (Syslog Server)** auf **Bearbeiten (Edit)**.
- 4 Geben Sie die IP-Adresse oder den Hostnamen, Port und Protokoll des Syslog-Servers ein.  
  
Beispiel:



**Syslog Server** [X]

You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).

Syslog Server:

Port:

Protocol:

[OK] [Cancel]

5 Klicken Sie auf **OK**.

### Ergebnisse

Die Remoteprotokollierung von NSX Manager ist aktiviert und die Protokolle werden auf Ihrem eigenständigen Syslog-Server gespeichert.

## Ändern des FIPS-Modus und der TLS-Einstellungen für NSX Manager

Wenn Sie den FIPS-Modus aktivieren, werden für die sichere Kommunikation an oder vom NSX Manager kryptografische Algorithmen und Protokolle verwendet, die laut der US-Amerikanischen Federal Information Processing Standards (FIPS) zulässig sind.

- In einer Cross-vCenter NSX-Umgebung sollten Sie den FIPS-Modus für alle NSX Manager-Instanzen separat aktivieren.
- Wenn kein NSX Manager für FIPS konfiguriert ist, müssen Sie trotzdem sicherstellen, dass er eine sichere Kommunikationsmethode verwendet, die den FIPS-Standards entspricht.
- Damit die globale Synchronisierung ordnungsgemäß funktioniert, müssen sowohl primäre wie sekundäre NSX Manager über die gleiche TLS-Version verfügen.

**Wichtig** Bei einer Änderung des FIPS-Modus wird die virtuelle Appliance von NSX Manager neu gestartet.

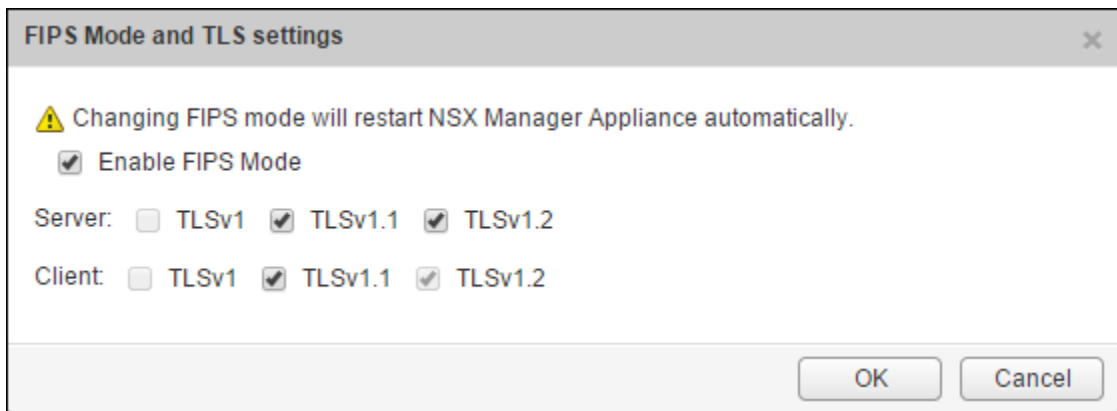
### Voraussetzungen

- Stellen Sie sicher, dass Partnerlösungen für den FIPS-Modus zertifiziert sind. Weitere Informationen finden Sie im VMware-Kompatibilitätshandbuch unter <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=security>.
- Wenn Sie ein Upgrade von einer früheren NSX-Version durchgeführt haben, aktivieren Sie den FIPS-Modus erst nach Abschluss des Upgrades auf NSX 6.3.0. Siehe „Informationen zum Verständnis des FIPS-Modus und NSX-Upgrades“ im *Upgrade-Handbuch für NSX*.
- Stellen Sie sicher, dass NSX Manager der Version NSX 6.3.0 oder höher entspricht.

- Stellen Sie sicher, dass das NSX Controller-Cluster der Version NSX 6.3.0 oder höher entspricht.
- Stellen Sie sicher, dass alle Host-Cluster, auf denen NSX-Arbeitslasten ausgeführt werden, mit NSX 6.3.0 oder höher vorbereitet wurden.
- Stellen Sie sicher, dass alle NSX Edge-Appliances der Version 6.3.0 oder höher entsprechen und dass der FIPS-Modus auf den erforderlichen NSX Edge-Appliances aktiviert wurde. Weitere Informationen dazu finden Sie unter [Ändern des FIPS-Modus in NSX Edge](#).

#### Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 2 Klicken Sie unter **Appliance-Verwaltung (Appliance Management)** auf **Appliance-Einstellungen verwalten (Manage Appliance Settings)**.
- 3 Klicken Sie im Fensterbereich „Einstellungen“ auf **Allgemein (General)**.
- 4 Klicken Sie neben **FIPS-Modus und TLS-Einstellungen (FIPS Mode and TLS settings)** auf **Bearbeiten (Edit)**.



- 5 Aktivieren Sie zur Aktivierung des FIPS-Modus das Kontrollkästchen **FIPS-Modus aktivieren (Enable FIPS Mode)**.
- 6 Aktivieren Sie für Server und Client die Kontrollkästchen für die erforderliche TLS-Protokollversion.

---

**Hinweis** Bei aktiviertem FIPS-Modus deaktiviert NSX Manager die TLS-Protokolle, die die FIPS-Standards nicht erfüllen.

---

- 7 Klicken Sie auf **OK**.

Die NSX Manager-Appliance wird neu gestartet, und FIPS ist aktiviert.

## Bearbeiten von DNS-Servern

Sie können die während der Manager-Installation angegebenen DNS-Server ändern.

#### Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.

- 2 Klicken Sie unter **Appliance-Verwaltung (Appliance Management)** auf **Appliance-Einstellungen verwalten (Manage Appliance Settings)**.
- 3 Klicken Sie im Fensterbereich „Einstellungen“ auf **Netzwerk (Network)**.
- 4 Klicken Sie auf **Bearbeiten (Edit)** neben **DNS-Server (DNS Servers)**.
- 5 Nehmen Sie die entsprechenden Änderungen vor.
- 6 Klicken Sie auf **OK**.

## Bearbeiten von Lookup Service-Details

Sie können die während der anfänglichen Anmeldung angegebenen Lookup Service-Details ändern.

### Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 2 Klicken Sie unter **Appliance-Verwaltung (Appliance Management)** auf **Appliance-Einstellungen verwalten (Manage Appliance Settings)**.
- 3 Klicken Sie im Bereich „Einstellungen“ auf **NSX Management Service**.
- 4 Klicken Sie auf **Bearbeiten (Edit)** neben **Lookup Service**.
- 5 Nehmen Sie die entsprechenden Änderungen vor.
- 6 Klicken Sie auf **OK**.

## Bearbeiten von vCenter Server

Sie können den vCenter Server ändern, bei dem Sie NSX Manager bei der Installation registriert haben. Sie sollten dies nur dann tun, wenn Sie die IP-Adresse Ihres aktuellen vCenter Servers ändern.


### Verfahren

- 1 Wenn Sie bei vSphere Web Client angemeldet sind, melden Sie sich ab.
- 2 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 3 Klicken Sie unter **Appliance-Verwaltung (Appliance Management)** auf **Appliance-Einstellungen verwalten (Manage Appliance Settings)**.
- 4 Klicken Sie im Bereich „Einstellungen“ auf **NSX Management Service**.
- 5 Klicken Sie auf **Bearbeiten (Edit)** neben **vCenter Server**.
- 6 Nehmen Sie die entsprechenden Änderungen vor.
- 7 Klicken Sie auf **OK**.

## Herunterladen der Protokolle des technischen Supports für NSX

Sie können die Systemprotokolle von NSX Manager und die Protokolle des Web-Managers auf Ihren Desktop herunterladen.

## Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 2 Klicken Sie unter Appliance-Verwaltung auf **Appliance-Einstellungen verwalten**.
- 3 Klicken Sie auf  und anschließend auf **Tech-Support-Protokoll herunterladen**.
- 4 Klicken Sie auf **Herunterladen**.
- 5 Wenn das Protokoll fertig gestellt wurde, klicken Sie auf **Speichern**, um das Protokoll auf Ihren Desktop herunterzuladen.

Das Protokoll ist komprimiert und hat die Dateierweiterung .gz.

## Nächste Schritte

Sie können das Protokoll mit einem Dienstprogramm für die Dekomprimierung öffnen, indem Sie das Speicherverzeichnis für die Datei mit der Option **Alle Dateien** durchsuchen.

## NSX Manager – SSL-Zertifizierung

NSX Manager benötigt ein signiertes Zertifikat, um die Identität des NSX Manager-Webservice zu authentifizieren und um Informationen, die an den NSX Manager-Webserver gesendet werden, zu verschlüsseln. Dazu muss eine Zertifikatsignieranforderung (CSR) generiert werden. Anschließend muss die Anforderung von einer Zertifizierungsstelle signiert und das signierte SSL-Zertifikat in NSX Manager importiert werden. Als empfohlene Vorgehensweise zur Gewährleistung der Sicherheit sollten Sie mit der Option zum Generieren eines Zertifikats einen privaten und einen öffentlichen Schlüssel generieren. Der private Schlüssel wird in NSX Manager gespeichert.

Sie können den integrierten CSR-Generator von NSX Manager oder ein anderes Tool, z. B. OpenSSL, verwenden, um das NSX Manager-Zertifikat abzurufen.

Eine Zertifikatsignieranforderung, die mithilfe des integrierten CSR-Generators von NSX Manager generiert wurde, darf keine erweiterten Attribute enthalten, wie z. B. den alternativen Antragstellernamen (SAN). Wenn Sie erweiterte Attribute aufnehmen möchten, müssen Sie für die Generierung der Zertifikatsignieranforderung ein anderes Tool verwenden. Wenn Sie ein anderes Tool, wie z. B. OpenSSL, zum Generieren der Zertifikatsignieranforderung verwenden, müssen Sie zuerst die Zertifikatsignieranforderung generieren, diese signieren lassen und anschließend mit dem Abschnitt [Konvertieren der NSX Manager-Zertifikatsdatei in das PKCS 12-Format](#) fortfahren.

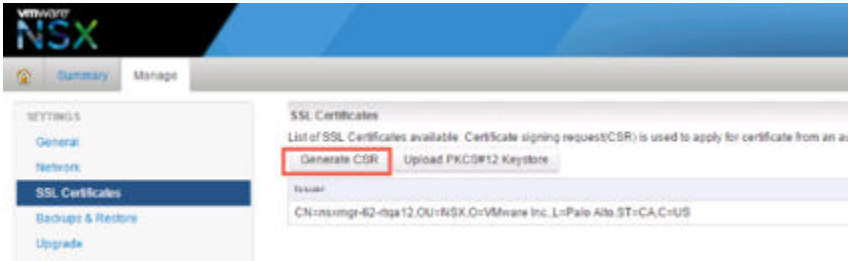
## Verwenden des integrierten CSR-Generators

Eine Möglichkeit, ein SSL-Zertifikat für NSX Manager zu erhalten, besteht darin, den integrierten CSR-Generator zu verwenden.

Diese Methode ist insofern begrenzt, da die Zertifikatsignieranforderung (CSR) keine erweiterten Attribute enthalten darf, wie z. B. den alternativen Antragstellernamen (SAN). Wenn Sie erweiterte Attribute aufnehmen möchten, müssen Sie für die Generierung der Zertifikatsignieranforderung ein anderes Tool verwenden. Wenn Sie ein anderes Tool zur CSR-Generierung einsetzen, können Sie diesen Schritt überspringen.

## Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 2 Klicken Sie auf **Appliance-Einstellungen verwalten (Manage Appliance Settings)**.
- 3 Klicken Sie im Bereich „Einstellungen“ auf **SSL-Zertifikate (SSL Certificates)**.
- 4 Klicken Sie auf **CSR erzeugen (Generate CSR)**.



- 5 Füllen Sie das Formular aus, indem Sie Angaben in den folgenden Feldern machen:

Option	Aktion
<b>Schlüsselgröße (Key Size)</b>	Wählen Sie die Schlüsselgröße aus, die im ausgewählten Algorithmus verwendet wird.
<b>Allgemeiner Name (Common Name)</b>	Geben Sie die IP-Adresse oder den vollqualifizierten Domännennamen (FQDN) von NSX Manager ein. Es wird empfohlen, den FQDN einzugeben.
<b>Organisationseinheit (Organization Unit)</b>	Geben Sie die Abteilung innerhalb des Unternehmens ein, die das Zertifikat anfordert.
<b>Name der Organisation (Organization Name)</b>	Geben Sie den vollständigen eingetragenen Namen des Unternehmens ein.
<b>Ort (City Name)</b>	Geben Sie den vollständigen Namen der Stadt ein, in der Ihr Unternehmen ansässig ist.
<b>Land (State Name)</b>	Geben Sie den vollständigen Namen des Bundeslands/Kantons ein, in dem Ihr Unternehmen ansässig ist.
<b>Ländercode (Country Code)</b>	Geben Sie den zweistelligen Ländercode ein. Der Code für die Vereinigten Staaten lautet beispielsweise <b>US</b> .

- 6 Klicken Sie auf **OK**.
- 7 Senden Sie die Zertifikatsignieranforderung zum Signieren an Ihre Zertifizierungsstelle.
  - a Laden Sie die generierte Anforderung herunter, indem Sie auf **CSR herunterladen (Download CSR)** klicken.  
Bei Verwendung dieser Methode verlässt der private Schlüssel den NSX Manager nie.
  - b Reichen Sie diese Anforderung bei Ihrer Zertifizierungsstelle ein.
  - c Rufen Sie das signierte Zertifikat und das Stamm-CA-Zertifikat sowie alle zwischengeschalteten CA-Zertifikate im PEM-Format ab.

- d Verwenden Sie den folgenden OpenSSL-Befehl, um CER-/DER-formatierte Zertifikate in das PEM-Format zu konvertieren:
- ```
openssl x509 -inform der -in Cert.cer -out 4-nsx_signed.pem
```
- e Fügen Sie alle Zertifikate (Server-, zwischengeschaltete und Rootzertifikate) in einer Textdatei zusammen.
 - f Klicken Sie in der Benutzeroberfläche von NSX Manager auf **Importieren (Import)** und navigieren Sie zur Textdatei mit den Zertifikaten.
 - g Nach erfolgreichem Abschluss des Importvorgangs werden das Serverzertifikat sowie alle CA-Zertifikate auf der Seite „SSL-Zertifikate“ angezeigt.

Nächste Schritte

Importieren Sie das signierte SSL-Zertifikat in NSX Manager.

Konvertieren der NSX Manager-Zertifikatdatei in das PKCS 12-Format

Wenn Sie ein anderes Tool, z. B. OpenSSL, verwendet haben, um das NSX Manager-Zertifikat abzurufen, stellen Sie sicher, dass sowohl das Zertifikat als auch der private Schlüssel im PKCS 12-Format vorliegen. Wenn das NSX Manager-Zertifikat und der private Schlüssel nicht im PKCS 12-Format vorliegen, müssen Sie diese in das PKCS 12-Format konvertieren und dann die PKCS 12-Zertifikatdatei in NSX Manager importieren.

Voraussetzungen

- Stellen Sie sicher, dass OpenSSL auf dem System installiert ist. Sie können OpenSSL von <http://www.openssl.org> herunterladen.
- Generieren Sie ein Schlüsselpaar mit öffentlichem und privatem Schlüssel. Führen Sie beispielsweise folgenden OpenSSL-Befehl aus:

```
openssl req -x509 -days [number of days] -newkey rsa:2048 -keyout my-key.pem -out my-cert.pem
```

Verfahren

- ◆ Führen Sie nach dem Erhalt des signierten Zertifikats vom autorisierten Signierer einen OpenSSL-Befehl aus, um aus der öffentlichen Zertifikatdatei und Ihrem privaten Schlüssel eine PKCS 12-Keystore-Datei (.pfx oder .p12) zu generieren.

Beispiel:

```
openssl pkcs12 -export -in my-cert.pem -inkey my-key.pem -out nsx-manager.p12
```

Dabei gilt:

- my-cert.pem ist das signierte Zertifikat.
- my-key.pem ist der private Schlüssel.

- `nsx-manager.p12` ist der Name der generierten Ausgabedatei nach der Konvertierung in das PKCS 12-Format.

Nächste Schritte

Importieren Sie die PKCS 12-Zertifikatsdatei in NSX Manager.

Importieren eines SSL-Zertifikats

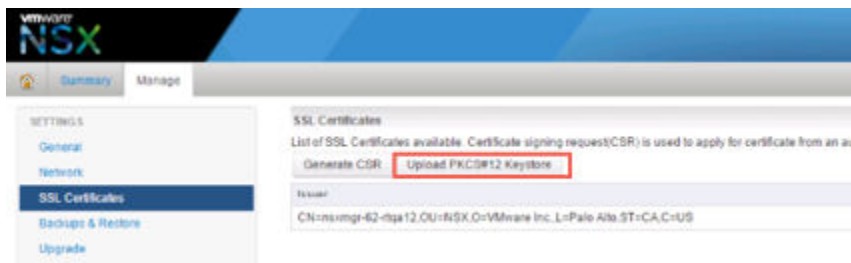
Sie können ein bereits vorhandenes oder von einer Zertifizierungsstelle signiertes SSL-Zertifikat für die Verwendung durch NSX Manager importieren.

Voraussetzungen

Beim Installieren eines Zertifikats auf NSX Manager wird nur das Keystore-Format PKCS#12 unterstützt. Das Zertifikat muss einen einzelnen privaten Schlüssel und das entsprechend signierte Zertifikat oder die Zertifikatskette enthalten.

Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 2 Klicken Sie auf **Appliance-Einstellungen verwalten (Manage Appliance Settings)**.
- 3 Klicken Sie im Bereich „Einstellungen“ auf **SSL-Zertifikate (SSL Certificates)**.
- 4 Klicken Sie auf **PKCS#12-Keystore hochladen (Upload PKCS#12 Keystore)**.



- 5 Klicken Sie auf **Datei auswählen (Choose File)**, um die Datei auszuwählen.
- 6 Klicken Sie auf **Import**.
- 7 Starten Sie die NSX Manager-Appliance neu, um das Zertifikat anzuwenden.

Ergebnisse

Das Zertifikat wird in NSX Manager gespeichert.

Sichern und Wiederherstellen von NSX

Die ordnungsgemäße Sicherung aller NSX-Komponenten ist entscheidend, um bei einem Ausfall das System in einem funktionsfähigen Zustand wiederherzustellen.

Die NSX Manager-Sicherung enthält die gesamte NSX-Konfiguration, inklusive logische Switches und Routing-Entitäten, Sicherheits- und Firewallregeln sowie alle anderen Festlegungen zur Konfiguration mit der NSX Manager-Benutzeroberfläche oder -API. Die vCenter-Datenbank sowie zugehörige Elemente wie die virtuellen Switches müssen gesondert gesichert werden.

Es wird empfohlen, zumindest von NSX Manager und vCenter regelmäßig Sicherungskopien zu erstellen. Je nach geschäftlichen Anforderungen und operativen Verfahren können die Sicherungshäufigkeit und der Zeitplan variieren. Es wird empfohlen, in Zeiten häufiger Konfigurationsänderungen NSX häufig zu sichern.

Sicherungen von NSX Manager können bei Bedarf stündlich, täglich oder wöchentlich vorgenommen werden.

Es wird empfohlen, in den folgenden Szenarios Sicherungskopien zu erstellen:

- Vor der Durchführung eines Upgrades von NSX oder vCenter.
- Nach der Durchführung eines Upgrades von NSX oder vCenter.
- Nach der Bereitstellung von Day Zero und der Erstkonfiguration der NSX-Komponenten, z. B. nach dem Erstellen der NSX-Controller, logischen Switches, logischen Router, Edge Services Gateways, Sicherheit und der Firewallrichtlinien.
- Nach Änderungen an der Infrastruktur oder der Topologie.
- Nach jeder größeren Tag 2-Änderung.

Damit Sie ein Rollback auf den gesamten Systemzustand zu einem bestimmten Zeitpunkt vornehmen können, wird empfohlen, Sicherungen von NSX-Komponenten (z. B. NSX Manager) mit Ihrem Sicherungszeitplan für andere interagierende Komponenten, z. B. vCenter, Cloud-Managementsysteme, operative Tools usw., zu synchronisieren.

Sichern und Wiederherstellen von NSX Manager

Die Sicherung und Wiederherstellung von NSX Manager-Daten kann über die Webschnittstelle der virtuellen Appliance von NSX Manager oder über die NSX Manager-API konfiguriert werden. Stündliche, tägliche oder wöchentliche Backups können geplant werden.

Die Sicherungsdatei wird an einem Remote-FTP- oder SFTP-Speicherort gespeichert, auf den NSX Manager zugreifen kann. Zu den NSX Manager-Daten gehören die Konfiguration, Ereignisse und Audit-Protokolltabellen. Konfigurationstabellen sind in jeder Sicherung enthalten.

Die Wiederherstellung wird nur unterstützt, wenn die Version von NSX Manager mit der Sicherungsversion identisch ist. Aus diesem Grund ist es wichtig, eine Sicherungsdatei vor und nach dem Durchführen eines Upgrades von NSX zu erstellen: eine Datensicherung für die alte Version und eine weitere Datensicherung für die neue Version.

Sichern von NSX Manager-Daten

Sie können NSX Manager-Daten sichern, indem Sie eine bedarfsbasierte oder eine geplante Sicherung durchführen.

Verfahren

- 1 Melden Sie sich bei der virtuellen NSX Manager-Appliance an.
- 2 Klicken Sie auf **Sichern und Wiederherstellen (Backup & Restore)**.
- 3 Um den Sicherungsspeicherort anzugeben, klicken Sie neben den FTP-Server-Einstellungen auf **Ändern (Change)**.
 - a Geben Sie die IP-Adresse oder den Hostnamen des Sicherungssystems ein.
 - b Wählen Sie im Dropdown-Menü **Übertragungsprotokoll (Transfer Protocol)** basierend auf der Unterstützung durch das Zielsystem entweder das Protokoll **SFTP** oder das Protokoll **FTP** aus.
 - c Bearbeiten Sie den Standardport, falls erforderlich.
 - d Geben Sie den Benutzernamen und das Kennwort ein, die zur Anmeldung beim Sicherungssystem erforderlich sind.
 - e Geben Sie im Textfeld **Sicherungsverzeichnis (Backup Directory)** den absoluten Pfad zum Speichern der Sicherungen ein.

Hinweis Wenn Sie kein Sicherungsverzeichnis angeben, wird die Sicherung im Standardverzeichnis (Basisverzeichnis) des FTP-Servers gespeichert.

Um den absoluten Pfad festzustellen, melden Sie sich auf dem FTP-Server an, wechseln Sie in das Verzeichnis, das Sie verwenden möchten, und führen Sie den Befehl zum Anzeigen des aktuellen Arbeitsverzeichnisses (pwd) aus. Beispiel:

```
PS C:\Users\Administrator> ftp 192.168.110.60
Connected to 192.168.110.60.
220 server-nfs FTP server ready.
User (192.168.110.60:(none)): admin
331 Password required for admin.
Password:
230 User admin logged in.
ftp> ls
200 PORT command successful.
150 Opening BINARY mode data connection for 'file list'.
datastore-01
226 Transfer complete.
ftp: 22 bytes received in 0.00Seconds 22000.00Kbytes/sec.
ftp> cd datastore-01
250 CWD command successful.
ftp> pwd
257 "/datastore-01" is current directory.
```

- f Geben Sie in das Feld **Präfix des Dateinamens (Filename Prefix)** eine Textzeichenfolge als Präfix für den Dateinamen ein.

Dieser Text wird jedem Sicherungsdateinamen vorangestellt, damit Sie die Datei einfacher im Sicherungssystem erkennen können. Wenn Sie beispielsweise **ppdb** eingeben, lautet der Sicherungsname *ppdbHH_MM_SS_JJJJ_Mon_Tag*.

Hinweis Dateien im Backup-Verzeichnis müssen auf 100 begrenzt werden. Wenn die Anzahl der Dateien im Verzeichnis diesen Grenzwert überschreitet, wird eine Warnmeldung angezeigt.

- g Geben Sie zum Sichern der Sicherung einen Kennwortsatz ein.

Dieser Kennwortsatz wird benötigt, um die Sicherung wiederherzustellen.

- h Klicken Sie auf **OK**.

Beispiel:

| Option | Beispiel |
|------------------------|----------------|
| IP/Hostname | 192.168.110.60 |
| Übertragungsprotokoll | FTP |
| Port | 21 |
| Benutzername | Admin |
| Kennwort | ***** |
| Sicherungsverzeichnis | /datastore-01 |
| Präfix des Dateinamens | nsxmgr-backup |
| Kennwortsatz | ***** |

- 4 Klicken Sie für eine bedarfsbasierte Sicherung auf **Sichern (Backup)**.

Unter **Sicherungsverlauf (Backup History)** wird eine neue Datei hinzugefügt.

- 5 (Erforderlich) Klicken Sie für geplante Sicherungen neben „Zeitplan“ auf **Ändern (Change)**.
- Wählen Sie im Dropdown-Menü **Häufigkeit der Sicherungsvorgänge (Backup Frequency)** die Option **Stündlich (Hourly)**, **Täglich (Daily)** oder **Wöchentlich (Weekly)** aus. Je nach ausgewählter Häufigkeit werden die Dropdown-Menüs „Wochentag“, „Stunde des Tages“ und „Minute“ deaktiviert. Wenn Sie beispielsweise „Täglich“ auswählen, wird das Dropdown-Menü „Wochentag“ deaktiviert, da dieses Dropdown-Menü bei einer täglichen Sicherung nicht zum Tragen kommt.
 - Wählen Sie für eine wöchentliche Sicherung den Wochentag aus, an dem die Daten gesichert werden sollen.
 - Wählen Sie für eine wöchentliche oder tägliche Sicherung die Stunde aus, zu der die Sicherung beginnen soll.
 - Wählen Sie die Minute aus, zu der die Sicherung beginnen soll, und klicken Sie auf **Zeitplan (Schedule)**.

| Option | Beispiel |
|-----------------------------------|-------------|
| Häufigkeit der Sicherungsvorgänge | Wöchentlich |
| Wochentag | Fr |
| Stunde des Tages | 15 |
| Minute | 45 |

- 6 Um Protokolle und Flussdaten von der Sicherung auszuschließen, klicken Sie neben „Ausschließen“ auf **Ändern (Change)**.
 - a Wählen Sie die Objekte aus, die Sie von der Sicherung ausschließen möchten.
 - b Klicken Sie auf **OK**.
- 7 Bewahren Sie die IP-Adresse bzw. den Hostnamen Ihres FTP-Servers, die Anmeldedaten, die Verzeichnisdetails und die Passphrase auf. Diese Informationen sind erforderlich, um die Sicherung wiederherzustellen.

Wiederherstellen eines NSX Manager-Backups

Durch das Wiederherstellen von NSX Manager wird eine Sicherungsdatei auf eine NSX Manager-Appliance geladen. Die Sicherungsdatei muss in einem Remote-FTP- oder SFTP-Speicherort gespeichert werden, auf den NSX Manager zugreifen kann. Zu den NSX Manager-Daten gehören die Konfiguration, Ereignisse und Audit-Protokolltabellen.

Wichtig Sichern Sie Ihre aktuellen Daten, bevor Sie eine Sicherungsdatei wiederherstellen.

Voraussetzungen

Bevor Sie NSX Manager-Daten wiederherstellen, sollten Sie die NSX Manager-Appliance neu installieren. Das Ausführen des Wiederherstellungsvorgangs auf einer vorhandenen NSX Manager-Appliance kann zwar gelingen, wird jedoch nicht unterstützt. Es wird davon ausgegangen, dass der bestehende NSX Manager ausgefallen ist. Daher wird eine neue NSX Manager-Appliance bereitgestellt.

Gemäß Best Practice notieren Sie die aktuellen Einstellungen der alten NSX Manager-Appliance, damit sie für die Angabe von Informationen zu IP-Adressen und zum Sicherungsspeicherort für die neu bereitgestellte NSX Manager-Appliance verfügbar sind.

Verfahren

- 1 Notieren Sie alle Einstellungen auf der vorhandenen NSX Manager-Appliance. Notieren Sie auch die FTP-Servereinstellungen.
- 2 Stellen Sie eine neue NSX Manager-Appliance bereit.
Die Version muss mit der gesicherten NSX Manager-Appliance identisch sein.
- 3 Melden Sie sich bei der neuen NSX Manager-Appliance an.
- 4 Klicken Sie unter „Appliance-Verwaltung“ auf **Sicherung und Wiederherstellung (Backups & Restore)**.

- 5 Klicken Sie in den FTP-Servereinstellungen auf **Ändern (Change)** und fügen Sie die FTP-Servereinstellungen hinzu.

Die Felder **Host-IP-Adresse (Host IP Address)**, **Benutzername (User Name)**, **Kennwort (Password)**, **Sicherungsverzeichnis (Backup Directory)**, **Präfix des Dateinamens (Filename Prefix)** und **Kennwortsatz (Pass Phrase)** im Bildschirm „Sicherungsspeicherort“ müssen den Speicherort der wiederherzustellenden Sicherungsdatei identifizieren.

Im Abschnitt **Sicherungsverlauf (Backup History)** wird der Sicherungsordner angezeigt.

Hinweis Wenn der Sicherungsordner im Abschnitt **Sicherungsverlauf (Backup History)** nicht enthalten ist, überprüfen Sie die FTP-Servereinstellungen. Prüfen Sie, ob Sie eine Verbindung mit dem FTP-Server herstellen können, und zeigen Sie den Sicherungsordner an.

- 6 Wählen Sie im Abschnitt **Sicherungsverlauf (Backup History)** den erforderlichen Sicherungsordner für die Wiederherstellung aus und klicken Sie auf **Wiederherstellen (Restore)**.

Die Wiederherstellung der NSX Manager-Daten wird gestartet.

Ergebnisse


Die NSX-Konfiguration wird für den NSX Manager wiederhergestellt.

Vorsicht Nach der Wiederherstellung einer NSX Manager-Sicherung müssen Sie möglicherweise zusätzliche Maßnahmen für den ordnungsgemäßen Betrieb der NSX Edge-Appliances und der logischen Switches durchführen. Siehe [Wiederherstellen von NSX Edges](#) und [Auflösen von Synchronisationsfehlern auf logischen Switches](#).

Wiederherstellen von NSX Edges

Alle NSX Edge-Konfigurationen (logische Router und Gateways für Edge-Dienste) werden als Teil der NSX Manager-Datensicherung gesichert.

Individuelle Sicherungen von NSX Edge werden nicht unterstützt.

Wenn Sie über eine intakte NSX Manager-Konfiguration verfügen, können Sie eine Edge-Appliance-VM, auf die nicht zugegriffen werden kann oder auf der ein Fehler aufgetreten ist, durch erneutes Bereitstellen des NSX Edge neu erstellen (klicken Sie auf **NSX Edge erneut bereitstellen (Redeploy NSX Edge)** ) in vSphere Web Client). Weitere Informationen finden Sie unter „Erneutes Bereitstellen von NSX Edge“ im Dokument *Administratorhandbuch für NSX*.

Vorsicht Nach der Wiederherstellung einer NSX-Manager-Sicherung müssen Sie möglicherweise zusätzliche Maßnahmen für den ordnungsgemäßen Betrieb der NSX Edge-Appliances durchführen.

- Edge-Appliances, die nach der letzten Sicherung erstellt wurden, werden bei der Wiederherstellung nicht entfernt. Sie müssen die virtuelle Maschine manuell löschen.
- Edge-Appliances, die nach der letzten Sicherung gelöscht wurden, werden nicht wiederhergestellt, solange sie nicht erneut bereitgestellt werden.
- Wenn bei der Wiederherstellung einer Sicherung sowohl die konfigurierten wie die aktuellen Speicherorte einer in der Sicherung gespeicherten NSX Edge-Appliance nicht mehr vorhanden sind, können Vorgänge wie das erneute Bereitstellen, das Migrieren oder das Aktivieren/Deaktivieren der Hochverfügbarkeit nicht durchgeführt werden. Sie müssen die Appliance-Konfiguration bearbeiten und gültige Speicherortinformationen zur Verfügung stellen. Bearbeiten Sie mit `PUT /api/4.0/edges/{edgeId}/appliances` die Konfiguration des Appliance-Speicherorts (*resourcePoolId*, *datastoreId*, *hostId* und *vmFolderId* wie erforderlich). Informationen dazu finden Sie unter „Arbeiten mit der NSX Edge-Appliance-Konfiguration“ im Dokument *Handbuch zu NSX-API*.

Wenn eine der im Folgenden aufgeführten Änderungen seit der letzten NSX Manager-Sicherung vorgenommen wurden, unterscheiden sich die wiederhergestellte NSX Manager-Konfiguration und die Konfiguration auf der NSX Edge-Appliance. Sie müssen die Option **Synchronisierung erzwingen (Force Sync)** für das NSX Edge ausführen, um diese Änderungen für die Appliance rückgängig zu machen und den ordnungsgemäßen Betrieb des NSX Edge zu gewährleisten. Informationen dazu finden Sie unter „Erzwingen der Synchronisierung von NSX Edge mit NSX Manager“ im Dokument *Administratorhandbuch für NSX*.

- Änderungen, die über die verteilte Firewall für vordefinierte Regeln für die NSX Edge-Firewall vorgenommen wurden.
- Änderungen bei der Mitgliedschaft gruppierter Objekte.

Wenn eine der im Folgenden aufgeführten Änderungen seit der letzten NSX Manager-Sicherung vorgenommen wurden, unterscheiden sich die wiederhergestellte NSX Manager-Konfiguration und die Konfiguration auf der NSX Edge-Appliance. Sie müssen die Option **Erneut bereitstellen (Redeploy)** für NSX Edge aufrufen, um diese Änderungen für die Appliance wiederherzustellen und den ordnungsgemäßen Betrieb des NSX Edge zu gewährleisten. Weitere Informationen finden Sie unter „Erneutes Bereitstellen von NSX Edge“ im Dokument *Administratorhandbuch für NSX*.

- Änderungen der Edge-Appliance-Einstellungen:
 - HA aktiviert oder deaktiviert
 - Status der Appliance von „Bereitgestellt“ zu „Nicht bereitgestellt“ geändert
 - Status der Appliance von „Nicht bereitgestellt“ zu „Bereitgestellt“ geändert
 - Einstellungen für die Ressourcenreservierung geändert
- Änderungen der vNIC-Einstellungen der Edge-Appliance:
 - Hinzufügen, Entfernen oder Trennen der vNIC
 - Portgruppen
 - Trunk-Ports

Auflösen von Synchronisationsfehlern auf logischen Switches

Wenn zwischen dem Zeitpunkt der Sicherung und Wiederherstellung von NSX Manager auf logischen Switches Änderungen aufgetreten sind, melden die logischen Switches möglicherweise, dass sie nicht synchron laufen.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Navigieren Sie zu **Netzwerk und Sicherheit (Networking & Security) > Logische Switches (Logical Switches)**.
- 3 Falls vorhanden, klicken Sie auf den Link **+++Nicht synchron+++ (Out of sync)** in der Spalte „Status“, um Details zu dem Fehler anzuzeigen.
- 4 Klicken Sie auf **Auflösen (Resolve)**, um fehlende Backing-Portgruppen für den logischen Switch neu zu erstellen.

Sichern von vSphere Distributed Switches

Sie können Konfigurationen von vSphere Distributed Switches und verteilten Portgruppen in eine Datei exportieren.

Die Datei behält gültige Netzwerkkonfigurationen bei, sodass die Verteilung dieser Konfigurationen an andere Bereitstellungen möglich ist.

vSphere Distributed Switch- und Portgruppeneinstellungen werden im Rahmen des Importvorgangs importiert.

Best Practice ist, die vSphere Distributed Switch-Konfiguration zu exportieren, bevor Sie den Cluster für VXLAN vorbereiten. Eine detaillierte Anleitung finden Sie unter <http://kb.vmware.com/kb/2034602>.

Sichern von vCenter

Zum Sichern Ihrer NSX-Bereitstellung ist es wichtig, ein Backup der vCenter-Datenbank und Snapshots der virtuellen Maschinen zu erstellen.

Weitere Informationen zu den vCenter-Sicherungs- und -Wiederherstellungsverfahren sowie zu den Best Practices finden Sie in der vCenter-Dokumentation.

Weitere Informationen zu VM-Snapshots finden Sie unter <http://kb.vmware.com/kb/1015180>.

Nützliche Links für vCenter 5.5:

- <http://kb.vmware.com/kb/2057353>
- <http://kb.vmware.com/kb/2034505>
- <http://www.vmware.com/files/pdf/techpaper/vmware-vcenter-server-availability-guide.pdf>

Nützliche Links für vCenter 6.0:

- <https://pubs.vmware.com/vsphere-60/topic/com.vmware.vsphere.install.doc/GUID-539B47B4-114B-49BC-9736-F14058127ECA.html>

- <http://kb.vmware.com/kb/2110294>

Flow Monitoring

Flow Monitoring ist ein Tool zur Datenverkehrsanalyse, das Ihnen detaillierte Informationen zum Datenverkehr zu und von geschützten virtuellen Maschinen liefert. Wenn Flow Monitoring aktiviert ist, definiert die Ausgabe, welche Maschinen Daten über welche Anwendung austauschen. Diese Daten umfassen die Anzahl von Sitzungen und Paketen, die pro Sitzung übertragen werden. Die Sitzungsdetails umfassen die Quellen, Ziele, Anwendungen sowie die verwendeten Ports. Anhand der Sitzungsdetails können Firewallregeln für das Zulassen oder Blockieren von Datenverkehr erstellt werden.

Sie können Flow-Daten für viele verschiedene Protokolltypen anzeigen, z. B. für TCP, UDP, ARP, ICMP usw. Sie können TCP- und UDP-Verbindungen zu und von einer ausgewählten vNIC in Echtzeit überwachen. Sie können auch Flows durch das Festlegen von Filtern ausschließen.

Flow Monitoring kann demzufolge als forensisches Tool zum Ermitteln von nicht autorisierten Diensten sowie zum Untersuchen ausgehender Sitzungen genutzt werden.

Anzeigen von Flow Monitoring-Daten

Sie können Datenverkehrssitzungen auf virtuellen Maschinen innerhalb der angegebenen Zeitspanne anzeigen. Standardmäßig werden die Daten der letzten 24 Stunden angezeigt. Der Minimalwert für die Zeitspanne beträgt eine Stunde, der Maximalwert zwei Wochen.

Voraussetzungen

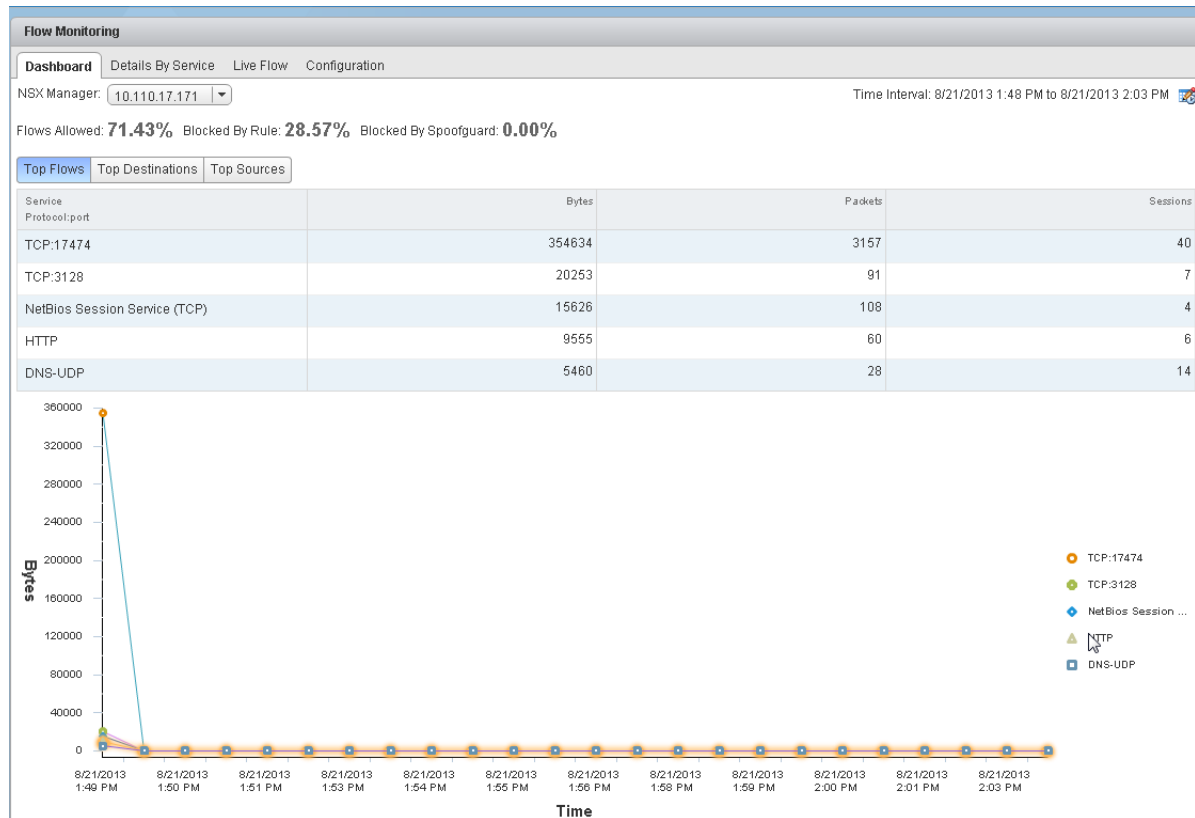
Flow Monitoring-Daten sind nur für virtuelle Maschinen in Clustern verfügbar, auf denen die Netzwerkvirtualisierungskomponenten installiert und die Firewall aktiviert ist. Weitere Informationen finden Sie unter *Installationshandbuch für NSX*.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Networking & Security** im linken Navigationsbereich und wählen Sie anschließend **Flow Monitoring**.
- 3 Stellen Sie sicher, dass Sie sich auf der Registerkarte **Dashboard** befinden.

4 Klicken Sie auf **Flow Monitoring**.

Das Laden dieser Seite kann einige Sekunden in Anspruch nehmen. Der obere Rand der Seite zeigt den Prozentsatz für den zulässigen Datenverkehr, für den durch die Firewallregeln blockierten Datenverkehr und für den durch SpoofGuard blockierten Datenverkehr an. Das Mehrfach-Liniendiagramm zeigt den Datenfluss für jeden Dienst in Ihrer Umgebung an. Wenn Sie auf einen Dienst in der Legenden-Area zeigen, wird der Plot für diesen Dienst hervorgehoben.



Die Statistiken zum Datenverkehr werden auf drei Registerkarten angezeigt:

- **Wichtigste Flows (Top Flows)** zeigt den gesamten eingehenden und ausgehenden Datenverkehr pro Dienst über den angegebenen Zeitraum an, basierend auf dem Gesamtbytewert (nicht basierend auf Sitzungen/Paketen). Es werden die fünf Top-Dienste angezeigt. Blockierte Flows werden bei der Berechnung der wichtigsten Flows nicht berücksichtigt.
- **Wichtigste Ziele (Top Destinations)** zeigt den eingehenden Datenverkehr pro Ziel über den angegebenen Zeitraum an. Es werden die fünf Top-Ziele angezeigt.
- **Wichtigste Quellen (Top Sources)** zeigt den ausgehenden Datenverkehr pro Quelle über den angegebenen Zeitraum an. Es werden die fünf Top-Quellen angezeigt.

5 Klicken Sie auf die Registerkarte **Details je nach Dienst (Details by Service)**.

Es werden detaillierte Informationen zum gesamten Datenverkehr für den ausgewählten Dienst angezeigt. Die Registerkarte **Zulässige Flows (Allowed Flows)** enthält die zulässigen Datenverkehrssitzungen, die Registerkarte **Gesperrte Flows (Blocked Flows)** den blockierten Datenverkehr.

Sie können nach Dienstnamen suchen.

Flow Monitoring

Dashboard **Details By Service** Live Flow Configuration

NSX Manager: 10.110.17.171 Time Interval: 8/23/2013 6:10 AM to 8/23/2013 6:25 AM

Allowed Flows Blocked Flows

Filter

| Type | Service | Bytes | Sessions |
|-------|-----------------|-------|----------|
| UDP | DHCP-Server | 4954 | 6 |
| TCP | TCP:17474 | 2224 | 1 |
| OTHER | IPv6-ICMP:0 | 1872 | 18 |
| OTHER | ARP | 1196 | 26 |
| OTHER | 0xfff | 162 | 2 |
| UDP | NTP Time Server | 152 | 1 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

6 items

Filter

| Rule Id | Time Stamp | Source | Source User(s) | Destination | Packets | Actions |
|---------|-------------------|----------------|----------------|---------------|---------|--------------------|
| 1021 | 8/23/2013 6:15 AM | 10.112.243.233 | Unknown | 10.112.192.5 | 2 | Add Rule Edit Rule |
| 1021 | 8/23/2013 6:15 AM | DB_server | Unknown | 10.112.192.5 | 2 | Add Rule Edit Rule |
| 1021 | 8/23/2013 6:15 AM | win32rdpclone | Unknown | 10.112.192.6 | 2 | Add Rule Edit Rule |
| 1021 | 8/23/2013 6:14 AM | 10.112.243.214 | Unknown | 10.112.192.6 | 2 | Add Rule Edit Rule |
| 1021 | 8/23/2013 6:12 AM | win32rdpclone | Unknown | 10.112.192.5 | 2 | Add Rule Edit Rule |
| 1021 | 8/23/2013 6:11 AM | 10.112.243.229 | Unknown | 10.112.192.6 | 2 | Add Rule Edit Rule |
| 1021 | 8/23/2013 6:13 AM | win32rdpclone | Unknown | 10.113.60.150 | 12 | Add Rule Edit Rule |


6 Klicken Sie auf ein Element in der Tabelle, um die Regeln anzuzeigen, die den Datenverkehr zugelassen oder blockiert haben.

7 Klicken Sie auf **Regel-ID (Rule Id)**, um die Regeldetails anzuzeigen.

Ändern des Datumsbereichs der Flow Monitoring-Diagramme

Sie können den Datumsbereich der Flow Monitoring-Daten ändern, um die Registerkarten „Dashboard“ und „Details“ anzuzeigen.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Networking & Security** im linken Navigationsbereich und wählen Sie anschließend **Flow Monitoring**.
- 3 Klicken Sie neben **Zeitintervall (Time interval)** auf .

- 4 Wählen Sie den Zeitraum aus oder geben Sie ein neues Start- und Enddatum ein.

Die maximale Zeitspanne, für die Sie Verkehrsflussdaten anzeigen können, sind die letzten zwei Wochen.

- 5 Klicken Sie auf **OK**.

Hinzufügen oder Bearbeiten einer Firewallregel vom Flow Monitoring-Bericht aus

Indem Sie einen Drilldown für die Datenverkehrsdaten durchführen, können Sie die Nutzung Ihrer Ressourcen auswerten und Sitzungsinformationen an die verteilte Firewall senden, um auf jeder beliebigen Ebene eine neue Regel zum Zulassen oder Ablehnen von Datenverkehr zu erstellen.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Networking & Security** im linken Navigationsbereich und wählen Sie anschließend **Flow Monitoring**.
- 3 Klicken Sie auf die Registerkarte **Details je nach Dienst (Details by Service)**.
- 4 Klicken Sie auf einen Dienst, um den Datenfluss für diesen Dienst anzuzeigen.

Je nach der ausgewählten Registerkarte werden Regeln, die Datenverkehr für diesen Dienst zugelassen oder abgelehnt haben, angezeigt.

- 5 Klicken Sie auf eine Regel-ID, um die Regeldetails anzuzeigen.
- 6 Führen Sie einen der folgenden Schritte aus:

- So bearbeiten Sie eine Regel:

- 1 Klicken Sie in der Spalte **Aktionen (Actions)** auf **Regel bearbeiten (Edit Rule)**.
- 2 Ändern Sie den Namen, die Aktion oder die Anmerkungen zur Regel.
- 3 Klicken Sie auf „OK“.

- So fügen Sie eine Regel hinzu:

- 1 Klicken Sie in der Spalte **Aktionen (Actions)** auf **Regel hinzufügen (Add Rule)**.
- 2 Füllen Sie das Formular vollständig aus, um die Regel hinzuzufügen. Weitere Informationen zum Ausfüllen des Formulars für Firewallregeln finden Sie unter [Hinzufügen einer Regel für die verteilte Firewall](#).
- 3 Klicken Sie auf **OK**.

Die Regel wird oben in den Firewallregelabschnitt eingefügt.

Anzeigen von Live-Flow

Sie können UDP- und TCP-Verbindungen von und zu einer ausgewählten vNIC anzeigen. Wenn Sie den Datenverkehr zwischen zwei virtuellen Maschinen anzeigen möchten, können Sie den Live-Datenverkehr

für eine virtuelle Maschine auf einem Computer und die andere virtuelle Maschine auf einem zweiten Computer anzeigen. Sie können den Datenverkehr für maximal zwei vNICs pro Host und für fünf vNICs pro Infrastruktur anzeigen.

Das Anzeigen von Live-Flows kann sich auf die Leistung des NSX Manager und auf die entsprechende virtuelle Maschine auswirken.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Wählen Sie **Networking & Security** im linken Navigationsbereich und wählen Sie anschließend **Flow Monitoring**.
- 3 Klicken Sie auf die Registerkarte **Live-Flow (Live Flow)**.
- 4 Klicken Sie auf **Durchsuchen (Browse)** und wählen Sie eine vNIC aus.
- 5 Klicken Sie auf **Start**, um die Anzeige des Live-Flows zu beginnen.

Diese Seite wird alle 5 Sekunden aktualisiert. Sie können eine andere Frequenz aus dem Dropdown-Menü **Aktualisierungsrate (Refresh Rate)** auswählen.

Flow Monitoring

Dashboard Details By Service **Live Flow** Configuration

NSX Manager: 10.24.130.213

Live Flow will be shown for the selected vNic. Please select a vNic and press start to see the live flows

vNic: app-sv12 - Network adapter 1 [Browse](#)

Refresh Rate: 5 Seconds

Legend: ■ New active flows ■ Flows with state change ■ Terminated flows

| RuleId | Direction | Flow Type | Protocol | Source IP | Source Port | Destination IP | Destination Port | state | Incoming Bytes | Incoming Packets | Outgoing Bytes | Outgoing Packets |
|--------|-----------|-----------|----------|---------------|-------------|----------------|------------------|----------|----------------|------------------|----------------|------------------|
| 1026 | OUT | Active | TCP | 172.16.40.121 | 49099 | 172.16.40.131 | 3306 | FINWAIT2 | 747 | 11 | 2077 | 9 |
| 1026 | OUT | Inactive | TCP | 172.16.40.121 | 49098 | 172.16.40.131 | 3306 | FINWAIT2 | 747 | 11 | 2077 | 9 |

- 6 Klicken Sie auf **Beenden (Stop)**, wenn das Debugging oder die Fehlerbehebung abgeschlossen ist, um Auswirkungen auf die Leistung des NSX Manager oder auf die ausgewählte virtuelle Maschine zu vermeiden.

Konfigurieren der Erfassung von Flow Monitoring-Daten

Nachdem Sie die Flow Monitoring-Daten, die Sie erfassen möchten, angezeigt und gefiltert haben, können Sie die Datenerfassung konfigurieren. Angezeigte Daten können mithilfe eines Ausschlusskriteriums gefiltert werden. Beispielsweise möchten Sie möglicherweise einen Proxy-Server ausschließen, um das Anzeigen doppelter Flows zu vermeiden. Wenn Sie eine Nessus-Prüfung auf den virtuellen Maschinen in Ihrer Bestandsliste ausführen, möchten Sie die Prüfungs-Flows möglicherweise von der Erfassung ausschließen. Sie können IPFix konfigurieren, sodass Informationen für bestimmte Flows direkt aus einer Firewall in einen Flow-Collector exportiert werden. Die Flow Monitoring-Diagramme enthalten nicht die IPFix-Flows. Diese werden in der Schnittstelle des IPFix-Collectors angezeigt.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.

- 2 Wählen Sie **Networking & Security** im linken Navigationsbereich und wählen Sie anschließend **Flow Monitoring**.
- 3 Wählen Sie die Registerkarte **Konfiguration (Configuration)**.
- 4 Stellen Sie sicher, dass **Globaler Flow-Erfassungstatus (Global Flow Collection Status)** auf **Aktiviert (Enabled)** eingestellt ist.

Alle auf die Firewall bezogenen Flows werden über Ihre Bestandsliste außer für die in **Ausschlusseinstellungen (Exclusion Settings)** angegebenen Objekte erfasst.

- 5 Klicken Sie zum Festlegen der Filterkriterien auf **Flow-Ausschluss (Flow Exclusion)** und führen Sie die folgenden Schritte aus.

- a Klicken Sie auf die entsprechende Registerkarte zum Ausschließen der Flows.

Flow Monitoring

Dashboard Details By Service Live Flow **Configuration**

NSX Manager: 10.110.8.93

Global Flow Collection Status: **Enabled** Disable

Flow Exclusion IPFIX

Exclusion Settings
System will not collect flows that match the specified condition

| Filter | |
|-----------------------|--|
| Collect Blocked Flows | Yes |
| Collect Layer2 Flows | Yes |
| Source | |
| Destination | system-generated-broadcast-macset, 224.0.0.0/24, 255.255.255.255 |
| Destination ports | 138,137 |
| Service | |

System is configured to collect all firewall related flows except those that match the conditions specified below

Detail Collection Policy: (Click Save to commit changes to settings)

| | |
|------------------------|---|
| Collect Blocked Flows: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Collect Layer2 Flows: | <input checked="" type="radio"/> Yes <input type="radio"/> No |

Save

- b Geben Sie die erforderlichen Informationen an.

| Bei Auswahl von | Geben Sie die folgenden Informationen an |
|---------------------------------|---|
| Gesperrte Flows erfassen | Wählen Sie „Nein“ aus, um blockierte Flows auszuschließen. |
| Schicht 2-Flows erfassen | Wählen Sie „Nein“ aus, um Schicht 2-Flows auszuschließen. |
| Quelle | Flows werden nicht für die angegebenen Quellen erfasst.
1 Klicken Sie auf das Symbol Hinzufügen (Add) .
2 Wählen Sie in „Ansicht“ den entsprechenden Container aus.
3 Wählen Sie die auszuschließenden Objekte aus. |
| Ziel | Flows werden nicht für die angegebenen Ziele erfasst.
1 Klicken Sie auf das Symbol Hinzufügen (Add) .
2 Wählen Sie in „Ansicht“ den entsprechenden Container aus.
3 Wählen Sie die auszuschließenden Objekte aus. |
| Zielports | Schließt Flows zu den angegebenen Ports aus.
Geben Sie die auszuschließenden Portnummern ein. |
| Dienst | Schließt Flows für die angegebenen Dienste und Dienstgruppen aus.
1 Klicken Sie auf das Symbol Hinzufügen (Add) .
2 Wählen Sie die entsprechenden Dienste und/oder Dienstgruppen aus. |

- c Klicken Sie auf **Speichern (Save)**.

- 6 Zum Konfigurieren der Flow-Erfassung klicken Sie auf **IPFIX** und folgen Sie den aufgeführten Schritten in [IPFIX für verteilte Firewall](#).

7 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

Konfigurieren von IPFIX

IPFIX (Internet Protocol Flow Information Export) ist ein IETF-Protokoll, das den Standard-Export der Flow-Informationen von einem Endgerät auf ein Überwachungssystem definiert. NSX unterstützt IPFIX für den Export von IP-Flow-Informationen an einen Collector.

IPFIX kann aktiviert werden auf:

- vSphere Distributed Switch (VDS)
- Verteilte Firewall (Distributed Firewall, DFW)

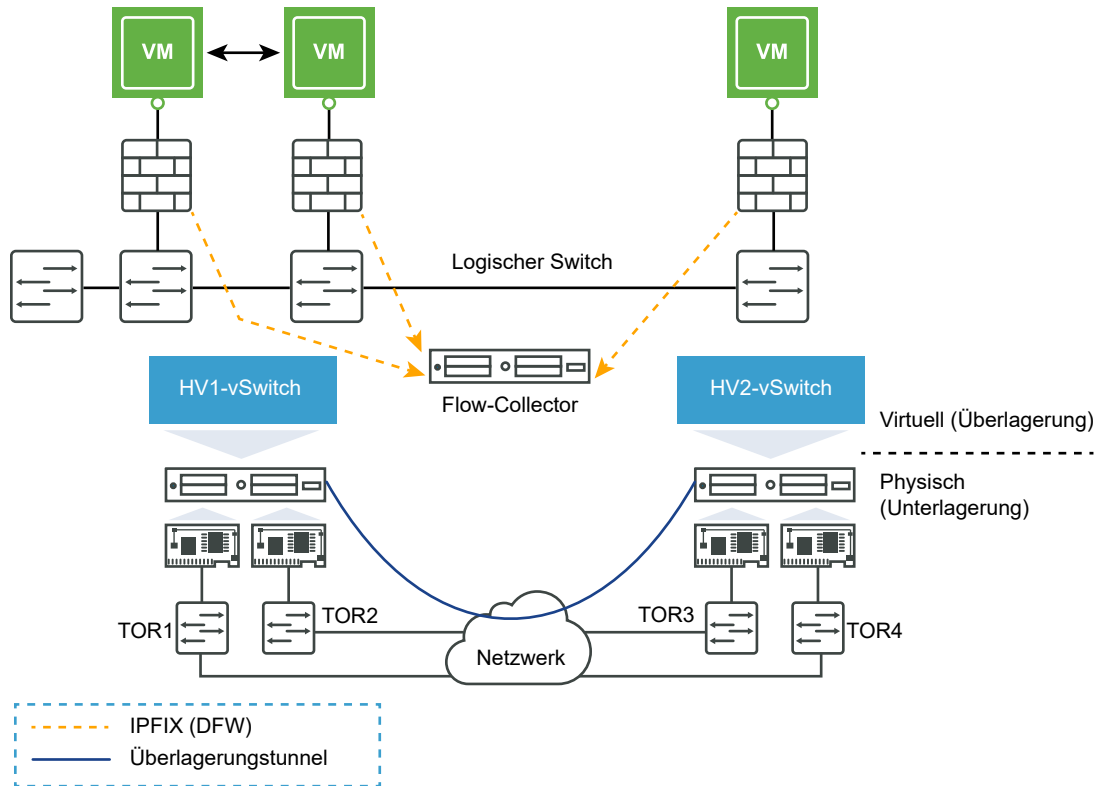
In der vSphere-Umgebung ist vSphere Distributed Switch der Exporteur, und der Collector ist ein beliebiges Überwachungstool, das von jedem beliebigen Netzwerkanbieter verfügbar ist.

Der IPFIX-Standard gibt an, wie IP-Flow-Informationen präsentiert und von einem Exporteur an einen Collector übertragen werden.

Nach der Aktivierung von IPFIX auf dem vSphere Distributed Switch werden in regelmäßigen Abständen Nachrichten an das Collector-Tool gesendet. Die Inhalte dieser Meldungen werden unter Verwendung der Vorlagen definiert. Weitere Informationen zu den Vorlagen finden Sie unter [IPFIX-Vorlagen](#).

IPFIX für verteilte Firewall

Sie können IPFIX auf einer verteilten Firewall aktivieren. Verteilte Firewall implementiert die zustandsabhängige Verfolgung von Datenflüssen, und die nachverfolgten Datenflüsse durchlaufen eine Reihe von Zustandsänderungen. IPFIX kann verwendet werden, um Daten über den Status eines Flows zu exportieren. Die nachverfolgten Ereignisse enthalten eine Flow-Erstellung, Flow-Verweigerung, Flow-Aktualisierung und einen Flow-Abbau.



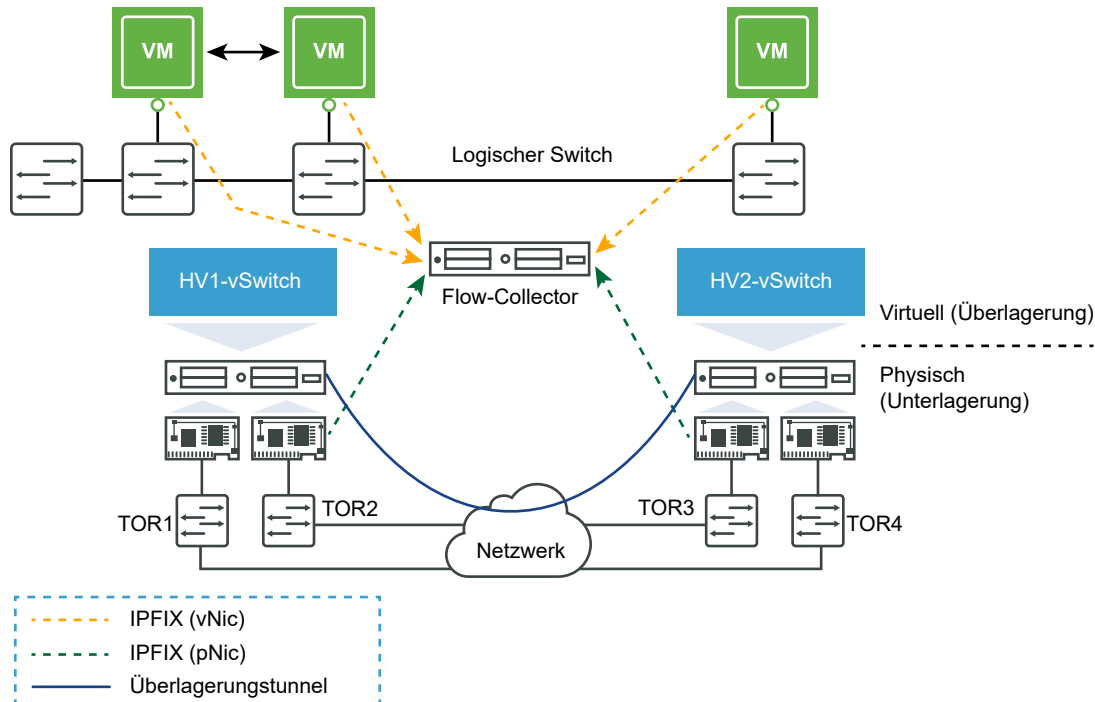
Sie können einen Flow-Export für IPFIX auf einer verteilten Firewall wie folgt aktivieren:

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann unter **Tools** auf **Flow Monitoring**.
- 3 Wählen Sie die Registerkarte **Konfiguration (Configuration)**.
- 4 Stellen Sie sicher, dass **Globaler Flow-Erfassungstatus (Global Flow Collection Status)** auf **Aktiviert (Enabled)** eingestellt ist.
- 5 Zum Konfigurieren der Flow-Erfassung klicken Sie auf **IPFix** und folgen den unten aufgeführten Schritten.
 - a Klicken Sie neben „IPFix-Konfiguration“ auf **Bearbeiten (Edit)** und anschließend auf **IPFix-Konfiguration aktivieren (Enable IPFix Configuration)**.
 - b Geben Sie in **Beobachtungs-DomainID (Observation DomainID)** einen 32-Bit-Bezeichner ein, der den Firewall-Exporter für den Flow-Collector identifiziert. Der gültige Bereich ist 0-65535.
 - c Geben Sie im Feld **Zeitüberschreitung bei aktivem Flow-Export (Active Flow Export Timeout)** die Zeit (in Minuten) ein, nach der aktive Flows in den Flow-Collector exportiert werden sollen. Die Standardwert ist fünf. Beispiel: Wenn der Flow für 30 Minuten aktiv ist und die Zeitüberschreitung für das Exportieren fünf Minuten beträgt, wird der Flow während seiner Lebensdauer sieben Mal exportiert. Einmal für jede Erstellung und Löschung und fünf Mal während des aktiven Zeitraums.

- d Klicken Sie in **Collector-IPs (Collector IPs)** auf das Symbol „Hinzufügen (add)“ und geben Sie die IP-Adresse und den UDP-Port des Flow-Collectors ein. Informationen zur Bestimmung der Portnummer finden Sie in Ihrer NetFlow-Collector-Dokumentation.
 - e Klicken Sie auf **OK**.
- 6 Klicken Sie auf **Änderungen veröffentlichen (Publish Changes)**.

IPFIX für Logischen Switch

Sie können IPFIX auf dem vSphere Distributed Switch aktivieren.



Sie können IPFIX für ein Logischer Switch wie folgt aktivieren:

- 1 Konfigurieren Sie den NetFlow-Collector auf dem vSphere Distributed Switch, der die Transportzone NSX unterstützt (logischer Switch). Weitere Informationen zum Konfigurieren des NetFlow-Collectors finden Sie unter „Konfigurieren der NetFlow-Einstellungen eines vSphere Distributed Switch“ im vSphere-Netzwerkhandbuch.
- 2 Sie können die NetFlow-Überwachung für die dem logischen Switch entsprechende verteilte Portgruppe aktivieren. Wenn sich die Transportzone NSX über mehrere vSphere Distributed Switches (VDS) erstreckt, wiederholen Sie diese Schritte für jede VDS/verteilte Portgruppe. Weitere Informationen zum Aktivieren der NetFlow-Überwachung finden Sie unter „Aktivieren oder Deaktivieren der NetFlow-Überwachung für eine verteilte Portgruppe oder einen verteilten Port“ in der vSphere-Dokumentation.

In einer NSX-Umgebung ist der Datenverkehr der virtuellen Maschine auf einem logischen Switch, der den NSX Uplink von ESXi durchquert, VXLAN-verkapselt. Wenn NetFlow auf dem Host Uplink aktiviert ist, werden die IP-Flow-Datensätze mithilfe einer benutzerdefinierten IPFIX Flow-Datensatz-Vorlage exportiert. Die Vorlage enthält die äußeren VXLAN UDP/IP-Header-Informationen und die Informationen des internen gekapselten IP-Pakets. Ein solcher Flow-Datensatz bietet daher einen Einblick in den VTEP, der das Paket (äußerer Header) einkapselt und die Details der virtuellen Maschine, die der Inter-Host-Datenverkehr (innerer Header) auf einem NSX logischen Switch (VXLAN) erzeugt.

Weitere Informationen zu den IPFIX-Vorlagen für vSphere Distributed Switch finden Sie unter [IPFIX-Vorlagen](#).

IPFIX-Vorlagen

IPFIX-Vorlagen bieten einen Einblick in die VXLAN- und Nicht-VXLAN-Datenflüsse. Die Vorlagen verfügen über zusätzliche Parameter, die weitere Informationen zum gekapselten Datenverkehr bereitstellen.

Die Vorlagen werden in vSphere Distributed Switch (Exporteur) unterstützt. Die IPFIX-Unterstützung auf vSphere Distributed Switch bietet die erforderliche Transparenz der virtuellen Maschinen- und VXLAN-Datenflüsse. Wenn Sie ein beliebiges Collector-Tool eines Drittanbieters verwenden, können Sie zusätzliche Informationen in den Vorlagen verwenden, um eine Korrelation zwischen den internen und externen Datenflüssen und den Port-Verbindungen herzustellen.

IPv4-Vorlage

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port= Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

IPv4-VXLAN-Vorlage

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_VXLAN)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_END()

```

IPv4-ICMP-VXLAN-Vorlage

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP_VXLAN)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv4, 4)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv4, 4)

```

```
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access port,N.A
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

IPv4-ICMP-Vorlage

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv4_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv4TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
// Specify the Interface port- Uplink Port, Access Port,or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()
```

IPv6-ICMP-VXLAN-Vorlage

```
IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP_VXLAN)
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_VMW_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
//VXLAN Specific
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
```

```

IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()

```

IPv6-ICMP-Vorlage

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6_ICMP)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
// Specify the Interface port- Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 2)
IPFIX_TEMPLATE_END()

```

IPv6-Vorlage

```

IPFIX_TEMPLATE_START(IPFIX_FLOW_TYPE_IPv6)
IPFIX_TEMPLATE_FIELD(sourceIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(destinationIPv6Address, 16)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)

```

```
IPFIX_TEMPLATE_FIELD(flowDir, 1)
// Specify the Interface port- Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_PADDING(paddingOctets, 1)
IPFIX_TEMPLATE_END()
```

IPv6-VXLAN-Vorlage

```
IPFIX_TEMPLATE_FIELD(sourceIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(destinationIPv4Address, 4)
IPFIX_TEMPLATE_FIELD(octetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(packetDeltaCount, 8)
IPFIX_TEMPLATE_FIELD(flowStartSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(flowEndSysUpTime, 8)
IPFIX_TEMPLATE_FIELD(sourceTransportPort, 2)
IPFIX_TEMPLATE_FIELD(destinationTransportPort, 2)
IPFIX_TEMPLATE_FIELD(ingressInterface, 4)
IPFIX_TEMPLATE_FIELD(egressInterface, 4)
IPFIX_TEMPLATE_FIELD(protocolIdentifier, 1)
IPFIX_TEMPLATE_FIELD(flowEndReason, 1)
IPFIX_TEMPLATE_FIELD(tcpFlags, 1)
IPFIX_TEMPLATE_FIELD(IPv6TOS, 1)
IPFIX_TEMPLATE_FIELD(maxTTL, 1)
IPFIX_TEMPLATE_FIELD(flowDir, 1)
//VXLAN specific
IPFIX_TEMPLATE_FIELD(vxlanId, 8)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourceIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestIPv6, 16)
IPFIX_VMW_TEMPLATE_FIELD(tenantSourcePort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantDestPort, 2)
IPFIX_VMW_TEMPLATE_FIELD(tenantProtocol, 1)
// Specify the Interface port- Uplink Port, Access Port, or NA.
IPFIX_VMW_TEMPLATE_FIELD(ingressInterfaceAttr, 2)
IPFIX_VMW_TEMPLATE_FIELD(egressInterfaceAttr, 2)
// TUNNEL-GW or no.
IPFIX_VMW_TEMPLATE_FIELD(vxlanExportRole, 1)
IPFIX_TEMPLATE_END()
```

Zusätzliche Parameter

Im Folgenden finden Sie die zusätzlichen Parameter:

- 1 VXLAN-spezifische Parameter: Die mandantenspezifischen Felder entsprechen den inneren Flow IP-Adressen, Ports und Protokollinformationen.
 - tenantSourceIPv4
 - tenantSourceIPv6
 - tenantDestIPv4
 - tenantDestIPv6
 - tenantSourcePort

- tenantDestPort
- tenantProtocol
- Schnittstellen-Port-Parameter

2 Schnittstellen-Port-Parameter: Diese Parameter können für VXLAN- und Nicht-VXLAN-Vorlagen verwendet werden.

- ingressInterfaceAttr
- egressInterfaceAttr
- vxlanExportRole

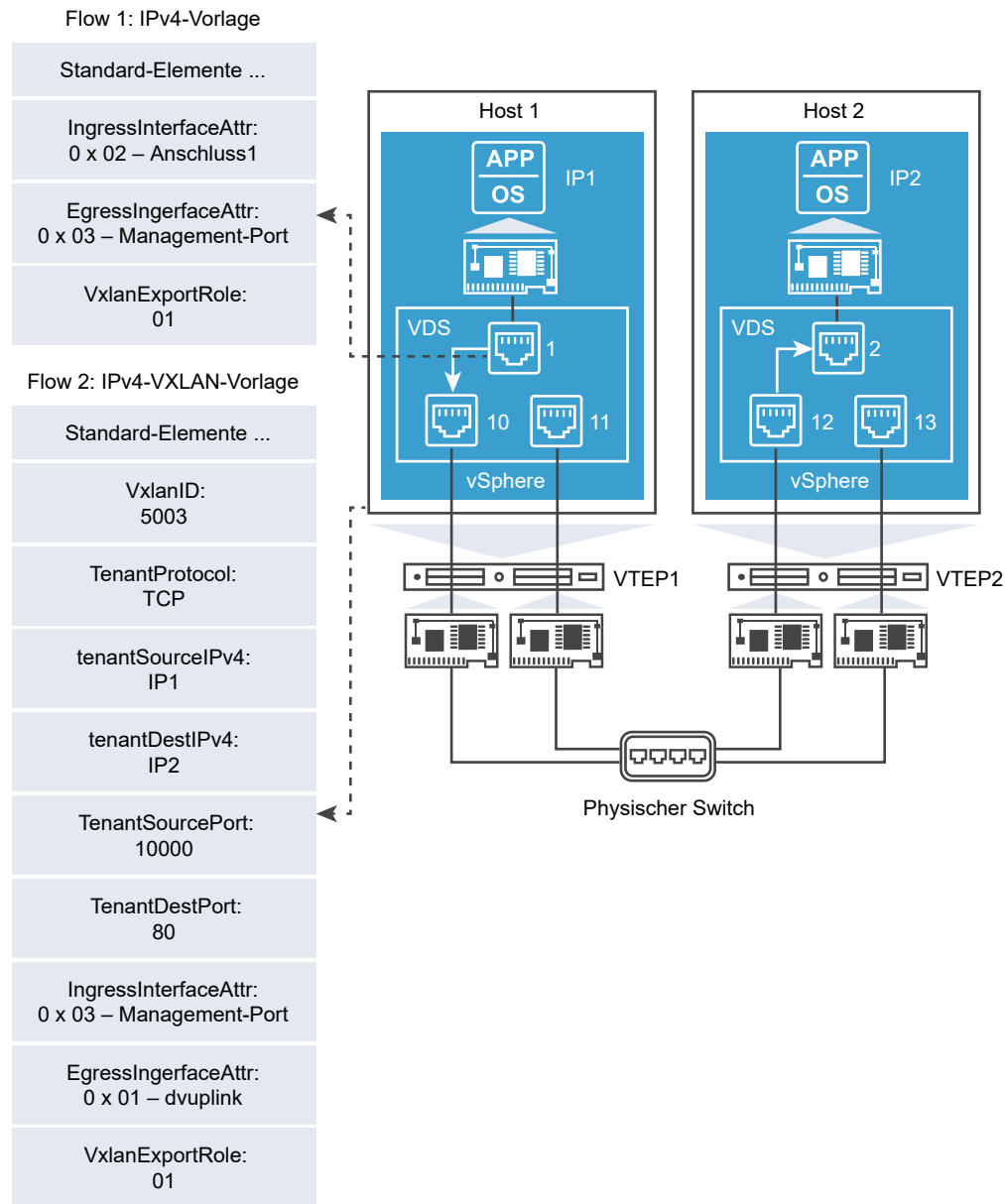
Die Attribute für Eingangs- und Ausgangs-Schnittstelle basieren je nach Port-Typ auf den folgenden Werten:

- IPFIX_UPLINK_PORT 0X01
- IPFIX_ACCESS_PORT 0X02
- IPFIX_VXLAN_TUNNEL_PORT 0X03

Die *VxlanExportRole* definiert, ob der Exporteur ein ESXi-Host oder ein anderes Netzwerkgerät ist. IPFIX_END_POINT 0X01 bedeutet, dass der Host die Daten exportiert. Wenn andere Geräte die IPFIX-Vorlagen exportieren, kann dieses Feld einen anderen Wert (noch nicht definiert) haben.

Von IPFIX für vSphere Distributed Switch überwachte Datenflüsse

Die vorangehenden Diagramme zeigen die Kommunikation zwischen den beiden VMs, die auf zwei verschiedenen Hosts ausgeführt werden und die Flows, die von der IPFIX-Funktion für vSphere Distributed Switch überwacht werden.

Abbildung 22-2. Flows auf Host 1

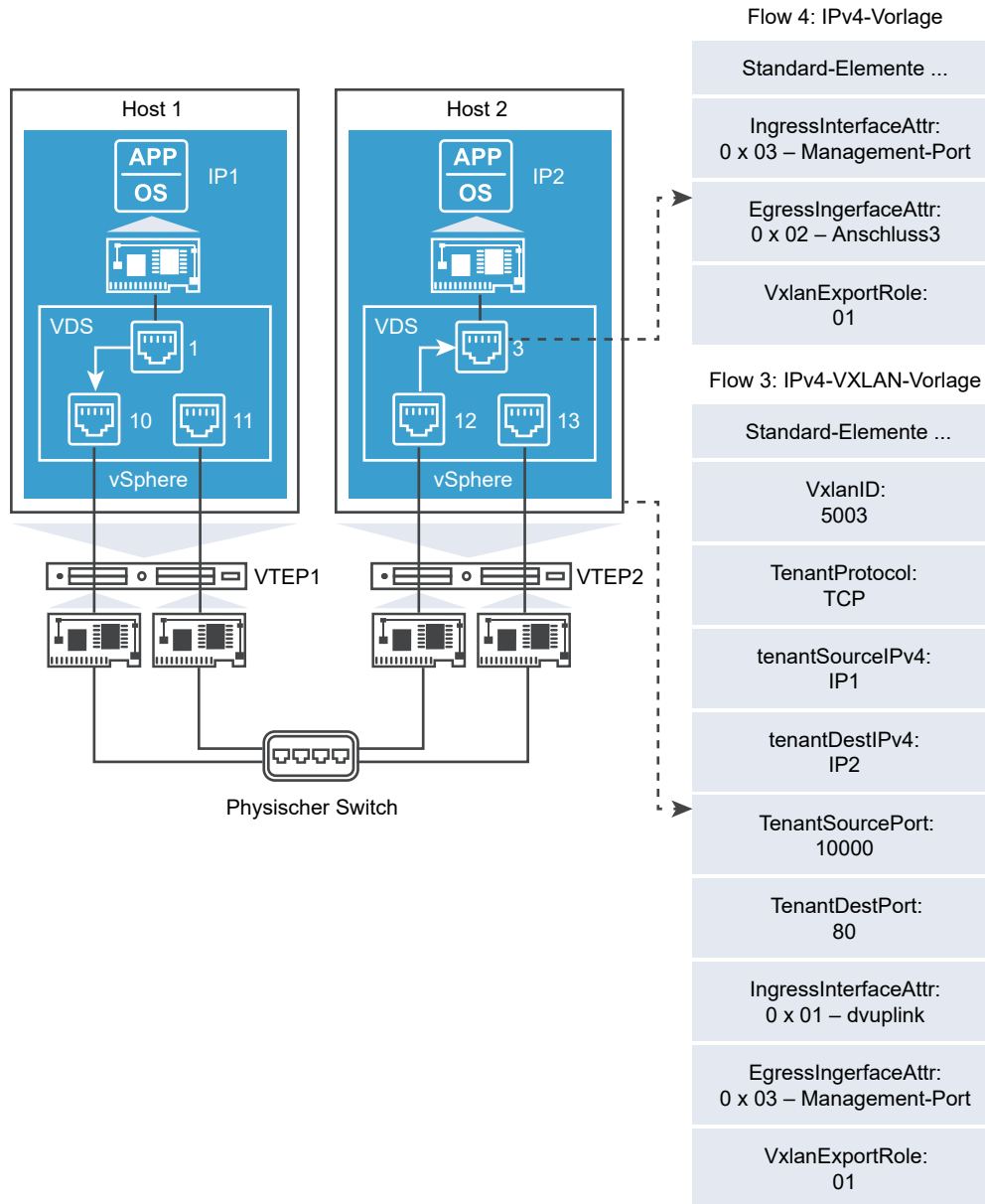
Der [Abbildung 22-2. Flows auf Host 1](#) zeigt an, dass die Flows von Host 1 erfasst werden. Die IPv4-Vorlage verfügt über zusätzliche Informationen zum Eingangs- und Ausgangs-Port und den Standardelementen.

Das Textfeld *IngressInterfaceAttr* im Feld 0 x 02 gibt an, dass es sich um einen Zugriffspunkt handelt, an dem die virtuelle Maschine angeschlossen ist. Die Zugriffspunktnummer ist dem *IngressInterface*-Parameter in der Vorlage zugewiesen.

Der *EgressInterfaceAttr*-Wert von 0 x 03 zeigt, dass es sich um einen VXLAN-Tunnel-Port handelt und die damit verknüpfte Portnummer ein Verwaltungs-VMKNic-Port ist. Diese Portnummer ist dem *EgressInterface*-Parameter in der Vorlage zugewiesen.

Die IPv4-VXLAN-Vorlage verfügt dagegen über zusätzliche Informationen zur VXLAN-ID, zur internen Quelle und zum Ziel-IP/Port und -Protokoll. Die Ein- und Ausgangsschnittstellen sind *VXLAN-Tunnel-Port* bzw. *Dvuplink-Port*.

Abbildung 22-3. Flow on Host 2



Der [Abbildung 22-2. Flows auf Host 1](#) zeigt die Flüsse bei Host 2 an.

Die Vorlagen in den [Abbildung 22-2. Flows auf Host 1](#) unterscheiden sich von den [Abbildung 22-2. Flows auf Host 1](#) nur in den Ein- und Ausgangsattributen und Portnummern.

Die zusätzlichen Informationen, die diese Vorlage bereitstellt, helfen den Anbietern des Collector-Tools, die externen VXLAN-Datenflüsse und die internen Datenflüsse der virtuelle Maschine zu korrelieren.

Informationen, die für den Collector-Tool-Anbieter relevant sind

Die IPFIX-Unterstützung auf vSphere Distributed Switch bietet die erforderliche Transparenz der virtuellen Maschinen- und VXLAN-Datenflüsse. Wenn Sie das Collector-Anbieter-Tool verwenden, können Sie zusätzliche Informationen verwenden, die in den Vorlagen zur Verfügung stehen, um so eine Korrelation zwischen den internen und externen Datenflüssen und den Portverbindungen bereitzustellen.

Der folgende Abschnitt enthält Details zum Dekodieren der neuen Parameter, die zu den VXLAN-Vorlagen hinzugefügt wurden. IANA definiert IPFIX-Informationselemente und deren Element-IDs. Sie finden die Liste der Standardelement-IDs unter <http://www.iana.org/assignments/ipfix/ipfix.xml>.

Alle neuen Elemente, die als Teil der VXLAN-Vorlage definiert sind, haben ihren neuen Element-IDs.

Diese benutzerdefinierten Parameter oder Elemente verfügen über zusätzliche Informationen zu VXLAN und internen Flüssen. Im folgenden finden Sie die neuen Elemente und ihre IDs:

Tabelle 22-4. Benutzerdefinierte Parameter

| Element-ID | Parametername | Datentyp | Einheit |
|------------|----------------------|-------------|---------|
| 880 | tenantProtocol | unsigned8 | 1 Byte |
| 881 | tenantSourceIPv4 | ipv4Address | 4 Byte |
| 882 | tenantDestIPv4 | ipv4Address | 4 Byte |
| 883 | tenantSourceIPv6 | ipv6Address | 16 Byte |
| 884 | tenantDestIPv6 | ipv6Address | 16 Byte |
| 886 | tenantSourcePort | unsigned16 | 2 Byte |
| 887 | tenantDestPort | unsigned16 | 2 Byte |
| 888 | egressInterfaceAttr | unsigned16 | 2 Byte |
| 889 | vxlanExportRole | unsigned8 | 1 Byte |
| 890 | ingressInterfaceAttr | unsigned16 | 2 Byte |

Hinweis Die *Unternehmens-ID* wird an alle der oben festgelegten, benutzerdefinierten Elemente angehängt. Die Unternehmens-ID für VMware ist 6876.

Die folgende Tabelle zeigt ein Beispiel für eine vollständige Liste der Element-IDs. Sie finden Datentyp und Einheit für Standardelement-IDs unter <http://www.iana.org/assignments/ipfix/ipfix.xml>.

| Element-ID | Parametername |
|------------|---------------------|
| 1 | octetDeltaCount |
| 2 | packetDeltaCount |
| 4 | protocolIdentifier |
| 5 | IPv4TOS |
| 5 | IPv6TOS |
| 6 | tcpFlags |
| 7 | sourceTransportPort |

| Element-ID | Parametername |
|------------|--------------------------|
| 8 | sourceIPv4Address |
| 10 | ingressInterface |
| 11 | destinationTransportPort |
| 12 | destinationIPv4Address |
| 14 | egressInterface |
| 15 | nextHopIPv4 |
| 27 | sourceIPv6Address |
| 28 | destinationIPv6Address |
| 53 | maxTTL |
| 61 | flowDir |
| 136 | flowEndReason |
| 152 | flowStartSysUpTime |
| 153 | flowEndSysUpTime |
| 210 | paddingOctets |
| 351 | vxlanId |
| 880 | tenantProtocol |
| 881 | tenantSourceIPv4 |
| 882 | tenantDestIPv4 |
| 883 | tenantSourceIPv6 |
| 884 | tenantDestIPv6 |
| 886 | tenantSourcePort |
| 887 | tenantDestPort |
| 888 | egressInterfaceAttr |
| 889 | vxlanExportRole |
| 890 | ingressInterfaceAttr |

Application Rule Manager

Das Tool „Application Rule Manager“ vereinfacht den Prozess der Mikrosegmentierung einer Anwendung durch das Erstellen von Sicherheitsgruppen und Firewallregeln für vorhandene Anwendungen.

Das Flow Monitoring wird für die langfristige Datenerfassung im System verwendet, während der Application Rule Manager der gezielten Modellierung einer Anwendung dient.

Der Workflow für den Application Rule Manager besteht aus drei Schritten:

- 1 Wählen Sie die virtuellen Maschinen (VMs) aus, aus denen die Anwendung besteht und die überwacht werden müssen. Nach der entsprechenden Konfiguration werden alle eingehenden und ausgehenden Flows für eine definierte Gruppe von vNICs (Virtualized Network Interface Cards) in den VMs überwacht. Es können bis zu fünf Sitzungen gleichzeitig Flows erfassen.
- 2 Halten Sie die Überwachung für die Generierung der Flow-Tabellen an. Die Flows werden analysiert, um die Interaktion zwischen den VMs anzuzeigen. Die Flows können zur Erstellung eines reduzierten Arbeits-Sets gefiltert werden.
- 3 Mithilfe von Flow-Tabellen können Sie Gruppierungsobjekte wie Sicherheitsgruppen, IP Sets, Dienste und Dienstgruppen sowie Firewallregeln erstellen.

Erstellen einer Überwachungssitzung

Eine Überwachungssitzung erfasst alle eingehenden und ausgehenden Flows für bis zu 30 vNICs in einer bestimmten Sitzung.

Voraussetzungen

Bevor Sie eine Überwachungssitzung starten, müssen Sie die VMs und vNICs festlegen, die überwacht werden sollen.

Die aktuelle Version von VMware Tools muss auf Ihren Windows-Desktop-VMs ausgeführt werden.

Die ausgewählten VMs müssen sich in einem Cluster mit einer aktivierten Firewall befinden (sie dürfen nicht in der Ausschlussliste enthalten sein).

Für die Dauer der Überwachungssitzung muss eine Standard-Firewallregel mit beliebiger Zulassung erstellt werden, die für die ausgewählten vNICs gilt. Damit wird verhindert, dass Flows zu und von den vNICs von anderen Firewallregeln verworfen werden.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an und wählen Sie dann „Networking & Security“ aus dem linken Navigationsbereich aus.
- 2 Wählen Sie **Flow Monitoring** aus.
- 3 Wählen Sie die Registerkarte **Application Rule Manager** aus.
- 4 Klicken Sie auf **Neue Sitzung starten (Start New Session)**.
- 5 Geben Sie im Dialogfeld **Neue Sitzung starten (Start New Session)** einen Namen für die Sitzung ein.
- 6 Wählen Sie für den Objekttyp vNICs oder VMs aus.

In der Spalte **Verfügbare Objekte (Available Objects)** werden dann die verfügbaren Objekte dargestellt.

- 7 Doppelklicken Sie auf die vNICs oder VMs, die überwacht werden sollen. Die ausgewählten vNICs oder VMs werden in die Spalte **Ausgewählte Objekte (Selected Objects)** verschoben.

- 8 Klicken Sie auf **OK**, um die Erfassung der Flows zu starten.

Der Status lautet nun **Datenerfassung (Collecting Data)**. Das letzte erfasste Flow-Set wird in der Flow-Tabelle angezeigt.

- 9 Klicken Sie auf **Beenden (Stop)**, um die Erfassung der Flows zu beenden.

Ergebnisse

Es wurde eine Flow-Überwachungssitzung für die ausgewählten vNICs und VMs erstellt.

Nächste Schritte

Nach der Erfassung der Flows analysieren Sie diese.

Analysieren von Flows

Nach der Erfassung einer Flow-Überwachungssitzung werden die Ergebnisse analysiert. Diese können für die Gruppierung von Objekten und Firewallregeln gefiltert werden.

Die analysierten Flows lassen sich zur Reduzierung der Anzahl der Flows in einem Arbeits-Set filtern. Das Symbol für die Filteroption befindet sich auf der rechten Seite neben dem Dropdown-Menü „Verarbeitete Ansicht“.

Voraussetzungen

Damit eine Analyse durchgeführt werden kann, muss eine Flow-Überwachungssitzung aus ausgewählten vNICs oder VMs erfasst werden.

Verfahren

- 1 Nach der Erfassung der Flows klicken Sie auf **Analysieren (Analyze)**.

Die definierten Dienste werden aufgelöst, die Übersetzung der IP-Adresse in die VM startet und Duplikate werden entfernt.

- 2 Nach dem Abschluss der Analyse werden die folgenden Daten zu den Flows angezeigt:

| Feld | Optionen |
|----------|---|
| Richtung | <p>Eingehend – Der Flow fließt in eine VM und vNIC, die als Teil der Eingabe ausgewählt wurden.</p> <p>Ausgehend – Der Flow wird generiert von einer VM und vNIC, die als Teil der Eingabe ausgewählt wurden.</p> <p>INTRA – Der Flow fließt zwischen der VM und vNIC, die als Teil der Eingabe ausgewählt wurden.</p> |
| Quelle | <p>VM-Name, wenn die Quell-IP-Adresse des Flow-Datensatzes in eine VM im NSX-Bestand aufgelöst wurde. Beachten Sie, dass die IP-Adresse nur in VMs aufgelöst werden kann, wenn VM Tools auf diesen VMs aktiviert sind.</p> <p>RAW-IP, wenn für diese Quell-IP-Adresse keine VM im NSX-Bestand vorhanden ist. Beachten Sie, dass Multicast- und Broadcast-IP-Adressen nicht in VMs aufgelöst werden.</p> <p>Anzahl der VMs (z. B. 2 virtuelle Maschinen), wenn es sich um eine überlappende IP-Adresse handelt, die mehreren VMs in unterschiedlichen Netzwerken zugeordnet ist. Der Benutzer muss virtuelle Maschinen in die korrekte virtuelle Maschine auflösen, die zu diesem Flow-Datensatz gehört.</p> |

| Feld | Optionen |
|--------|---|
| Ziel | Identische Werte wie im Feld „Quelle“. |
| Dienst | NSX-definierter Dienst für Protokoll/Port.
RAW-Protokoll/Port, wenn im NSX Manager kein definierter Dienst vorhanden ist.
Anzahl der Dienste. Wenn einem Protokoll/Port mehrere Dienste zugeordnet sind, muss der Benutzer diese in einen Dienst auflösen, der für den Flow-Datensatz angewendet werden kann. |

Nächste Schritte

Analysierte Flows lassen sich für eine benutzerspezifische Anpassung ändern. Als Nächstes erstellen Sie mit den analysierten Flows Firewallregeln.

Flow-Konsolidierung und -Anpassung

Nach Abschluss der Systemanalyse ist unter **Verarbeitete Ansicht (Processed View)** die Tabelle mit dem analysierten Flow enthalten. Benutzer haben die Möglichkeit, die Flows durch Änderung der Felder „Quelle“, „Ziel“ und „Dienst“ weiter zu konsolidieren. Siehe [Anpassen von Diensten in Flow-Datensätzen](#) und [Anpassen von Quelle und Ziel in den Flow-Datensätzen](#).

Hinweis Verarbeitete Ansicht

Die erfassten Flows werden in einer Tabelle mit den folgenden Spalten angezeigt:

| Feld | Optionen |
|----------|---|
| Richtung | Eingehend – Der Flow fließt in eine VM oder vNIC, die als Teil der Eingabe ausgewählt wurde.
Ausgehend – Der Flow wird generiert von einer VM oder vNIC, die als Teil der Eingabe ausgewählt wurde.
INTRA – Der Flow fließt zwischen der VM oder vNIC, die als Teil der Eingabe ausgewählt wurde. |
| Quelle | VM-Name, wenn die Quell-IP-Adresse des Flow-Datensatzes in eine VM im NSX-Bestand aufgelöst wurde.
RAW-IP, wenn für diese Quell-IP-Adresse keine VM im NSX-Bestand vorhanden ist. Beachten Sie, dass Multicast- und Broadcast-IP-Adressen nicht in VMs aufgelöst werden.
Anzahl der VMs, wenn es sich um eine überlappende IP-Adresse handelt, die mehreren VMs in unterschiedlichen Netzwerken zugeordnet ist. Der Benutzer muss mehrere VMs in eine VM auflösen, die zu diesem Flow-Datensatz gehört. |
| Ziel | Identische Werte wie im Feld „Quelle“. |
| Dienst | NSX-definierter Dienst für Protokoll/Port.
RAW-Protokoll/Port, wenn im NSX Manager kein definierter Dienst vorhanden ist.
Anzahl der Dienste. Wenn einem Protokoll/Port mehrere Dienste zugeordnet sind, muss der Benutzer diese in einen Dienst auflösen, der für den Flow-Datensatz angewendet werden kann. |

Flow-Tabellen können bearbeitet und die Flows für eine vereinfachte Erstellung von Regeln konsolidiert werden. So lässt sich z. B. das Feld „Quelle“ durch „ANY“ ersetzen. Mehrere VMs, die Flows mit HTTP und HTTPS empfangen, können durch die Dienstgruppe „WEB-Dienst“ ersetzt werden, die sowohl den HTTP- als auch den HTTPS-Dienst enthält. Dadurch ähneln sich möglicherweise mehrere Flows und es kommt eventuell zu Flow-Mustern, die einfach in eine Firewallregel übersetzt werden können.

Beachten Sie, dass jede Zelle des Flows zwar geändert werden kann, die Zellen aber nicht automatisch mit Daten versehen werden. Wenn beispielsweise die IP-Adresse 196.1.1.1 dem DHCP-Server-IPSet hinzugefügt wird, werden die nachfolgenden Vorkommen dieser IP-Adresse nicht automatisch für die Angabe der DHCP-Server-Gruppe eingetragen. Sie werden gefragt, ob Sie alle Instanzen der IP-Adresse mit dem IPSet ersetzen möchten. So können Sie selbst entscheiden, ob diese IP-Adresse zu mehreren IPSet-Gruppen gehören soll.

Hinweis Konsolidierte Ansicht

Der Zugriff auf die konsolidierte Ansicht ist über die Dropdown-Liste rechts oben möglich. In der konsolidierten Ansicht sind keine doppelten Flows enthalten. Es wird die Mindestanzahl an Flows angezeigt. In dieser Ansicht können Sie Firewallregeln erstellen.

Wenn Sie auf den Pfeil in der linken Ecke der Spalte „Richtung“ klicken, werden die entsprechenden zugehörigen Flow-Rohinformationen angezeigt:

- Für Intra-Flows werden die entsprechenden eingehenden und ausgehenden Flows mit Rohdaten angezeigt.
- Die ursprünglichen Quell-IP-, Ziel-IP-, Port- und Protokollinformationen in allen Roh-Flows, die in dem Datensatz konsolidiert wurden.
- Für ALG-Flows wird der entsprechende Daten-Flow für den Steuerungs-Flow angezeigt.

Anpassen von Diensten in Flow-Datensätzen

Es können einzelne Flow-Zellen für Dienste durch den Benutzer angepasst werden.

Nach der Flow-Analyse können Benutzer jede nicht definierte Protokoll/Port-Kombination zuordnen und einen Dienst erstellen. Dienstgruppen lassen sich für alle Dienste erstellen, die in den erfassten Flows aufgeführt sind. Weitere Informationen zur Bearbeitung von Flow-Datensätzen finden Sie unter [Flow-Konsolidierung und -Anpassung](#).

Voraussetzungen

Die Flow-Daten müssen aus einem Set von vNICs und VMs erfasst worden sein. Weitere Informationen dazu finden Sie unter [Erstellen einer Überwachungssitzung](#).

Verfahren

- ◆ Wenn für den Flow-Status **Analyse abgeschlossen (Analysis Completed)** gilt, werden in der Flow-Tabelle Daten unter **Verarbeitete Ansicht (Processed View)** angezeigt. Für die Anpassung von Zelldaten setzen Sie den Cursor auf die betreffende Zelle. In der oberen rechten Ecke der Zeile wird dann ein Zahnradsymbol angezeigt. Klicken Sie in der Spalte **Dienst (Service)** auf das Zahnradsymbol und wählen Sie eine der folgenden Optionen aus:

| Option | Beschreibung |
|---|--|
| Dienste auflösen | Wenn der Port und das Protokoll in mehrere Dienste übersetzt wurden, können Sie mit dieser Option den korrekten Dienst auswählen. |
| Dienste erstellen und ersetzen | <p>So fügen Sie einen Dienst hinzu:</p> <ul style="list-style-type: none"> a Geben Sie einen Namen (name) für den Dienst ein. b Wählen Sie ein Protokoll aus der Dropdown-Liste aus. c Geben Sie die Zielports für den Dienst ein. d Klicken Sie auf Erweiterte Optionen (Advanced options), um die Quellports des Dienstes einzugeben. Der Quellport wird für das Nachverfolgen neuer eingehender Verbindungen und Datenstreams verwendet. e Optional – Aktivieren Sie Vererbung aktivieren, um die Sichtbarkeit auf zugrunde liegenden Geltungsbereichen zuzulassen (Enable inheritance to allow visibility at underlying scopes), um eine allgemeine Gruppe oder Kriterien zu erstellen, die auf Ebene individueller Edges wiederverwendet werden können. f Klicken Sie auf OK. Daraufhin wird in der Spalte „Dienst“ ein neuer Dienst erstellt und gefüllt. Beachten Sie, dass bei weiteren Flow-Datensätzen mit der gleichen nicht definierten Port/Protokoll-Kombination alle mit dem neu erstellten Dienst ersetzt werden. Diesen Vorgang müssen Sie bestätigen. Das ist nur für Flows der Fall, bei denen in der Analysephase nicht definierte Dienste ermittelt wurden. |
| Dienstgruppe erstellen und ersetzen | <p>Sie können eine neue Dienstgruppe mit dem Dienst aus dem Flow erstellen, der darin enthalten ist. Anschließend wird der Dienst durch die neue Dienstgruppe ersetzt. So fügen Sie eine Dienstgruppe hinzu:</p> <ul style="list-style-type: none"> a Geben Sie unter Name einen Namen für die Dienstgruppe ein. b Optional – Geben Sie eine Beschreibung der Dienstgruppe ein. c Wählen Sie den Objekttyp (Object type) aus. d Wählen Sie die verfügbaren Objekte aus, die Sie der Dienstgruppe hinzufügen möchten, und klicken Sie auf den Pfeil, um die markierten Objekte in die Spalte „Ausgewählte Objekte“ zu verschieben. e Es wird eine neue Dienstgruppe erstellt und in die Spalte „Dienst“ übernommen. |
| Dienst durch beliebiges Element ersetzen | Ersetzt den spezifischen Dienst durch einen beliebigen Dienst. |

| Option | Beschreibung |
|--|---|
| Dienst durch Dienstgruppe ersetzen | <p>Wenn der ausgewählte Dienst zu mehreren Dienstgruppen gehört, müssen Sie die jeweilige Dienstgruppe auswählen, die Sie anwenden möchten.</p> <ol style="list-style-type: none"> Klicken Sie auf die gewünschte Dienstgruppe in der Liste der verfügbaren Objekte. Klicken Sie auf OK. |
| Protokoll und Port wiederherstellen | Macht alle Zelländerungen rückgängig und stellt die ursprünglichen Daten wieder her. |

Ergebnisse

An der Seite des geänderten Flow-Datensatzes wird ein pinkfarbener Balken angezeigt. Wenn Sie den Cursor über eine beliebige Zelle bewegen, die geändert wurde, wird ein grünes Häkchen angezeigt. Beim Klicken auf das Häkchen wird ein Popupfenster mit den vorherigen und neuen Werten für die jeweilige Zelle angezeigt. Der geänderte Flow-Datensatz lässt sich leichter in Firewallregeln übersetzen.

Nächste Schritte

Als Nächstes kann der Flow-Datensatz für das Erstellen von Firewallregeln verwendet werden.

Nach der Änderung der Flows können diese weiter gruppiert werden, um das kleinstmögliche benötigte Arbeits-Set zu erstellen. Unter **Verarbeitete Ansicht (Processed View)** können Sie Dienstgruppen sowie IPSets erstellen und die Flows ändern. Unter **Konsolidierte Ansicht (Consolidated view)** lassen sich diese geänderten Flows weiter komprimieren, um das Erstellen von Firewallregeln zu vereinfachen.

Anpassen von Quelle und Ziel in den Flow-Datensätzen

Es können einzelne Flow-Zellen für Quelle und Ziel durch den Benutzer angepasst werden.

Nach dem Abschluss der Flow-Analyse können Flow-Zellen vom Benutzer geändert werden.

Voraussetzungen

Die Flow-Daten müssen aus einem Set von vNICs und VMs erfasst worden sein. Siehe [Erstellen einer Überwachungssitzung](#).

Verfahren

- ◆ Wenn für den Flow-Status **Analyse abgeschlossen (Analysis Completed)** gilt, werden in der Flow-Tabelle Daten angezeigt. Für die Anpassung von Zelldaten setzen Sie den Cursor auf die betreffende Zelle. In der oberen rechten Ecke der Zeile wird dann ein Zahnradsymbol angezeigt. Klicken Sie in der Spalte **Quelle (Source)** oder **Ziel (Destination)** auf das Zahnradsymbol und wählen Sie eine der folgenden Optionen aus:

| Option | Beschreibung |
|--|---|
| VMs auflösen | Diese Option steht zur Verfügung, wenn mehrere VMs über die gleiche IP-Adresse verfügen. Mit dieser Option wird der betreffende VM-Name für den Flow-Datensatz ausgewählt. |
| Durch beliebiges Element ersetzen | Wenn der Zugriff auf die Quelle nicht beschränkt werden soll, kann jede Quell-IP-Adresse verwendet werden. In allen anderen Fällen müssen Sie die zulässige Quelladresse angeben. Die Konfiguration eines Zielwerts für jede Ziel-IP-Adresse ist nicht möglich. |
| Durch Mitgliedschaft ersetzen | Wenn die VM Bestandteil von Sicherheitsgruppen ist, werden diese hier angezeigt. Diese können den VM-Namen ersetzen. |
| Sicherheitsgruppe erstellen | <ol style="list-style-type: none"> Geben Sie einen Namen und eine optionale Beschreibung für die Sicherheitsgruppe ein. Klicken Sie auf Weiter (Next). Definieren Sie die Kriterien, die ein Objekt erfüllen muss, bevor es zur von Ihnen erstellten Sicherheitsgruppe hinzugefügt werden kann. Dies hilft Ihnen dabei, virtuelle Maschinen aufzunehmen, indem Sie die Filterkriterien mit einer Anzahl an unterstützten Parametern zur Übereinstimmung mit den Suchkriterien definieren. Wählen Sie eine oder mehrere Ressourcen aus, die der Sicherheitsgruppe hinzugefügt werden sollen. Beachten Sie, dass wenn Sie einer Sicherheitsgruppe eine Ressource hinzufügen, automatisch auch alle dieser Ressource zugeordneten Ressourcen hinzugefügt werden. Wenn Sie beispielsweise eine virtuelle Maschine auswählen, wird die zugewiesene vNIC automatisch zur Sicherheitsgruppe hinzugefügt. Sie können die folgenden Objekte zu einer Sicherheitsgruppe hinzufügen: <ul style="list-style-type: none"> Cluster Logischer Switch Legacy-Portgruppe vApp Datencenter Klicken Sie auf Weiter (Next). Wählen Sie die Objekte aus, die nicht in der Sicherheitsgruppe enthalten sein sollen. Die hier ausgewählten Objekte sind immer aus der Sicherheitsgruppe ausgeschlossen, unabhängig davon, ob die Kriterien für die dynamische Mitgliedschaft erfüllt werden. Klicken Sie auf Weiter (Next). Überprüfen Sie im Fenster Bereit zum Abschließen (Ready to complete) die Details der Sicherheitsgruppe. Klicken Sie auf Beenden (Finish). |

| Option | Beschreibung |
|---|--|
| Zu bestehender Sicherheitsgruppe hinzufügen und ersetzen | <p>Wenn bei VMs die ausgewählte VM zu mehreren Sicherheitsgruppen gehört, wählen Sie die jeweilige Sicherheitsgruppe aus, die Sie anwenden möchten. Diese Option ist nicht verfügbar, wenn die IP-Adresse im Quell- oder Zielfeld vorhanden ist. Verwenden Sie für IP-Rohadressen die Option „Zu bestehendem IPSet hinzufügen und ersetzen“.</p> <ul style="list-style-type: none"> a Klicken Sie auf die gewünschte Dienstgruppe in der Liste der verfügbaren Objekte. b Klicken Sie auf OK. |
| IPSet erstellen und ersetzen | <p>Ein IPSet ermöglicht die gleichzeitige Anwendung einer Firewallregel für ein komplettes Set von IP-Adressen.</p> <ul style="list-style-type: none"> a Geben Sie einen Namen für das IPSet ein. b Optional – Geben Sie eine Beschreibung ein. c Geben Sie IP-Adressen oder einen Bereich von Adressen in das neue IP Set ein. d Klicken Sie auf OK. |
| Zu bestehendem IPSet hinzufügen und ersetzen | <p>Eine IP-Adresse kann zu mehreren IPSets gehören. Mit dieser Option haben Sie die Möglichkeit, die angezeigte IP-Adresse durch eine andere IP-Adresse zu ersetzen.</p> <ul style="list-style-type: none"> a Wählen Sie das gewünschte IPSet unter „Verfügbare Objekte“ aus. b Klicken Sie auf OK. |
| Ursprüngliche Daten wiederherstellen | <p>Macht alle Zelländerungen rückgängig und stellt die ursprünglichen Daten wieder her.</p> |

Nächste Schritte

Erstellen Sie eine Firewallregel auf der Grundlage des Flow Monitoring.

Erstellen von Firewallregeln mit dem Application Rule Manager

Firewallregeln können bearbeitet, gelöscht sowie nach oben und unten im Application Rule Manager verschoben werden.

Voraussetzungen


Nach der Analyse der Flow-Datensätze können Sie Firewallregeln erstellen.

Verfahren

- 1 Öffnen Sie eine Flow-Sitzung. Wenn Sie sich in der Ansicht **Verarbeitete Ansicht (Processed View)** befinden, klicken Sie mit der rechten Maustaste auf eine einzelne Flow-Zelle oder halten Sie die Umschalttaste gedrückt, klicken Sie auf die erste und letzte Zelle eines Bereichs von Flow-Zellen und klicken Sie mit der rechten Maustaste. Wenn Sie sich in der Ansicht **Konsolidierte Ansicht (Consolidated View)** befinden, wählen Sie eine Flow-Zelle aus, und klicken Sie auf das Symbol **Aktion (Action)**. Wählen Sie **Firewall-Regel erstellen (Create Firewall rule)** aus.

Das Popup-Fenster **Neue Firewallregel (New Firewall Rule)** wird mit allen Zellen mit Daten auf der Basis der ausgewählten Zeilendaten angezeigt. Wenn mehrere Zellen ausgewählt wurden, werden alle Quell-, Ziel- und Dienstobjekte den entsprechenden Feldern der Regel hinzugefügt.

- 2 Geben Sie einen Namen für die neue Regel ein.
- 3 (Optional) Um eine andere Quelle oder ein anderes Ziel auszuwählen, klicken Sie auf **Auswählen (Select)** neben dem Feld „Quelle“ oder „Ziel“. Legen eine neue Quelle oder ein neues Ziel aus den verfügbaren Objekten fest und klicken Sie auf **OK**.
- 4 (Optional) Um einen anderen Dienst auszuwählen, klicken Sie auf **Auswählen (Select)** neben dem Feld „Dienst“. Die verteilte Firewall unterstützt ALG (Application Level Gateway) für die folgenden Protokolle: FTP, CIFS, ORACLE, TNS, MS-RPC und SUN-RPC. Edge unterstützt ALG nur für FTP. Legen einen neuen Dienst aus den verfügbaren Objekten fest und klicken Sie auf **OK**.
- 5 (Optional) Um die Regel auf einen anderen Bereich anzuwenden, klicken Sie auf **Auswählen (Select)** neben dem Feld „Angewendet auf“. Treffen Sie eine entsprechende Auswahl, wie in der nachfolgenden Tabelle beschrieben, und klicken Sie auf **OK**. Standardmäßig wird die Regel auf die VNICs angewendet, auf die Sie ursprünglich mit der rechten Maustaste geklickt haben.

| Zum Anwenden einer Regel auf | Führen Sie Folgendes durch |
|--|--|
| Alle vorbereiteten Cluster in Ihrer Umgebung | Wählen Sie Wenden Sie diese Regel auf alle Cluster an, auf denen die verteilte Firewall aktiviert ist (Apply this rule on all clusters on which Distributed Firewall is enabled) . Nachdem Sie auf OK geklickt haben, wird in der Spalte „Angewendet auf“ für diese Regel die Option verteilte Firewall (Distributed Firewall) angezeigt. |
| Mindestens ein Cluster, Datencenter, Netzwerk, logischen Switch, eine verteilte virtuelle Portgruppe, NSX Edge, virtuelle Maschine oder vNIC | <ol style="list-style-type: none"> 1 Wählen Sie unter Containertyp (Container type) das entsprechende Objekt aus. 2 Wählen Sie in der Liste Verfügbar (Available) mindestens ein Objekt aus und klicken Sie auf . |

Wenn die Regel virtuelle Maschinen und vNICs in den Feldern „Quelle“ und „Ziel“ enthält, müssen Sie sowohl die Quell-VMs und Quell-vNICs als auch die Ziel-VMs und Ziel-vNICs zu **Angewendet auf (Applied To)** hinzufügen, damit die Regel richtig angewendet werden kann.

- 6 Wählen Sie in **Aktion (Action)** eine in der nachfolgenden Tabelle dargestellte Aktion aus.

| Aktion | Ergebnis |
|-------------------|--|
| Zulassen | Lässt Datenverkehr von oder zu angegebener/n Quelle/n, Ziel/en und Dienst/en zu. |
| Blockieren | Blockiert Datenverkehr von oder zu angegebener/n Quelle/n, Ziel/en und Dienst/en. |
| Ablehnen | <p>Versendet Ablehnungsmeldungen für nicht angenommene Pakete.</p> <p>RST-Pakete werden für TCP-Verbindungen versendet.</p> <p>ICMP-Meldungen mit vom Administrator verbotenen Code werden für UDP-, ICMP- und andere IP-Verbindungen versendet.</p> |

- 7 Legen Sie unter **Richtung (Direction)** die Richtung der Regel durch Klicken auf den Dropdown-Pfeil fest.
- 8 Klicken Sie auf **OK**.

Nächste Schritte

Veröffentlichen Sie die Firewallregeln. Weitere Informationen dazu finden Sie unter [Veröffentlichen und Verwalten von Firewallregeln mit dem Application Rule Manager](#).

Veröffentlichen und Verwalten von Firewallregeln mit dem Application Rule Manager

Firewallregeln können im Application Rule Manager bearbeitet und veröffentlicht werden.

Nach der Erstellung von Firewallregeln können diese auf der Registerkarte **Firewallregeln (Firewall Rules)** des Application Rule Manager verwaltet werden.

Voraussetzungen

Erstellen Sie Firewallregeln von einer Flow-Überwachungssitzung.

Verfahren

- ◆ Wenn Sie Firewallregeln von einer Flow-Überwachungssitzung erstellt haben, werden diese auf der Registerkarte **Firewallregeln (Firewall Rules)** angezeigt. Wählen Sie eine der folgenden Optionen aus:

| Option | Beschreibung |
|-------------------------|---|
| Veröffentlichen | <ul style="list-style-type: none"> a Klicken Sie auf Veröffentlichen (Publish), um die erstellten Firewallregeln zu veröffentlichen. Die Regeln werden als neuer Abschnitt veröffentlicht. b Geben Sie in Abschnittsname (Section Name) einen Abschnittsnamen für die Firewallregel ein. c Wählen Sie aus, wo der neue Firewallabschnitt in der vorhandenen Firewallkonfiguration eingefügt werden soll. d Klicken Sie auf OK. |
| Bearbeiten | Wählen Sie für die Bearbeitung der Firewallregeln das Bleistiftsymbol aus. |
| Löschen | Wählen Sie für das Löschen der Firewallregel das X-Symbol aus. |
| Pfeil nach unten | Wählen Sie für das Verschieben der Regel nach unten den Pfeil nach unten aus. |
| Pfeil nach oben | Wählen Sie für das Verschieben der Regel nach oben den Pfeil nach oben aus. |

Hinweis Wenn Firewallregeln mit dem **Application Rule Manager** veröffentlicht werden, wird der Schaltfläche **Veröffentlichen (Publish)** der Abschnittsname hinzugefügt. Jede nachfolgende Veröffentlichung mit dem **Application Rule Manager** überschreibt den vorhandenen Abschnitt in der Firewallkonfiguration mit den Regeln, die aktuell im **Application Rule Manager** verfügbar sind.

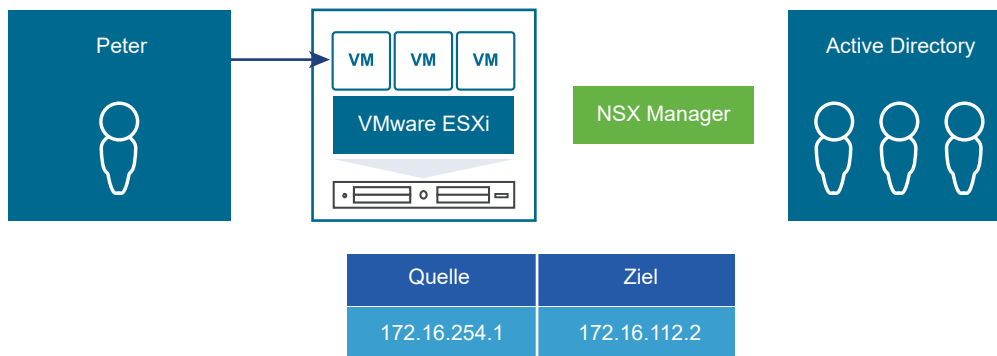
Activity Monitoring

Activity Monitoring bietet einen Überblick über die Anwendungen, die in den von vCenter verwalteten virtuellen Maschinen auf dem Windows-Desktop ausgeführt werden. Diese Transparenz hilft sicherzustellen, dass die Sicherheitsrichtlinien in Ihrem Unternehmen eingehalten werden.

Hinweis Ab der Version NSX 6.3.0 wird die NSX Activity Monitoring-Funktion eingestellt. Sie können diese Funktion noch auf eigene Verantwortung weiter benutzen. In künftigen NSX-Versionen ist diese Funktion jedoch nicht mehr enthalten. Ab Version 6.3.0 wird empfohlen, anstelle der Activity Monitoring-Funktion die Endpoint-Überwachungsfunktion zu verwenden.

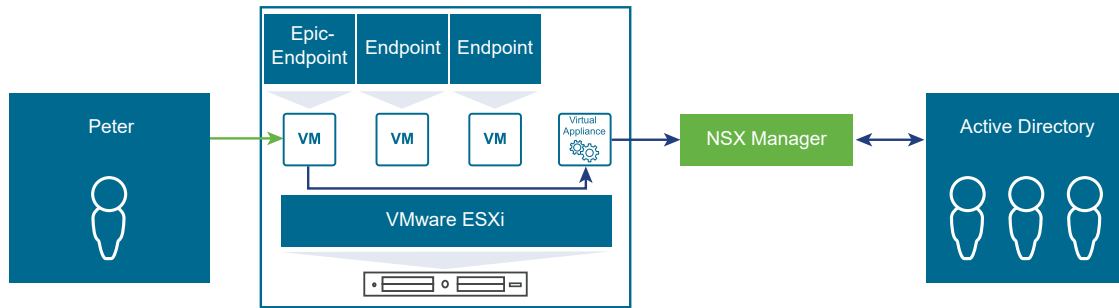
Eine Sicherheitsrichtlinie kann zum Beispiel festlegen, wer auf welche Anwendungen zugreifen darf. Der Cloud-Administrator kann Activity Monitoring-Berichte generieren, um zu überprüfen, ob die IP-basierte Firewallregel, die er festgelegt hat, die beabsichtigte Arbeit durchführt. Durch das Bereitstellen von Daten auf Benutzer- und Anwendungsebene wandelt übergeordnete Activity Monitoring Sicherheitsrichtlinien in eine untergeordnete IP-Adress- und netzwerkbasierte Implementierung um.

Abbildung 22-4. Ihre virtuelle Umgebung heute



Nachdem Sie die Datenerfassung für Activity Monitoring aktiviert haben, können Sie Berichte ausführen, um den eingehenden Datenverkehr (z. B. die virtuellen Maschinen, auf die Benutzer zugreifen) und den ausgehenden Datenverkehr (Ressourcennutzung, Interaktion zwischen Bestandslisten-Containern und AD-Gruppen, die auf einen Server zugegriffen haben) anzuzeigen.

Abbildung 22-5. Ihre virtuelle Umgebung mit Activity Monitoring



| Benutzer | AD-Gruppe | App-Name | Quell-VM-Name | Ziel-VM-Name | Quell-IP-Adresse | Ziel-IP-Adresse |
|----------|-----------|----------|---------------|--------------|------------------|-----------------|
| Peter | Ärzte | Epic.exe | DoctorsWS13 | EpicSVR3 | 172.16.254.1 | 172.16.112.2 |

Wichtig Activity Monitoring auf Linux-VMs wird nicht unterstützt.

Einrichten von Activity Monitoring

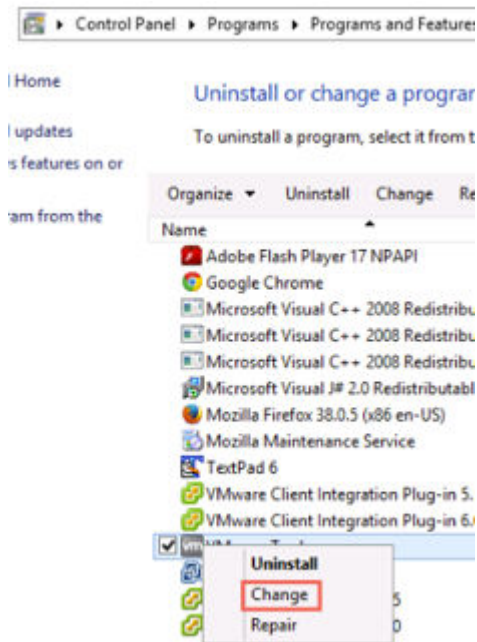
Damit Activity Monitoring funktioniert, müssen mehrere erforderliche Vorgänge durchgeführt werden, darunter die Installation des Guest Introspection-Treibers, die Installation der Guest Introspection-VMs und das Aktivieren von NSX Activity Monitoring. Sie können Service Composer auch einsetzen, um zu steuern, welche virtuellen Maschinen überwacht werden (optional).

Voraussetzungen

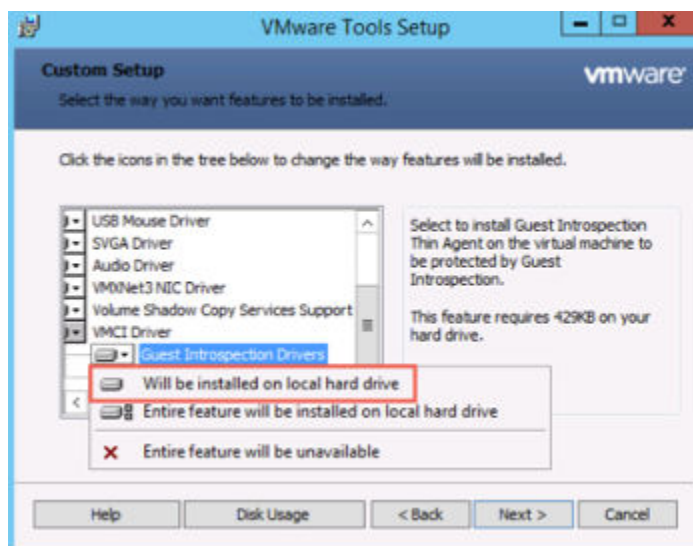
- NSX Manager muss installiert und betriebsbereit sein.
- NSX Manager muss mit dem AD-Server verlinkt werden, wo Gruppen abgerufen werden, die mit Benutzern von virtuellen Windows-Maschinen abgeglichen werden.
- Die vCenter-Bestandsliste muss mindestens eine Windows-Desktop-VM enthalten.
- Die aktuelle Version von VMware Tools muss auf Ihren Windows-Desktop-VMs ausgeführt werden.

Verfahren

- 1 Installieren Sie auf den Windows-VMs in Ihrer vCenter-Bestandsliste den Guest Introspection-Treiber, sofern er noch nicht bereits installiert ist.
 - a Navigieren Sie zu **Systemsteuerung\Programme\Programme und Funktionen (Control Panel\Programs\Programs and Features)**, klicken Sie mit der rechten Maustaste auf **VMware Tools** und wählen Sie **Ändern (Change)**.



- b Wählen Sie **Ändern (Modify)** aus.
 - c Klicken Sie in **VMCI-Treiber (VMCI Driver)** auf **Treiber für Guest Introspection > Wird auf lokaler Festplatte installiert (Guest Introspection Drivers > Will be installed on local hard drive)**.



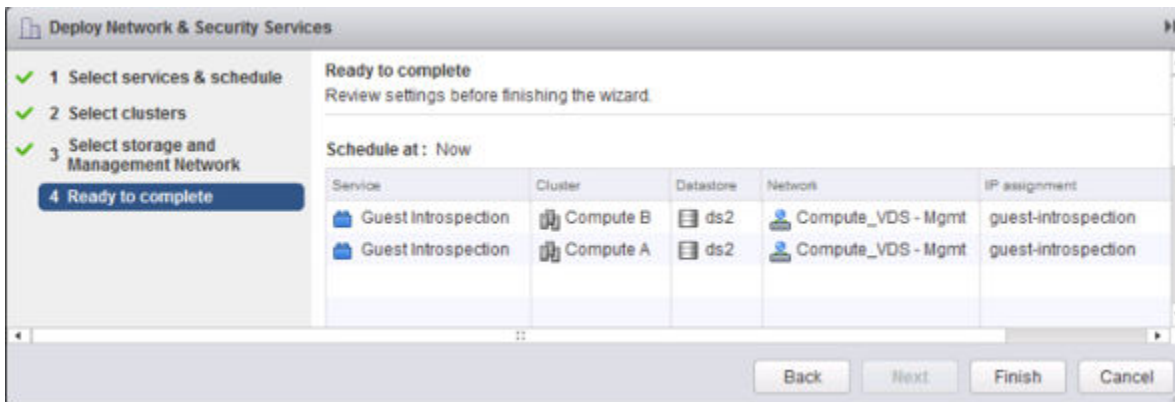
Der Guest Introspection-Treiber erkennt die Anwendungen, die auf jeder virtuellen Windows-Maschine ausgeführt werden, und sendet diese Informationen an die Guest Introspection-VM.

2 Installieren Sie die Guest Introspection-VMs.

Wenn Sie das VMware Tools-Installationsprogramm erstmals starten, wählen Sie die Option **Benutzerdefiniert (Custom)** aus. Wählen Sie im VMCI-Ordner **Guest Introspection-Treiber (Guest Introspection Driver)** aus. Der Treiber ist standardmäßig nicht ausgewählt.

So fügen Sie den Treiber hinzu, wenn VMware Tools bereits installiert ist:

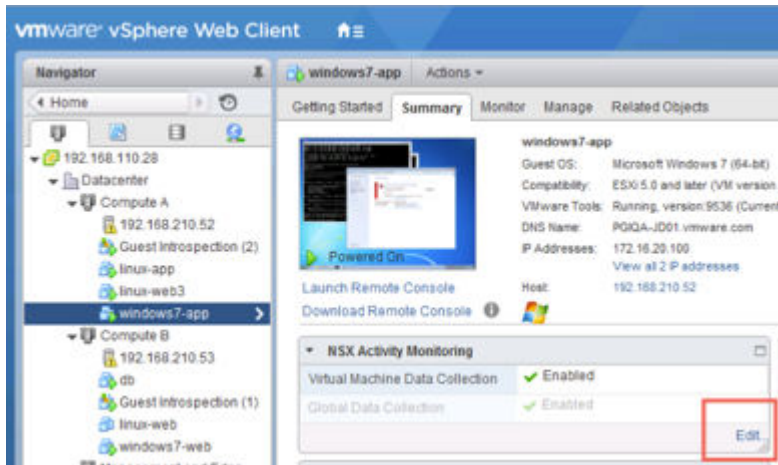
- Navigieren Sie im vCenter Web Client zu **Networking & Security > Installation > Dienstbereitstellungen (Networking & Security > Installation > Service Deployments)**.
- Fügen Sie eine neue Dienstbereitstellung hinzu.
- Wählen Sie **Guest Introspection**.
- Wählen Sie die Host-Cluster aus, die virtuelle Windows-Maschinen enthalten.
- Wählen Sie die entsprechenden Datenspeicher, Netzwerke und den entsprechenden IP-Adressierungsmechanismus aus. Wenn Sie für Ihre Guest Introspection-VMs nicht DHCP verwenden, muss die Erstellung und Zuweisung eines IP-Pools erfolgen.



Es werden zwei Guest Introspection-VMs installiert: eine auf jedem Host innerhalb eines jeden Clusters.



- 3 Aktivieren Sie Activity Monitoring auf den virtuellen Windows-Maschinen.
 - a Wählen Sie in der Ansicht **Hosts und Cluster (Hosts and Clusters)** die virtuelle Windows-Maschine und dann die Registerkarte **Übersicht (Summary)** aus.
 - b Klicken Sie unter NSX Activity Monitoring auf **Bearbeiten (Edit)** und dann auf **Ja (Yes)**.



Wiederholen Sie diesen Schritt für alle virtuellen Windows-Maschinen, die Sie überwachen möchten.

- 4 (Optional) Ändern Sie die Liste der überwachten vCenter-Objekte oder definieren Sie eine dynamische Mitgliedschaftsregel.
 - a Navigieren Sie im vCenter Web Client zu **Networking & Security > Service Composer**.
 - b Bearbeiten Sie die Sicherheitsgruppe **Datenerfassung von Activity Monitoring (Activity Monitoring Data Collection)**.
 - c Definieren Sie eine dynamische Mitgliedschaftsregel, sodass die virtuelle Maschine automatisch überwacht wird, wenn neue virtuelle Windows-Maschinen zum Cluster hinzugefügt werden.
 - d Wählen Sie vCenter-Objekte aus, die Sie in die Activity Monitoring-Sicherheitsgruppe aufnehmen bzw. von dieser ausschließen möchten.

Die virtuellen Maschinen, auf denen Sie Activity Monitoring aktiviert haben, werden automatisch in die Activity Monitoring-Sicherheitsgruppe aufgenommen.

In diesem Beispiel werden alle virtuellen Maschinen, deren Namen mit „win“ beginnen, automatisch in die Activity Monitoring-Sicherheitsgruppe aufgenommen. Dies bedeutet, dass Activity Monitoring automatisch für sie aktiviert wird.

Edit Security Group

Ready to complete

Name: Activity Monitoring Data Collection

Description:

Scope: Global

Dynamic membership

Members matching (Any) of the criteria below

| Key | Criteria | Value |
|---------|-------------|-------|
| VM Name | Starts with | win |

Objects to Include

| Name |
|--------------|
| windows7-app |
| windows7-web |

Objects to Exclude

| Name |
|------|
|------|

Back Next Finish Cancel

Szenarien zum Activity Monitoring

In diesem Abschnitt werden einige hypothetische Szenarien für das Activity Monitoring beschrieben.

Benutzerzugriff auf Anwendungen

Unser hypothetisches Unternehmen ACME Enterprise erlaubt nur genehmigten Benutzern, auf bestimmte Anwendungen auf Unternehmensressourcen zuzugreifen.

Ihre Sicherheitsrichtlinie verlangt folgende Vorgaben:

- Nur autorisierten Benutzern den Zugriff auf kritische Geschäftsanwendungen erlauben
- Nur autorisierte Anwendungen auf Unternehmensservern erlauben
- Zugang nur zu erforderlichen Ports über bestimmte Netzwerke erlauben

Dementsprechend wird der kontrollierte Zugang für Mitarbeiter basierend auf der Benutzeridentität benötigt, um Unternehmensressourcen zu sichern. Als Startpunkt muss der Sicherheitsoperator von ACME Enterprise sicherstellen können, dass nur der Administratorzugriff auf die MS SQL-Server erlaubt ist.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Activity Monitoring**.
- 3 Klicken Sie auf die Registerkarte **Eingehende Aktivität (Inbound Activity)**.
- 4 Lassen Sie unter **Ausgehend von (Outbound from)** den Wert **Alle beobachteten AD-Gruppen (All Observed AD Groups)** unverändert, um den Zugriff von allen Mitarbeitern anzuzeigen.

- 5 Wählen Sie unter **Mit der virtuellen Zielmaschine (Where destination virtual machine)** die Option **enthält (includes)** und lassen Sie **alle beobachteten virtuellen Zielmaschinen (all observed destination virtual machines)** ausgewählt.
- 6 Wählen Sie unter **Und mit der Zielanwendung (And where destination application)** die Option **enthält (includes)**, klicken Sie auf **alle beobachteten Zielanwendungen (all observed destination applications)** und wählen Sie die MS SQL-Server aus.
- 7 Klicken Sie auf **Suchen (Search)**.
Die Suchergebnisse zeigen, dass nur administrative Benutzer auf die MS SQL-Server zugreifen. Beachten Sie, dass keine anderen Gruppen (wie z. B. Finanzen oder Personal) auf diese Server zugreifen.
- 8 Wir können diese Suchabfrage umkehren, indem der Wert **Ausgehend von (Outbound from)** auf Personal- und Finanz-AD-Gruppen festgelegt wird.
- 9 Klicken Sie auf **Suchen (Search)**.
Es werden keine Datensätze angezeigt, die bestätigen, dass weder Benutzer aus der einen noch aus der anderen Gruppe auf MS SQL-Server zugreifen können.

Anwendungen im Datencenter

Als Teil der Sicherheitsrichtlinien benötigt ACME Enterprise Zugriff auf alle Datencenter-Anwendungen. Dies kann dazu beitragen, fehlerhafte Anwendungen zu identifizieren, die entweder vertrauliche Informationen erfassen oder vertrauliche Daten an externen Quellen weitergeben.

Peter, Cloud-Administrator bei ACME Enterprise, möchte bestätigen, dass nur über Internet Explorer auf den SharePoint-Server zugegriffen werden kann und dass keine potenziell schädliche Anwendung (wie FTP oder RDP) auf diesen Server zugreifen kann.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Activity Monitoring**.
- 3 Klicken Sie auf die Registerkarte **VM-Aktivität (VM Activity)**.
- 4 Wählen Sie unter **Mit folgender Quell-VM (Where source VM)** die Option **enthält (includes)** und lassen Sie die Option **Alle beobachteten virtuellen Maschinen (All observed virtual machines)** aktiviert, um den ausgehenden Datenverkehr aller virtuellen Maschinen im Datencenter zu erfassen.
- 5 Wählen Sie unter **Mit der Ziel-VM (Where destination VM)** die Option **enthält (includes)**, klicken Sie auf **Alle beobachteten virtuellen Maschinen (All observed virtual machines)** und wählen Sie den SharePoint-Server aus.
- 6 Klicken Sie auf **Suchen (Search)**.

Ergebnisse

In der Spalte **Produktname der ausgehenden Anwendung (Outbound App Product Name)** der Suchergebnisse wird angezeigt, dass der Zugriff auf den SharePoint-Server ausschließlich über den Internet Explorer erfolgte. Die relativ homogenen Suchergebnisse zeigen an, dass eine Firewallregel auf diesen SharePoint-Server angewendet wird, um alle anderen Zugriffsmethoden zu verhindern.

Beachten Sie zudem, dass die Suchergebnisse die Quellbenutzer des überwachten Datenverkehrs anstatt die Quellgruppe anzeigen. Durch Klicken auf den Pfeil in den Suchergebnissen werden Details über die Quellbenutzer wie die AD-Gruppe, zu der der Benutzer gehört, angezeigt.

Prüfen von offenen Ports

Peter Admin hat festgestellt, dass nur autorisierte Anwendungen auf den SharePoint-Server von ACME Enterprise zugreifen. Damit kann er nun gewährleisten, dass das Unternehmen nur die Öffnung der erforderlichen Ports basierend auf der voraussichtlichen Nutzung zulässt.

Voraussetzungen

Im Szenario [Anwendungen im Datencenter](#) hatte Peter Admin den Datenverkehr zum SharePoint-Server von ACME Enterprise beobachtet. Er möchte jetzt gewährleisten, dass alle Zugriffe vom SharePoint-Server auf den MSSQL-Server über die erwarteten Protokolle und Anwendungen erfolgen.

Verfahren

- 1 Klicken Sie auf das Symbol **Zur Startseite wechseln (Go Home)**.
- 2 Klicken Sie auf **vCenter-Home (vCenter Home)** und anschließend auf **Virtuelle Maschinen (Virtual Machines)**.
- 3 Wählen Sie **win_sharepoint** aus und klicken Sie dann auf die Registerkarte **Überwachen (Monitor)**.
- 4 Klicken Sie auf **Activity Monitoring**.
- 5 Wählen Sie unter **Mit folgendem Ziel (Where destination)** die Option **win2K-MSSQL** aus.
- 6 Klicken Sie auf **Suchen (Search)**.

Ergebnisse

In den Suchergebnissen wird der Datenverkehr vom SharePoint-Server zum MSSQL-Server gezeigt. Die Spalten **Benutzer (User)** und **Ausgehende Anwendung (Outbound App)** zeigen, dass sich nur Systemprozesse mit dem MSSQL-Server verbinden. Das entspricht der Erwartung von Peter Admin.

Die Spalten **Eingehender Port (Inbound Port)** und **App** zeigen, dass sämtliche Zugriffe auf den MSSQL-Server erfolgen, der auf dem Zielsystem ausgeführt wird.

Da die Suchergebnisse zu viele Datensätze enthalten, als dass Peter Admin sie in einem Webbrowser analysieren könnte, kann er die gesamten Ergebnisse exportieren und die Datei im CSV-Format

speichern. Dazu klickt er auf das Symbol  unten rechts auf der Seite.

Aktivieren der Datenerfassung

Sie müssen die Datenerfassung für eine oder mehrere virtuelle Maschinen auf einem vCenter Server aktivieren, bevor Sie den Activity Monitoring-Bericht ausführen. Stellen Sie vor dem Ausführen des Berichts sicher, dass die aktivierten virtuellen Maschinen aktiv sind und Datenverkehr im Netzwerk erzeugen.

Sie sollten außerdem NSX Manager beim AD-Domänencontroller registrieren. Weitere Informationen dazu finden Sie unter [Registrieren einer Windows-Domäne mit NSX Manager](#).

Beachten Sie, dass nur aktive Verbindungen von Activity Monitoring aufgezeichnet werden. Datenverkehr von virtuellen Maschinen, der von Firewallregeln auf der vNIC-Ebene blockiert wird, wird in den Berichten nicht ausgewiesen.

Aktivieren der Datenerfassung auf einer einzelnen virtuellen Maschine

Sie müssen die Datenerfassung mindestens fünf Minuten vor Ausführung eines Activity Monitoring-Berichts aktivieren.

Voraussetzungen

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **vCenter** und anschließend auf **VMs und Vorlagen (VMs and Templates)**.
- 3 Wählen Sie aus der linken Bestandsliste eine virtuelle Maschine aus.
- 4 Klicken Sie auf die Registerkarte **Verwalten (Manage)** und anschließend auf die Registerkarte **Einstellungen (Settings)**.
- 5 Klicken Sie im linken Fensterbereich auf **NSX Activity Monitoring**.
- 6 Klicken Sie auf **Bearbeiten (Edit)**.
- 7 Klicken Sie im Dialogfeld „Datenerfassungseinstellung für NSX Activity Monitoring bearbeiten“ auf **Ja (Yes)**.


Aktivieren der Datenerfassung für mehrere virtuelle Maschinen

Die Sicherheitsgruppe (Security Group) für die Datenerfassung von Activity Monitoring ist eine vordefinierte Sicherheitsgruppe. Sie können dieser Sicherheitsgruppe mehrere virtuelle Maschinen gleichzeitig hinzufügen. Die Datenerfassung ist dann für alle diese virtuellen Maschinen aktiviert.

Sie müssen die Datenerfassung mindestens fünf Minuten vor Ausführung eines Activity Monitoring-Berichts aktivieren.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und dann auf **Service Composer**.

- 3 Klicken Sie auf die Registerkarte **Security Groups**.
- 4 Wählen Sie die Sicherheitsgruppe für die Datenerfassung von Activity Monitoring aus und klicken Sie auf das Symbol **Bearbeiten (Edit)** ().
- 5 Befolgen Sie die Anweisungen des Assistenten, um der Sicherheitsgruppe virtuelle Maschinen hinzuzufügen.

Die Datenerfassung ist für alle virtuelle Maschinen aktiviert, die Sie dieser Sicherheitsgruppe hinzugefügt haben. Für virtuelle Maschinen, die Sie aus der Sicherheitsgruppe ausgeschlossen haben, ist die Datenerfassung deaktiviert.

Anzeigen des Aktivitätsberichts für virtuelle Maschinen

Sie können den Datenverkehr zu oder von einer virtuellen Maschine oder einer Gruppe virtueller Maschinen in Ihrer Umgebung anzeigen.

Sie können entweder eine schnelle Abfrage mithilfe der Standardsuchkriterien durchführen oder die Abfrage Ihren Anforderungen entsprechend konfigurieren. Klicken Sie für die schnelle Abfrage auf **Suchen (Search)**.

Voraussetzungen


- Guest Introspection muss in Ihrer Umgebung installiert sein.
- Eine Domäne muss mit NSX Manager registriert sein. Hinweise zur Domänenregistrierung finden Sie unter [Registrieren einer Windows-Domäne mit NSX Manager](#).
- Die Datenerfassung muss auf einer oder mehreren virtuellen Maschinen aktiviert sein.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Activity Monitoring**.
- 3 Klicken Sie auf die Registerkarte **VM-Aktivität (VM Activity)**.
- 4 Klicken Sie auf den Link neben **Mit folgender Quelle (Where source)**. Wählen Sie die virtuellen Maschinen aus, für die Sie den ausgehenden Datenverkehr anzeigen lassen möchten. Geben Sie an, ob die ausgewählten virtuellen Maschinen in den Bericht eingeschlossen oder von diesem ausgeschlossen werden sollen.
- 5 Klicken Sie auf den Link neben **Mit folgendem Ziel (Where destination)**. Wählen Sie die virtuellen Maschinen aus, für die Sie den eingehenden Datenverkehr anzeigen lassen möchten. Geben Sie an, ob die ausgewählten virtuellen Maschinen in den Bericht eingeschlossen oder von diesem ausgeschlossen werden sollen.
- 6 Klicken Sie auf das Symbol **Während des Zeitraums (During period)** () und suchen Sie den Zeitraum für die Suche aus.
- 7 Klicken Sie auf **Suchen (Search)**.

Ergebnisse

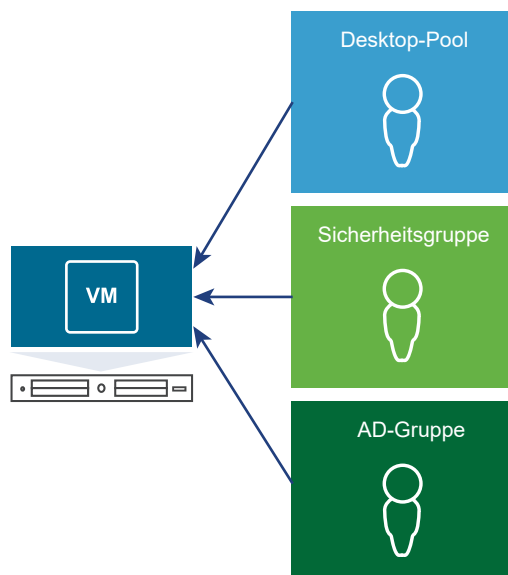
Die Suchergebnisse, gefiltert nach dem angegebenen Kriterium, werden angezeigt. Klicken Sie auf eine Zeile, um detaillierte Informationen über den Benutzer für die betreffende Zeile anzuzeigen.

Sie können bestimmte Datensätze oder alle Datensätze auf dieser Seite exportieren und sie in einem CSV-Format in einem Verzeichnis speichern, indem Sie auf das Symbol  unten rechts auf der Seite klicken.

Anzeigen eingehender Aktivität

Sie können die gesamte auf einem Server eingehende Aktivität nach Desktop-Pool, Sicherheitsgruppe oder AD-Gruppe anzeigen.

Abbildung 22-6. Anzeigen eingehender Aktivität




Sie können entweder eine schnelle Abfrage mithilfe der Standardsuchkriterien durchführen oder die Abfrage Ihren Anforderungen entsprechend konfigurieren. Klicken Sie für die schnelle Abfrage auf **Suchen (Search)**.

Voraussetzungen

- Guest Introspection muss in Ihrer Umgebung installiert sein.
- Eine Domäne muss mit NSX Manager registriert sein. Hinweise zur Domänenregistrierung finden Sie unter [Registrieren einer Windows-Domäne mit NSX Manager](#).
- Die Datenerfassung muss auf einer oder mehreren virtuellen Maschinen aktiviert sein.


Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Activity Monitoring**.

- 3 Klicken Sie auf die Registerkarte **Eingehende Aktivität (Inbound Activity)**.
- 4 Klicken Sie auf den Link neben **Ursprung von (Originating from)**.
- 5 Wählen Sie den Typ der Benutzergruppe aus, für die Sie die Aktivität anzeigen möchten.
- 6 Wählen Sie unter **Filtertyp (Filter type)** eine oder mehrere Gruppen aus und klicken Sie auf „OK“.
- 7 Wählen Sie in **Mit der virtuellen Zielmaschine (Where destination virtual machine)** die Option **schließt ein (includes)** oder **schließt aus (excludes)**, um festzulegen, ob die ausgewählten virtuellen Maschinen in die Suche eingeschlossen oder aus der Suche ausgeschlossen werden sollen.
- 8 Klicken Sie auf den Link neben **Mit der virtuellen Zielmaschine (And where destination virtual machine)**.
- 9 Wählen Sie eine oder mehrere virtuelle Maschinen aus und klicken Sie auf **OK**.
- 10 Wählen Sie in **Und mit der Zielanwendung (And where destination application)** die Option **schließt ein (includes)** oder **schließt aus (excludes)**, um festzulegen, ob die ausgewählten Anwendungen in die Suche eingeschlossen oder aus der Suche ausgeschlossen werden sollen.
- 11 Klicken Sie auf den Link neben **Und mit der Zielanwendung (And where destination application)**.
- 12 Wählen Sie eine oder mehrere Anwendungen aus und klicken Sie auf **OK**.
- 13 Klicken Sie auf das Symbol **Während des Zeitraums (During period)** () und suchen Sie den Zeitraum für die Suche aus.
- 14 Klicken Sie auf **Suchen (Search)**.

Ergebnisse

Die Suchergebnisse, gefiltert nach dem angegebenen Kriterium, werden angezeigt. Klicken Sie auf eine beliebige Stelle in der Ergebnistabelle, um Informationen über die Benutzer anzuzeigen, die auf die angegebenen virtuellen Maschinen und Anwendungen zugegriffen haben.

Sie können bestimmte Datensätze oder alle Datensätze auf dieser Seite exportieren und sie in einem CSV-Format in einem Verzeichnis speichern, indem Sie auf das Symbol  unten rechts auf der Seite klicken.

Anzeigen ausgehender Aktivität

Sie können anzeigen, welche Anwendungen von einer Sicherheitsgruppe oder einem Desktop-Pool ausgeführt werden, und dann einen Drilldown für den Bericht durchführen, um zu ermitteln, welche Clientanwendungen ausgehende Verbindungen durch eine bestimmte Gruppe von Benutzern herstellen. Sie können auch alle Benutzergruppen und Benutzer erkennen lassen, die auf eine bestimmte Anwendung zugreifen. Auf diese Weise können Sie ermitteln, ob Sie die Identitäts-Firewall in Ihrer Umgebung anpassen müssen.


Abbildung 22-7. Anzeigen ausgehender Aktivität



Voraussetzungen

- Guest Introspection muss in Ihrer Umgebung installiert sein.
- Eine Domäne muss mit NSX Manager registriert sein. Hinweise zur Domänenregistrierung finden Sie unter [Registrieren einer Windows-Domäne mit NSX Manager](#).
- Die Datenerfassung muss auf einer oder mehreren virtuellen Maschinen aktiviert sein.


Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Activity Monitoring**.
- 3 Stellen Sie sicher, dass die Registerkarte **Ausgehende Aktivität (Outbound Activity)** im linken Bereich ausgewählt ist.
- 4 Klicken Sie auf den Link neben **Ursprung von (Originating from)**.
Alle über Guest Introspection gefundenen Gruppen werden angezeigt.
- 5 Wählen Sie den Typ der Benutzergruppe aus, für die Sie die Ressourcennutzung anzeigen möchten.
- 6 Wählen Sie unter **Filter** eine oder mehrere Gruppen aus und klicken Sie auf **OK**.
- 7 Wählen Sie unter **Anwendungen sind (Where application)** die Option **schließt ein (includes)** oder **schließt aus (excludes)**, um anzugeben, ob die ausgewählte Anwendung in die Suche eingeschlossen oder von der Suche ausgeschlossen werden soll.
- 8 Klicken Sie auf den Link neben **Anwendungen sind (Where application)**.
- 9 Wählen Sie eine oder mehrere Anwendungen aus und klicken Sie auf **OK**.
- 10 Wählen Sie unter **Mit folgendem Ziel (And where destination)** die Option **schließt ein (includes)** oder **schließt aus (excludes)**, um anzugeben, ob die ausgewählten virtuellen Maschinen in die Suche eingeschlossen oder von der Suche ausgeschlossen werden sollen.
- 11 Klicken Sie auf den Link neben **Mit folgendem Ziel (And where destination)**.
- 12 Wählen Sie eine oder mehrere virtuelle Maschinen aus und klicken Sie auf **OK**.
- 13 Klicken Sie auf das Symbol **Während des Zeitraums (During period)** () und suchen Sie den Zeitraum für die Suche aus.
- 14 Klicken Sie auf **Suchen (Search)**.

Führen Sie einen Bildlauf nach rechts durch, um alle angezeigten Informationen zu sehen.

Ergebnisse

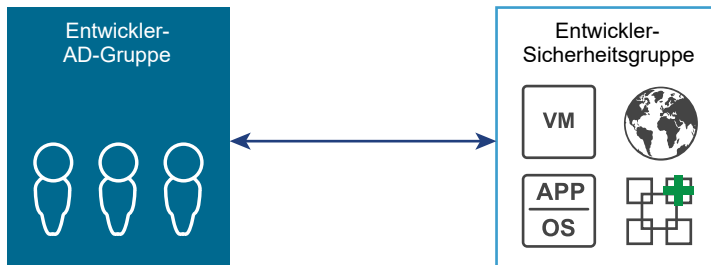
Die Suchergebnisse, gefiltert nach dem angegebenen Kriterium, werden angezeigt. Klicken Sie auf eine Zeile, um Informationen über Benutzer innerhalb der AD-Gruppe anzuzeigen, die mithilfe der betreffenden Anwendung auf die betreffenden virtuellen Maschinen zugegriffen haben.

Sie können bestimmte Datensätze oder alle Datensätze auf dieser Seite exportieren und sie in einem CSV-Format in einem Verzeichnis speichern, indem Sie auf das Symbol  unten rechts auf der Seite klicken.

Anzeigen der Interaktion zwischen Bestandslisten-Containern

Sie können den Datenverkehr zwischen definierten Containern wie z. B. AD-Gruppen, Sicherheitsgruppen und/oder Desktop-Pools anzeigen. Auf diese Weise können Sie den Zugriff auf gemeinsam genutzte Dienste ermitteln und konfigurieren sowie falsch konfigurierte Beziehungen zwischen Bestandslisten-Container-Definitionen, Desktop-Pools und AD-Gruppen auflösen.

Abbildung 22-8. Interaktionen zwischen Containern



Sie können entweder eine schnelle Abfrage mithilfe der Standardsuchkriterien durchführen oder die Abfrage Ihren Anforderungen entsprechend konfigurieren. Klicken Sie für die schnelle Abfrage auf **Suchen (Search)**.


Voraussetzungen

- Guest Introspection muss in Ihrer Umgebung installiert sein.
- Eine Domäne muss mit NSX Manager registriert sein. Hinweise zur Domänenregistrierung finden Sie unter [Registrieren einer Windows-Domäne mit NSX Manager](#).
- Die Datenerfassung muss auf einer oder mehreren virtuellen Maschinen aktiviert sein.

Verfahren


- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Activity Monitoring**.
- 3 Wählen Sie im linken Fensterbereich die Registerkarte **Inter-Container-Interaktion (Inter Container Interaction)** aus.
- 4 Klicken Sie auf den Link neben **Ursprung von (Originating from)**.

Alle über Guest Introspection gefundenen Gruppen werden angezeigt.

- 5 Wählen Sie den Typ der Benutzergruppe aus, für die Sie die Ressourcennutzung anzeigen möchten.
- 6 Wählen Sie unter **Filter** eine oder mehrere Gruppen aus und klicken Sie auf **OK**.
- 7 Wählen Sie in **Mit folgendem Ziel (Where the destination is)** die Option **ist (is)** oder **ist nicht (is not)** aus, um festzulegen, ob die angegebene Gruppe in die Suche eingeschlossen oder aus der Suche ausgeschlossen werden soll.
- 8 Klicken Sie auf den Link neben **Mit folgendem Ziel (Where the destination is)**.
- 9 Wählen Sie den Gruppentyp aus.
- 10 Wählen Sie unter **Filter** eine oder mehrere Gruppen aus und klicken Sie auf **OK**.
- 11 Klicken Sie auf das Symbol **Während des Zeitraums (During period)** () und suchen Sie den Zeitraum für die Suche aus.
- 12 Klicken Sie auf **Suchen (Search)**.

Ergebnisse

Die Suchergebnisse, gefiltert nach dem angegebenen Kriterium, werden angezeigt. Klicken Sie in eine Zeile, um Informationen über die Benutzer anzuzeigen, die auf die angegebenen Container zugegriffen haben.

Sie können bestimmte Datensätze oder alle Datensätze auf dieser Seite exportieren und sie in einem CSV-Format in einem Verzeichnis speichern, indem Sie auf das Symbol  unten rechts auf der Seite klicken.

Beispiel: Abfrage „Interaktion zwischen Bestandslisten-Containern“

■ Zugelassene Kommunikation überprüfen

Wenn Sie Container in Ihrer vCenter-Bestandsliste definiert und dann eine Regel hinzugefügt haben, um die Kommunikation zwischen diesen Containern zuzulassen, können Sie die Funktion der Regel überprüfen, indem Sie die beiden Container in den Feldern **Ursprung von (Originating from)** und **Mit folgendem Ziel (Where the destination is)** angeben und die Abfrage ausführen.

■ Nicht zugelassene Kommunikation überprüfen

Wenn Sie Container in Ihrer vCenter-Bestandsliste definiert und dann eine Regel hinzugefügt haben, um keine Kommunikation zwischen diesen Containern zuzulassen, können Sie die Funktion der Regel überprüfen, indem Sie die beiden Container in den Feldern **Ursprung von (Originating from)** und **Mit folgendem Ziel (Where the destination is)** angeben und die Abfrage ausführen.

■ Nicht zugelassene Kommunikation innerhalb eines Containers überprüfen

Wenn Sie eine Richtlinie implementiert haben, die keine Kommunikation von Mitgliedern eines Containers mit anderen Mitgliedern desselben Containers zulässt, können Sie die Funktion der Richtlinie mit dieser Abfrage überprüfen. Wählen Sie den Container in den beiden Feldern **Ursprung von (Originating from)** und **Mit folgendem Ziel (Where the destination is)** aus.

■ Nicht erforderlichen Zugriff ausschließen

Angenommen, Sie haben in Ihrer vCenter-Bestandsliste Container definiert und dann eine Regel hinzugefügt, um die Kommunikation zwischen diesen Containern zuzulassen. Möglicherweise gibt es in den Containern Mitglieder, die überhaupt nicht mit dem anderen Container interagieren. Diese Mitglieder können Sie aus dem entsprechenden Container entfernen, um die Sicherheitsüberwachung zu optimieren. Um eine entsprechende Liste abzurufen, wählen Sie den betreffenden Container in den beiden Feldern **Ursprung von (Originating from)** und **Mit folgendem Ziel (Where the destination is)** aus. Wählen Sie **ist nicht (is not)** neben dem Feld **Mit folgendem Ziel (Where the destination is)** aus.

Anzeigen der ausgehenden AD-Gruppenaktivität

Sie können den Datenverkehr zwischen Mitgliedern definierter Active Directory-Gruppen anzeigen und diese Daten verwenden, um Ihre Firewallregeln zu optimieren.

Sie können entweder eine schnelle Abfrage mithilfe der Standardsuchkriterien durchführen oder die Abfrage Ihren Anforderungen entsprechend konfigurieren. Klicken Sie für die schnelle Abfrage auf **Suchen (Search)**.

Voraussetzungen

- Guest Introspection muss in Ihrer Umgebung installiert sein.
- Eine Domäne muss mit NSX Manager registriert sein. Hinweise zur Domänenregistrierung finden Sie unter [Registrieren einer Windows-Domäne mit NSX Manager](#).
- Die Datenerfassung muss auf einer oder mehreren virtuellen Maschinen aktiviert sein.

Verfahren


- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Activity Monitoring**.
- 3 Wählen Sie im linken Fenster die Registerkarte **AD-Gruppen und -Container (AD Groups & Containers)** aus.
- 4 Klicken Sie auf den Link neben **Ursprung von (Originating from)**.
Alle über Guest Introspection gefundenen Gruppen werden angezeigt.
- 5 Wählen Sie den Benutzergruppentyp aus, den Sie in die Suche einschließen möchten.
- 6 Wählen Sie unter **Filter** eine oder mehrere Gruppen aus und klicken Sie auf **OK**.
- 7 Wählen Sie in **Mit der AD-Gruppe (Where AD Group)** die Option **schließt ein (includes)** oder **schließt aus (excludes)**, um festzulegen, ob die angegebene AD-Gruppe in die Suche eingeschlossen oder aus der Suche ausgeschlossen werden soll.
- 8 Klicken Sie auf den Link neben **Mit der AD-Gruppe (Where AD Group)**.
- 9 Wählen Sie eine oder mehrere AD-Gruppen aus und klicken Sie auf **OK**.

10 Klicken Sie auf das Symbol **Während des Zeitraums (During period)** () und suchen Sie den Zeitraum für die Suche aus.

11 Klicken Sie auf **Suchen (Search)**.

Ergebnisse

Die Suchergebnisse, gefiltert nach dem angegebenen Kriterium, werden angezeigt. Klicken Sie in eine Zeile, um Informationen über die Mitglieder der angegebenen AD-Gruppe anzuzeigen, die auf Netzwerkressourcen aus der angegebenen Sicherheitsgruppe oder dem angegebenen Desktop-Pool heraus zugreifen.

Sie können bestimmte Datensätze oder alle Datensätze auf dieser Seite exportieren und sie in einem CSV-Format in einem Verzeichnis speichern, indem Sie auf das Symbol  unten rechts auf der Seite klicken.

Überschreiben der Datenerfassung

In einem Notfall (beispielsweise bei einer Netzwerküberlastung) können Sie die Datenerfassung auf globaler Ebene deaktivieren. Dadurch werden alle anderen Einstellungen für die Datenerfassung außer Kraft gesetzt.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an.
- 2 Klicken Sie auf **Networking & Security** und anschließend auf **Activity Monitoring**.
- 3 Klicken Sie auf die Registerkarte **Einstellungen (Settings)**.
- 4 Wählen Sie den vCenter Server aus, für den Sie die Datenerfassung außer Kraft setzen möchten.
- 5 Klicken Sie auf **Bearbeiten (Edit)**.
- 6 Deaktivieren Sie die Option **Berichtsdaten erfassen (Collect reporting data)**.
- 7 Klicken Sie auf **OK**.

Datenerfassung für die Endpunktüberwachung

Durch die Endpunktüberwachung können Benutzer bestimmte Prozesse auf dem Gastbetriebssystem zu den Netzwerkverbindungen zuordnen, die die Prozesse verwenden.

Hinweis Nachdem Daten erfasst wurden, werden sie täglich um 2:00 Uhr gelöscht. Während der Datenlöschung wird die Anzahl der Flow-Datensätze für alle Sitzungen insgesamt geprüft und alle Datensätze mit über 20 Millionen Einträgen (oder rund 4 GB) werden gelöscht. Die Löschung beginnt bei der ältesten Sitzung und wird fortgesetzt, bis die Anzahl der Flow-Datensätze in der Datenbank unter 15 Millionen beträgt. Wenn während der Datenlöschung eine Sitzung ausgeführt wird, können einige Datensätze verloren gehen.

Voraussetzungen

- Endpunktüberwachung wird auf folgenden Windows-Betriebssystemen unterstützt:
Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 2008, Windows 2008 R2, Windows 2012, Windows 10 und Windows 2016. Es wird auf Linux nicht unterstützt.
- Guest Introspection muss auf den virtuellen Maschinen (VMs) installiert sein.
- Die aktuelle Version von VMware Tools muss auf Ihren Windows-Desktop-VMs ausgeführt werden.
- Es werden Sicherheitsgruppen mit maximal 20 VMs für die Datenerfassung benötigt, bevor die Endpunktüberwachung beginnen kann. Weitere Informationen hierzu finden Sie unter [Erstellen einer Sicherheitsgruppe](#).
- Die Datenerfassung muss für eine oder mehrere virtuelle Maschinen auf einem vCenter Server aktiviert sein, bevor Sie den Endpunktüberwachungsbericht ausführen. Stellen Sie vor dem Ausführen des Berichts sicher, dass die aktivierten virtuellen Maschinen aktiv sind und Verkehr im Netzwerk erzeugen.

Verfahren

- 1 Melden Sie sich beim vSphere Web Client an und wählen Sie dann **Networking & Security** aus dem linken Navigationsbereich aus.
- 2 Wählen Sie **Endpunktüberwachung (Endpoint Monitoring)** aus.
- 3 Klicken Sie auf der Registerkarte „Übersicht“ auf **Datenerfassung starten (Start Collecting Data)**.
- 4 Wählen Sie aus dem Popup-Fenster „Datenerfassung für Sicherheitsgruppen starten“ die Sicherheitsgruppen aus, für die Sie Daten erfassen möchten. Klicken Sie auf **OK**.

Die VMs sind in dem Feld aufgeführt.
- 5 Schalten Sie die Datenerfassung auf **EIN (ON)**.
- 6 Klicken Sie auf **OK**.

Der Hauptbildschirm der Endpunktüberwachung wird angezeigt. Links oben wird der Status „Datenerfassung“ eingeblendet.
- 7 Klicken Sie auf **Datenerfassung stoppen (Stop Collecting Data)**, um die Datenerfassung zu beenden.

Der Bildschirm der Endpunktüberwachung wird mit der Registerkarte „Übersicht“ angezeigt, die Daten enthält.

Endpunktüberwachung

Die Endpunktüberwachung ermöglicht Sichtbarkeit für bestimmte Anwendungsprozesse und die zugeordneten Netzwerkverbindungen.

Registerkarte „Übersicht“

Nach dem Abschluss der Datenerfassung werden im Übersichtsbildschirm die Details zum NSX Manager, die Sicherheitsgruppe und das Zeitfenster der erfassten Daten angezeigt. Im ersten Feld finden Sie die Anzahl der ausgeführten virtuellen Maschinen (VMs) und die Gesamtzahl der Prozesse, die Datenverkehr generieren. Wenn Sie auf die Anzahl der ausgeführten virtuellen Maschinen klicken, wird die Registerkarte „VM-Flows“ (siehe weiter unten) aufgerufen. Wenn Sie auf die Gesamtzahl der Prozesse klicken, die Datenverkehr generieren, wird die Registerkarte „Prozess-Flows“ (siehe weiter unten) aufgerufen.

Das zweite Feld zeigt ein Symbol mit der Anzahl der gesamten Flows an. Bei einem Flow handelt es sich um einen eindeutigen Datenstrom des Netzwerkdatenverkehrs, der durch seinen Pakettyp, die Quell- und Ziel-ID sowie den Port gekennzeichnet ist. Wenn Sie den Cursor auf einen Abschnitt setzen, wird die Anzahl der Flows innerhalb oder außerhalb der Sicherheitsgruppe angezeigt.

Registerkarte „VM-Flows“

In diesem Bildschirm sind die Details der Flows in den VMs aufgeführt. Dazu gehören:

- VM-Name – Name der VM, die überwacht wird
- Flows innerhalb der Sicherheitsgruppe – Datenverkehr zwischen den VMs, wobei sich die Quelle oder das Ziel innerhalb der überwachten Sicherheitsgruppe befindet
- Flows außerhalb der Sicherheitsgruppe – Datenverkehr zwischen den VMs, wobei sich die Quelle oder das Ziel außerhalb der überwachten Sicherheitsgruppe befindet
- Gemeinsame Dienst-Flows außerhalb der Sicherheitsgruppe – Gemeinsame Dienst-Flows wie DHCP, LDAP, DNS oder NTP außerhalb der überwachten Sicherheitsgruppe
- Gemeinsame Dienst-Flows innerhalb der Sicherheitsgruppe – Gemeinsame Dienst-Flows wie DHCP, LDAP, DNS oder NTP innerhalb der überwachten Sicherheitsgruppe

Durch Klicken auf einen VM-Namen in der Tabelle wird eine Bubble-Grafik mit folgendem Inhalt angezeigt:

- Flows zwischen VMs in derselben Sicherheitsgruppe
- Flows mit gemeinsamen Diensten
- Flows zwischen unterschiedlichen Sicherheitsgruppen

Klicken Sie auf eine Bubble-Grafik, um die Details der VM anzuzeigen. Die Flow-Detailansicht enthält den Prozessnamen, die Version und die Anzahl der Flows, die von jedem Prozess generiert werden. Wenn darin gemeinsame Dienste angezeigt werden, wird ein spezielles Symbol dargestellt. Durch Klicken auf eine Linie zwischen zwei VM-Bubble-Grafiken werden die Prozess-Flow-Details der Flows zwischen diesen beiden VMs eingeblendet. Dazu gehören:

- Quellprozess – Name der Anwendung bzw. der ausführbaren Datei, die Datenverkehr generiert und den Flow initiiert
- Quellversion – Dateiversion der Quelle
- Protokoll – TCP

- Zielprozess – Name der Serveranwendung bzw. der ausführbaren Serverdatei des Prozesses, die das Ziel des Flows darstellt
- Zielport – Portnummer des Ziels

Registerkarte „Prozess-Flows“

Dieser Bildschirm enthält eine Liste aller Anwendungen, die Flows generieren. In der Tabelle sind folgenden Informationen enthalten:

- Prozessname – Name der Anwendung, die Datenverkehr generiert
- VM-Name
- Flows innerhalb der Sicherheitsgruppe – Datenverkehr zwischen den VMs, wobei sich die Quelle oder das Ziel innerhalb der überwachten Sicherheitsgruppe befindet
- Flows außerhalb der Sicherheitsgruppe – Datenverkehr zwischen den VMs, wobei sich die Quelle oder das Ziel außerhalb der überwachten Sicherheitsgruppe befindet
- Gemeinsame Flows innerhalb der Sicherheitsgruppe – gemeinsame Flows, innerhalb der überwachten Sicherheitsgruppe
- Gemeinsame Flows außerhalb der Sicherheitsgruppe – gemeinsame Flows, außerhalb der überwachten Sicherheitsgruppe

Die Bubble-Grafik stellt die Flows dar, die mit dem Prozess oder der Anwendung auf der ausgewählten VM als Anker auftreten. Klicken Sie auf eine Bubble-Grafik, um den Prozessnamen und die Prozessversion anzuzeigen. Durch Klicken auf eine beliebige Linie wird Folgendes angezeigt:

- Quell-VM – Name der Client-VM, die den Clientprozess hostet
- Quell-IP – IP-Adresse des Flows
- Protokoll – TCP
- Ziel-VM – Name der Server-VM, die den Serverprozess hostet
- Ziel-IP – IP-Adresse des Ziels
- Zielport – Portnummer des Ziels

Traceflow

Traceflow ist ein Problembehebungstool, das in ein Paket eingefügt werden kann, um den Weg dieses Pakets durch das physische und das logische Netzwerk zu verfolgen. Auf diese Weise erhalten Sie Informationen über das Netzwerk und können so etwa ausgefallene Knoten oder Firewallregeln feststellen, die den Empfang des Pakets an seinem Ziel verhindern.

Informationen zu Traceflow

Traceflow injiziert Pakete in einen vSphere Distributed Switch-Port (VDS-Port) und bietet mehrere Beobachtungspunkte entlang des Paketpfads, wenn es in den Overlay- und Underlay-Netzwerken

physische und logische Entitäten durchläuft (wie z. B. ESXi-Hosts, logische Switches und logische Router). Dadurch können Sie identifizieren, welchen Pfad (bzw. welche Pfade) ein Paket zu seinem Ziel nimmt, oder im umgekehrten Fall wo ein Paket auf dem Weg abgelegt wird. Jede Entität meldet die Verarbeitung des Pakets an der Eingabe und Ausgabe, damit Sie ermitteln können, ob Probleme beim Empfang oder bei der Weiterleitung des Pakets auftreten.

Beachten Sie, dass Traceflow sich von einer Ping-Anforderung/-Antwort, die von Gast-VM-Stack zu Gast-VM-Stack verläuft, unterscheidet. Traceflow verfolgt ein markiertes Paket beim Durchlauf durch ein Overlay-Netzwerk. Jedes Paket wird auf seinem Weg über das Overlay-Netzwerk überwacht, bis es die Ziel-Gast-VM erreicht und dort zugestellt werden kann. Allerdings wird das injizierte Traceflow-Paket selbst nicht an die Ziel-Gast-VM übermittelt. Das bedeutet, dass Traceflow auch dann erfolgreich ausgeführt werden kann, wenn die Gast-VM heruntergefahren wurde.

Traceflow unterstützt die folgenden Arten des Datenverkehrs:

- Schicht 2-Unicast
- Schicht 3-Unicast
- Schicht 2-Broadcast
- Schicht 2-Multicast

Sie können Pakete mit benutzerdefinierten Kopfzeilen und Paketgrößen erstellen. Die Quelle des Traceflows ist immer die virtuelle Netzwerkkarte (vNIC) einer virtuellen Maschine. Der Zielpunkt kann ein beliebiges Gerät im NSX Overlay oder Underlay sein. Sie dürfen jedoch kein Ziel auswählen, dass sich im Norden eines NSX Edge Services Gateway (ESG) befindet. Das Ziel muss sich in demselben Subnetz befinden oder durch die NSX Distributed Logical Router erreichbar sein.

Der Traceflow-Vorgang wird als Schicht 2 betrachtet, wenn sich die Quell- und Ziel-vNICs in derselben Schicht 2-Domäne befinden. In NSX bedeutet dies, dass sie sich auf demselben VXLAN-Netzwerkbezeichner (VNI oder Segment-ID) befinden. Dies geschieht beispielsweise, wenn zwei VMs mit demselben logischen Switch verbunden sind.

Wenn das NSX-Bridging konfiguriert ist, werden unbekannte Schicht 2-Pakete immer zur Bridge gesendet. Normalerweise leitet die Bridge diese Pakete an ein VLAN weiter und meldet das Traceflow-Paket als zugestellt. Wenn ein Paket als zugestellt gemeldet wird, bedeutet dies nicht zwangsläufig, dass das Traceflow-Paket an das angegebene Ziel übermittelt wurde.

Für Schicht 3-Traceflow-Unicast-Datenverkehr befinden sich die beiden Endpunkte auf unterschiedlichen logischen Switches und haben unterschiedliche VNIs, die mit einem verteilten logischen Router (Distributed Logical Switch, DLR) verbunden sind.

Für Multicast-Datenverkehr ist die Quelle die vNIC einer VM und das Ziel eine Multicast-Gruppenadresse.

Traceflow-Beobachtungen können auch Beobachtungen von gesendeten Traceflow-Paketen beinhalten. Der ESXi-Host sendet ein Traceflow-Paket, wenn er die MAC-Adresse des Ziel-Hosts nicht kennt. Für den Broadcast-Datenverkehr ist die Quelle die vNIC einer VM. Die Schicht 2-MAC-Zieladresse für Broadcast-Datenverkehr lautet FF:FF:FF:FF:FF:FF. Der Broadcast-Traceflow-Vorgang benötigt für die Erstellung eines gültigen Pakets für eine Firewallinspektion die Länge eines Subpräfixes. Die Subnetzmaske ermöglicht NSX die Berechnung einer IP-Netzwerkadresse für das Paket.

Vorsicht Je nach Anzahl der logischen Ports in Ihrer Bereitstellung erzeugen die Multicast- und Broadcast-Traceflow-Vorgänge möglicherweise ein hohes Datenverkehrsaufkommen.

Es gibt zwei Verwendungsmöglichkeiten von Traceflow: über die API oder die grafische Benutzeroberfläche (Graphical User Interface, GUI). Bei der API handelt es sich um dieselbe API, die von der GUI verwendet wird, außer dass Ihnen die API die Angabe der genauen Einstellungen innerhalb des Pakets ermöglicht, während es bei der GUI mehr Einschränkungen bezüglich den Einstellungen gibt.

Die GUI ermöglicht Ihnen die Festlegung der folgenden Werte:

- Protokoll – TCP, UDP, ICMP
- Time-To-Live (TTL) Die Standardeinstellung ist 64 Hops.
- Portnummern für TCP- und UDP-Quelle und -Ziel. Die Standardwerte sind 0.
- TCP-Flags
- ICMP-ID und Sequenznummer Beide sind standardmäßig 0.
- Zeitlimit für Ablauf des Traceflow-Vorgangs in Millisekunden Die Standardeinstellung ist 10.000 ms.
- Größe des Ethernet-Frames Die Standardeinstellung ist 128 Byte pro Frame Die maximale Frame-Größe beträgt 1000 Byte pro Frame.
- Nutzlast-Kodierung Die Standardeinstellung ist Base64.
- Nutzlast-Wert

Fehlerbehebung mithilfe von Traceflow

Es gibt mehrere Szenarien, in denen Traceflow nützlich ist.

Traceflow ist in den folgenden Szenarien nützlich:

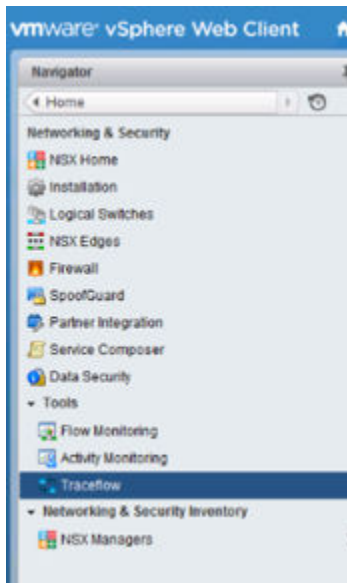
- Fehlerbehebung von Netzwerkfehlern, um den exakten Pfad des Datenverkehrs anzuzeigen
- Leistungsüberwachung, um die Linkauslastung anzuzeigen
- Netzwerkplanung, um anzuzeigen, wie sich ein Netzwerk in Produktionsumgebungen verhält

Voraussetzungen

- Für Traceflow-Vorgänge ist die Kommunikation zwischen vCenter, NSX Manager, dem NSX Controller-Cluster und den netcpa-Benutzerwelt-Agenten auf den Hosts erforderlich.
- Damit Traceflow wie erwartet funktioniert, stellen Sie sicher, dass der Controller-Cluster verbunden ist und einen ordnungsgemäßen Status aufweist.

Verfahren

- 1 Navigieren Sie im vCenter Web Client zu **Home > Networking & Security > Traceflow**.



- 2 Wählen Sie den Datenverkehrstyp aus: Unicast, Broadcast oder Multicast.
- 3 Wählen Sie die Quell-VM-vNIC aus.

Wenn die VM im selben vCenter Server verwaltet wird, in der Traceflow ausgeführt wird, können Sie die VM und vNIC aus einer Liste auswählen.

- 4 Geben Sie für einen Unicast-Traceflow die Ziel-vNIC-Informationen ein.

Das Ziel kann eine vNIC eines beliebigen Geräts in dem NSX-Overlay oder -Underlay sein, wie beispielsweise ein Host, eine VM, ein logischer Router oder ein Edge Services Gateway. Wenn das Ziel eine VM ist, auf der VMware Tools ausgeführt wird und die im selben vCenter Server verwaltet wird, von dem aus der Traceflow ausgeführt wird, können Sie die VM und vNIC aus einer Liste auswählen.

Andernfalls müssen Sie die IP-Zieladresse eingeben (und die MAC-Adresse für einen Unicast-Traceflow Schicht 2). Sie können diese Informationen auf dem Gerät selbst in der Gerätekonsole oder in einer SSH-Sitzung erfassen. Beispiel: Wenn es sich um eine Linux-VM handelt, können Sie ihre IP- und MAC-Adresse abrufen, indem Sie den `ifconfig`-Befehl im Linux-Terminal ausführen. Für einen logischen Router oder ein Edge Services Gateway können Sie die Informationen über den `show interface`-CLI-Befehl erfassen.

- 5 Geben Sie für einen Broadcast-Traceflow Schicht 2 die Länge des Subnetzpräfixes ein.

Das Paket wird nur basierend auf der MAC-Adresse gewechselt. Die Ziel-MAC-Adresse ist `FF:FF:FF:FF:FF:FF`.

Sowohl Quell- als auch Ziel-IP-Adressen sind erforderlich, damit das IP-Paket für eine Firewallinspektion in Frage kommt.

- 6 Für einen Multicast-Traceflow Schicht 2 geben Sie die Multicast-Gruppenadresse ein.

Das Paket wird nur basierend auf der MAC-Adresse gewechselt.

Sowohl Quell- als auch Ziel-IP-Adressen sind erforderlich, damit das IP-Paket gültig ist. Im Fall von Multicast wird die MAC-Adresse aus der IP-Adresse abgeleitet.

- 7 Konfigurieren Sie andere erforderliche und optionale Einstellungen.

- 8 Klicken Sie auf **Ablaufverfolgung (Trace)**.

Beispiel: Szenarien

Im folgenden Beispiel wird ein Schicht 2-Traceflow gezeigt, der zwei VMs umfasst, die auf einem einzelnen ESXi-Host ausgeführt werden. Die zwei VMs sind mit einem einzelnen logischen Switch verbunden.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **Unicast**

Source: web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: web-02a - Network adapter 1 Change...
IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b

Advanced Options

Protocol: **TCP**

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

| Sequence | Observation Type | Host | Component Type | Component Name |
|----------|------------------|--------------------|----------------|----------------|
| 0 | Injected | esx-01a.corp.local | vNIC | vNIC |
| 1 | Received | esx-01a.corp.local | Firewall | Firewall |
| 2 | Forwarded | esx-01a.corp.local | Firewall | Firewall |
| 3 | Received | esx-01a.corp.local | Firewall | Firewall |
| 4 | Forwarded | esx-01a.corp.local | Firewall | Firewall |
| 5 | Delivered | esx-01a.corp.local | vNIC | vNIC |

Im folgenden Beispiel wird ein Schicht 2-Traceflow gezeigt, der zwei VMs umfasst, die auf zwei verschiedenen ESXi-Hosts ausgeführt werden. Die zwei VMs sind mit einem einzelnen logischen Switch verbunden.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **Unicast**

Source: web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: web-03a - Network adapter 1 Change...
IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

▼ Advanced Options

Protocol: **TCP**

Source Port: 0

Destination Port: 0

TCP Flags: ☐ FIN ☒ SYN ☐ RST

Timeout (ms): 10000

Frame Size: 128

TTL: 64

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

| Sequence | Observation Type | Host | Component Type | Component Name |
|----------|------------------|-----------------------|----------------|-----------------------|
| 0 | Injected | esx-01a.corp.local | vNIC | vNIC |
| 1 | Received | esx-01a.corp.local | Firewall | Firewall |
| 2 | Forwarded | esx-01a.corp.local | Firewall | Firewall |
| 3 | Forwarded | esx-01a.corp.local | Physical | esx-01a.corp.local |
| 3 | Forwarded | esx-01a.corp.local | Physical | esx-01a.corp.local |
| 4 | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | Received | esx-02a.corp.local | Physical | esx-02a.corp.local |
| 4 | Received | esx-02a.corp.local | Physical | esx-02a.corp.local |
| 5 | Received | esx-02a.corp.local | Firewall | Firewall |
| 6 | Forwarded | esx-02a.corp.local | Firewall | Firewall |
| 7 | Delivered | esx-02a.corp.local | vNIC | vNIC |

Im folgenden Beispiel wird ein Schicht 3-Traceflow gezeigt. Die zwei VMs sind mit zwei verschiedenen logischen Switches verbunden, die durch einen logischen Router getrennt sind.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * db-01a - Network adapter 1 Change...
IP: 172.16.30.11, MAC: 00:50:56:ae:d4:2b

► Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

| Sequence | 1 ▲ | Observation Type | Host | Component Type | Component Name |
|----------|-----|------------------|--------------------|----------------|--------------------------|
| 0 | | Injected | esx-01a.corp.local | vNIC | vNIC |
| 1 | | Received | esx-01a.corp.local | Firewall | Firewall |
| 2 | | Forwarded | esx-01a.corp.local | Firewall | Firewall |
| 3 | | Forwarded | esx-01a.corp.local | Logical Switch | Web-Tier-01 |
| 4 | | Received | esx-01a.corp.local | Logical Router | Local-Distributed-Router |
| 5 | | Forwarded | esx-01a.corp.local | Logical Router | Local-Distributed-Router |
| 6 | | Received | esx-01a.corp.local | Logical Switch | DB-Tier-01 |
| 7 | | Forwarded | esx-01a.corp.local | Physical | esx-01a.corp.local |
| 8 | | Received | esx-02a.corp.local | Physical | esx-02a.corp.local |
| 8 | | Received | esx-02a.corp.local | Physical | esx-02a.corp.local |
| 9 | | Received | esx-02a.corp.local | Firewall | Firewall |
| 10 | | Forwarded | esx-02a.corp.local | Firewall | Firewall |
| 11 | | Delivered | esx-02a.corp.local | vNIC | vNIC |

Im folgenden Beispiel wird ein Broadcast-Traceflow in einer Bereitstellung gezeigt, in der drei VMs mit einem einzelnen logischen Switch verbunden sind. Zwei der VMs befinden sich auf einem Host (esx-01a) und die dritte VM befindet sich auf einem anderen Host (esx-02a). Der Broadcast wird von einer der VMs auf Host 192.168.210.53 gesendet.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **L2 Broadcast** ⚠ High volume of traffic may get generated for this traffic type.

Source: * web-01a - Network adapter 1 [Change...](#) Subnet Prefix Length: * **24**

IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d IP: 172.16.10.255, MAC: FF:FF:FF:FF:FF:FF

► Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

3 Delivered

| Sequence | 1 ▲ | Observation Type | Host | Component Type | Component Name |
|----------|-----|------------------|-----------------------|----------------|-----------------------|
| 0 | | Injected | esx-01a.corp.local | vNIC | vNIC |
| 1 | | Received | esx-01a.corp.local | Firewall | Firewall |
| 2 | | Forwarded | esx-01a.corp.local | Firewall | Firewall |
| 3 | | Forwarded | esx-01a.corp.local | Logical Switch | Web-Tier-01 |
| 3 | | Received | esx-01a.corp.local | Firewall | Firewall |
| 3 | | Forwarded | esx-01a.corp.local | Physical | esx-01a.corp.local |
| 3 | | Forwarded | esx-01a.corp.local | Physical | esx-01a.corp.local |
| 4 | | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | | Forwarded | esx-01a.corp.local | Firewall | Firewall |
| 4 | | Received | esx-02a.corp.local | Physical | esx-02a.corp.local |
| 4 | | Received | esx-02a.corp.local | Physical | esx-02a.corp.local |
| 5 | | Forwarded | esxmgt-02a.corp.local | Logical Switch | Web-Tier-01 |
| 5 | | Forwarded | esxmgt-02a.corp.local | Logical Switch | Web-Tier-01 |
| 5 | | Forwarded | esxmgt-02a.corp.local | Logical Switch | Web-Tier-01 |
| 5 | | Forwarded | esxmgt-02a.corp.local | Logical Switch | Web-Tier-01 |
| 5 | | Delivered | esxmgt-02a.corp.local | vNIC | vNIC |
| 5 | | Delivered | esx-01a.corp.local | vNIC | vNIC |
| 5 | | Forwarded | esx-02a.corp.local | Logical Switch | Web-Tier-01 |
| 5 | | Forwarded | esx-02a.corp.local | Logical Switch | Web-Tier-01 |
| 5 | | Received | esx-02a.corp.local | Firewall | Firewall |
| 6 | | Forwarded | esx-02a.corp.local | Firewall | Firewall |
| 7 | | Delivered | esx-02a.corp.local | vNIC | vNIC |

Im folgenden Beispiel wird gezeigt, was geschieht, wenn Multicast-Datenverkehr in einer Bereitstellung gesendet wird, für die Multicast konfiguriert ist.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: **L2 Multicast** ⚠ High volume of traffic may get generated for this traffic type.

Source: * web-01a - Network adapter 1 [Change...](#) Destination IP: * 239.0.0.1 e.g. 239.0.0.1
 IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d IP: 239.0.0.1, MAC: 01:00:5e:00:00:01

► Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

3 Delivered

| Sequence | 1 ▲ | Observation Type | Host | Component Type | Component Name |
|----------|-----|------------------|-----------------------|----------------|-----------------------|
| 0 | | Injected | esx-01a.corp.local | vNIC | vNIC |
| 1 | | Received | esx-01a.corp.local | Firewall | Firewall |
| 2 | | Forwarded | esx-01a.corp.local | Firewall | Firewall |
| 3 | | Received | esx-01a.corp.local | Firewall | Firewall |
| 3 | | Forwarded | esx-01a.corp.local | Physical | esx-01a.corp.local |
| 3 | | Forwarded | esx-01a.corp.local | Physical | esx-01a.corp.local |
| 4 | | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | | Received | esxmgt-02a.corp.local | Physical | esxmgt-02a.corp.local |
| 4 | | Forwarded | esx-01a.corp.local | Firewall | Firewall |
| 4 | | Received | esx-02a.corp.local | Physical | esx-02a.corp.local |
| 4 | | Received | esx-02a.corp.local | Physical | esx-02a.corp.local |
| 5 | | Delivered | esxmgt-02a.corp.local | vNIC | vNIC |
| 5 | | Delivered | esx-01a.corp.local | vNIC | vNIC |
| 5 | | Received | esx-02a.corp.local | Firewall | Firewall |
| 6 | | Forwarded | esx-02a.corp.local | Firewall | Firewall |
| 7 | | Delivered | esx-02a.corp.local | vNIC | vNIC |

Im folgenden Beispiel wird gezeigt, was passiert, wenn ein Traceflow aufgrund einer Regel für die verteilte Firewall gelöscht wird, die ICMP-Datenverkehr blockiert, der zur Zieladresse gesendet wird. Hinweis: Der Datenverkehr verlässt den ursprünglichen Host nie, selbst wenn sich die Ziel-VM auf einem anderen Host befindet.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-02a - Network adapter 1 Change...
IP: 172.16.10.12, MAC: 00:50:56:ae:f8:6b

Destination: * web-03a - Network adapter 1 Change...
IP: 172.17.10.11, MAC: 00:50:56:ae:cf:88

► Advanced Options

Trace

Trace Result: Traceflow dropped observation(s) reported

1 Dropped

| Sequence | Observation Type | Host | Component Type | Component Name |
|----------|------------------|--------------------|----------------|------------------------|
| 0 | Injected | esx-01a.corp.local | vNIC | vNIC |
| 1 | Received | esx-01a.corp.local | Firewall | Firewall |
| 2 | Dropped | esx-01a.corp.local | Firewall | Firewall (Rule - 1013) |

Im folgenden Beispiel wird gezeigt, was passiert, wenn sich ein Traceflow-Ziel auf der anderen Seite eines Edge Services Gateways befindet, wie beispielsweise eine IP-Adresse im Internet oder ein beliebiges internes Ziel, das durch das Edge Services Gateway geleitet werden muss. Der Traceflow ist gemäß Programm-Design nicht zulässig, weil er nur für Ziele unterstützt wird, die sich im selben Subnetz befinden oder über Distributed Logical Router (DLRs) erreichbar sind.

Select Traceflow Destination

Destination IP address should be on the same subnet or should be reachable via the Distributed Logical Router

IP Address: * 40.1.2.3

☐ Select Destination vNIC

Selected: web-03a - Network adapter 1

Filter

Available Objects

- app-01a
- db-01a
- web-01a
- web-02a

5 items

OK Cancel

Im folgenden Beispiel wird gezeigt, was passiert, wenn das Traceflow-Ziel eine VM ist, die sich in einem anderen Subnetz befindet und ausgeschaltet ist.

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * app-01a - Network adapter 1 Change...
IP: 172.16.20.11, MAC: 00:50:56:ae:23:b9

Destination: * db-01a - Network adapter 1 Change...
IP: 172.16.30.11, MAC: 00:50:56:ae:d...

► Advanced Options

Trace

Trace Result: No delivered or dropped observations reported

| Sequence | 1 ▲ | Observation Type | Host | Component Type | Component Name |
|----------|-----|------------------|--------------------|----------------|--------------------------|
| 0 | | Injected | esx-02a.corp.local | vNIC | vNIC |
| 1 | | Received | esx-02a.corp.local | Firewall | Firewall |
| 2 | | Forwarded | esx-02a.corp.local | Firewall | Firewall |
| 3 | | Forwarded | esx-02a.corp.local | Logical Switch | App-Tier-01 |
| 4 | | Received | esx-02a.corp.local | Logical Router | Local-Distributed-Router |
| 5 | | Forwarded | esx-02a.corp.local | Logical Router | Local-Distributed-Router |
| 6 | | Received | esx-02a.corp.local | Logical Switch | DB-Tier-01 |