

vSphere-Netzwerk

Update 2

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

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

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

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

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

Copyright © 2009-2018 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

Grundlegende Informationen zu vSphere-Netzwerken 11

Aktualisierte Informationen 12

1 Einführung in Netzwerke 13

Übersicht über Netzwerkkonzepte 13

Netzwerkdienste in ESXi 15

VMware ESXi Dump Collector-Unterstützung 16

2 Einrichten von Netzwerken mit vSphere Standard-Switches 17

vSphere Standard-Switches 17

vSphere Standard-Switch erstellen 19

Konfiguration von Portgruppen für virtuelle Maschinen 20

Hinzufügen einer Portgruppe für virtuelle Maschinen 21

Bearbeiten einer Portgruppe für den Standard-Switch 22

Entfernen einer Portgruppe aus einem vSphere Standard-Switch 23

Eigenschaften des vSphere Standard-Switches 24

Ändern der MTU-Größe für einen vSphere Standard-Switch 24

Ändern der Geschwindigkeit eines physischen Adapters 25

Hinzufügen und Gruppieren von physischen Adapters in einem vSphere Standard-Switch
25

Anzeigen des Topologie-Diagramms eines vSphere Standard-Switches 26

3 Einrichten von Netzwerken mit vSphere Distributed Switches 28

vSphere Distributed Switch-Architektur 28

Einen vSphere Distributed Switch erstellen 32

Upgrade eines vSphere Distributed Switch auf eine höhere Version 34

Bearbeiten allgemeiner und erweiterter vSphere Distributed Switch-Einstellungen 35

Verwalten von Netzwerken auf mehreren Hosts auf einem vSphere Distributed Switch 37

Aufgaben für das Verwalten von Host-Netzwerken auf einem vSphere Distributed Switch
38

Hosts zu einem vSphere Distributed Switch hinzufügen 39

Konfigurieren von physischen Netzwerkadapters auf einem vSphere Distributed Switch 41

Migrieren von VMkernel-Adapters zu einem vSphere Distributed Switch 42

Erstellen eines VMkernel-Adapters auf einem vSphere Distributed Switch 43

Migrieren von Netzwerken virtueller Maschinen zu einem vSphere Distributed Switch 46

Aktualisieren der maximalen Anzahl der verteilten Ports auf Hosts 47

Verwenden eines Hosts als Vorlage zur Erstellung einer einheitlichen Netzwerkkonfiguration
auf einem vSphere Distributed Switch 48

Entfernen von Hosts aus einem vSphere Distributed Switch	50
Verwalten von Netzwerken auf Host-Proxy-Switches	51
Migrieren von Netzwerkadaptern auf einem Host zu einem vSphere Distributed Switch	51
Migrieren eines VMkernel-Adapters auf einem Host zu einem vSphere Standard-Switch	52
Zuweisen einer physischen Netzwerkkarte eines Hosts zu einem vSphere Distributed Switch	53
Entfernen einer physischen Netzwerkkarte aus einem vSphere Distributed Switch	53
Festlegen der Anzahl der Ports auf einem Host-Proxy-Switch	54
Entfernen von NICs von den aktiven virtuellen Maschinen	55
Verteilte Portgruppen	55
Hinzufügen einer verteilten Portgruppe	55
Bearbeiten der allgemeinen Einstellungen von verteilten Portgruppen	61
Entfernen einer verteilten Portgruppe	62
Arbeiten mit verteilten Ports	62
Überwachen des Status von verteilten Ports	63
Konfigurieren der Einstellungen für verteilte Ports	63
Konfigurieren von Netzwerken von virtuellen Maschinen auf einem vSphere Distributed Switch	64
Migrieren von virtuellen Maschinen auf einen oder von einem vSphere Distributed Switch	64
Verbinden einer individuellen virtuellen Maschine mit einer verteilten Portgruppe	65
Topologie-Diagramme eines vSphere Distributed Switch im vSphere Web Client	65
Anzeigen der Topologie eines vSphere Distributed Switch	66
Anzeigen der Topologie eines Host-Proxy-Switch	68

4 Einrichten von VMkernel-Netzwerken 69

VMkernel-Netzwerkebene	70
Anzeigen von Informationen über VMkernel-Adapter auf einem Host	73
Erstellen eines VMkernel-Adapters auf einem vSphere Standard-Switch	73
Erstellen eines VMkernel-Adapters auf einem Host, der einem vSphere Distributed Switch zugeordnet ist	76
Bearbeiten einer VMkernel-Adapterkonfiguration	79
Anzeigen der TCP/IP-Stack-Konfiguration auf einem Host	81
Ändern der Konfiguration eines TCP/IP-Stack auf einem Host	82
Erstellen eines benutzerdefinierten TCP/IP-Stacks	83
Entfernen eines VMkernel-Adapters	83

5 LACP-Support auf einem vSphere Distributed Switch 85

Konvertieren zur erweiterten LACP-Unterstützung auf einem vSphere Distributed Switch	88
Konfiguration von LACP-Teaming und -Failover für verteilte Portgruppen	89
Konfigurieren einer Linkzusammenfassungsgruppe zur Regelung des Datenverkehrs für verteilte Portgruppen	90
Linkzusammenfassungsgruppe erstellen	91

Festlegen einer Linkzusammenfassungsgruppe als Standby in der Teaming- und Failover-Reihenfolge für verteilte Portgruppen	93
Zuweisen physischer Netzwerkkarten zu den Ports der Linkzusammenfassungsgruppe	93
Festlegen einer Linkzusammenfassungsgruppe als aktiv in der Teaming- und Failover-Reihenfolge für eine verteilte Portgruppe	94
Bearbeiten einer Linkzusammenfassungsgruppe	95
Aktivieren der LACP 5.1-Unterstützung für eine Uplink-Portgruppe	96
Einschränkungen der LACP-Unterstützung für einen vSphere Distributed Switch	97

6 Sichern und Wiederherstellen von Netzwerkkonfigurationen 99

Sichern und Wiederherstellen einer vSphere Distributed Switch-Konfiguration	99
Exportieren von vSphere Distributed Switch-Konfigurationen	99
Importieren einer vSphere Distributed Switch-Konfiguration	100
Wiederherstellen einer vSphere Distributed Switch-Konfiguration	101
Exportieren, Importieren und Wiederherstellen der Konfigurationen für verteilte vSphere-Portgruppen	102
Exportieren der Konfigurationen für verteilte vSphere-Portgruppen	102
Importieren einer Konfiguration für verteilte vSphere-Portgruppen	103
Wiederherstellen einer Konfiguration für verteilte vSphere-Portgruppen	104

7 Rollback und Wiederherstellung des Verwaltungsnetzwerks 106

vSphere-Netzwerk-Rollback	106
Deaktivieren des Netzwerk-Rollbacks	108
Deaktivieren des Netzwerk-Rollbacks unter Verwendung der vCenter Server-Konfigurationsdatei	108
Beheben von Fehlern bei der Konfiguration des Verwaltungsnetzwerks auf einem vSphere Distributed Switch	109

8 Netzwerkrichtlinien 111

Anwenden von Netzwerkrichtlinien auf einen vSphere Standard oder Distributed Switch	112
Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene	114
Teaming- und Failover-Richtlinie	115
Verfügbare Lastausgleichsalgorithmen für virtuelle Switches	117
Konfigurieren von NIC-Gruppierung, Failover und Lastausgleich auf einem vSphere Standard-Switch oder in einer Standardportgruppe	123
Konfigurieren von NIC-Teaming, Failover und Lastausgleich in einer verteilten Portgruppe oder einem verteilten Port	125
VLAN-Richtlinie	128
Konfigurieren von VLAN-Tagging in einer verteilten Portgruppe oder einem verteilten Port	128
Konfigurieren von VLAN-Tagging auf einer Uplink-Portgruppe oder einem Uplink-Port	129
Sicherheitsrichtlinie	130
Konfigurieren der Sicherheitsrichtlinie für einen vSphere Standard-Switch oder eine Standardportgruppe	131

Konfigurieren der Sicherheitsrichtlinie für eine verteilte Portgruppe oder einen verteilten Port	132
Traffic-Shaping-Richtlinie	134
Konfigurieren von Traffic-Shaping für einen vSphere Standard-Switch oder eine Standardportgruppe	135
Bearbeiten der Traffic-Shaping-Richtlinie für eine verteilte Portgruppe oder einen verteilten Port	136
Ressourcenzuteilungsrichtlinie	138
Bearbeiten der Ressourcenzuteilungsrichtlinie für eine verteilte Portgruppe	138
Bearbeiten der Ressourcenzuteilungsrichtlinie für verteilte Ports	139
Überwachungsrichtlinie	140
Aktivieren oder Deaktivieren der NetFlow-Überwachung auf einer verteilten Portgruppe oder einem verteilten Port	140
Richtlinien für das Filtern und Markieren des Datenverkehrs	141
Filtern und Markieren des Datenverkehrs in verteilten oder Uplink-Portgruppen	141
Filtern und Markieren des Datenverkehrs in verteilten oder Uplink-Ports	150
Qualifizieren des Datenverkehrs für die Filterung und Markierung	160
Verwalten von Richtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch	163
Portblockierungsrichtlinien	171
Bearbeiten der Portblockierungsrichtlinie für eine verteilte Portgruppe	171
Bearbeiten der Portblockierungsrichtlinie für verteilte oder Uplink-Portgruppen	172

9 Isolieren des Netzwerkverkehrs mithilfe von VLANs 173

VLAN-Konfiguration	173
Private VLANs	174
Erstellen eines privaten VLAN	174
Entfernen eines primären privaten VLAN	175
Entfernen eines sekundären privaten VLAN	176

10 Verwalten von Netzwerkressourcen 177

DirectPath I/O	177
Aktivieren des Passthroughs für ein Netzwerkgerät auf einem Host	178
Konfigurieren eines PCI-Geräts auf einer virtuellen Maschine	179
Aktivieren von DirectPath I/O mit vMotion auf einer virtuellen Maschine	180
Single Root I/O Virtualization (SR-IOV)	181
SR-IOV-Unterstützung	181
SR-IOV-Komponentenarchitektur und -Interaktion	184
Interaktion von vSphere und virtueller Funktion	186
DirectPath I/O im Vergleich zu SR-IOV	187
Konfigurieren einer virtuellen Maschine zur Verwendung von SR-IOV	187
Netzwerkoptionen für den Datenverkehr einer SR-IOV-fähigen virtuellen Maschine	191
Bewältigen des Datenverkehrs von virtuellen Maschinen mit einem SR-IOV-fähigen physischen Adapter	191

Aktivieren von SR-IOV mit Hostprofilen oder mit einem ESXCLI-Befehl	192
Eine virtuelle Maschine, die eine virtuelle SR-IOV-Funktion verwendet, kann nicht eingeschaltet werden, weil der Host den Status „Out of Interrupt Vectors“ aufweist	195
Jumbo-Frames	196
Aktivieren von Jumbo-Frames auf einem vSphere Distributed Switch	196
Aktivieren von Jumbo-Frames auf einem vSphere Standard-Switch	196
Aktivieren von Jumbo-Frames für einen VMkernel-Adapter	197
Aktivieren der Jumbo Frame-Unterstützung auf einer virtuellen Maschine	197
TCP-Segmentierungs-Offload	198
Aktivieren oder Deaktivieren von Software-TSO im VMkernel	199
Ermitteln, ob TSO auf den physischen Netzwerkadaptern eines ESXi-Hosts unterstützt wird	199
Aktivieren oder Deaktivieren von TSO auf einem ESXi-Host	200
Ermitteln, ob TSO auf einem ESXi-Host aktiviert ist	201
Aktivieren oder Deaktivieren von TSO auf einer Linux-VM	201
Aktivieren oder Deaktivieren von TSO auf einer Windows-VM	202
Large Receive Offload	203
Aktivieren von Hardware-LRO für alle VMXNET3-Adapter auf einem ESXi-Host	203
Aktivieren oder Deaktivieren von Software-LRO für alle VMXNET3-Adapter auf einem ESXi-Host	203
Ermitteln, ob LRO für VMXNET3-Adapter auf einem ESXi-Host aktiviert ist	204
Ändern der Größe des LRO-Puffers für VMXNET 3-Adapter	204
Aktivieren oder Deaktivieren von LRO für alle VMkernel-Adapter auf einem ESXi-Host	205
Ändern der Größe des LRO-Puffers für VMkernel-Adapter	205
Aktivieren oder Deaktivieren von LRO auf einem VMXNET3-Adapter auf einer Linux-VM	205
Aktivieren oder Deaktivieren von LRO auf einem VMXNET3-Adapter auf einer Windows-VM	206
Globales Aktivieren von LRO auf einer virtuellen Windows-Maschine	207
NetQueue und Netzwerkleistung	208
Aktivieren von NetQueue auf einem Host	208
Deaktivieren von NetQueue auf einem Host	208

11 vSphere Network I/O Control 210

Info zu vSphere Network I/O Control Version 3	211
Upgrade von Network I/O Control auf Version 3 auf einem vSphere Distributed Switch	212
Aktivieren von Network I/O Control auf einem vSphere Distributed Switch	215
Bandbreitenzuteilung für Systemdatenverkehr	215
Bandbreitenzuteilungsparameter für Systemdatenverkehr	216
Beispiel-Bandbreitenreservierung für Systemdatenverkehr	218
Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr	218
Bandbreitenzuteilung für Datenverkehr über virtuelle Maschinen	220
Info zur Zuteilung von Bandbreite zu virtuellen Maschinen	220

Bandbreitenzuteilungsparameter für Datenverkehr virtueller Maschinen	222
Zugangssteuerung für Bandbreite virtueller Maschinen	223
Erstellen eines Netzwerkressourcenpools	224
Hinzufügen einer verteilten Portgruppe zu einem Netzwerkressourcenpool	226
Konfigurieren der Bandbreitenzuteilung für eine virtuelle Maschine	226
Konfigurieren der Bandbreitenzuteilung auf mehreren virtuellen Maschinen	228
Ändern des Kontingents eines Netzwerkressourcenpools	229
Entfernen von verteilten Portgruppen aus einem Netzwerkressourcenpool	230
Löschen eines Netzwerkressourcenpools	230
Verschieben eines physischen Adapters aus dem Bereich von Network I/O Control	231
Arbeiten mit Network I/O Control Version 2	231
Erstellen eines Netzwerkressourcenpools in Network I/O Control, Version 2	233
Bearbeiten der Einstellungen eines Netzwerkressourcenpools in Network I/O Control, Version 2	234

12 Verwaltung von MAC-Adressen 236

Zuweisen von MAC-Adressen in vCenter Server	236
VMware-OUI-Zuteilung	237
Zuteilen von präfixbasierten MAC-Adressen	238
Zuteilen von bereichsbasierten MAC-Adressen	238
Zuweisen von MAC-Adressen	238
Generierung von MAC-Adressen auf ESXi-Hosts	241
Festlegen einer statischen MAC-Adresse für eine virtuelle Maschine	242
VMware-OUI in statischen MAC-Adressen	243
Zuweisen einer statischen MAC-Adresse über den vSphere Web Client	243
Zuweisen von statischen MAC-Adressen in der Konfigurationsdatei der virtuellen Maschine	244

13 Konfigurieren von vSphere für IPv6 245

vSphere IPv6-Konnektivität	245
Bereitstellen von vSphere auf IPv6	247
Aktivieren von IPv6 in einer vSphere-Installation	248
Aktivieren von IPv6 in einer vSphere-Umgebung mit Upgrade	249
Aktivieren oder Deaktivieren der IPv6-Unterstützung auf einem Host	251
Einrichten von IPv6 auf einem ESXi-Host	251
Einrichten von IPv6 auf vCenter Server	252
Einrichten von IPv6 auf der vCenter Server Appliance	252
Einrichten von vCenter Server unter Windows mit IPv6	253

14 Überwachen der Netzwerkverbindung und des Netzwerkdatenverkehrs 254

Erfassen und Nachverfolgen von Netzwerkpaketen unter Verwendung des Dienstprogramms pktcap-uw	254
-----------------------------------------------------------------------------------------------	-----

Befehlssyntax von pktcap-uw zum Erfassen von Paketen	255
Befehlssyntax von pktcap-uw zum Nachverfolgen von Paketen	258
Optionen von pktcap-uw zum Kontrollieren der Ausgabe	259
Optionen von pktcap-uw zum Filtern von Paketen	260
Erfassen von Paketen mithilfe des Dienstprogramms pktcap-uw	261
Nachverfolgen von Paketen mithilfe des Dienstprogramms pktcap-uw	273
Konfigurieren der NetFlow-Einstellungen eines vSphere Distributed Switch	275
Arbeiten mit der Portspiegelung	276
Portspiegelung - Versionskompatibilität	276
Portspiegelung - Interoperabilität	277
Erstellen einer Portspiegelungssitzung	280
Anzeigen von Details zu einer Portspiegelungssitzung	283
Bearbeiten der Details, Quellen und Ziele von Portspiegelungssitzungen	284
Überprüfung des Systemzustands des vSphere Distributed Switch	286
Aktivieren oder Deaktivieren der Überprüfung des Systemzustands des vSphere Distributed Switch	286
Anzeigen des Systemstatus von vSphere Distributed Switch	287
Switch-Discovery-Protokoll	288
Aktivieren des Cisco Discovery-Protokolls auf einem vSphere Distributed Switch	288
Aktivieren des Link Layer Discovery Protocol (LLDP) auf einem vSphere Distributed Switch	289
Anzeigen von Switch-Informationen	290
15 Konfigurieren von Protokollprofilen für Netzwerke virtueller Maschinen	291
Hinzufügen eines Netzwerkprotokollprofils	292
Benennen des Netzwerkprotokollprofils und Auswählen des Netzwerks	292
Festlegen der IPv4-Konfiguration des Netzwerkprotokollprofils	293
Festlegen der IPv6-Konfiguration für das Netzwerkprotokollprofil	293
Festlegen des DNS und weiterer Konfigurationseinstellungen für das Netzwerkprotokollprofil	294
Abschließen der Erstellung des Netzwerkprotokollprofils	294
Zuordnen einer Portgruppe zu einem Netzwerkprotokollprofil	295
Konfigurieren einer virtuellen Maschine oder von vApp zur Verwendung eines Netzwerkprotokollprofils	295
16 Multicast-Filter	297
Multicast-Filtermodi	297
Multicast-Snooping auf einem vSphere Distributed Switch aktivieren	299
Bearbeiten des Abfragezeitintervalls für Multicast-Snooping	299
Bearbeiten der Anzahl von IP-Adressen der Quelle für IGMP und MLD	300
17 Statusfreie Netzwerkbereitstellung	301

18 Optimale Vorgehensweisen für Netzwerke 304

Grundlegende Informationen zu vSphere-Netzwerken

vSphere-Netzwerk bietet Informationen zum Konfigurieren von Netzwerken für VMware HL0707vSphere®, beispielsweise zum Erstellen von vSphere Distributed Switches und vSphere Standard-Switches.

vSphere-Netzwerk bietet darüber hinaus Informationen zum Überwachen von Netzwerken, zum Verwalten von Netzwerkressourcen und zu optimalen Vorgehensweisen für Netzwerke.

Zielgruppe

Die bereitgestellten Informationen sind für erfahrene Windows- oder Linux-Systemadministratoren bestimmt, die mit der Netzwerkkonfiguration und der VM-Technologie vertraut sind.

Aktualisierte Informationen

Dieses Handbuch *vSphere-Netzwerk* wird mit jeder Version des Produkts oder bei Bedarf aktualisiert.

Diese Tabelle enthält den Update-Verlauf für das Handbuch *vSphere-Netzwerk*.

Revision	Beschreibung
31. MAR 2021	Verschiedene Updates.
13. APR 2020	Die Beschreibung der Überprüfung des Systemzustands des vSphere Distributed Switch wurde erweitert und beinhaltet den Hinweis, dass Sie die Überprüfung des Systemzustands zur Fehlerbehebung bei Netzwerkproblemen durchführen und diese dann deaktivieren sollten, nachdem Sie das Problem identifiziert und behoben haben. Weitere Informationen finden Sie unter Überprüfung des Systemzustands des vSphere Distributed Switch und Aktivieren oder Deaktivieren der Überprüfung des Systemzustands des vSphere Distributed Switch .
13. APR 2020	Die Muster für das Filtern oder Markieren des Netzwerkdatenverkehrs mithilfe einer MAC-Adresse wurden aktualisiert, um die Verwendung eines regulären Platzhalterausdrucks zu entfernen. Eine MAC-Adresse wird als abgeglichen betrachtet, wenn der UND-Vorgang der Maske auf der Mac-Adresse dasselbe Ergebnis erzielt. Siehe MAC-Bezeichner für Datenverkehr
12. FEB 2018	Die Informationen im Abschnitt Aktivieren von IPv6 in einer vSphere-Umgebung mit Upgrade wurden aktualisiert.
DE-002007-02	<ul style="list-style-type: none">■ Die Konsolenbefehle in Aktivieren oder Deaktivieren von Software-TSO im VMkernel wurden aktualisiert.■ Die Informationen zum Bereitstellungsdatenverkehr wurden aktualisiert, um darauf hinzuweisen, dass er für die Snapshot-Migration verwendet wird. Siehe VMkernel-Netzwerkebene, Bearbeiten einer VMkernel-Adapterkonfiguration und Erstellen eines VMkernel-Adapters auf einem vSphere Standard-Switch.■ Die Informationen zu Auto Deploy in IPv6-Konnektivität von vSphere-Funktionen wurden aktualisiert.
DE-002007 -01	<ul style="list-style-type: none">■ Die Informationen im Abschnitt Überprüfung des Systemzustands des vSphere Distributed Switch wurden mit einem Hinweis aktualisiert, dass die Überprüfung des Systemzustands des vSphere Distributed Switch möglicherweise zusätzlichen Netzwerkverkehr generiert.■ Die Informationen im Abschnitt Verwenden eines Hosts als Vorlage zur Erstellung einer einheitlichen Netzwerkkonfiguration auf einem vSphere Distributed Switch wurden aktualisiert.
DE-002007-00	Erstversion.

Einführung in Netzwerke

1

Erläutert die grundlegenden Konzepte von ESXi-Netzwerken sowie die Einrichtung und Konfiguration von Netzwerken in einer vSphere-Umgebung.

Dieses Kapitel enthält die folgenden Themen:

- [Übersicht über Netzwerkkonzepte](#)
- [Netzwerkdienste in ESXi](#)
- [VMware ESXi Dump Collector-Unterstützung](#)

Übersicht über Netzwerkkonzepte

Es sind bestimmte Grundlagen notwendig, um virtuelle Netzwerke vollständig zu verstehen. Wenn Sie bisher noch nicht mit ESXi gearbeitet haben, sollten Sie sich diese Konzepte ansehen.

Physisches Netzwerk

Ein Netzwerk aus physischen Computern, die so miteinander verbunden sind, dass sie untereinander Daten empfangen und versenden können. VMware ESXi wird auf einem physischen Computer ausgeführt.

Virtuelles Netzwerk

Ein Netzwerk aus virtuellen Computern (virtuellen Maschinen), die auf einem physischen Computer ausgeführt werden. Diese sind logisch miteinander verbunden, sodass sie untereinander Daten empfangen und versenden können. Virtuelle Maschinen können an die virtuellen Netzwerke angeschlossen werden, die Sie beim Hinzufügen eines Netzwerks erstellen.

Physischer Ethernet-Switch

Ein physischer Ethernet-Switch verwaltet den Netzwerkdatenverkehr zwischen den Computern im physischen Netzwerk. Ein Switch verfügt über mehrere Ports. Jeder dieser Ports kann an einen einzigen Computer oder einen anderen Switch im Netzwerk angeschlossen sein. Jeder Port kann je nach Bedarf des angeschlossenen Computers so konfiguriert werden, dass er sich auf eine bestimmte Art verhält. Der Switch stellt fest, welche Hosts an welche seiner Ports angeschlossen sind, und verwendet diese Informationen, um Daten an den entsprechenden richtigen physischen Computer weiterzuleiten. Switches bilden

den Kern eines physischen Netzwerks. Es können mehrere Switches zusammengeschlossen werden, um größere Netzwerke zu bilden.

vSphere Standard-Switch

Ein vSphere Standard-Switch funktioniert ähnlich wie ein physischer Ethernet-Switch. Er weiß, welche virtuellen Maschinen logisch an welche virtuellen Ports angeschlossen sind, und verwendet diese Informationen, um Daten an die entsprechende richtige virtuelle Maschine weiterzuleiten. Ein vSphere Standard-Switch kann über physische Ethernet-Adapter (auch Uplink-Adapter) an physische Switches angeschlossen werden, um virtuelle und physische Netzwerke zu verbinden. Diese Verbindung ähnelt der Vernetzung physischer Switches zur Bildung größerer Netzwerke. Obwohl ein vSphere Standard-Switch ähnlich wie ein physischer Switch funktioniert, verfügt er nicht über alle erweiterten Funktionsmerkmale eines physischen Switches.

Standard-Portgruppe

Eine Standard-Portgruppe legt Port-Konfigurationsoptionen, z. B. Bandbreitenbeschränkungen oder VLAN-Tagging-Richtlinien, für jeden Port in der Portgruppe fest. Netzwerkdienste werden über Portgruppen an Standard-Switches angeschlossen. Portgruppen definieren, wie eine Verbindung über den Switch an das physische Netzwerk erfolgt. Standardmäßig wird ein einzelner Standard-Switch mindestens einer Portgruppe zugeordnet.

vSphere Distributed Switch

Ein vSphere Distributed Switch agiert als einzelner Switch über alle verbundenen Hosts in einem Datacenter hinweg, um die zentrale Bereitstellung, Verwaltung und Überwachung von virtuellen Netzwerken zu ermöglichen. Sie konfigurieren einen vSphere Distributed Switch im vCenter Server-System, und die Konfiguration wird an alle Hosts weitergegeben, die dem Switch zugeordnet sind. Dies ermöglicht virtuellen Maschinen bei der Migration zwischen mehreren Hosts die Beibehaltung einer konsistenten Netzwerkkonfiguration.

Host-Proxy-Switch

Ein versteckter Standard-Switch, der sich auf jedem Host befindet, dem ein vSphere Distributed Switch zugeordnet ist. Der Host-Proxy-Switch repliziert die Netzwerkkonfiguration des vSphere Distributed Switch auf den entsprechenden Host.

Verteilter Port

Ein Port auf einem vSphere Distributed Switch, der eine Verbindung zum VMkernel eines Hosts oder zum Netzwerkadapter einer virtuellen Maschine herstellt.

Verteilte Portgruppe

Eine Portgruppe, die einem vSphere Distributed Switch zugeordnet ist und Port-Konfigurationsoptionen für jeden Port der Portgruppe angibt. Verteilte Portgruppen definieren, wie anhand des vSphere Distributed Switch eine Verbindung zum Netzwerk vorgenommen wird.

NIC-Gruppierung

NIC-Gruppierung tritt auf, wenn einem Switch mehrere Uplink-Adapter zugewiesen werden, um eine Gruppe zu bilden. Eine Gruppe kann entweder den Datenverkehr zwischen dem physischen und dem virtuellen Netzwerk auf einige oder alle Netzwerkkarten der Gruppe aufteilen oder ein passives Failover im Falle einer Hardwarestörung oder eines Netzwerkausfalls bereitstellen.

VLAN

Mit einem VLAN kann ein einzelnes physisches LAN-Segment weiter aufgeteilt werden, sodass Portgruppen derart voneinander isoliert werden, als befänden sie sich in unterschiedlichen physischen Segmenten. Der Standard ist 802.1Q.

VMkernel-TCP/IP-Netzwerkschicht

Die VMkernel-Netzwerkschicht bietet Verbindung zu Hosts und verarbeitet den Standard-Infrastrukturdatenverkehr von vSphere vMotion, IP-Speicher, Fault Tolerance und dem Virtual SAN.

IP-Speicher

Jedwede Art von Speicher, der auf TCP/IP-Netzwerkkommunikation beruht. iSCSI kann als Datenspeicher für virtuelle Maschinen verwendet werden. NFS kann als Datenspeicher für virtuelle Maschinen oder für die direkte Einbindung von .ISO-Dateien, die dann von der virtuellen Maschine als CD-ROMs erkannt werden, verwendet werden.

TCP-Segmentierungs-Offload

TCP Segmentation Offload, TSO, ermöglicht einem TCP/IP-Stapel das Senden großer Datenblöcke (bis zu 64 KB), obgleich die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) der Schnittstelle kleiner ist. Der Netzwerkadapter trennt anschließend den großen Datenblock in Datenblöcke mit MTU-Größe und stellt eine angepasste Kopie der einleitenden TCP/IP-Header voran.

Netzwerkdienste in ESXi

Ein virtuelles Netzwerk stellt für den Host und die virtuellen Maschinen mehrere Dienste zur Verfügung.

Sie können zwei Typen von Netzwerkdiensten in ESXi aktivieren:

- Die Verbindung von virtuellen Maschinen zum physischen Netzwerk sowie die Verbindung untereinander.
- VMkernel-Dienste (zum Beispiel NFS, iSCSI oder vMotion) mit dem physischen Netzwerk verbinden.

VMware ESXi Dump Collector-Unterstützung

Der ESXi Dump Collector sendet den Status des VMkernel-Arbeitsspeichers, das heißt einen Core-Dump, zu einem Netzwerkserver, wenn ein kritischer Systemausfall auftritt.

Der ESXi Dump Collector in ESXi 5.1 und höher unterstützt vSphere Standard- und Distributed Switches. Der ESXi Dump Collector kann auch jeden aktiven Uplink-Adapter aus dem Team der Portgruppe verwenden, die der Verarbeitung des VMkernel-Adapters für den Collector dient.

Änderungen an der IP-Adresse für die ESXi Dump Collector-Schnittstelle werden automatisch aktualisiert, wenn sich die IP-Adressen für den konfigurierten VMkernel-Adapter ändern. Der ESXi Dump Collector passt auch das Standard-Gateway an, wenn sich die Gateway-Konfiguration des VMkernel-Adapters ändert.

Wenn Sie versuchen, den VMkernel-Netzwerkadapter zu löschen, der vom ESXi Dump Collector verwendet wird, schlägt der Vorgang fehl und eine Warnung wird angezeigt. Um den VMkernel-Netzwerkadapter zu löschen, deaktivieren Sie die Dump-Erfassung und löschen Sie den Adapter.

Es gibt keine Authentifizierung bzw. Verschlüsselung in der Dateiübertragungssitzung von einem abgestürzten Host zum ESXi Dump Collector. Es wird empfohlen, dass Sie den ESXi Dump Collector möglichst auf einem separaten VLAN konfigurieren, um den ESXi-Core Dump vom regulären Netzwerkdatenverkehr zu isolieren.

Weitere Informationen zur Installation und Konfiguration von ESXi Dump Collector finden Sie in der *Installations- und Einrichtungshandbuch für vSphere*-Dokumentation.

Einrichten von Netzwerken mit vSphere Standard-Switches

2

vSphere Standard-Switches steuern den Datenverkehr auf dem Netzwerk auf Hostebene in einer vSphere-Bereitstellung.

Dieses Kapitel enthält die folgenden Themen:

- [vSphere Standard-Switches](#)
- [vSphere Standard-Switch erstellen](#)
- [Konfiguration von Portgruppen für virtuelle Maschinen](#)
- [Eigenschaften des vSphere Standard-Switches](#)

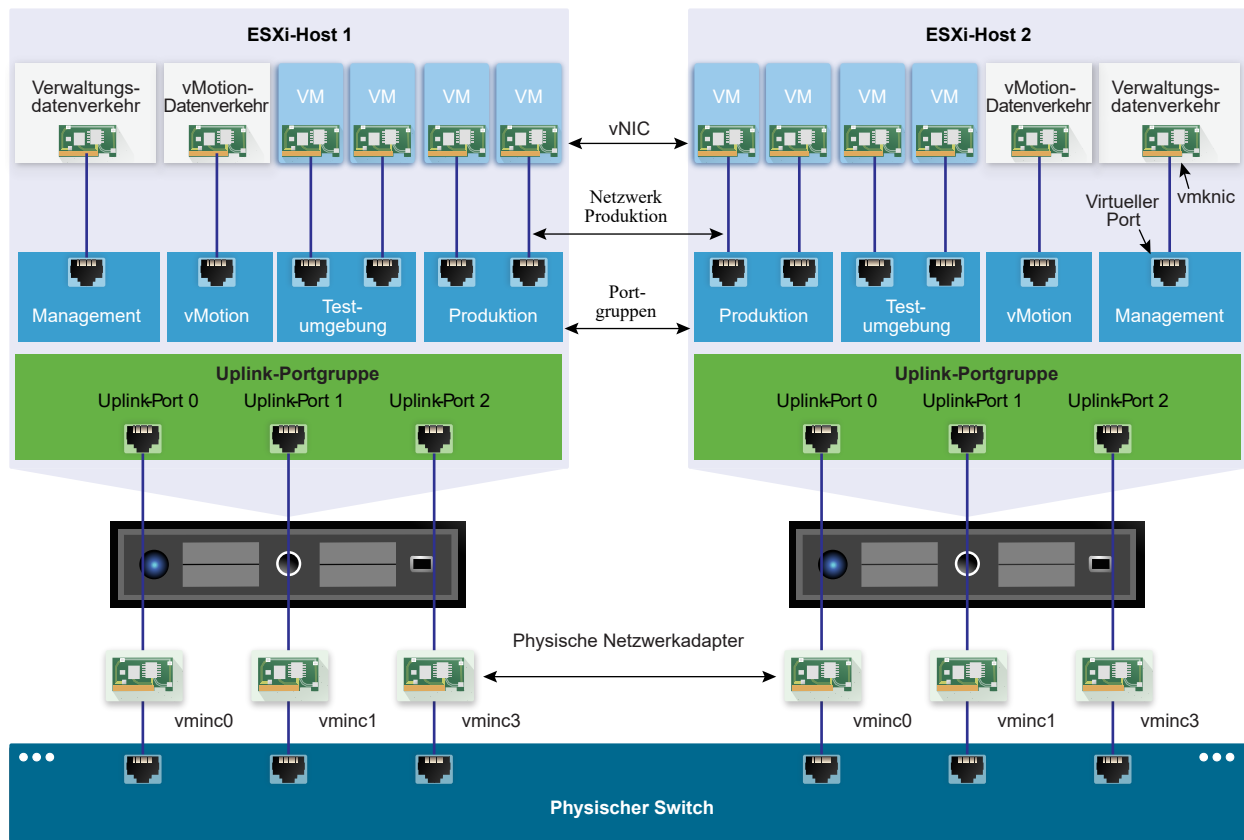
vSphere Standard-Switches

Sie können abstrakte Netzwerkgeräte erstellen, die als vSphere Standard-Switches bezeichnet werden. Mithilfe von Standard-Switches können Sie Hosts und virtuellen Maschinen Netzwerkkonnektivität bereitstellen. Ein Standard-Switch kann den Datenverkehr intern über virtuelle Maschinen im selben VLAN hinweg ermöglichen und eine Verbindung zu externen Netzwerken herstellen.

Standard-Switch – Überblick

Um Hosts und virtuellen Maschinen Netzwerkkonnektivität bereitzustellen, verbinden Sie die physischen Netzwerkkarten der Hosts mit Uplink-Ports am Standard-Switch. Virtuelle Maschinen verfügen über Netzwerkadapter (vNICs), die an Portgruppen am Standard-Switch angeschlossen werden. Jede Portgruppe kann eine oder mehrere physische Netzwerkkarten verwenden, um den Netzwerkdatenverkehr der Portgruppe zu verarbeiten. Wenn an eine Portgruppe keine physische Netzwerkkarte angeschlossen ist, können die virtuellen Maschinen dieser Portgruppe nur miteinander kommunizieren, nicht aber mit dem externen Netzwerk.

Abbildung 2-1. vSphere-Standard-Switch-Architektur



Ein vSphere Standard-Switch ist einem physischen Ethernet-Switch sehr ähnlich. Netzwerkadapter von virtuellen Maschinen und physische Netzwerkkarten auf dem Host nutzen die logischen Ports auf dem Switch, da jeder Adapter einen Port nutzt. Jeder logische Port auf dem Standard-Switch gehört zu einer einzelnen Portgruppe. Informationen zur maximal zulässigen Anzahl an Ports und Portgruppen finden Sie unter *Maximalwerte für die Konfiguration*.

Standard-Portgruppen

Jede Portgruppe an einem Standard-Switch wird durch eine Netzwerkbezeichnung gekennzeichnet, die im aktuellen Host eindeutig sein muss. Mithilfe von Netzwerkbezeichnungen können Sie dafür sorgen, dass die Netzwerkkonfiguration der virtuellen Maschinen zwischen den Hosts portierbar ist. Wenn Portgruppen in einem Datacenter physische Netzwerkkarten verwenden, die mit einer Broadcast-Domäne im physischen Netzwerk verbunden sind, weisen Sie diesen Portgruppen dieselbe Bezeichnung zu. Wenn dagegen zwei Portgruppen mit physischen Netzwerkkarten in verschiedenen Broadcast-Domänen verbunden sind, weisen Sie den Portgruppen unterschiedliche Bezeichnungen zu.

Beispielsweise können Sie Portgruppen für *Produktions*- und *Testumgebungen* als Netzwerke mit virtuellen Maschinen auf Hosts erstellen, die dieselbe Broadcast-Domäne auf dem physischen Netzwerk verwenden.

Eine VLAN-ID, die den Datenverkehr der Portgruppe auf ein logisches Ethernet-Segment im physischen Netzwerk einschränkt, kann optional zugewiesen werden. Damit Portgruppen den Datenverkehr erhalten, der auf demselben Host angezeigt wird, aber von mehr als einem VLAN, muss die VLAN-ID auf VGT (VLAN 4095) eingestellt sein.

Anzahl der Standardports

Für eine effiziente Nutzung der Hostressourcen wird auf ESXi 5.5 und höher die Anzahl der Ports von Standard-Switches dynamisch nach oben und unten korrigiert. Ein Standard-Switch auf einem solchen Host kann auf die maximale Anzahl von Ports, die auf dem Host unterstützt wird, erweitert werden.

vSphere Standard-Switch erstellen

Erstellen Sie einen vSphere Standard-Switch, um für Hosts und virtuelle Maschinen Netzwerkkonnektivität bereitzustellen und den VMkernel-Datenverkehr zu verwalten. Je nach dem Verbindungstyp, den Sie erstellen möchten, können Sie einen neuen vSphere Standard-Switch mit einem VMkernel-Adapter erstellen, nur physische Netzwerkadapter mit dem neuen Switch verbinden oder den Switch mit einer Portgruppe der virtuellen Maschine erstellen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Wählen Sie unter **Verwalten** die Option **Netzwerk** und dann **Virtuelle Switches** aus.
- 3 Klicken Sie auf **Hostnetzwerk hinzufügen**.
- 4 Wählen Sie den Verbindungstyp aus, für den Sie den neuen Standard-Switch verwenden möchten, und klicken Sie auf **Weiter**.

Option	Beschreibung
VMkernel-Netzwerkadapter	Erstellen Sie einen neuen VMkernel-Adapter für den Hostverwaltungsdatenverkehr, vMotion, den Netzwerkspeicher, Fault Tolerance oder den Datenverkehr des Virtual SAN.
Physischer Netzwerkadapter	Fügen Sie einem vorhandenen oder einem neuen Standard-Switch physische Netzwerkadapter hinzu.
Portgruppe der virtuellen Maschine für einen Standard-Switch	Erstellen Sie eine neue Portgruppe für das Netzwerk virtueller Maschinen.

- 5 Wählen Sie **Neuer Standard-Switch** und klicken Sie auf **Weiter**.
- 6 Fügen Sie dem neuen Standard-Switch physische Netzwerkadapter hinzu.
 - a Klicken Sie unter „Zugewiesene Adapter“ auf **Adapter hinzufügen**.
 - b Wählen Sie einen oder mehrere physische Netzwerkadapter aus der Liste aus.

- c Wählen Sie im Dropdown-Menü **Gruppe für Failover-Reihenfolge** aus den Failover-Listen „Aktiv“ oder „Standby“ aus.

Konfigurieren Sie für einen höheren Durchsatz und zum Bereitstellen von Redundanz mindestens zwei physische Netzwerkadapter in der Liste „Aktiv“.

- d Klicken Sie auf **OK**.

- 7 Wenn Sie den neuen Standard-Switch mit einem VMkernel-Adapter oder einer Portgruppe der virtuellen Maschine erstellen, geben Sie Verbindungseinstellungen für den Adapter oder die Portgruppe ein.

Option	Beschreibung
VMkernel-Adapter	<ul style="list-style-type: none"> a Geben Sie eine Bezeichnung ein, die die Art des Datenverkehrs für den VMkernel-Adapter kennzeichnet, zum Beispiel vMotion. b Legen Sie eine VLAN-ID zum Identifizieren des VLANs fest, das vom Netzwerkdatenverkehr des VMkernel-Adapters verwendet wird. c Wählen Sie IPv4, IPv6 oder beide aus. d Wählen Sie einen TCP/IP-Stack aus. Der TCP/IP-Stack, den Sie für den VMkernel-Adapter festlegen, kann später nicht mehr geändert werden. Wenn Sie den vMotion- oder den Bereitstellungs-TCP/IP-Stack auswählen, können Sie nur diesen Stack für vMotion- oder Bereitstellungsdatenverkehr auf dem Host verwenden. e Wenn Sie den Standard-TCP/IP-Stack verwenden, wählen Sie aus den verfügbaren Diensten aus. f Konfigurieren Sie IPv4- und IPv6-Einstellungen.
Portgruppe der virtuellen Maschine	<ul style="list-style-type: none"> a Geben Sie eine Netzwerkbezeichnung für die Portgruppe ein oder akzeptieren Sie die generierte Bezeichnung. b Legen Sie die VLAN-ID fest, um die VLAN-Handhabung in der Portgruppe zu konfigurieren.

- 8 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **OK**.

Nächste Schritte

- Sie müssen möglicherweise die Teaming- und Failover-Richtlinie des neuen Standard-Switches ändern. Beispiel: Wenn der Host mit einem Etherchannel auf dem physischen Switch verbunden ist, müssen Sie den vSphere Standard-Switch mit „Anhand des IP-Hashs routen“ als Lastausgleichsalgorithmus konfigurieren. Weitere Informationen hierzu finden Sie unter [Teaming- und Failover-Richtlinie](#).
- Wenn Sie den neuen Standard-Switch mit einer Portgruppe für ein Netzwerk virtueller Maschinen erstellen, verbinden Sie virtuelle Maschinen mit der Portgruppe.

Konfiguration von Portgruppen für virtuelle Maschinen

Sie können eine Portgruppe einer virtuellen Maschine hinzufügen oder ändern, um die Datenverkehrsverwaltung für eine Gruppe virtueller Maschinen einzurichten.

Der Assistent **Netzwerk hinzufügen** im vSphere Web Client führt Sie durch das Erstellen eines virtuellen Netzwerks, mit dem virtuelle Maschinen eine Verbindung herstellen können, einschließlich des Erstellens eines vSphere Standard-Switches und des Konfigurierens von Einstellungen für eine Netzwerkbezeichnung.

Bedenken Sie beim Einrichten von Netzwerken mit virtuellen Maschinen, ob Sie die virtuellen Maschinen des Netzwerks zwischen Hosts migrieren möchten. Falls ja, stellen Sie sicher, dass sich beide Hosts in derselben Broadcast-Domäne befinden, also im selben Schicht 2-Subnetz.

ESXi unterstützt die Migration virtueller Maschinen zwischen Hosts unterschiedlicher Broadcast-Domänen nicht, weil die migrierte virtuelle Maschine möglicherweise Systeme und Ressourcen benötigt, auf die sie im neuen Netzwerk keinen Zugriff mehr hätte. Selbst wenn Ihre Netzwerkkonfiguration als Hochverfügbarkeitsumgebung eingerichtet ist oder intelligente Switches enthält, die in der Lage sind, dem Bedarf einer virtuellen Maschine auch in verschiedenen Netzwerken zu entsprechen, könnte es sein, dass es in der ARP-Tabelle (Address Resolution Protocol) zu Verzögerungen bei der Aktualisierung und der Wiederaufnahme des Netzwerkverkehrs der virtuellen Maschine kommt.

Virtuelle Maschinen greifen über Uplink-Adapter auf physische Netzwerke zu. Ein vSphere Standard-Switch kann nur dann Daten an externe Netzwerke übertragen, wenn mindestens ein Netzwerkadapter an den vSwitch angeschlossen ist. Wenn zwei oder mehr Adapter an einen einzelnen Standard-Switch angeschlossen sind, werden sie transparent gruppiert.

Hinzufügen einer Portgruppe für virtuelle Maschinen

Erstellen Sie Portgruppen für einen vSphere Standard-Switch, um die Konnektivität und die allgemeine Netzwerkkonfiguration für virtuelle Maschinen bereitzustellen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Netzwerk hinzufügen** aus.
- 3 Wählen Sie unter **Verbindungstyp auswählen** die Option **Portgruppe der virtuellen Maschine für einen Standard-Switch** aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie unter **Zielgerät auswählen** einen vorhandenen Standard-Switch aus oder erstellen Sie einen neuen Standard-Switch.
- 5 Falls die neue Portgruppe für einen vorhandenen Standard-Switch dient, navigieren Sie zu dem Switch.
 - a Klicken Sie auf **Durchsuchen**.
 - b Wählen Sie einen Standard-Switch aus der Liste aus und klicken Sie auf **OK**.
 - c Klicken Sie auf **Weiter** und gehen Sie zu [Schritt 8](#).
- 6 (Optional) Weisen Sie auf der Seite „Standard-Switch erstellen“ dem Standard-Switch physische Netzwerkadapter zu.

Sie können einen Standard-Switch mit oder ohne Adapter erstellen.

Wenn Sie einen Standard-Switch ohne physische Netzwerkadapter erstellen, ist der gesamte Datenverkehr auf diesem Switch auf diesen Switch beschränkt. Andere Hosts im physischen Netzwerk oder virtuelle Maschinen auf anderen Standard-Switches können dann keine Daten über diesen Standard-Switch senden oder empfangen. Sie können einen Standard-Switch ohne physische Netzwerkadapter erstellen, wenn eine Gruppe virtueller Maschinen untereinander, nicht jedoch mit anderen Hosts oder virtuellen Maschinen außerhalb der Gruppe kommunizieren soll.

- a Klicken Sie auf **Adapter hinzufügen**.
 - b Wählen Sie in der Liste **Netzwerkadapter** einen Adapter aus.
 - c Verwenden Sie das Dropdown-Menü **Gruppe für Failover-Reihenfolge**, um den Adapter „Aktive Adapter“, „Standby-Adapter“ oder „Nicht verwendete Adapter“ zuzuweisen, und klicken Sie auf **OK**.
 - d (Optional) Ändern Sie bei Bedarf mithilfe der Pfeiltasten in der Liste **Zugewiesene Adapter** die Position des Adapters.
 - e Klicken Sie auf **Weiter**.
- 7** Identifizieren Sie auf der Seite „Verbindungseinstellungen“ Datenverkehr über die Ports der Gruppe.
- a Geben Sie eine **Netzwerkbezeichnung** für die Portgruppe ein oder akzeptieren Sie die generierte Bezeichnung.
 - b Legen Sie die **VLAN-ID** fest, um die VLAN-Handhabung in der Portgruppe zu konfigurieren.

Die VLAN-ID spiegelt auch den VLAN-Tagging-Modus in der Portgruppe wider.

VLAN-Tagging-Modus	VLAN-ID	Beschreibung
External Switch Tagging (EST)	0	Der virtuelle Switch übermittelt keinen Datenverkehr im Zusammenhang mit einem VLAN.
Virtual Switch Tagging (VST)	Zwischen 1 und 4094	Datenverkehr wird vom virtuellen Switch mit dem eingegebenen Tag gekennzeichnet.
Virtual Guest Tagging (VGT)	4095	VLANs werden von virtuellen Maschinen abgewickelt. Der virtuelle Switch übermittelt Datenverkehr über jedes VLAN.

- c Klicken Sie auf **Weiter**.
- 8** Überprüfen Sie die Einstellungen der Portgruppe auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Beenden**.

Klicken Sie auf **Zurück**, wenn Sie Einstellungen ändern möchten.

Bearbeiten einer Portgruppe für den Standard-Switch

Mit dem vSphere Web Client können Sie den Namen und die VLAN-ID einer Portgruppe für den Standard-Switch bearbeiten sowie Netzwerkrichtlinien auf Portgruppenebene überschreiben.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie einen Standard-Switch aus der Liste aus.
Das Topologie-Diagramm für den Switch wird angezeigt.
- 4 Klicken Sie im Topologie-Diagramm für den Switch auf den Namen der Portgruppe.
- 5 Klicken Sie unter dem Titel des Topologie-Diagramms auf **Bearbeiten**.
- 6 Benennen Sie im Abschnitt **Eigenschaften** die Portgruppe im Textfeld **Netzwerkbezeichnung** um.
- 7 Konfigurieren Sie das VLAN-Tagging im Dropdown-Menü **VLAN-ID**.

VLAN-Tagging-Modus	VLAN-ID	Beschreibung
External Switch Tagging (EST)	0	Der virtuelle Switch übermittelt keinen Datenverkehr im Zusammenhang mit einem VLAN.
Virtual Switch Tagging (VST)	Zwischen 1 und 4094	Datenverkehr wird vom virtuellen Switch mit dem eingegebenen Tag gekennzeichnet.
Virtual Guest Tagging (VGT)	4095	VLANs werden von virtuellen Maschinen abgewickelt. Der virtuelle Switch übermittelt Datenverkehr über jedes VLAN.

- 8 Überschreiben Sie im Abschnitt **Sicherheit** die Switch-Einstellungen, um Schutz vor der Imitation von MAC-Adressen und vor der Ausführung von virtuellen Maschinen im Promiscuous-Modus zu bieten.
- 9 Überschreiben Sie im Abschnitt **Traffic-Shaping** auf der Portgruppenebene die Größe für die Durchschnitts- und Spitzenbandbreite und für Bursts.
- 10 Überschreiben Sie im Abschnitt **Teaming und Failover** die Einstellungen für Teaming und Failover, die vom Standard-Switch übernommen wurden.

Sie können die Verteilung und das erneute Routing des Datenverkehrs zwischen den physischen Adaptern für die Portgruppe konfigurieren. Darüber hinaus können Sie die Reihenfolge ändern, in der physische Hostadapter bei einem Fehler verwendet werden.
- 11 Klicken Sie auf **OK**.

Entfernen einer Portgruppe aus einem vSphere Standard-Switch

Sie können Portgruppen aus vSphere Standard-Switches entfernen, wenn Sie die zugeordneten bezeichneten Netzwerke nicht mehr benötigen.

Voraussetzungen

Stellen Sie sicher, dass keine eingeschalteten virtuellen Maschinen mit der Portgruppe verbunden sind, die Sie entfernen möchten.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie den Standard-Switch aus.
- 4 Wählen Sie aus dem Topologie-Diagramm des Switches die Portgruppe aus, die Sie entfernen möchten, indem Sie auf ihre Bezeichnung klicken.
- 5 Klicken Sie auf der Symbolleiste in der Switch-Topologie auf das Aktionssymbol **Ausgewählte Portgruppe entfernen**.

Eigenschaften des vSphere Standard-Switches

Die vSphere Standard-Switch-Einstellungen steuern Portstandardeinstellungen für den gesamten Switch, die durch Portgruppeneinstellungen für jeden Standard-Switch außer Kraft gesetzt werden können. Sie können Standard-Switch-Eigenschaften, wie beispielsweise die Uplink-Konfiguration und die Anzahl der verfügbaren Ports, bearbeiten.

Anzahl der Ports auf ESXi-Hosts

Für eine effiziente Verwendung der Hostressourcen wird auf ESXi 5.5-Hosts (und höher) die Anzahl der Ports von virtuellen Switches dynamisch nach oben und unten korrigiert. Ein Switch auf einem solchen Host kann auf die maximale Anzahl von Ports, die auf dem Host unterstützt wird, erweitert werden. Der Portgrenzwert wird bestimmt anhand der maximalen Anzahl von virtuellen Maschinen, die der Host verarbeiten kann.

Jeder virtuelle Switch auf ESXi 5.1-Hosts (und früher) stellt eine bestimmte Anzahl von Ports bereit, über die virtuelle Maschinen und Netzwerkdienste auf mindestens ein Netzwerk zugreifen können. Sie müssen die Anzahl von Ports gemäß Ihren Bereitstellungsanforderungen manuell erhöhen oder verringern.

Hinweis Durch die Erhöhung der Anzahl von Ports für einen Switch werden mehr Ressourcen auf dem Host reserviert und verbraucht. Falls einige Ports nicht belegt sind, bleiben Hostressourcen, die möglicherweise für andere Vorgänge benötigt werden, gesperrt und ungenutzt.

Ändern der MTU-Größe für einen vSphere Standard-Switch

Ändern Sie die Größe der maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) für einen vSphere Standard-Switch, um die Netzwerkeffizienz zu verbessern, indem der Umfang der mit einem einzigen Paket übertragenen Nutzlastdaten erhöht wird, was der Aktivierung von Jumbo-Frames entspricht.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.

- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie einen Standard-Switch aus der Tabelle aus und klicken Sie auf **Einstellungen bearbeiten**.
- 4 Ändern Sie den Wert für **MTU (Byte)** für den Standard-Switch.
 Sie können Jumbo-Frames aktivieren, indem Sie für **MTU (Byte)** einen Wert festlegen, der größer als 1500 Byte ist. 9000 Byte ist der maximal zulässige Wert für die MTU-Größe.
- 5 Klicken Sie auf **OK**.

Ändern der Geschwindigkeit eines physischen Adapters

Ein physischer Adapter kann einen Engpass für den Netzwerkdatenverkehr darstellen, wenn die Adaptergeschwindigkeit nicht den Anforderungen der Anwendung entspricht. Sie können die Verbindungsgeschwindigkeit und Duplex-Einstellung eines physischen Adapters ändern, um Daten in Übereinstimmung mit der Datenverkehrsrate übertragen zu können.

Wenn der physische Adapter SR-IOV unterstützt, können Sie diese Option aktivieren und die Anzahl der virtuellen Funktionen konfigurieren, die Sie für das Netzwerk der virtuellen Maschine verwenden möchten.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zu einem Host.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und wählen Sie die Option **Physische Adapter** aus **Netzwerk**.
 Die physischen Netzwerkadapter, die dem Host zugewiesen wurden, werden in einer Tabelle angezeigt, die Details zu jedem physischen Netzwerkadapter enthält.
- 3 Wählen Sie den physischen Netzwerkadapter aus der Liste aus und klicken Sie auf **Bearbeiten**.
- 4 Wählen Sie die Geschwindigkeit und die Duplex-Einstellung für den physischen Netzwerkadapter aus dem Dropdown-Menü aus.
- 5 Klicken Sie auf **OK**.

Hinzufügen und Gruppieren von physischen Adapters in einem vSphere Standard-Switch

Weisen Sie einem Standard-Switch einen physischen Adapter zu, um Konnektivität für virtuelle Maschinen und VMKernel-Adapter auf dem Host bereitzustellen. Sie können ein Team von NICs erstellen, um die Datenverkehrslast zu verteilen und den Failover zu konfigurieren.

Bei der NIC-Gruppierung werden mehrere Netzwerkverbindungen kombiniert, um den Durchsatz zu erhöhen und für den Fall, dass ein Link ausfällt, eine redundante Verbindung anzubieten. Um ein Gruppe zu erstellen, verknüpfen Sie mehrere physische Adapter mit einem einzelnen vSphere Standard-Switch.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie den Standard-Switch, dem Sie einen physischen Adapter hinzufügen möchten.
- 4 Klicken Sie auf **Physische Netzwerkadapter verwalten**.
- 5 Fügen Sie einen oder mehrere verfügbare physische Netzwerkadapter zum Switch hinzu.
 - a Klicken Sie auf **Adapter hinzufügen**.
 - b Wählen Sie die Gruppe für Failover-Reihenfolge aus, der die Adapter zugewiesen werden sollen.

Die Failover-Gruppe bestimmt die Rolle des Adapters für den Austausch von Daten mit dem externen Netzwerk („aktiv“, „Standby“ oder „nicht verwendet“). Standardmäßig werden die Adapter als „aktiv“ zum Standard-Switch hinzugefügt.
 - c Klicken Sie auf **OK**

Die ausgewählten Adapter werden in der Liste der ausgewählten Failover-Gruppen unter „Zugewiesene Adapter“ angezeigt.
- 6 (Optional) Ändern Sie die Position eines Adapters in den Failover-Gruppen mithilfe der Pfeiltasten.
- 7 Klicken Sie auf **OK**, um die Konfiguration der physischen Adapter anzuwenden.

Anzeigen des Topologie-Diagramms eines vSphere Standard-Switches

Die Struktur und die Komponenten eines vSphere Standard-Switches können Sie mithilfe des Topologie-Diagramms analysieren.

Das Topologie-Diagramm eines Standard-Switches liefert eine visuelle Darstellung der Adapter und Portgruppen, die mit dem Switch verbunden sind.

In diesem Diagramm können Sie die Einstellungen einer ausgewählten Portgruppe und eines ausgewählten Adapters bearbeiten.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie den Standard-Switch aus der Liste aus.

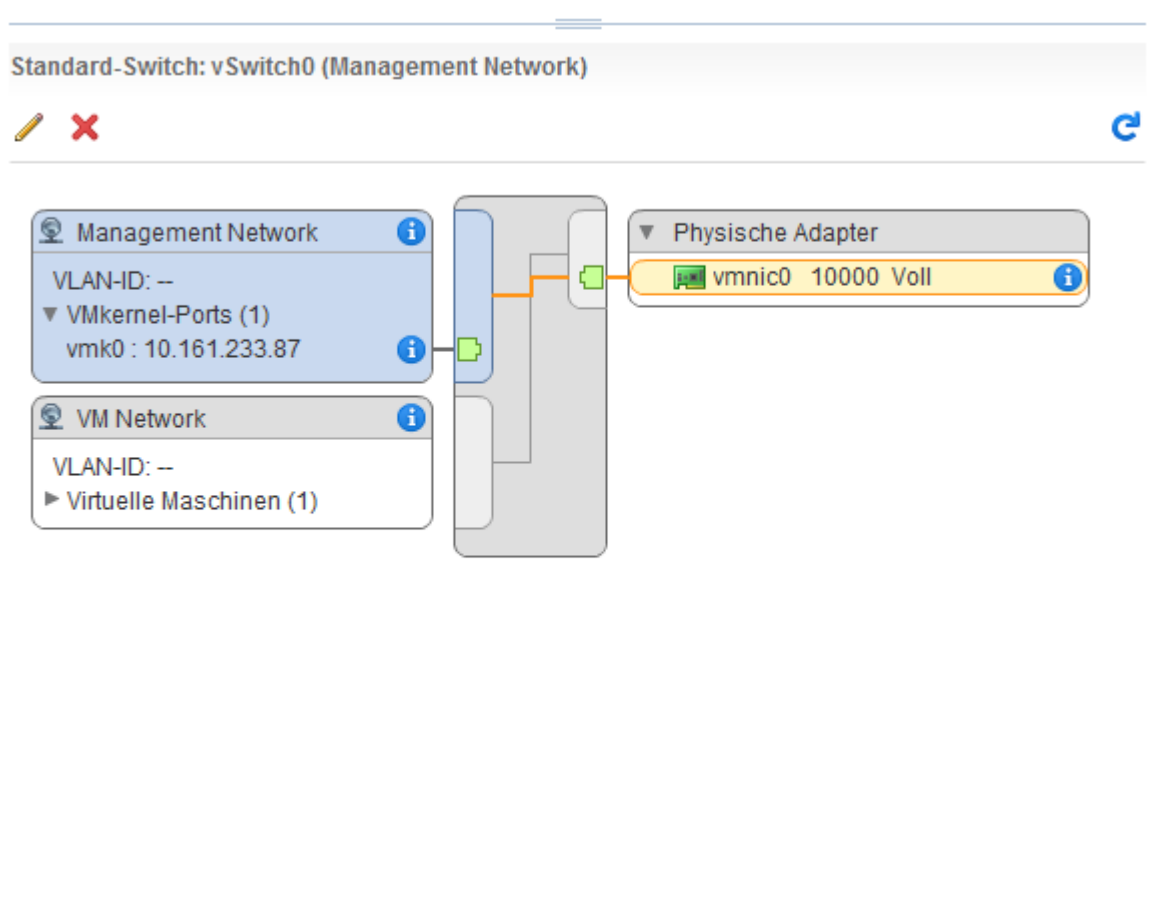
Ergebnisse

Das Diagramm wird unter der Liste der virtuellen Switches auf dem Host angezeigt.

Beispiel: Diagramm eines Standard-Switches, der den VMkernel und virtuelle Maschinen mit dem Netzwerk verbindet

In Ihrer virtuellen Umgebung steuert ein vSphere Standard-Switch VMkernel-Adapter für vSphere vMotion und für das Verwaltungsnetzwerk sowie gruppierte virtuelle Maschinen. Mithilfe des zentralen Topologie-Diagramms können Sie feststellen, ob eine virtuelle Maschine oder ein VMkernel-Adapter mit dem externen Netzwerk verbunden ist. Weiterhin können Sie den physischen Adapter bestimmen, über den Daten übertragen werden.

Abbildung 2-2. Topologie-Diagramm eines Standard-Switches, der den VMkernel und virtuelle Maschinen mit dem Netzwerk verbindet



Einrichten von Netzwerken mit vSphere Distributed Switches

3

Mit vSphere Distributed Switches können Sie in einer vSphere-Umgebung Netzwerke einrichten und konfigurieren.

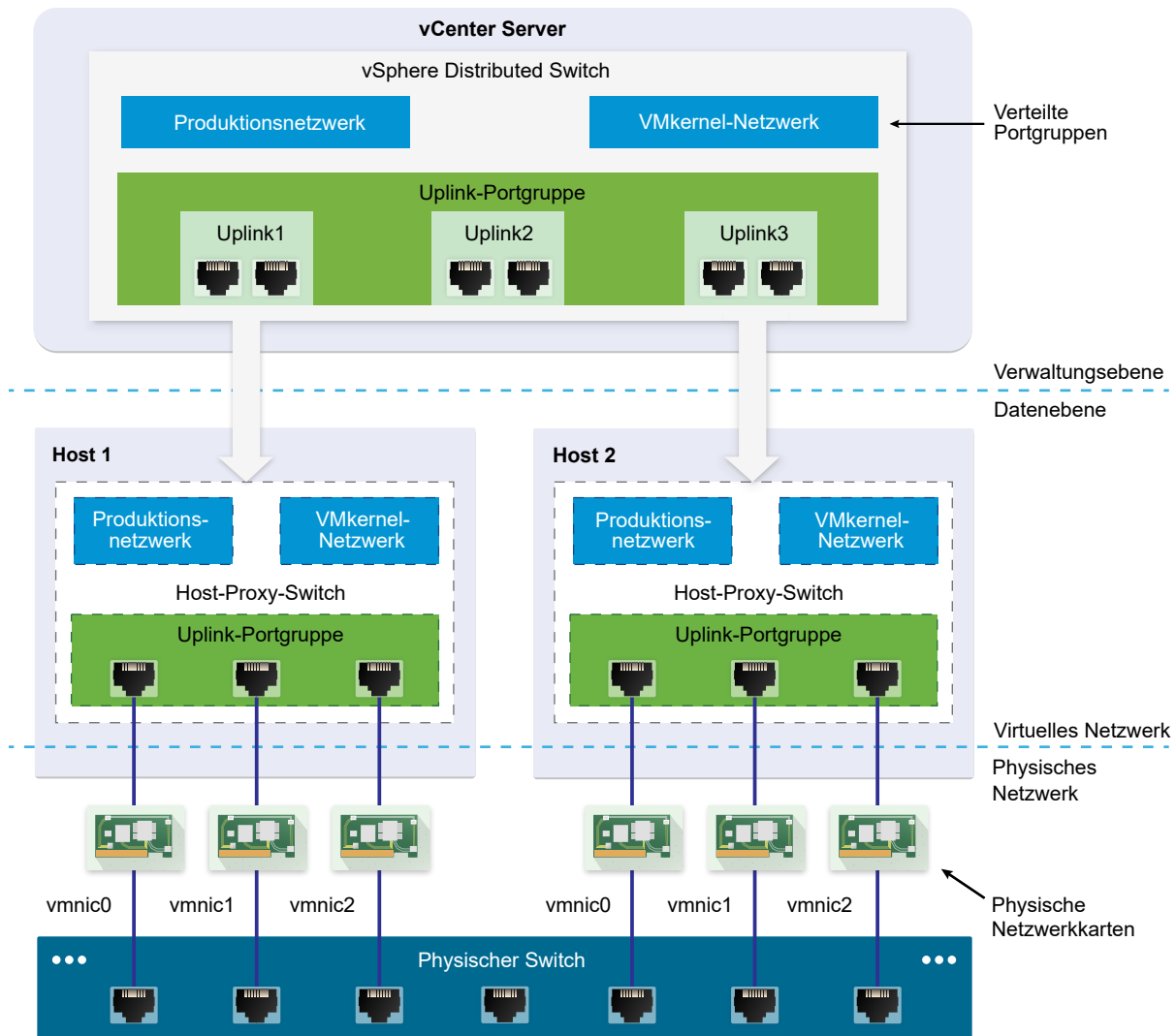
Dieses Kapitel enthält die folgenden Themen:

- vSphere Distributed Switch-Architektur
- Einen vSphere Distributed Switch erstellen
- Upgrade eines vSphere Distributed Switch auf eine höhere Version
- Bearbeiten allgemeiner und erweiterter vSphere Distributed Switch-Einstellungen
- Verwalten von Netzwerken auf mehreren Hosts auf einem vSphere Distributed Switch
- Verwalten von Netzwerken auf Host-Proxy-Switches
- Verteilte Portgruppen
- Arbeiten mit verteilten Ports
- Konfigurieren von Netzwerken von virtuellen Maschinen auf einem vSphere Distributed Switch
- Topologie-Diagramme eines vSphere Distributed Switch im vSphere Web Client

vSphere Distributed Switch-Architektur

Mit einem vSphere Distributed Switch kann die Netzwerkkonfiguration aller Hosts, die dem Switch zugeordnet sind, zentral verwaltet und überwacht werden. Sie konfigurieren einen Distributed Switch auf einem vCenter Server-System, und die Konfiguration wird an alle Hosts weitergegeben, die dem Switch zugeordnet sind.

Abbildung 3-1. vSphere Distributed Switch-Architektur



Ein Netzwerk-Switch in vSphere besteht aus zwei logischen Bereichen, der Datenebene und der Verwaltungsebene. Auf der Datenebene werden das Wechseln von Paketen, das Filtern, Kennzeichnen usw. implementiert. Die Verwaltungsebene ist die Steuerstruktur, mit der Sie die Funktionalität der Datenebene konfigurieren. Ein vSphere Standard-Switch enthält sowohl Daten- als auch Verwaltungsebenen, und Sie konfigurieren und verwalten jeden Standard-Switch individuell.

Ein vSphere Distributed Switch trennt die Datenebene von der Verwaltungsebene. Die Verwaltungsfunktionalität des Distributed Switch befindet sich in dem vCenter Server-System, mit dem Sie die Netzwerkkonfiguration Ihrer Umgebung auf Datencenterebene verwalten können. Die Datenebene verbleibt lokal auf jedem Host, der mit dem Distributed Switch verknüpft ist. Der Datenebenenabschnitt des Distributed Switch wird Host-Proxy-Switch genannt. Die Netzwerkkonfiguration, die Sie auf vCenter Server (Verwaltungsebene) erstellen, wird automatisch auf alle Host-Proxy-Switches (Datenebene) übertragen.

Der vSphere Distributed Switch führt zwei Abstraktionen ein, die Sie zum Erstellen einer konsistenten Netzwerkkonfiguration für physische Netzwerkkarten, virtuelle Maschinen und VMkernel-Dienste verwenden.

Uplink-Portgruppe

Während der Erstellung des Distributed Switch wird eine Uplink-Portgruppe oder DVUplink-Portgruppe definiert, die einen oder mehrere Uplinks enthalten kann. Ein Uplink ist eine Vorlage, mit der Sie physische Verbindungen von Hosts sowie Failover- und Lastausgleichsrichtlinien konfigurieren. Sie ordnen den Uplinks auf dem Distributed Switch physische Netzwerkkarten von Hosts zu. Auf der Hostebene ist jede physische Netzwerkkarte mit einem Uplink-Port mit einer bestimmten Kennung verbunden. Sie legen Failover- und Lastausgleichsrichtlinien über Uplinks fest, und die Richtlinien werden automatisch auf die Host-Proxy-Switches oder die Datenebene übertragen. Auf diese Weise können Sie eine konsistente Failover- und Lastausgleichskonfiguration für die physischen Netzwerkkarten aller Hosts, die mit dem Distributed Switch verknüpft sind, anwenden.

Verteilte Portgruppe

Verteilte Portgruppen stellen Netzwerkkonnektivität für virtuelle Maschinen bereit und ermöglichen VMkernel-Datenverkehr. Sie kennzeichnen jede verteilte Portgruppe durch eine Netzwerkbezeichnung, die im aktuellen Datencenter eindeutig sein muss. Sie konfigurieren NIC-Gruppierung, Failover, Lastausgleich, VLAN, Sicherheit, Traffic-Shaping und andere Richtlinien auf verteilten Portgruppen. Die virtuellen Ports, die mit einer verteilten Portgruppe verbunden sind, verfügen über dieselben Eigenschaften wie die verteilte Portgruppe. Wie bei Uplink-Portgruppen wird die Konfiguration, die Sie bei verteilten Portgruppen auf vCenter Server (Verwaltungsebene) festlegen, automatisch auf alle Hosts auf dem Distributed Switch durch ihre Host-Proxy-Switches (Datenebene) übertragen. Auf diese Weise können Sie eine VM-Gruppe so konfigurieren, dass dieselbe Netzwerkkonfiguration verwendet wird, indem Sie die virtuellen Maschinen derselben verteilten Portgruppe zuordnen.

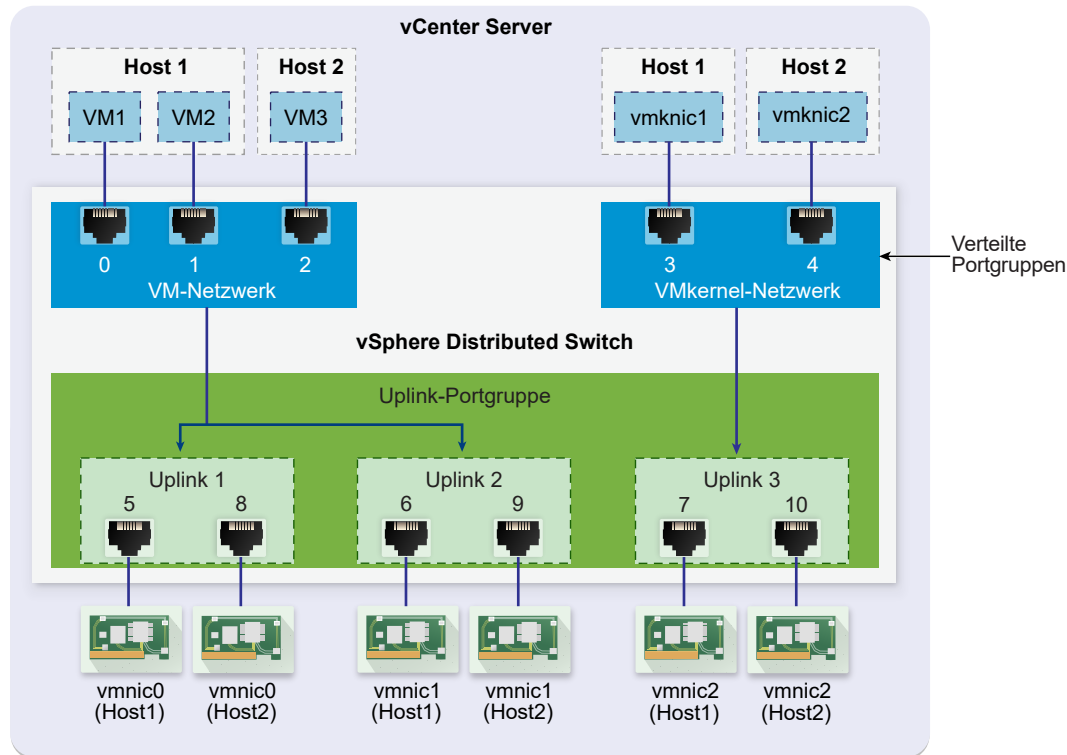
Beispiel: Angenommen, Sie erstellen einen vSphere Distributed Switch auf Ihrem Datencenter und verknüpfen zwei Hosts damit. Sie konfigurieren drei Uplinks zur Uplink-Portgruppe und schließen eine physische Netzwerkkarte von jedem Host zu einem Uplink an. Auf diese Weise werden jedem Uplink zwei physische Netzwerkkarten von jedem Host zugeordnet, zum Beispiel wird Uplink 1 mit vmnic0 von Host 1 und Host 2 konfiguriert. Dann erstellen Sie die verteilten Portgruppen des Produktions- und des VMkernel-Netzwerks für VM-Netzwerke und VMkernel-Dienste. Auf Host 1 und Host 2 wird außerdem eine Darstellung der Portgruppen des Produktions- und des VMkernel-Netzwerks erstellt. Alle Richtlinien, die Sie für die Portgruppen des Produktions- und des VMkernel-Netzwerks festlegen, werden auf ihre Darstellungen auf Host 1 und Host 2 übertragen.

Um die effiziente Nutzung der Hostressourcen sicherzustellen, wird die Anzahl der verteilten Ports von Proxy-Switches auf Hosts mit ESXi 5.5 oder höher dynamisch nach oben oder unten skaliert. Ein Proxy-Switch auf einem solchen Host kann auf die maximale Anzahl von Ports, die auf dem Host unterstützt wird, erweitert werden. Der Portgrenzwert wird bestimmt anhand der maximalen Anzahl von virtuellen Maschinen, die der Host verarbeiten kann.

Datenfluss beim vSphere Distributed Switch

Der Datenfluss von den virtuellen Maschinen und VMkernel-Adaptoren zum physischen Netzwerk hängt von der NIC-Gruppierung und den Lastausgleichsrichtlinien ab, die für die verteilten Portgruppen festgelegt wurden. Der Datenfluss hängt auch von der Portzuteilung am Distributed Switch ab.

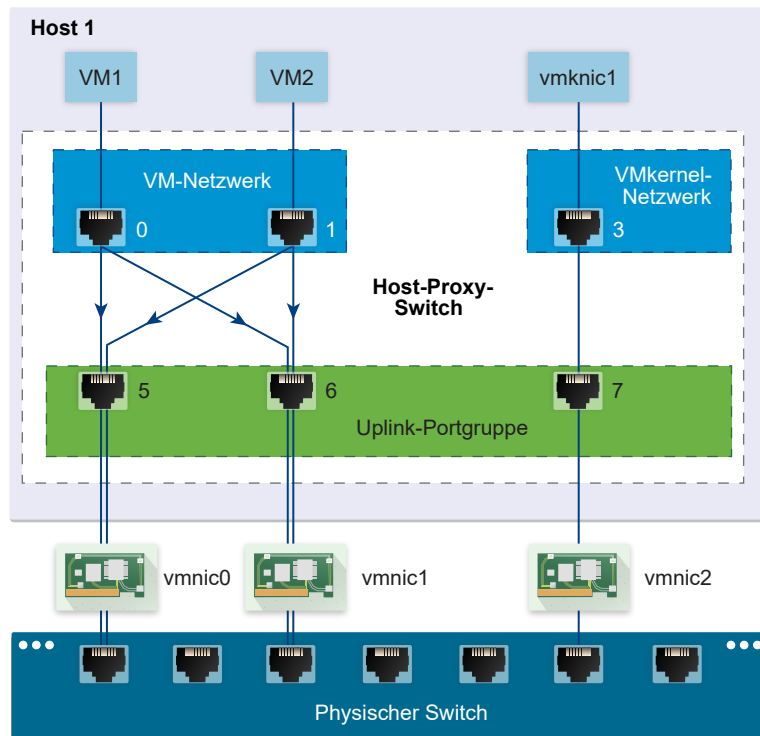
Abbildung 3-2. NIC-Gruppierung und Portzuteilung auf einem vSphere Distributed Switch



Beispiel: Angenommen, Sie erstellen die verteilten Portgruppen des VM- und des VMkernel-Netzwerks mit 3 bzw. 2 verteilten Ports. Der Distributed Switch weist Ports mit den IDs 0 bis 4 in der Reihenfolge zu, in der Sie die verteilten Portgruppen erstellt haben. Dann verknüpfen Sie Host 1 und Host 2 mit dem Distributed Switch. Der Distributed Switch weist Ports für jede physische Netzwerkkarte auf den Hosts zu, während die Nummerierung der Ports von 5 in der Reihenfolge fortschreitet, in der Sie die Hosts hinzufügen. Um Netzwerkkonnektivität auf jedem Host bereitzustellen, ordnen Sie vmnic0 Uplink 1, vmnic1 Uplink 2 und vmnic2 Uplink 3 zu.

Um Konnektivität für virtuelle Maschinen bereitzustellen und VMkernel-Datenverkehr zu ermöglichen, konfigurieren Sie Teaming und Failover für die VM-Netzwerk- und VMkernel-Netzwerkportgruppen. Uplink 1 und Uplink 2 handhaben den Datenverkehr für die VM-Netzwerkportgruppe und Uplink 3 handhabt den Datenverkehr für die VMkernel-Netzwerkportgruppe.

Abbildung 3-3. Paketfluss auf dem Host-Proxy-Switch



Auf der Hostseite geht der Paketfluss von virtuellen Maschinen und VMkernel-Diensten durch bestimmte Ports, um das physische Netzwerk zu erreichen. Beispiel: Ein von VM1 auf Host 1 gesendetes Paket erreicht zuerst Port 0 auf der verteilten Portgruppe des VM-Netzwerks. Weil Uplink 1 und Uplink 2 den Datenverkehr für die Portgruppe des VM-Netzwerks handhaben, kann das Paket von Uplink-Port 5 oder Uplink-Port 6 weitergehen. Wenn das Paket durch Uplink-Port 5 geht, geht es zu vmnic0 weiter, und wenn das Paket zu Uplink-Port 6 geht, geht es zu vmnic1 weiter.

Einen vSphere Distributed Switch erstellen

Erstellen Sie einen vSphere Distributed Switch auf einem Datacenter, um die Netzwerkkonfiguration mehrerer Hosts gleichzeitig von einer zentralen Stelle aus zu regeln.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zu einem Datacenter.
- 2 Klicken Sie mit der rechten Maustaste auf das Datacenter im Navigator und wählen Sie **Distributed Switch > Neuer Distributed Switch** aus.
- 3 Geben Sie unter **Name und Speicherort** einen Namen für den neuen Distributed Switch ein oder akzeptieren Sie den generierten Namen und klicken Sie auf **Weiter**.

- 4 Wählen Sie unter **Version auswählen** eine Distributed Switch-Version aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Distributed Switch: 6.0.0	Kompatibel mit ESXi Version 6.0 und höher.
Distributed Switch: 5.5.0	Kompatibel mit ESXi Version 5.5 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Distributed Switch: 5.1.0	Kompatibel mit VMware ESXi Version 5.1 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Distributed Switch: 5.0.0	Kompatibel mit VMware ESXi Version 5.0 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.

- 5 Konfigurieren Sie in **Einstellungen bearbeiten** die Einstellungen des Distributed Switch.

- a Wählen Sie mit den Pfeilschaltflächen die **Anzahl an Uplinks** aus.

Uplink-Ports verbinden den verteilten Distributed Switch mit physischen Netzwerkkarten auf zugehörigen Hosts. Die Anzahl der Uplink-Ports ist die maximale Anzahl der zulässigen physischen Verbindungen zum verteilten Switch pro Host.

- b Aktivieren oder deaktivieren Sie über das Dropdown-Menü **Network I/O Control**.

Mit Network I/O Control können Sie den Zugang zu den Netzwerkressourcen für bestimmte Typen von Infrastruktur- und Arbeitslastdatenverkehr entsprechend den Anforderungen Ihrer Bereitstellung priorisieren. Network I/O Control überwacht kontinuierlich die E/A-Last auf dem Netzwerk und weist dynamisch verfügbare Ressourcen zu.

- c Aktivieren Sie das Kontrollkästchen **Standard-Portgruppe erstellen**, um eine neue verteilte Portgruppe mit Standardeinstellungen für diesen Switch zu erstellen.

- d (Optional) Um eine verteilte Standard-Portgruppe zu erstellen, geben Sie den Namen der Portgruppe unter **Name der Portgruppe** ein oder akzeptieren Sie den generierten Namen.

Wenn Ihr System benutzerdefinierte Portgruppenanforderungen hat, erstellen Sie eine verteilte Portgruppe, die diese Anforderungen erfüllt, nachdem Sie den Distributed Switch hinzugefügt haben.

- e Klicken Sie auf **Weiter**.

- 6 Überprüfen Sie Ihre Einstellungen unter **Bereit zum Abschließen** und klicken Sie auf **Beenden**.
Klicken Sie auf **Zurück**, wenn Sie Ihre Einstellungen bearbeiten möchten.

Ergebnisse

Ein Distributed Switch wird auf dem Datacenter erstellt. Sie können die unterstützten Funktionen auf dem Distributed Switch sowie weitere Details anzeigen, indem Sie zum neuen Distributed Switch navigieren und auf die Registerkarte **Übersicht** klicken.

Nächste Schritte

Fügen Sie Hosts zum Distributed Switch hinzu und konfigurieren Sie deren Netzwerkadapter auf dem Switch.

Upgrade eines vSphere Distributed Switch auf eine höhere Version

Sie können ein Upgrade von vSphere Distributed Switch, Version 5.x, auf eine höhere Version durchführen. Nach dem Upgrade kann der Distributed Switch Funktionen nutzen, die nur in der neueren Version verfügbar sind.

Das Upgrade eines Distributed Switch ist ein unterbrechungsfreier Vorgang. Das heißt, dass es keine Ausfallzeiten für die Hosts und die virtuellen Maschinen gibt, die an den Switch angeschlossen sind.

Hinweis Damit die Konnektivität der virtuellen Maschinen und VMkernel-Adapter wiederhergestellt werden kann, falls das Upgrade fehlschlägt, sollten Sie die Konfiguration des Distributed Switch sichern.

Wenn das Upgrade fehlschlägt, können Sie den Switch zusammen mit seinen Portgruppen und verbundenen Hosts wiederherstellen, indem Sie die Switch-Konfigurationsdatei importieren. Siehe [Exportieren von vSphere Distributed Switch-Konfigurationen](#) und [Importieren einer vSphere Distributed Switch-Konfiguration](#).

Voraussetzungen

- Aktualisieren Sie vCenter Server auf Version 6.0.
- Aktualisieren Sie alle Hosts, die mit dem Distributed Switch verbunden sind, auf ESXi 6.0.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Upgrade > Upgrade des Distributed Switch durchführen** aus.

- 3 Wählen Sie die vSphere Distributed Switch-Version aus, auf die Sie den Switch aktualisieren möchten, und klicken Sie auf **Weiter**.

Option	Beschreibung
Version 6.0.0	Kompatibel mit ESXi Version 6.0 und höher.
Version 5.5.0	Kompatibel mit ESXi Version 5.5 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Version 5.1.0	Kompatibel mit ESXi Version 5.1 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.

- 4 Prüfen Sie die Hostkompatibilität und klicken Sie auf **Weiter**.

Einige der mit dem Distributed Switch verbundenen ESXi-Instanzen sind möglicherweise mit der ausgewählten Zielversion nicht kompatibel. Führen Sie ein Upgrade für die inkompatiblen Hosts durch, entfernen Sie sie oder wählen Sie eine andere Upgradeversion für den Distributed Switch aus.

- 5 Schließen Sie die Upgradekonfiguration ab und klicken Sie auf **Beenden**.

Vorsicht Nach dem Upgrade des vSphere Distributed Switch kann er nicht auf eine ältere Version zurückgesetzt werden. Sie können auch keine ESXi-Hosts hinzufügen, auf denen eine ältere Version als die neue Version des Switches ausgeführt wird.

- a Überprüfen Sie die Upgrade-Einstellungen.
- b Falls Sie ein Upgrade von vSphere Distributed Switch 5.1 durchführen, planen Sie die Konvertierung zur erweiterten LACP-Unterstützung ein.
- c Falls Sie ein Upgrade von vSphere Distributed Switch 5.1 und höher durchführen, planen Sie die Konvertierung zu Network I/O Control, Version 3, ein.

Ergebnisse

Informationen zur Konvertierung zur erweiterten LACP-Unterstützung finden Sie unter [Konvertieren zur erweiterten LACP-Unterstützung auf einem vSphere Distributed Switch](#).

Informationen zur Konvertierung zu Network I/O Control, Version 3, finden Sie unter [Upgrade von Network I/O Control auf Version 3 auf einem vSphere Distributed Switch](#).

Bearbeiten allgemeiner und erweiterter vSphere Distributed Switch-Einstellungen

Zu den allgemeinen Einstellungen des vSphere Distributed Switch gehören der Name des Switch und die Anzahl der Uplinks. Erweiterte Einstellungen eines Distributed Switch sind beispielsweise das Cisco Discovery-Protokoll und der Maximalwert für MTU für den Switch.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf die Registerkarte **Verwalten**, klicken Sie auf **Einstellungen** und wählen Sie **Eigenschaften** aus.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Klicken Sie auf **Allgemein**, um die Einstellungen des vSphere Distributed Switch zu bearbeiten.

Option	Beschreibung
Name	Geben Sie den Namen für den Distributed Switch ein.
Anzahl an Uplinks	Wählen Sie die Anzahl der Uplink-Ports für den Distributed Switch aus. Klicken Sie auf Uplink-Namen bearbeiten , um die Namen der Uplinks zu ändern.
Anzahl der Ports	Die Anzahl der Ports für diesen Distributed Switch. Dieser Wert kann nicht bearbeitet werden.
Network I/O Control	Verwenden Sie das Dropdown-Menü, um die E/A-Steuerung für das Netzwerk zu aktivieren oder zu deaktivieren.
Beschreibung	Fügen Sie eine Beschreibung der Einstellungen des Distributed Switch hinzu oder ändern Sie diese.

- 5 Klicken Sie auf **Erweitert**, um die Einstellungen des vSphere Distributed Switch zu bearbeiten.

Option	Beschreibung
MTU (Byte)	Maximalwert für MTU für den vSphere Distributed Switch. Legen Sie einen Wert auf größer als 1500 Byte, um Jumbo-Frames zu aktivieren.
Multicast-Filtermodus	<ul style="list-style-type: none"> ■ Allgemein. Der Distributed Switch leitet Datenverkehr im Zusammenhang mit einer Multicast-Gruppe basierend auf einer MAC-Adresse weiter, die von den letzten 23 Bits der IPv4-Adresse der Gruppe generiert wurde. ■ IGMP/MLD-Snooping. Der Distributed Switch leitet Datenverkehr an virtuelle Maschinen gemäß den IPv4- und IPv6-Adressen von abonnierten Multicast-Gruppen mithilfe von Mitgliedschaftsnachrichten weiter, die mit IGMP (Internet Group Management Protocol) und dem MLDP-Protokoll (Multicast Listener Discovery) definiert werden.
Discovery-Protokoll	<ol style="list-style-type: none"> a Wählen Sie im Dropdown-Menü Typ die Option „Cisco Discovery-Protokoll“, „Link-Layer Discovery Protocol (LLDP)“ oder „Deaktiviert“ aus. b Legen Sie „Vorgang“ auf „Überwachen“, „Werben“ oder „Beide“ fest. Weitere Informationen zum Discovery-Protokoll finden Sie unter Switch-Discovery-Protokoll.
Administratorkontakt	Geben Sie den Namen und andere Details des Administrators für den Distributed Switch ein.

- 6 Klicken Sie auf **OK**.

Verwalten von Netzwerken auf mehreren Hosts auf einem vSphere Distributed Switch

Auf einem vSphere Distributed Switch können Sie virtuelle Netzwerke erstellen und verwalten, indem Sie Hosts zu dem Switch hinzufügen und für deren Netzwerkadapter eine Verbindung mit dem Switch herstellen. Sie können einen Host als Vorlage verwenden und dessen Konfiguration auf andere Hosts anwenden, um für mehrere Hosts auf dem Distributed Switch eine einheitliche Netzwerkkonfiguration zu erstellen.

■ Aufgaben für das Verwalten von Host-Netzwerken auf einem vSphere Distributed Switch

Sie können neue Hosts zu einem vSphere Distributed Switch hinzufügen, Netzwerkadapter mit dem Switch verbinden und Hosts vom Switch entfernen. Sie müssen in einer Produktionsumgebung möglicherweise die Netzwerkkonnektivität für virtuelle Maschinen und VMkernel-Dienste aufrechterhalten, während Sie das Hostnetzwerk auf dem Distributed Switch verwalten.

■ Hosts zu einem vSphere Distributed Switch hinzufügen

Sie müssen dem Switch Hosts zuweisen, um das Netzwerk Ihrer vSphere-Umgebung mithilfe eines vSphere Distributed Switch zu verwalten. Sie können physische Netzwerkkarten, VMkernel-Adapter und Netzwerkadapter virtueller Maschinen mit dem Distributed Switch verbinden.

■ Konfigurieren von physischen Netzwerkadaptern auf einem vSphere Distributed Switch

Für Hosts, die mit einem Distributed Switch verbunden sind, können Sie physische Netzwerkkarten zu Uplinks auf dem Switch zuweisen. Auf dem Distributed Switch können Sie jeweils physische Netzwerkkarten für mehrere Hosts konfigurieren.

■ Migrieren von VMkernel-Adaptern zu einem vSphere Distributed Switch

Migrieren Sie VMkernel-Adapter auf einen Distributed Switch, wenn Sie den Datenverkehr für VMkernel-Dienste nur mit diesem Switch verwalten möchten und die Adapter auf anderen Standard-Switches oder Distributed Switches nicht mehr benötigen.

■ Erstellen eines VMkernel-Adapters auf einem vSphere Distributed Switch

Erstellen Sie einen VMkernel-Adapter auf Hosts, die einem Distributed Switch zugeordnet sind, um eine Netzwerkverbindung für die Hosts bereitzustellen und den Datenverkehr für vSphere vMotion, IP-Speicher, Fault Tolerance-Protokollierung oder Virtual SAN zu regeln. Mit dem Assistenten **Hosts hinzufügen und verwalten** können Sie VMkernel-Adapter auf mehreren Hosts gleichzeitig erstellen.

■ Migrieren von Netzwerken virtueller Maschinen zu einem vSphere Distributed Switch

Für die Verwaltung von Netzwerken virtueller Maschinen mit einem Distributed Switch migrieren Sie Netzwerkadapter der virtuellen Maschine auf benannte Netzwerke auf dem Switch.

- **Aktualisieren der maximalen Anzahl der verteilten Ports auf Hosts**

Wenn auf einem Host ESXi 5.1 oder früher ausgeführt wird, können Sie die maximale Anzahl von verteilten Ports auf dem Proxy-Switch des Hosts ändern.

- **Verwenden eines Hosts als Vorlage zur Erstellung einer einheitlichen Netzwerkkonfiguration auf einem vSphere Distributed Switch**

Wenn Sie Hosts mit einheitlicher Netzwerkkonfiguration einrichten möchten, können Sie einen Host als Vorlage auswählen und seine Konfiguration für physische Netzwerkkarten und VMkernel-Adapter auf andere Hosts im Distributed Switch anwenden.

- **Entfernen von Hosts aus einem vSphere Distributed Switch**

Entfernen Sie Hosts von einem vSphere Distributed Switch, falls Sie einen anderen Switch für die Hosts konfiguriert haben.

Aufgaben für das Verwalten von Host-Netzwerken auf einem vSphere Distributed Switch

Sie können neue Hosts zu einem vSphere Distributed Switch hinzufügen, Netzwerkadapter mit dem Switch verbinden und Hosts vom Switch entfernen. Sie müssen in einer Produktionsumgebung möglicherweise die Netzwerkkonnektivität für virtuelle Maschinen und VMkernel-Dienste aufrechterhalten, während Sie das Hostnetzwerk auf dem Distributed Switch verwalten.

Hinzufügen von Hosts zu einem vSphere Distributed Switch

Überlegen Sie, ob Ihre Umgebung vorbereitet werden muss, bevor Sie die neuen Hosts zu einem Distributed Switch hinzufügen.

- Erstellen Sie verteilte Portgruppen für das VM-Netzwerk.
- Erstellen Sie verteilte Portgruppen für VMkernel-Dienste. Erstellen Sie beispielsweise verteilte Portgruppen für Verwaltungsnetzwerk, vMotion und Fault Tolerance.
- Konfigurieren Sie genügend Uplinks auf dem Distributed Switch für alle physischen Netzwerkkarten, die Sie mit dem Switch verbinden möchten. Wenn beispielsweise die Hosts, die Sie mit dem Distributed Switch verbinden möchten, über jeweils acht physische Netzwerkkarten verfügen, konfigurieren Sie acht Uplinks auf dem Distributed Switch.
- Stellen Sie sicher, dass die Konfiguration des Distributed Switch für Dienste mit spezifischen Netzwerkanforderungen vorbereitet ist. iSCSI verfügt beispielsweise über spezifische Anforderungen für die Teaming- und Failover-Konfiguration der verteilten Portgruppe, in der Sie den iSCSI-VMkernel-Adapter verbinden.

Sie können den Assistenten **Hosts hinzufügen und verwalten** im vSphere Web Client verwenden, um gleichzeitig mehrere Hosts hinzuzufügen.

Verwalten von Netzwerkadaptern auf einem vSphere Distributed Switch

Nachdem Sie Hosts zu einem Distributed Switch hinzugefügt haben, können Sie physische Netzwerkkarten mit Uplinks auf dem Switch verbinden, VM-Netzwerkadapter konfigurieren und das VMkernel-Netzwerk verwalten.

Wenn einige Hosts auf einem Distributed Switch anderen Switches in Ihrem Datacenter zugewiesen sind, können Sie Netzwerkadapter zum oder vom Distributed Switch migrieren.

Wenn Sie VM-Netzwerkadapter oder VMkernel-Adapter migrieren, stellen Sie sicher, dass die verteilten Zielpartgruppen über mindestens einen aktiven Uplink verfügen und dass der Uplink mit einer physischen Netzwerkkarte auf den Hosts verbunden ist. Ein anderer Ansatz ist, physische Netzwerkkarten, virtuelle Netzwerkadapter und VMkernel-Adapter gleichzeitig zu migrieren.

Wenn Sie physische Netzwerkkarten migrieren, behalten Sie mindestens eine aktive Netzwerkkarte bei, die den Datenverkehr der Portgruppen regelt. Wenn beispielsweise *vmnic0* und *vmnic1* den Datenverkehr der *VM-Netzwerk*-Portgruppe regeln, migrieren Sie *vmnic0* und lassen Sie *vmnic1* mit der Gruppe verbunden.

Entfernen von Hosts von einem vSphere Distributed Switch

Bevor Sie Hosts von einem Distributed Switch entfernen, müssen Sie die verwendeten Netzwerkadapter zu einem anderen Switch migrieren.

- Um Hosts zu einem anderen Distributed Switch hinzuzufügen, können Sie den Assistenten **Hosts hinzufügen und verwalten** verwenden, um die Netzwerkadapter auf den Hosts zu einem neuen Switch zu migrieren. Anschließend können Sie die Hosts sicher vom aktuellen Distributed Switch entfernen.
- Um ein Hostnetzwerk zu Standard-Switches zu migrieren, müssen Sie die Netzwerkadapter schrittweise migrieren. Entfernen Sie beispielsweise physische Netzwerkkarten auf den Hosts vom Distributed Switch, indem Sie eine physische Netzwerkkarte auf jedem mit dem Switch verbundenen Host lassen, um die Netzwerkkonnektivität beizubehalten. Ordnen Sie danach die physischen Netzwerkkarten den Standard-Switches zu und migrieren Sie VMkernel-Adapter und VM-Netzwerkadapter zu Switches. Zuletzt migrieren Sie die physische Netzwerkkarte, die Sie mit dem Distributed Switch verbunden gelassen haben, zu den Standard-Switches.

Hosts zu einem vSphere Distributed Switch hinzufügen

Sie müssen dem Switch Hosts zuweisen, um das Netzwerk Ihrer vSphere-Umgebung mithilfe eines vSphere Distributed Switch zu verwalten. Sie können physische Netzwerkkarten, VMkernel-Adapter und Netzwerkadapter virtueller Maschinen mit dem Distributed Switch verbinden.

Voraussetzungen

- Stellen Sie sicher, dass genügend Uplinks auf dem Distributed Switch zur Verfügung stehen, um sie den physischen Netzwerkkarten zuzuordnen, die Sie mit dem Switch verbinden möchten.

- Stellen Sie sicher, dass mindestens eine verteilte Portgruppe auf dem Distributed Switch vorhanden ist.
- Stellen Sie sich, dass sich in der verteilten Portgruppe aktive Uplinks befinden, die in der Teaming- und Failover-Richtlinie konfiguriert sind.

Wenn Sie VMkernel-Adapter für iSCSI migrieren oder erstellen, stellen Sie sicher, dass die Teaming- und Failover-Richtlinie der verteilten Zielpartgruppe die Anforderungen für iSCSI erfüllt:

- Stellen Sie sicher, dass nur ein Uplink aktiviert ist, die Standby-Liste leer ist und die restlichen Uplinks nicht verwendet werden.
- Stellen Sie sicher, dass pro Host nur eine physische Netzwerkkarte zum aktiven Uplink zugewiesen ist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.
- 3 Wählen Sie **Host hinzufügen** aus und klicken Sie auf **Weiter**.
- 4 Klicken Sie auf **Neue Hosts**, treffen Sie Ihre Auswahl aus den Hosts in Ihrem Datacenter und klicken Sie auf **OK**.
- 5 Wählen Sie die Aufgaben für die Konfiguration der Netzwerkkarten zum Distributed Switch aus und klicken Sie auf **Weiter**.
- 6 Konfigurieren Sie die physischen Netzwerkkarten auf dem Distributed Switch.
 - a Wählen Sie aus der Liste „Auf anderen Switches/frei“ eine physische Netzwerkkarte aus.
Wenn Sie bereits mit anderen Switches verbundene physische Netzwerkkarten auswählen, werden sie zum aktuellen Distributed Switch migriert.
 - b Klicken Sie auf **Uplink zuweisen**.
 - c Wählen Sie einen Uplink aus und klicken Sie auf **OK**.

Sie können für eine konsistente Netzwerkkonfiguration dieselbe physische Netzwerkkarte auf jedem Host mit demselben Uplink auf dem Distributed Switch verbinden.

Wenn Sie beispielsweise zwei Hosts hinzufügen, verbinden Sie *vmnic1* auf jedem Host mit *Uplink1* auf dem Distributed Switch.
- 7 Klicken Sie auf **Weiter**.
- 8 Konfigurieren Sie VMkernel-Adapter.
 - a Wählen Sie einen VMkernel-Adapter aus und klicken Sie auf **Portgruppe zuweisen**.
 - b Wählen Sie eine verteilte Portgruppe aus und klicken Sie auf **OK**.

9 Überprüfen Sie die betroffenen Dienste sowie den Auswirkungsgrad.

Option	Beschreibung
Keine Auswirkung	iSCSI funktioniert wie gewohnt, nachdem die neue Netzwerkkonfiguration angewendet wurde.
Wichtige Auswirkung	Die gewohnte Funktionsweise von iSCSI kann unterbrochen werden, wenn die neue Netzwerkkonfiguration angewendet wird.
Kritische Auswirkung	Die gewohnte Funktionsweise von iSCSI wird unterbrochen, wenn die neue Netzwerkkonfiguration angewendet wird.

- Wenn eine bedeutende oder kritische Auswirkung auf iSCSI vorliegt, klicken Sie auf den Eintrag **iSCSI** und überprüfen Sie die Gründe, die im Bereich „Analysedetails“ angezeigt werden.
- Nachdem Sie die Auswirkung auf iSCSI behoben haben, fahren Sie mit der Netzwerkkonfiguration fort.

10 Klicken Sie auf **Weiter**.

11 Konfigurieren Sie das VM-Netzwerk.

- Um alle Netzwerkadapter einer virtuellen Maschine mit einer verteilten Portgruppe zu verbinden, wählen Sie die virtuelle Maschine aus, oder wählen Sie einen einzelnen Netzwerkadapter aus, um nur diesen Adapter zu verbinden.
- Klicken Sie auf **Portgruppe zuweisen**.
- Wählen Sie eine verteilte Portgruppe aus der Liste aus und klicken Sie auf **OK**.

12 Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

Nächste Schritte

Durch das Vorhandensein von dem Distributed Switch zugewiesenen Hosts können Sie physische Netzwerkkarten, VMkernel-Adapter und VM-Netzwerkadapter verwalten.

Konfigurieren von physischen Netzwerkadaptern auf einem vSphere Distributed Switch

Für Hosts, die mit einem Distributed Switch verbunden sind, können Sie physische Netzwerkkarten zu Uplinks auf dem Switch zuweisen. Auf dem Distributed Switch können Sie jeweils physische Netzwerkkarten für mehrere Hosts konfigurieren.

Für eine einheitliche Netzwerkkonfiguration auf allen Hosts können Sie dieselbe physische Netzwerkkarte auf jedem Host demselben Uplink auf dem Distributed Switch zuweisen. Beispielsweise können Sie *vmnic1* der Hosts *ESXi A* und *ESXi B* zu *Uplink 1* zuweisen.

Verfahren

- Navigieren Sie im vSphere Web Client zum Distributed Switch.
- Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.

- 3 Wählen Sie **Hostnetzwerk verwalten** aus und klicken Sie auf **Weiter**.
- 4 Klicken Sie auf **Angeschlossene Hosts** und wählen Sie aus den Hosts aus, die dem Distributed Switch zugeordnet sind.
- 5 Klicken Sie auf **Weiter**.
- 6 Wählen Sie **Physische Adapter verwalten** aus und klicken Sie auf **Weiter**.
- 7 Wählen Sie aus der Liste „Auf anderen Switches/frei“ eine physische Netzwerkkarte aus.
Wenn Sie physische Netzwerkkarten auswählen, die bereits anderen Switches zugewiesen sind, werden sie zum aktuellen Distributed Switch migriert.
- 8 Klicken Sie auf **Uplink zuweisen**.
- 9 Wählen Sie einen Uplink oder wählen Sie **Automatisch zuweisen** aus.
- 10 Klicken Sie auf **Weiter**.
- 11 Überprüfen Sie die betroffenen Dienste sowie den Auswirkungsgrad.

Option	Beschreibung
Keine Auswirkung	iSCSI funktioniert wie gewohnt, nachdem die neue Netzwerkkonfiguration angewendet wurde.
Wichtige Auswirkung	Die gewohnte Funktionsweise von iSCSI kann unterbrochen werden, wenn die neue Netzwerkkonfiguration angewendet wird.
Kritische Auswirkung	Die gewohnte Funktionsweise von iSCSI wird unterbrochen, wenn die neue Netzwerkkonfiguration angewendet wird.

- a Wenn eine bedeutende oder kritische Auswirkung auf iSCSI vorliegt, klicken Sie auf den Eintrag **iSCSI** und überprüfen Sie die Gründe, die im Bereich „Analysedetails“ angezeigt werden.
 - b Nachdem Sie die Auswirkung auf iSCSI behoben haben, fahren Sie mit der Netzwerkkonfiguration fort.
- 12 Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

Migrieren von VMkernel-Adaptoren zu einem vSphere Distributed Switch

Migrieren Sie VMkernel-Adapter auf einen Distributed Switch, wenn Sie den Datenverkehr für VMkernel-Dienste nur mit diesem Switch verwalten möchten und die Adapter auf anderen Standard-Switches oder Distributed Switches nicht mehr benötigen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.
- 3 Wählen Sie **Hostnetzwerk verwalten** aus und klicken Sie auf **Weiter**.

- 4 Klicken Sie auf **Angeschlossene Hosts** und wählen Sie aus den Hosts aus, die dem Distributed Switch zugeordnet sind.
- 5 Klicken Sie auf **Weiter**.
- 6 Wählen Sie **VMkernel-Adapter verwalten** aus und klicken Sie auf **Weiter**.
- 7 Wählen Sie den Adapter aus und klicken Sie auf **Portgruppe zuweisen**.
- 8 Wählen Sie eine verteilte Portgruppe aus und klicken Sie auf **OK**.
- 9 Klicken Sie auf **Weiter**.
- 10 Überprüfen Sie die betroffenen Dienste sowie den Auswirkungsgrad.

Option	Beschreibung
Keine Auswirkung	iSCSI funktioniert wie gewohnt, nachdem die neue Netzwerkkonfiguration angewendet wurde.
Wichtige Auswirkung	Die gewohnte Funktionsweise von iSCSI kann unterbrochen werden, wenn die neue Netzwerkkonfiguration angewendet wird.
Kritische Auswirkung	Die gewohnte Funktionsweise von iSCSI wird unterbrochen, wenn die neue Netzwerkkonfiguration angewendet wird.

- a Wenn eine bedeutende oder kritische Auswirkung auf iSCSI vorliegt, klicken Sie auf den Eintrag **iSCSI** und überprüfen Sie die Gründe, die im Bereich „Analysedetails“ angezeigt werden.
 - b Nachdem Sie die Auswirkung auf iSCSI behoben haben, fahren Sie mit der Netzwerkkonfiguration fort.
- 11 Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

Erstellen eines VMkernel-Adapters auf einem vSphere Distributed Switch

Erstellen Sie einen VMkernel-Adapter auf Hosts, die einem Distributed Switch zugeordnet sind, um eine Netzwerkverbindung für die Hosts bereitzustellen und den Datenverkehr für vSphere vMotion, IP-Speicher, Fault Tolerance-Protokollierung oder Virtual SAN zu regeln. Mit dem Assistenten **Hosts hinzufügen und verwalten** können Sie VMkernel-Adapter auf mehreren Hosts gleichzeitig erstellen.

Für jeden VMkernel-Adapter sollten Sie jeweils eine verteilte Portgruppe vorsehen. Ein VMkernel-Adapter sollte nur einen Datenverkehrstyp verwalten.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.
- 3 Wählen Sie **Hostnetzwerk verwalten** aus und klicken Sie auf **Weiter**.

- 4 Klicken Sie auf **Angeschlossene Hosts** und wählen Sie aus den Hosts aus, die dem Distributed Switch zugeordnet sind.
- 5 Klicken Sie auf **Weiter**.
- 6 Wählen Sie **VMkernel-Adapter verwalten** aus und klicken Sie auf **Weiter**.
- 7 Klicken Sie auf **Neuer Adapter**.

Der **Assistent zum Hinzufügen von Netzwerken** wird geöffnet.

- 8 Wählen Sie auf der Seite „Zielgerät auswählen“ des **Assistenten zum Hinzufügen von Netzwerken** eine verteilte Portgruppe aus.
- 9 Konfigurieren Sie auf der Seite „Porteigenschaften“ die Einstellungen für den VMkernel-Adapter.

Option	Beschreibung
Netzwerkbezeichnung	Als Netzwerkbezeichnung wird die Bezeichnung der verteilten Portgruppe übernommen.
IP-Einstellungen	<p>Wählen Sie IPv4, IPv6 oder beide aus.</p> <p>Hinweis Die IPv6-Option wird auf Hosts, bei denen IPv6 nicht aktiviert ist, nicht angezeigt.</p>

Option	Beschreibung
TCP/IP-Stack	Wählen Sie in der Liste einen TCP/IP-Stack aus. Der TCP/IP-Stack, den Sie für den VMkernel-Adapter festlegen, kann später nicht mehr geändert werden. Wenn Sie den vMotion- oder den Bereitstellungs-TCP/IP-Stack auswählen, können Sie nur diese Stacks für vMotion- oder Bereitstellungsdatenverkehr auf dem Host verwenden. Alle VMkernel-Adapter für vMotion im Standard-TCP/IP-Stack werden für zukünftige vMotion-Sitzungen deaktiviert. Wenn Sie den Bereitstellungs-TCP/IP-Stack festlegen, werden VMkernel-Adapter im Standard-TCP/IP-Stack für Vorgänge mit Bereitstellungsdatenverkehr deaktiviert, wie beispielsweise Cold-Migration, Klonen und Snapshot-Migration von virtuellen Maschinen.
Dienste aktivieren	<p>Für den Standard-TCP/IP-Stack auf dem Host können Dienste aktiviert werden. Zur Auswahl stehen die folgenden Dienste:</p> <ul style="list-style-type: none"> ■ vMotion-Datenverkehr – Dieser Dienst ermöglicht es, dass der VMkernel-Adapter sich einem anderen Host als die Netzwerkverbindung bekannt gibt, über die vMotion-Datenverkehr gesendet wird. Die Migration mit vMotion zum ausgewählten Host ist nicht möglich, wenn der vMotion-Dienst für keinen VMkernel-Adapter im Standard-TCP/IP-Stack aktiviert ist oder wenn keine Adapter den vMotion-TCP/IP-Stack verwenden. ■ Bereitstellungsdatenverkehr. Verarbeitet die übertragenen Daten für Cold-Migration, Klonen und Snapshot-Migration von virtuellen Maschinen. ■ Datenverkehr von Fault Tolerance – Aktiviert die Fault Tolerance-Protokollierung auf dem Host. Pro Host können Sie nur einen VMkernel-Adapter für FT-Datenverkehr verwenden. ■ Verwaltungsdatenverkehr – Ermöglicht den Verwaltungsdatenverkehr für den Host und vCenter Server. Üblicherweise verfügen Hosts über einen derartigen VMkernel-Adapter, der bei der Installation der ESXi-Software erstellt wird. Sie können zum Zweck der Redundanz einen weiteren VMkernel-Adapter für Verwaltungsdatenverkehr auf dem Host erstellen. ■ vSphere Replication-Datenverkehr. Verarbeitet die ausgehenden Replizierungsdaten, die vom ESXi-Quellhost an den vSphere Replication-Server gesendet werden. ■ vSphere Replication-NFC-Datenverkehr. Verarbeitet die eingehenden Replizierungsdaten auf der Zielreplizierungsseite. ■ Virtual SAN – Ermöglicht den Datenverkehr des Virtual SAN auf dem Host. Jeder Host, der Teil eines Clusters für Virtual SAN ist, muss über einen derartigen VMkernel-Adapter verfügen.

- 10 Wenn Sie den vMotion-TCP/IP-Stack oder den Bereitstellungs-Stack ausgewählt haben, klicken Sie im angezeigten Warnungsdiaologfeld auf **OK**.

Falls bereits eine Live-Migration gestartet wurde, wird diese erfolgreich abgeschlossen, selbst wenn die beteiligten VMkernel-Adapter im Standard-TCP/IP-Stack für vMotion deaktiviert wurden. Dies gilt auch für Vorgänge mit VMkernel-Adapttern im Standard-TCP/IP-Stack, die für den Bereitstellungsdatenverkehr festgelegt sind.

- 11 (Optional) Wählen Sie auf der Seite „IPv4-Einstellungen“ eine Option zum Abrufen von IP-Adressen aus.

Option	Beschreibung
IP-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IP-Einstellungen verwenden	Geben Sie die IPv4-Adresse und die Subnetzmaske für den VMkernel-Adapter ein. Das Standard-Gateway für VMkernel und die DNS-Server-Adressen für IPv4 werden vom ausgewählten TCP/IP-Stack bezogen.

- 12 (Optional) Wählen Sie auf der „Seite IPv6-Einstellungen“ eine Option zum Abrufen von IPv6-Adressen aus.

Option	Beschreibung
IPv6-Adressen automatisch mittels DHCP erhalten	Verwenden Sie DHCP zum Abrufen von IPv6-Adressen. Ein DHCPv6-Server muss im Netzwerk vorhanden sein.
IPv6-Adressen automatisch mittels Router-Ankündigung abrufen	Verwenden Sie die Router-Ankündigung zum Abrufen von IPv6-Adressen.
Statische IPv6-Adressen	<ul style="list-style-type: none"> a Klicken Sie auf Hinzufügen, um eine neue IPv6-Adresse hinzuzufügen. b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein und klicken Sie auf OK. c Klicken Sie auf Bearbeiten, um das Standard-Gateway des VMkernels zu ändern. <p>Die Adresse des Standard-Gateways für VMkernel für IPv6 wird vom ausgewählten TCP/IP-Stack bezogen.</p>

- 13 Überprüfen Sie Ihre Einstellungen auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Beenden**.
- 14 Folgen Sie den Eingabeaufforderungen, um den Assistenten abzuschließen.

Migrieren von Netzwerken virtueller Maschinen zu einem vSphere Distributed Switch

Für die Verwaltung von Netzwerken virtueller Maschinen mit einem Distributed Switch migrieren Sie Netzwerkadapter der virtuellen Maschine auf benannte Netzwerke auf dem Switch.

Voraussetzungen

Stellen Sie sicher, dass mindestens eine verteilte Portgruppe, die für Netzwerke virtueller Maschinen vorgesehen ist, auf dem Distributed Switch vorhanden ist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.
- 3 Wählen Sie **Hostnetzwerk verwalten** aus und klicken Sie auf **Weiter**.

- 4 Klicken Sie auf **Angeschlossene Hosts** und wählen Sie aus den Hosts aus, die dem Distributed Switch zugeordnet sind.
- 5 Klicken Sie auf **Weiter**.
- 6 Wählen Sie **Netzwerk von virtuellen Maschinen migrieren** aus und klicken Sie auf **Weiter**.
- 7 Konfigurieren Sie Netzwerkadapter der virtuellen Maschine für den Distributed Switch.
 - a Um alle Netzwerkadapter einer virtuellen Maschine mit einer verteilten Portgruppe zu verbinden, wählen Sie die virtuelle Maschine aus, oder wählen Sie einen einzelnen Netzwerkadapter aus, um nur diesen Adapter zu verbinden.
 - b Klicken Sie auf **Portgruppe zuweisen**.
 - c Wählen Sie eine verteilte Portgruppe aus der Liste aus und klicken Sie auf **OK**.
- 8 Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

Aktualisieren der maximalen Anzahl der verteilten Ports auf Hosts

Wenn auf einem Host ESXi 5.1 oder früher ausgeführt wird, können Sie die maximale Anzahl von verteilten Ports auf dem Proxy-Switch des Hosts ändern.

Jeder Proxy-Switch auf ESXi 5.1-Hosts (und früher) stellt eine bestimmte Anzahl von Ports bereit, über die virtuelle Maschinen und Netzwerkdienste auf mindestens ein Netzwerk zugreifen können. Sie müssen die Anzahl von Ports gemäß Ihren Bereitstellungsanforderungen manuell erhöhen oder verringern.

Hinweis Durch die Erhöhung der Anzahl von verteilten Ports der Proxy-Switches auf Hosts werden mehr Ressourcen auf den Hosts reserviert und verbraucht. Falls einige Ports nicht belegt sind, bleiben Hostressourcen, die möglicherweise für andere Vorgänge benötigt werden, gesperrt und ungenutzt.

Für eine effiziente Verwendung der Hostressourcen wird auf ESXi 5.5-Hosts und 6.0-Hosts die Anzahl der verteilten Ports von Proxy-Switches dynamisch nach oben und unten korrigiert. Ein Proxy-Switch auf einem solchen Host kann auf die maximale Anzahl von Ports, die auf dem Host unterstützt wird, erweitert werden. Der Portgrenzwert wird bestimmt anhand der maximalen Anzahl von virtuellen Maschinen, die der Host verarbeiten kann.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.
- 3 Wählen Sie **Hostnetzwerk verwalten** aus und klicken Sie auf **Weiter**.
- 4 Klicken Sie auf **Angeschlossene Hosts** und wählen Sie aus den Hosts aus, die dem Distributed Switch zugeordnet sind.
- 5 Klicken Sie auf **Weiter**.
- 6 Wählen Sie einen Host aus und klicken Sie auf **Einstellungen bearbeiten**.

- 7 Ändern Sie die maximale Anzahl von verteilten Ports auf dem Host und klicken Sie auf **OK**.
- 8 Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

Verwenden eines Hosts als Vorlage zur Erstellung einer einheitlichen Netzwerkkonfiguration auf einem vSphere Distributed Switch

Wenn Sie Hosts mit einheitlicher Netzwerkkonfiguration einrichten möchten, können Sie einen Host als Vorlage auswählen und seine Konfiguration für physische Netzwerkkarten und VMkernel-Adapter auf andere Hosts im Distributed Switch anwenden.

Verfahren

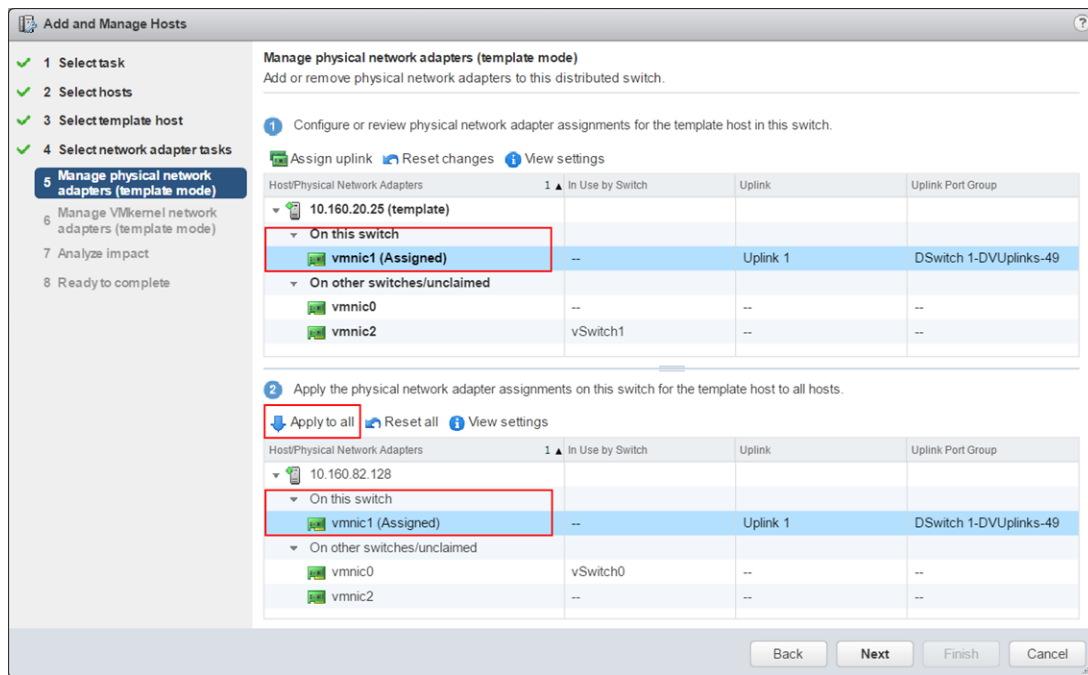
- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.
- 3 Wählen Sie eine Aufgabe zum Verwalten von Host-Netzwerkfunktionen aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie die Hosts aus, die dem Distributed Switch hinzugefügt oder dort verwaltet werden sollen.
- 5 Wählen Sie unten im Dialogfeld die Option **Konfigurieren Sie identische Netzwerkeinstellungen auf mehreren Hosts** aus und klicken Sie auf **Weiter**.
- 6 Wählen Sie einen Host aus, den Sie als Vorlage verwenden möchten, und klicken Sie auf **Weiter**.
- 7 Wählen Sie die Netzwerkadaptersaufgaben aus, und klicken Sie auf **Weiter**.
- 8 Ändern Sie auf den Seiten „Physische Netzwerkadapter verwalten“ und „VMkernel-Netzwerkadapter verwalten“ die für den Vorlagehost benötigten Konfigurationseinstellungen und klicken Sie für alle anderen Hosts auf **Auf alle anwenden**.
- 9 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Beenden**.

Beispiel: Konfigurieren von physischen Adaptern und VMkernel-Adaptoren mithilfe eines Vorlagenhosts

Mit dem Vorlagenhost-Modus im Assistenten **Hosts hinzufügen und verwalten** können Sie eine einheitliche Netzwerkkonfiguration für alle Hosts auf einem Distributed Switch einrichten.

Weisen Sie auf der Seite „Physische Netzwerkadapter verwalten“ des Assistenten zwei physische Netzwerkkarten zu Uplinks auf dem Vorlagenhost zu und klicken Sie dann auf **Auf alle anwenden**, um die gleiche Konfiguration auf dem anderen Host zu erstellen.

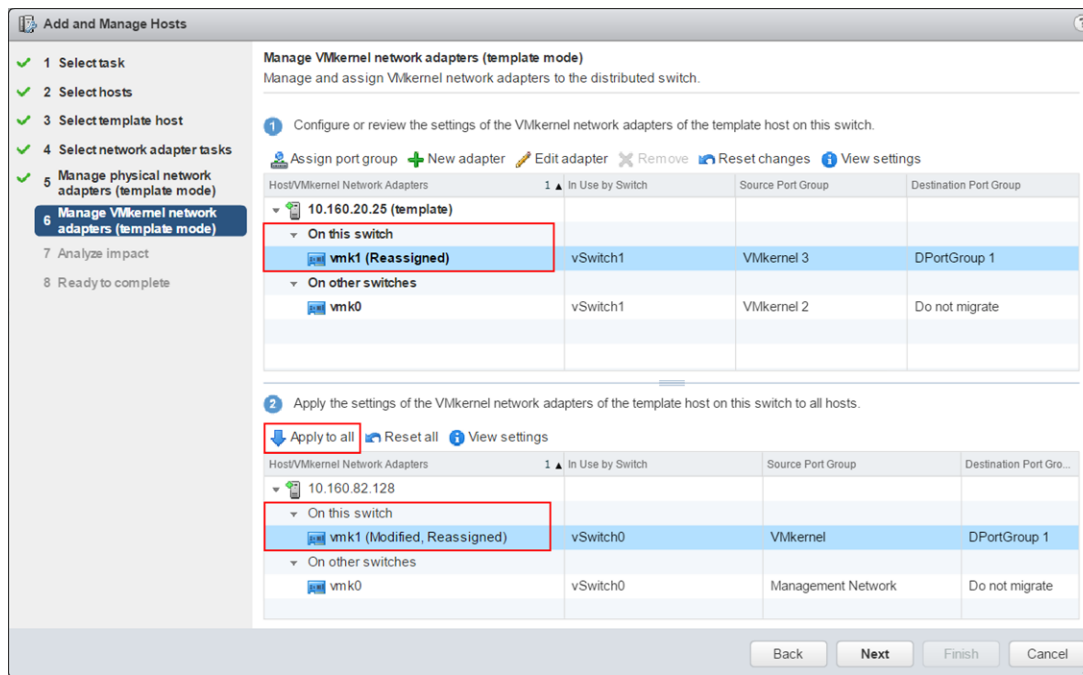
Abbildung 3-4. Anwenden der Konfiguration von physischen Netzwerkkarten auf einen vSphere Distributed Switch anhand eines Vorlagenhosts



Weisen Sie auf der Seite „VMkernel-Netzwerkadapter verwalten“ einen VMkernel-Adapter einer Portgruppe zu und klicken Sie auf **Auf alle anwenden**, um dieselbe Konfiguration auf den anderen Host anzuwenden.

Nachdem Sie auf die Schaltfläche **Auf alle anwenden** geklickt haben, weist der VMkernel-Zieladapter den Bezeichner „Geändert“ und „Neu zugewiesen“ auf. Der Bezeichner „Geändert“ wird angezeigt, weil vCenter Server beim Klicken auf die Schaltfläche **Auf alle anwenden** die Konfigurationsspezifikationen des Vorlagen-VMkernel-Adapters in den VMkernel-Zieladapter kopiert, selbst wenn die Konfigurationen des Vorlagenadapters und des Zieladapters identisch sind. Deshalb werden die Zieladapter stets geändert.

Abbildung 3-5. Anwenden der Konfiguration des VMkernel-Adapters auf einen vSphere Distributed Switch anhand eines Vorlagenhosts



Entfernen von Hosts aus einem vSphere Distributed Switch

Entfernen Sie Hosts von einem vSphere Distributed Switch, falls Sie einen anderen Switch für die Hosts konfiguriert haben.

Voraussetzungen

- Stellen Sie sicher, dass physische Netzwerkkarten auf den Zielhosts auf einen anderen Switch migriert werden.
- Stellen Sie sicher, dass VMkernel-Adapter auf den Hosts auf einen anderen Switch migriert werden.
- Stellen Sie sicher, dass Netzwerkadapter der virtuellen Maschine auf einen anderen Switch migriert werden.

Weitere Informationen zum Migrieren von Netzwerkadaptern auf andere Switches finden Sie unter [Aufgaben für das Verwalten von Host-Netzwerken auf einem vSphere Distributed Switch](#)

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.
- 3 Wählen Sie **Hosts entfernen** aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie die zu entfernenden Hosts aus, und klicken Sie auf **Weiter**.
- 5 Klicken Sie auf **Beenden**.

Verwalten von Netzwerken auf Host-Proxy-Switches

Sie können die Konfiguration des Proxy-Switches auf jedem Host ändern, der einem vSphere Distributed Switch zugeordnet ist. Sie können physische Netzwerkkarten, VMkernel-Adapter und Netzwerkadapter virtueller Maschinen verwalten.

Weitere Informationen zum Einrichten von VMkernel-Netzwerken auf Host-Proxy-Switches finden Sie unter [Erstellen eines VMkernel-Adapters auf einem vSphere Distributed Switch](#).

Migrieren von Netzwerkadaptern auf einem Host zu einem vSphere Distributed Switch

Für Hosts, die einem Distributed Switch zugeordnet sind, können Sie Netzwerkadapter von einem Standard-Switch auf den Distributed Switch migrieren. Sie können physische Netzwerkkarten, VMkernel-Adapter und VM-Netzwerkadapter gleichzeitig migrieren.

Wenn Sie VM-Netzwerkadapter oder VMkernel-Adapter migrieren, stellen Sie sicher, dass die verteilten Zielportgruppen über mindestens einen aktiven Uplink verfügen und dass der Uplink mit einer physischen Netzwerkkarte auf diesem Host verbunden ist. Alternativ können Sie physische Netzwerkkarten, virtuelle Netzwerkadapter und VMkernel-Adapter gleichzeitig migrieren.

Wenn Sie physische Netzwerkkarten migrieren möchten, müssen Sie sicherstellen, dass die Quellportgruppen auf dem Standard-Switch mindestens eine physische Netzwerkkarte zur Verarbeitung des Datenverkehrs aufweisen. Angenommen, Sie migrieren eine physische Netzwerkkarte, die einer Portgruppe für das Netzwerk der virtuellen Maschine zugewiesen ist. Stellen Sie in diesem Fall sicher, dass die Portgruppe mit mindestens einer physischen Netzwerkkarte verbunden ist. Andernfalls sind die virtuellen Maschinen im selben VLAN auf dem Standard-Switch zwar miteinander verbunden, jedoch nicht mit dem externen Netzwerk.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie den als Ziel verwendeten Distributed Switch aus und klicken Sie auf **Physische oder virtuelle Netzwerkadapter migrieren**.
- 4 Wählen Sie die Aufgaben zum Migrieren von Netzwerkadaptern aus und klicken Sie auf **Weiter**.
- 5 Konfigurieren Sie physische Netzwerkkarten.
 - a Wählen Sie aus der Liste **Auf anderen Switches/frei** eine physische Netzwerkkarte aus und klicken Sie auf **Uplink zuweisen**.
 - b Wählen Sie einen Uplink aus und klicken Sie auf **OK**.
 - c Klicken Sie auf **Weiter**.

6 Konfigurieren Sie VMkernel-Adapter.

- a Wählen Sie einen Adapter aus und klicken Sie auf **Portgruppe zuweisen**.
- b Wählen Sie eine verteilte Portgruppe aus und klicken Sie auf **OK**.

Sie sollten jeweils einen VMkernel-Adapter mit einer verteilten Portgruppe verbinden.

- c Klicken Sie auf **Weiter**.

7 Überprüfen Sie die Dienste, die von der neuen Netzwerkkonfiguration betroffen sind.

- a Wenn eine wichtige oder kritische Auswirkung für einen Dienst gemeldet wird, klicken Sie auf den Dienst und überprüfen Sie die Analysedetails.

Beispielsweise könnte eine wichtige Auswirkung für iSCSI aufgrund einer fehlerhaften Teaming- und Failover-Konfiguration für die verteilte Portgruppe, in der Sie den iSCSI-VMkernel-Adapter migrieren, gemeldet werden. Ein aktiver Uplink muss in der Teaming- und Failover-Reihenfolge der verteilten Portgruppe vorhanden bleiben, die Standbyliste muss leer sein und die restlichen Uplinks müssen in die nicht verwendeten Uplinks verschoben werden.

- b Klicken Sie nach der Behebung von Auswirkungen auf die betroffenen Dienste auf **Weiter**.

8 Konfigurieren Sie VM-Netzwerkadapter.

- a Wählen Sie eine virtuelle Maschine oder einen VM-Netzwerkadapter aus und klicken Sie auf **Portgruppe zuweisen**.

Wenn Sie eine virtuelle Maschine auswählen, migrieren Sie alle Netzwerkadapter auf der virtuellen Maschine. Wenn Sie einen Netzwerkadapter auswählen, migrieren Sie nur diesen Netzwerkadapter.

- b Wählen Sie eine verteilte Portgruppe aus der Liste aus und klicken Sie auf **OK**.
- c Klicken Sie auf **Weiter**.

9 Überprüfen Sie auf der Seite „Bereit zum Abschließen“ die neue Netzwerkkonfiguration und klicken Sie auf **Beenden.**

Migrieren eines VMkernel-Adapters auf einem Host zu einem vSphere Standard-Switch

Wenn ein Host einem Distributed Switch zugeordnet ist, können Sie VMkernel-Adapter von dem Distributed Switch auf einen Standard-Switch migrieren.

Weitere Informationen zum Erstellen von VMkernel-Adaptoren auf einem vSphere Distributed Switch finden Sie unter [Erstellen eines VMkernel-Adapters auf einem vSphere Distributed Switch](#).

Voraussetzungen

Stellen Sie sicher, dass der Ziel-Standard-Switch über mindestens eine physische Netzwerkkarte verfügt.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie den Ziel-Standard-Switch aus der Liste aus.
- 4 Klicken Sie auf **VMkernel-Adapter migrieren**.
- 5 Wählen Sie auf der Seite „VMkernel-Netzwerkadapter auswählen“ aus der Liste den virtuellen Netzwerkadapter aus, der auf den Standard-Switch migriert werden soll.
- 6 Bearbeiten Sie auf der Seite „Einstellungen konfigurieren“ die **Netzwerkbezeichnung** und die **VLAN-ID** für den Netzwerkadapter.
- 7 Überprüfen Sie die Migrationsdetails auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Beenden**.

Klicken Sie auf **Zurück**, um die Einstellungen zu bearbeiten.

Zuweisen einer physischen Netzwerkkarte eines Hosts zu einem vSphere Distributed Switch

Sie können physische Netzwerkkarten eines Hosts, der mit einem Distributed Switch verbunden ist, zum Uplink-Port auf dem Host-Proxy-Switch zuweisen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie einen Distributed Switch aus der Liste aus.
- 4 Klicken Sie auf **Physische Netzwerkadapter verwalten**.
- 5 Wählen Sie einen freien Uplink aus der Liste aus und klicken Sie auf **Adapter hinzufügen**.
- 6 Wählen Sie eine physische Netzwerkkarte aus und klicken Sie auf **OK**.

Entfernen einer physischen Netzwerkkarte aus einem vSphere Distributed Switch

Sie können eine physische Netzwerkkarte eines Hosts aus einem Uplink auf einem vSphere Distributed Switch entfernen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.

- 3 Wählen Sie den Distributed Switch aus.
- 4 Klicken Sie auf **Physische Netzwerkkarten verwalten**.
- 5 Wählen Sie einen Uplink aus und klicken Sie auf **Ausgewählte Adapter entfernen**.
- 6 Klicken Sie auf **OK**.

Nächste Schritte

Wenn Sie physische Netzwerkkarten aus aktiven virtuellen Maschinen entfernen, sehen Sie möglicherweise, dass die entfernten Netzwerkkarten im vSphere Web Client angezeigt werden. Weitere Informationen hierzu finden Sie unter [Entfernen von NICs von den aktiven virtuellen Maschinen](#).

Festlegen der Anzahl der Ports auf einem Host-Proxy-Switch

Sie können die Höchstzahl der verteilten Ports, die am Proxy-Switch von ESXi 5.1-Hosts und niedriger verfügbar sind und die mit einem vSphere Distributed Switch verbunden sind, erhöhen oder senken.

Jeder Proxy-Switch auf Hosts, die ESXi 5.1 und niedriger ausführen, stellt eine endliche Anzahl Ports bereit, über die virtuelle Maschinen und Netzwerkdienste ein oder mehrere Netzwerke erreichen können. Sie müssen die Anzahl von Ports gemäß Ihren Bereitstellungsanforderungen manuell erhöhen oder verringern.

Hinweis Durch die Erhöhung der Anzahl von verteilten Ports der Proxy-Switches auf Hosts werden mehr Ressourcen auf den Hosts reserviert und verbraucht. Falls einige Ports nicht belegt sind, bleiben Hostressourcen, die möglicherweise für andere Vorgänge benötigt werden, gesperrt und ungenutzt.

Für eine effiziente Verwendung der Hostressourcen wird auf ESXi 5.5-Hosts und 6.0-Hosts die Anzahl der verteilten Ports von Proxy-Switches dynamisch nach oben und unten korrigiert. Ein Proxy-Switch auf einem solchen Host kann auf die maximale Anzahl von Ports, die auf dem Host unterstützt wird, erweitert werden. Der Portgrenzwert wird bestimmt anhand der maximalen Anzahl von virtuellen Maschinen, die der Host verarbeiten kann.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie einen Distributed Switch aus der Liste aus.
- 4 Klicken Sie auf **Die maximale Anzahl an verteilten Ports auf diesem Host aktualisieren**.
- 5 Stellen Sie mit den Pfeilen nach oben und unten die maximale Anzahl von Ports für den Host ein, und klicken Sie auf **OK**.

Nächste Schritte

Wenn Sie die maximale Anzahl an Ports für einen Host ändern, nachdem der Host zum Distributed Switch hinzugefügt wurde, müssen Sie den Host neu starten, bevor der neue Maximalwert wirksam wird.

Entfernen von NICs von den aktiven virtuellen Maschinen

Wenn Sie Netzwerkkarten (NICs) aus aktiven virtuellen Maschinen entfernen, werden die entfernten Netzwerkkarten möglicherweise weiterhin im vSphere Web Client angezeigt.

Entfernen von Netzwerkkarten von einer aktiven virtuellen Maschine ohne installiertes Gastbetriebssystem

Sie können Netzwerkkarten nicht von einer aktiven virtuellen Maschine entfernen, auf der kein Betriebssystem installiert ist.

Der vSphere Web Client meldet möglicherweise, dass die Netzwerkkarte entfernt wurde, aber sie wird weiterhin als der virtuellen Maschine zugehörig angezeigt.

Entfernen von Netzwerkkarten von einer aktiven virtuellen Maschine mit installiertem Gastbetriebssystem

Sie können eine Netzwerkkarte von einer aktiven virtuellen Maschine entfernen, aber dies wird dem vSphere Web Client möglicherweise erst einige Zeit später gemeldet. Wenn Sie für die virtuelle Maschine auf **Einstellungen bearbeiten** klicken, wird die entfernte Netzwerkkarte möglicherweise weiterhin angezeigt, selbst wenn die Aufgabe abgeschlossen ist. Das Dialogfeld „Einstellungen bearbeiten“ für die virtuelle Maschine zeigt die Netzwerkkarte nicht sofort als entfernt an.

Die Netzwerkkarte wird möglicherweise weiterhin als der virtuellen Maschine zugeordnet angezeigt, wenn das Gastbetriebssystem der virtuellen Maschine das Entfernen von Netzwerkkarten im laufenden Betrieb nicht unterstützt.

Verteilte Portgruppen

Eine verteilte Portgruppe gibt Port-Konfigurationsoptionen für jeden Port der Portgruppe auf einem vSphere Distributed Switch an. Verteilte Portgruppen legen fest, wie eine Verbindung zum Netzwerk hergestellt wird.

Hinzufügen einer verteilten Portgruppe

Fügen Sie eine verteilte Portgruppe zu einem vSphere Distributed Switch hinzu, um ein Distributed Switch-Netzwerk für Ihre virtuellen Maschinen zu erstellen und VMkernel-Adapter zuzuordnen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.

- 2 Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Verteilte Portgruppe > Neue verteilte Portgruppe** aus.
- 3 Geben Sie im Abschnitt **Name und Speicherort auswählen** den Namen der neuen verteilten Portgruppe ein oder akzeptieren Sie den generierten Namen und klicken Sie auf **Weiter**.
- 4 Legen Sie im Abschnitt **Einstellungen konfigurieren** die allgemeinen Eigenschaften für die neue verteilte Portgruppe fest und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Port-Bindung	<p>Wählen Sie aus, wann Ports virtuellen Maschinen zugewiesen werden, die mit dieser verteilten Portgruppe verbunden sind.</p> <ul style="list-style-type: none"> ■ Statische Bindung: Weisen Sie einer virtuellen Maschine einen Port zu, wenn die virtuelle Maschine mit der verteilten Portgruppe verbunden wird. ■ Dynamische Bindung: Weisen Sie einer virtuellen Maschine einen Port zu, wenn die virtuelle Maschine zum ersten Mal eingeschaltet wird, nachdem sie mit der verteilten Portgruppe verbunden wurde. Die dynamische Bindung läuft seit ESXi 5.0 aus. ■ Flüchtig: Keine Port-Bindung. Sie können einer verteilten Portgruppe mit einer temporären Port-Bindung eine virtuelle Maschine auch dann zuweisen, wenn sie mit dem Host verbunden ist.
Portzuteilung	<ul style="list-style-type: none"> ■ Elastisch: Die Standardanzahl der Ports ist acht. Wenn alle Ports zugewiesen wurden, wird ein neues Set aus acht Ports erstellt. Dies ist die Standardeinstellung. ■ Fest: Die Standardanzahl der Ports ist auf acht festgelegt. Es werden keine weiteren Ports angelegt, wenn alle Ports zugewiesen wurden.
Anzahl der Ports	Geben Sie die Anzahl der Ports in der verteilten Portgruppe ein.
Netzwerkressourcenpool	Über das Dropdown-Menü können Sie die neue verteilte Portgruppe einem benutzerdefinierten Netzwerkressourcenpool zuweisen. Wenn Sie keinen Netzwerkressourcenpool erstellt haben, bleibt dieses Menü leer.
VLAN	<p>Verwenden Sie das Dropdown-Menü Typ, um die VLAN-Optionen auszuwählen:</p> <ul style="list-style-type: none"> ■ Keine: Verwenden Sie VLAN nicht. ■ VLAN: Geben Sie im Feld VLAN-ID eine Zahl zwischen 1 und 4094 ein. ■ VLAN-Trunking: Geben Sie einen VLAN-Trunk-Bereich ein. ■ Privates VLAN: Wählen Sie einen Eintrag für ein privates VLAN. Wenn Sie keine privaten VLANs erstellt haben, bleibt dieses Menü leer.
Erweitert	Aktivieren Sie dieses Kontrollkästchen, um die Richtlinienkonfigurationen für die neue verteilte Portgruppe anzupassen.

- 5 (Optional) Bearbeiten Sie im Abschnitt **Sicherheit** die Sicherheitsausnahmen und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Promiscuous-Modus	<ul style="list-style-type: none"> ■ Ablehnen. Wenn ein Adapter von einem Gastbetriebssystem in den Promiscuous-Modus versetzt wird, führt dies dazu, dass keine Frames für andere virtuelle Maschinen empfangen werden. ■ Akzeptieren. Wenn ein Adapter von einem Gastbetriebssystem in den Promiscuous-Modus versetzt wird, ermöglicht der Switch es dem Gastadapter, alle Frames, die am Switch übergeben werden, in Einhaltung der aktiven VLAN-Richtlinie für den Port, an den der Adapter angeschlossen ist, zu empfangen. <p>Firewalls, Portscanner, Erkennungssysteme für Eindringversuche usw. müssen im Promiscuous-Modus ausgeführt werden.</p>
MAC-Adressänderungen	<ul style="list-style-type: none"> ■ Ablehnen. Wenn Sie diese Option auf Ablehnen festlegen und das Gastbetriebssystem die MAC-Adresse des Adapters in einen anderen Wert als die Adresse in der Konfigurationsdatei ändert (.vmx), verwirft der Switch alle eingehenden Frames an den Adapter der virtuellen Maschine. . <p>Wenn das Gastbetriebssystem die MAC-Adresse zurück ändert, empfängt die virtuelle Maschine wieder Frames.</p> <ul style="list-style-type: none"> ■ Akzeptieren. Wenn das Gastbetriebssystem die MAC-Adresse eines Netzwerkadapters ändert, empfängt der Adapter Frames an der neuen Adresse.
Gefälschte Übertragungen	<ul style="list-style-type: none"> ■ Ablehnen. Der Switch verwirft alle ausgehenden Frames mit einer Quell-MAC-Adresse, die von der Adresse in der .vmx-Konfigurationsdatei abweicht. ■ Akzeptieren. Der Switch führt keine Filterung durch und lässt alle ausgehenden Frames zu.

- 6 (Optional) Aktivieren oder deaktivieren Sie im Abschnitt **Traffic-Shaping** entweder „Ingress-Traffic-Shaping“ oder „Egress-Traffic-Shaping“ und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Status	Wenn Sie entweder Ingress-Traffic-Shaping oder Egress-Traffic-Shaping aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für alle mit der betreffenden Portgruppe verknüpften virtuellen Adapter. Wenn Sie die Richtlinie deaktivieren, besteht für Dienste standardmäßig eine uneingeschränkte Verbindung zum physischen Netzwerk.
Durchschnittliche Bandbreite	Legt fest, wie viele Bit pro Sekunde im Durchschnitt einen Port durchlaufen dürfen. Bei diesem Wert handelt es sich um die zulässige durchschnittliche Last.

Einstellung	Beschreibung
Spitzenbandbreite	Die maximale Zahl der Bit pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet und empfängt. Dies begrenzt die Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet.
Burstgröße	Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte ihm zugeteilte Bandbreite nutzt. Immer wenn dieser Port mehr Bandbreite benötigt als von der Einstellung Durchschnittliche Bandbreite angegeben, kann er möglicherweise vorübergehend Daten mit einer höheren Geschwindigkeit übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt werden und somit mit einer höheren Geschwindigkeit übertragen werden können.

- 7 (Optional) Bearbeiten Sie im Abschnitt **Teaming und Failover** die Einstellungen und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Lastausgleich	<p>Geben Sie an, wie ein Uplink ausgewählt werden soll.</p> <ul style="list-style-type: none"> ■ Anhand des ursprünglichen virtuellen Ports routen. Wählen Sie den Uplink basierend auf dem virtuellen Port, durch den der Datenverkehr in den Distributed Switch gelangt ist. ■ Anhand des IP-Hashs routen. Wählen Sie einen Uplink anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets aus. Bei Paketen ohne IP wird zur Berechnung des Hashs der Wert verwendet, der im Offset eingetragen ist. ■ Anhand des Quell-MAC-Hashs routen. Wählen Sie einen Uplink anhand eines Hashs des Quell-Ethernets aus. ■ Anhand der physischen Netzwerkkartenauslastung routen. Wählen Sie einen Uplink auf Grundlage der aktuellen Auslastungen der physischen Netzwerkkarten. ■ Ausdrückliche Failover-Reihenfolge verwenden. Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Ermittlungskriterien erfüllt. <p>Hinweis Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit „etherchannel“ konfiguriert wird. Deaktivieren Sie „etherchannel“ bei allen anderen Optionen.</p>
Netzwerk-Failover-Ermittlung	<p>Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an.</p> <ul style="list-style-type: none"> ■ Nur Verbindungsstatus. Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt, nicht jedoch Konfigurationsfehler, z. B. die Blockierung eines Ports des physischen Switches durch STP (Spanning Tree Protocol), eine Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel an der anderen Seite eines physischen Switches. ■ Signalprüfung. Sendet Signale, wartet auf Signalprüfpakete auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. Dadurch können viele der zuvor genannten Ausfälle erkannt werden, die durch den Verbindungsstatus allein nicht erkannt werden können. <p>Hinweis Verwenden Sie die Signalprüfung nicht zusammen mit dem IP-Hash-Lastausgleich.</p>

Einstellung	Beschreibung
Switches benachrichtigen	<p>Wählen Sie Ja oder Nein, um Switches bei einem Failover zu benachrichtigen. Wenn Sie Ja wählen, wird jedes Mal, wenn eine virtuelle Netzwerkkarte an einen Distributed Switch angeschlossen wird oder ein Failover-Ereignis dazu führt, dass der Datenverkehr einer virtuellen Netzwerkkarte über eine andere physische Netzwerkkarte geleitet wird, über das Netzwerk eine Benachrichtigung gesendet, um die Verweistabellen auf physischen Switches zu aktualisieren. In fast allen Fällen ist dies wünschenswert, um die Wartezeiten für Failover-Ereignisse und Migrationen mit vMotion zu minimieren.</p> <p>Hinweis Verwenden Sie diese Option nicht, wenn die an die Portgruppe angeschlossenen virtuellen Maschinen den Netzwerklastausgleich (NLB) von Microsoft im Unicast-Modus verwenden. Im Multicast-Modus von NLB treten keine Probleme auf.</p>
Failback	<p>Wählen Sie Ja oder Nein, um die Failback-Funktion zu deaktivieren bzw. zu aktivieren.</p> <p>Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Wenn die Option auf Ja (Standard) gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert. Er ersetzt in diesem Fall den ggf. vorhandenen Ersatzadapter, der seinen Platz eingenommen hatte. Wenn diese Option auf Nein gesetzt wurde, bleibt ein ausgefallener Adapter nach der Wiederherstellung seiner Funktionsfähigkeit deaktiviert, bis der gegenwärtig aktive Adapter ausfällt und ersetzt werden muss.</p>
Failover-Reihenfolge	<p>Geben Sie an, wie die Verarbeitungslast für Uplinks verteilt werden soll. Um bestimmte Uplinks zu verwenden und andere für Notfälle zu reservieren, z. B. wenn die verwendeten Uplinks ausfallen, legen Sie diese Bedingung fest, indem Sie sie in unterschiedliche Gruppen verschieben:</p> <ul style="list-style-type: none"> ■ Aktive Uplinks. Dieser Uplink wird weiter verwendet, wenn die Verbindung zum Netzwerkadapter hergestellt und aktiv ist. ■ Standby-Uplinks. Dieser Uplink wird verwendet, wenn mindestens eine Verbindung zum aktiven Adapter nicht verfügbar ist. ■ Nicht verwendete Uplinks. Verwenden Sie diesen Uplink nicht. <p>Hinweis Wenn Sie den IP-Hash-Lastausgleich verwenden, konfigurieren Sie keine Standby-Uplinks.</p>

- 8 (Optional) Aktivieren oder deaktivieren Sie im Abschnitt **Überwachen** die Option „NetFlow“ und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Deaktiviert	NetFlow ist für die verteilte Portgruppe deaktiviert.
Aktiviert	NetFlow ist für die verteilte Portgruppe aktiviert. NetFlow-Einstellungen können auf der Ebene der vSphere Distributed Switches konfiguriert werden.

- 9 (Optional) Wählen Sie im Abschnitt **SonstigesJa** oder **Nein** und klicken Sie auf **Weiter**.

Wenn Sie **Ja** wählen, werden alle Ports in der Portgruppe deaktiviert. Durch diese Aktion wird möglicherweise der normale Netzwerkbetrieb auf den Hosts oder virtuellen Maschinen gestört, die die Ports verwenden.

- 10 (Optional) Fügen Sie im Abschnitt **Weitere Einstellungen bearbeiten** eine Beschreibung der Portgruppe hinzu, legen Sie eventuelle Außerkraftsetzungen von Richtlinien pro Port fest und klicken Sie auf **Weiter**.
- 11 Überprüfen Sie Ihre Einstellungen im Abschnitt **Bereit zum Abschließen** und klicken Sie auf **Beenden**.

Klicken Sie auf **Zurück**, wenn Sie Ihre Einstellungen ändern möchten.

Bearbeiten der allgemeinen Einstellungen von verteilten Portgruppen

Sie können die allgemeinen Einstellungen für verteilte Portgruppen bearbeiten, beispielsweise den Namen der verteilten Portgruppe, die Porteinstellungen und den Netzwerkressourcenpool.

Verfahren

- 1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**.
- 2 Klicken Sie mit der rechten Maustaste auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Allgemein** aus, um die folgenden Einstellungen für verteilte Portgruppen zu bearbeiten.

Option	Beschreibung
Name	Dies ist der Name der verteilten Portgruppe. Sie können den Namen im Textfeld bearbeiten.
Port-Bindung	<p>Wählen Sie aus, wann Ports virtuellen Maschinen zugewiesen werden, die mit dieser verteilten Portgruppe verbunden sind.</p> <ul style="list-style-type: none"> ■ Statische Bindung: Weisen Sie einer virtuellen Maschine einen Port zu, wenn die virtuelle Maschine mit der verteilten Portgruppe verbunden wird. ■ Dynamische Bindung: Weisen Sie einer virtuellen Maschine einen Port zu, wenn die virtuelle Maschine zum ersten Mal eingeschaltet wird, nachdem sie mit der verteilten Portgruppe verbunden wurde. Die dynamische Bindung läuft seit ESXi 5.0 aus. ■ Flüchtig: Keine Port-Bindung. Sie können auch eine virtuelle Maschine einer verteilten Portgruppe mit temporärer Port-Bindung während der Verbindung mit dem Host zuweisen.

Option	Beschreibung
Portzuteilung	<ul style="list-style-type: none"> ■ Elastisch: Die Standardanzahl der Ports ist auf acht festgelegt. Wenn alle Ports zugewiesen wurden, wird ein neues Set aus acht Ports erstellt. Dies ist die Standardeinstellung. ■ Fest: Die Standardanzahl der Ports ist auf acht festgelegt. Es werden keine weiteren Ports angelegt, wenn alle Ports zugewiesen wurden.
Anzahl der Ports	Geben Sie die Anzahl der Ports in der verteilten Portgruppe ein.
Netzwerkressourcenpool	Über das Dropdown-Menü können Sie die neue verteilte Portgruppe einem benutzerdefinierten Netzwerkressourcenpool zuweisen. Wenn Sie keinen Netzwerkressourcenpool erstellt haben, bleibt dieses Menü leer.
Beschreibung	Geben Sie im Beschreibungsfeld beliebige Informationen zur verteilten Portgruppe ein.

4 Klicken Sie auf **OK**.

Entfernen einer verteilten Portgruppe

Entfernen Sie eine verteilte Portgruppe, wenn Sie das entsprechende benannte Netzwerk nicht länger zur Bereitstellung der Konnektivität und zum Konfigurieren von Verbindungseinstellungen für virtuelle Maschinen oder VMkernel-Netzwerke benötigen.

Voraussetzungen

- Vergewissern Sie sich, dass alle mit dem entsprechenden benannten Netzwerk verbundenen virtuellen Maschinen in ein anderes benanntes Netzwerk migriert worden sind.
- Vergewissern Sie sich, dass alle mit der verteilten Portgruppe verbundenen VMkernel-Adapter in eine andere Portgruppe migriert oder gelöscht worden sind.

Verfahren

- Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
 - Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - Klicken Sie auf **Verteilte Portgruppen**.
- Wählen Sie die verteilte Portgruppe aus.
- Wählen Sie im Menü **Aktionen** die Option **Löschen** aus.

Arbeiten mit verteilten Ports

Ein verteilter Port ist ein Port auf einem vSphere Distributed Switch, der eine Verbindung zum VMkernel oder zum Netzwerkadapter einer virtuellen Maschine herstellt.

Die Standardkonfiguration für verteilte Ports wird durch die Einstellungen für die verteilte Portgruppe festgelegt, aber für einzelne verteilte Ports können einige Einstellungen außer Kraft gesetzt werden.

Überwachen des Status von verteilten Ports

vSphere kann verteilte Ports überwachen und Informationen zum aktuellen Zustand und zu den Laufzeitstatistiken eines jeden Ports liefern.

Verfahren

- 1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**.
- 2 Wählen Sie eine verteilte Portgruppe aus.
- 3 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Ports**.
- 4 Klicken Sie auf **Port-Zustand-Überwachung starten**.

Die Porttabelle für die verteilte Portgruppe zeigt Laufzeitstatistiken für jeden verteilten Port an.

Die Spalte **Zustand** gibt den aktuellen Zustand der verteilten Ports an.

Option	Beschreibung
Link aktiviert	Die Verbindung für diesen verteilten Port ist aktiv.
Link deaktiviert	Die Verbindung für diesen verteilten Port ist nicht aktiv.
Blockiert	Dieser verteilte Port ist blockiert.
--	Der Zustand dieses verteilten Ports ist derzeit nicht verfügbar.

Konfigurieren der Einstellungen für verteilte Ports

Sie können allgemeine Einstellungen für verteilte Ports ändern, wie z. B. Portnamen und -beschreibung.

Verfahren

- 1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**.
- 2 Wählen Sie eine verteilte Portgruppe aus.
- 3 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Ports**.
- 4 Wählen Sie einen Distributed Port aus der Tabelle aus.

Am unteren Rand des Bildschirms werden Informationen zum verteilten Port angezeigt.
- 5 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.

- 6 Bearbeiten Sie auf der Seite **Eigenschaften** und auf den Richtlinienseiten die Informationen zum verteilten Port und klicken Sie auf **OK**.

Wenn Außerkraftsetzungen nicht zulässig sind, sind die Richtlinienoptionen deaktiviert.

Sie können Außerkraftsetzungen auf Portebene zulassen, indem Sie die Optionen unter **Erweiterte Einstellungen** der verteilten Portgruppe ändern. Weitere Informationen hierzu finden Sie unter [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Konfigurieren von Netzwerken von virtuellen Maschinen auf einem vSphere Distributed Switch

Verbinden Sie virtuelle Maschinen mit einem vSphere Distributed Switch entweder durch die Konfiguration einer individuellen virtuellen Netzwerkkarte oder durch die Migration von Gruppen virtueller Maschinen vom vSphere Distributed Switch selbst.

Verbinden Sie virtuelle Maschinen mit vSphere Distributed Switches, indem Sie die ihnen zugewiesenen virtuellen Netzwerkkarten mit verteilten Portgruppen verbinden. Dies kann entweder für eine individuelle virtuelle Maschine durch Ändern der Konfiguration des Netzwerkkartens der virtuellen Maschine oder für eine Gruppe von virtuellen Maschinen durch ihre Migration von einem vorhandenen virtuellen Netzwerk auf einen vSphere Distributed Switch geschehen.

Migrieren von virtuellen Maschinen auf einen oder von einem vSphere Distributed Switch

Zusätzlich zum Verbinden einzelner virtueller Maschinen mit einem Distributed Switch können Sie eine Gruppe von virtuellen Maschinen zwischen vSphere Distributed Switch- und einem vSphere Standard Switch-Netzwerk migrieren.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zu einem Datencenter.
- 2 Klicken Sie mit der rechten Maustaste auf das Datencenter im Navigator und wählen Sie **VM auf ein anderes Netzwerk migrieren**.
- 3 Wählen Sie ein Quellnetzwerk aus.
 - Wählen Sie **Spezifisches Netzwerk** und verwenden Sie die Schaltfläche **Durchsuchen**, um ein spezifisches Quellnetzwerk auszuwählen.
 - Wählen Sie **Kein Netzwerk** aus, um alle Netzwerkkarten von virtuellen Maschinen auszuwählen, die nicht mit einem anderen Netzwerk verbunden sind.
- 4 Wählen Sie **Durchsuchen**, um ein Zielnetzwerk auszuwählen, und klicken Sie auf **Weiter**.
- 5 Wählen Sie virtuelle Maschinen aus der Liste aus, die vom Quellnetzwerk in das Zielnetzwerk migriert werden sollen, und klicken Sie auf **Weiter**.

- 6 Überprüfen Sie Ihre Auswahl und klicken Sie auf **Beenden**.

Klicken Sie auf **Zurück**, um die Auswahl zu bearbeiten.

Verbinden einer individuellen virtuellen Maschine mit einer verteilten Portgruppe

Verbinden Sie eine einzelne virtuelle Maschine durch Ändern der Netzwerkkartenkonfiguration der virtuellen Maschine mit einem vSphere Distributed Switch.

Verfahren

- 1 Ermitteln Sie die virtuelle Maschine im vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus der Liste aus.
- 2 Wählen Sie auf der Registerkarte **Verwalten** der virtuellen Maschine **Einstellungen > VM-Hardware** aus.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Erweitern Sie den Abschnitt **Netzwerkadapter** und wählen Sie eine verteilte Portgruppe aus dem Dropdown-Menü aus.
- 5 Klicken Sie auf **OK**.

Topologie-Diagramme eines vSphere Distributed Switch im vSphere Web Client

Die Topologie-Diagramme eines vSphere Distributed Switch im vSphere Web Client zeigen die Struktur von VM-Adaptoren, VMkernel-Adaptoren und physischen Adaptoren im Switch.

Sie können die in Portgruppen angeordneten Komponenten, deren Datenverkehr vom Switch verarbeitet wird, und die Verbindungen zwischen diesen untersuchen. Das Diagramm zeigt Informationen über den physischen Adapter an, der die virtuellen Adapter mit dem externen Netzwerk verbindet.

Sie können die Komponenten anzeigen, die auf dem gesamten Distributed Switch und auf jedem Host, der an diesem teilnimmt, ausgeführt werden.

Das Video enthält Informationen über die Vorgänge, die Sie über das Topologie-Diagramm von vSphere Distributed Switch ausführen können.



Umgang mit virtuellen Netzwerken durch Verwendung des VDS-Topologie-Diagramms (https://vmwaretv.vmware.com/media/t/1_9umngsr4)

Zentrales Topologie-Diagramm

Sie können das zentrale Topologie-Diagramm des Switch verwenden, um die Einstellungen für verteilte Portgruppen und Uplink-Gruppen, die mehreren Hosts zugeordnet sind, zu suchen und zu bearbeiten. Sie können eine Migration von VM-Adaptern aus einer Portgruppe zu einem Ziel auf demselben oder auf einem anderen Switch initiieren. Sie können die Hosts und deren Netzwerke auf dem Switch neu organisieren, indem Sie den Assistenten **Hosts hinzufügen und verwalten** verwenden.

Topologie-Diagramm eines Host-Proxy-Switch

Das Topologie-Diagramm eines Host-Proxy-Switch zeigt die Adapter, die mit den Switch-Ports auf dem Host verbunden sind. Sie können die Einstellungen des VMkernel- und physischen Adapters bearbeiten.

Diagrammfilter

Sie können Diagrammfilter verwenden, um die im Topologie-Diagramm angezeigten Informationen zu begrenzen. Der Standard-Filter begrenzt das Topologie-Diagramm, um 32 Portgruppen, 32 Hosts und 1024 virtuelle Maschinen anzuzeigen.

Sie können den Diagrammbereich ändern, indem Sie keinen Filter verwenden oder benutzerdefinierte Filter anwenden. Wenn Sie einen benutzerdefinierten Filter verwenden, können Sie nur die Informationen zu einer Gruppe von virtuellen Maschinen, einer Gruppe von Portgruppen auf gewissen Hosts oder einem Port anzeigen. Sie können vom zentralen Topologie-Diagramm des Distributed Switch Filter erstellen.

Anzeigen der Topologie eines vSphere Distributed Switch

Untersuchen Sie die Organisation der Komponenten, die über die Hosts in einem vCenter Server-System mit dem Distributed Switch verbunden sind.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum vSphere Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen** und wählen Sie **Topologie**.

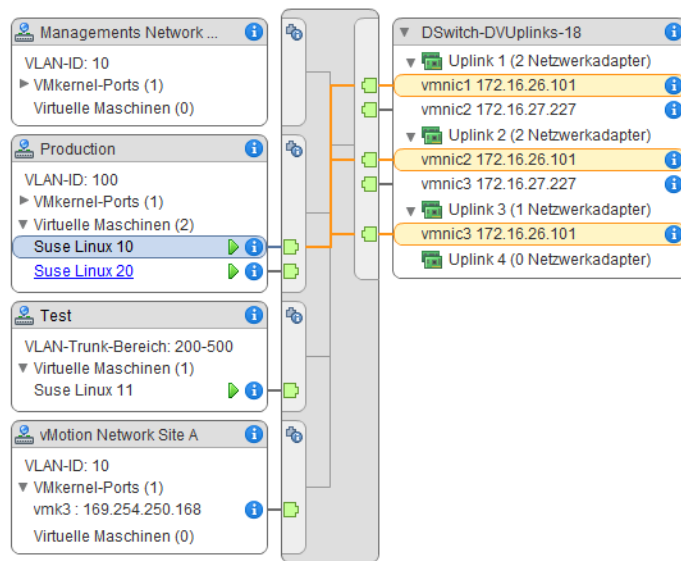
Ergebnisse

Standardmäßig zeigt das Diagramm bis zu 32 verteilte Portgruppen, 32 Hosts und 1024 virtuelle Maschinen.

Beispiel: Diagramm eines Distributed Switch, der den VMkernel und virtuelle Maschinen mit dem Netzwerk verbindet

In Ihrer virtuellen Umgebung steuert ein vSphere Distributed Switch VMkernel-Adapter für vSphere vMotion und für das Verwaltungsnetzwerk sowie gruppierte virtuelle Maschinen. Mithilfe des zentralen Topologie-Diagramms können Sie feststellen, ob eine virtuelle Maschine oder ein VMkernel-Adapter mit dem externen Netzwerk verbunden ist. Weiterhin können Sie den physischen Adapter bestimmen, über den Daten übertragen werden.

Abbildung 3-6. Topologie-Diagramm eines Distributed Switch, der VMkernel und virtuelle Maschinen im Netzwerk steuert



Nächste Schritte

Sie können die folgenden allgemeinen Aufgaben in der Topologie des Distributed Switch ausführen:

- Verwenden von Filtern, um nur die Netzwerkkomponenten von ausgewählten Portgruppen auf bestimmten Hosts, für ausgewählte virtuelle Maschinen oder für einen Port anzuzeigen.
- Suchen, Konfigurieren und Migrieren der Netzwerkkomponenten virtueller Maschinen für Hosts und Portgruppen mithilfe des Assistenten **Netzwerk virtueller Maschinen migrieren**.
- Erkennen der Adapter virtueller Maschinen, denen kein Netzwerk zugewiesen ist, und Verschieben dieser Adapter in die ausgewählte Portgruppe mithilfe des Assistenten **Netzwerk virtueller Maschinen migrieren**.
- Verwalten von Netzwerkkomponenten auf mehreren Hosts mithilfe des Assistenten **Hosts hinzufügen und verwalten**.
- Anzeigen der physischen Netzwerkkarte oder Netzwerkkarten-Gruppe, die den Datenverkehr des ausgewählten Adapters einer virtuellen Maschine oder eines ausgewählten VMkernel-Adapters überträgt.

Auf diese Weise können Sie auch den Host anzeigen, auf dem sich ein ausgewählter VMkernel-Adapter befindet. Wählen Sie den Adapter aus und verfolgen Sie die Route zur zugehörigen physischen Netzwerkkarte. Sie sehen dann die IP-Adresse oder den Domännennamen neben der Netzwerkkarte.

- Bestimmen des VLAN-Modus und der VLAN-ID für eine Portgruppe. Informationen über VLAN-Modi finden Sie unter [VLAN-Konfiguration](#).

Anzeigen der Topologie eines Host-Proxy-Switch

Analysieren und reorganisieren Sie die Netzwerkfunktionen des VMkernels und der virtuellen Maschinen, die vom vSphere Distributed Switch auf einem Host verarbeitet werden.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie den Distributed Switch aus der Liste aus.

Ergebnisse

Die Topologie des Host-Proxy-Switches wird unter der Liste angezeigt.

Einrichten von VMkernel-Netzwerken

4

Sie richten VMkernel-Adapter ein, um die Netzwerkkonnektivität für Hosts zu ermöglichen und den Systemdatenverkehr von vMotion, IP-Speicher, Fault Tolerance-Protokollierung, Virtual SAN usw. aufzunehmen.

- **VMkernel-Netzwerkebene**

Die VMkernel-Netzwerkebene stellt Konnektivität zu Hosts bereit und bearbeitet den Standard-Systemdatenverkehr von vSphere vMotion, IP-Speicher, Fault Tolerance, Virtual SAN u.a. Darüber hinaus können Sie VMkernel-Adapter auf den vSphere Replication-Quellhosts und -Zielhosts erstellen, um den Replizierungsdatenverkehr zu isolieren.

- **Anzeigen von Informationen über VMkernel-Adapter auf einem Host**

Sie können für jeden VMkernel-Adapter dessen zugewiesenen Dienste, zugeordneten Switch, Porteinstellungen, IP-Einstellungen, TCP/IP-Stack, VLAN-ID und Richtlinien anzeigen.

- **Erstellen eines VMkernel-Adapters auf einem vSphere Standard-Switch**

Erstellen Sie einen VMkernel-Netzwerkadapter auf einem vSphere Standard-Switch, um eine Netzwerkverbindung für Hosts bereitzustellen und den Systemdatenverkehr für vSphere vMotion, IP-Speicher, Fault Tolerance-Protokollierung, Virtual SAN usw. zu regeln. Darüber hinaus können Sie VMkernel-Adapter auf den vSphere Replication-Quellhosts und -Zielhosts erstellen, um den Replizierungsdatenverkehr zu isolieren. Weisen Sie jeweils einem Datenverkehrstyp einen VMkernel-Adapter zu.

- **Erstellen eines VMkernel-Adapters auf einem Host, der einem vSphere Distributed Switch zugeordnet ist**

Erstellen Sie einen VMkernel-Adapter auf einem Host, der einem Distributed Switch zugeordnet ist, um Netzwerkkonnektivität für den Host bereitzustellen und den Datenverkehr für vSphere vMotion, IP-Speicher, Fault Tolerance-Protokollierung, Virtual SAN u.a. zu regeln. Sie können VMkernel-Adapter für den Standard-Systemdatenverkehr auf vSphere-Standard-Switches und auf vSphere Distributed Switches einrichten.

- **Bearbeiten einer VMkernel-Adapterkonfiguration**

Sie müssen möglicherweise den unterstützten Datenverkehrstyp für einen VMkernel-Adapter oder die Art und Weise, wie IPv4- oder IPv6-Adressen abgerufen werden, ändern.

- **Anzeigen der TCP/IP-Stack-Konfiguration auf einem Host**

Sie können das DNS und die Routingkonfiguration eines TCP/IP-Stack auf einem Host anzeigen. Sie können auch die IPv4- und IPv6-Routing-Tabellen, den Algorithmus zur Überlastungssteuerung und die maximale Anzahl zulässiger Verbindungen anzeigen.

- **Ändern der Konfiguration eines TCP/IP-Stack auf einem Host**

Sie können das DNS und die Standard-Gatewaykonfiguration eines TCP/IP-Stack auf einem Host ändern. Sie können auch den Algorithmus zur Überlastungssteuerung, die maximale Anzahl der Verbindungen und den Namen der benutzerdefinierten TCP/IP-Stacks ändern.

- **Erstellen eines benutzerdefinierten TCP/IP-Stacks**

Sie können auf einem Host einen benutzerdefinierten TCP/IP-Stack erstellen, um Netzwerkdatenverkehr über eine benutzerdefinierte Anwendung weiterzuleiten.

- **Entfernen eines VMkernel-Adapters**

Entfernen Sie einen VMkernel-Adapter aus einem vSphere Distributed Switch oder Standard-Switch, wenn Sie den Adapter nicht mehr benötigen. Vergewissern Sie sich, dass Sie mindestens einen VMkernel-Adapter für den Verwaltungsdatenverkehr auf dem Host beibehalten, um die Netzwerkkonnektivität aufrechtzuerhalten.

VMkernel-Netzwerkebene

Die VMkernel-Netzwerkebene stellt Konnektivität zu Hosts bereit und bearbeitet den Standard-Systemdatenverkehr von vSphere vMotion, IP-Speicher, Fault Tolerance, Virtual SAN u.a. Darüber hinaus können Sie VMkernel-Adapter auf den vSphere Replication-Quellhosts und -Zielhosts erstellen, um den Replizierungsdatenverkehr zu isolieren.

TCP/IP-Stacks auf VMkernel-Ebene

Standard-TCP/IP-Stack

Stellt Netzwerkunterstützung für den Verwaltungsdatenverkehr zwischen vCenter Server und ESXi-Hosts sowie für den Systemdatenverkehr wie vMotion, IP-Speicher, Fault Tolerance usw. bereit.

vMotion TCP/IP-Stack

Unterstützt den Datenverkehr für die Live-Migration virtueller Maschinen. Verwenden Sie den vMotion TCP/IP-Stack für eine besser Isolierung des vMotion-Datenverkehrs. Nachdem Sie einen VMkernel-Adapter auf dem vMotion TCP/IP-Stack erstellt haben, können Sie nur diesen Stack für vMotion auf dem betreffenden Host verwenden. Die VMkernel-Adapter auf dem Standard-TCP/IP-Stack werden für den vMotion-Dienst deaktiviert. Wenn eine Live-Migration den Standard-TCP/IP-Stack verwendet, während Sie VMkernel-Adapter mit dem vMotion TCP/IP-Stack konfigurieren, wird die Migration erfolgreich abgeschlossen. Die betroffenen VMkernel-Adapter auf dem Standard-TCP/IP-Stack sind aber für künftige vMotion-Sitzungen deaktiviert.

Bereitstellen von TCP/IP-Stacks

Unterstützt den Datenverkehr für Cold-Migration, Klonen und Snapshot-Migration von virtuellen Maschinen. Sie können den TCP/IP-Stack für die Verarbeitung des NFC (Network File Copy)-Datenverkehrs bei vMotion für große Entfernungen verwenden. NFC bietet einen FTP-Dienst für vSphere, bei dem der Dateityp beachtet wird, und ESXi verwendet NFC zum Kopieren und Verschieben von Daten zwischen Datenspeichern. VMkernel-Adapter, die mit dem Bereitstellungs-TCP/IP-Stack konfiguriert sind, verarbeiten den Datenverkehr vom Klonen der virtuellen Festplatten der migrierten virtuellen Maschinen in vMotion für große Entfernungen. Mit dem Bereitstellungs-TCP/IP-Stack können Sie den Datenverkehr von den Klonvorgängen auf einem getrennten Gateway isolieren. Nachdem Sie einen VMkernel-Adapter mit dem Bereitstellungs-TCP/IP-Stack konfiguriert haben, werden alle Adapter auf dem Standard-TCP/IP-Stack für den Bereitstellungsdatenverkehr deaktiviert.

Benutzerdefinierte TCP/IP-Stacks

Sie können benutzerdefinierte TCP/IP-Stacks auf der VMkernel-Ebene hinzufügen, um Netzwerkdatenverkehr von benutzerdefinierten Anwendungen zu verarbeiten.

Sichern von Systemdatenverkehr

Treffen Sie adäquate Sicherheitsvorkehrungen, um nicht autorisierten Zugriff auf den Verwaltungs- und Systemdatenverkehr in der vSphere-Umgebung zu verhindern. Lagern Sie beispielsweise den vMotion-Datenverkehr in ein separates Netzwerk aus, das nur die an der Migration beteiligten ESXi-Hosts enthält. Isolieren Sie den Verwaltungsdatenverkehr in einem Netzwerk, zu dem nur Netzwerk- und Sicherheitsadministratoren Zugang haben. Weitere Informationen finden Sie unter *vSphere-Sicherheit* und *Installations- und Einrichtungshandbuch für vSphere*.

Systemdatenverkehrstypen

Stellen Sie einen separaten VMkernel-Adapter für jeden Datenverkehrstyp bereit. Für Distributed Switches stellen Sie eine separate verteilte Portgruppe für jeden VMkernel-Adapter bereit.

Verwaltungsdatenverkehr

Darüber erfolgt die Konfigurations- und Verwaltungskommunikation für ESXi-Hosts und vCenter Server sowie für den Host-zu-Host-Hochverfügbarkeitsdatenverkehr. Standardmäßig wird beim Installieren der ESXi-Software ein vSphere-Standard-Switch auf dem Host zusammen mit einem VMkernel-Adapter für den Verwaltungsdatenverkehr erstellt. Um Redundanz zu ermöglichen, können Sie für den Verwaltungsdatenverkehr mindestens zwei physische Netzwerkkarten an einen VMkernel-Adapter anschließen.

vMotion-Datenverkehr

Für vMotion geeignet. Ein VMkernel-Adapter für vMotion ist sowohl auf den Quell- als auch auf den Zielhosts erforderlich. Die VMkernel-Adapter für vMotion dürfen nur den vMotion-Datenverkehr verarbeiten. Zur besseren Leistung können Sie mehrere vMotion-Netzwerkkarten konfigurieren. Für mehrere vMotion-Netzwerkkarten können Sie zwei oder

mehr Portgruppen für den vMotion-Datenverkehr bereitstellen, bzw. jeder Portgruppe muss ein vMotion VMkernel-Adapter zugeordnet sein. Dann können Sie eine oder mehrere physische Netzwerkkarten mit jeder Portgruppe verbinden. So werden mehrere physische Netzwerkkarten für vMotion verwendet, was zu mehr Bandbreite führt.

Hinweis vMotion-Netzwerkdatenverkehr ist nicht verschlüsselt. Sie sollten sichere private Netzwerke nur für die Verwendung durch vMotion bereitstellen.

Bereitstellungsdatenverkehr

Verarbeitet die Daten, die für Cold-Migration, Klonen und Snapshot-Migration von virtuellen Maschinen übertragen werden.

IP-Speicherdatenverkehr und Erkennung

Verarbeitet die Verbindung für Speichertypen, die Standard-TCP/IP-Netzwerke verwenden und vom VMkernel-Netzwerk abhängen. Diese Speichertypen sind Software-iSCSI, abhängige Hardware-iSCSI und NFS. Wenn Sie mehr als zwei physische Netzwerkkarten für iSCSI haben, können Sie den iSCSI-Mehrfachpfad konfigurieren. ESXi-Hosts unterstützen nur NFS Version 3 über TCP/IP. Um einen Software-FCoE-Adapter (Fibre Channel over Ethernet) zu konfigurieren, benötigen Sie einen dedizierten VMkernel-Adapter. Software-FCoE übergibt Konfigurationsinformationen über das Data Center Bridging Exchange-Protokoll (DCBX), indem das Cisco Discovery Protocol (CDP) VMkernel-Modul verwendet wird.

Datenverkehr von Fault Tolerance

Verarbeitet den Datenverkehr, den die primäre fehlertolerante virtuelle Maschine über die VMkernel-Netzwerkschicht an die zweite fehlertolerante virtuelle Maschine sendet. Ein separater VMkernel-Adapter ist für die Fault Tolerance-Protokollierung auf jedem Host erforderlich, der Teil eines vSphere-HA-Clusters ist.

vSphere Replication-Datenverkehr

Verarbeitet die ausgehenden Replikationsdaten, die der ESXi-Quellhost an den vSphere Replication-Server überträgt. Reservieren Sie einen VMkernel-Adapter auf der Quell-Site, um den ausgehenden Replikationsdatenverkehr zu isolieren.

vSphere Replication-NFC-Datenverkehr

Verarbeitet die eingehenden Replizierungsdaten auf der Zielreplizierungsseite.

Datenverkehr von Virtual SAN

Jeder Host, der an einem Virtual SAN-Cluster beteiligt ist, benötigt einen VMkernel-Adapter zum Bearbeiten des Datenverkehrs von Virtual SAN.

Anzeigen von Informationen über VMkernel-Adapter auf einem Host

Sie können für jeden VMkernel-Adapter dessen zugewiesenen Dienste, zugeordneten Switch, Porteinstellungen, IP-Einstellungen, TCP/IP-Stack, VLAN-ID und Richtlinien anzeigen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf **Verwalten** und anschließend auf **Netzwerk**.
- 3 Wählen Sie **VMkernel-Adapter** aus, um Informationen über alle VMkernel-Adapter auf dem Host anzuzeigen.
- 4 Wählen Sie einen Adapter aus der Liste der VMkernel-Adapter aus, um dessen Einstellungen anzuzeigen.

Registerkarte	Beschreibung
Alle	Zeigt alle Informationen zur Konfiguration des VMkernel-Adapters an. Die Informationen beinhalten Port- und NIC-Einstellungen, IPv4- und IPv6-Einstellungen und Richtlinien für Traffic-Shaping, Teaming und Failover sowie Sicherheit.
Eigenschaften	Zeigt die Porteigenschaften und NIC-Einstellungen des VMkernel-Adapters an. Die Porteigenschaften beinhalten die Portgruppe (Netzwerkbezeichnung), mit der der Adapter verbunden ist, die VLAN-ID und die aktivierten Dienste. Zu den NIC-Einstellungen gehören die MAC-Adresse und die konfigurierte MTU-Größe.
IP-Einstellungen	Zeigt alle IPv4- und IPv6-Einstellungen für den VMkernel-Adapter an. Informationen zu IPv6 werden nicht angezeigt, wenn IPv6 noch auf dem Host aktiviert wurde.
Richtlinien	Zeigt die konfigurierten Richtlinien für Traffic-Shaping, Teaming und Failover sowie Sicherheit an, die für die Portgruppe gelten, mit denen der VMkernel-Adapter verbunden ist.

Erstellen eines VMkernel-Adapters auf einem vSphere Standard-Switch

Erstellen Sie einen VMkernel-Netzwerkadapter auf einem vSphere Standard-Switch, um eine Netzwerkverbindung für Hosts bereitzustellen und den Systemdatenverkehr für vSphere vMotion, IP-Speicher, Fault Tolerance-Protokollierung, Virtual SAN usw. zu regeln. Darüber hinaus können Sie VMkernel-Adapter auf den vSphere Replication-Quellhosts und -Zielhosts erstellen, um den Replizierungsdatenverkehr zu isolieren. Weisen Sie jeweils einem Datenverkehrstyp einen VMkernel-Adapter zu.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Wählen Sie unter **Verwalten** die Option **Netzwerk** und dann **VMkernel-Adapter** aus.
- 3 Klicken Sie auf **Hostnetzwerk hinzufügen**.

- 4 Wählen Sie auf der Seite „Verbindungstyp auswählen“ die Option **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite „Zielgerät auswählen“ einen bestehenden Standard-Switch oder die Option **Neuer vSphere Standard-Switch** aus.
- 6 (Optional) Weisen Sie auf der Seite „Standard-Switch erstellen“ dem Switch physische Netzwerkkarten zu.

Sie können den Standard-Switch ohne physische Netzwerkkarten erstellen und diese zu einem späteren Zeitpunkt konfigurieren. Während des Zeitraums, in dem keine physischen Netzwerkkarten mit dem Host verbunden sind, weist der Host keine Netzwerkverbindung mit den anderen Hosts im physischen Netzwerk auf. Die virtuellen Maschinen auf dem Host können miteinander kommunizieren.

- a Klicken Sie auf **Hinzufügen** und wählen Sie so viele physische Netzwerkkarten wie erforderlich aus.
 - b Konfigurieren Sie mithilfe der Aufwärts- und Abwärtspfeile die aktiven Netzwerkkarten und die Standby-Netzwerkkarten.
- 7 Konfigurieren Sie auf der Seite „Porteigenschaften“ die Einstellungen für den VMkernel-Adapter.

Option	Beschreibung
Netzwerkbezeichnung	Geben Sie für diese Bezeichnung einen Wert ein, um den Datenverkehrstyp für den VMkernel-Adapter anzugeben, beispielsweise Verwaltungsdatenverkehr oder vmotion .
VLAN-ID	Legen Sie eine VLAN-ID zum Identifizieren des VLANs fest, das vom Netzwerkdatenverkehr des VMkernel-Adapters verwendet wird.
IP-Einstellungen	Wählen Sie IPv4, IPv6 oder beide aus. Hinweis Die IPv6-Option wird auf Hosts, bei denen IPv6 nicht aktiviert ist, nicht angezeigt.

Option	Beschreibung
TCP/IP-Stack	Wählen Sie in der Liste einen TCP/IP-Stack aus. Der TCP/IP-Stack, den Sie für den VMkernel-Adapter festlegen, kann später nicht mehr geändert werden. Wenn Sie den vMotion- oder den Bereitstellungs-TCP/IP-Stack auswählen, können Sie nur diesen Stack für vMotion- oder Bereitstellungsdatenverkehr auf dem Host verwenden. Alle VMkernel-Adapter für vMotion im Standard-TCP/IP-Stack werden für zukünftige vMotion-Sitzungen deaktiviert. Wenn Sie den Bereitstellungs-TCP/IP-Stack verwenden, werden VMkernel-Adapter im Standard-TCP/IP-Stack für Vorgänge mit Bereitstellungsdatenverkehr deaktiviert, wie beispielsweise Cold-Migration, Klonen und Snapshot-Migration von virtuellen Maschinen.
Dienste aktivieren	<p>Für den Standard-TCP/IP-Stack auf dem Host können Dienste aktiviert werden. Zur Auswahl stehen die folgenden Dienste:</p> <ul style="list-style-type: none"> ■ vMotion-Datenverkehr – Dieser Dienst ermöglicht es, dass der VMkernel-Adapter sich einem anderen Host als die Netzwerkverbindung bekannt gibt, über die vMotion-Datenverkehr gesendet wird. Die Migration mit vMotion zum ausgewählten Host ist nicht möglich, wenn der vMotion-Dienst für keinen VMkernel-Adapter im Standard-TCP/IP-Stack aktiviert ist oder wenn keine Adapter den vMotion-TCP/IP-Stack verwenden. ■ Bereitstellungsdatenverkehr. Verarbeitet die übertragenen Daten für Cold-Migration, Klonen und Snapshot-Migration von virtuellen Maschinen. ■ Datenverkehr von Fault Tolerance – Aktiviert die Fault Tolerance-Protokollierung auf dem Host. Pro Host können Sie nur einen VMkernel-Adapter für FT-Datenverkehr verwenden. ■ Verwaltungsdatenverkehr – Ermöglicht den Verwaltungsdatenverkehr für den Host und vCenter Server. Üblicherweise verfügen Hosts über einen derartigen VMkernel-Adapter, der bei der Installation der Software ESXi erstellt wird. Sie können zum Zweck der Redundanz einen weiteren VMkernel-Adapter für Verwaltungsdatenverkehr auf dem Host erstellen. ■ vSphere Replication-Datenverkehr. Verarbeitet die ausgehenden Replizierungsdaten, die vom ESXi-Quellhost an den vSphere Replication-Server gesendet werden. ■ vSphere Replication-NFC-Datenverkehr. Verarbeitet die eingehenden Replizierungsdaten auf der Zielreplizierungsseite. ■ Virtual SAN – Ermöglicht den Datenverkehr des Virtual SAN auf dem Host. Jeder Host, der Teil eines Virtual SAN-Clusters ist, muss über einen derartigen VMkernel-Adapter verfügen.

- 8 Wenn Sie den vMotion-TCP/IP-Stack oder den Bereitstellungs-Stack ausgewählt haben, klicken Sie im angezeigten Warnungsdialegfeld auf **OK**.

Falls bereits eine Live-Migration gestartet wurde, wird diese erfolgreich abgeschlossen, selbst wenn die beteiligten VMkernel-Adapter im Standard-TCP/IP-Stack für vMotion deaktiviert wurden. Dies gilt auch für Vorgänge mit VMkernel-Adapttern im Standard-TCP/IP-Stack, die für den Bereitstellungsdatenverkehr festgelegt sind.

- 9 (Optional) Wählen Sie auf der Seite „IPv4-Einstellungen“ eine Option zum Abrufen von IP-Adressen aus.

Option	Beschreibung
IP-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IP-Einstellungen verwenden	Geben Sie die IPv4-Adresse und die Subnetzmaske für den VMkernel-Adapter ein. Das Standard-Gateway für VMkernel und die DNS-Server-Adressen für IPv4 werden vom ausgewählten TCP/IP-Stack bezogen.

- 10 (Optional) Wählen Sie auf der „Seite IPv6-Einstellungen“ eine Option zum Abrufen von IPv6-Adressen aus.

Option	Beschreibung
IPv6-Adressen automatisch mittels DHCP erhalten	Verwenden Sie DHCP zum Abrufen von IPv6-Adressen. Ein DHCPv6-Server muss im Netzwerk vorhanden sein.
IPv6-Adressen automatisch mittels Router-Ankündigung abrufen	Verwenden Sie die Router-Ankündigung zum Abrufen von IPv6-Adressen.
Statische IPv6-Adressen	<ul style="list-style-type: none"> a Klicken Sie auf Hinzufügen, um eine neue IPv6-Adresse hinzuzufügen. b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein und klicken Sie auf OK. c Klicken Sie auf Bearbeiten, um das Standard-Gateway des VMkernels zu ändern. <p>Die Adresse des Standard-Gateways für VMkernel für IPv6 wird vom ausgewählten TCP/IP-Stack bezogen.</p>

- 11 Überprüfen Sie Ihre Einstellungen auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Beenden**.

Erstellen eines VMkernel-Adapters auf einem Host, der einem vSphere Distributed Switch zugeordnet ist

Erstellen Sie einen VMkernel-Adapter auf einem Host, der einem Distributed Switch zugeordnet ist, um Netzwerkkonnektivität für den Host bereitzustellen und den Datenverkehr für vSphere vMotion, IP-Speicher, Fault Tolerance-Protokollierung, Virtual SAN u.a. zu regeln. Sie können VMkernel-Adapter für den Standard-Systemdatenverkehr auf vSphere-Standard-Switches und auf vSphere Distributed Switches einrichten.

Pro VMkernel-Adapter sollten Sie jeweils eine verteilte Portgruppe vorsehen. Für bessere Isolierung sollten Sie einen VMkernel-Adapter pro Datenverkehrstyp konfigurieren.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Wählen Sie unter **Verwalten** die Option **Netzwerk** und dann **VMkernel-Adapter** aus.

- 3 Klicken Sie auf **Hostnetzwerk hinzufügen**.
- 4 Wählen Sie auf der Seite „Verbindungstyp auswählen“ die Option **VMkernel-Netzwerkadapter** aus und klicken Sie auf **Weiter**.
- 5 Wählen Sie über die Option **Vorhandenes Netzwerk auswählen** eine verteilte Portgruppe aus und klicken Sie auf **Weiter**.
- 6 Konfigurieren Sie auf der Seite „Porteigenschaften“ die Einstellungen für den VMkernel-Adapter.

Option	Beschreibung
Netzwerkbezeichnung	Als Netzwerkbezeichnung wird die Bezeichnung der verteilten Portgruppe übernommen.
IP-Einstellungen	Wählen Sie IPv4, IPv6 oder beide aus. Hinweis Die IPv6-Option wird auf Hosts, bei denen IPv6 nicht aktiviert ist, nicht angezeigt.

Option	Beschreibung
TCP/IP-Stack	Wählen Sie in der Liste einen TCP/IP-Stack aus. Der TCP/IP-Stack, den Sie für den VMkernel-Adapter festlegen, kann später nicht mehr geändert werden. Wenn Sie den vMotion- oder den Bereitstellungs-TCP/IP-Stack auswählen, können Sie nur diese Stacks für vMotion- oder Bereitstellungsdatenverkehr auf dem Host verwenden. Alle VMkernel-Adapter für vMotion im Standard-TCP/IP-Stack werden für zukünftige vMotion-Sitzungen deaktiviert. Wenn Sie den Bereitstellungs-TCP/IP-Stack festlegen, werden VMkernel-Adapter im Standard-TCP/IP-Stack für Vorgänge mit Bereitstellungsdatenverkehr deaktiviert, wie beispielsweise Cold-Migration, Klonen und Snapshot-Migration von virtuellen Maschinen.
Dienste aktivieren	<p>Für den Standard-TCP/IP-Stack auf dem Host können Dienste aktiviert werden. Zur Auswahl stehen die folgenden Dienste:</p> <ul style="list-style-type: none"> ■ vMotion-Datenverkehr – Dieser Dienst ermöglicht es, dass der VMkernel-Adapter sich einem anderen Host als die Netzwerkverbindung bekannt gibt, über die vMotion-Datenverkehr gesendet wird. Die Migration mit vMotion zum ausgewählten Host ist nicht möglich, wenn der vMotion-Dienst für keinen VMkernel-Adapter im Standard-TCP/IP-Stack aktiviert ist oder wenn keine Adapter den vMotion-TCP/IP-Stack verwenden. ■ Bereitstellungsdatenverkehr. Verarbeitet die übertragenen Daten für Cold-Migration, Klonen und Snapshot-Migration von virtuellen Maschinen. ■ Datenverkehr von Fault Tolerance – Aktiviert die Fault Tolerance-Protokollierung auf dem Host. Pro Host können Sie nur einen VMkernel-Adapter für FT-Datenverkehr verwenden. ■ Verwaltungsdatenverkehr – Ermöglicht den Verwaltungsdatenverkehr für den Host und vCenter Server. Üblicherweise verfügen Hosts über einen derartigen VMkernel-Adapter, der bei der Installation der ESXi-Software erstellt wird. Sie können zum Zweck der Redundanz einen weiteren VMkernel-Adapter für Verwaltungsdatenverkehr auf dem Host erstellen. ■ vSphere Replication-Datenverkehr. Verarbeitet die ausgehenden Replizierungsdaten, die vom ESXi-Quellhost an den vSphere Replication-Server gesendet werden. ■ vSphere Replication-NFC-Datenverkehr. Verarbeitet die eingehenden Replizierungsdaten auf der Zielreplizierungsseite. ■ Virtual SAN – Ermöglicht den Datenverkehr des Virtual SAN auf dem Host. Jeder Host, der Teil eines Clusters für Virtual SAN ist, muss über einen derartigen VMkernel-Adapter verfügen.

- 7 Wenn Sie den vMotion-TCP/IP-Stack oder den Bereitstellungs-Stack ausgewählt haben, klicken Sie im angezeigten Warnungsdiaologfeld auf **OK**.

Falls bereits eine Live-Migration gestartet wurde, wird diese erfolgreich abgeschlossen, selbst wenn die beteiligten VMkernel-Adapter im Standard-TCP/IP-Stack für vMotion deaktiviert wurden. Dies gilt auch für Vorgänge mit VMkernel-Adapttern im Standard-TCP/IP-Stack, die für den Bereitstellungsdatenverkehr festgelegt sind.

- 8 (Optional) Wählen Sie auf der Seite „IPv4-Einstellungen“ eine Option zum Abrufen von IP-Adressen aus.

Option	Beschreibung
IP-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IP-Einstellungen verwenden	Geben Sie die IPv4-Adresse und die Subnetzmaske für den VMkernel-Adapter ein. Das Standard-Gateway für VMkernel und die DNS-Server-Adressen für IPv4 werden vom ausgewählten TCP/IP-Stack bezogen.

- 9 (Optional) Wählen Sie auf der „Seite IPv6-Einstellungen“ eine Option zum Abrufen von IPv6-Adressen aus.

Option	Beschreibung
IPv6-Adressen automatisch mittels DHCP erhalten	Verwenden Sie DHCP zum Abrufen von IPv6-Adressen. Ein DHCPv6-Server muss im Netzwerk vorhanden sein.
IPv6-Adressen automatisch mittels Router-Ankündigung abrufen	Verwenden Sie die Router-Ankündigung zum Abrufen von IPv6-Adressen.
Statische IPv6-Adressen	<ul style="list-style-type: none"> a Klicken Sie auf Hinzufügen, um eine neue IPv6-Adresse hinzuzufügen. b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein und klicken Sie auf OK. c Klicken Sie auf Bearbeiten, um das Standard-Gateway des VMkernels zu ändern. <p>Die Adresse des Standard-Gateways für VMkernel für IPv6 wird vom ausgewählten TCP/IP-Stack bezogen.</p>

- 10 Überprüfen Sie Ihre Einstellungen auf der Seite „Bereit zum Abschließen“ und klicken Sie auf **Beenden**.

Bearbeiten einer VMkernel-Adapterkonfiguration

Sie müssen möglicherweise den unterstützten Datenverkehrstyp für einen VMkernel-Adapter oder die Art und Weise, wie IPv4- oder IPv6-Adressen abgerufen werden, ändern.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Wählen Sie unter **Verwalten** die Option **Netzwerk** und dann **VMkernel-Adapter** aus.
- 3 Wählen Sie den VMkernel-Adapter aus, der sich auf dem Ziel-Distributed Switch oder Ziel-Standard-Switch befindet und klicken Sie auf **Bearbeiten**.

- 4 Wählen Sie auf der Seite „Porteigenschaften“ die zu aktivierenden Dienste aus.

Kontrollkästchen	Beschreibung
vMotion-Datenverkehr	Dieser Dienst ermöglicht es, dass der VMkernel-Adapter sich einem anderen Host als die Netzwerkverbindung bekannt gibt, über die vMotion-Datenverkehr gesendet wird. Wenn diese Eigenschaft für keinen der VMkernel-Adapter aktiviert wurde, ist eine vMotion-Migration auf den ausgewählten Host nicht möglich.
Bereitstellungsdatenverkehr	Verarbeitet die übertragenen Daten für Cold-Migration, Klonen und Snapshot-Migration von virtuellen Maschinen.
Datenverkehr von Fault Tolerance	Aktiviert die Fault Tolerance-Protokollierung auf dem Host. Pro Host können Sie nur einen VMkernel-Adapter für FT-Datenverkehr verwenden.
Verwaltungsdatenverkehr	Ermöglicht den Verwaltungsdatenverkehr für den Host und vCenter Server. Üblicherweise verfügen Hosts über einen derartigen VMkernel-Adapter, der bei der Installation der Software ESXi erstellt wird. Sie können über einen zusätzlichen VMkernel-Adapter für den Verwaltungsdatenverkehr auf dem Host verfügen, um Redundanz bereitzustellen.
vSphere Replication-Datenverkehr	Verarbeitet die ausgehenden Replizierungsdaten, die vom ESXi-Quellhost an den vSphere Replication-Server gesendet werden.
vSphere Replication-NFC-Datenverkehr	Verarbeitet die eingehenden Replizierungsdaten auf der Zielreplizierungsseite.
Virtual SAN	Aktiviert den Virtual SAN-Datenverkehr auf dem Host. Jeder Host, der Teil eines Virtual SAN-Clusters ist, muss über einen derartigen VMkernel-Adapter verfügen.

- 5 Legen Sie auf der Seite „NIC-Einstellungen“ die MTU für den Netzwerkadapter fest.
- 6 Wählen Sie bei aktivierter IPv4-Adressierung im Abschnitt „IPv4-Einstellungen“ die Methode aus, mit der IP-Adressen abgerufen werden.

Option	Beschreibung
IP-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IP-Einstellungen verwenden	Geben Sie die IPv4-Adresse und die Subnetzmaske für den VMkernel-Adapter ein. Das Standard-Gateway für VMkernel und die DNS-Server-Adressen für IPv4 werden vom ausgewählten TCP/IP-Stack bezogen.

- 7 Wählen Sie bei aktivierter IPv6-Adressierung im Abschnitt IPv6-Einstellungen eine Option für das Abrufen von IPv6-Adressen aus.

Hinweis Die IPv6-Option wird auf Hosts, bei denen IPv6 nicht aktiviert ist, nicht angezeigt.

Option	Beschreibung
IPv6-Adressen automatisch mittels DHCP erhalten	Verwenden Sie DHCP zum Abrufen von IPv6-Adressen. Ein DHCPv6-Server muss im Netzwerk vorhanden sein.
IPv6-Adressen automatisch mittels Router-Ankündigung abrufen	Verwenden Sie die Router-Ankündigung zum Abrufen von IPv6-Adressen.
Statische IPv6-Adressen	<ol style="list-style-type: none"> a Klicken Sie auf Hinzufügen, um eine neue IPv6-Adresse hinzuzufügen. b Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein und klicken Sie auf OK. c Klicken Sie auf Bearbeiten, um das Standard-Gateway des VMkernel zu ändern. <p>Die Adresse des Standard-Gateways für VMkernel für IPv6 wird vom ausgewählten TCP/IP-Stack bezogen.</p>

Im Abschnitt „Erweiterte Einstellungen“ der IP-Einstellungen können Sie die IPv6-Adressen entfernen. Wenn die Router-Ankündigung aktiviert ist, können die entfernten Adressen aus dieser Quelle wieder erscheinen. Das Entfernen von DHCP-Adressen auf dem VMkernel-Adapter wird nicht unterstützt. Diese Adressen werden nur entfernt, wenn die DHCP-Option deaktiviert ist.

- 8 Stellen Sie auf der Seite „Änderungen überprüfen“ sicher, dass die am VMkernel-Adapter vorgenommenen Änderungen andere Vorgänge nicht stören.
- 9 Klicken Sie auf **OK**.

Anzeigen der TCP/IP-Stack-Konfiguration auf einem Host

Sie können das DNS und die Routingkonfiguration eines TCP/IP-Stack auf einem Host anzeigen. Sie können auch die IPv4- und IPv6-Routing-Tabellen, den Algorithmus zur Überlastungssteuerung und die maximale Anzahl zulässiger Verbindungen anzeigen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf **Verwalten**, klicken Sie auf **Netzwerk** und wählen Sie **TCP/IP-Konfiguration** aus.
- 3 Wählen Sie einen Stack in der Tabelle mit den TCP/IP-Stacks aus.

Wenn auf dem Host keine benutzerdefinierten TCP/IP-Stacks konfiguriert wurden, können Sie die Standard-, vMotion- und Bereitstellungs-TCP/IP-Stacks auf dem Host anzeigen.

Ergebnisse

DNS- und Routing-Details zu dem ausgewählten TCP/IP-Stack werden unterhalb der Tabelle mit den TCP/IP-Stacks angezeigt. Hier können Sie die IPv4- und IPv6-Routing-Tabellen sowie die DNS- und Routing-Konfiguration für den Stack sehen.

Hinweis Die IPv6-Routing-Tabelle wird nur angezeigt, wenn auf dem Host IPv6 aktiviert ist.

Die Registerkarte **Erweitert** enthält Informationen zu dem konfigurierten Algorithmus zur Überlastungssteuerung und zu der maximal zulässigen Anzahl an Verbindungen mit dem Stack.

Ändern der Konfiguration eines TCP/IP-Stack auf einem Host

Sie können das DNS und die Standard-Gatewaykonfiguration eines TCP/IP-Stack auf einem Host ändern. Sie können auch den Algorithmus zur Überlastungssteuerung, die maximale Anzahl der Verbindungen und den Namen der benutzerdefinierten TCP/IP-Stacks ändern.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Erweitern Sie **Netzwerk** auf der Registerkarte **Konfigurieren** und wählen Sie **TCP/IP-Konfiguration** aus.
- 3 Wählen Sie einen Stack aus der Tabelle aus, klicken Sie auf **Bearbeiten** und nehmen Sie die gewünschten Änderungen vor.

Seite	Option
Name	Ändern des Namens eines benutzerdefinierten TCP/IP-Stack
DNS-Konfiguration	<p>Wählen Sie eine Methode zum Abrufen des DNS-Server aus.</p> <ul style="list-style-type: none"> ■ Wählen Sie Einstellungen automatisch von einem VMkernel-Netzwerkadapter abrufen und wählen Sie einen Netzwerkadapter aus dem Dropdown-Menü VMKernel-Netzwerkadapter aus. ■ Wählen Sie Einstellungen manuell eingeben aus und bearbeiten Sie die DNS-Konfigurationseinstellungen. <ul style="list-style-type: none"> a Bearbeiten Sie den Hostnamen. b Bearbeiten Sie den Domännennamen. c Geben Sie die IP-Adresse eines bevorzugten DNS-Servers ein. d Geben Sie die IP-Adresse eines alternativen DNS-Servers ein. e (Optional) Verwenden Sie das Textfeld Domänen durchsuchen, um DNS-Suffixe anzugeben, die während der DNS-Suche beim Auflösen nicht qualifizierter Domännennamen verwendet werden.
Routing	<p>Bearbeiten Sie die VMkernel-Gatewayinformationen.</p> <p>Hinweis Durch Entfernen des Standard-Gateways kann die Verbindung zwischen Client und Host getrennt werden.</p>
Erweitert	Bearbeiten Sie die maximale Anzahl Verbindungen und den Algorithmus für die Überlastungssteuerung des Stack.

- 4 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Nächste Schritte

Mithilfe von CLI-Befehlen können Sie zusätzlichen Gateways statische Routen hinzufügen. Weitere Informationen finden Sie unter <http://kb.vmware.com/kb/2001426>

Erstellen eines benutzerdefinierten TCP/IP-Stacks

Sie können auf einem Host einen benutzerdefinierten TCP/IP-Stack erstellen, um Netzwerkdatenverkehr über eine benutzerdefinierte Anwendung weiterzuleiten.

Verfahren

- 1 Stellen Sie eine SSH-Verbindung mit dem Host her.
- 2 Melden Sie sich als Root-Benutzer an.
- 3 Führen Sie den vSphere-CLI-Befehl aus.

```
esxcli network ip netstack add -N="stack_name"
```

Ergebnisse

Der benutzerdefinierte TCP/IP-Stack wird auf dem Host erstellt. Sie können dem Stack VMkernel-Adapter zuweisen.

Entfernen eines VMkernel-Adapters

Entfernen Sie einen VMkernel-Adapter aus einem vSphere Distributed Switch oder Standard-Switch, wenn Sie den Adapter nicht mehr benötigen. Vergewissern Sie sich, dass Sie mindestens einen VMkernel-Adapter für den Verwaltungsdatenverkehr auf dem Host beibehalten, um die Netzwerkkonnektivität aufrechtzuerhalten.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Wählen Sie unter **Verwalten** die Option **Netzwerk** und dann **VMkernel-Adapter** aus.
- 3 Wählen Sie den VMkernel-Adapter aus der Liste aus und klicken Sie auf **Entfernen**.
- 4 Klicken Sie im Bestätigungsdiaologfeld auf **Auswirkungen analysieren**.

- 5 Wenn Sie Software-iSCSI-Adapter mit Portbindung verwenden, überprüfen Sie die Auswirkung auf deren Netzwerkkonfiguration.

Option	Beschreibung
Keine Auswirkung	iSCSI funktioniert wie gewohnt, nachdem die neue Netzwerkkonfiguration angewendet wurde.
Wichtige Auswirkung	Die gewohnte Funktionsweise von iSCSI kann unterbrochen werden, wenn die neue Netzwerkkonfiguration angewendet wird.
Kritische Auswirkung	Die gewohnte Funktionsweise von iSCSI wird unterbrochen, wenn die neue Netzwerkkonfiguration angewendet wird.

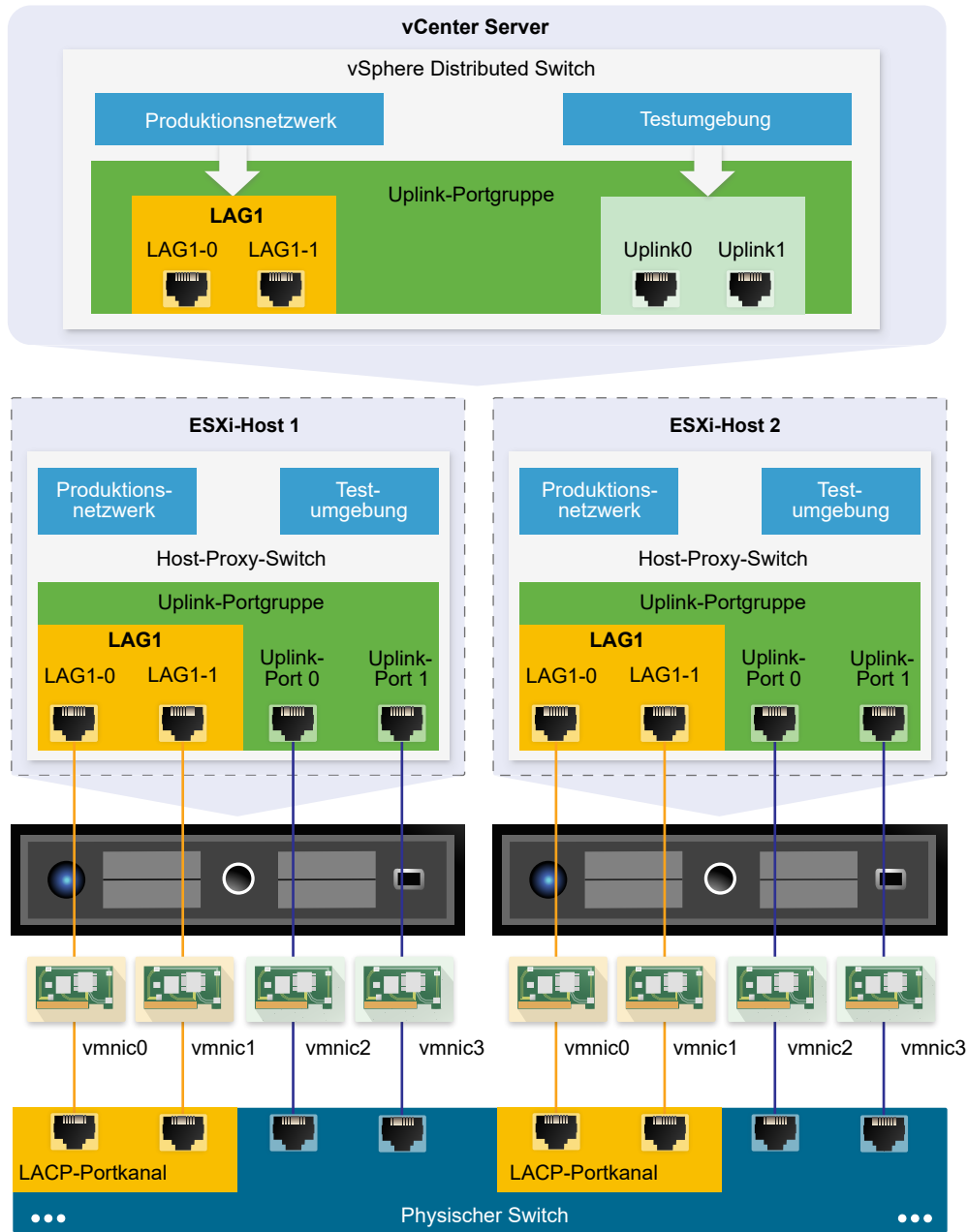
- a Wenn eine bedeutende oder kritische Auswirkung auf iSCSI vorliegt, klicken Sie auf den Eintrag **iSCSI** und überprüfen Sie die Gründe, die im Bereich „Analysedetails“ angezeigt werden.
 - b Brechen Sie die Entfernung des VMkernel-Adapters ab, bis Sie alle Vorkommnisse von kritischen oder wichtigen Auswirkungen auf einen Dienst behoben haben. Wenn keine betroffenen Dienste vorliegen, schließen Sie das Dialogfeld „Auswirkungen analysieren“.
- 6 Klicken Sie auf **OK**.

LACP-Support auf einem vSphere Distributed Switch

5

Mit der LACP-Unterstützung auf einem vSphere Distributed Switch können Sie mithilfe der dynamischen Linkzusammenfassung ESXi-Hosts mit physischen Switches verbinden. Auf einem Distributed Switch können mehrere Linkzusammenfassungsgruppen erstellt werden, um die Bandbreite von physischen Netzwerkkarten auf ESXi-Hosts zu aggregieren, die mit LACP-Portkanälen verbunden sind.

Abbildung 5-1. Erweiterte LACP-Unterstützung auf einem vSphere Distributed Switch



LACP-Konfiguration auf dem Distributed Switch

Sie konfigurieren eine Linkzusammenfassengruppe mit zwei oder mehr Ports und verbinden physische Netzwerkkarten mit den Ports. Ports von Linkzusammenfassengruppen werden innerhalb der Linkzusammenfassengruppe gruppiert und für den Lastausgleich des Netzwerkdatenverkehrs zwischen den Ports wird ein LACP-Hashing-Algorithmus verwendet. Mithilfe einer Linkzusammenfassengruppe können Sie den Datenverkehr von verteilten Portgruppen regeln, um eine höhere Netzwerkbandbreite und Redundanz sowie einen besseren Lastausgleich für die Portgruppen zu erzielen.

Wenn Sie eine Linkzusammenfassungsgruppe auf einem Distributed Switch erstellen, wird auf dem Proxy-Switch jedes Hosts, der mit dem Distributed Switch verbunden ist, auch ein Linkzusammenfassungsobjekt erstellt. Wenn Sie beispielsweise Linkzusammenfassungsgruppe1 mit zwei Ports erstellen, wird auf jedem Host, der mit dem Distributed Switch verbunden ist, Linkzusammenfassungsgruppe1 mit derselben Anzahl an Ports erstellt.

Auf einem Host-Proxy-Switch können Sie eine physische Netzwerkkarte mit nur einem Port der Linkzusammenfassungsgruppe verbinden. Auf der Seite des Distributed Switches können mit einem Port der Linkzusammenfassungsgruppe mehrere physische Netzwerkkarten von verschiedenen Hosts verbunden werden. Die physischen Netzwerkkarten auf einem Host, die Sie mit den Ports der Linkzusammenfassungsgruppe verbinden, müssen mit Links verknüpft sein, die einen LACP-Portkanal auf einem physischen Switch verwenden.

Auf einem Distributed Switch können Sie bis zu 64 Linkzusammenfassungsgruppen erstellen. Ein Host kann maximal 32 Linkzusammenfassungsgruppen unterstützen. Die Anzahl der Linkzusammenfassungsgruppen, die tatsächlich verwendet werden können, hängt jedoch von der Leistungsfähigkeit der zugrundeliegenden physischen Umgebung sowie der Topologie des virtuellen Netzwerks ab. Wenn der physische Switch beispielsweise maximal vier Ports in einem LACP-Portkanal unterstützt, können Sie bis zu vier physische Netzwerkkarten pro Host mit einer Linkzusammenfassungsgruppe verbinden.

Portkanal-Konfiguration auf dem physischen Switch

Für jeden Host, auf dem Sie LACP nutzen wollen, müssen Sie einen separaten LACP-Portkanal auf dem physischen Switch erstellen. Wenn Sie LACP auf dem physischen Switch konfigurieren, müssen Sie die folgenden Anforderungen beachten:

- Die Anzahl der Ports im LACP-Portkanal muss der Anzahl von physischen Netzwerkkarten entsprechen, die Sie auf dem Host gruppieren möchten. Möchten Sie beispielsweise die Bandbreite von zwei physischen Netzwerkkarten auf einem Host aggregieren, müssen Sie einen LACP-Portkanal mit zwei Ports auf dem physischen Switch erstellen. Die Linkzusammenfassung auf dem Distributed Switch muss mit mindestens zwei Ports konfiguriert werden.
- Der Hashing-Algorithmus des LACP-Portkanals auf dem physischen Switch muss dem Hashing-Algorithmus entsprechen, der für die Linkzusammenfassung auf dem Distributed Switch konfiguriert ist.
- Alle physischen Netzwerkkarten, die Sie mit dem LACP-Portkanal verbinden möchten, müssen mit der gleichen Geschwindigkeit und Duplex-Einstellung konfiguriert werden.

Dieses Kapitel enthält die folgenden Themen:

- [Konvertieren zur erweiterten LACP-Unterstützung auf einem vSphere Distributed Switch](#)
- [Konfiguration von LACP-Teaming und -Failover für verteilte Portgruppen](#)
- [Konfigurieren einer Linkzusammenfassungsgruppe zur Regelung des Datenverkehrs für verteilte Portgruppen](#)

- Bearbeiten einer Linkzusammenfassungsgruppe
- Aktivieren der LACP 5.1-Unterstützung für eine Uplink-Portgruppe
- Einschränkungen der LACP-Unterstützung für einen vSphere Distributed Switch

Konvertieren zur erweiterten LACP-Unterstützung auf einem vSphere Distributed Switch

Nachdem Sie für einen vSphere Distributed Switch ein Upgrade von Version 5.1 auf Version 5.5 oder 6.0 durchgeführt haben, können Sie eine Konvertierung zur erweiterten LACP-Unterstützung durchführen und mehrere Linkzusammenfassungsgruppen auf dem Distributed Switch erstellen.

Wenn auf dem Distributed Switch bereits eine LACP-Konfiguration vorhanden ist, wird durch das Erweitern der LACP-Unterstützung eine neue Linkzusammenfassungsgruppe erstellt und alle physischen Netzwerkkarten werden von den eigenständigen Uplinks auf die Ports der Linkzusammenfassungsgruppe migriert. Um eine andere LACP-Konfiguration zu erstellen, sollten Sie die LACP-Unterstützung in der Uplink-Portgruppe deaktivieren, bevor die Konvertierung gestartet wird.

Wenn die Konvertierung zur erweiterten LACP-Unterstützung fehlschlägt, finden Sie Details zum manuellen Abschließen der Konvertierung im *vSphere-Fehlerbehebungshandbuch*.

Voraussetzungen

- Stellen Sie sicher, dass der vSphere Distributed Switch Version 5.5 oder 6.0 entspricht.
- Stellen Sie sicher, dass keine der verteilten Portgruppen die Außerkraftsetzung der Uplink-Teaming-Richtlinie auf einzelnen Ports zulässt.
- Falls Sie eine Konvertierung von einer vorhandenen LACP-Konfiguration durchführen, stellen Sie sicher, dass auf dem Distributed Switch nur eine Uplink-Portgruppe vorhanden ist.
- Stellen Sie sicher, dass die Hosts im Distributed Switch verbunden sind und reagieren.
- Stellen Sie sicher, dass Sie in den verteilten Portgruppen auf dem Switch über das Recht **dvPort-Gruppe.Ändern** verfügen.
- Stellen Sie sicher, dass Sie auf den Hosts im Distributed Switch über das Recht **Host.Konfiguration.Ändern** verfügen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie **Zusammenfassung** aus.
- 3 Klicken Sie unter „Funktionen“ neben „LACP (Link Aggregation Control Protocol)“ auf **Erweitern**.

- 4 (Optional) Wählen Sie **Konfiguration exportieren** aus, um die Konfiguration der Distributed Switch zu sichern, und klicken Sie auf **Weiter**.

In der Sicherung wird nur die Konfiguration der Distributed Switch auf der vCenter Server-Seite gespeichert. Wenn die Konvertierung zur erweiterten LACP-Unterstützung fehlschlägt, können Sie entweder mithilfe der Sicherung einen neuen Distributed Switch mit derselben Konfiguration erstellen oder die Konvertierung manuell abschließen.

- 5 Überprüfen Sie die Voraussetzungen für die Validierung.

Voraussetzung	Beschreibung
Portgruppenzugriff	Sie verfügen über ausreichende Rechte, um auf den Uplink und die verteilten Portgruppen auf dem Switch zuzugreifen und diese zu ändern.
LACP-Konfiguration	Auf dem Distributed Switch ist nur eine Uplink-Portgruppe vorhanden.
Außerkraftsetzung der Uplink-Teaming-Richtlinie	Verteilte Portgruppen lassen nicht zu, dass ihre Uplink-Teaming-Richtlinie auf einzelnen Ports außer Kraft gesetzt wird.
Zugriffsfähigkeit auf den Host	Sie müssen über ausreichende Rechte verfügen, um die Netzwerkkonfiguration der Hosts zu ändern, die mit dem Distributed Switch verbunden sind.
Hostkonnektivität	Hosts, die den Distributed Switch verwenden, sind verbunden und reagieren.

- 6 Klicken Sie auf **Weiter**.
- 7 Wenn Sie die Konvertierung von einer vorhandenen LACP-Konfiguration durchführen, geben Sie den Namen der neuen Linkzusammenfassungsgruppe in das Textfeld „Name“ ein.
- 8 Klicken Sie auf **Weiter**, um die Details zur Konvertierung zu überprüfen, und anschließend auf **Beenden**.

Ergebnisse

Sie haben die Konvertierung zur erweiterten LACP-Unterstützung auf dem vSphere Distributed Switch durchgeführt.

Nächste Schritte

Erstellen Sie Linkzusammenfassungsgruppen auf dem Distributed Switch, um die Bandbreite von mehreren physischen Netzwerkkarten auf den zugeordneten Hosts zu aggregieren.

Konfiguration von LACP-Teaming und -Failover für verteilte Portgruppen

Um den Netzwerkdatenverkehr von verteilten Portgruppen mithilfe einer Linkzusammenfassungsgruppe zu bearbeiten, weisen Sie physische Netzwerkkarten zu den Linkzusammenfassungsgruppen-Ports zu und legen Sie die Linkzusammenfassungsgruppe in der Teaming- und Failover-Reihenfolge für eine verteilte Portgruppe als aktiv fest.

Tabelle 5-1. Konfiguration von LACP-Teaming und -Failover für verteilte Portgruppen

Failover-Reihenfolge	Uplinks	Beschreibung
Aktiv	Eine einzelne Linkzusammenfassungsgruppe	Sie können nur eine aktive Linkzusammenfassungsgruppe oder mehrere eigenständige Uplinks für die Verarbeitung des Datenverkehrs von verteilten Portgruppen verwenden. Es ist nicht möglich, mehrere aktive Linkzusammenfassungsgruppen oder aber aktive Linkzusammenfassungsgruppen mit eigenständigen Uplinks zu konfigurieren.
Standby	Leer	Das Vorhandensein einer aktiven Linkzusammenfassungsgruppe und von Standby-Uplinks und umgekehrt wird nicht unterstützt. Das Vorhandensein einer Linkzusammenfassungsgruppe und einer anderen Standby-Linkzusammenfassungsgruppe wird nicht unterstützt.
Nicht verwendet	Alle eigenständige Uplinks und ggf. andere Linkzusammenfassungsgruppen	Da nur eine Linkzusammenfassungsgruppe aktiv sein darf und die Standbyliste leer sein muss, müssen Sie alle eigenständigen Uplinks und andere Linkzusammenfassungsgruppen als nicht verwendet festlegen.

Konfigurieren einer Linkzusammenfassungsgruppe zur Regelung des Datenverkehrs für verteilte Portgruppen

Zum Aggregieren der Bandbreite von mehreren physischen Netzwerkkarten auf Hosts können Sie auf dem Distributed Switch eine Linkzusammenfassungsgruppe erstellen, mit deren Hilfe der Datenverkehr der verteilten Portgruppen geregelt werden kann.

Bei neu erstellten Linkzusammenfassungsgruppen wurden den Ports keine physischen Netzwerkkarten zugewiesen und werden nicht in der Teaming- und Failover-Reihenfolge von verteilten Portgruppen verwendet. Um den Netzwerkdatenverkehr von verteilten Portgruppen mithilfe einer Linkzusammenfassungsgruppe zu regeln, müssen Sie den Datenverkehr von eigenständigen Links in der Linkzusammenfassungsgruppe migrieren.

Voraussetzungen

- Vergewissern Sie sich, dass für jeden Host, auf dem Sie LACP verwenden, ein separater LACP-Port auf dem physischen Switch vorhanden ist. Weitere Informationen hierzu finden Sie unter [Kapitel 5 LACP-Support auf einem vSphere Distributed Switch](#).
- Stellen Sie sicher, dass der vSphere Distributed Switch, auf dem Sie die Linkzusammenfassungsgruppe konfigurieren, Version 5.5 oder 6.0 entspricht.

- Stellen Sie sicher, dass erweitertes LCAP auf dem Distributed Switch unterstützt wird.

Verfahren

1 Linkzusammenfassungsgruppe erstellen

Um den Netzwerkdatenverkehr von verteilten Portgruppen zu einer Linkzusammenfassungsgruppe zu migrieren, erstellen Sie auf dem Distributed Switch eine neue Linkzusammenfassungsgruppe.

2 Festlegen einer Linkzusammenfassungsgruppe als Standby in der Teaming- und Failover-Reihenfolge für verteilte Portgruppen

Die neue Linkzusammenfassungsgruppe (LAG) wird standardmäßig in der Teaming- und Failover-Reihenfolge von verteilten Portgruppen nicht verwendet. Da nur eine Linkzusammenfassungsgruppe oder nur eigenständige Uplinks für verteilte Portgruppen aktiv sein können, müssen Sie eine Zwischenkonfiguration für Teaming und Failover erstellen, bei der die Linkzusammenfassungsgruppe „standby“ ist. Mit dieser Konfiguration können physische Netzwerkkarten zu LAG-Ports migriert werden, indem die Netzwerkkonnektivität erhalten bleibt.

3 Zuweisen physischer Netzwerkkarten zu den Ports der Linkzusammenfassungsgruppe

Sie haben die neue Linkzusammenfassungsgruppe (LAG) als Standby in der Teaming- und Failover-Reihenfolge von verteilten Portgruppen festgelegt. Durch die Festlegung der Linkzusammenfassungsgruppe als Standby können Sie die physischen Netzwerkkarten sicher von eigenständigen Uplinks zu den LAG-Ports migrieren, ohne Netzwerkkonnektivität zu verlieren.

4 Festlegen einer Linkzusammenfassungsgruppe als aktiv in der Teaming- und Failover-Reihenfolge für eine verteilte Portgruppe

Sie haben physische Netzwerkkarten zu den Ports der Linkzusammenfassungsgruppe migriert. Legen Sie die Linkzusammenfassungsgruppe als aktiv fest und verschieben Sie alle eigenständigen Uplinks als nicht verwendet in die Teaming- und Failover-Reihenfolge der verteilten Portgruppen.

Linkzusammenfassungsgruppe erstellen

Um den Netzwerkdatenverkehr von verteilten Portgruppen zu einer Linkzusammenfassungsgruppe zu migrieren, erstellen Sie auf dem Distributed Switch eine neue Linkzusammenfassungsgruppe.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie **Verwalten** und wählen Sie dann **Einstellungen**.
- 3 Klicken Sie unter **LACP** auf **Neue Linkzusammenfassungsgruppe**.
- 4 Benennen Sie die neue Linkzusammenfassungsgruppe.

- 5 Legen Sie die Anzahl an Ports für die Linkzusammenfassungsgruppe fest.

Legen Sie dieselbe Anzahl an Ports für die Linkzusammenfassungsgruppe wie die Anzahl an Ports im LACP-Portkanal auf dem physischen Switch fest. Ein Port der Linkzusammenfassungsgruppe hat dieselbe Funktion wie ein Uplink auf dem Distributed Switch. Die Ports der Linkzusammenfassungsgruppe bilden zusammen eine NIC-Gruppierung im Kontext der Linkzusammenfassungsgruppe.

- 6 Wählen Sie den LACP-Aushandlungsmodus der Linkzusammenfassungsgruppe aus.

Option	Beschreibung
Aktiv	Alle Ports der Linkzusammenfassungsgruppe befinden sich in einem aktiven Aushandlungsmodus. Die Ports der Linkzusammenfassungsgruppe initiieren die Aushandlungen mit dem LACP-Portkanal auf dem physischen Switch durch Senden von LACP-Paketen.
Passiv	Die Ports der Linkzusammenfassungsgruppe befinden sich im passiven Aushandlungsmodus. Sie reagieren auf empfangene LACP-Pakete, initiieren jedoch keine LACP-Aushandlung.

Wenn sich die für LACP aktivierten Ports auf dem physischen Switch im aktiven Aushandlungsmodus befinden, können Sie die Ports der Linkzusammenfassungsgruppe in den passiven Modus versetzen und umgekehrt.

- 7 Wählen Sie von den Hashing-Algorithmen, die vom LACP definiert werden, einen Lastausgleichsmodus aus.

Hinweis Die Hashing-Algorithmen müssen dieselben sein wie die für den LACP-Port-Kanal auf dem physischen Switch festgelegten Hashing-Algorithmen.

- 8 Legen Sie die VLAN- und die NetFlow-Richtlinien für die Linkzusammenfassungsgruppe fest.

Diese Option ist aktiviert, wenn die VLAN- und die NetFlow-Richtlinien in der Uplink-Portgruppe pro einzeltem Uplink-Port aktiviert sind. Wenn Sie die VLAN- und die NetFlow-Richtlinien für die Linkzusammenfassungsgruppe festlegen, werden die Richtlinien außer Kraft gesetzt, die auf der Ebene der Uplink-Portgruppe festgelegt sind.

- 9 Klicken Sie auf **OK**.

Ergebnisse

Die neue Linkzusammenfassungsgruppe wird nicht in der Teaming- und Failover-Reihenfolge von verteilten Portgruppen verwendet. Den Ports der Linkzusammenfassungsgruppe sind keine physischen Netzwerkkarten zugewiesen.

Ebenso wie eigenständige Uplinks wird die Linkzusammenfassungsgruppe auf jedem Host dargestellt, der mit dem Distributed Switch verbunden ist. Wenn Sie beispielsweise auf dem Distributed Switch eine Linkzusammenfassungsgruppe1 mit zwei Ports erstellen, wird auf jedem dem Distributed Switch zugeordneten Host eine Linkzusammenfassungsgruppe1 mit zwei Ports erstellt.

Nächste Schritte

Legen Sie die Linkzusammenfassungsgruppe als Standby in der Teaming- und Failover-Konfiguration von verteilten Portgruppen fest. Auf diese Weise erstellen Sie eine Zwischenkonfiguration, die es Ihnen ermöglicht, den Netzwerkdatenverkehr ohne Verlust der Netzwerkkonnektivität zur Linkzusammenfassungsgruppe zu migrieren.

Festlegen einer Linkzusammenfassungsgruppe als Standby in der Teaming- und Failover-Reihenfolge für verteilte Portgruppen

Die neue Linkzusammenfassungsgruppe (LAG) wird standardmäßig in der Teaming- und Failover-Reihenfolge von verteilten Portgruppen nicht verwendet. Da nur eine Linkzusammenfassungsgruppe oder nur eigenständige Uplinks für verteilte Portgruppen aktiv sein können, müssen Sie eine Zwischenkonfiguration für Teaming und Failover erstellen, bei der die Linkzusammenfassungsgruppe „standby“ ist. Mit dieser Konfiguration können physische Netzwerkkarten zu LAG-Ports migriert werden, indem die Netzwerkkonnektivität erhalten bleibt.

Verfahren

- 1 Navigieren Sie zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Verteilte Portgruppen verwalten** aus.
- 3 Wählen Sie **Teaming und Failover** aus, und klicken Sie auf **Weiter**.
- 4 Wählen Sie die Portgruppen aus, in denen Sie die Linkzusammenfassungsgruppe verwenden möchten.
- 5 Wählen Sie in „Failover-Reihenfolge“ die Linkzusammenfassungsgruppe aus, und verschieben Sie sie mithilfe des Pfeils nach oben in die Standby-Uplinks-Liste.
- 6 Klicken Sie auf **Weiter**, überprüfen Sie die Meldung, die Sie über die Nutzung der Zwischenkonfiguration für Teaming und Failover informiert, und klicken Sie auf **OK**.
- 7 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Beenden**.

Nächste Schritte

Migrieren Sie physische Netzwerkkarten von eigenständigen Uplinks zu den LAG-Ports.

Zuweisen physischer Netzwerkkarten zu den Ports der Linkzusammenfassungsgruppe

Sie haben die neue Linkzusammenfassungsgruppe (LAG) als Standby in der Teaming- und Failover-Reihenfolge von verteilten Portgruppen festgelegt. Durch die Festlegung der Linkzusammenfassungsgruppe als Standby können Sie die physischen Netzwerkkarten sicher von eigenständigen Uplinks zu den LAG-Ports migrieren, ohne Netzwerkkonnektivität zu verlieren.

Voraussetzungen

- Vergewissern Sie sich, dass sich entweder alle LAG-Ports oder die entsprechenden LACP-aktivierten Ports am physischen Switch in einem aktiven LACP-Aushandlungsmodus befinden.

- Vergewissern Sie sich, dass die physischen Netzwerkkarten, die Sie den LAG-Ports zuweisen möchten, die gleiche Geschwindigkeit haben und mit dem Vollduplexmodus konfiguriert sind.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch, auf dem sich die Linkzusammenfassungsgruppe befindet.
- 2 Wählen Sie im Menü **Aktionen** die Option **Hosts hinzufügen und verwalten** aus.
- 3 Wählen Sie **Hostnetzwerk verwalten** aus.
- 4 Wählen Sie den Host aus, dessen physische Netzwerkkarten Sie den LAG-Ports zuweisen möchten, und klicken Sie auf **Weiter**.
- 5 Wählen Sie auf der Seite „Netzwerkadapteraufgaben auswählen“ die Option **Physische Adapter verwalten** aus und klicken Sie auf **Weiter**.
- 6 Wählen Sie auf der Seite „Physische Netzwerkadapter verwalten“ eine Netzwerkkarte aus und klicken Sie auf **Uplink zuweisen**.
- 7 Wählen Sie einen LAG-Port aus und klicken Sie auf **OK**.
- 8 Wiederholen Sie die Schritte [Schritt 6](#) und [Schritt 7](#) für alle physischen Netzwerkkarten, die Sie den LAG-Ports zuweisen möchten.
- 9 Schließen Sie den Assistenten ab.

Beispiel: Konfigurieren von zwei physischen Netzwerkkarten für eine Linkzusammenfassungsgruppe im Assistenten „Hosts hinzufügen und verwalten“

Wenn Sie z. B. eine Linkzusammenfassungsgruppe mit zwei Ports haben, konfigurieren Sie eine physische Netzwerkkarte für jeden LAG-Port im Assistenten **Hosts hinzufügen und verwalten**.

Nächste Schritte

Legen Sie in der Teaming- und Failover-Reihenfolge der verteilten Portgruppen die Linkzusammenfassungsgruppe als aktiv und alle eigenständigen Uplinks als nicht verwendet fest.

Festlegen einer Linkzusammenfassungsgruppe als aktiv in der Teaming- und Failover-Reihenfolge für eine verteilte Portgruppe

Sie haben physische Netzwerkkarten zu den Ports der Linkzusammenfassungsgruppe migriert. Legen Sie die Linkzusammenfassungsgruppe als aktiv fest und verschieben Sie alle eigenständigen Uplinks als nicht verwendet in die Teaming- und Failover-Reihenfolge der verteilten Portgruppen.

Verfahren

- 1 Navigieren Sie zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Verteilte Portgruppen verwalten** aus.

- 3 Wählen Sie **Teaming und Failover** aus und klicken Sie auf **Weiter**.
- 4 Wählen Sie die Portgruppen aus, in denen Sie die Linkzusammenfassungsgruppe als Standby festgelegt haben und klicken Sie auf **Weiter**.
- 5 Verwenden Sie in der Failover-Reihenfolge die Pfeiltasten, um die Linkzusammenfassungsgruppe in die aktive Liste, alle eigenständigen Uplinks in die nicht verwendete Liste zu verschieben und lassen Sie die Standbyliste leer.
- 6 Klicken Sie auf **Weiter** und anschließend auf **Beenden**.

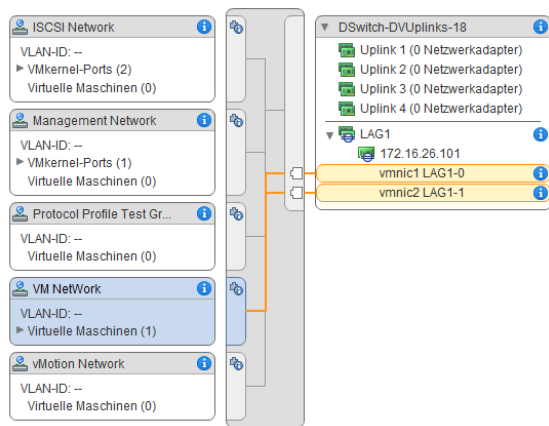
Ergebnisse

Sie haben den Datenverkehr im Netzwerk von eigenständigen Uplinks zu einer Linkzusammenfassungsgruppe für verteilte Portgruppen sicher migriert und eine gültige Konfiguration von LACP-Teaming und -Failover für die Gruppen erstellt.

Beispiel: Topologie eines Distributed Switch, der eine Linkzusammenfassungsgruppe verwendet

Wenn Sie eine Linkzusammenfassungsgruppe mit zwei Ports konfigurieren, um den Datenverkehr einer verteilten Portgruppe zu verarbeiten, können Sie die Topologie des Distributed Switch prüfen, um dessen Änderungen infolge der neuen Konfiguration anzuzeigen.

Abbildung 5-2. Topologie des Distributed Switch mit einer Linkzusammenfassungsgruppe



Bearbeiten einer Linkzusammenfassungsgruppe

Bearbeiten Sie die Einstellungen einer Linkzusammenfassungsgruppe, wenn Sie der Gruppe mehr Ports hinzufügen oder den LACP-Aushandlungsmodus, den Lastenausgleichsalgorithmus oder die VLAN- und NetFlow-Richtlinien ändern möchten.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum vSphere Distributed Switch.
- 2 Wählen Sie **Verwalten** und dann **Einstellungen** aus.
- 3 Wählen Sie **LACP** aus.

- 4 Geben Sie im Textfeld **Name** einen neuen Namen für die Linkzusammenfassungsgruppe ein.
- 5 Ändern Sie die Anzahl an Ports für die Linkzusammenfassungsgruppe, wenn Sie weitere physische Netzwerkkarten hinzufügen möchten.

Die neuen Netzwerkkarten müssen mit den Ports verbunden werden, die Teil eines LACP-Portkanals am physischen Switch bilden.

- 6 Ändern Sie den LACP-Aushandlungsmodus der Linkzusammenfassungsgruppe.

Wenn alle Ports im physischen LACP-Portkanal im aktiven LACP-Modus sind, können Sie den LACP-Modus der Linkzusammenfassungsgruppe zu „Passiv“ ändern und umgekehrt.

- 7 Ändern Sie den Lastausgleichsmodus der Linkzusammenfassungsgruppe.

Sie können unter den von LACP definierten Lastausgleichsalgorithmen auswählen.

- 8 Ändern Sie die VLAN- und die NetFlow-Richtlinien.

Diese Option ist aktiv, wenn die Option für die Außerkraftsetzung der VLAN- und NetFlow-Richtlinien für individuelle Ports in der Uplink-Portgruppe aktiviert ist. Wenn Sie die VLAN- und NetFlow-Richtlinien für die Linkzusammenfassungsgruppe ändern, setzen sie die Richtlinien außer Kraft, die auf der Ebene der Uplink-Portgruppe festgelegt sind.

- 9 Klicken Sie auf **OK**.

Aktivieren der LACP 5.1-Unterstützung für eine Uplink-Portgruppe

Sie können die LACP-Unterstützung für eine Uplink-Portgruppe für vSphere Distributed Switches der Version 5.1 sowie für Switches aktivieren, für die ein Upgrade auf Version 5.5 oder 6.0 durchgeführt wurde und die keine erweiterte LACP-Unterstützung aufweisen.

Voraussetzungen

- Vergewissern Sie sich, dass für jeden Host, auf dem Sie LACP verwenden, ein separater LACP-Port auf dem physischen Switch vorhanden ist.
- Vergewissern Sie sich, dass die Lastausgleichsrichtlinie für verteilte Portgruppen auf „IP-Hash“ festgelegt ist.
- Vergewissern Sie sich, dass der LACP-Portkanal auf dem physischen Switch mit IP-Hash-Lastausgleich konfiguriert ist.
- Vergewissern Sie sich, dass die Richtlinie für die Netzwerkausfallerkennung auf „Nur Verbindungsstatus“ festgelegt ist.
- Vergewissern Sie sich, dass alle Uplinks der verteilten Portgruppen in der Teaming- und Failover-Reihenfolge auf „Aktiv“ festgelegt sind.
- Vergewissern Sie sich, dass alle physischen Netzwerkkarten, die mit den Uplinks verbunden sind, die gleiche Geschwindigkeit haben und im Vollduplexmodus konfiguriert sind.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zu einer Uplink-Portgruppe.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf **Verwandte Objekte**.
 - b Klicken Sie auf **Uplink-Portgruppen** und wählen Sie die Uplink-Portgruppe.
- 2 Klicken Sie auf **Verwalten** und anschließend auf **Einstellungen**.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Aktivieren Sie LACP mithilfe der Dropdown-Liste im LACP-Abschnitt.
- 5 Legen Sie den LACP-Aushandlungsmodus für die Uplink-Portgruppe fest.

Option	Beschreibung
Aktiv	Alle Uplink-Ports der Gruppe befinden sich im aktiven Aushandlungsmodus. Die Uplink-Ports initiieren die Aushandlungen mit den für LACP aktivierten Ports auf dem physischen Switch durch Senden von LACP-Paketen.
Passiv	Alle Uplink-Ports befinden sich im passiven Aushandlungsmodus. Sie reagieren auf empfangene LACP-Pakete, initiieren jedoch keine LACP-Aushandlung.

Wenn sich die für LACP aktivierten Ports auf dem physischen Switch im aktiven Aushandlungsmodus befinden, können Sie die Uplink-Ports in den passiven Modus versetzen und umgekehrt.

- 6 Klicken Sie auf **OK**.

Einschränkungen der LACP-Unterstützung für einen vSphere Distributed Switch

Die LACP-Unterstützung auf einem vSphere Distributed Switch ermöglicht Netzwerkgeräten die Aushandlung der automatischen Paketgenerierung für Links, indem LACP-Pakete an einen Peer gesendet werden. Für die LACP-Unterstützung auf einem vSphere Distributed Switch gelten jedoch einige Einschränkungen.

- Die LACP-Unterstützung ist nicht kompatibel mit dem Software-iSCSI-Mehrfachpfad.
- Die Einstellungen zur LACP-Unterstützung sind in Hostprofilen nicht verfügbar.
- Die LACP-Unterstützung ist zwischen verschachtelten ESXi-Hosts nicht möglich.
- Die LACP-Unterstützung funktioniert nicht mit dem ESXi Dump Collector.
- Die LACP-Steuerungspakete (LACPDU) werden bei Aktivierung der Portspiegelung nicht gespiegelt.
- Die Systemzustandsprüfung für Teaming und Failover funktioniert nicht für Ports von Linkzusammenfassungsgruppen. LACP überprüft die Konnektivität der Ports von Linkzusammenfassungsgruppen.

- Die erweiterte LACP-Unterstützung funktioniert ordnungsgemäß, wenn der Datenverkehr pro verteiltem Port oder verteilter Portgruppe von nur einer Linkzusammenfassengruppe geregelt wird.
- Die Unterstützung von LACP 5.1 funktioniert nur mit IP-Hash-Lastausgleich und Verbindungsstatus-Netzwerk-Failover-Ermittlung.
- Die Unterstützung von LACP 5.1 stellt nur eine Linkzusammenfassengruppe pro Distributed Switch und pro Host bereit.

Sichern und Wiederherstellen von Netzwerkkonfigurationen

6

vSphere 5.1 und höher erlauben die Sicherung und Wiederherstellung der Konfiguration von vSphere Distributed Switches sowie verteilten und Uplink-Portgruppen im Fall von ungültigen Änderungen oder Übertragungen in eine andere Bereitstellung.

Dieses Kapitel enthält die folgenden Themen:

- [Sichern und Wiederherstellen einer vSphere Distributed Switch-Konfiguration](#)
- [Exportieren, Importieren und Wiederherstellen der Konfigurationen für verteilte vSphere-Portgruppen](#)

Sichern und Wiederherstellen einer vSphere Distributed Switch-Konfiguration

vCenter Server bietet die Möglichkeit, die Konfiguration eines vSphere Distributed Switch zu sichern und wiederherzustellen. Sie können die Konfiguration des virtuellen Netzwerks wiederherstellen, nachdem es zu Datenbank- oder Upgrade-Fehlern gekommen ist. Sie können auch eine gespeicherte Switch-Konfiguration als Vorlage nutzen, um eine Kopie des Switch in der gleichen oder einer neuen vSphere-Umgebung zu erstellen.

Sie können eine Konfiguration eines Distributed Switches einschließlich der Portgruppen importieren bzw. exportieren. Weitere Informationen zum Exportieren, Importieren und Wiederherstellen der Konfiguration einer Portgruppe finden Sie unter [Exportieren, Importieren und Wiederherstellen der Konfigurationen für verteilte vSphere-Portgruppen](#).

Hinweis Sie können eine gespeicherte Konfigurationsdatei verwenden, um Richtlinien und Host-Verknüpfungen auf dem Distributed Switch wiederherzustellen. Sie können die Verbindung physischer Netzwerkkarten zu Uplink-Ports oder zu Ports von Linkzusammenfassungsgruppen nicht wiederherstellen.

Exportieren von vSphere Distributed Switch-Konfigurationen

Sie können Konfigurationen von vSphere Distributed Switches und verteilten Portgruppen in eine Datei exportieren. In der Datei werden gültige Netzwerkkonfigurationen aufbewahrt, damit sie an andere Umgebungen übertragen werden können.

Diese Funktion ist nur für vCenter Server 5.1 und höher verfügbar.

Sie können eine Switch-Konfiguration vor dem Upgrade von vCenter Server exportieren, wenn Sie ein Upgrade von vCenter Server 5.1 durchführen. Wenn Sie ein vCenter Server-Upgrade von einer älteren Version als 5.1 durchführen, sichern Sie die Switch-Konfiguration, nachdem Sie vCenter Server auf Version 6.0 aktualisiert haben.

Voraussetzungen

Stellen Sie sicher, dass vCenter Server Version 5.1 oder höher installiert ist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Einstellungen > Konfiguration exportieren**.
- 3 Geben Sie an, dass Sie die Distributed Switch-Konfiguration exportieren möchten, oder exportieren Sie die Distributed Switch-Konfiguration sowie alle Portgruppen.
- 4 (Optional) Geben Sie im Feld **Beschreibungen** Hinweise zu dieser Konfiguration ein.
- 5 Klicken Sie auf **OK**.
- 6 Klicken Sie auf **Ja**, um die Konfigurationsdatei auf Ihrem lokalen System zu speichern.

Nächste Schritte

Mit der exportierten Konfigurationsdatei können Sie die folgenden Aufgaben ausführen:

- Erstellen Sie eine Kopie des exportierten Distributed Switch in einer vSphere-Umgebung. Siehe [Importieren einer vSphere Distributed Switch-Konfiguration](#).
- Überschreiben Sie die Einstellungen eines vorhandenen Distributed Switch. Siehe [Wiederherstellen einer vSphere Distributed Switch-Konfiguration](#).

Sie können auch nur Portgruppenkonfigurationen exportieren, importieren und wiederherstellen. Siehe [Exportieren, Importieren und Wiederherstellen der Konfigurationen für verteilte vSphere-Portgruppen](#).

Importieren einer vSphere Distributed Switch-Konfiguration

Sie können eine gespeicherte Konfigurationsdatei importieren, um einen neuen vSphere Distributed Switch zu erstellen oder um einen zuvor gelöschten Switch wiederherzustellen.

In vSphere 5.1 und höher können Sie einen Distributed Switch mit dem vSphere Web Client importieren.

Die Konfigurationsdatei enthält die Netzwerkeinstellungen für den Switch. Sie können den Switch damit auch in anderen virtuellen Umgebungen replizieren.

Hinweis Sie können eine gespeicherte Konfigurationsdatei verwenden, um die Switch-Instanz, deren Hostzuordnungen und die Richtlinien zu replizieren. Die Verbindung von physischen Netzwerkkarten zu Uplink-Ports oder Ports in Linkzusammenfassungsgruppen kann nicht repliziert werden.

Voraussetzungen

Stellen Sie sicher, dass vCenter Server die Version 5.1.0 oder höher aufweist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zu einem Datacenter.
- 2 Klicken Sie mit der rechten Maustaste auf das Datacenter und wählen Sie **Distributed Switch > Distributed Switch importieren** aus.
- 3 Wechseln Sie zum Verzeichnis der Konfigurationsdatei.
- 4 Um dem Switch und seinen Portgruppen die Schlüssel aus der Konfigurationsdatei zuzuweisen, aktivieren Sie das Kontrollkästchen **Ursprünglichen Distributed Switch und Portgruppen-IDs beibehalten** und klicken Sie auf **Weiter**.

Die Option **Ursprünglichen Distributed Switch und Portgruppen-IDs beibehalten** können Sie in folgenden Fällen verwenden:

- Neuerstellen eines gelöschten Switches
- Wiederherstellen eines Switches, dessen Upgrade fehlgeschlagen ist

Alle Portgruppen werden neu erstellt, und die Hosts, die mit dem Switch verbunden waren, werden wieder hinzugefügt.

- 5 Überprüfen Sie die Einstellungen für den Switch und klicken Sie auf **Beenden**.

Ergebnisse

Ein neuer Distributed Switch wird mit Einstellungen aus der Konfigurationsdatei erstellt. Wenn Informationen über verteilte Portgruppen in Ihrer Konfigurationsdatei enthalten sind, werden auch die Portgruppen erstellt.

Wiederherstellen einer vSphere Distributed Switch-Konfiguration

Verwenden Sie die Wiederherstellungsoption, um die Konfiguration eines bestehenden Distributed Switch auf die Einstellungen in der Konfigurationsdatei zurückzusetzen. Das

Wiederherstellen eines Distributed Switch ändert die Einstellungen auf dem ausgeählten Switch zurück auf die Einstellungen, die in der Konfigurationsdatei gespeichert sind.

Hinweis Sie können eine gespeicherte Konfigurationsdatei verwenden, um Richtlinien und Host-Verknüpfungen auf dem Distributed Switch wiederherzustellen. Sie können die Verbindung physischer Netzwerkkarten zu Uplink-Ports oder zu Ports von Linkzusammenfassungsgruppen nicht wiederherstellen.

Voraussetzungen

Stellen Sie sicher, dass vCenter Server Switch Version 5.1 oder höher ist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie mit der rechten Maustaste auf den Distributed Switch im Navigator und wählen Sie **Einstellungen > Konfiguration wiederherstellen** aus.
- 3 Navigieren Sie zur Konfigurationssicherungsdatei, die Sie verwenden möchten.
- 4 Wählen Sie **Distributed Switch und alle Portgruppen wiederherstellen** oder **Nur Distributed Switch wiederherstellen**, und klicken Sie auf **Weiter**.
- 5 Prüfen Sie die zusammengefassten Informationen für die Wiederherstellung.

Das Wiederherstellen eines Distributed Switch überschreibt die aktuellen Einstellungen des Distributed Switch und seiner Portgruppe. Dabei werden bestehende Portgruppen nicht gelöscht, die nicht Teil der Konfigurationsdatei sind.

- 6 Klicken Sie auf **Beenden**.

Die Distributed Switch-Konfiguration wurde auf die Einstellungen in der Konfigurationsdatei zurückgesetzt.

Exportieren, Importieren und Wiederherstellen der Konfigurationen für verteilte vSphere-Portgruppen

Sie können die Konfigurationen verteilter vSphere-Portgruppen in eine Datei exportieren. Mithilfe der Konfigurationsdatei können Sie gültige Portgruppenkonfigurationen beibehalten, sodass die Verteilung dieser Konfigurationen an andere Bereitstellungen möglich ist.

Sie können Informationen zu Portgruppen und Distributed Switch-Konfigurationen gleichzeitig exportieren. Siehe [Sichern und Wiederherstellen einer vSphere Distributed Switch-Konfiguration](#).

Exportieren der Konfigurationen für verteilte vSphere-Portgruppen

Sie können die Konfigurationen einer verteilten Portgruppe in eine Datei exportieren. Die Konfiguration behält gültige Netzwerkkonfigurationen bei, sodass die Verteilung dieser Konfigurationen an andere Bereitstellungen möglich ist.

Diese Funktionen sind nur für vSphere Web Client 5.1 oder höher verfügbar. Sie können jedoch Einstellungen aus allen Versionen eines verteilten Ports exportieren, wenn Sie vSphere Web Client 5.1 oder höher verwenden.

Verfahren

- 1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**.
- 2 Klicken Sie mit der rechten Maustaste auf die verteilte Portgruppe und wählen Sie **Konfiguration exportieren** aus.
- 3 (Optional) Geben Sie im Feld **Beschreibungen** Hinweise zu dieser Konfiguration ein.
- 4 Klicken Sie auf **OK**.

Klicken Sie auf **Ja**, um die Konfigurationsdatei auf Ihrem lokalen System zu speichern.

Ergebnisse

Sie verfügen jetzt über eine Konfigurationsdatei, in der alle Einstellungen für die ausgewählte verteilte Portgruppe enthalten sind. Sie können diese Datei zum Erstellen mehrerer Kopien dieser Konfiguration auf einer vorhandenen Bereitstellung verwenden oder Einstellungen bestehender verteilter Portgruppen überschreiben, damit diese den ausgewählten Einstellungen entsprechen.

Nächste Schritte

Mit der exportierten Konfigurationsdatei können Sie die folgenden Aufgaben ausführen:

- Informationen zum Erstellen einer Kopie der exportierten verteilten Portgruppe finden Sie unter [Importieren einer Konfiguration für verteilte vSphere-Portgruppen](#).
- Informationen zum Überschreiben der Einstellungen einer vorhandenen verteilten Portgruppe finden Sie unter [Wiederherstellen einer Konfiguration für verteilte vSphere-Portgruppen](#).

Importieren einer Konfiguration für verteilte vSphere-Portgruppen

Verwenden Sie die Importfunktion, um eine verteilte Portgruppe aus einer Konfigurationsdatei zu erstellen.

Falls eine bestehende Portgruppe denselben Namen wie die importierte Portgruppe besitzt, wird dem Namen der neuen Portgruppe eine Zahl in Klammern angefügt. Die Einstellungen aus der importierten Konfiguration werden auf die neue Portgruppe angewendet, und die Einstellungen der ursprünglichen Portgruppe bleiben unverändert.

Diese Funktionen sind nur für vSphere Web Client 5.1 oder höher verfügbar. Sie können jedoch Einstellungen aus allen Versionen eines verteilten Ports exportieren, wenn Sie den vSphere Web Client 5.1 und höher verwenden.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Verteilte Portgruppe > Verteilte Portgruppe importieren** aus.
- 3 Wechseln Sie zum Verzeichnis Ihrer gespeicherten Konfigurationsdatei und klicken Sie auf **Weiter**.
- 4 Prüfen Sie die Importeinstellungen, bevor Sie den Import durchführen.
- 5 Klicken Sie auf **Beenden**.

Wiederherstellen einer Konfiguration für verteilte vSphere-Portgruppen

Verwenden Sie die Wiederherstellungsoption, um die Konfiguration einer bestehenden verteilten Portgruppe auf die Einstellungen in einer Konfigurationsdatei zurückzusetzen.

Diese Funktionen sind nur für vSphere Web Client 5.1 oder höher verfügbar. Sie können aber Einstellungen von jeder Distributed Switch-Version wiederherstellen, wenn Sie den vSphere Web Client 5.1 oder höher verwenden.

Verfahren

- 1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**.
- 2 Klicken Sie mit der rechten Maustaste auf die verteilte Portgruppe und wählen Sie **Konfiguration wiederherstellen** aus.
- 3 Wählen Sie eine der folgenden Optionen, und klicken Sie auf **Weiter**:
 - ◆ **Auf frühere Konfiguration zurücksetzen**, um die Portgruppenkonfiguration um einen Schritt zurückzusetzen. Sie können die Portgruppenkonfiguration nicht vollständig wiederherstellen, falls Sie mehr als einen Schritt ausgeführt haben.
 - ◆ **Konfiguration aus einer Datei wiederherstellen** ermöglicht das Wiederherstellen der Portgruppenkonfiguration aus einer exportierten Sicherungsdatei. Sie können auch eine Distributed Switch-Sicherungsdatei verwenden, sofern sie Konfigurationsinformationen für die Portgruppe enthält.

- 4 Prüfen Sie die zusammengefassten Informationen für die Wiederherstellung.

Beim Wiederherstellungsvorgang werden die aktuellen Einstellungen der verteilten Portgruppe mit den Einstellungen aus der Sicherungsdatei überschrieben. Falls Sie die Portgruppenkonfiguration aus einer Switch-Sicherungsdatei wiederherstellen, werden beim Wiederherstellungsvorgang vorhandene Portgruppen, die nicht Bestandteil der Datei sind, nicht gelöscht.

5 Klicken Sie auf **Beenden**.

Rollback und Wiederherstellung des Verwaltungsnetzwerks

7

In vSphere 5.1 und höher können Sie eine fehlerhafte Konfiguration des Verwaltungsnetzwerks mithilfe der Rollback- und Wiederherstellungsunterstützung des vSphere Distributed Switch und vSphere Standard-Switch verhindern bzw. frühere Konfigurationen wiederherstellen.

Rollback ist für den Einsatz auf Standard und Distributed Switches verfügbar. Für die Korrektur einer fehlerhaften Konfiguration des Verwaltungsnetzwerks können Sie eine direkte Verbindung mit einem Host herstellen, um die Probleme über die DCUI zu beheben.

Dieses Kapitel enthält die folgenden Themen:

- [vSphere-Netzwerk-Rollback](#)
- [Beheben von Fehlern bei der Konfiguration des Verwaltungsnetzwerks auf einem vSphere Distributed Switch](#)

vSphere-Netzwerk-Rollback

Durch das Rollback von Konfigurationsänderungen verhindert vSphere, dass Hosts die Verbindung mit vCenter Server aufgrund einer Fehlkonfiguration des Verwaltungsnetzwerks verlieren.

Das Netzwerk-Rollback ist in vSphere 5.1 und höher standardmäßig aktiviert. Allerdings können Sie Rollbacks auf vCenter Server-Ebene aktivieren bzw. deaktivieren.

Host-Netzwerk-Rollbacks

Host-Netzwerk-Rollbacks werden vorgenommen, wenn eine ungültige Änderung an der Netzwerk-Konfiguration für die Verbindung mit vCenter Server vorgenommen wird. Jede Netzwerkänderung, die einen Host trennt, löst ebenfalls ein Rollback aus. Die folgenden Beispiele für Änderungen an der Host-Netzwerk-Konfiguration können ein Rollback auslösen:

- Aktualisieren der Geschwindigkeit oder der Duplex-Einstellung einer physischen Netzwerkkarte.
- Aktualisieren der DNS- und Routing-Einstellungen.
- Aktualisieren der Gruppierungs- und Failover-Richtlinien bzw. der Traffic-Shaping-Richtlinien einer Standard-Portgruppe, die den VMkernel-Netzwerkadapter für die Verwaltung enthält.

- Aktualisieren des VLAN einer Standard-Portgruppe, die den VMkernel-Netzwerkadapter für die Verwaltung enthält.
- Erhöhen des MTU-Werts des VMkernel-Netzwerkadapters für die Verwaltung und dessen Switch auf Werte, die von der physischen Infrastruktur nicht unterstützt werden.
- Ändern der IP-Einstellungen der VMkernel-Netzwerkadapter für die Verwaltung.
- Entfernen der VMkernel-Netzwerkadapter für die Verwaltung von einem Standard-Switch oder einem Distributed Switch.
- Entfernen einer physischen Netzwerkkarte eines Standard-Switch oder eines Distributed Switch, der den VMkernel-Netzwerkadapter für die Verwaltung enthält.
- Migrieren des VMkernel-Verwaltungsadapters von vSphere Standard zu einem Distributed Switch.

Wenn ein Netzwerk aus einem dieser Gründe getrennt wird, schlägt die Aufgabe fehl und der Host wird auf die letzte gültige Konfiguration zurückgesetzt.

vSphere Distributed Switch-Rollbacks

Distributed Switch-Rollbacks werden vorgenommen, wenn ungültige Updates an Distributed Switches, verteilten Portgruppen oder verteilten Ports vorgenommen werden. Die folgenden Änderungen an der Konfiguration von Distributed Switches lösen ein Rollback aus:

- Ändern des MTU-Werts eines Distributed Switch.
- Ändern der folgenden Einstellungen in der verteilten Portgruppe des VMkernel-Netzwerkadapters für die Verwaltung:
 - Teaming und Failover
 - VLAN
 - Traffic-Shaping
- Blockieren aller Ports in der verteilten Portgruppe, die den VMkernel-Netzwerkadapter für die Verwaltung enthält.
- Außerkraftsetzen der Richtlinien auf der Ebene des verteilten Ports für den VMkernel-Netzwerkadapter für die Verwaltung.

Wenn eine Änderung zu einer ungültigen Konfiguration führt, sind möglicherweise ein oder mehrere Hosts nicht mehr mit dem Distributed Switch synchron.

Wenn Sie wissen, durch welche Einstellung dieser Konflikt hervorgerufen wird, können Sie die Einstellung manuell ändern. Wenn Sie beispielsweise einen VMkernel-Netzwerkadapter für die Verwaltung auf ein neues VLAN migriert haben, wird das VLAN möglicherweise nicht vom physischen Switch gebündelt. Wenn Sie die Konfiguration des physischen Switches korrigieren, behebt die nächste Synchronisierung des Distributed Switch mit dem Host das Konfigurationsproblem.

Wenn Sie die Ursache des Problems nicht ermitteln können, führen Sie ein Rollback des Distributed Switch oder der verteilten Portgruppe auf eine frühere Konfiguration durch. Siehe [Wiederherstellen einer Konfiguration für verteilte vSphere-Portgruppen](#).

Deaktivieren des Netzwerk-Rollbacks

Das Rollback ist in vSphere 5.1 und höher standardmäßig aktiviert. Sie können das Rollback in vCenter Server mit dem vSphere Web Client deaktivieren.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zu einer vCenter Server-Instanz.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Wählen Sie **Erweiterte Einstellungen** aus und klicken Sie auf **Bearbeiten**.
- 4 Wählen Sie den Schlüssel `config.vpxd.network.rollback` aus und ändern Sie den Wert in „false“.

Wenn der Schlüssel nicht vorhanden ist, können Sie ihn hinzufügen und den Wert auf „false“ setzen.

- 5 Klicken Sie auf **OK**.
- 6 Starten Sie vCenter Server neu, um die Änderungen anzuwenden.

Deaktivieren des Netzwerk-Rollbacks unter Verwendung der vCenter Server-Konfigurationsdatei

Das Rollback ist in vSphere 5.1 und höher standardmäßig aktiviert. Sie können das Rollback durch direkte Bearbeitung der Konfigurationsdatei `vpxd.cfg` von vCenter Server deaktivieren.

Verfahren

- 1 Navigieren Sie auf der Hostmaschine von vCenter Server zu dem Verzeichnis, in dem die Konfigurationsdatei gespeichert ist:
 - Bei einem Windows Server-Betriebssystem finden Sie dieses Verzeichnis unter `C:\ProgramData\VMware\CIS\cfg\vmware-vpx`.
 - Bei der vCenter Server Appliance finden Sie dieses Verzeichnis unter `/etc/vmware-vpx`.
- 2 Öffnen Sie die Datei `vpxd.cfg` zur Bearbeitung.
- 3 Legen Sie im Element `<network>` das Element `<rollback>` auf **false** fest:

```
<config>
  <vpxd>
    <network>
      <rollback>false</rollback>
    </network>
  </vpxd>
</config>
```

- 4 Speichern und schließen Sie die Datei.
- 5 Starten Sie das vCenter Server-System neu.

Beheben von Fehlern bei der Konfiguration des Verwaltungsnetzwerks auf einem vSphere Distributed Switch

In vSphere 5.1 und höher können Sie mithilfe der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) die Verbindung zwischen vCenter Server und einem Host, der über einen Distributed Switch auf das Verwaltungsnetzwerk zugreift, wiederherstellen.

Falls das Netzwerk-Rollback deaktiviert ist, wird durch eine fehlerhafte Konfiguration der Portgruppe für das Verwaltungsnetzwerk auf dem Distributed Switch die Verbindung zwischen vCenter Server und den Hosts, die diesem Switch hinzugefügt wurden, getrennt. Sie müssen mithilfe von DCUI mit jedem Host einzeln eine Verbindung herstellen.

Wenn die Uplinks, die Sie zum Wiederherstellen des Verwaltungsnetzwerks verwenden, auch von VMkernel-Adaptern verwendet werden, die andere Datenverkehrstypen verarbeiten (vMotion, Fault Tolerance usw.), dann verlieren die Adapter nach der Wiederherstellung die Verbindung zum Netzwerk.

Weitere Informationen zum Zugriff auf und zum Verwenden von DCUI finden Sie in der Dokumentation *vSphere-Sicherheit*.

Hinweis Die Wiederherstellung der Verwaltungsverbindung auf einem Distributed Switch wird für statusfreie ESXi-Instanzen nicht unterstützt.

Voraussetzungen

Vergewissern Sie sich, dass für das Verwaltungsnetzwerk eine Portgruppe auf dem Distributed Switch konfiguriert ist.

Verfahren

- 1 Stellen Sie eine Verbindung mit der DCUI des Hosts her.
- 2 Wählen Sie im Menü **Optionen der Netzwerkwiederherstellung** die Option **vDS wiederherstellen** aus.
- 3 Konfigurieren Sie die Uplinks und optional das VLAN für das Verwaltungsnetzwerk.
- 4 Wenden Sie die Konfiguration an.

Ergebnisse

Die DCUI erstellt einen lokalen flüchtigen Port und wendet die von Ihnen für das VLAN und die Uplinks angegebenen Werte an. Die DCUI verschiebt den VMkernel-Adapter für das Verwaltungsnetzwerk auf den neuen lokalen Port, um die Konnektivität mit vCenter Server wiederherzustellen.

Nächste Schritte

Nachdem die Verbindung des Hosts zu vCenter Server wiederhergestellt wurde, korrigieren Sie die Konfiguration der verteilten Portgruppe und fügen den VMkernel-Adapter erneut zur Gruppe hinzu.

Richtlinien, die auf der Ebene der Standard-Switches oder der verteilten Portgruppen festgelegt werden, gelten für alle Portgruppen auf dem Standard-Switch bzw. für alle Ports in der verteilten Portgruppe. Ausnahmen bilden die Konfigurationsoptionen, die auf der Ebene der Standard-Portgruppe oder der verteilten Ports außer Kraft gesetzt werden.

Das Video enthält Informationen zur Anwendung von Netzwerkrichtlinien auf vSphere Standard-Switches und Distributed Switches.



Arbeiten mit Netzwerkrichtlinien

(https://vmwaretv.vmware.com/media/t/1_Objjobp2b)

- **Anwenden von Netzwerkrichtlinien auf einen vSphere Standard oder Distributed Switch**

Netzwerkrichtlinien werden auf vSphere Standard Switches und vSphere Distributed Switches unterschiedlich angewandt. Nicht alle für einen vSphere Distributed Switch verfügbaren Richtlinien sind auch für einen vSphere Standard Switch verfügbar.

- **Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene**

Um verschiedene Richtlinien für verteilte Ports anzuwenden, konfigurieren Sie das Pro-Port-Überschreiben der Richtlinien, die auf der Portgruppenebene festgelegt sind. Sie können außerdem eine beliebige Konfiguration, die auf der Pro-Port-Ebene festgelegt ist, zurücksetzen, wenn die Verbindung eines verteilten Ports mit einer virtuellen Maschine aufgehoben wird.

- **Teaming- und Failover-Richtlinie**

Anhand der NIC-Gruppierung können Sie die Netzwerkkapazität eines virtuellen Switch erhöhen, indem Sie zwei oder mehr physische Netzwerkkarten in einer Gruppe zusammenfassen. Um zu bestimmen, wie der Datenverkehr im Fall eines Adapterfehlers umgeleitet wird, schließen Sie physische Netzwerkkarten in einer Failover-Reihenfolge ein. Um zu bestimmen, wie der virtuelle Switch den Netzwerkdatenverkehr zwischen den physischen Netzwerkkarten in einer Gruppe verteilt, wählen Sie Lastausgleichsalgorithmen aus, die sich für die Bedürfnisse und Kapazitäten Ihrer Umgebung eignen.

- **VLAN-Richtlinie**

Die VLAN-Richtlinien legen fest, wie VLANs in Ihrer Netzwerkumgebung funktionieren.

- **Sicherheitsrichtlinie**

Die Netzwerksicherheitsrichtlinie bietet Schutz des Datenverkehrs vor der Imitation von MAC-Adressen und unerwünschten Portprüfungen.

- **Traffic-Shaping-Richtlinie**

Eine Traffic-Shaping-Richtlinie wird anhand der durchschnittlichen Bandbreite, der Spitzenbandbreite und der Burstgröße definiert. Sie können für jede Portgruppe sowie jede verteilte Portgruppe und jeden verteilten Port eine Traffic-Shaping-Richtlinie erstellen.

- **Ressourcenzuteilungsrichtlinie**

Mit der Ressourcenzuteilungsrichtlinie können Sie einen verteilten Port oder eine verteilte Portgruppe zu einem von einem Benutzer erstellten Netzwerkressourcenpool zuordnen. Mit dieser Richtlinie lässt sich die Bandbreite für den Port oder die Portgruppe besser steuern.

- **Überwachungsrichtlinie**

Die Überwachungsrichtlinie aktiviert oder deaktiviert die NetFlow-Überwachung auf einem verteilten Port oder einer Portgruppe.

- **Richtlinien für das Filtern und Markieren des Datenverkehrs**

In vSphere Distributed Switch 5.5 und neueren Versionen können Sie das virtuelle Netzwerk durch Verwendung der Richtlinie zum Filtern und Markieren des Datenverkehrs vor unerwünschtem Datenverkehr und Angriffen auf die Sicherheit schützen oder einer bestimmten Art von Datenverkehr ein QoS-Tag zuordnen.

- **Verwalten von Richtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch**

Sie können die Netzwerkrichtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch ändern.

- **Portblockierungsrichtlinien**

Mit Portblockierungsrichtlinien können Sie ausgewählte Ports daran hindern, Daten zu senden oder zu empfangen.

Anwenden von Netzwerkrichtlinien auf einen vSphere Standard oder Distributed Switch

Netzwerkrichtlinien werden auf vSphere Standard Switches und vSphere Distributed Switches unterschiedlich angewandt. Nicht alle für einen vSphere Distributed Switch verfügbaren Richtlinien sind auch für einen vSphere Standard Switch verfügbar.

Tabelle 8-1. Virtual Switch-Objekte, für die Richtlinien gelten

Virtueller Switch	Virtual Switch-Objekt	Beschreibung
vSphere Standard-Switch	Gesamter Switch	Wenn Sie Richtlinien auf den gesamten Standard-Switch anwenden, werden die Richtlinien auf alle Standardportgruppen auf dem Switch ausgeweitet.
	Standard-Portgruppe	Sie können unterschiedliche Richtlinien auf einzelne Portgruppen anwenden, indem Sie die vom Switch vererbten Richtlinien außer Kraft setzen.
vSphere Distributed Switch	Verteilte Portgruppe	Wenn Sie Richtlinien auf eine verteilte Portgruppe anwenden, werden die Richtlinien an alle Ports in der Gruppe weitergegeben.
	Verteilter Port	Sie können unterschiedliche Richtlinien auf einzelne verteilte Ports anwenden, indem Sie die von der verteilten Portgruppe vererbten Richtlinien außer Kraft setzen.
	Uplink-Portgruppe	Sie können Richtlinien auf der Ebene der Uplink-Portgruppe anwenden, und die Richtlinien werden an alle Ports in der Gruppe weitergegeben.
	Uplink-Port	Sie können unterschiedliche Richtlinien auf einzelne Uplink-Ports anwenden, indem Sie die von der Uplink-Portgruppe vererbten Richtlinien außer Kraft setzen.

Tabelle 8-2. Verfügbare Richtlinien für einen vSphere Standard Switch und vSphere Distributed Switch

Richtlinie	Standard-Switch	Distributed Switch	Beschreibung
Teaming und Failover	Ja	Ja	Damit können Sie die physischen Netzwerkkarten konfigurieren, die den Netzwerkverkehr für einen Standard-Switch, eine Standard-Portgruppe, eine verteilte Portgruppe oder einen verteilten Port bearbeiten. Sie ordnen die physischen Netzwerkkarten in einer Failover-Reihenfolge an und wenden unterschiedliche Lastausgleichrichtlinien darauf an.
Sicherheit	Ja	Ja	Bietet Schutz des Datenverkehrs vor der Imitation von MAC-Adressen und unerwünschten Portprüfungen. Die Netzwerksicherheitsrichtlinie ist in Schicht 2 des Netzwerk-Protokoll-Stacks implementiert.
Traffic-Shaping	Ja	Ja	Damit beschränken Sie die Netzwerkbandbreite, die Ports zur Verfügung steht, ermöglichen aber auch Datenverkehr-Bursts mit höherer Geschwindigkeit. ESXi steuert den ausgehenden Netzwerkverkehr auf Standard-Switches sowie den ein- und ausgehenden Datenverkehr auf Distributed Switches.

Tabelle 8-2. Verfügbare Richtlinien für einen vSphere Standard Switch und vSphere Distributed Switch (Fortsetzung)

Richtlinie	Standard-Switch	Distributed Switch	Beschreibung
VLAN	Ja	Ja	Damit können Sie VLAN-Tagging für einen Standard- oder Distributed Switch konfigurieren. Sie können External Switch Tagging (EST), Virtual Switch Tagging (VST) und Virtual Guest Tagging (VGT) konfigurieren.
Überwachen	Nein	Ja	Aktiviert und deaktiviert die NetFlow-Überwachung an einem verteilten Port oder einer Portgruppe.
Filtern und Markieren des Datenverkehrs	Nein	Ja	Ermöglicht den Schutz des virtuellen Netzwerks vor unerwünschtem Datenverkehr und Sicherheitsangriffen bzw. die Anwendung eines QoS-Tag auf einen bestimmten Datenverkehrstyp.
Ressourcenzuteilung	Nein	Ja	Ermöglicht die Zuordnung eines verteilten Ports oder einer Portgruppe zu einem benutzerdefinierten Netzwerkressourcenpool. So können Sie die für den Port oder die Portgruppe verfügbare Bandbreite besser kontrollieren. Die Ressourcenzuteilungsrichtlinie kann für vSphere Network I/O Control Version 2 und 3 verwendet werden.
Portblockierung	Nein	Ja	Ermöglicht die selektive Blockierung von Ports für das Senden und Empfangen von Daten.

Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene

Um verschiedene Richtlinien für verteilte Ports anzuwenden, konfigurieren Sie das Pro-Port-Überschreiben der Richtlinien, die auf der Portgruppenebene festgelegt sind. Sie können außerdem eine beliebige Konfiguration, die auf der Pro-Port-Ebene festgelegt ist, zurücksetzen, wenn die Verbindung eines verteilten Ports mit einer virtuellen Maschine aufgehoben wird.

Verfahren

- 1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**.
- 2 Klicken Sie mit der rechten Maustaste auf die verteilte Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.

3 Wählen Sie die Seite **Erweitert** aus.

Option	Beschreibung
Zurücksetzen bei Verbindungstrennung konfigurieren	Aktivieren oder deaktivieren Sie im Dropdown-Menü das Zurücksetzen bei einer Verbindungstrennung. Wenn ein verteilter Port von einer virtuellen Maschine getrennt wird, wird seine Konfiguration auf die Einstellung der verteilten Portgruppe zurückgesetzt. Alle portspezifischen Außerkraftsetzungen werden verworfen.
Portrichtlinien außer Kraft setzen	Wählen Sie die Richtlinien für verteilte Portgruppen aus, die für einzelne Ports außer Kraft gesetzt werden sollen.

4 (Optional) Verwenden Sie die Richtlinienseiten, um Außerkraftsetzungen für jede Portrichtlinie festzulegen.

5 Klicken Sie auf **OK**.

Teaming- und Failover-Richtlinie

Anhand der NIC-Gruppierung können Sie die Netzwerkkapazität eines virtuellen Switch erhöhen, indem Sie zwei oder mehr physische Netzwerkkarten in einer Gruppe zusammenfassen. Um zu bestimmen, wie der Datenverkehr im Fall eines Adapterfehlers umgeleitet wird, schließen Sie physische Netzwerkkarten in einer Failover-Reihenfolge ein. Um zu bestimmen, wie der virtuelle Switch den Netzwerkdatenverkehr zwischen den physischen Netzwerkkarten in einer Gruppe verteilt, wählen Sie Lastausgleichsalgorithmen aus, die sich für die Bedürfnisse und Kapazitäten Ihrer Umgebung eignen.

NIC-Gruppierungsrichtlinien

Anhand der NIC-Gruppierung können Sie einen virtuellen Switch mit mehreren physischen Netzwerkkarten auf einem Host verbinden, um die Netzwerkbandbreite des Switch zu erhöhen und Redundanz bereitzustellen. Eine NIC-Gruppe kann den Datenverkehr zwischen ihren Mitgliedern verteilen und bei einem Adapterfehler oder einem Netzwerkausfall passives Failover bereitstellen. NIC-Gruppierungsrichtlinien werden für einen vSphere Standard Switch auf der Ebene des virtuellen Switch oder der Portgruppe und für einen vSphere Distributed Switch auf der Ebene des Ports oder der Portgruppe festgelegt.

Hinweis Alle Ports am physischen Switch in der gleichen Gruppe müssen sich in der gleichen Broadcast-Domäne der Ebene 2 befinden.

Lastausgleichsrichtlinie

Die Lastausgleichsrichtlinie bestimmt, wie der Netzwerkdatenverkehr zwischen den Netzwerkadaptern in einer NIC-Gruppe verteilt wird. Bei virtuellen vSphere-Switches erfolgt der Lastausgleich nur für den ausgehenden Datenverkehr. Der eingehende Datenverkehr wird durch die Lastausgleichsrichtlinie auf dem physischen Switch gesteuert.

Weitere Informationen zu den einzelnen Lastausgleichsalgorithmen finden Sie unter [Verfügbare Lastausgleichsalgorithmen für virtuelle Switches](#).

Richtlinie für die Netzwerkausfallerkennung

Sie können eine der folgenden Methoden festlegen, die von einem virtuellen Switch für die Ausfallerkennung verwendet werden.

Nur Verbindungsstatus

Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Ermittelt Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches. Der Verbindungsstatus ermittelt jedoch nicht die folgenden Konfigurationsfehler:

- Die Blockierung eines Ports des physischen Switches durch STP (Spanning Tree Protocol), eine Zuweisung zum falschen VLAN.
- Nicht angeschlossene Kabel zwischen einem physischen Switch und einem anderen Netzwerkgerät, z. B. einem Upstream-Switch.

Signalprüfung

Sendet Ethernet-Broadcast-Frames und hört diese ab (Signalprüfung), welche von physischen Netzwerkkarten gesendet werden, um Verbindungsfehler in allen physischen Netzwerkkarten in einer Gruppe zu ermitteln. ESXi-Hosts senden jede Sekunde Signalkarte. Die Signalprüfung eignet sich am besten zur Fehlerermittlung in dem physischen Switch, der dem ESXi-Host am nächsten liegt, bei dem der Fehler kein „Link deaktiviert“-Ereignis für den Host verursacht.

Verwenden Sie die Signalprüfung bei mindestens drei Netzwerkkarten in einer Gruppe, da ESXi Fehler eines einzelnen Adapters erkennen kann. Wenn nur zwei Netzwerkkarten zugewiesen sind und für eine der Netzwerkkarten die Verbindung getrennt wird, kann der Switch nicht ermitteln, welche Netzwerkkarte außer Betrieb genommen werden muss, da beide Netzwerkkarten keine Signale empfangen und demzufolge alle Pakete an beide Uplinks gesendet werden. Die Verwendung von mindestens drei Netzwerkkarten in einer solchen Gruppe erlaubt $n-2$ Fehler, wobei n für die Anzahl der Netzwerkkarten in der Gruppe steht, bevor eine unklare Situation eintritt.

Failback-Richtlinie

Standardmäßig ist für eine NIC-Gruppe eine Failback-Richtlinie aktiviert. Wenn eine ausgefallene physische Netzwerkkarte wieder online geht, legt der virtuelle Switch die Netzwerkkarte wieder als aktiv fest, indem die Standby-Netzwerkkarte ersetzt wird, die deren Steckplatz übernommen hatte.

Wenn die physische Netzwerkkarte, die in der Failover-Reihenfolge an erster Stelle steht, immer wieder ausfällt, kann die Failback-Richtlinie häufige Änderungen der verwendeten Netzwerkkarte verursachen. Der physische Switch stellt häufige Änderungen der MAC-Adressen fest, und möglicherweise akzeptiert der Port des physischen Switch nicht sofort Datenverkehr, wenn der Adapter online geschaltet wird. Um diese Verzögerungen zu minimieren, können die folgenden Einstellungen des physischen Switch geändert werden:

- Deaktivieren Sie das Spanning-Tree-Protocol (STP) für physische Netzwerkkarten, die mit den ESXi-Hosts verbunden sind.
- Aktivieren Sie für Cisco-basierte Netzwerke den PortFast-Modus für Zugriffsschnittstellen oder den PortFast-Trunk-Modus für Trunk-Schnittstellen. Dadurch können ca. 30 Sekunden während der Initialisierung des Ports des physischen Switches eingespart werden.
- Deaktivieren Sie die Trunking-Aushandlung.

Richtlinie zur Switch-Benachrichtigung

Wenn Sie die Richtlinie zur Switch-Benachrichtigung verwenden, können Sie festlegen, wie der ESXi-Host über Failover-Ereignisse benachrichtigt. Wenn eine physische Netzwerkkarte eine Verbindung zum virtuellen Switch herstellt oder wenn der Datenverkehr zu einer anderen physischen Netzwerkkarte in der Gruppe umgeleitet wird, sendet der virtuelle Switch Benachrichtigungen über das Netzwerk, um die Lookup-Tabellen der physischen Switches zu aktualisieren. Durch das Benachrichtigen des physischen Switches wird die geringste Latenz bei Eintreten eines Failovers oder einer Migration mit vSphere vMotion erreicht.

Verfügbare Lastausgleichsalgorithmen für virtuelle Switches

Sie können verschiedene Lastausgleichsalgorithmen auf einem virtuellen Switch konfigurieren und bestimmen, wie der Netzwerkverkehr zwischen den physischen Netzwerkkarten in einer Teaming-Gruppe verteilt wird.

- **Routen anhand des ursprünglichen virtuellen Ports**
Der virtuelle Switch wählt Uplinks auf der Grundlage der Port-IDs der virtuellen Maschine auf dem vSphere Standard-Switch oder vSphere Distributed Switch aus.
- **Routen anhand des Quell-MAC-Hash**
Der virtuelle Switch wählt einen Uplink für eine virtuelle Maschine auf der Grundlage der MAC-Adresse der virtuellen Maschine aus. Zum Berechnen eines Uplinks für eine virtuelle Maschine verwendet der virtuelle Switch die MAC-Adresse der virtuellen Maschine und die Anzahl der Uplinks in der Netzwerkkartengruppe.
- **Routen anhand des IP-Hash**
Der virtuelle Switch wählt Uplinks für virtuelle Maschinen anhand der Quell- und Ziel-IP-Adresse jedes Pakets aus.

- **Routen anhand der physischen Netzwerkkartenauslastung**

„Anhand der physischen Netzwerkkartenauslastung routen“ basiert auf „Anhand des ursprünglichen virtuellen Ports routen“, wobei der virtuelle Switch die effektive Auslastung der Uplinks prüft und die entsprechenden Schritte zum Verringern der Last auf überlasteten Uplinks ausführt. Ist nur für vSphere Distributed Switch verfügbar.

- **Ausdrückliche Failover-Reihenfolge verwenden**

Bei dieser Richtlinie ist kein effektiver Lastausgleich verfügbar. Der virtuelle Switch verwendet immer den Uplink, der an erster Stelle der Liste der aktiven Adapter in der Failover-Reihenfolge steht und die Failover-Ermittlungskriterien erfüllt. Wenn keine Uplinks in der Liste „Aktiv“ verfügbar sind, verwendet der virtuelle Switch die Uplinks aus der Standby-Liste.

Routen anhand des ursprünglichen virtuellen Ports

Der virtuelle Switch wählt Uplinks auf der Grundlage der Port-IDs der virtuellen Maschine auf dem vSphere Standard-Switch oder vSphere Distributed Switch aus.

Jede virtuelle Maschine, die auf einem ESXi-Host ausgeführt wird, verfügt über eine zugehörige virtuelle Port-ID auf dem virtuellen Switch. Zum Berechnen eines Uplinks für eine virtuelle Maschine verwendet der virtuelle Switch die Port-ID der virtuellen Maschine und die Anzahl der Uplinks in der Netzwerkkartengruppe. Nachdem der virtuelle Switch einen Uplink für eine virtuelle Maschine ausgewählt hat, leitet er den Datenverkehr immer durch denselben Uplink für diese virtuelle Maschine weiter, solange das System auf demselben Port ausgeführt wird. Der virtuelle Switch berechnet Uplinks für virtuelle Maschinen nur einmal, es sei denn, es werden Uplinks der Netzwerkkartengruppe hinzugefügt oder aus dieser entfernt.

Die Port-ID einer virtuellen Maschine ist unveränderlich, während die virtuelle Maschine auf demselben Host ausgeführt wird. Wenn Sie die virtuelle Maschine migrieren, ausschalten oder löschen, wird die Port-ID auf dem virtuellen Switch wieder verfügbar. Der virtuelle Switch sendet keine Daten mehr zu diesem Anschluss, was den Datenverkehr für den zugehörigen Uplink insgesamt reduziert. Wenn eine virtuelle Maschine eingeschaltet oder migriert wird, wird sie möglicherweise auf einem anderen Port angezeigt und verwendet eventuell den Uplink, der mit dem neuen Port verknüpft ist.

Tabelle 8-3. Überlegungen zur Verwendung der Route auf der Basis des ursprünglichen virtuellen Ports

Überlegungen	Beschreibung
Vorteile	<ul style="list-style-type: none"> ■ Eine gleichmäßige Verteilung des Datenverkehrs, wenn die Anzahl virtueller Netzwerkkarten größer als die Anzahl physischer Netzwerkkarten in der Gruppe ist. ■ Niedriger Ressourcenverbrauch, weil in den meisten Fällen der virtuelle Switch Uplinks für virtuelle Maschinen nur einmal berechnet. ■ Beim physischen Switch sind keine Änderungen erforderlich.
Nachteile	<ul style="list-style-type: none"> ■ Der virtuelle Switch kennt nicht die Datenverkehrslast auf den Uplinks und gleicht nicht die Datenverkehrslast zu Uplinks aus, die weniger beansprucht werden. ■ Die für eine virtuelle Maschine verfügbare Bandbreite ist auf die Geschwindigkeit des Uplinks beschränkt, der mit der relevanten Port-ID verknüpft ist, es sei denn, die virtuelle Maschine ist mit mehreren virtuellen Netzwerkkarten ausgestattet.

Routen anhand des Quell-MAC-Hash

Der virtuelle Switch wählt einen Uplink für eine virtuelle Maschine auf der Grundlage der MAC-Adresse der virtuellen Maschine aus. Zum Berechnen eines Uplinks für eine virtuelle Maschine verwendet der virtuelle Switch die MAC-Adresse der virtuellen Maschine und die Anzahl der Uplinks in der Netzwerkkartengruppe.

Tabelle 8-4. Überlegungen zur Verwendung von „Anhand des Quell-MAC-Hashs routen“

Überlegungen	Beschreibung
Vorteile	<ul style="list-style-type: none"> ■ Eine gleichmäßigere Verteilung des Datenverkehrs als beim Routen anhand des ursprünglichen virtuellen Ports, weil der virtuelle Switch einen Uplink für jedes Paket berechnet. ■ Virtuelle Maschinen verwenden denselben Uplink, weil die MAC-Adresse statisch ist. Beim Ein- bzw. Ausschalten einer virtuellen Maschine wird der Uplink, den die virtuelle Maschine verwendet, nicht geändert. ■ Beim physischen Switch sind keine Änderungen erforderlich.
Nachteile	<ul style="list-style-type: none"> ■ Die für eine virtuelle Maschine verfügbare Bandbreite ist auf die Geschwindigkeit des Uplinks beschränkt, der mit der relevanten Port-ID verknüpft ist, es sei denn, die virtuelle Maschine verwendet mehrere Quell-MAC-Adressen. ■ Ein höherer Ressourcenverbrauch als beim Routen anhand des ursprünglichen virtuellen Ports, weil der virtuelle Switch einen Uplink für jedes Paket berechnet. ■ Der virtuelle Switch kennt nicht die Last auf den Uplinks, diese können deshalb überlastet werden.

Routen anhand des IP-Hash

Der virtuelle Switch wählt Uplinks für virtuelle Maschinen anhand der Quell- und Ziel-IP-Adresse jedes Pakets aus.

Um den Uplink für eine virtuelle Maschine zu berechnen, unterzieht der virtuelle Switch das letzte Oktett der Quell- und der Ziel-Adresse im Paket einer XOR-Operation und nimmt am Ergebnis eine weitere Berechnung anhand der Anzahl von Uplinks in der NIC-Gruppe vor. Das Ergebnis ist eine Zahl zwischen 0 und der Anzahl von Uplinks in der Gruppe minus 1. Beispiel: Bei einer NIC-Gruppe mit vier Uplinks ist das Ergebnis eine Zahl zwischen 0 und 3, da jede Zahl einer Netzwerkkarte in der NIC-Gruppe zugeordnet ist. Bei Nicht-IP-Paketen nimmt der virtuelle Switch zwei 32-Bit-Binärwerte aus dem Frame oder Paket, in dem die IP-Adresse angesiedelt sein würde.

Jede virtuelle Maschine kann jeden Uplink in der NIC-Gruppe verwenden, je nach Quell- und Ziel-IP-Adresse. Auf diese Weise kann jede virtuelle Maschine die Bandbreite jedes Uplinks in der Gruppe nutzen. Bei virtuellen Maschinen in einer Umgebung mit vielen unabhängigen virtuellen Maschinen kann der IP-Hash-Algorithmus eine gleichmäßige Verteilung des Datenverkehrs zwischen den Netzwerkkarten in der Gruppe bewirken. Wenn eine virtuelle Maschine mit mehreren Ziel-IP-Adressen kommuniziert, kann der virtuelle Switch für jede Ziel-IP-Adresse einen anderen Hashwert generieren. So können die Pakete verschiedene Uplinks auf dem virtuellen Switch nutzen und einen potenziell höheren Durchsatz erzielen.

In Umgebungen mit wenigen IP-Adressen ist es jedoch möglich, dass der virtuelle Switch den Datenverkehr immer über denselben Uplink in einer Gruppe leitet. Wenn auf Ihren Datenbankserver beispielsweise von einem einzigen Anwendungsserver zugegriffen wird, berechnet der virtuelle Switch immer denselben Uplink, da nur ein Quell-Ziel-Paar existiert.

Konfiguration von physischen Switches

Damit der IP-Hash-Lastausgleich korrekt funktionieren kann, müssen Sie auf dem physischen Switch einen Etherchannel konfiguriert haben. Mit dem Etherchannel werden mehrere Netzwerkadapter zu einer einzigen logischen Verknüpfung gebündelt. Wenn Ports zu einem Etherchannel gebündelt sind, wird jedes Mal, wenn auf dem physischen Switch über unterschiedliche Ports ein Paket von derselben MAC-Adresse eingeht, die Tabelle des Content Addressable Memory (CAM) auf dem Switch korrekt aktualisiert.

Angenommen, der physische Switch empfängt Pakete von der MAC-Adresse A auf den Ports 01 und 02. Der Switch trägt nun 01-A und 02-A in seine CAM-Tabelle ein. Der Switch kann also den eingehenden Datenverkehr auf die korrekten Ports verteilen. Ohne Etherchannel vermerkt der Port zunächst, dass ein Paket von MAC-Adresse A auf Port 01 eingegangen ist. Wenn anschließend ein Paket von MAC-Adresse A über Port 02 eingeht, wird einfach derselbe Eintrag aktualisiert. Das bewirkt, dass der physische Switch den eingehenden Datenverkehr nur an Port 02 weiterleitet und Pakete ihr Ziel eventuell nicht erreichen oder den entsprechenden Uplink überladen.

Einschränkungen und Konfigurationsanforderungen

- ESXi-Hosts unterstützen die IP-Hash-Gruppierung auf einem einzelnen physischen Switch oder auf gestapelten Switches.
- ESXi-Hosts unterstützen nur die 802.3ad-Linkzusammenfassung im statischen Modus. Bei vSphere Standard Switches kann nur ein statischer Etherchannel verwendet werden. LACP wird nicht unterstützt. Um LACP verwenden zu können, müssen Sie mit vSphere Distributed Switch 5.1 und höher oder Cisco Nexus 1000V arbeiten. Wenn Sie den IP-Hash-Lastausgleich ohne 802.3ad-Linkzusammenfassung oder umgekehrt aktivieren, kann es zu Störungen im Netzwerk kommen.
- Beim IP-Hash-Lastausgleich darf ausschließlich die Netzwerkausfallerkennung „Nur Verbindungsstatus“ verwendet werden.
- Alle Uplinks aus der Gruppe müssen in der Failover-Liste der aktiven Uplinks enthalten sein. Die Listen der Standby-Uplinks und ungenutzten Uplinks müssen leer sein.
- Die Anzahl der Ports im Etherchannel muss gleich sein wie die Anzahl der Uplinks in der Gruppe.

Überlegungen zum Routen anhand des IP-Hash

Überlegungen	Beschreibung
Vorteile	<ul style="list-style-type: none"> ■ Gleichmäßigere Verteilung der Last im Vergleich zum Routen anhand des ursprünglichen virtuellen Ports und dem Routen anhand des Quell-MAC-Hash, da der virtuelle Switch den Uplink für jedes Paket berechnet ■ Potenziell höherer Durchsatz bei virtuellen Maschinen, die mit mehreren IP-Adressen kommunizieren
Nachteile	<ul style="list-style-type: none"> ■ Höchste Ressourcennutzung gegenüber allen anderen Lastausgleichsalgorithmen ■ Der virtuelle Switch kennt die tatsächliche Last auf den Uplinks nicht. ■ Erfordert Änderungen am physischen Netzwerk. ■ Komplexe Fehlerbehebung

Routen anhand der physischen Netzwerkkartenauslastung

„Anhand der physischen Netzwerkkartenauslastung routen“ basiert auf „Anhand des ursprünglichen virtuellen Ports routen“, wobei der virtuelle Switch die effektive Auslastung der Uplinks prüft und die entsprechenden Schritte zum Verringern der Last auf überlasteten Uplinks ausführt. Ist nur für vSphere Distributed Switch verfügbar.

Der Distributed Switch berechnet Uplinks für virtuelle Maschinen mithilfe ihrer Port-ID und der Anzahl der Uplinks in der Netzwerkkartengruppe. Der Distributed Switch testet die Uplinks alle 30 Sekunden, und wenn ihre Auslastung 75 Prozent der Nutzung übersteigt, wird die Port-ID der virtuellen Maschine mit der höchsten E/A zu einem anderen Uplink verschoben.

Tabelle 8-5. Überlegungen zur Verwendung von „Anhand der physischen Netzwerkkartenauslastung routen“

Überlegungen	Beschreibung
Vorteile	<ul style="list-style-type: none"> ■ Niedriger Ressourcenverbrauch, weil der Distributed Switch Uplinks für virtuelle Maschinen nur einmal berechnet und das Prüfen der Uplinks nur minimale Auswirkungen hat. ■ Der Distributed Switch kennt die Auslastung von Uplinks und verringert sie, falls notwendig. ■ Beim physischen Switch sind keine Änderungen erforderlich.
Nachteile	<ul style="list-style-type: none"> ■ Die Bandbreite, die für virtuelle Maschinen verfügbar ist, ist auf die Uplinks beschränkt, die mit dem Distributed Switch verbunden sind.

Ausdrückliche Failover-Reihenfolge verwenden

Bei dieser Richtlinie ist kein effektiver Lastausgleich verfügbar. Der virtuelle Switch verwendet immer den Uplink, der an erster Stelle der Liste der aktiven Adapter in der Failover-Reihenfolge

steht und die Failover-Ermittlungskriterien erfüllt. Wenn keine Uplinks in der Liste „Aktiv“ verfügbar sind, verwendet der virtuelle Switch die Uplinks aus der Standby-Liste.

Konfigurieren von NIC-Gruppierung, Failover und Lastausgleich auf einem vSphere Standard-Switch oder in einer Standardportgruppe

Fügen Sie zwei oder mehr physische Netzwerkkarten einer Gruppe hinzu, um die Netzwerkkapazität eines vSphere Standard-Switches oder einer Standard-Portgruppe zu erhöhen. Konfigurieren Sie die Failover-Reihenfolge, um festzulegen, wie der Netzwerkdatenverkehr beim Ausfall eines Adapters umgeleitet wird. Wählen Sie einen Lastausgleichsalgorithmus aus, um zu ermitteln, wie der Standard-Switch den Datenverkehr zwischen den physischen Netzwerkkarten in einer Gruppe verteilt.

Konfigurieren Sie NIC-Gruppierung, Failover und Lastausgleich je nach der Netzwerkkonfiguration auf dem physischen Switch und der Topologie des Standard-Switches. Weitere Informationen hierzu finden Sie unter [Teaming- und Failover-Richtlinie](#) und [Verfügbare Lastausgleichsalgorithmen für virtuelle Switches](#).

Wenn Sie die Teaming- und Failover-Richtlinie auf einem Standard-Switch konfigurieren, wird die Richtlinie auf alle Portgruppen im Switch übertragen. Wenn Sie die Richtlinie auf einer Standard-Portgruppe konfigurieren, überschreibt sie die vom Switch übernommene Richtlinie.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Navigieren Sie zu der Teaming- und Failover-Richtlinie für den Standard-Switch oder zur Standard-Portgruppe.

Option	Aktion
Standard-Switch	<ol style="list-style-type: none"> Wählen Sie den Switch aus der Liste aus. Klicken Sie auf Einstellungen bearbeiten und wählen Sie Teaming und Failover aus.
Standard-Portgruppe	<ol style="list-style-type: none"> Wählen Sie den Switch aus, bei dem sich die Portgruppe befindet. Wählen Sie im Switch-Topologiediagramm die Standardportgruppe aus und klicken Sie auf Einstellungen bearbeiten. Wählen Sie Teaming und Failover aus. Wählen Sie Außer Kraft setzen neben den Richtlinien aus, die Sie überschreiben möchten.

- 4 Legen Sie über das Dropdown-Menü **Lastausgleich** fest, wie der virtuelle Switch die Last des ausgehenden Datenverkehrs zwischen den physischen Netzwerkkarten in einer Gruppe ausgleicht.

Option	Beschreibung
Anhand des ursprünglichen virtuellen Ports routen	Wählen Sie einen Uplink basierend auf den virtuellen Port-IDs auf dem Switch aus. Nachdem der virtuelle Switch einen Uplink für eine virtuelle Maschine oder einen VMkernel-Adapter ausgewählt hat, leitet er den Datenverkehr immer durch denselben Uplink für diese virtuelle Maschine bzw. den VMkernel-Adapter weiter.
Anhand des IP-Hashs routen	Wählen Sie einen Uplink anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets aus. Bei Paketen ohne IP verwendet der Switch die Daten in diesen Feldern zur Berechnung des Hashs. Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit „EtherChannel“ konfiguriert ist.
Anhand des Quell-MAC-Hashs routen	Wählen Sie einen Uplink anhand eines Hashs des Quell-Ethernets aus.
Anhand der physischen Netzwerkkartenauslastung routen	Verfügbar für verteilte Portgruppen oder verteilte Ports. Wählen Sie auf der Basis der aktuellen Last der an die Portgruppe oder den Port angeschlossenen physischen Netzwerkkarten einen Uplink aus. Wenn ein Uplink 30 Sekunden zu mindestens 75 % ausgelastet ist, verschiebt der Host-Proxy-Switch einen Teil des Datenverkehrs der virtuellen Maschine zu einem physischen Adapter mit freier Kapazität.
Ausdrückliche Failover-Reihenfolge verwenden	Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Ermittlungskriterien erfüllt. Bei dieser Option wird kein effektiver Lastausgleich durchgeführt.

- 5 Wählen Sie über das Dropdown-Menü **Netzwerk-Failover-Ermittlung** die Methode aus, die der virtuelle Switch für die Failover-Ermittlung verwendet.

Option	Beschreibung
Nur Verbindungsstatus	Als Grundlage dient ausschließlich der vom Netzwerkkarten angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt.
Signalprüfung	Sendet Signale, wartet auf Signalprüfpakete auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. ESXi sendet jede Sekunde Signale. Die Netzwerkkarten müssen eine Aktiv/Aktiv- oder Aktiv/Standby-Konfiguration aufweisen, da Netzwerkkarten mit dem Status „Nicht verwendet“ nicht an der Signalprüfung beteiligt sind.

- 6 Wählen Sie aus dem Dropdown-Menü **Switches benachrichtigen** aus, ob der physische Switch im Falle eines Failovers vom Standard-Switch oder Distributed Switch benachrichtigt wird.

Hinweis Legen Sie diese Option auf **Nein** fest, wenn eine verbundene virtuelle Maschine den Netzwerklastausgleich (NLB) von Microsoft im Unicast-Modus verwendet. Im Multicast-Modus von NLB treten keine Probleme auf.

- 7 Wählen Sie über das Dropdown-Menü **Failback** aus, ob ein physischer Adapter nach einem Ausfall wieder in den Status „Aktiv“ geschaltet wird.

Wenn die Option auf **Ja** (die Standardauswahl) gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert. Er ersetzt in diesem Fall den ggf. vorhandenen Ersatzadapter, der seinen Platz eingenommen hatte.

Wenn das Failback für einen Standard-Port auf **Nein** gesetzt wurde, bleibt ein ausgefallener Adapter nach der Wiederherstellung inaktiv, bis der gegenwärtig aktive Adapter ausfällt und ersetzt werden muss.

- 8 Legen Sie fest, wie die Uplinks in einem Team im Falle eines Failovers verwendet werden, indem Sie die Liste für die Failover-Reihenfolge konfigurieren.

Wenn Sie bestimmte Uplinks verwenden und andere für Notfälle, z. B. bei einem Ausfall der verwendeten Uplinks, reservieren möchten, verschieben Sie Uplinks mithilfe der Pfeiltasten in unterschiedliche Gruppen.

Option	Beschreibung
Aktive Adapter	Dieser Uplink wird weiter verwendet, wenn die Verbindung zum Netzwerkadapter hergestellt und aktiv ist.
Standby-Adapter	Dieser Uplink wird verwendet, wenn einer der aktiven physischen Adapter nicht verfügbar ist.
Nicht verwendete Adapter	Verwenden Sie diesen Uplink nicht.

- 9 Klicken Sie auf **OK**.

Konfigurieren von NIC-Teaming, Failover und Lastausgleich in einer verteilten Portgruppe oder einem verteilten Port

Mit zwei oder mehreren physischen Netzwerkkarten in einer Teaming-Gruppe steigern Sie die Netzwerkkapazität einer verteilten Portgruppe oder eines einzelnen Ports. Konfigurieren Sie die Failover-Reihenfolge, um festzulegen, wie der Netzwerkdatenverkehr beim Ausfall eines Adapters umgeleitet wird. Wählen Sie einen Lastausgleichsalgorithmus und bestimmen Sie, wie der verteilte Switch die Datenverkehrslast zwischen den physischen Netzwerkkarten in einer Teaming-Gruppe ausgleicht.

Berücksichtigen Sie bei der Konfiguration von NIC-Teaming, Failover und Lastausgleich die Netzwerkkonfiguration des physischen Switch und die Topologie des verteilten Switch. Weitere Informationen finden Sie unter [Teaming- und Failover-Richtlinie](#) und [Verfügbare Lastausgleichsalgorithmen für virtuelle Switches](#).

Die Teaming- und Failover-Richtlinie, die Sie für eine verteilte Portgruppe konfigurieren, wird an alle Ports in der Portgruppe weitergegeben. Wenn Sie die Richtlinie für einen einzelnen verteilten Port festlegen, überschreibt diese die von der Portgruppe übernommene Richtlinie.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Gehen Sie zur Teaming- und Failover-Richtlinie in der verteilten Portgruppe oder im Port.

Option	Aktion
Verteilte Portgruppe	<ol style="list-style-type: none"> Wählen Sie im Menü Aktionen die Option Verteilte Portgruppe > Verteilte Portgruppen verwalten. Wählen Sie Teaming und Failover. Wählen Sie die Portgruppe aus und klicken Sie auf Weiter.
Verteilter Port	<ol style="list-style-type: none"> Wählen Sie Verwandte Objekte und anschließend Verteilte Portgruppen. Wählen Sie eine verteilte Portgruppe aus. Wählen Sie unter Verwalten die Option Ports. Wählen Sie einen Port aus und klicken Sie auf Einstellungen des verteilten Ports bearbeiten. Wählen Sie Teaming und Failover. Wählen Sie neben den Eigenschaften, die überschrieben werden sollen, die Option Außer Kraft setzen.

- 3 Legen Sie über das Dropdown-Menü **Lastausgleich** fest, wie der virtuelle Switch die Last des ausgehenden Datenverkehrs zwischen den physischen Netzwerkkarten in einer Gruppe ausgleicht.

Option	Beschreibung
Anhand des ursprünglichen virtuellen Ports routen	Wählen Sie einen Uplink basierend auf den virtuellen Port-IDs auf dem Switch aus. Nachdem der virtuelle Switch einen Uplink für eine virtuelle Maschine oder einen VMkernel-Adapter ausgewählt hat, leitet er den Datenverkehr immer durch denselben Uplink für diese virtuelle Maschine bzw. den VMkernel-Adapter weiter.
Anhand des IP-Hashs routen	Wählen Sie einen Uplink anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets aus. Bei Paketen ohne IP verwendet der Switch die Daten in diesen Feldern zur Berechnung des Hashs. Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit „EtherChannel“ konfiguriert ist.
Anhand des Quell-MAC-Hashs routen	Wählen Sie einen Uplink anhand eines Hashs des Quell-Ethernets aus.

Option	Beschreibung
Anhand der physischen Netzwerkkartenauslastung routen	Verfügbar für verteilte Portgruppen oder verteilte Ports. Wählen Sie auf der Basis der aktuellen Last der an die Portgruppe oder den Port angeschlossenen physischen Netzwerkadapter einen Uplink aus. Wenn ein Uplink 30 Sekunden zu mindestens 75 % ausgelastet ist, verschiebt der Host-Proxy-Switch einen Teil des Datenverkehrs der virtuellen Maschine zu einem physischen Adapter mit freier Kapazität.
Ausdrückliche Failover-Reihenfolge verwenden	Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Ermittlungskriterien erfüllt. Bei dieser Option wird kein effektiver Lastausgleich durchgeführt.

- 4 Wählen Sie über das Dropdown-Menü **Netzwerk-Failover-Ermittlung** die Methode aus, die der virtuelle Switch für die Failover-Ermittlung verwendet.

Option	Beschreibung
Nur Verbindungsstatus	Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt.
Signalprüfung	Sendet Signale, wartet auf Signalprüfpakete auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. ESXi sendet jede Sekunde Signalepakete. Die Netzwerkkarten müssen eine Aktiv/Aktiv- oder Aktiv/Standby-Konfiguration aufweisen, da Netzwerkkarten mit dem Status „Nicht verwendet“ nicht an der Signalprüfung beteiligt sind.

- 5 Wählen Sie aus dem Dropdown-Menü **Switches benachrichtigen** aus, ob der physische Switch im Falle eines Failovers vom Standard-Switch oder Distributed Switch benachrichtigt wird.

Hinweis Legen Sie diese Option auf **Nein** fest, wenn eine verbundene virtuelle Maschine den Netzwerklastausgleich (NLB) von Microsoft im Unicast-Modus verwendet. Im Multicast-Modus von NLB treten keine Probleme auf.

- 6 Wählen Sie über das Dropdown-Menü **Failback** aus, ob ein physischer Adapter nach einem Ausfall wieder in den Status „Aktiv“ geschaltet wird.

Wenn die Option auf **Ja** (die Standardauswahl) gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert. Er ersetzt in diesem Fall den ggf. vorhandenen Ersatzadapter, der seinen Platz eingenommen hatte.

Wenn das Failback für einen verteilten Port auf **Nein** gesetzt wurde, bleibt ein ausgefallener Adapter nach der Wiederherstellung nur dann inaktiv, wenn die zugeordnete virtuelle Maschine ausgeführt wird. Wenn die Option **Failback** auf **Nein** festgelegt ist und eine virtuelle Maschine ausgeschaltet wird, geschieht Folgendes: Wenn alle aktiven physischen Adapter ausfallen wird und dann einer der Adapter wiederhergestellt wird, dann wird nach Einschalten der virtuellen Maschine die virtuelle Netzwerkkarte mit dem wiederhergestellten Adapter

und nicht mit einem Standby-Adapter verbunden. Wenn eine virtuelle Maschine aus- und wieder eingeschaltet wird, führt dies dazu, dass die virtuelle Netzwerkkarte wieder mit einem verteilten Port verbunden wird. Der Distributed Switch betrachtet den Port als neu hinzugefügt und weist ihm den standardmäßigen Uplink-Port zu, also den aktiven Uplink-Adapter.

- 7 Legen Sie fest, wie die Uplinks in einem Team im Falle eines Failovers verwendet werden, indem Sie die Liste für die Failover-Reihenfolge konfigurieren.

Wenn Sie bestimmte Uplinks verwenden und andere für Notfälle, z. B. bei einem Ausfall der verwendeten Uplinks, reservieren möchten, verschieben Sie Uplinks mithilfe der Pfeiltasten in unterschiedliche Gruppen.

Option	Beschreibung
Aktive Adapter	Dieser Uplink wird weiter verwendet, wenn die Verbindung zum Netzwerkadapter hergestellt und aktiv ist.
Standby-Adapter	Dieser Uplink wird verwendet, wenn einer der aktiven physischen Adapter nicht verfügbar ist.
Nicht verwendete Adapter	Verwenden Sie diesen Uplink nicht.

- 8 Prüfen Sie die Einstellungen und übernehmen Sie die Konfiguration.

VLAN-Richtlinie

Die VLAN-Richtlinien legen fest, wie VLANs in Ihrer Netzwerkkumgebung funktionieren.

Ein virtuelles lokales Netzwerk (VLAN) ist eine Gruppe von Hosts mit einer gemeinsamen Gruppe von Anforderungen, die so kommunizieren, als wären sie an dieselbe Broadcast-Domäne angeschlossen, unabhängig von ihrem physischen Standort. Ein VLAN hat dieselben Attribute wie ein physisches lokales Netzwerk (LAN), ermöglicht aber das Gruppieren der Endstationen, auch wenn sie nicht an demselben Netzwerk-Switch angeschlossen sind.

Die VLAN-Richtlinien können verteilte Portgruppen und Ports sowie Uplink-Portgruppen und Ports umfassen.

Konfigurieren von VLAN-Tagging in einer verteilten Portgruppe oder einem verteilten Port

Um VLAN-Tagging global auf alle verteilten Ports anzuwenden, müssen Sie die VLAN-Richtlinie für eine verteilte Portgruppe festlegen. Um den virtuellen Datenverkehr durch den Port mit physischen VLANs anders als in der übergeordneten verteilten Portgruppe zu integrieren, müssen Sie die VLAN-Richtlinie für einen verteilten Port anwenden.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Navigieren Sie zur VLAN-Richtlinie für die verteilte Portgruppe oder den verteilten Port.

Option	Aktion
Verteilte Portgruppe	<ol style="list-style-type: none"> Wählen Sie im Menü Aktionen die Option Verteilte Portgruppe > Verteilte Portgruppen verwalten. Wählen Sie VLAN. Wählen Sie die Portgruppe aus und klicken Sie auf Weiter.
Verteilter Port	<ol style="list-style-type: none"> Wählen Sie Verwandte Objekte und anschließend Verteilte Portgruppen. Wählen Sie eine verteilte Portgruppe aus. Wählen Sie unter Verwalten die Option Ports aus. Wählen Sie einen Port aus und klicken Sie auf Einstellungen des verteilten Ports bearbeiten. Wählen Sie VLAN. Wählen Sie neben den außer Kraft zu setzenden Eigenschaften Außer Kraft setzen aus.

- 3 Wählen Sie im Dropdown-Menü **Typ** den Typ des VLAN-Datenverkehrsfilters und der Markierung aus und klicken Sie auf **Weiter**.

Option	Beschreibung
Keine	Verwenden Sie VLAN nicht. Verwenden Sie diese Option im Falle von External Switch Tagging.
VLAN	Kennzeichnen Sie den Datenverkehr mit der ID aus dem Feld VLAN-ID . Geben Sie eine Zahl zwischen 1 und 4094 für Virtual Switch Tagging ein.
VLAN-Trunking	Übergeben Sie den VLAN-Datenverkehr mit einer ID innerhalb des VLAN-Trunk-Bereichs an das Gastbetriebssystem. Sie können mithilfe einer kommagetrennten Liste mehrere Bereiche und individuelle VLANs festlegen. Verwenden Sie diese Option für Virtual Guest Tagging.
Privates VLAN	Ordnen Sie den Datenverkehr einem privaten VLAN zu, das auf dem Distributed Switch erstellt wurde.

- 4 Prüfen Sie die Einstellungen und übernehmen Sie die Konfiguration.

Konfigurieren von VLAN-Tagging auf einer Uplink-Portgruppe oder einem Uplink-Port

Um die Verarbeitung des VLAN-Datenverkehrs allgemein für alle Mitglieds-Uplinks zu konfigurieren, müssen Sie die VLAN-Richtlinie an einem Uplink-Port festlegen. Damit der VLAN-Datenverkehr durch den Port anders als für die übergeordnete Uplink-Portgruppe abgewickelt wird, müssen Sie die die VLAN-Richtlinie für einen Uplink festlegen.

Verwenden Sie die VLAN-Richtlinie auf Uplink-Portebene, um zum Filtern des Datenverkehrs einen Trunk-Bereich von VLAN-IDs an die physischen Netzwerkadapter weiterzuleiten. Die physischen Netzwerkadapter werfen die Pakete von anderen VLANs, sofern die Adapter das Filtern nach VLAN unterstützen. Das Festlegen eines Trunk-Bereichs optimiert die Netzwerkleistung, da physische Netzwerkadapter den Datenverkehr anstelle der Uplink-Ports in der Gruppe filtern.

Wenn Sie über einen physischen Netzwerkadapter verfügen, der den VLAN-Filter nicht unterstützt, sind die VLANs möglicherweise immer noch nicht blockiert. Konfigurieren Sie in diesem Fall den VLAN-Filter auf einer verteilten Portgruppe oder einem verteilten Port.

Weitere Informationen zur Unterstützung von VLAN-Filtern finden Sie in der technischen Dokumentation der Adapteranbieter.

Voraussetzungen

Aktivieren Sie die Außerkraftsetzungen auf Portebene, um die VLAN-Richtlinie auf Portebene außer Kraft zu setzen. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Wechseln Sie im vSphere Web Client zu einem Distributed Switch.
- 2 Klicken Sie auf die Registerkarte **Uplink-Portgruppen**.
- 3 Navigieren Sie zur VLAN-Richtlinie für die Uplink-Portgruppe oder den Port.

Option	Aktion
Uplink-Portgruppe	<ol style="list-style-type: none"> a Klicken Sie mit der rechten Maustaste auf eine Uplink-Portgruppe in der Liste und wählen Sie Einstellungen bearbeiten aus. b Klicken Sie auf VLAN.
Uplink-Port	<ol style="list-style-type: none"> a Klicken Sie auf eine Uplink-Portgruppe. b Wählen Sie Verwalten und dann Ports aus. c Wählen Sie einen Port aus und klicken Sie auf Einstellungen bearbeiten. d Klicken Sie auf VLAN und wählen Sie Außer Kraft setzen.

- 4 Geben Sie einen Wert für den **VLAN-Trunk-Bereich** ein, der an die physischen Netzwerkadapter weitergeleitet werden soll.

Trennen Sie die Einträge beim Trunking mehrerer Bereiche und individueller VLANs durch Kommas.

- 5 Klicken Sie auf **OK**.

Sicherheitsrichtlinie

Die Netzwerksicherheitsrichtlinie bietet Schutz des Datenverkehrs vor der Imitation von MAC-Adressen und unerwünschten Portprüfungen.

Die Sicherheitsrichtlinie eines Standard-Switches oder eines Distributed Switch ist auf Schicht 2 (Sicherungsschicht) des Netzwerkprotokoll-Stacks implementiert. Die drei Elemente der Sicherheitsrichtlinie sind der Promiscuous-Modus, Änderungen der MAC-Adresse und gefälschte Übertragungen. Weitere Informationen zu möglichen Netzwerkbedrohungen finden Sie in der Dokumentation *vSphere-Sicherheit*.

Konfigurieren der Sicherheitsrichtlinie für einen vSphere Standard-Switch oder eine Standardportgruppe

Sie können die Sicherheitsrichtlinie zur Ablehnung von Änderungen der MAC-Adresse und des Promiscuous-Modus im Gastbetriebssystem einer virtuellen Maschine für einen vSphere Standard-Switch konfigurieren. Sie können die vom Standard-Switch geerbte Sicherheitsrichtlinie für einzelne Portgruppen außer Kraft setzen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Navigieren Sie zur Sicherheitsrichtlinie für den Standard-Switch oder die Portgruppe.

Option	Aktion
vSphere Standard-Switch	<ol style="list-style-type: none"> a Wählen Sie einen Standard-Switch aus der Liste aus. b Klicken Sie auf Einstellungen bearbeiten. c Wählen Sie Sicherheit aus.
Standard-Portgruppe	<ol style="list-style-type: none"> a Wählen Sie den Standard-Switch aus, bei dem sich die Portgruppe befindet. b Wählen Sie im Topologie-Diagramm eine Standard-Portgruppe aus. c Klicken Sie auf Einstellungen bearbeiten. d Wählen Sie Sicherheit und dann Außer Kraft setzen neben den außer Kraft zu setzenden Optionen aus.

- 4 Lehnen Sie die Promiscuous-Modus-Aktivierung oder die MAC-Adressänderungen im Gastbetriebssystem der an den Standard-Switch oder die Portgruppe angeschlossenen virtuellen Maschinen ab bzw. nehmen Sie diese an.

Option	Beschreibung
Promiscuous-Modus	<ul style="list-style-type: none"> ■ Ablehnen. Der VM-Netzwerkadapter empfängt nur Frames, die an die virtuelle Maschine adressiert sind. ■ Akzeptieren. Der virtuelle Switch leitet alle Frames an die virtuellen Maschinen in Übereinstimmung mit der aktiven VLAN-Richtlinie für den Port weiter, mit dem der VM-Netzwerkadapter verbunden ist. <p>Hinweis Der Promiscuous-Modus ist ein unsicherer Betriebsmodus. Firewalls, Portscanner und Erkennungssysteme für Eindringversuche müssen im Promiscuous-Modus ausgeführt werden.</p>
MAC-Adressänderungen	<ul style="list-style-type: none"> ■ Ablehnen. Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine auf einen Wert ändert, der von der MAC-Adresse des VM-Netzwerkadapters abweicht (festgelegt in der <code>.vmx</code>-Konfigurationsdatei), unterbindet der Switch alle eingehenden Frames zum Adapter. <p>Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine wieder zur MAC-Adresse des VM-Netzwerkadapters ändert, empfängt die virtuelle Maschine wieder Frames.</p> <ul style="list-style-type: none"> ■ Akzeptieren. Wenn das Gastbetriebssystem die effektive MAC-Adresse einer virtuellen Maschine auf einen Wert ändert, der von der MAC-Adresse des VM-Netzwerkadapters abweicht, lässt der Switch Frames zu der neuen Adresse passieren.
Gefälschte Übertragungen	<ul style="list-style-type: none"> ■ Ablehnen. Der Switch verwirft alle ausgehenden Frames von einem Adapter einer virtuellen Maschine mit einer Quell-MAC-Adresse, die von der Adresse in der <code>.vmx</code>-Konfigurationsdatei abweicht. ■ Akzeptieren. Der Switch führt keine Filterung durch und lässt alle ausgehenden Frames zu.

- 5 Klicken Sie auf **OK**.

Konfigurieren der Sicherheitsrichtlinie für eine verteilte Portgruppe oder einen verteilten Port

Richten Sie eine Sicherheitsrichtlinie für eine verteilte Portgruppe ein, um den Promiscuous-Modus und MAC-Adressänderungen vom Gastbetriebssystem der virtuellen Maschinen, die der Portgruppe zugeordnet sind, zuzulassen oder abzulehnen. Sie können die von den verteilten Portgruppen oder von einzelnen Ports geerbte Sicherheitsrichtlinie außer Kraft setzen.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Navigieren Sie zur Sicherheitsrichtlinie für die verteilte Portgruppe oder den Port.

Option	Aktion
Verteilte Portgruppe	<ol style="list-style-type: none"> a Wählen Sie im Menü Aktionen die Option Verteilte Portgruppe > Verteilte Portgruppen verwalten. b Wählen Sie Sicherheit aus. c Wählen Sie die Portgruppe aus und klicken Sie auf Weiter.
Verteilter Port	<ol style="list-style-type: none"> a Wählen Sie Verwandte Objekte und anschließend Verteilte Portgruppen. b Wählen Sie eine verteilte Portgruppe aus. c Wählen Sie unter Verwalten die Option Ports aus. d Wählen Sie einen Port aus und klicken Sie auf Einstellungen des verteilten Ports bearbeiten. e Wählen Sie Sicherheit aus. f Wählen Sie neben den außer Kraft zu setzenden Eigenschaften Außer Kraft setzen aus.

- 3 Lehnen Sie die Promiscuous-Modus-Aktivierung oder die MAC-Adressänderungen im Gastbetriebssystem der an die verteilte Portgruppe oder den Port angeschlossenen virtuellen Maschinen ab bzw. nehmen Sie diese an.

Option	Beschreibung
Promiscuous-Modus	<ul style="list-style-type: none"> ■ Ablehnen. Der VM-Netzwerkadapter empfängt nur Frames, die an die virtuelle Maschine adressiert sind. ■ Akzeptieren. Der virtuelle Switch leitet alle Frames an die virtuellen Maschinen in Übereinstimmung mit der aktiven VLAN-Richtlinie für den Port weiter, mit dem der VM-Netzwerkadapter verbunden ist. <p>Hinweis Der Promiscuous-Modus ist ein unsicherer Betriebsmodus. Firewalls, Portscanner und Erkennungssysteme für Eindringversuche müssen im Promiscuous-Modus ausgeführt werden.</p>
MAC-Adressänderungen	<ul style="list-style-type: none"> ■ Ablehnen. Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine auf einen Wert ändert, der von der MAC-Adresse des VM-Netzwerkadapters abweicht (festgelegt in der <code>.vmx</code>-Konfigurationsdatei), unterbindet der Switch alle eingehenden Frames zum Adapter. <p>Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine wieder zur MAC-Adresse des VM-Netzwerkadapters ändert, empfängt die virtuelle Maschine wieder Frames.</p> <ul style="list-style-type: none"> ■ Akzeptieren. Wenn das Gastbetriebssystem die effektive MAC-Adresse einer virtuellen Maschine auf einen Wert ändert, der von der MAC-Adresse des VM-Netzwerkadapters abweicht, lässt der Switch Frames zu der neuen Adresse passieren.
Gefälschte Übertragungen	<ul style="list-style-type: none"> ■ Ablehnen. Der Switch verwirft alle ausgehenden Frames von einem Adapter einer virtuellen Maschine mit einer Quell-MAC-Adresse, die von der Adresse in der <code>.vmx</code>-Konfigurationsdatei abweicht. ■ Akzeptieren. Der Switch führt keine Filterung durch und lässt alle ausgehenden Frames zu.

- 4 Prüfen Sie die Einstellungen und übernehmen Sie die Konfiguration.

Traffic-Shaping-Richtlinie

Eine Traffic-Shaping-Richtlinie wird anhand der durchschnittlichen Bandbreite, der Spitzenbandbreite und der Burstgröße definiert. Sie können für jede Portgruppe sowie jede verteilte Portgruppe und jeden verteilten Port eine Traffic-Shaping-Richtlinie erstellen.

ESXi steuert den ausgehenden Netzwerkverkehr auf Standard-Switches sowie den ein- und ausgehenden Datenverkehr auf Distributed Switches. Das Traffic-Shaping beschränkt die verfügbare Netzwerkbandbreite für einen Port, kann aber auch so konfiguriert werden, dass Datenverkehr-Bursts mit höherer Geschwindigkeit zulässig sind.

Durchschnittsbandbreite

Legt fest, wie viele Bit pro Sekunde im Durchschnitt einen Port durchlaufen dürfen. Bei diesem Wert handelt es sich um die zulässige durchschnittliche Last.

Spitzenbandbreite

Die maximale Zahl der Bit pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet oder empfängt. Dieser Wert begrenzt die Bandbreite, die ein Port nutzt, wenn er seinen Burst-Bonus verwendet.

Burstgröße

Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte ihm zugeteilte Bandbreite nutzt. Wenn dieser Port mehr Bandbreite benötigt als von der durchschnittlichen Bandbreite angegeben, kann er vorübergehend die Erlaubnis erhalten, Daten mit einer höheren Geschwindigkeit zu übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt wurden, und überträgt den Datenverkehr mit einer höheren Geschwindigkeit.

Konfigurieren von Traffic-Shaping für einen vSphere Standard-Switch oder eine Standardportgruppe

ESXi ermöglicht Ihnen das Traffic-Shaping des ausgehenden Datenverkehrs auf Standard-Switches oder Portgruppen. Der Traffic-Shaper beschränkt die verfügbare Netzwerkbandbreite für jeden Port, kann aber auch so konfiguriert werden, dass er vorübergehende Datenverkehr-Bursts mit höherer Geschwindigkeit für einen Port zulässt.

Die Traffic-Shaping-Richtlinien, die Sie auf der Ebene eines Switch oder einer Portgruppe festlegen, werden auf die einzelnen Ports im Switch oder in der Portgruppe angewendet. Wenn Sie z. B. eine durchschnittliche Bandbreite von 100000 KBit/s für eine Standardportgruppe festlegen, können 100000 KBit/s im Zeitdurchschnitt durch jeden Port fließen, der mit der Standardportgruppe verbunden ist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.

3 Navigieren Sie zur Traffic-Shaping-Richtlinie am Standard-Switch oder an der Portgruppe.

Option	Aktion
vSphere Standard-Switch	a Wählen Sie einen Standard-Switch aus der Liste aus. b Klicken Sie auf Einstellungen bearbeiten . c Wählen Sie Traffic-Shaping aus.
Standard-Portgruppe	a Wählen Sie den Standard-Switch aus, bei dem sich die Portgruppe befindet. b Wählen Sie im Topologie-Diagramm eine Standard-Portgruppe aus. c Klicken Sie auf Einstellungen bearbeiten . d Wählen Sie Traffic-Shaping und dann Außer Kraft setzen neben den außer Kraft zu setzenden Optionen aus.

4 Konfigurieren Sie Traffic-Shaping-Richtlinien.

Option	Beschreibung
Status	Ermöglicht die Einstellung von Einschränkungen für die Netzwerkbandbreite, die jedem Port des Standard-Switch oder der Portgruppe zugeordnet ist.
Durchschnittliche Bandbreite	Legt die zulässige Menge der Bit pro Sekunde fest, die einen Port im Durchschnitt durchlaufen darf (die zulässige durchschnittliche Datenlast).
Spitzenbandbreite	Die maximale Anzahl an Bits pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet. Diese Einstellung begrenzt die Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet. Dieser Parameter kann niemals kleiner als die durchschnittliche Bandbreite sein.
Burstgröße	Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte ihm zugeteilte Bandbreite nutzt. Immer wenn dieser Port mehr Bandbreite benötigt als von der durchschnittlichen Bandbreite angegeben, kann er möglicherweise vorübergehend Daten mit einer höheren Geschwindigkeit übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt und mit einer höheren Geschwindigkeit übertragen werden können.

5 Geben Sie für jede Traffic-Shaping-Richtlinie (**Durchschnittliche Bandbreite**, **Spitzenbandbreite** und **Burstgröße**) einen Bandbreitenwert ein.

6 Klicken Sie auf **OK**.

Bearbeiten der Traffic-Shaping-Richtlinie für eine verteilte Portgruppe oder einen verteilten Port

Traffic-Shaping ist auf verteilten Portgruppen und verteilten Ports von vSphere sowohl für eingehenden als auch für ausgehenden Datenverkehr möglich. Der Traffic-Shaper beschränkt die Netzwerkbandbreite für jeden Port in der Gruppe, kann aber auch so konfiguriert werden, dass er vorübergehende Datenverkehr-Bursts mit höherer Geschwindigkeit für einen Port zulässt.

Die Traffic-Shaping-Richtlinien, die Sie auf der Ebene einer verteilten Portgruppe festlegen, werden auf die einzelnen Ports in der Portgruppe angewendet. Wenn Sie beispielsweise eine durchschnittliche Bandbreite von 100.000 KBit/s für eine verteilte Portgruppe festlegen, können 100.000 KBit/s im Zeitdurchschnitt durch jeden Port fließen, der mit der verteilten Portgruppe verbunden ist.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Navigieren Sie zur Traffic-Shaping-Richtlinie für die verteilte Portgruppe oder den Port.

Option	Aktion
Verteilte Portgruppe	<ol style="list-style-type: none"> Wählen Sie im Menü Aktionen die Option Verteilte Portgruppe > Verteilte Portgruppen verwalten. Wählen Sie Traffic-Shaping aus. Wählen Sie die Portgruppe aus und klicken Sie auf Weiter.
Verteilter Port	<ol style="list-style-type: none"> Wählen Sie Verwandte Objekte und anschließend Verteilte Portgruppen. Wählen Sie eine verteilte Portgruppe aus. Wählen Sie unter Verwalten die Option Ports aus. Wählen Sie einen Port aus und klicken Sie auf Einstellungen des verteilten Ports bearbeiten. Wählen Sie Traffic-Shaping aus. Wählen Sie neben den außer Kraft zu setzenden Eigenschaften Außer Kraft setzen aus.

- 3 Konfigurieren Sie Traffic-Shaping-Richtlinien.

Hinweis Der Datenverkehr wird als Ingress und Egress klassifiziert, je nachdem, welche Richtung er im Switch (nicht im Host) hat.

Option	Beschreibung
Status	Aktivieren Sie entweder Ingress-Traffic-Shaping oder Egress-Traffic-Shaping in den Dropdown-Menüs Status .
Durchschnittliche Bandbreite	Legt fest, wie viele Bit pro Sekunde im Durchschnitt einen Port durchlaufen dürfen (zulässige durchschnittliche Datenlast).

Option	Beschreibung
Spitzenbandbreite	Die maximale Zahl der Bit pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet/endet oder empfängt. Dieser Parameter begrenzt die Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet.
Burstgröße	Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte ihm zugeteilte Bandbreite nutzt. Immer wenn dieser Port mehr Bandbreite benötigt als von der durchschnittlichen Bandbreite angegeben, kann er möglicherweise vorübergehend Daten mit einer höheren Geschwindigkeit übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Bytes, die im Burst-Bonus angesammelt und mit einer höheren Geschwindigkeit übertragen werden können.

- 4 Prüfen Sie die Einstellungen und übernehmen Sie die Konfiguration.

Ressourcenzuteilungsrichtlinie

Mit der Ressourcenzuteilungsrichtlinie können Sie einen verteilten Port oder eine verteilte Portgruppe zu einem von einem Benutzer erstellten Netzwerkressourcenpool zuordnen. Mit dieser Richtlinie lässt sich die Bandbreite für den Port oder die Portgruppe besser steuern.

Weitere Informationen zum Erstellen und Konfigurieren von Netzwerkressourcenpools finden Sie unter [Kapitel 11 vSphere Network I/O Control](#).

Bearbeiten der Ressourcenzuteilungsrichtlinie für eine verteilte Portgruppe

Ordnen Sie eine verteilte Portgruppe einem Netzwerkressourcenpool zu, um mehr Kontrolle über die Bandbreite zu haben, die der verteilten Portgruppe zugeteilt wird.

Voraussetzungen

- Aktivieren Sie Network I/O Control auf dem Distributed Switch. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).
- Erstellen und konfigurieren Sie Netzwerkressourcenpools. Siehe [Erstellen eines Netzwerkressourcenpools](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie im Navigator mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Verteilte Portgruppen > Verteilte Portgruppen verwalten** aus.
- 3 Aktivieren Sie das Kontrollkästchen **Ressourcenzuteilung**, und klicken Sie auf **Weiter**.
- 4 Wählen Sie die verteilte Portgruppe aus, die konfiguriert werden soll, und klicken Sie auf **Weiter**.

- 5 Fügen Sie die verteilte Portgruppe dem Netzwerkressourcenpool hinzu bzw. entfernen Sie sie, und klicken Sie auf **Weiter**.
 - Wählen Sie zum Hinzufügen der verteilten Portgruppe im Dropdown-Menü **Netzwerkressourcenpool** einen benutzerdefinierten Ressourcenpool aus.
 - Wählen Sie zum Entfernen der verteilten Portgruppe im Dropdown-Menü **Netzwerkressourcenpool** die Option **Standard** aus.
- 6 Überprüfen Sie Ihre Einstellungen im Abschnitt **Bereit zum Abschließen** und klicken Sie auf **Beenden**.

Verwenden Sie die Schaltfläche **Zurück**, um Einstellungen zu ändern.

Bearbeiten der Ressourcenzuteilungsrichtlinie für verteilte Ports

Wenn Sie Network I/O Control Version 2 auf einem vSphere Distributed Switch verwenden, können Sie spezifisch einen verteilten Port einem benutzerdefinierten Ressourcenpool zuordnen, um Network I/O Control für die Kontrolle der Bandbreite zu verwenden, die der am Port angeschlossenen virtuellen Maschine bereitgestellt wird.

Voraussetzungen

- Überprüfen Sie, ob Network I/O Control Version 2 installiert ist.
- Aktivieren Sie Network I/O Control auf dem Distributed Switch. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).
- Erstellen und konfigurieren Sie Netzwerkressourcenpools in Network I/O Control, Version 2. Siehe [Erstellen eines Netzwerkressourcenpools in Network I/O Control, Version 2](#).
- Aktivieren Sie Außerkraftsetzungen auf Portebene für die Ressourcenzuteilungsrichtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 3 Wählen Sie in der Liste einen Port aus, und klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Wählen Sie **Eigenschaften**.
- 5 Aktivieren Sie unter „Netzwerkressourcenpool“ das Kontrollkästchen **Außer Kraft setzen**, und weisen Sie dem Port aus dem Dropdown-Menü einen Netzwerkressourcenpool zu.

Wenn Sie die Außerkraftsetzung auf Portebene für die Ressourcenzuteilungsrichtlinie nicht aktiviert haben, ist die Option deaktiviert.

- Um den verteilten Port einem Ressourcenpool zuzuordnen, wählen Sie einen benutzerdefinierten Ressourcenpool aus.

- Um die Zuordnung zwischen dem verteilten Port und einem Ressourcenpool zu entfernen, wählen Sie **Standard** aus.

6 Klicken Sie auf **OK**.

Überwachungsrichtlinie

Die Überwachungsrichtlinie aktiviert oder deaktiviert die NetFlow-Überwachung auf einem verteilten Port oder einer Portgruppe.

NetFlow-Einstellungen können auf der Ebene der vSphere Distributed Switches konfiguriert werden. Weitere Informationen hierzu finden Sie unter [Konfigurieren der NetFlow-Einstellungen eines vSphere Distributed Switch](#).

Aktivieren oder Deaktivieren der NetFlow-Überwachung auf einer verteilten Portgruppe oder einem verteilten Port

Sie können NetFlow zum Überwachen von IP-Paketen aktivieren, die durch die Ports einer verteilten Portgruppe oder durch einzelne verteilte Ports fließen.

Sie konfigurieren die NetFlow-Einstellungen auf dem vSphere Distributed Switch. Siehe [Konfigurieren der NetFlow-Einstellungen eines vSphere Distributed Switch](#).

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Navigieren Sie zur Überwachungsrichtlinie für die verteilte Portgruppe oder den verteilten Port.

Option	Aktion
Verteilte Portgruppe	<ol style="list-style-type: none"> Wählen Sie im Menü Aktionen die Option Verteilte Portgruppe > Verteilte Portgruppen verwalten. Wählen Sie Überwachen aus. Wählen Sie die Portgruppe aus und klicken Sie auf Weiter.
Verteilter Port	<ol style="list-style-type: none"> Wählen Sie Verwandte Objekte und anschließend Verteilte Portgruppen. Wählen Sie eine verteilte Portgruppe aus. Wählen Sie unter Verwalten die Option Ports aus. Wählen Sie einen Port aus und klicken Sie auf Einstellungen des verteilten Ports bearbeiten. Wählen Sie Überwachen aus. Wählen Sie neben dem Dropdown-Menü Außer Kraft setzen aus.

- 3 Aktivieren oder deaktivieren Sie NetFlow im Dropdown-Menü **NetFlow** und klicken Sie auf **Weiter**.
- 4 Überprüfen Sie die Einstellungen und wenden Sie die Konfiguration an.

Richtlinien für das Filtern und Markieren des Datenverkehrs

In vSphere Distributed Switch 5.5 und neueren Versionen können Sie das virtuelle Netzwerk durch Verwendung der Richtlinie zum Filtern und Markieren des Datenverkehrs vor unerwünschtem Datenverkehr und Angriffen auf die Sicherheit schützen oder einer bestimmten Art von Datenverkehr ein QoS-Tag zuordnen.

Die Richtlinie für das Filtern und Markieren des Datenverkehrs stellt einen sortierten Satz von Regeln für den Netzwerkdatenverkehr dar, die für Sicherheit und die Kennzeichnung mit QoS-Tags des Datenflusses über die Ports eines Distributed Switch gelten. Im Allgemeinen besteht eine Regel aus einem Bezeichner für Datenverkehr und einer Aktion zum Einschränken oder Priorisieren des entsprechenden Datenverkehrs.

Der vSphere Distributed Switch wendet Regeln an verschiedenen Stellen im Datenstrom auf den Datenverkehr an. Durch den Distributed Switch werden Filterregeln für den Datenverkehr auf den Datenpfad zwischen dem VM-Netzwerkadapter und dem verteilten Port oder zwischen dem Uplink-Port und physischen Netzwerkadapter für Uplink-Regeln angewendet.

Filtern und Markieren des Datenverkehrs in verteilten oder Uplink-Portgruppen

Legen Sie Datenverkehrsregeln auf der Ebene der verteilten Portgruppen oder Uplink-Portgruppen ein, um Filterung und Prioritätskennzeichnung für den Datenverkehrszugang über virtuelle Maschinen, VMkernel-Adapter oder physische Adapter einzuführen.

- [Aktivieren der Filterung und Markierung des Datenverkehrs in verteilten oder Uplink-Portgruppen](#)

Aktivieren Sie die Richtlinie zum Filtern und Markieren von Datenverkehr für eine Portgruppe, wenn Sie Datenverkehrssicherheit und -markierung auf allen Netzwerkadaptern von virtuellen Maschinen oder Uplink-Adaptern in der Gruppe konfigurieren möchten.

- [Markieren des Datenverkehrs in verteilten oder Uplink-Portgruppen](#)

Weisen Sie Prioritäts-Tags zum Datenverkehr wie VoIP und Streaming-Video zu, der höhere Netzwerkanforderungen an die Bandbreite, geringe Latenz usw. hat. Sie können den Datenverkehr mit einem CoS-Tag in Schicht 2 des Netzwerkprotokoll-Stacks oder mit einem DSCP-Tag in Schicht 3 markieren.

- [Filtern des Datenverkehrs in verteilten oder Uplink-Portgruppen](#)

Damit wird der Datenverkehr zum Sichern der Daten, die durch die Ports einer verteilten Portgruppe oder einer Uplink-Portgruppe fließen, zugelassen oder angehalten.

- [Arbeiten mit Netzwerkverkehrsregeln für eine verteilte Portgruppe oder eine Uplink-Portgruppe](#)

Definieren Sie Datenverkehrsregeln in einer verteilten Portgruppe oder einer Uplink-Portgruppe, um eine Richtlinie zur Verarbeitung von Datenverkehr von virtuellen Maschinen oder physischen Adaptern festzulegen. Sie können bestimmten Datenverkehr filtern oder seinen QoS-Bedarf beschreiben.

- [Deaktivieren der Filterung und Markierung des Datenverkehrs in verteilten oder Uplink-Portgruppen](#)

Dies ermöglicht den Datenverkehrsfluss an virtuelle Maschinen oder physische Adapter ohne zusätzliche Kontrolle bezüglich der Sicherheit oder QoS, indem die Richtlinie zum Filtern und Markieren von Datenverkehr deaktiviert wird.

Aktivieren der Filterung und Markierung des Datenverkehrs in verteilten oder Uplink-Portgruppen

Aktivieren Sie die Richtlinie zum Filtern und Markieren von Datenverkehr für eine Portgruppe, wenn Sie Datenverkehrssicherheit und -markierung auf allen Netzwerkadaptern von virtuellen Maschinen oder Uplink-Adaptern in der Gruppe konfigurieren möchten.

Hinweis Sie können die Richtlinie zum Filtern und Markieren von Datenverkehr deaktivieren, um die Verarbeitung des durch den Port fließenden Datenverkehrs zu vermeiden. Weitere Informationen hierzu finden Sie unter [Deaktivieren der Filterung und Markierung des Datenverkehrs in verteilten oder Uplink-Ports](#).

Verfahren

- 1 Suchen Sie im vSphere Web Client eine verteilte Portgruppe oder eine Uplink-Portgruppe.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**, um die Liste der verteilten Portgruppen anzuzeigen, oder klicken Sie auf **Uplink-Portgruppen**, um die Liste der Uplink-Portgruppen anzuzeigen.
- 2 Klicken Sie mit der rechten Maustaste auf die Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 4 Wählen Sie im Dropdown-Menü **Status** die Option **Aktiviert** aus.
- 5 Klicken Sie auf **OK**.

Nächste Schritte

Richten Sie die Markierung oder Filterung des Datenverkehrs für die durch den Port der verteilten Portgruppe bzw. der Uplink-Portgruppe fließenden Daten ein. Siehe [Markieren des Datenverkehrs in verteilten oder Uplink-Portgruppen](#) und [Filtern des Datenverkehrs in verteilten oder Uplink-Portgruppen](#).

Markieren des Datenverkehrs in verteilten oder Uplink-Portgruppen

Weisen Sie Prioritäts-Tags zum Datenverkehr wie VoIP und Streaming-Video zu, der höhere Netzwerkanforderungen an die Bandbreite, geringe Latenz usw. hat. Sie können den Datenverkehr mit einem CoS-Tag in Schicht 2 des Netzwerkprotokoll-Stacks oder mit einem DSCP-Tag in Schicht 3 markieren.

Prioritäts-Tagging ist ein Mechanismus, mit dem Datenverkehr gekennzeichnet wird, der höhere QoS-Anforderungen hat. So kann das Netzwerk verschiedene Klassen von Datenverkehr erkennen. Die Netzwerkgeräte können Datenverkehr jeder Klasse gemäß seiner Priorität und Anforderungen handhaben.

Sie können den Datenverkehr auch neu taggen, um die Wichtigkeit des Datenflusses zu erhöhen oder als weniger wichtig zu kennzeichnen. Durch Verwendung eines niedrigeren QoS-Tags können Sie Daten beschränken, die in einem Gast-Betriebssystem getaggt sind.

Verfahren

- 1 Suchen Sie im vSphere Web Client eine verteilte Portgruppe oder eine Uplink-Portgruppe.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**, um die Liste der verteilten Portgruppen anzuzeigen, oder klicken Sie auf **Uplink-Portgruppen**, um die Liste der Uplink-Portgruppen anzuzeigen.
- 2 Klicken Sie mit der rechten Maustaste auf die Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 4 Wenn das Filtern und Markieren von Datenverkehr deaktiviert ist, aktivieren Sie dies über das Dropdown-Menü **Status**.
- 5 Klicken Sie auf **Neu**, um eine neue Regel zu erstellen, oder wählen Sie eine Regel und klicken Sie auf **Bearbeiten**, um sie zu bearbeiten.
- 6 Wählen Sie im Dialogfeld zu Netzwerkverkehrsregeln die Option **Tag** aus dem **Aktion**-Dropdown-Menü.
- 7 Legen Sie den Prioritäts-Tag für den Datenverkehr im Geltungsbereich der Regel fest.

Option	Beschreibung
CoS-Wert	Markieren Sie den Datenverkehr, welcher der Regel entspricht, mit einem CoS-Prioritäts-Tag in der Netzwerkschicht 2. Wählen Sie CoS-Tag aktualisieren und geben Sie einen Wert zwischen 0 und 7 ein.
DSCP-Wert	Markieren Sie den mit der Regel verbundenen Datenverkehr mit einem DSCP-Tag in der Netzwerkschicht 3. Wählen Sie DSCP-Tag aktualisieren und geben Sie einen Wert zwischen 0 und 63 ein.

8 Spezifizieren Sie die Art von Datenverkehr, für den die Regel angewendet werden soll.

Um zu bestimmen, ob der Datenfluss im Geltungsbereich der Regel für die Markierung oder Filterung ist, untersucht der vSphere Distributed Switch die Richtung des Datenverkehrs und die Eigenschaften wie Quelle und Ziel, VLAN, Nächste-Schicht-Protokoll, Infrastrukturverkehrstyp und so weiter.

- a Wählen Sie aus dem Dropdown-Menü **Datenverkehrsrichtung**, ob der Datenverkehr eingehend oder ausgehend (Ingress oder Egress) oder beides sein muss, damit die Regel ihn als passend erkennt.

Die Datenverkehrsrichtung beeinflusst auch, wie Sie Datenverkehrsquelle und -Ziel identifizieren.

- b Legen Sie durch die Bezeichner für den Systemdatentyp, Schicht-2-Paketattribute und Schicht-3-Paketattribute die Eigenschaften fest, die Pakete haben müssen, um der Regel zu entsprechen.

Ein Bezeichner repräsentiert einen Satz passender Kriterien, verbunden mit der Netzwerkschicht. Sie können den Datenverkehr an den Systemdatentyp, Schicht-2-Datenverkehreigenschaften und Schicht-3-Datenverkehreigenschaften anpassen. Sie können den Bezeichner für eine bestimmte Netzwerkschicht verwenden oder Bezeichner kombinieren, um die Pakete genauer anzupassen.

- Verwenden Sie den Systemverkehrbezeichner, um Pakete an den Typ der virtuellen Infrastrukturdaten anzupassen, die durch die Ports der Gruppe fließen. Sie können beispielsweise NFS für Datentransfers an Netzwerkspeicher wählen.
- Verwenden Sie den MAC-Datenverkehrbezeichner, um Pakete nach MAC-Adresse, VLAN-ID und Nächste-Schicht-Protokoll anzupassen.

Das Auffinden von Datenverkehr über VLAN-ID in einer Distributed Port-Gruppe erfolgt über Virtual Guest Tagging (VGT). Um Datenverkehr an eine VLAN-ID, wenn Virtual Switch Tagging (VST) aktiviert ist, verwenden Sie eine Regel für eine Uplink-Portgruppe oder einen Uplink-Port.

- Verwenden Sie den IP-Datenverkehrbezeichner, um Pakete nach IP-Version, IP-Adresse und Nächste-Schicht-Protokoll anzupassen.

9 Klicken Sie im Dialogfeld auf **OK**, um die Regel zu speichern.

Beispiel: Markierung des Datenverkehrs über VoIP

Voice over IP (VoIP)-Flows müssen speziellen Anforderungen an QoS hinsichtlich geringen Verlusts und geringer Verzögerung genügen. Der Datenverkehr, der mit dem SIP (Session Initiation-Protokoll) für VoIP verbunden ist, hat in der Regel einen DSCP-Tag gleich 26, der für eine sichergestellte Weiterleitungsklasse 3 mit geringer Drop-Wahrscheinlichkeit (AF31) steht.

Sie können beispielsweise zum Markieren von ausgehenden SIP-UDP-Paketen an ein Subnetz 192.168.2.0/24 die folgende Regel verwenden:

Regelparameter	Parameterwert
Aktion	Tag
DSCP-Wert	26
Datenverkehrsrichtung	Egress
Datenverkehrsbezeichner	IP-Bezeichner
Protokoll	UDP
Zielport	5060
Quelladresse	IP-Adresse entspricht 192.168.2.0 mit der Präfixlänge 24

Filtern des Datenverkehrs in verteilten oder Uplink-Portgruppen

Damit wird der Datenverkehr zum Sichern der Daten, die durch die Ports einer verteilten Portgruppe oder einer Uplink-Portgruppe fließen, zugelassen oder angehalten.

Verfahren

- 1 Suchen Sie im vSphere Web Client eine verteilte Portgruppe oder eine Uplink-Portgruppe.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**, um die Liste der verteilten Portgruppen anzuzeigen, oder klicken Sie auf **Uplink-Portgruppen**, um die Liste der Uplink-Portgruppen anzuzeigen.
- 2 Klicken Sie mit der rechten Maustaste auf die Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 4 Wenn das Filtern und Markieren von Datenverkehr deaktiviert ist, aktivieren Sie dies über das Dropdown-Menü **Status**.
- 5 Klicken Sie auf **Neu**, um eine neue Regel zu erstellen, oder wählen Sie eine Regel und klicken Sie auf **Bearbeiten**, um sie zu bearbeiten.
- 6 Verwenden Sie im Dialogfeld „Netzwerkverkehrsregel“ eine Option unter „Aktion“, um den Datenverkehr durch die Ports der verteilten Portgruppe oder Uplink-Portgruppe fließen zu lassen bzw. ihn zu beschränken.

7 Spezifizieren Sie die Art von Datenverkehr, für den die Regel angewendet werden soll.

Um zu bestimmen, ob der Datenfluss im Geltungsbereich der Regel für die Markierung oder Filterung ist, untersucht der vSphere Distributed Switch die Richtung des Datenverkehrs und die Eigenschaften wie Quelle und Ziel, VLAN, Nächste-Schicht-Protokoll, Infrastrukturverkehrstyp und so weiter.

- a Wählen Sie aus dem Dropdown-Menü **Datenverkehrsrichtung**, ob der Datenverkehr eingehend oder ausgehend (Ingress oder Egress) oder beides sein muss, damit die Regel ihn als passend erkennt.

Die Datenverkehrsrichtung beeinflusst auch, wie Sie Datenverkehrsquelle und -Ziel identifizieren.

- b Legen Sie durch die Bezeichner für den Systemdatentyp, Schicht-2-Paketattribute und Schicht-3-Paketattribute die Eigenschaften fest, die Pakete haben müssen, um der Regel zu entsprechen.

Ein Bezeichner repräsentiert einen Satz passender Kriterien, verbunden mit der Netzwerkschicht. Sie können den Datenverkehr an den Systemdatentyp, Schicht-2-Datenverkehreigenschaften und Schicht-3-Datenverkehreigenschaften anpassen. Sie können den Bezeichner für eine bestimmte Netzwerkschicht verwenden oder Bezeichner kombinieren, um die Pakete genauer anzupassen.

- Verwenden Sie den Systemverkehrbezeichner, um Pakete an den Typ der virtuellen Infrastrukturdaten anzupassen, die durch die Ports der Gruppe fließen. Sie können beispielsweise NFS für Datentransfers an Netzwerkspeicher wählen.
- Verwenden Sie den MAC-Datenverkehrbezeichner, um Pakete nach MAC-Adresse, VLAN-ID und Nächste-Schicht-Protokoll anzupassen.

Das Auffinden von Datenverkehr über VLAN-ID in einer Distributed Port-Gruppe erfolgt über Virtual Guest Tagging (VGT). Um Datenverkehr an eine VLAN-ID, wenn Virtual Switch Tagging (VST) aktiviert ist, verwenden Sie eine Regel für eine Uplink-Portgruppe oder einen Uplink-Port.

- Verwenden Sie den IP-Datenverkehrbezeichner, um Pakete nach IP-Version, IP-Adresse und Nächste-Schicht-Protokoll anzupassen.

8 Klicken Sie im Dialogfeld auf **OK**, um die Regel zu speichern.

Arbeiten mit Netzwerkverkehrsregeln für eine verteilte Portgruppe oder eine Uplink-Portgruppe

Definieren Sie Datenverkehrsregeln in einer verteilten Portgruppe oder einer Uplink-Portgruppe, um eine Richtlinie zur Verarbeitung von Datenverkehr von virtuellen Maschinen oder physischen

Adaptern festzulegen. Sie können bestimmten Datenverkehr filtern oder seinen QoS-Bedarf beschreiben.

Hinweis Sie können die Regeln der Richtlinie zum Filtern und Markieren von Datenverkehr außer Kraft setzen, die auf Portebene festgelegt sind. Siehe [Arbeiten mit Netzwerkverkehrsregeln in verteilten oder Uplink-Ports](#).

- [Anzeigen der Verkehrsregeln in verteilten oder Uplink-Portgruppen](#)

Zeigen Sie die Verkehrsregeln an, die die Grundlage für die Richtlinie zum Filtern und Markieren von Datenverkehr einer verteilten Portgruppe oder Uplink-Portgruppe sind.

- [Bearbeiten einer Verkehrsregel in verteilten oder Uplink-Portgruppen](#)

Erstellen oder bearbeiten Sie Datenverkehrsregeln und verwenden Sie die Parameter, um eine Richtlinie zum Filtern und Markieren von Datenverkehr auf einer verteilten Portgruppe oder einer Uplink-Portgruppe zu konfigurieren.

- [Ändern der Regelprioritäten in verteilten oder Uplink-Portgruppen](#)

Ordnen Sie die Regeln, die die Richtlinie für das Filtern und Markieren des Datenverkehrs eines verteilten Ports oder Uplink-Ports darstellen, neu an, um die Handlungsabfolge für die Verarbeitung des Datenverkehrs zu ändern.

- [Löschen einer Verkehrsregel für eine verteilte Portgruppe oder eine Uplink-Portgruppe](#)

Löschen Sie eine Verkehrsregel für eine verteilte Portgruppe oder eine Uplink-Portgruppe, um die Verarbeitung von Paketen zu beenden, die in einer bestimmten Weise an virtuelle Maschinen oder physische Adapter übertragen werden.

Anzeigen der Verkehrsregeln in verteilten oder Uplink-Portgruppen

Zeigen Sie die Verkehrsregeln an, die die Grundlage für die Richtlinie zum Filtern und Markieren von Datenverkehr einer verteilten Portgruppe oder Uplink-Portgruppe sind.

Verfahren

- 1 Suchen Sie im vSphere Web Client eine verteilte Portgruppe oder eine Uplink-Portgruppe.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**, um die Liste der verteilten Portgruppen anzuzeigen, oder klicken Sie auf **Uplink-Portgruppen**, um die Liste der Uplink-Portgruppen anzuzeigen.
- 2 Klicken Sie mit der rechten Maustaste auf die Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 4 Wenn das Filtern und Markieren von Datenverkehr deaktiviert ist, aktivieren Sie dies über das Dropdown-Menü **Status**.

- 5 Untersuchen Sie **Aktion**, um zu sehen, ob die Regel Datenverkehr filtert (Zulassen oder Ablehnen) oder markiert (Tag) mit speziellen QoS-Anforderungen.
- 6 Wählen Sie aus der oberen Liste die Regel, für die Sie die Kriterien für die Auswahl von Datenverkehr anzeigen möchten.

Die bezeichnenden Parameter für den Datenverkehr der Regel werden in der Datenverkehrsbezeichner-Liste angezeigt.

Bearbeiten einer Verkehrsregel in verteilten oder Uplink-Portgruppen

Erstellen oder bearbeiten Sie Datenverkehrsregeln und verwenden Sie die Parameter, um eine Richtlinie zum Filtern und Markieren von Datenverkehr auf einer verteilten Portgruppe oder einer Uplink-Portgruppe zu konfigurieren.

Verfahren

- 1 Suchen Sie im vSphere Web Client eine verteilte Portgruppe oder eine Uplink-Portgruppe.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**, um die Liste der verteilten Portgruppen anzuzeigen, oder klicken Sie auf **Uplink-Portgruppen**, um die Liste der Uplink-Portgruppen anzuzeigen.
- 2 Klicken Sie mit der rechten Maustaste auf die Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 4 Wenn das Filtern und Markieren von Datenverkehr deaktiviert ist, aktivieren Sie dies über das Dropdown-Menü **Status**.
- 5 Klicken Sie auf **Neu**, um eine neue Regel zu erstellen, oder wählen Sie eine Regel und klicken Sie auf **Bearbeiten**, um sie zu bearbeiten.

Nächste Schritte

Benennen Sie die Netzwerkverkehrsregel und wählen Sie für den Zielverkehr „Verweigern“, „Zulassen“ oder „Tag“.

Ändern der Regelprioritäten in verteilten oder Uplink-Portgruppen

Ordnen Sie die Regeln, die die Richtlinie für das Filtern und Markieren des Datenverkehrs eines verteilten Ports oder Uplink-Ports darstellen, neu an, um die Handlungsabfolge für die Verarbeitung des Datenverkehrs zu ändern.

Der vSphere Distributed Switch wendet die Netzwerkverkehrsregeln in einer strengen Reihenfolge an. Wenn ein Paket einer Regel bereits entspricht, wird das Paket möglicherweise nicht der nächsten Regel in der Richtlinie übergeben.

Verfahren

- 1 Suchen Sie im vSphere Web Client eine verteilte Portgruppe oder eine Uplink-Portgruppe.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**, um die Liste der verteilten Portgruppen anzuzeigen, oder klicken Sie auf **Uplink-Portgruppen**, um die Liste der Uplink-Portgruppen anzuzeigen.
- 2 Klicken Sie mit der rechten Maustaste auf die Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 4 Wenn das Filtern und Markieren von Datenverkehr deaktiviert ist, aktivieren Sie dies über das Dropdown-Menü **Status**.
- 5 Wählen Sie eine Regel und verwenden Sie die Pfeiltasten, um ihre Priorität zu ändern.
- 6 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Löschen einer Verkehrsregel für eine verteilte Portgruppe oder eine Uplink-Portgruppe

Löschen Sie eine Verkehrsregel für eine verteilte Portgruppe oder eine Uplink-Portgruppe, um die Verarbeitung von Paketen zu beenden, die in einer bestimmten Weise an virtuelle Maschinen oder physische Adapter übertragen werden.

Verfahren

- 1 Suchen Sie im vSphere Web Client eine verteilte Portgruppe oder eine Uplink-Portgruppe.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**, um die Liste der verteilten Portgruppen anzuzeigen, oder klicken Sie auf **Uplink-Portgruppen**, um die Liste der Uplink-Portgruppen anzuzeigen.
- 2 Klicken Sie mit der rechten Maustaste auf die Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 4 Wenn das Filtern und Markieren von Datenverkehr deaktiviert ist, aktivieren Sie dies über das Dropdown-Menü **Status**.
- 5 Wählen Sie die entsprechende Regel aus und klicken Sie auf **Löschen**.
- 6 Klicken Sie auf **OK**.

Deaktivieren der Filterung und Markierung des Datenverkehrs in verteilten oder Uplink-Portgruppen

Dies ermöglicht den Datenverkehrsfluss an virtuelle Maschinen oder physische Adapter ohne zusätzliche Kontrolle bezüglich der Sicherheit oder QoS, indem die Richtlinie zum Filtern und Markieren von Datenverkehr deaktiviert wird.

Hinweis Sie können die Richtlinie zum Filtern und Markieren des Datenverkehrs an einem bestimmten Port aktivieren. Siehe [Aktivieren von Filtern und Markieren des Datenverkehrs an einem verteilten Port oder Uplink-Port](#).

Verfahren

- 1 Suchen Sie im vSphere Web Client eine verteilte Portgruppe oder eine Uplink-Portgruppe.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**, um die Liste der verteilten Portgruppen anzuzeigen, oder klicken Sie auf **Uplink-Portgruppen**, um die Liste der Uplink-Portgruppen anzuzeigen.
- 2 Klicken Sie mit der rechten Maustaste auf die Portgruppe und wählen Sie **Einstellungen bearbeiten** aus.
- 3 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 4 Wählen Sie im Dropdown-Menü **Status** die Option **Deaktiviert** aus.
- 5 Klicken Sie auf **OK**.

Filtern und Markieren des Datenverkehrs in verteilten oder Uplink-Ports

Filtern Sie den Datenverkehr oder beschreiben Sie dessen QoS-Anforderungen an einzelne virtuelle Maschinen, einen VMkernel-Adapter oder physischen Adapter, indem Sie die Richtlinien für das Filtern und Markieren des Datenverkehrs für einen verteilten Port oder Uplink-Port konfigurieren.

- [Aktivieren von Filtern und Markieren des Datenverkehrs an einem verteilten Port oder Uplink-Port](#)

Aktivieren Sie die Richtlinie für Filterung und Markierung des Datenverkehrs für einen Port, um die Sicherheit des Datenverkehrs zu konfigurieren und Netzwerkadapter, VMkernel-Adapter oder Uplink-Adapter auf einer virtuellen Maschine zu markieren.

■ Markieren des Datenverkehrs in verteilten oder Uplink-Ports

Weisen Sie Prioritäts-Tags in einer Regel für den Datenverkehr zu, der eine besondere Behandlung wie VoIP und Streaming-Video benötigt. Sie können den Datenverkehr für eine virtuelle Maschine, einen VMkernel-Adapter oder einen physischen Adapter mit einem CoS-Tag in Schicht 2 des Netzwerk-Protokoll-Stacks oder mit einem DSCP-Tag in Schicht 3 markieren.

■ Filtern des Datenverkehrs in einem verteilten Port oder einem Uplink-Port

Sie können mithilfe einer Regel Datenverkehr zulassen oder stoppen, um den Datenfluss über eine virtuelle Maschine, einen VMkernel-Adapter oder einen physischen Adapter zu sichern.

■ Arbeiten mit Netzwerkverkehrsregeln in verteilten oder Uplink-Ports

Definieren Sie Datenverkehrsregeln in einer verteilten oder Uplink-Portgruppe, um eine Richtlinie für die Bearbeitung des Datenverkehrs im Zusammenhang mit einer virtuellen Maschine oder einem physischen Adapter einzuführen. Sie können bestimmten Datenverkehr filtern oder seinen QoS-Bedarf beschreiben.

■ Deaktivieren der Filterung und Markierung des Datenverkehrs in verteilten oder Uplink-Ports

Deaktivieren Sie die Richtlinie für Filterung und Markierung des Datenverkehrs für einen Port, damit der Datenverkehr ohne Sicherheitsfilterung oder Markierung für QoS zu einer virtuellen Maschine oder einem physischen Adapter fließen kann.

Aktivieren von Filtern und Markieren des Datenverkehrs an einem verteilten Port oder Uplink-Port

Aktivieren Sie die Richtlinie für Filterung und Markierung des Datenverkehrs für einen Port, um die Sicherheit des Datenverkehrs zu konfigurieren und Netzwerkadapter, VMkernel-Adapter oder Uplink-Adapter auf einer virtuellen Maschine zu markieren.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie zu einem verteilten Port oder zu einem Uplink-Port.
 - Klicken Sie auf **Verwalten > Ports**, um zu den verteilten Ports des Switches zu navigieren.
 - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Verwandte Objekte > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 2 Wählen Sie einen Port aus der Liste aus.
- 3 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Wählen Sie **Filtern und Markieren des Datenverkehrs**.

- 5 Aktivieren Sie das Kontrollkästchen **Außer Kraft setzen** und wählen Sie im Dropdown-Menü **Status** die Option **Aktiviert** aus.
- 6 Klicken Sie auf **OK**.

Nächste Schritte

Konfigurieren Sie die Filterung oder Markierung des Datenverkehrs für die Daten, die über den verteilten Port oder den Uplink-Port geleitet werden. Siehe [Markieren des Datenverkehrs in verteilten oder Uplink-Ports](#) und [Filtern des Datenverkehrs in einem verteilten Port oder einem Uplink-Port](#).

Markieren des Datenverkehrs in verteilten oder Uplink-Ports

Weisen Sie Prioritäts-Tags in einer Regel für den Datenverkehr zu, der eine besondere Behandlung wie VoIP und Streaming-Video benötigt. Sie können den Datenverkehr für eine virtuelle Maschine, einen VMkernel-Adapter oder einen physischen Adapter mit einem CoS-Tag in Schicht 2 des Netzwerk-Protokoll-Stacks oder mit einem DSCP-Tag in Schicht 3 markieren.

Prioritäts-Tagging ist ein Mechanismus, mit dem Datenverkehr gekennzeichnet wird, der höhere QoS-Anforderungen hat. So kann das Netzwerk verschiedene Klassen von Datenverkehr erkennen. Die Netzwerkgeräte können Datenverkehr jeder Klasse gemäß seiner Priorität und Anforderungen handhaben.

Sie können den Datenverkehr auch neu taggen, um die Wichtigkeit des Datenflusses zu erhöhen oder als weniger wichtig zu kennzeichnen. Durch Verwendung eines niedrigeren QoS-Tags können Sie Daten beschränken, die in einem Gast-Betriebssystem getaggt sind.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie zu einem verteilten Port oder zu einem Uplink-Port.
 - Klicken Sie auf **Verwalten > Ports**, um zu den verteilten Ports des Switches zu navigieren.
 - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Verwandte Objekte > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 2 Wählen Sie einen Port aus der Liste aus.
- 3 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Wenn das Filtern und Markieren auf Portebene nicht aktiviert ist, klicken Sie auf **Überschreiben**, und wählen Sie im Dropdown-Menü **Status** die Option **Aktiviert**.

- 5 Klicken Sie auf **Neu**, um eine neue Regel zu erstellen, oder wählen Sie eine Regel und klicken Sie auf **Bearbeiten**, um sie zu bearbeiten.

Sie können eine aus der verteilte Portgruppe oder Uplink-Portgruppe geerbte Regel ändern. So ist die Regel im Geltungsbereich des Ports eindeutig.

- 6 Wählen Sie im Dialogfeld zu Netzwerkverkehrsregeln die Option **Tag** aus dem **Aktion**-Dropdown-Menü.
- 7 Legen Sie den Prioritäts-Tag für den Datenverkehr im Geltungsbereich der Regel fest.

Option	Beschreibung
CoS-Wert	Markieren Sie den Datenverkehr, welcher der Regel entspricht, mit einem CoS-Prioritäts-Tag in der Netzwerkschicht 2. Wählen Sie CoS-Tag aktualisieren und geben Sie einen Wert zwischen 0 und 7 ein.
DSCP-Wert	Markieren Sie den mit der Regel verbundenen Datenverkehr mit einem DSCP-Tag in der Netzwerkschicht 3. Wählen Sie DSCP-Tag aktualisieren und geben Sie einen Wert zwischen 0 und 63 ein.

8 Spezifizieren Sie die Art von Datenverkehr, für den die Regel angewendet werden soll.

Um zu bestimmen, ob der Datenfluss im Geltungsbereich der Regel für die Markierung oder Filterung ist, untersucht der vSphere Distributed Switch die Richtung des Datenverkehrs und die Eigenschaften wie Quelle und Ziel, VLAN, Nächste-Schicht-Protokoll, Infrastrukturverkehrstyp und so weiter.

- a Wählen Sie aus dem Dropdown-Menü **Datenverkehrsrichtung**, ob der Datenverkehr eingehend oder ausgehend (Ingress oder Egress) oder beides sein muss, damit die Regel ihn als passend erkennt.

Die Datenverkehrsrichtung beeinflusst auch, wie Sie Datenverkehrsquelle und -Ziel identifizieren.

- b Legen Sie durch die Bezeichner für den Systemdatentyp, Schicht-2-Paketattribute und Schicht-3-Paketattribute die Eigenschaften fest, die Pakete haben müssen, um der Regel zu entsprechen.

Ein Bezeichner repräsentiert einen Satz passender Kriterien, verbunden mit der Netzwerkschicht. Sie können den Datenverkehr an den Systemdatentyp, Schicht-2-Datenverkehreigenschaften und Schicht-3-Datenverkehreigenschaften anpassen. Sie können den Bezeichner für eine bestimmte Netzwerkschicht verwenden oder Bezeichner kombinieren, um die Pakete genauer anzupassen.

- Verwenden Sie den Systemverkehrbezeichner, um Pakete an den Typ der virtuellen Infrastrukturdaten anzupassen, die durch die Ports der Gruppe fließen. Sie können beispielsweise NFS für Datentransfers an Netzwerkspeicher wählen.
- Verwenden Sie den MAC-Datenverkehrbezeichner, um Pakete nach MAC-Adresse, VLAN-ID und Nächste-Schicht-Protokoll anzupassen.

Das Auffinden von Datenverkehr über VLAN-ID in einer Distributed Port-Gruppe erfolgt über Virtual Guest Tagging (VGT). Um Datenverkehr an eine VLAN-ID, wenn Virtual Switch Tagging (VST) aktiviert ist, verwenden Sie eine Regel für eine Uplink-Portgruppe oder einen Uplink-Port.

- Verwenden Sie den IP-Datenverkehrbezeichner, um Pakete nach IP-Version, IP-Adresse und Nächste-Schicht-Protokoll anzupassen.

9 Klicken Sie im Dialogfeld auf **OK**, um die Regel zu speichern.

Filtern des Datenverkehrs in einem verteilten Port oder einem Uplink-Port

Sie können mithilfe einer Regel Datenverkehr zulassen oder stoppen, um den Datenfluss über eine virtuelle Maschine, einen VMkernel-Adapter oder einen physischen Adapter zu sichern.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie zu einem verteilten Port oder zu einem Uplink-Port.
 - Klicken Sie auf **Verwalten > Ports**, um zu den verteilten Ports des Switches zu navigieren.
 - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Verwandte Objekte > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 2 Wählen Sie einen Port aus der Liste aus.
- 3 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Wenn das Filtern und Markieren auf Portebene nicht aktiviert ist, klicken Sie auf **Überschreiben**, und wählen Sie im Dropdown-Menü **Status** die Option **Aktiviert**.
- 5 Klicken Sie auf **Neu**, um eine neue Regel zu erstellen, oder wählen Sie eine Regel und klicken Sie auf **Bearbeiten**, um sie zu bearbeiten.

Sie können eine aus der verteilte Portgruppe oder Uplink-Portgruppe geerbte Regel ändern. So ist die Regel im Geltungsbereich des Ports eindeutig.
- 6 Wählen Sie im Dialogfeld für die Netzwerkverkehrsregel die Aktion **Zulassen** aus, damit Datenverkehr über den verteilten Port oder den Uplink-Port weitergeleitet wird, oder die Aktion **Verwerfen** aus, um den Datenverkehr zu beschränken.

7 Spezifizieren Sie die Art von Datenverkehr, für den die Regel angewendet werden soll.

Um zu bestimmen, ob der Datenfluss im Geltungsbereich der Regel für die Markierung oder Filterung ist, untersucht der vSphere Distributed Switch die Richtung des Datenverkehrs und die Eigenschaften wie Quelle und Ziel, VLAN, Nächste-Schicht-Protokoll, Infrastrukturverkehrstyp und so weiter.

- a Wählen Sie aus dem Dropdown-Menü **Datenverkehrsrichtung**, ob der Datenverkehr eingehend oder ausgehend (Ingress oder Egress) oder beides sein muss, damit die Regel ihn als passend erkennt.

Die Datenverkehrsrichtung beeinflusst auch, wie Sie Datenverkehrsquelle und -Ziel identifizieren.

- b Legen Sie durch die Bezeichner für den Systemdatentyp, Schicht-2-Paketattribute und Schicht-3-Paketattribute die Eigenschaften fest, die Pakete haben müssen, um der Regel zu entsprechen.

Ein Bezeichner repräsentiert einen Satz passender Kriterien, verbunden mit der Netzwerkschicht. Sie können den Datenverkehr an den Systemdatentyp, Schicht-2-Datenverkehreigenschaften und Schicht-3-Datenverkehreigenschaften anpassen. Sie können den Bezeichner für eine bestimmte Netzwerkschicht verwenden oder Bezeichner kombinieren, um die Pakete genauer anzupassen.

- Verwenden Sie den Systemverkehrbezeichner, um Pakete an den Typ der virtuellen Infrastrukturdaten anzupassen, die durch die Ports der Gruppe fließen. Sie können beispielsweise NFS für Datentransfers an Netzwerkspeicher wählen.
- Verwenden Sie den MAC-Datenverkehrbezeichner, um Pakete nach MAC-Adresse, VLAN-ID und Nächste-Schicht-Protokoll anzupassen.

Das Auffinden von Datenverkehr über VLAN-ID in einer Distributed Port-Gruppe erfolgt über Virtual Guest Tagging (VGT). Um Datenverkehr an eine VLAN-ID, wenn Virtual Switch Tagging (VST) aktiviert ist, verwenden Sie eine Regel für eine Uplink-Portgruppe oder einen Uplink-Port.

- Verwenden Sie den IP-Datenverkehrbezeichner, um Pakete nach IP-Version, IP-Adresse und Nächste-Schicht-Protokoll anzupassen.

8 Klicken Sie im Dialogfeld auf **OK**, um die Regel zu speichern.

Arbeiten mit Netzwerkverkehrsregeln in verteilten oder Uplink-Ports

Definieren Sie Datenverkehrsregeln in einer verteilten oder Uplink-Portgruppe, um eine Richtlinie für die Bearbeitung des Datenverkehrs im Zusammenhang mit einer virtuellen Maschine oder einem physischen Adapter einzuführen. Sie können bestimmten Datenverkehr filtern oder seinen QoS-Bedarf beschreiben.

■ [Anzeigen von Verkehrsregeln von verteilten Ports oder Uplink-Ports](#)

Überprüfen Sie die Verkehrsregeln, die die Richtlinie für das Filtern und Markieren des Datenverkehrs eines verteilten Ports oder Uplink-Ports darstellen.

■ Bearbeiten von Verkehrsregeln für verteilte Ports oder Uplink-Ports

Erstellen oder bearbeiten Sie Verkehrsregeln und verwenden Sie die entsprechenden Parameter, um eine Richtlinie für die Filterung oder Markierung des Datenverkehrs auf einem verteilten Port oder Uplink-Port zu konfigurieren.

■ Ändern der Regelprioritäten in verteilten oder Uplink-Ports

Ordnen Sie die Regeln neu an, die die Richtlinie zum Filtern und Markieren von Datenverkehr eines Distributed Port oder Uplink-Ports festlegen, um die Reihenfolge der Aktionen zur Analyse von Datenverkehr bezüglich Sicherheit und QoS zu ändern.

■ Löschen von Verkehrsregeln für verteilte Ports oder Uplink-Ports

Löschen Sie eine Verkehrsregel für einen verteilten Port oder einen Uplink-Port, um das Filtern zu beenden oder um bestimmte Pakettypen zu kennzeichnen, die an eine virtuelle Maschine oder einen physischen Adapter übertragen werden.

Anzeigen von Verkehrsregeln von verteilten Ports oder Uplink-Ports

Überprüfen Sie die Verkehrsregeln, die die Richtlinie für das Filtern und Markieren des Datenverkehrs eines verteilten Ports oder Uplink-Ports darstellen.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie zu einem verteilten Port oder zu einem Uplink-Port.
 - Klicken Sie auf **Verwalten > Ports**, um zu den verteilten Ports des Switches zu navigieren.
 - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Verwandte Objekte > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 2 Wählen Sie einen Port aus der Liste aus.
- 3 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 5 Wenn das Filtern und Markieren auf Portebene nicht aktiviert ist, klicken Sie auf **Überschreiben**, und wählen Sie im Dropdown-Menü **Status** die Option **Aktiviert**.
- 6 Untersuchen Sie **Aktion**, um zu sehen, ob die Regel Datenverkehr filtert (Zulassen oder Ablehnen) oder markiert (Tag) mit speziellen QoS-Anforderungen.
- 7 Wählen Sie aus der oberen Liste die Regel, für die Sie die Kriterien für die Auswahl von Datenverkehr anzeigen möchten.

Die bezeichnenden Parameter für den Datenverkehr der Regel werden in der Datenverkehrsbezeichner-Liste angezeigt.

Bearbeiten von Verkehrsregeln für verteilte Ports oder Uplink-Ports

Erstellen oder bearbeiten Sie Verkehrsregeln und verwenden Sie die entsprechenden Parameter, um eine Richtlinie für die Filterung oder Markierung des Datenverkehrs auf einem verteilten Port oder Uplink-Port zu konfigurieren.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie zu einem verteilten Port oder zu einem Uplink-Port.
 - Klicken Sie auf **Verwalten > Ports**, um zu den verteilten Ports des Switches zu navigieren.
 - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Verwandte Objekte > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 2 Wählen Sie einen Port aus der Liste aus.
- 3 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 5 Wenn das Filtern und Markieren auf Portebene nicht aktiviert ist, klicken Sie auf **Überschreiben**, und wählen Sie im Dropdown-Menü **Status** die Option **Aktiviert**.
- 6 Klicken Sie auf **Neu**, um eine neue Regel zu erstellen, oder wählen Sie eine Regel und klicken Sie auf **Bearbeiten**, um sie zu bearbeiten.

Sie können eine aus der verteilte Portgruppe oder Uplink-Portgruppe geerbte Regel ändern. So ist die Regel im Geltungsbereich des Ports eindeutig.

Nächste Schritte

Benennen Sie die Netzwerkverkehrsregel und wählen Sie für den Zielverkehr „Verweigern“, „Zulassen“ oder „Tag“.

Ändern der Regelprioritäten in verteilten oder Uplink-Ports

Ordnen Sie die Regeln neu an, die die Richtlinie zum Filtern und Markieren von Datenverkehr eines Distributed Port oder Uplink-Ports festlegen, um die Reihenfolge der Aktionen zur Analyse von Datenverkehr bezüglich Sicherheit und QoS zu ändern.

Der vSphere Distributed Switch wendet die Netzwerkverkehrsregeln in einer strengen Reihenfolge an. Wenn ein Paket einer Regel bereits entspricht, wird das Paket möglicherweise nicht der nächsten Regel in der Richtlinie übergeben.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie zu einem verteilten Port oder zu einem Uplink-Port.
 - Klicken Sie auf **Verwalten > Ports**, um zu den verteilten Ports des Switches zu navigieren.
 - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Verwandte Objekte > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 2 Wählen Sie einen Port aus der Liste aus.
- 3 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 5 Wenn das Filtern und Markieren auf Portebene nicht aktiviert ist, klicken Sie auf **Überschreiben**, und wählen Sie im Dropdown-Menü **Status** die Option **Aktiviert**.
- 6 Wählen Sie eine Regel und verwenden Sie die Pfeiltasten, um ihre Priorität zu ändern.
- 7 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Löschen von Verkehrsregeln für verteilte Ports oder Uplink-Ports

Löschen Sie eine Verkehrsregel für einen verteilten Port oder einen Uplink-Port, um das Filtern zu beenden oder um bestimmte Pakettypen zu kennzeichnen, die an eine virtuelle Maschine oder einen physischen Adapter übertragen werden.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie zu einem verteilten Port oder zu einem Uplink-Port.
 - Klicken Sie auf **Verwalten > Ports**, um zu den verteilten Ports des Switches zu navigieren.
 - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Verwandte Objekte > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 2 Wählen Sie einen Port aus der Liste aus.
- 3 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Wählen Sie **Filtern und Markieren des Datenverkehrs**.

- 5 Wenn das Filtern und Markieren auf Portebene nicht aktiviert ist, klicken Sie auf **Überschreiben**, und wählen Sie im Dropdown-Menü **Status** die Option **Aktiviert**.
- 6 Wählen Sie die entsprechende Regel aus und klicken Sie auf **Löschen**.
- 7 Klicken Sie auf **OK**.

Deaktivieren der Filterung und Markierung des Datenverkehrs in verteilten oder Uplink-Ports

Deaktivieren Sie die Richtlinie für Filterung und Markierung des Datenverkehrs für einen Port, damit der Datenverkehr ohne Sicherheitsfilterung oder Markierung für QoS zu einer virtuellen Maschine oder einem physischen Adapter fließen kann.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie zu einem verteilten Port oder zu einem Uplink-Port.
 - Klicken Sie auf **Verwalten > Ports**, um zu den verteilten Ports des Switches zu navigieren.
 - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Verwandte Objekte > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 2 Wählen Sie einen Port aus der Liste aus.
- 3 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Wählen Sie **Filtern und Markieren des Datenverkehrs**.
- 5 Klicken Sie auf **Außer Kraft setzen**, und wählen Sie im Dropdown-Menü **Status** die Option **Deaktiviert** aus.
- 6 Klicken Sie auf **OK**.

Qualifizieren des Datenverkehrs für die Filterung und Markierung

Der Datenverkehr, den Sie filtern oder mit QoS-Tags markieren möchten, kann nach dem Typ der übertragenen Infrastrukturdaten abgeglichen werden, wie Daten für Speicher, vCenter Server-Verwaltung usw., sowie nach Eigenschaften der Schichten 2 und 3.

Um dem Datenverkehr im Geltungsbereich der Regel genauer zu entsprechen, können Sie Kriterien für Systemdatentyp, Schicht-2-Header und Schicht-3-Header kombinieren.

Systemdatenverkehrsbezeichner

Wenn der Systemdatenverkehrsbezeichner in einer Regel für eine Portgruppe oder einen Port verwendet wird, können Sie festlegen, ob bestimmter Systemdatenverkehr mit einem QoS-Tag markiert, zugelassen oder verworfen werden soll.

Systemdatenverkehrstyp

Sie können den Datenverkehrstyp über die Ports der Gruppe auswählen, die Systemdaten enthält, also den Datenverkehr für die Verwaltung von vCenter Server, Speicher, VMware vSphere[®] vMotion[®] und vSphere Fault Tolerance. Sie können nur einen bestimmten Datenverkehrstyp oder den gesamten Systemdatenverkehr (mit Ausnahme einer Infrastrukturfunktion) markieren oder filtern. Sie können z. B. den Datenverkehr für die Verwaltung von vCenter Server, Speicher und vMotion mit einem QoS-Wert markieren oder filtern, nicht aber den Datenverkehr mit Fault Tolerance-Daten.

MAC-Bezeichner für Datenverkehr

Wenn Sie den MAC-Datenverkehrsbezeichner in einer Regel verwenden, können Sie übereinstimmende Kriterien für die Eigenschaften der Schicht 2 (Sicherheitsschicht) von Paketen wie die MAC-Adresse, die VLAN-ID und das Nächste-Schicht-Protokoll, das die Rahmennutzlast verbraucht, festlegen.

Protokolltyp

Das Attribut **Protokolltyp** des MAC-Datenverkehrsbezeichners entspricht dem Feld „EtherType“ in Ethernet-Frames. EtherType stellt den Typ des Nächste-Schicht-Protokolls dar, das die Nutzlast des Frames verbraucht.

Sie können ein Protokoll aus dem Dropdown-Menü auswählen oder seine Hexadezimalzahl eingeben. Um beispielsweise Datenverkehr für das LLDP-Protokoll (Link Layer Discovery Protocol) zu erfassen, geben Sie **88CC** ein.

VLAN-ID

Mit dem Attribut „VLAN-ID“ des MAC-Datenverkehrsbezeichners können Sie Datenverkehr in einem bestimmten VLAN markieren oder filtern.

Hinweis Der VLAN-ID-Bezeichner in einer verteilten Portgruppe funktioniert mit Virtual Guest Tagging (VGT).

Wenn ein Fluss mit einer VLAN-ID durch Virtual Switch Tagging (VST) gekennzeichnet wird, kann er mit dieser ID in einer Regel für eine verteilte Portgruppe bzw. für einen verteilten Port nicht aufgefunden werden. Das liegt daran, dass der Distributed Switch die Regelbedingungen einschließlich der VLAN-ID prüft, nachdem der Switch die Kennzeichnung des Datenverkehrs bereits aufgehoben hat. Um in diesem Fall den Datenverkehr erfolgreich nach VLAN-ID abzugleichen, müssen Sie eine Regel für eine Uplink-Portgruppe oder einen Uplink-Port verwenden.

Quelladresse

Wenn Sie die Attributgruppe „Quelladresse“ verwenden, können Sie Pakete nach der Quell-MAC-Adresse oder nach dem Netzwerk abgleichen.

Sie können einen Vergleichsoperator verwenden, um Pakete zu markieren oder zu filtern, die die angegebene Quelladresse oder das Netzwerk haben bzw. nicht haben.

Sie können die Datenverkehrsquelle auf mehreren Wegen abgleichen.

Tabelle 8-6. Muster für das Filtern oder Markieren von Datenverkehr nach MAC-Quelladresse

Parameter zum Abgleichen der Datenverkehr-Quelladresse	Vergleichsoperator	Netzwerkargumentformat
MAC-Adresse	ist oder ist nicht	Geben Sie die MAC-Adresse für den Abgleich ein. Trennen Sie die Oktette durch Doppelpunkte.
MAC-Netzwerk	matches oder does not match	Geben Sie die niedrigste Adresse im Netzwerk und eine Maske ein. Setzen Sie Einsen an die Positionen der Netzwerkbits und Nullen für den Host-Teil.

Legen Sie z. B. für ein MAC-Netzwerk mit dem Präfix 05:50:56, das 23 Bit lang ist, die Adresse als **00:50:56:00:00:00** und die Maske als **ff:ff:fe:00:00:00** fest.

Zieladresse

Wenn Sie die Attributgruppe „Zieladresse“ verwenden, können Sie Pakete mit ihren Zieladressen abgleichen. Die MAC-Zieladressenoptionen haben das gleiche Format wie die Optionen für die Quelladresse.

Vergleichsoperatoren

Um einen MAC-Bezeichner genauer auf Ihre Bedürfnisse abzustimmen, können Sie zustimmende oder verneinende Vergleiche verwenden. Sie können Operatoren verwenden, sodass z. B. alle Pakete außer denjenigen mit bestimmten Attributen im Bereich einer Regel liegen.

IP-Bezeichner für Datenverkehr

Wenn der IP-Datenverkehrsbezeichner in einer Regel verwendet wird, können Sie Kriterien definieren, um Datenverkehr an die Schicht 3-Eigenschaften (Netzwerkschicht) anzupassen, beispielsweise IP-Version, IP-Adresse, Nächste-Schicht-Protokoll und Port.

Protokoll

Das Attribut **Protocol** des IP-Datenverkehrsbezeichners stellt das Nächste-Schicht-Protokoll dar, das die Nutzdaten des Pakets verarbeitet. Wählen Sie im Dropdown-Menü ein Protokoll aus oder geben Sie die entsprechende Dezimalzahl gemäß RFC 1700 ein.

Bei TCP- und UDP-Protokollen können Sie den Datenverkehr auch nach Quell- und Zielports anpassen.

Quellport

Wenn das Attribut „Source Port“ verwendet wird, können Sie TCP- oder UDP-Pakete nach dem Quellport anpassen. Beachten Sie die Datenverkehrsrichtung, wenn der Datenverkehr an einen Quellport angepasst wird.

Zielport

Wenn das Attribut „Destination Port“ verwendet wird, können Sie TCP- oder UDP-Pakete nach dem Zielport anpassen. Beachten Sie die Datenverkehrsrichtung, wenn der Datenverkehr an einen Zielport angepasst wird.

Quelladresse

Wenn das Attribut „Source Address“ verwendet wird, können Sie Pakete nach der Quelladresse oder dem Subnetz anpassen. Beachten Sie die Datenverkehrsrichtung, wenn der Datenverkehr an eine Quelladresse oder ein Netz angepasst wird.

Es gibt mehrere Möglichkeiten, die Datenverkehrsquelle anzupassen.

Tabelle 8-7. Muster zum Filtern oder Markieren von Datenverkehr nach Quell-IP-Adresse

Parameter zum Abgleichen der Datenverkehr-Quelladresse	Vergleichsoperator	Netzwerkargumentformat
IP-Version	alle	Wählen Sie im Dropdown-Menü die IP-Version aus.
IP-Adresse	is oder is not	Geben Sie die IP-Adresse für die Anpassung ein.
IP-Subnetz	matches oder does not match	Geben Sie die niedrigste Adresse im Subnetz und die Bitlänge des Subnetzpräfixes ein.

Zieladresse

Verwenden Sie die Zieladresse, um Pakete nach IP-Adresse, Subnetz oder IP-Version anzupassen. Die Zieladresse weist dasselbe Format wie die Quelladresse auf.

Vergleichsoperatoren

Um Datenverkehr in einem IP-Bezeichner besser an Ihre Anforderungen anzupassen, können Sie positive oder negative Vergleiche verwenden. Sie können definieren, dass alle Pakete in den Bereich einer Regel fallen, mit Ausnahme von Paketen mit bestimmten Attributen.

Verwalten von Richtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch

Sie können die Netzwerkrichtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch ändern.

Voraussetzungen

Erstellen Sie einen vSphere Distributed Switch mit einer oder mehreren Portgruppen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie im Objektnavigator mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Verteilte Portgruppen > Verteilte Portgruppen verwalten** aus.
- 3 Aktivieren Sie auf der Seite „Portgruppenrichtlinien auswählen“ das Kontrollkästchen neben den Richtlinienkategorien, die geändert werden sollen, und klicken Sie auf **Weiter**.

Option	Beschreibung
Sicherheit	Nehmen Sie Einstellungen zu MAC-Adressänderungen, zu gefälschten Übertragungen und zum Promiscuous-Modus für die ausgewählten Portgruppen vor.
Traffic-Shaping	Legen Sie die durchschnittliche Bandbreite, die Spitzenbandbreite und die Burstgröße für den ein- und ausgehenden Datenverkehr auf den ausgewählten Portgruppen fest.
VLAN	Konfigurieren Sie die Art der Verbindung der ausgewählten Portgruppen zu physischen VLANs.
Teaming und Failover	Legen Sie den Lastausgleich, die Failover-Erkennung, die Switch-Benachrichtigung und die Failover-Reihenfolge für die ausgewählten Portgruppen fest.
Ressourcenzuteilung	Legen Sie die Zuordnung des Netzwerkressourcenpools für die ausgewählten Portgruppen fest. Diese Option ist für vSphere Distributed Switch Version 5.0 und höher verfügbar.
Überwachung	Aktivieren oder deaktivieren Sie NetFlow auf den ausgewählten Portgruppen. Diese Option ist für vSphere Distributed Switch Version 5.0.0 und höher verfügbar.
Filtern und Markieren des Datenverkehrs	Konfigurieren Sie eine Richtlinie für das Filtern (zulassen oder verwerfen) und Markieren bestimmter Datenverkehrstypen über die Ports von ausgewählten Portgruppen. Diese Option ist für vSphere Distributed Switch Version 5.5 und höher verfügbar.
Sonstiges	Aktivieren oder deaktivieren Sie die Portblockierung auf den ausgewählten Portgruppen.

- 4 Wählen Sie auf der Seite „Portgruppen auswählen“ die zu bearbeitende(n) verteilte(n) Portgruppe(n) aus und klicken Sie auf **Weiter**.

- 5 (Optional) Verwenden Sie die Dropdown-Menüs auf der Seite „Sicherheit“, um die Sicherheitsausnahmen zu bearbeiten, und klicken Sie auf **Weiter**.

Option	Beschreibung
Promiscuous-Modus	<ul style="list-style-type: none"> ■ Ablehnen. Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden. ■ Akzeptieren. Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames erkannt, die über den vSphere Distributed Switch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
MAC-Adressänderungen	<ul style="list-style-type: none"> ■ Ablehnen. Wenn die Option auf Ablehnen festgelegt ist und die MAC-Adresse des Adapters im Gastbetriebssystem in einen anderen Wert geändert wird als in den, der in der <code>.vmx</code>-Konfigurationsdatei angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der <code>.vmx</code>-Konfigurationsdatei ändert, werden wieder alle eingehenden Frames durchgeleitet. ■ Akzeptieren. Die Änderung der MAC-Adresse des Gastbetriebssystems hat die gewünschte Auswirkung. Frames an die neue MAC-Adresse werden empfangen.
Gefälschte Übertragungen	<ul style="list-style-type: none"> ■ Ablehnen. Alle ausgehenden Frames, bei denen sich die MAC-Quelladresse von der für den Adapter festgelegten MAC-Adresse unterscheidet, werden verworfen. ■ Akzeptieren. Es wird keine Filterung vorgenommen und alle ausgehenden Frames werden durchgeleitet.

- 6 (Optional) Verwenden Sie die Dropdown-Menüs auf der Seite „Traffic-Shaping“, um das Ingress- oder Egress-Traffic-Shaping zu aktivieren bzw. zu deaktivieren, und klicken Sie auf **Weiter**.

Option	Beschreibung
Status	Wenn Sie entweder Ingress-Traffic-Shaping oder Egress-Traffic-Shaping aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für jeden mit der betreffenden Portgruppe verknüpften VMkernel-Adapter oder virtuellen Netzwerkadapter. Wenn Sie die Richtlinie deaktivieren, besteht für Dienste standardmäßig eine uneingeschränkte Verbindung zum physischen Netzwerk.
Durchschnittliche Bandbreite	Legt fest, wie viele Bit pro Sekunde im Durchschnitt einen Port durchlaufen dürfen (zulässige durchschnittliche Datenlast).

Option	Beschreibung
Spitzenbandbreite	Die maximale Zahl der Bit pro Sekunde, die einen Port durchlaufen darf, wenn er einen Datenverkehr-Burst sendet oder empfängt. Diese maximale Zahl begrenzt die Bandbreite, die ein Port nutzen kann, wenn er seinen Burst-Bonus verwendet.
Burstgröße	Die maximal zulässige Byte-Anzahl in einem Burst. Wenn dieser Parameter gesetzt ist, kann ein Port einen Burst-Bonus erhalten, wenn er nicht die gesamte ihm zugeteilte Bandbreite nutzt. Immer wenn dieser Port mehr Bandbreite benötigt als von der Einstellung Durchschnittliche Bandbreite angegeben, kann er die Erlaubnis erhalten, Daten mit einer höheren Geschwindigkeit zu übertragen, wenn ein Burst-Bonus verfügbar ist. Dieser Parameter begrenzt die Anzahl der Byte, die im Burst-Bonus angesammelt werden und mit einer höheren Geschwindigkeit übertragen werden können.

- 7 (Optional) Verwenden Sie die Dropdown-Menüs auf der Seite „VLAN“, um die VLAN-Richtlinie zu bearbeiten, und klicken Sie auf **Weiter**.

Option	Beschreibung
Keine	Verwenden Sie VLAN nicht.
VLAN	Geben Sie im Feld VLAN-ID eine Zahl zwischen 1 und 4094 ein.
VLAN-Trunking	Geben Sie einen VLAN-Trunk-Bereich ein.
Privates VLAN	Wählen Sie ein verfügbares privates VLAN aus, das verwendet werden soll.

- 8 (Optional) Verwenden Sie die Dropdown-Menüs auf der Seite „Teaming und Failover“, um die Einstellungen zu bearbeiten, und klicken Sie auf **Weiter**.

Option	Beschreibung
Lastausgleich	<p>Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit Ether-Channel konfiguriert wird. Bei allen anderen Optionen muss Ether-Channel deaktiviert sein. Wählen Sie, wie ein Uplink ausgewählt werden soll.</p> <ul style="list-style-type: none"> ■ Anhand des virtuellen Quellports routen. Wählen Sie den Uplink basierend auf dem virtuellen Port, durch den der Datenverkehr in den Distributed Switch gelangt ist. ■ Anhand des IP-Hashs routen. Wählen Sie einen Uplink anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets aus. Bei Paketen ohne IP wird zur Berechnung des Hashs der Wert verwendet, der im Offset eingetragen ist. ■ Anhand des Quell-MAC-Hashs routen. Wählen Sie einen Uplink anhand eines Hashs des Quell-Ethernets aus. ■ Anhand der physischen Netzwerkkartenauslastung routen. Wählen Sie einen Uplink auf Grundlage der aktuellen Auslastungen der physischen Netzwerkkarten. ■ Ausdrückliche Failover-Reihenfolge verwenden. Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Ermittlungskriterien erfüllt.
Netzwerk-Failover-Ermittlung	<p>Wählen Sie die Verfahrensweise zur Verwendung der Failover-Erkennung aus.</p> <ul style="list-style-type: none"> ■ Nur Verbindungsstatus. Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt, nicht jedoch Konfigurationsfehler, z. B. die Blockierung eines Ports des physischen Switches durch STP (Spanning Tree Protocol), eine Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel an der anderen Seite eines physischen Switches. ■ Signalprüfung. Sendet Signale, wartet auf Signalprüfpakete auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. Verwenden Sie die Signalprüfung nicht zusammen mit dem IP-Hash-Lastausgleich.
Switches benachrichtigen	<p>Wählen Sie Ja oder Nein, um Switches bei einem Failover zu benachrichtigen. Verwenden Sie diese Option nicht, wenn die an die Portgruppe angeschlossenen virtuellen Maschinen den Netzwerklasterausgleich (NLB) von Microsoft im Unicast-Modus verwenden.</p> <p>Wenn Sie Ja wählen, wird jedes Mal, wenn eine virtuelle Netzwerkkarte an einen Distributed Switch angeschlossen wird oder ein Failover-Ereignis dazu führt, dass der Datenverkehr einer virtuellen Netzwerkkarte über eine andere physische Netzwerkkarte im Team geleitet wird, eine Benachrichtigung über das Netzwerk gesendet, um die Verweistabellen auf den physischen Switches zu aktualisieren. Verwenden Sie diesen Prozess, um die niedrigste Latenz von Failover-Vorkommen und Migrationen mit vMotion zu erreichen.</p>

Option	Beschreibung
Failback	<p>Wählen Sie Ja oder Nein, um die Failback-Funktion zu deaktivieren bzw. zu aktivieren.</p> <p>Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird.</p> <ul style="list-style-type: none"> ■ Ja (Standard). Der Adapter wird sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert und ersetzt damit den Standby-Adapter, der ggf. seinen Platz eingenommen hatte. ■ Nein. Ein ausgefallener Adapter bleibt nach der Wiederherstellung seiner Funktionsfähigkeit deaktiviert, bis ein anderer gegenwärtig aktiver Adapter ausfällt und ersetzt werden muss.
Failover-Reihenfolge	<p>Wählen Sie, wie die Verarbeitungslast für Uplinks verteilt werden soll. Um bestimmte Uplinks zu verwenden und andere für den Fall zu reservieren, dass die verwendeten Uplinks ausfallen, legen Sie diese Bedingung fest, indem Sie sie in unterschiedliche Gruppen verschieben.</p> <ul style="list-style-type: none"> ■ Aktive Uplinks. Dieser Uplink wird weiter verwendet, wenn die Verbindung zum Netzwerkadapter hergestellt und aktiv ist. ■ Standby-Uplinks. Dieser Uplink wird verwendet, wenn mindestens eine Verbindung zum aktiven Adapter nicht verfügbar ist. Wenn Sie den IP-Hash-Lastenausgleich verwenden, konfigurieren Sie keine Standby-Uplinks. ■ Nicht verwendete Uplinks. Verwenden Sie diesen Uplink nicht.

- 9 (Optional) Verwenden Sie auf der Seite „Ressourcenzuteilung“ das Dropdown-Menü „Netzwerkressourcenpool“, um Ressourcenzuteilungen hinzuzufügen oder zu entfernen, und klicken Sie auf **Weiter**.
- 10 (Optional) Verwenden Sie das Dropdown-Menü auf der Seite „Überwachen“, um NetFlow zu aktivieren bzw. zu deaktivieren, und klicken Sie auf **Weiter**.

Option	Beschreibung
Deaktiviert	NetFlow ist für die verteilte Portgruppe deaktiviert.
Aktiviert	NetFlow ist für die verteilte Portgruppe aktiviert. Sie können auf der vSphere Distributed Switch-Ebene NetFlow-Einstellungen konfigurieren.

- 11 (Optional) Aktivieren oder deaktivieren Sie auf der Seite „Filtern und Markieren des Datenverkehrs“ im Dropdown-Menü **Status** Datenverkehrsregeln für das Filtern oder Markieren bestimmter Datenflüsse und klicken Sie auf **Weiter**.

Sie können die folgenden Attribute einer Regel festlegen, die den Zieldatenverkehr und die zugehörige Aktion bestimmen:

Option	Beschreibung
Name	Name der Regel
Aktion	<ul style="list-style-type: none"> ■ Zulassen. Gewährt den Zugriff auf einen bestimmten Datenverkehrstyp. ■ Verwerfen. Verweigert den Zugriff auf einen bestimmten Datenverkehrstyp. ■ Tag. Klassifiziert den Datenverkehr bezüglich QoS, indem CoS- und DSCP-Tags eingefügt werden oder Datenverkehr damit erneut gekennzeichnet wird.
Datenverkehrsrichtung	<p>Legt fest, ob die Regel für eingehenden, ausgehenden oder ein- und ausgehenden Datenverkehr gilt.</p> <p>Die Datenverkehrsrichtung beeinflusst auch, wie Sie Datenverkehrsquelle und -Ziel identifizieren.</p>
Systemdatenverkehrsbezeichner	Gibt an, dass die Regel für Systemdatenverkehr gilt, und legt den Infrastrukturprotokolltyp fest, für den die Regel gelten soll. Markieren Sie z. B. den Datenverkehr für die Verwaltung durch vCenter Server mit einem Prioritäts-Tag.

Option	Beschreibung
MAC-Bezeichner	<p>Qualifiziert den Datenverkehr für die Regel anhand des Layer 2-Headers.</p> <ul style="list-style-type: none"> ■ Protokolltyp. Legt das Nächste-Schicht-Protokoll fest (IPv4, IPv6 usw.), das die Nutzlast verarbeitet. <p>Dieses Attribut entspricht dem Feld „EtherType“ in Ethernet-Frames.</p> <p>Sie können ein Protokoll aus dem Dropdown-Menü auswählen oder seine Hexadezimalzahl eingeben.</p> <p>Um beispielsweise nach Datenverkehr für das LLDP-Protokoll (Link Layer Discovery Protocol) zu suchen, geben Sie 88cc ein.</p> ■ VLAN-ID. Sucht Datenverkehr anhand des VLAN. <p>Der VLAN-ID-Bezeichner in einer verteilten Portgruppe funktioniert mit Virtual Guest Tagging (VGT).</p> <p>Wenn ein Datenfluss mit einer VLAN-ID durch Virtual Switch Tagging (VST) gekennzeichnet wird, kann er mit dieser ID in einer Regel für eine verteilte Portgruppe nicht aufgefunden werden. Das liegt daran, dass der Distributed Switch die Regelbedingungen einschließlich der VLAN-ID prüft, nachdem der Switch die Kennzeichnung des Datenverkehrs bereits aufgehoben hat. Um den Datenverkehr erfolgreich nach VLAN-ID abzugleichen, verwenden Sie eine Regel für eine Uplink-Portgruppe oder einen Uplink-Port.</p> ■ Quellfilter. Legt eine einzelne MAC-Adresse oder ein einzelnes MAC-Netzwerk zum Abgleichen von Paketen anhand der Quelladresse fest. <p>Für ein MAC-Netzwerk geben Sie die niedrigste Adresse im Netzwerk und eine Platzhaltermaske ein. Die Maske enthält Nullen an den Positionen der Netzwerkbits und Einsen für den Host-Teil.</p> <p>Legen Sie z. B. für ein MAC-Netzwerk mit dem Präfix 05:50:56, das 23 Bit lang ist, die Adresse als 00:50:56:00:00:00 und die Maske als 00:00:01:ff:ff:ff fest.</p> ■ Zielfilter. Legt eine einzelne MAC-Adresse oder ein einzelnes MAC-Netzwerk zum Abgleichen von Paketen anhand der Zieladresse fest. Die MAC-Zieladresse unterstützt das gleiche Format wie die Quelladresse.
IP-Bezeichner	<p>Qualifiziert den Datenverkehr für die Regel anhand des Layer 3-Headers.</p> ■ Protokoll. Legt das Nächste-Schicht-Protokoll fest (TCP, UDP usw.), das die Nutzlast verarbeitet. <p>Wählen Sie im Dropdown-Menü ein Protokoll aus oder geben Sie die entsprechende Dezimalzahl gemäß <i>RFC 1700, Assigned Numbers</i> ein.</p> <p>Beim TCP- und UDP-Protokoll können Sie auch den Quell- und Zielport festlegen.</p> ■ Quellport. Gleicht TCP- oder UDP-Pakete mit einem Quellport ab. Beachten Sie die Richtung des Datenverkehrs, der im Geltungsbereich der Regel liegt, wenn Sie den Quellport bestimmen, mit dem Pakete abgeglichen werden sollen. ■ Zielport. Gleicht TCP- oder UDP-Pakete mit dem Zielport ab. Beachten Sie die Richtung des Datenverkehrs, der im Geltungsbereich der Regel liegt, wenn Sie den Zielport bestimmen, mit dem Pakete abgeglichen werden sollen.

Option	Beschreibung
	<ul style="list-style-type: none"> ■ Quellfilter. Legt die IP-Version, eine einzelne IP-Adresse oder ein Subnetz zum Abgleichen von Paketen anhand der Quelladresse fest. Für ein Subnetz geben Sie die niedrigste Adresse und die Bitlänge des Präfixes ein. ■ Zielfilter. Legt die IP-Version, eine einzelne IP-Adresse oder ein Subnetz zum Abgleichen von Paketen anhand der Quelladresse fest. Die IP-Zieladresse unterstützt das gleiche Format wie die Quelladresse.

- 12 (Optional) Wählen Sie auf der Seite „Verschiedenes“ **Ja** oder **Nein** aus dem Dropdown-Menü aus und klicken Sie auf **Weiter**.

Wählen Sie **Ja**, um alle Ports in der Portgruppe zu schließen. Durch das Herunterfahren wird möglicherweise der normale Netzwerkbetrieb auf den Hosts oder virtuellen Maschinen gestört, die die Ports verwenden.

- 13 Überprüfen Sie Ihre Einstellungen auf der Seite Bereit zum Abschließen, und klicken Sie auf **Beenden**.

Verwenden Sie die Schaltfläche **Zurück**, um Einstellungen zu ändern.

Portblockierungsrichtlinien

Mit Portblockierungsrichtlinien können Sie ausgewählte Ports daran hindern, Daten zu senden oder zu empfangen.

Bearbeiten der Portblockierungsrichtlinie für eine verteilte Portgruppe

Sie können alle Ports in einer verteilten Portgruppe blockieren.

Durch die Blockierung der Ports einer verteilten Portgruppe wird möglicherweise der normale Netzwerkbetrieb auf den Hosts oder virtuellen Maschinen gestört, die die Ports verwenden.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie im Objektnavigators mit der rechten Maustaste auf den Distributed Switch und wählen Sie **Verteilte Portgruppen > Verteilte Portgruppen verwalten** aus.
- 3 Aktivieren Sie das Kontrollkästchen **Sonstiges**, und klicken Sie auf **Weiter**.
- 4 Wählen Sie die verteilte(n) Portgruppe(n) aus, die Sie konfigurieren möchten, und klicken Sie auf **Weiter**.
- 5 Aktivieren oder deaktivieren Sie im Dropdown-Menü **Alle Ports blockieren** die Portblockierung und klicken Sie auf **Weiter**.
- 6 Überprüfen Sie die gewählten Einstellungen, und klicken Sie auf **Beenden**.

Bearbeiten der Portblockierungsrichtlinie für verteilte oder Uplink-Portgruppen

Sie können einzelne verteilte Ports oder Uplink-Ports blockieren.

Die Blockierung des Datenverkehrs in einem Port kann die normalen Netzwerkvorgänge der Hosts oder der virtuellen Maschinen stören, die diese Ports verwenden.

Voraussetzungen

Aktivieren Sie die Außerkraftsetzungen auf Portebene. Siehe [Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene](#).

Verfahren

- 1 Navigieren Sie zu einem verteilten Port oder zu einem Uplink-Port.
 - Klicken Sie auf **Verwalten > Ports**, um zu den verteilten Ports des Switches zu navigieren.
 - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Verwandte Objekte > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken Sie auf der Registerkarte **Verwalten** auf **Ports**.
- 2 Wählen Sie einen Port aus der Liste aus.
- 3 Klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**.
- 4 Aktivieren Sie im Abschnitt **Sonstiges** das Kontrollkästchen **Außer Kraft setzen** und aktivieren oder deaktivieren Sie die Portblockierung im Dropdown-Menü.
- 5 Klicken Sie auf **OK**.

Isolieren des Netzwerkverkehrs mithilfe von VLANs

9

Mit VLANs können Sie ein Netzwerk in mehrere logische Broadcast-Domänen auf Layer 2 des Netzwerkprotokoll-Stacks segmentieren.

Dieses Kapitel enthält die folgenden Themen:

- VLAN-Konfiguration
- Private VLANs

VLAN-Konfiguration

Mit virtuellen LANs (VLANs) kann ein einzelnes physisches LAN-Segment weiter isoliert werden, sodass Portgruppen derart voneinander isoliert werden, als befänden sie sich in unterschiedlichen physischen Segmenten.

Vorteile der Verwendung von VLANs in vSphere

Die VLAN-Konfiguration in einer vSphere-Umgebung bringt bestimmte Vorteile mit sich.

- ESXi-Hosts werden in eine bereits bestehende VLAN-Topologie integriert.
- Der Netzwerkdatenverkehr wird isoliert und abgesichert.
- Die Überlastung durch Netzwerkdatenverkehr wird verringert.

Sehen Sie sich das Video zu den Vorteilen und wichtigsten Prinzipien der Einführung von VLANs in eine vSphere-Umgebung ein.



Verwenden von VLANs in einer vSphere-Umgebung:
(https://vmwaretv.vmware.com/media/t/1_hff29dl8)

VLAN-Tagging-Modi

vSphere unterstützt drei Modi des VLAN-Taggings in ESXi: External Switch Tagging (EST), Virtual Switch Tagging (VST) und Virtual Guest Tagging (VGT).

Tagging-Modus	VLAN-ID in Switch-Portgruppen	Beschreibung
EST	0	Der physische Switch führt das VLAN-Tagging durch. Die Host-Netzwerkadapter sind verbunden, um auf Ports auf dem physischen Switch zuzugreifen.
VST	Zwischen 1 und 4094	Das VLAN-Tagging wird vom virtuellen Switch durchgeführt, bevor die Pakete den Host verlassen. Die Host-Netzwerkadapter müssen mit Trunk-Ports auf dem physischen Switch verbunden sein.
VGT	<ul style="list-style-type: none"> ■ 4095 für Standard-Switch ■ VLAN-Bereich und einzelne VLANs für verteilten Switch 	<p>Die virtuelle Maschine führt das VLAN-Tagging durch. Der virtuelle Switch behält die VLAN-Tags bei, wenn die Pakete zwischen dem VM-Netzwerkstapel und dem externen Switch weitergeleitet werden. Die Host-Netzwerkadapter müssen mit Trunk-Ports auf dem physischen Switch verbunden sein.</p> <p>Der vSphere Distributed Switch unterstützt eine Änderung von VGT. Aus Sicherheitsgründen können Sie einen Distributed Switch so konfigurieren, dass nur Pakete bestimmter VLANs durchgelassen werden.</p> <p>Hinweis Für VGT muss ein 802.1Q-VLAN-Trunking-Treiber auf dem Gastbetriebssystem der virtuellen Maschine installiert sein.</p>

Sehen Sie sich das Video mit Erklärungen der VLAN-Tagging-Modi in virtuellen Switches an.



VLAN-Tagging-Modi in vSphere

(https://vmwaretv.vmware.com/media/t/1_3bluh3s4)

Private VLANs

Private VLANs werden verwendet, um VLAN-ID-Beschränkungen zu beheben, indem die logische Broadcast-Domäne weiter in mehrere kleinere Broadcast-Unterdomänen segmentiert wird.

Ein privates VLAN wird durch seine primäre VLAN-ID identifiziert. Einer primären VLAN-ID können mehrere sekundäre VLAN-IDs zugeordnet sein. Primäre VLANs sind **Promiscuous**, sodass Ports in einem privaten VLAN mit Ports kommunizieren können, die als primäres VLAN konfiguriert sind. Ports in einem sekundären VLAN können entweder **Isoliert** sein und nur mit Promiscuous-Ports kommunizieren oder es handelt sich um **Community**-Ports, die sowohl mit Promiscuous-Ports als auch mit anderen Ports im gleichen sekundären VLAN kommunizieren.

Wenn Sie private VLANs zwischen einem Host und dem Rest des physischen Netzwerks verwenden möchten, muss der physische Switch, der mit dem Host verbunden ist, privates VLAN unterstützen und ordnungsgemäß mit den von ESXi verwendeten VLAN-IDs konfiguriert sein, damit das private VLAN funktioniert. Für physische Switches, die dynamisches MAC+VLAN-ID-basiertes Lernen verwenden, müssen alle entsprechenden privaten VLAN-IDs zuerst in die VLAN-Datenbank des Switches eingegeben werden.

Erstellen eines privaten VLAN

Erstellen Sie auf dem vSphere Distributed Switch die erforderlichen privaten VLANs, damit Sie verteilte Ports für ein privates VLAN zuweisen können.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Wählen Sie **Privates VLAN** aus und klicken Sie auf **Bearbeiten**.
- 4 Um ein primäres VLAN hinzuzufügen, klicken Sie unter „Primäre VLAN-ID“ auf **Hinzufügen** und geben Sie die ID eines primären VLAN ein.
- 5 Klicken Sie auf das **Pluszeichen (+)** vor der primären VLAN-ID, um sie der Liste hinzuzufügen.
Das primäre private VLAN wird auch unter „ID des sekundären privaten VLANs“ angezeigt.
- 6 Um ein sekundäres VLAN hinzuzufügen, klicken Sie im rechten Fensterbereich auf **Hinzufügen** und geben Sie die VLAN-ID ein.
- 7 Klicken Sie auf das **Pluszeichen (+)** vor der sekundären VLAN-ID, um sie der Liste hinzuzufügen.
- 8 Wählen Sie im Dropdown-Menü in der Spalte **Typ des sekundären VLANs** entweder **Isoliert** oder **Community** aus.
- 9 Klicken Sie auf **OK**.

Nächste Schritte

Konfigurieren Sie eine verteilte Portgruppe oder einen verteilten Port, um dem privaten VLAN Datenverkehr zuzuordnen. Siehe [Konfigurieren von VLAN-Tagging in einer verteilten Portgruppe oder einem verteilten Port](#).

Entfernen eines primären privaten VLAN

Entfernen Sie nicht verwendete primäre VLANs aus der Konfiguration eines vSphere Distributed Switch.

Wenn Sie ein primäres privates VLAN entfernen, werden auch die verbunden sekundären privaten VLANs entfernt.

Voraussetzungen

Stellen Sie sicher, dass für Portgruppen nicht die Verwendung des primären VLAN und der verbundenen sekundären VLANs konfiguriert ist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Wählen Sie **Privates VLAN** aus und klicken Sie auf **Bearbeiten**.
- 4 Wählen Sie das primäre private VLAN aus, das entfernt werden soll.
- 5 Klicken Sie auf **Entfernen** unter der Liste „Primäre VLAN-ID“.

- 6 Klicken Sie auf **OK**, um zu bestätigen, dass Sie das primäre VLAN entfernen möchten.
- 7 Klicken Sie auf **OK**.

Entfernen eines sekundären privaten VLAN

Entfernen Sie sekundäre private VLANs, die nicht verwendet werden, aus der Konfiguration eines vSphere Distributed Switch.

Voraussetzungen

Stellen Sie sicher, dass für Portgruppen nicht die Verwendung des sekundären VLAN konfiguriert ist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Wählen Sie **Privates VLAN** aus und klicken Sie auf **Bearbeiten**.
- 4 Wählen Sie ein primäres privates VLAN aus.
Die damit verbundenen sekundären privaten VLANs werden rechts angezeigt.
- 5 Wählen Sie das sekundäre private VLAN aus, das entfernt werden soll.
- 6 Klicken Sie unter der Liste „Sekundäre VLAN-ID“ auf **Entfernen** und klicken Sie dann auf **OK**.

Verwalten von Netzwerkressourcen

10

vSphere bietet mehrere unterschiedliche Methoden zur Vereinfachung der Verwaltung von Netzwerkressourcen.

Dieses Kapitel enthält die folgenden Themen:

- [DirectPath I/O](#)
- [Single Root I/O Virtualization \(SR-IOV\)](#)
- [Jumbo-Frames](#)
- [TCP-Segmentierungs-Offload](#)
- [Large Receive Offload](#)
- [NetQueue und Netzwerkleistung](#)

DirectPath I/O

DirectPath-I/O ermöglicht den Zugriff virtueller Maschinen auf physische PCI-Funktionen auf Plattformen mit einer E/A-Arbeitsspeicherverwaltungseinheit.

Die folgenden Funktionen sind nicht für virtuelle Maschinen verfügbar, die mit DirectPath konfiguriert sind:

- Hinzufügen und Entfernen von virtuellen Geräten bei laufendem Betrieb
- Anhalten und Fortsetzen
- Aufzeichnen und Wiedergabe
- Fault Tolerance
- Hohe Verfügbarkeit
- DRS (eingeschränkte Verfügbarkeit. Die virtuelle Maschine kann Teil eines Clusters sein, kann aber nicht über Hosts hinweg migriert werden)
- Snapshots

Die folgenden Funktionen sind nur für virtuelle Maschinen verfügbar, die mit DirectPath I/O auf Cisco Unified Computing Systems (UCS) über Cisco Virtual Machine Fabric Extender (VM-FEX) Distributed Switches konfiguriert sind.

- vMotion
- Hinzufügen und Entfernen von virtuellen Geräten bei laufendem Betrieb
- Anhalten und Fortsetzen
- Hohe Verfügbarkeit
- DRS
- Snapshots

Detaillierte Informationen über unterstützte Switches und Switch-Konfigurationen finden Sie in der Dokumentation zu Cisco VM-FEX.

- **Aktivieren des Passthroughs für ein Netzwerkgerät auf einem Host**

Passthrough-Geräte ermöglichen eine effiziente Nutzung der Ressourcen und verbessern die Leistung in Ihrer Umgebung. Sie können „DirectPath-I/O-Passthrough“ für ein Netzwerkgerät auf einem Host aktivieren.

- **Konfigurieren eines PCI-Geräts auf einer virtuellen Maschine**

Passthrough-Geräte ermöglichen eine effizientere Nutzung der Ressourcen und verbessern die Leistung in Ihrer Umgebung. Sie können auf einer virtuellen Maschine im vSphere Web Client ein Passthrough-PCI-Gerät konfigurieren.

- **Aktivieren von DirectPath I/O mit vMotion auf einer virtuellen Maschine**

Sie können DirectPath I/O mit vMotion für virtuelle Maschinen in einem Datacenter auf einem Cisco UCS-System aktivieren, das über mindestens einen unterstützten Cisco UCS Virtual Machine Fabric Extender (VM-FEX) Distributed Switch verfügt.

Aktivieren des Passthroughs für ein Netzwerkgerät auf einem Host

Passthrough-Geräte ermöglichen eine effiziente Nutzung der Ressourcen und verbessern die Leistung in Ihrer Umgebung. Sie können „DirectPath-I/O-Passthrough“ für ein Netzwerkgerät auf einem Host aktivieren.

Vorsicht Wenn Ihr ESXi-Host zum Starten von einem USB-Gerät oder einer an einen USB-Kanal angeschlossenen SD-Karte konfiguriert ist, stellen Sie sicher, dass Sie „DirectPath-I/O-Passthrough“ für den USB-Controller nicht aktivieren. Das Passthrough durch einen USB-Controller auf einem ESXi-Host, der von einem USB-Gerät oder einer SD-Karte startet, kann dazu führen, dass der Host in einen Zustand gerät, in dem die Konfiguration nicht registriert werden kann.

Verfahren

- 1 Navigieren Sie zum Host im vSphere Web Client-Navigator.

- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Einstellungen**.
- 3 Klicken Sie im Abschnitt „Hardware“ auf **PCI-Geräte**.
- 4 Um „DirectPath I/O-Passthrough“ für ein PCI-Netzwerkgerät auf dem Host zu aktivieren, klicken Sie auf **Bearbeiten**.

Eine Liste der verfügbaren Passthrough-Geräte wird angezeigt.

Symbol	Beschreibung
Grünes Symbol	Ein Gerät ist aktiv und kann aktiviert werden.
Oranges Symbol	Der Zustand des Geräts hat sich geändert und Sie müssen den Host neu starten, bevor Sie das Gerät verwenden können.

- 5 Wählen Sie die für das Passthrough zu verwendenden Netzwerkgeräte aus und klicken Sie auf **OK**.

Das ausgewählte PCI-Gerät wird in der Tabelle angezeigt. Die Geräteinformationen werden am unteren Rand des Bildschirms angezeigt.

- 6 Starten Sie den Host neu, damit das PCI-Netzwerkgerät zum Einsatz zur Verfügung steht.

Konfigurieren eines PCI-Geräts auf einer virtuellen Maschine

Passthrough-Geräte ermöglichen eine effizientere Nutzung der Ressourcen und verbessern die Leistung in Ihrer Umgebung. Sie können auf einer virtuellen Maschine im vSphere Web Client ein Passthrough-PCI-Gerät konfigurieren.

Vermeiden Sie bei Verwendung von Passthrough-Geräten mit einem Linux-Kernel der Version 2.6.20 oder früher den MSI- und MSI-X-Modus, da sich diese negativ auf die Leistung auswirken.

Voraussetzungen

Stellen Sie sicher, dass ein Passthrough-Netzwerkgerät auf dem Host der virtuellen Maschine konfiguriert ist. Siehe [Aktivieren des Passthroughs für ein Netzwerkgerät auf einem Host](#).

Verfahren

- 1 Ermitteln Sie die virtuelle Maschine im vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus der Liste aus.
- 2 Schalten Sie die virtuelle Maschine aus.
- 3 Wählen Sie auf der Registerkarte **Verwalten** der virtuellen Maschine **Einstellungen > VM-Hardware** aus.
- 4 Klicken Sie auf **Bearbeiten** und klicken Sie dann auf die Registerkarte **Virtuelle Hardware**.
- 5 Erweitern Sie den Abschnitt **Arbeitsspeicher**, und legen Sie **Grenzwert** auf **Unbegrenzt** fest.

- 6 Wählen Sie im Dropdown-Menü **Neues Gerät** die Option **PCI-Gerät** aus und klicken Sie auf **Hinzufügen**.
- 7 Wählen Sie im Dropdown-Menü **Neues PCI-Gerät** das Passthrough-Gerät aus, das Sie verwenden möchten, und klicken Sie auf **OK**.
- 8 Schalten Sie die virtuelle Maschine ein.

Ergebnisse

Wird einer virtuellen Maschine ein DirectPath I/O-Gerät hinzugefügt, wird als Größe der Arbeitsspeicherreservierung die Arbeitsspeichergröße der virtuellen Maschine festgelegt.

Aktivieren von DirectPath I/O mit vMotion auf einer virtuellen Maschine

Sie können DirectPath I/O mit vMotion für virtuelle Maschinen in einem Datacenter auf einem Cisco UCS-System aktivieren, das über mindestens einen unterstützten Cisco UCS Virtual Machine Fabric Extender (VM-FEX) Distributed Switch verfügt.

Voraussetzungen

Aktivieren Sie Hochleistungsnetzwerk-E/A in mindestens einem Cisco UCS-Portprofil auf einem unterstützten Cisco VM-FEX Distributed Switch. Informationen zu unterstützten Switches und zur Switch-Konfiguration finden Sie in der Dokumentation auf der Cisco-Website <http://www.cisco.com/go/unifiedcomputing/b-series-doc>.

Verfahren

- 1 Ermitteln Sie die virtuelle Maschine im vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus der Liste aus.
- 2 Schalten Sie die virtuelle Maschine aus.
- 3 Wählen Sie auf der Registerkarte **Verwalten** der virtuellen Maschine **Einstellungen > VM-Hardware** aus.
- 4 Klicken Sie auf **Bearbeiten** und klicken Sie dann auf die Registerkarte **Virtuelle Hardware**.
- 5 Erweitern Sie den Abschnitt **Arbeitsspeicher**, und legen Sie **Grenzwert** auf **Unbegrenzt** fest.
- 6 Erweitern Sie den Abschnitt **Netzwerkadapter**, um ein Passthrough-Gerät zu konfigurieren.
- 7 Klicken Sie neben DirectPath I/O auf **Aktivieren**.
- 8 Wählen Sie im Dropdown-Menü „Netzwerk“ ein Portprofil aus, bei dem Hochleistung aktiviert ist, und klicken Sie auf **OK**.
- 9 Schalten Sie die virtuelle Maschine ein.

Single Root I/O Virtualization (SR-IOV)

vSphere 5.1 und höhere Releases unterstützen „Single Root I/O Virtualization“ (SR-IOV). Sie können SR-IOV für Netzwerke von virtuellen Maschinen verwenden, die latenzsensitiv sind oder weitere CPU-Ressourcen erfordern.

Überblick über SR-IOV

SR-IOV ist eine Spezifikation, wodurch ein einzelnes PCIe-Gerät (PCIe, Peripheral Component Interconnect Express) unter dem Root-Port dem Hypervisor oder dem Gastbetriebssystem als mehrere separate physische Geräte angezeigt wird.

SR-IOV verwendet physische Funktionen (PFs) und virtuelle Funktionen (VFs), um globale Funktionen für die SR-IOV-Geräte zu verwalten. PFs sind vollständige PCIe-Funktionen, die in der Lage sind, die SR-IOV-Funktion zu konfigurieren und zu verwalten. Es ist möglich, PCIe-Geräte unter Verwendung von PFs zu konfigurieren bzw. zu steuern, und die PF hat die Fähigkeit, Daten auf das und von dem Gerät zu verschieben. VFs sind leichtgewichtige PCIe-Funktionen, die Datenflüsse unterstützen, aber über einen eingeschränkten Satz Konfigurationsressourcen verfügen.

Die Anzahl der virtuellen Funktionen, die dem Hypervisor oder dem Gastbetriebssystem bereitgestellt werden, hängt vom Gerät ab. SR-IOV-aktivierte PCIe-Geräte erfordern entsprechende BIOS- und Hardwareunterstützung sowie SR-IOV-Unterstützung auf dem Treiber des Gastbetriebssystems oder der Hypervisor-Instanz. Weitere Informationen hierzu finden Sie unter [SR-IOV-Unterstützung](#).

Verwenden von SR-IOV in vSphere

In vSphere kann eine virtuelle Maschine eine virtuelle SR-IOV-Funktion für Netzwerkfunktionen verwenden. Die virtuelle Maschine und der physische Adapter tauschen Daten direkt aus, ohne den VMkernel als Zwischenkomponente zu nutzen. Durch die Umgehung des VMkernel für Netzwerkfunktionen wird die Latenz reduziert und die CPU-Effizienz verbessert.

In vSphere 5.5 und höher verarbeitet zwar kein virtueller Switch (Standard-Switch oder Distributed Switch) den Netzwerkverkehr einer SR-IOV-aktivierten virtuellen Maschine, die mit dem Switch verbunden ist; Sie können aber die zugewiesenen virtuellen Funktionen steuern, indem Sie die Switch-Konfigurationsrichtlinien auf Portgruppen- oder Portebene nutzen.

SR-IOV-Unterstützung

vSphere 5.1 und höher unterstützt SR-IOV nur in einer Umgebung mit einer bestimmten Konfiguration. Einige Funktionen von vSphere sind nicht nutzbar, wenn SR-IOV aktiviert ist.

Unterstützte Konfigurationen

Um SR-IOV in vSphere 6.0 zu verwenden, muss Ihre Umgebung verschiedene Konfigurationsanforderungen erfüllen:

Tabelle 10-1. Unterstützte Konfigurationen für die Verwendung von SR-IOV

Komponente	Anforderungen
vSphere	<ul style="list-style-type: none"> ■ Für Hosts mit Intel-Prozessoren ist ESXi 5.1 oder höher erforderlich. ■ Hosts mit AMD-Prozessoren werden von SR-IOV in ESXi 5.5 oder höher unterstützt.
Physischer Host	<ul style="list-style-type: none"> ■ Muss mit der ESXi-Version kompatibel sein. ■ Muss über einen Intel-Prozessor verfügen, wenn Sie ESXi 5.1 ausführen, bzw. über einen Intel- oder AMD-Prozessor verfügen, wenn Sie ESXi 5.5 oder höher ausführen. ■ Muss IOMMU (I/O Memory Management Unit) unterstützen, und IOMMU muss im BIOS aktiviert sein. ■ Muss SR-IOV unterstützen und SR-IOV muss im BIOS aktiviert sein. Fragen Sie Ihren Serveranbieter, ob der Host SR-IOV unterstützt.
Physische Netzwerkkarte	<ul style="list-style-type: none"> ■ Muss mit der ESXi-Version kompatibel sein. ■ Muss von dem Host und SR-IOV gemäß der technischen Dokumentation des Serveranbieters unterstützt werden. ■ SR-IOV muss in der Firmware aktiviert sein. ■ Muss MSI-X-Interrupts verwenden.
PF-Treiber in ESXi für die physische Netzwerkkarte	<ul style="list-style-type: none"> ■ Muss von VMware zertifiziert sein. ■ Muss auf dem ESXi-Host installiert sein. Die ESXi-Version stellt für bestimmte Netzwerkkarten einen Standardtreiber zur Verfügung. Für andere Netzwerkkarten müssen Sie den Treiber herunterladen und manuell installieren.
Gastbetriebssystem	Muss von der Netzwerkkarte der installierten ESXi-Version gemäß der technischen Dokumentation des Netzwerkkartenanbieters unterstützt werden.
VF-Treiber im Gastbetriebssystem	<ul style="list-style-type: none"> ■ Muss mit der Netzwerkkarte kompatibel sein. ■ Muss von der Version des Gastbetriebssystems gemäß der technischen Dokumentation des Netzwerkkartenanbieters unterstützt werden. ■ Muss für virtuelle Windows-Maschinen von Microsoft WLK- oder WHCK-zertifiziert sein. ■ Muss auf dem Betriebssystem installiert sein. Die Betriebssystemversion enthält einen Standardtreiber für bestimmte Netzwerkkarten. Für andere Netzwerkkarten müssen Sie den Treiber von einem vom Netzwerkkarten- bzw. Hostanbieter angegebenen Speicherort herunterladen und manuell installieren.

Informationen über das Verifizieren der Kompatibilität der physischen Hosts und Netzwerkkarten mit ESXi-Versionen finden Sie im *VMware-Kompatibilitätshandbuch*.

Verfügbarkeit von Funktionen

Die folgenden Funktionen sind nicht für virtuelle Maschinen verfügbar, die mit SR-IOV konfiguriert sind:

- vSphere vMotion
- Storage vMotion
- vShield
- NetFlow
- Virtuelle VXLAN-Leitung
- vSphere High Availability
- vSphere Fault Tolerance
- vSphere DRS
- vSphere DPM
- Anhalten und Fortsetzen einer virtuellen Maschine
- Snapshots einer virtuellen Maschine
- MAC-basiertes VLAN für virtuelle Passthrough-Funktionen
- Hinzufügen und Entfernen von virtuellen Geräten, Arbeitsspeicher und vCPU im laufenden Betrieb
- Beitritt einer Clusterumgebung
- Netzwerkstatistiken für eine VM-Netzwerkkarte mit SR-IOV-Passthrough

Hinweis Versuche, mit SR-IOV im vSphere Web Client nicht unterstützte Funktionen zu aktivieren oder zu konfigurieren, führen zu einem unerwarteten Verhalten in Ihrer Umgebung.

Unterstützte Netzwerkkarten

Alle Netzwerkkarten müssen über Treiber und Firmware verfügen, die SR-IOV unterstützen. Einige Netzwerkkarten benötigen möglicherweise die Aktivierung von SR-IOV in der Firmware. Informationen dazu, welche Netzwerkkarten für die mit SR-IOV konfigurierten virtuellen Maschinen unterstützt werden, finden Sie im [VMware-Kompatibilitätshandbuch](#).

Upgrade von vSphere 5.0 und früher

Wenn Sie ein Upgrade von vSphere 5.0 oder früher auf vSphere 5.5 oder höher durchführen, ist die SR-IOV-Unterstützung erst dann verfügbar, wenn Sie die Netzwerkkartentreiber für die vSphere-Version aktualisiert haben. Firmware und Treiber, die SR-IOV unterstützen, müssen auf der Netzwerkkarte aktiviert werden, damit die SR-IOV-Funktionalität eingesetzt werden kann.

Upgrade von vSphere 5.1

Zwar wird SR-IOV auf ESXi 5.1-Hosts, die die Anforderungen erfüllen, unterstützt, Sie können SR-IOV darauf aber nicht über den vSphere Web Client konfigurieren. Verwenden Sie den Parameter `max_vfs` des Netzwerkkarten-Treibermoduls, um SR-IOV auf diesen Hosts zu aktivieren. Weitere Informationen hierzu finden Sie unter [Aktivieren von SR-IOV mit Hostprofilen oder mit einem ESXCLI-Befehl](#).

Außerdem können Sie einer virtuellen Maschine auf einem solchen Host keinen SR-IOV-Passthrough-Adapter zuweisen. Der Adapter ist für virtuelle Maschinen, die mit ESXi 5.5 und höher kompatibel sind, verfügbar. Auch wenn eine vCenter Server 5.5-Version möglicherweise einen ESXi 5.1-Host verwaltet, ist die Konfiguration identisch mit der Konfiguration in Version 5.1. Sie müssen ein PCI-Gerät zur Hardware der virtuellen Maschine hinzufügen und manuell eine VF für das Gerät auswählen.

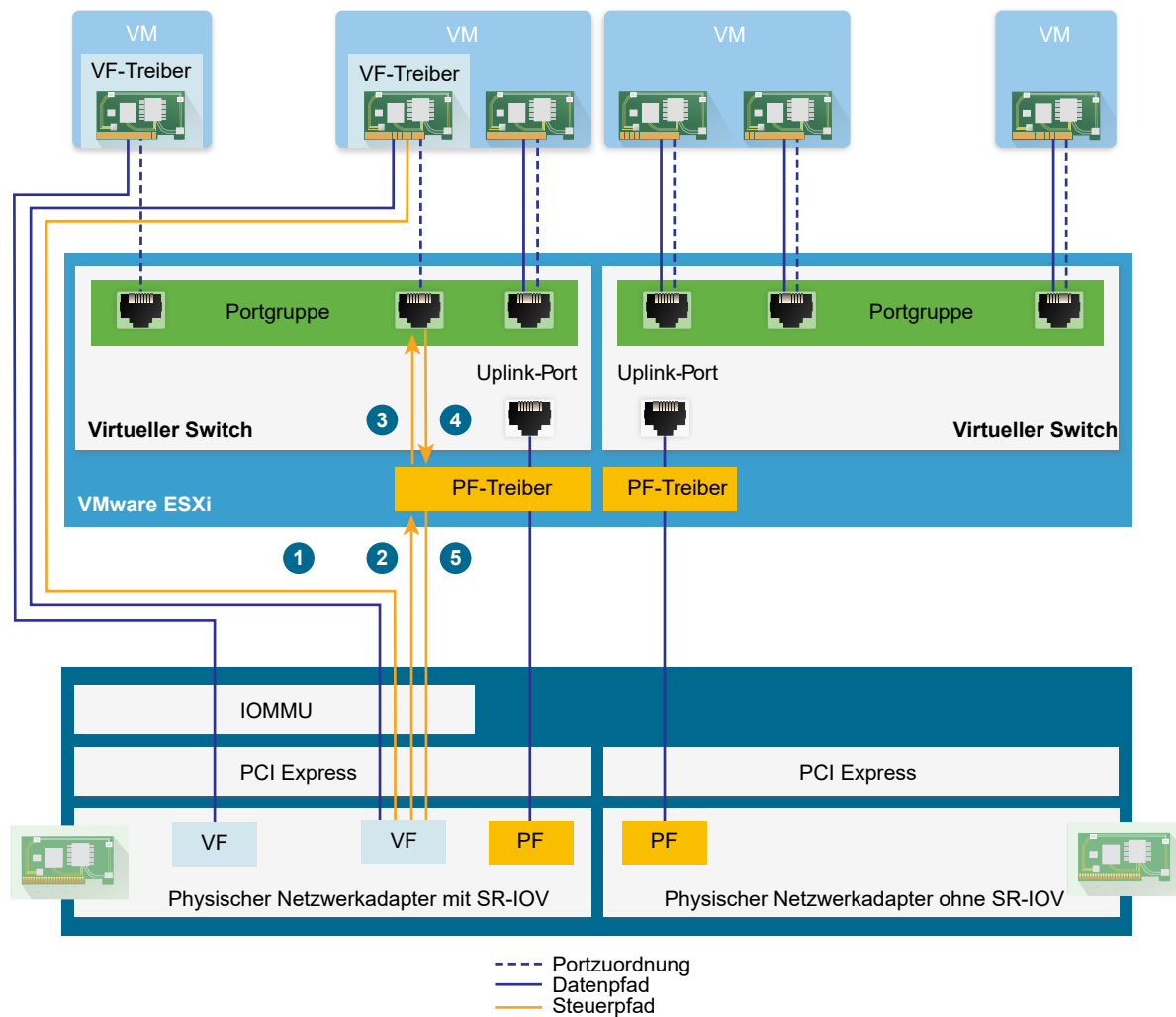
SR-IOV-Komponentenarchitektur und -Interaktion

Die vSphere SR-IOV-Unterstützung basiert auf der Interaktion zwischen den virtuellen Funktionen (VFs) und der physischen Funktion (PF) des Netzwerkkartenports für bessere Leistung und Interaktion zwischen dem Treiber der PF und dem Host-Switch für die Steuerung des Datenverkehrs.

In einem Host, der VM-Datenverkehr auf physischen SR-IOV-Adaptoren ausführt, nehmen VM-Adapter direkte Verbindung mit den virtuellen Funktionen auf, um Daten auszutauschen. Die Möglichkeit zur Konfiguration von Netzwerken basiert jedoch auf den aktiven Richtlinien für den Port, der die virtuellen Maschinen bereithält.

Auf einem ESXi-Host ohne SR-IOV sendet der virtuelle Switch externen Netzwerkverkehr über seine Ports auf dem Host vom oder zum physischen Adapter für die entsprechende Portgruppe. Der virtuelle Switch wendet die Netzwerkrichtlinien auch auf verwaltete Pakete an.

Abbildung 10-1. Daten- und Konfigurationspfade in der SR-IOV-Unterstützung von vSphere



Datenpfad in SR-IOV

Nachdem der Netzwerkadapter der virtuellen Maschine einer virtuellen Funktion zugewiesen wurde, verwendet der VF-Treiber im Gastbetriebssystem die IOMMU-Technologie (I/O Memory Management Unit) für den Zugriff auf die virtuelle Funktion, die die Daten über das Netzwerk senden oder empfangen muss. Der VMkernel, also speziell der virtuelle Switch, verarbeitet den Datenfluss nicht, was zu einer Reduzierung der Gesamtlatenz von SR-IOV-fähigen Arbeitslasten führt.

Konfigurationspfad in SR-IOV

Falls das Gastbetriebssystem versucht, die Konfiguration eines VM-Adapters zu ändern, der einer VF zugewiesen ist, wird die Änderung vorgenommen, wenn die Richtlinie auf dem Port, der mit dem VM-Adapter verknüpft ist, dies erlaubt.

Der Konfigurationsablauf besteht aus folgenden Vorgängen:

- 1 Das Gastbetriebssystem fordert eine Konfigurationsänderung für die VF an.

- 2 Die VF leitet die Anforderung über einen Mailbox-Mechanismus an die PF weiter.
- 3 Der PF-Treiber prüft die Konfigurationsanforderung mit dem virtuellen Switch (Standard-Switch oder Host-Proxy-Switch eines Distributed Switch).
- 4 Der virtuelle Switch prüft die Konfigurationsanforderung anhand der Richtlinie auf dem Port, mit dem der VF-fähige VM-Adapter verknüpft ist.
- 5 Der PF-Treiber konfiguriert die VF, wenn die neuen Einstellungen mit der Port-Richtlinie des VM-Adapters übereinstimmen.

Wenn beispielsweise der VF-Treiber versucht, die MAC-Adresse zu ändern, bleibt die Adresse gleich, falls die Änderung der MAC-Adresse in der Sicherheitsrichtlinie für die Portgruppe oder den Port nicht erlaubt ist. Das Gastbetriebssystem zeigt möglicherweise an, dass die Änderung erfolgreich war, aber eine Protokollmeldung gibt an, dass der Vorgang fehlgeschlagen ist. In der Folge speichern das Gastbetriebssystem und das virtuelle Gerät unterschiedliche MAC-Adressen ab. Die Netzwerkschnittstelle im Gastbetriebssystem ist dann möglicherweise nicht in der Lage, eine IP-Adresse abzurufen und zu kommunizieren. In diesem Fall müssen Sie die Schnittstelle im Gastbetriebssystem zurücksetzen, um die neueste MAC-Adresse vom virtuellen Gerät und dann eine IP-Adresse abzurufen.

Interaktion von vSphere und virtueller Funktion

Virtuelle Funktionen (VFs) sind leichtgewichtige PCIe-Funktionen, die alle für den Datenaustausch erforderlichen Ressourcen enthalten, aber über einen minimierten Satz an Konfigurationsressourcen verfügen. Die Interaktion zwischen vSphere und VFs ist beschränkt.

- Die physische Netzwerkkarte muss MSI-X-Interrupts verwenden.
- VFs implementieren die Steuerung der Übertragungsrate nicht in vSphere. Jede VF kann theoretisch die gesamte Bandbreite einer physischen Verbindung nutzen.
- Wenn ein VF-Gerät als Passthrough-Gerät in einer virtuellen Maschine konfiguriert ist, werden die Standby- und Ruhemodus-Funktionen für die virtuelle Maschine nicht unterstützt.
- Die maximale Anzahl der VFs, die Sie erstellen können, und die maximale Anzahl der VFs, die Sie für Passthrough verwenden können, sind unterschiedlich. Wie viele virtuelle Funktionen Sie maximal instanziierten können, hängt von der Kapazität der Netzwerkkarte und von der Hardwarekonfiguration des Hosts ab. Dennoch kann aufgrund der begrenzten Anzahl von für Passthrough-Geräte verfügbaren Interrupt-Vektoren nur eine begrenzte Anzahl aller instanziierten VFs auf einem ESXi-Host verwendet werden.

Die Gesamtanzahl von Interrupt-Vektoren auf jedem ESXi-Host kann bei 32 CPUs auf bis zu 4096 ansteigen. Wird der Host gestartet, verbrauchen Geräte auf dem Host (z. B. Speichercontroller, physische Netzwerkkarten und USB-Controller) einen Teil der 4096 Vektoren. Wenn diese Geräte mehr als 1024 Vektoren benötigen, wird die maximale Anzahl der potenziell unterstützten VFs reduziert.

- Für eine Intel-Netzwerkkarte und eine Emulex-Netzwerkkarte wird möglicherweise eine unterschiedliche Anzahl von VFs unterstützt. Weitere Informationen finden Sie in der technischen Dokumentation des Netzwerkkartenanbieters.

- Wenn Intel- und Emulex-Netzwerkkarten mit aktivierten SR-IOV vorhanden sind, hängt die Anzahl verfügbarer virtueller Funktionen für die Intel-Netzwerkkarten davon ab, wie viele virtuelle Funktionen für die Emulex-Netzwerkkarte konfiguriert sind, und umgekehrt. Mit der folgenden Formel können Sie die maximale Anzahl zum Gebrauch verfügbarer virtueller Funktionen einschätzen, wenn alle 3072 Interrupt-Vektoren für Passthrough verfügbar sind:

$$3X + 2Y < 3072$$

Dabei gilt: X ist die Anzahl der Intel-VFs und Y ist die Anzahl der Emulex-VFs.

Diese Zahl kann kleiner ausfallen, wenn andere Arten von Geräten auf dem Host mehr als 1024 Interrupt-Vektoren von den insgesamt 4096 Vektoren des Hosts verwenden.

- vSphere SR-IOV unterstützt bis zu 1024 VFs auf unterstützten Intel- und Emulex-Netzwerkkarten.
- vSphere SR-IOV unterstützt bis zu 64 VFs auf einer unterstützten Intel- oder Emulex-Netzwerkkarte.
- Wenn eine unterstützte Intel-Netzwerkkarte keine Verbindung mehr hat, stellen alle VFs von dieser physischen Netzwerkkarte die Kommunikation vollständig ein, auch zwischen den VFs.
- Wenn eine unterstützte Emulex-Netzwerkkarte keine Verbindung mehr hat, stellen alle VFs die Kommunikation mit der externen Umgebung ein, die Kommunikation zwischen den VFs bleibt aber aufrecht.
- VF-Treiber bieten verschiedene Leistungsmerkmale, beispielsweise IPv6-Unterstützung, TSO und LRO-Prüfsumme. Weitere Informationen finden Sie in der technischen Dokumentation des Netzwerkkartenanbieters.

DirectPath I/O im Vergleich zu SR-IOV

SR-IOV bietet Leistungsvorteile und Gestaltungsmöglichkeiten ähnlich wie DirectPath I/O. DirectPath I/O und SR-IOV haben ähnliche Funktionen, aber Sie verwenden sie für unterschiedliche Zwecke.

SR-IOV ist bei Arbeitslasten mit sehr hohem Paketdurchsatz oder bei Anforderungen mit sehr kurzen Latenzzeiten sinnvoll. Wie DirectPath I/O ist SR-IOV mit bestimmten Kernvirtualisierungsfunktionen wie vMotion nicht kompatibel. SR-IOV ermöglicht allerdings die gemeinsame Nutzung eines physischen Geräts durch mehrere Gäste.

Mit DirectPath I/O können Sie jeweils nur eine physische Funktion einer virtuellen Maschine zuweisen. Mit SR-IOV können Sie ein einzelnes physisches Gerät gemeinsam nutzen, sodass sich mehrere virtuelle Maschinen direkt mit der physischen Funktion verbinden können.

Konfigurieren einer virtuellen Maschine zur Verwendung von SR-IOV

Um die Funktionen von SR-IOV nutzen zu können, müssen Sie die virtuellen SR-IOV-Funktionen auf dem Host aktivieren und eine virtuelle Maschine mit den Funktionen verknüpfen.

Voraussetzungen

Stellen Sie sicher, dass die Konfiguration Ihrer Umgebung SR-IOV unterstützt. Informationen hierzu finden Sie unter [SR-IOV-Unterstützung](#).

Verfahren

1 Aktivieren von SR-IOV auf einem physischen Hostadapter

Bevor Sie virtuelle Maschinen mit virtuellen Funktionen verbinden können, verwenden Sie den vSphere Web Client, um SR-IOV zu aktivieren und die Anzahl der virtuellen Funktionen auf Ihrem Host festzulegen.

2 Zuweisen einer virtuellen Funktion als SR-IOV-Passthrough-Adapter zu einer virtuellen Maschine

Um sicherzustellen, dass eine virtuelle Maschine und eine physische Netzwerkkarte Daten austauschen können, müssen Sie die virtuelle Maschine mit einer oder mehreren virtuellen Funktionen als SR-IOV-Passthrough-Netzwerkadapter verknüpfen.

Ergebnisse

Der Datenverkehr verläuft von einem SR-IOV-Passthrough-Adapter zum physischen Adapter in Übereinstimmung mit der aktiven Richtlinie auf dem verknüpften Port auf dem Standard- oder Distributed Switch.

Um zu ermitteln, welche virtuelle Funktion einem SR-IOV-Passthrough-Adapter zugewiesen ist, erweitern Sie auf der Registerkarte **Übersicht** für die virtuelle Maschine den Bereich **VM-Hardware**, und überprüfen Sie die Eigenschaften des Adapters.

Das Topologie-Diagramm des Switches markiert VM-Adapter, die virtuelle Funktionen verwenden, mit dem Symbol .

Nächste Schritte

Richten Sie den Datenverkehr ein, der die mit der virtuellen Maschine verbundenen virtuellen Funktionen passiert, indem Sie die Netzwerkkontrolllinien auf dem Switch, der Portgruppe und dem Port verwenden. Weitere Informationen hierzu finden Sie unter [Netzwerkoptionen für den Datenverkehr einer SR-IOV-fähigen virtuellen Maschine](#).

Aktivieren von SR-IOV auf einem physischen Hostadapter

Bevor Sie virtuelle Maschinen mit virtuellen Funktionen verbinden können, verwenden Sie den vSphere Web Client, um SR-IOV zu aktivieren und die Anzahl der virtuellen Funktionen auf Ihrem Host festzulegen.

Verfahren

1 Navigieren Sie im vSphere Web Client zum Host.

- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Physische Adapter** aus.

Sie können sich die SR-IOV-Eigenschaft anzeigen lassen, um zu sehen, ob ein physischer Adapter SR-IOV unterstützt.

- 3 Wählen Sie den physischen Adapter aus und klicken Sie auf **Adapter-Einstellungen bearbeiten**.
- 4 Wählen Sie unter SR-IOV aus dem Dropdown-Menü **Status** die Option **Aktiviert** aus.
- 5 Geben Sie im Textfeld **Anzahl der virtuellen Funktionen** die Anzahl der virtuellen Funktionen ein, die Sie für den Adapter konfigurieren möchten.
- 6 Klicken Sie auf **OK**.
- 7 Starten Sie den Host neu.

Ergebnisse

Die virtuellen Funktionen werden auf dem Netzwerkkartenport aktiv, der vom Eintrag des physischen Adapters dargestellt wird. Sie werden in der PCI-Geräteliste auf der Registerkarte **Einstellungen** für den Host angezeigt.

Sie können die vCLI-Befehle `esxcli network sriovnic` verwenden, um die Konfiguration von virtuellen Funktionen auf dem Host zu untersuchen.

Nächste Schritte

Weisen Sie eine virtuelle Maschine über einen SR-IOV-Passthrough-Netzwerkadapter einer virtuellen Funktion zu.

Zuweisen einer virtuellen Funktion als SR-IOV-Passthrough-Adapter zu einer virtuellen Maschine

Um sicherzustellen, dass eine virtuelle Maschine und eine physische Netzwerkkarte Daten austauschen können, müssen Sie die virtuelle Maschine mit einer oder mehreren virtuellen Funktionen als SR-IOV-Passthrough-Netzwerkadapter verknüpfen.

Voraussetzungen

- Stellen Sie sicher, dass die virtuellen Funktionen auf dem Host vorhanden sind.
- Stellen Sie sicher, dass die Passthrough-Netzwerkgeräte für die virtuellen Funktionen in der Liste der PCI-Geräte auf der Registerkarte **Einstellungen** für den Host aktiv sind.
- Stellen Sie sicher, dass die virtuelle Maschine mit ESXi 5.5 und höher kompatibel ist.
- Stellen Sie sicher, dass bei der Erstellung der virtuellen Maschine Red Hat Enterprise Linux 6 oder höher bzw. Windows als Gastbetriebssystem ausgewählt wurde.

Verfahren

- 1 Ermitteln Sie die virtuelle Maschine im vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus der Liste aus.
- 2 Schalten Sie die virtuelle Maschine aus.
- 3 Wählen Sie auf der Registerkarte **Verwalten** der virtuellen Maschine **Einstellungen > VM-Hardware** aus.
- 4 Klicken Sie auf **Bearbeiten** und klicken Sie dann auf die Registerkarte **Virtuelle Hardware**.
- 5 Wählen Sie im Dropdown-Menü **Neues Gerät** die Option **Netzwerk** und klicken Sie auf **Hinzufügen**.
- 6 Erweitern Sie den Bereich „Neues Netzwerk“ und verbinden Sie die virtuelle Maschine mit einer Portgruppe.

Die virtuelle Netzwerkkarte verwendet diese Portgruppe nicht für den Datenverkehr. Die Portgruppe dient zum Extrahieren der Netzwerkeigenschaften, die auf den Datenverkehr angewendet werden sollen, wie beispielsweise das VLAN-Tagging.
- 7 Wählen Sie im Dropdown-Menü **Adaptertyp** die Option **SR-IOV-Passthrough**.
- 8 Wählen Sie im Dropdown-Menü **Physische Funktion** den physischen Adapter zur Unterstützung des Passthrough-Adapters der virtuellen Maschine.
- 9 Wenn Sie Änderungen am MTU-Wert für Pakete vom Gastbetriebssystem zulassen möchten, verwenden Sie das Dropdown-Menü **MTU-Änderung auf Gastbetriebssystem**.
- 10 Erweitern Sie den Bereich „Arbeitsspeicher“, wählen Sie **Gesamten Gastarbeitsspeicher reservieren (Alle gesperrt)** und klicken Sie auf **OK**.

IOMMU muss den gesamten Arbeitsspeicher der virtuellen Maschine erreichen, damit das Passthrough-Gerät mithilfe von DMA auf den Arbeitsspeicher zugreifen kann.
- 11 Schalten Sie die virtuelle Maschine ein.

Ergebnisse

Beim Einschalten der virtuellen Maschine wählt der ESXi-Host eine freie virtuelle Funktion vom physischen Adapter aus und ordnet sie dem SR-IOV-Passthrough-Adapter zu. Der Host überprüft alle Eigenschaften des Adapters der virtuellen Maschine und der zugrunde liegenden virtuellen Funktion anhand der Einstellungen der Portgruppe, zu der die virtuelle Maschine gehört.

Netzwerkoptionen für den Datenverkehr einer SR-IOV-fähigen virtuellen Maschine

In vSphere 5.5 und höher können Sie bestimmte Netzwerkfunktionen auf dem Adapter einer virtuellen Maschine konfigurieren, dem eine virtuelle Funktion (VF) zugewiesen ist. Verwenden Sie Einstellungen für den Switch, für die Portgruppe oder für einen Port, je nachdem, welchen Typ der virtuelle Switch hat, der den Datenverkehr verarbeitet (Standard-Switch oder Distributed Switch).

Tabelle 10-2. Netzwerkoptionen für den Adapter einer virtuellen Maschine, der eine VF verwendet

Netzwerkoption	Beschreibung
MTU-Größe	Ändern Sie die MTU-Größe, beispielsweise zum Aktivieren von Jumbo-Frames.
Sicherheitsrichtlinie für VF-Datenverkehr	<ul style="list-style-type: none"> ■ Wenn das Gastbetriebssystem die anfänglich festgelegte MAC-Adresse eines Netzwerkkadapters einer virtuellen Maschine ändert, der eine VF verwendet, legen Sie die Option MAC-Adressänderungen fest, um an die neue Adresse eingehende Frames zu verwerfen oder anzunehmen. ■ Aktivieren Sie den globalen Promiscuous-Modus für die Netzwerkkadapters von virtuellen Maschinen, auch für Adapter, die virtuelle Funktionen (VFs) verwenden.
VLAN-Tagging-Modus	Konfigurieren Sie das VLAN-Tagging für den Standard-Switch oder den Distributed Switch. Aktivieren Sie dazu VLAN Switch Tagging (VST) oder legen Sie fest, dass der gekennzeichnete Datenverkehr die virtuellen Maschinen erreicht, denen VFs zugeordnet sind, das heißt, aktivieren Sie Virtual Guest Tagging (VGT).

Bewältigen des Datenverkehrs von virtuellen Maschinen mit einem SR-IOV-fähigen physischen Adapter


In vSphere 5.5 und höher können die physischen Funktionen (PFs) und die virtuellen Funktionen (VFs) eines SR-IOV-fähigen physischen Adapters für die Bewältigung des Datenverkehrs von virtuellen Maschinen konfiguriert werden.

Die PF eines SR-IOV-fähigen physischen Adapters steuert die von virtuellen Maschinen verwendeten VFs und können den Datenverkehr bewältigen, der über den Standard-Switch oder Distributed Switch übertragen wird, der für die Netzwerkfunktionen dieser SR-IOV-fähigen virtuellen Maschinen verwendet wird.

Der SR-IOV-fähige physische Adapter arbeitet in verschiedenen Modi, je nachdem, ob der Datenverkehr auf dem Switch unterstützt wird.


Gemischter Modus

Der physische Adapter bietet virtuelle Funktionen für virtuelle Maschinen, die an den Switch angeschlossen sind, und verarbeitet den Datenverkehr von nicht SR-IOV-fähigen virtuellen Maschinen direkt auf dem Switch.

Anhand des Topologie-Diagramms des Switches können Sie überprüfen, ob der gemischte Modus für einen SR-IOV-fähigen physischen Adapter aktiviert ist. Für einen SR-IOV-fähigen physischen Adapter im gemischten Modus wird das Symbol  in der Liste der physischen Adapter für einen Standard-Switch oder in der Liste der Uplink-Gruppenadapter für einen Distributed Switch angezeigt.

Reiner SR-IOV-Modus

Der physische Adapter bietet virtuelle Funktionen für virtuelle Maschinen, die an einen virtuellen Switch angeschlossen sind, unterstützt aber keinen Datenverkehr von nicht SR-IOV-fähigen virtuellen Maschinen auf dem Switch.

Anhand des Topologie-Diagramms des Switches können Sie überprüfen, ob der reine SR-IOV-Modus für den physischen Adapter aktiviert ist. In diesem Modus befindet sich der physische Adapter in einer separaten Liste mit der Bezeichnung „Externe SR-IOV-Adapter“. Angezeigt wird dabei das Symbol .

Nicht-SR-IOV-Modus

Der physische Adapter wird nicht für Datenverkehr im Zusammenhang mit VF-fähigen virtuellen Maschinen verwendet. Nur Datenverkehr von anderen als SR-IOV-fähigen virtuellen Maschinen wird verwaltet.

Aktivieren von SR-IOV mit Hostprofilen oder mit einem ESXCLI-Befehl

Die virtuellen Funktionen auf einem ESXi-Host können Sie mit einem ESXCLI-Befehl oder mit einem Hostprofil konfigurieren, um mehrere Hosts gleichzeitig oder um statusfreie Hosts einzurichten.

Aktivieren von SR-IOV in einem Hostprofil

Für mehrere Hosts oder einen statusfreien Host können Sie die virtuellen Funktionen der physischen Netzwerkkarte unter Verwendung eines Hostprofils konfigurieren und das Profil mit Auto Deploy auf einen Host anwenden.

Informationen zum Ausführen von ESXi durch Verwenden von Auto Deploy bei Hostprofilen finden Sie in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere*.

Sie können auch virtuelle SR-IOV-Funktionen auf dem Host aktivieren, indem Sie entsprechend der Treiberdokumentation den vCLI-Befehl `esxcli system module parameters set` im Netzwerkkarten-Treiberparameter für virtuelle Funktionen verwenden. Weitere Informationen zur Verwendung von vCLI-Befehlen finden Sie unter *Dokumentation zur vSphere-Befehlszeilenschnittstelle*.

Voraussetzungen

- Stellen Sie sicher, dass die Konfiguration Ihrer Umgebung SR-IOV unterstützt. Informationen hierzu finden Sie unter [SR-IOV-Unterstützung](#).

- Erstellen Sie ein Hostprofil auf Basis des SR-IOV-fähigen Hosts. Weitere Informationen finden Sie in der Dokumentation *vSphere-Hostprofile*.

Verfahren

- 1 Klicken Sie auf der Startseite vom vSphere Web Client auf **Regeln und Profile > Hostprofile**.
- 2 Wählen Sie das Hostprofil aus der Liste aus und klicken Sie auf die Registerkarte **Verwalten**.
- 3 Klicken Sie auf **Hostprofil bearbeiten** und erweitern Sie den Knoten **Allgemeine Systemeinstellungen**.

- 4 Erweitern Sie den **Kernelmodulparameter** und wählen Sie den Parameter des physischen Funktionstreibers zum Erstellen virtueller Funktionen aus.

Beispielsweise lautet der Parameter des physischen Funktionstreibers einer physischen Intel-Netzwerkkarte `max_vfs`.

- 5 Geben Sie im Textfeld **Wert** eine kommagetrennte Liste mit gültigen Anzahlwerten für virtuelle Funktionen ein.

Jeder Listeneintrag gibt die Anzahl der virtuellen Funktionen an, die Sie für jede physische Funktion konfigurieren möchten. Der Wert 0 bedeutet, dass SR-IOV für diese physische Funktion nicht aktiviert wird.

Wenn Sie beispielsweise einen Dual-Port haben, setzen Sie den Wert auf `x,y`, wobei `x` oder `y` die Anzahl der virtuellen Funktionen ist, die Sie für einen einzelnen Port aktivieren möchten.

Wenn die Zielanzahl virtueller Funktionen auf einem einzelnen Host 30 ist, verfügen Sie möglicherweise über zwei Dual-Port-Karten, die auf `0,10,10,10` festgelegt sind.

Hinweis Die Anzahl an virtuellen Funktionen, die für die Konfiguration unterstützt wird und verfügbar ist, hängt von der Systemkonfiguration ab.

- 6 Klicken Sie auf **Beenden**.
- 7 Standardisieren Sie das Hostprofil nach Bedarf auf den Host.

Ergebnisse

Die virtuellen Funktionen werden in der PCI-Geräteliste auf der Registerkarte **Einstellungen** für den Host angezeigt.

Nächste Schritte

Weisen Sie eine virtuelle Funktion über den SR-IOV-Passthrough-Netzwerkadapterttyp einer virtuellen Maschine zu. Siehe [Zuweisen einer virtuellen Funktion als SR-IOV-Passthrough-Adapter zu einer virtuellen Maschine](#).

Aktivieren von SR-IOV auf einem physischen Hostadapter mithilfe eines ESXCLI-Befehls

In bestimmten Fehlerbehebungssituationen oder für die direkte Hostkonfiguration können Sie einen Konsolenbefehl auf ESXi ausführen, um virtuelle SR-IOV-Funktionen auf einem physischen Adapter zu erstellen.

Sie können virtuelle SR-IOV-Funktionen auf dem Host erstellen, indem Sie entsprechend der Treiberdokumentation den Netzwerkkarten-Treiberparameter für virtuelle Funktionen anpassen.

Voraussetzungen

Installieren Sie das vCLI-Paket, stellen Sie die virtuelle Maschine von vSphere Management Assistant (vMA) bereit oder verwenden Sie die ESXi Shell. Siehe *Erste Schritte mit vSphere Command-Line Interfaces*.

Verfahren

- 1 Um virtuelle Funktionen durch die Einstellung des Parameters für virtuelle Funktionen des Netzwerkkartentreibers zu erstellen, führen Sie auf der Befehlszeile den Befehl `esxcli system module parameters set` aus.

```
esxcli system module parameters set -m driver -p vf_param=w,x,y,z
```

Hierbei ist *driver* der Name des Netzwerkkartentreibers und *vf_param* der treiberspezifische Parameter zum Erstellen der virtuellen Funktion.

Sie können mit einer kommagetrennten Liste Werte für den Parameter *vf_param* setzen, wobei jeder Eintrag die Anzahl der virtuellen Funktionen für einen Port angibt. Der Wert 0 bedeutet, dass SR-IOV für diese physische Funktion nicht aktiviert wird.

Wenn Sie zwei Dual-Port-Netzwerkkarten haben, können Sie den Wert auf *w, x, y, z* setzen, wobei *w, x, y* und *z* die Anzahl der virtuellen Funktionen ist, die Sie für einen einzelnen Port aktivieren möchten. Um beispielsweise 30 virtuelle Funktionen zu erstellen, die auf zwei Dual-Port-Karten von Intel unter Verwendung des *ixgbe*-Treibers verteilt werden, führen Sie folgenden Befehl für den *ixgbe*-Treiber und den Parameter *max_vfs* aus:

```
esxcli system module parameters set -m ixgbe -p max_vfs=0,10,10,10
```

- 2 Starten Sie den Host neu, um die virtuellen Funktionen zu erstellen.

Nächste Schritte

Weisen Sie eine virtuelle Funktion über den SR-IOV-Passthrough-Netzwerkadaptertyp einer virtuellen Maschine zu. Weitere Informationen hierzu finden Sie unter [Zuweisen einer virtuellen Funktion als SR-IOV-Passthrough-Adapter zu einer virtuellen Maschine](#).

Eine virtuelle Maschine, die eine virtuelle SR-IOV-Funktion verwendet, kann nicht eingeschaltet werden, weil der Host den Status „Out of Interrupt Vectors“ aufweist

Auf einem ESXi-Host werden virtuelle Maschinen, die virtuelle SR-IOV-Funktionen (VFs) für Netzwerke verwenden, ausgeschaltet.

Problem

Auf einem ESXi-Host können virtuelle Maschinen, die virtuelle SR-IOV-Funktionen (VFs) für Netzwerke verwenden, nicht eingeschaltet werden, wenn die Gesamtanzahl der zugewiesenen virtuellen Funktionen sich der im Handbuch *Maximalwerte für die Konfiguration von vSphere* angegebenen, maximal zulässigen Anzahl von VFs nähert.

Die Protokolldatei `vmware.log` der virtuellen Maschine enthält eine Meldung ähnlich der Folgenden über die VF:

```
PCIPassthruChangeIntrSettings: vf_name failed to register interrupt (error code 195887110)
```

Die Protokolldatei `vmkernel.log` von VMkernel enthält Meldungen ähnlich der Folgenden über die der virtuellen Maschine zugewiesenen VF:

```
VMKPCIPassthru: 2565: BDF = vf_name intrType = 4 numVectors: 3
WARNING: IntrVector: 233: Out of interrupt vectors
```

Ursache

Die Anzahl der zuteilbaren Interrupt-Vektoren steigt mit der Anzahl der physischen CPUs auf einem ESXi-Host. Ein ESXi-Host mit 32 CPUs kann insgesamt 4096 Interrupt-Vektoren bereitstellen. Wird der Host gestartet, verbrauchen Geräte auf dem Host (z. B. Speichercontroller, physische Netzwerkadapter und USB-Controller) einen Teil der 4096-Vektoren. Wenn diese Geräte mehr als 1024 Vektoren benötigen, wird die maximale Anzahl der potenziell unterstützten VFs reduziert.

Mit dem Einschalten einer virtuellen Maschine und dem Starten des VF-Treibers des Gastbetriebssystems werden Interrupt-Vektoren verbraucht. Wenn die erforderliche Anzahl der Interrupt-Vektoren nicht verfügbar ist, wird das Gastbetriebssystem unerwartet und ohne Fehlermeldung heruntergefahren.

Derzeit ist keine Regel vorhanden, mit der die Anzahl der verbrauchten oder verfügbaren Interrupt-Vektoren auf einem Host ermittelt werden kann. Diese Anzahl hängt von der Hardwarekonfiguration des Hosts ab.

Lösung

- ◆ Um die virtuellen Maschinen einschalten zu können, verringern Sie die Gesamtanzahl der den virtuellen Maschinen auf dem Host zugewiesenen VFs.

Ändern Sie z. B. den SR-IOV-Netzwerkadapter einer virtuellen Maschine in einen Adapter, der mit einem vSphere Standard-Switch oder vSphere Distributed Switch verbunden ist.

Jumbo-Frames

Mithilfe von Jumbo-Frames können ESXi-Hosts größere Frames an das physische Netzwerk senden. Das Netzwerk muss Jumbo-Frames durchgängig unterstützen, was physische Netzwerkadapter, physische Switches und Speichergeräte einschließt.

Prüfen Sie vor der Aktivierung von Jumbo-Frames bei Ihrem Hardwareanbieter, ob Ihre physischen Netzwerkadapter Jumbo-Frames unterstützen.

Sie können Jumbo-Frames auf einem vSphere Distributed Switch oder vSphere Standard-Switch aktivieren, indem Sie die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) in einen Wert ändern, der größer als 1500 Byte ist. Die maximal konfigurierbare Frame-Größe beträgt 9000 Byte.

Aktivieren von Jumbo-Frames auf einem vSphere Distributed Switch

Aktivieren Sie Jumbo-Frames für den gesamten Datenverkehr, der über einen vSphere Distributed Switch übertragen wird.

Wichtig Wenn Sie die MTU-Größe eines vSphere Distributed Switch ändern, werden die physischen Netzwerkkarten, die als Uplinks zugewiesen sind, deaktiviert und wieder aktiviert. Dies führt zu einem kurzen Netzwerkausfall von 5 bis 10 Millisekunden für virtuelle Maschinen oder Dienste, die die Uplinks verwenden.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen** und wählen Sie **Eigenschaften** aus.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Klicken Sie auf **Erweitert** und legen Sie für die Eigenschaft **MTU** einen Wert fest, der größer als 1500 Byte ist.

9000 Byte ist der maximal zulässige Wert für die MTU-Größe.
- 5 Klicken Sie auf **OK**.

Aktivieren von Jumbo-Frames auf einem vSphere Standard-Switch

Aktivieren Sie Jumbo-Frames für den gesamten Datenverkehr über einen vSphere Standard-Switch auf einem Host.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
- 3 Wählen Sie einen Standard-Switch aus der Liste der virtuellen Switches aus und klicken Sie auf **Einstellungen bearbeiten**.
- 4 Setzen Sie im Abschnitt **Eigenschaften** die Eigenschaft **MTU** auf einen Wert größer als 1500 Byte.

Die MTU-Größe kann auf bis zu 9000 Byte vergrößert werden.

- 5 Klicken Sie auf **OK**.

Aktivieren von Jumbo-Frames für einen VMkernel-Adapter

Jumbo-Frames reduzieren die CPU-Auslastung, die durch die Übertragung von Daten verursacht wird. Aktivieren Sie Jumbo-Frames auf einem VMkernel-Adapter, indem Sie die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) des Adapters ändern.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Wählen Sie unter **Verwalten** die Option **Netzwerk** und dann **VMkernel-Adapter** aus.
- 3 Wählen Sie einen VMkernel-Adapter aus der Tabelle aus.
Die Eigenschaften des Adapters werden angezeigt.
- 4 Klicken Sie auf den Namen des VMkernel-Adapters.
- 5 Klicken Sie auf **Bearbeiten**.
- 6 Wählen Sie **NIC-Einstellungen** aus und legen Sie für die Eigenschaft **MTU** einen Wert fest, der größer als 1500 ist.

Die MTU-Größe kann auf bis zu 9000 Byte vergrößert werden.

- 7 Klicken Sie auf **OK**.

Aktivieren der Jumbo Frame-Unterstützung auf einer virtuellen Maschine

Für das Aktivieren der Jumbo-Frame-Unterstützung auf einer virtuellen Maschine ist ein erweiterter VMXNET-Adapter für diese virtuelle Maschine erforderlich.

Verfahren

- 1 Ermitteln Sie die virtuelle Maschine im vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus der Liste aus.
- 2 Wählen Sie auf der Registerkarte **Verwalten** der virtuellen Maschine **Einstellungen > VM-Hardware** aus.
- 3 Klicken Sie auf **Bearbeiten** und klicken Sie dann auf die Registerkarte **Virtuelle Hardware**.
- 4 Klicken Sie auf den Abschnitt **Virtuelle Hardware**, und erweitern Sie den Abschnitt „Netzwerkadapter“. Notieren Sie sich die Netzwerkeinstellungen und die MAC-Adresse des Netzwerkadapters.
- 5 Klicken Sie auf **Entfernen (Remove)**, um den Netzwerkadapter aus der virtuellen Maschine zu entfernen.
- 6 Wählen Sie im Dropdown-Menü **Neues Gerät** die Option **Netzwerk** aus und klicken Sie auf **Hinzufügen**.
- 7 Wählen Sie im Dropdown-Menü **Adaptertyp** die Option **VMXNET 2 (Erweitert)** oder **VMXNET 3** aus.
- 8 Legen Sie die Netzwerkeinstellungen auf die Einstellungen fest, die für den alten Netzwerkadapter aufgezeichnet wurden.
- 9 Legen Sie die **MAC-Adresse** auf **Manuell** fest, und geben Sie die MAC-Adresse ein, die für den alten Netzwerkadapter verwendet wurde.
- 10 Klicken Sie auf **OK**.

Nächste Schritte

- Stellen Sie sicher, dass der Adapter „VMXNET (erweitert)“ mit einem Standard-Switch oder Distributed Switch mit aktivierten Jumbo-Frames verbunden ist.
- Konfigurieren Sie im Gastbetriebssystem den Netzwerkadapter, so dass Jumbo Frames unterstützt werden. Informationen hierzu können Sie der Dokumentation Ihres Gastbetriebssystems entnehmen.
- Konfigurieren Sie alle physischen Switches sowie alle physischen oder virtuellen Maschinen für die Unterstützung von Jumbo Frames, mit denen diese virtuelle Maschine eine Verbindung herstellt.

TCP-Segmentierungs-Offload

Verwenden Sie TCP-Segmentierungs-Offload (TSO) in VMkernel-Netzwerkadaptern und virtuellen Maschinen, um die Netzwerkleistung in Arbeitslasten mit hohen Latenzanforderungen zu steigern.

TSO auf dem Übertragungspfad von physischen Netzwerkadaptern, VMkernel-Netzwerkadaptern und Netzwerkadaptern virtueller Maschinen steigert die Leistung von ESXi-Hosts durch das Reduzieren des Overheads der CPU für TCP/IP-Netzwerkvorgänge. Wenn TSO aktiviert ist, unterteilt der Netzwerkadapter anstelle der CPU größere Datenblöcke in TCP-Segmente. Der VMkernel und das Gastbetriebssystem können mehrere CPU-Zyklen zum Ausführen von Anwendungen verwenden.

Um die höhere Leistung, die TSO bietet, zu nutzen, aktivieren Sie TSO auf dem Datenpfad auf einem ESXi-Host, einschließlich physischer Netzwerkadapter, VMkernel und Gastbetriebssystem. Standardmäßig ist TSO im VMkernel des ESXi-Hosts und in den VMXNET 2- und VMXNET 3-VM-Adaptern aktiviert.

Informationen zur Position der TCP-Paketsegmentierung im Datenpfad finden Sie im VMware Knowledgebase-Artikel [Understanding TCP Segmentation Offload \(TSO\) and Large Receive Offload \(LRO\) in a VMware environment](#) (Funktionsweise von TCP Segmentation Offload (TSO) und Large Receive Offload (LRO) in einer VMware-Umgebung).

Aktivieren oder Deaktivieren von Software-TSO im VMkernel

Wenn ein physischer Netzwerkadapter Probleme mit TSO hat, können Sie vorübergehend die Softwaresimulation von TSO im VMkernel aktivieren, bis die Probleme behoben sind.

Verfahren

- ◆ Führen Sie die Konsolenbefehle `esxcli network nic software set` aus, um die Softwaresimulation von TSO im VMkernel zu aktivieren oder zu deaktivieren.
 - Aktivieren Sie die Softwaresimulation von TSO im VMkernel.

```
esxcli network nic software set --ipv4tso=1 -n vmnicX
esxcli network nic software set --ipv6tso=1 -n vmnicX
```

- Deaktivieren Sie die Softwaresimulation von TSO im VMkernel.

```
esxcli network nic software set --ipv4tso=0 -n vmnicX
esxcli network nic software set --ipv6tso=0 -n vmnicX
```

Wobei *X* in `vmnicX` die Nummer der Netzwerkkartenports im Host darstellt.

Die Konfigurationsänderung bleibt auch nach dem Neustart des Hosts erhalten.

Ermitteln, ob TSO auf den physischen Netzwerkadaptern eines ESXi-Hosts unterstützt wird

Untersuchen Sie, ob beim physischen Netzwerkadapter ein Offload der TCP/IP-Paketsegmentierung stattfindet, wenn Sie die Netzwerkleistung eines Hosts mit latenzempfindlichen Workloads schätzen. Wenn ein physischer Netzwerkadapter TSO unterstützt, dann ist TSO standardmäßig aktiviert.

Verfahren

- ◆ Führen Sie den Konsolenbefehl `esxcli network nic software get` aus, um zu ermitteln, ob TSO auf den physischen Netzwerkadaptern eines Hosts aktiviert ist.

```
esxcli network nic tso get
```

Aktivieren oder Deaktivieren von TSO auf einem ESXi-Host

Aktivieren Sie TCP Segmentation Offload (TSO) im Übertragungspfad, um der Netzwerkkarte die Unterteilung größerer Datenblöcke in TCP-Segmente zu ermöglichen. Deaktivieren Sie TSO, um die TCP-Segmentierung von der CPU durchführen zu lassen.

Standardmäßig verwendet ein Host Hardware-TSO, sofern dessen physische Adapter dies unterstützen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Erweitern Sie den Abschnitt „System“ und klicken Sie auf **Erweiterte Systemeinstellungen**.
- 4 Geben Sie für IPv4 den Wert des Parameters `Net.UseHwTSO` und für IPv6 des Parameters `Net.UseHwTSO6` ein.
 - Um TSO zu aktivieren, setzen Sie `Net.UseHwTSO` und `Net.UseHwTSO6` auf **1**.
 - Zum Deaktivieren von TSO setzen Sie `Net.UseHwTSO` und `Net.UseHwTSO6` auf **0**.
- 5 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

- 6 Um das Treibermodul des physischen Adapters neu zu laden, führen Sie den Konsolenbefehl `esxcli system module set` in der ESXi Shell auf dem Host aus.
- a Um den Treiber zu deaktivieren, führen Sie den Befehl `esxcli system module set` mit der Option `--enabled false` aus.

```
esxcli    system module set
--enabled false
--module
nic_driver_module
```

- b Um den Treiber zu aktivieren, führen Sie den Befehl `esxcli system module set` mit der Option `--enabled true` aus.

```
esxcli    system module set
--enabled true
--module
nic_driver_module
```

Ergebnisse

Wenn der physische Adapter Hardware-TSO nicht unterstützt, segmentiert der VMkernel große TCP-Pakete, die vom Gastbetriebssystem geschickt werden, und sendet sie an den Adapter.

Ermitteln, ob TSO auf einem ESXi-Host aktiviert ist

Ermitteln Sie, ob Hardware-TSO im VMkernel aktiviert ist, wenn Sie die Netzwerkleistung eines Hosts mit latenzempfindlicher Arbeitslast schätzen. Hardware-TSO ist standardmäßig auf einem ESXi-Host aktiviert.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Erweitern Sie den Abschnitt „System“ und klicken Sie auf **Erweiterte Systemeinstellungen**.
- 4 Sehen Sie sich die Werte der Parameter `Net.UseHwTSO` und `Net.UseHwTSO6` an.

`Net.UseHwTSO` zeigt den TSO-Status für IPv4, `Net.UseHwTSO6` jenen für IPv6 an. TSO ist aktiviert, wenn der Wert auf 1 festgelegt ist.

Aktivieren oder Deaktivieren von TSO auf einer Linux-VM

Aktivieren Sie TSO-Unterstützung auf dem Netzwerkadapter einer virtuellen Linux-Maschine, damit das Gastbetriebssystem TCP-Pakete, die segmentiert werden müssen, zum VMkernel weiterleitet.

Voraussetzungen

- Prüfen Sie, ob ESXi 6.0 das Linux-Gastbetriebssystem unterstützt.
Informationen finden Sie in der Dokumentation *VMware-Kompatibilitätshandbuch*.
- Stellen Sie sicher, dass der Netzwerkadapter auf der virtuellen Linux-Maschine vom Typ VMXNET2 oder VMXNET3 ist.

Verfahren

- ◆ Führen Sie in einem Terminalfenster auf dem Linux-Gastbetriebssystem zum Aktivieren oder Deaktivieren von TSO den Befehl `ethtool` mit den Optionen `-K` und `tso` aus.

- Führen Sie folgenden Befehl aus, um TSO zu aktivieren:

```
ethtool-K ethYtsoon
```

- Führen Sie folgenden Befehl aus, um TSO zu deaktivieren:

```
ethtool-K ethYtsooff
```

Das `Y` in „eth Y“ gibt hier die Sequenznummer der Netzwerkkarte in der virtuellen Maschine an.

Aktivieren oder Deaktivieren von TSO auf einer Windows-VM

Standardmäßig ist TSO auf einer virtuellen Windows-Maschine auf VMXNET2- und VMXNET3-Netzwerkadaptern aktiviert. Aus Leistungsgründen können Sie TSO deaktivieren.

Voraussetzungen

- Prüfen Sie, ob ESXi 6.0 das Windows-Gastbetriebssystem unterstützt. Informationen finden Sie in der Dokumentation *VMware-Kompatibilitätshandbuch*.
- Stellen Sie sicher, dass der Netzwerkadapter auf der virtuellen Windows-Maschine vom Typ VMXNET2 oder VMXNET3 ist.

Verfahren

- 1 Klicken Sie in „Netzwerk- und Freigabecenter“ in der Windows-Systemsteuerung auf den Namen des Netzwerkadapters.
- 2 Klicken Sie auf seinen Namen.
Ein Dialogfeld zeigt den Status des Adapters an.
- 3 Klicken Sie auf **Eigenschaften** und unter dem Netzwerkadaptertyp auf **Konfigurieren**.
- 4 Setzen Sie auf der Registerkarte **Erweitert** die Eigenschaften **Large Send Offload V2 (IPv4)** und **Large Send Offload V2 (IPv6)** auf **Aktiviert** oder **Deaktiviert**.
- 5 Klicken Sie auf **OK**.
- 6 Starten Sie die virtuelle Maschine neu.

Large Receive Offload

Mit Large Receive Offload (LRO) können Sie den CPU-Overhead bei der Verarbeitung von Paketen, die mit hoher Frequenz aus dem Netzwerk eingehen, reduzieren.

LRO fasst eingehende Netzwerkpakete zu größeren Puffern zusammen und überträgt die so entstandenen größeren und weniger zahlreichen Pakete an den Netzwerk-Stack des Hosts oder der virtuellen Maschine. Die CPU muss nun weniger Pakete als bei deaktiviertem LRO verarbeiten, was ihre Nutzung im Netzwerk reduziert, besonders bei Verbindungen mit hoher Bandbreite.

Um die höhere Leistung mit LRO zu nutzen, aktivieren Sie LRO entlang des gesamten Datenpfads auf dem ESXi-Host. Dazu gehören auch VMkernel und Gastbetriebssystem. LRO ist standardmäßig im VMkernel und den VMXNET3-Adaptoren von virtuellen Maschinen aktiviert.

Informationen über die Position der TCP-Paketzusammenfassung im Datenpfad erhalten Sie in der VMware-Knowledgebase im Artikel über [TCP Segmentation Offload \(TSO\) und Large Receive Offload \(LRO\) in VMware-Umgebungen](#).

Aktivieren von Hardware-LRO für alle VMXNET3-Adapter auf einem ESXi-Host

Aktivieren Sie die Hardwarefunktionen der physischen Hostadapter, um beim Aggregieren der eingehenden TCP-Pakete für VMXNET3-VM-Adapter die LRO-Technologie zu nutzen, anstatt die Assembling-Ressourcen des Gastbetriebssystems zu verbrauchen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Erweitern Sie den Abschnitt „System“ und klicken Sie auf **Erweiterte Systemeinstellungen**.
- 4 Bearbeiten Sie den Wert des Parameters `Net.Vmxnet3HwLRO`.
 - Zur Aktivierung von Hardware-LRO setzen Sie `Net.Vmxnet3HwLRO` auf **1**.
 - Zur Deaktivierung von Hardware-LRO setzen Sie `Net.Vmxnet3HwLRO` auf **0**.
- 5 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Aktivieren oder Deaktivieren von Software-LRO für alle VMXNET3-Adapter auf einem ESXi-Host

Bei mangelnder Unterstützung von Hardware-LRO durch die physischen Hostadapter verbessern Sie mit Software-LRO im VMkernel-Backend von VMXNET3-Adaptoren die Netzwerkleistung von virtuellen Maschinen.

vSphere 5.5 und höher unterstützen Software-LRO für IPv4- und IPv6-Pakete.

Voraussetzungen

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Erweitern Sie den Abschnitt „System“ und klicken Sie auf **Erweiterte Systemeinstellungen**.
- 4 Bearbeiten Sie den Wert des Parameters `Net.Vmxnet3SwLRO` für VMXNET3-Adapter.
 - Zur Aktivierung von Software-LRO setzen Sie `Net.Vmxnet3SwLRO` auf 1.
 - Um Software-LRO zu deaktivieren, setzen Sie `Net.Vmxnet3SwLRO` auf 0.
- 5 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Ermitteln, ob LRO für VMXNET3-Adapter auf einem ESXi-Host aktiviert ist

Untersuchen Sie den Status von LRO auf einem ESXi, wenn Sie die Netzwerkleistung auf einem Host mit latenzempfindlichen Arbeitslasten abschätzen.

Voraussetzungen**Verfahren**

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Erweitern Sie den Abschnitt „System“ und klicken Sie auf **Erweiterte Systemeinstellungen**.
- 4 Prüfen Sie den Wert der LRO-Parameter für VMXNET2 und VMXNET3.
 - Prüfen Sie für Hardware-LRO den Parameter `Net.Vmxnet3HwLRO`. Wenn er 1 beträgt, ist Hardware-LRO aktiviert.
 - Prüfen Sie für Software-LRO den Parameter `Net.Vmxnet3SwLRO`. Wenn er 1 beträgt, ist Hardware-LRO aktiviert.

Ändern der Größe des LRO-Puffers für VMXNET 3-Adapter

Sie können die Größe des Puffers für die Paketzusammenfassung für Verbindungen virtueller Maschinen durch VMXNET 3-Netzwerkadapter ändern. Erhöhen Sie die Puffergröße zum Verringern der Anzahl der TCP-Bestätigungen und zum Erhöhen der Effizienz in Arbeitslasten.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Erweitern Sie den Abschnitt „System“ und klicken Sie auf **Erweiterte Systemeinstellungen**.

- 4 Geben Sie einen Wert zwischen 1 und 65535 für den Parameter `Net.VmxnetLROMaxLength` zum Festlegen der LRO-Puffergröße in Byte ein.

Standardmäßig beträgt die Größe des LRO-Puffers 32000 Byte.

Aktivieren oder Deaktivieren von LRO für alle VMkernel-Adapter auf einem ESXi-Host

Mit LRO in VMkernel-Netzwerkadaptern auf einem ESXi-Host verbessern Sie die Netzwerkleistung bei eingehendem Infrastrukturdatenverkehr.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Erweitern Sie den Abschnitt „System“ und klicken Sie auf **Erweiterte Systemeinstellungen**.
- 4 Bearbeiten Sie den Wert des Parameters `Net.TcpipDefLROEnabled`.
 - Um LRO für die VMkernel-Netzwerkadapter auf dem Host zu aktivieren, setzen Sie `Net.TcpipDefLROEnabled` auf **1**.
 - Zum Deaktivieren von LRO für die VMkernel-Netzwerkadapter auf dem Host setzen Sie `Net.TcpipDefLROEnabled` auf **0**.
- 5 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Ändern der Größe des LRO-Puffers für VMkernel-Adapter

Sie können die Puffergröße für die Paketzusammenfassung in VMkernel-Verbindungen ändern. Erhöhen Sie die Puffergröße, um die Anzahl von TCP-Bestätigungen zu reduzieren und die Effizienz im VMkernel zu verbessern.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Erweitern Sie den Abschnitt „System“ und klicken Sie auf **Erweiterte Systemeinstellungen**.
- 4 Geben Sie für den Parameter `Net.TcpipDefLROMaxLength` einen Wert zwischen 1 und 65535 ein, um die Größe des LRO-Puffers in Byte anzugeben.

Standardmäßig beträgt die Größe des LRO-Puffers 32768 Byte.

Aktivieren oder Deaktivieren von LRO auf einem VMXNET3-Adapter auf einer Linux-VM

Wenn LRO für VMXNET3-Adapter auf dem Host aktiviert ist, aktivieren Sie auch die LRO-Unterstützung in einem Netzwerkadapter einer virtuellen Linux-Maschine. Dadurch stellen Sie

sicher, dass das Gastbetriebssystem keine Ressourcen darauf verwendet, eingehende Pakete zu größeren Paketen zusammenzufassen.

Voraussetzungen

Stellen Sie sicher, dass der Linux-Kernel die Version 2.6.24 oder höher aufweist.

Verfahren

- ◆ Geben Sie in einem Terminalfenster auf dem Linux-Gastbetriebssystem den Befehl `ethtool` mit den Optionen `-K` und `lro` aus.

- Führen Sie folgenden Befehl aus, um LRO zu aktivieren:

```
ethtool -K ethYlroon
```

Das `Y` in „eth `Y`“ gibt hier die Sequenznummer der Netzwerkkarte in der virtuellen Maschine an.

- Führen Sie folgenden Befehl aus, um LRO zu deaktivieren:

```
ethtool -K ethYlrooff
```

Das `Y` in „eth `Y`“ gibt hier die Sequenznummer der Netzwerkkarte in der virtuellen Maschine an.

Aktivieren oder Deaktivieren von LRO auf einem VMXNET3-Adapter auf einer Windows-VM

Wenn LRO für VMXNET3-Adapter auf dem Host aktiviert ist, aktivieren Sie auch die LRO-Unterstützung in einem Netzwerkadapter einer virtuellen Windows-Maschine. Dadurch stellen Sie sicher, dass das Gastbetriebssystem keine Ressourcen darauf verwendet, eingehende Pakete zu größeren Puffern zusammenzufassen.

Unter Windows wird die LRO-Technologie auch als „Empfangsseitige Zusammenfügung (Receive Side Coalescing, RSC)“ bezeichnet.

Voraussetzungen

- Überprüfen Sie, dass die virtuelle Maschine Windows Server 2012 oder höher bzw. Windows 8 oder höher ausführt.
- Stellen Sie sicher, dass die virtuelle Maschine mit ESXi 6.0 und höher kompatibel ist.
- Überprüfen Sie, dass die Version des auf dem Gastbetriebssystem installierten VMXNET3-Treibers 1.6.6.0 oder höher ist.
- Überprüfen Sie, dass LRO global auf einer virtuellen Maschine aktiviert ist, die Windows Server 2012 oder höher bzw. Windows 8 oder höher ausführt. Siehe [Globales Aktivieren von LRO auf einer virtuellen Windows-Maschine](#).

Verfahren

- 1 Klicken Sie in **Netzwerk- und Freigabecenter** in der Systemsteuerung des Gastbetriebssystems auf den Namen des Netzwerkadapters.
Ein Dialogfeld zeigt den Status des Adapters an.
- 2 Klicken Sie auf **Eigenschaften** und unter dem VMXNET3-Netzwerkadaptertyp auf **Konfigurieren**.
- 3 Legen Sie auf der Registerkarte **Erweitert** sowohl **Empfangssegmentzusammenfügung (IPv4)** als auch **Empfangssegmentzusammenfügung (IPv6)** auf **Aktiviert** bzw. **Deaktiviert** fest.
- 4 Klicken Sie auf **OK**.

Globales Aktivieren von LRO auf einer virtuellen Windows-Maschine

Um LRO auf einem VMXNET3-Adapter auf einer virtuellen Maschine unter Windows 8 oder Windows Server 2012 (und höher) zu verwenden, müssen Sie LRO global für das Gastbetriebssystem aktivieren. Unter Windows wird die LRO-Technologie auch als „Empfangsseitige Zusammenfügung (Receive Side Coalescing, RSC)“ bezeichnet.

Verfahren

- 1 Um zu überprüfen, ob LRO global auf einem Windows 8- oder Windows Server 2012-Gastbetriebssystem (und höher) deaktiviert ist, führen Sie den Befehl `netsh int tcp show global` an der Eingabeaufforderung aus.

```
netsh int tcp show global
```

Der Befehl zeigt den Status der globalen TCP-Parameter an, die auf dem Windows 8.x-Betriebssystem festgelegt sind.

```
Globale TCP-Parameter
-----
Skalierungsstatus Empfangsseite           : aktiviert
Chimney-Abladestatus: Deaktiviert
NetDMA-Status                             : Deaktiviert
Direktcachezugriff (DCA)                  : Deaktiviert
Autom. Abstimmungsgrad Empfangsfenster    : Normal
Add-On „Überlastungssteuerungsanbieter“   : keine
ECN-Funktion                             : Deaktiviert
RFC 1323-Zeitstempel                      : Deaktiviert
Initial RTO                               : 3000
Status Empfangssegmentzusammenfügung      : Deaktiviert
```

Wenn LRO auf dem Windows 8- oder Windows Server 2012-System (und höher) global deaktiviert ist, wird die Eigenschaft „Status Empfangssegmentzusammenfügung“ als deaktiviert angezeigt.

- 2 Um LRO global für das Windows-Betriebssystem zu aktivieren, führen Sie den Befehl `netsh int tcp set global` an der Befehlszeile aus:

```
netsh int tcp set global rsc=enabled
```

Nächste Schritte

Aktivieren Sie LRO auf dem VMXNET3-Adapter auf der virtuellen Windows 8- oder Windows Server 2012-Maschine (und höher). Siehe [Aktivieren oder Deaktivieren von LRO auf einem VMXNET3-Adapter auf einer Windows-VM](#).

NetQueue und Netzwerkleistung

NetQueue nutzt die Möglichkeit mancher Netzwerkadapter, den Netzwerkdatenverkehr in mehreren Empfangswarteschlangen, die getrennt verarbeitet werden können, an das System zu liefern. Somit ist es möglich, die Verarbeitung auf mehreren CPUs zu skalieren, was die empfangsseitige Netzwerkleistung verbessert.

Aktivieren von NetQueue auf einem Host

NetQueue ist standardmäßig aktiviert. Um NetQueue verwenden zu können, nachdem es deaktiviert wurde, muss es erneut aktiviert werden.

Voraussetzungen

Verfahren

- 1 Verwenden Sie in einer ESXi Shell für den Host den folgenden Befehl:

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="TRUE"
```

- 2 Verwenden Sie den Befehl `esxcli module parameters set`, um den Netzwerkkartentreiber für die Verwendung von NetQueue zu konfigurieren.

Führen Sie z. B. für eine Dual-Port-Emulex-Netzwerkkarte die folgenden ESXCLI-Befehle aus, um den Treiber mit 8 Empfangswarteschlangen zu konfigurieren.

```
esxcli system module parameters set -m tg3 -p force_netq=8,8
```

- 3 Starten Sie den Host neu.

Deaktivieren von NetQueue auf einem Host

NetQueue ist standardmäßig aktiviert.

Voraussetzungen

Informationen zur Konfiguration der Netzwerkkartentreiber finden Sie im Handbuch *Erste Schritte mit vSphere-Befehlszeilenschnittstellen*.

Verfahren

- 1 Verwenden Sie in der VMware vSphere-CLI je nach Hostversion den folgenden Befehl:

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="FALSE"
```

- 2 Verwenden Sie zum Deaktivieren von NetQueue auf dem Netzwerkkartentreiber den Befehl `esxcli module parameters set`.

Führen Sie beispielsweise auf einer Dual-Port-Emulex-Netzwerkkarte diesen ESXCLI-Befehl aus, um für den Treiber eine Empfangswarteschlange zu konfigurieren.

```
esxcli system module parameters set -m tg3 -p force_netq=1,1
```

- 3 Starten Sie den Host neu.

vSphere Network I/O Control

11

Verwenden Sie vSphere Network I/O Control, um geschäftskritischen Anwendungen Netzwerkbandbreite zuzuteilen und Situationen zu beheben, in denen verschiedene Datenverkehrstypen die gleichen Ressourcen beanspruchen.

- [Info zu vSphere Network I/O Control Version 3](#)

In vSphere Network I/O Control Version 3 wird ein Mechanismus eingeführt, mit dem Bandbreite für Systemdatenverkehr basierend auf der Kapazität der physischen Adapter eines Hosts reserviert werden kann. Dadurch lassen sich die Ressourcen auf VM-Netzwerkadapterebene ähnlich detailliert steuern wie bei dem Modell, das Sie zum Zuteilen von CPU- und Arbeitsspeicherressourcen verwenden.

- [Upgrade von Network I/O Control auf Version 3 auf einem vSphere Distributed Switch](#)

Wenn Sie für einen vSphere Distributed Switch ein Upgrade auf Version 6.0.0 durchgeführt haben, ohne Network I/O Control auf Version 3 zu konvertieren, können Sie ein Upgrade für Network I/O Control durchführen, um das erweiterte Modell zur Bandbreitenzuteilung für Systemdatenverkehr und einzelne virtuelle Maschinen zu verwenden.

- [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#)

Aktivieren Sie die Netzwerkressourcenverwaltung auf einem vSphere Distributed Switch, um eine Mindestbandbreite für Systemdatenverkehr der vSphere-Funktionen und für Datenverkehr der virtuellen Maschinen zu garantieren.

- [Bandbreitenzuteilung für Systemdatenverkehr](#)

Basierend auf Freigaben, Reservierung und Grenzwerten können Sie Network I/O Control so konfigurieren, dass eine bestimmte Bandbreitenkapazität für Datenverkehr zugeteilt wird, der von vSphere Fault Tolerance, iSCSI-Speicher, vSphere vMotion usw. generiert wird.

- [Bandbreitenzuteilung für Datenverkehr über virtuelle Maschinen](#)

Mit Version 3 von Network I/O Control können Sie Bandbreitenanforderungen für einzelne virtuelle Maschinen konfigurieren. Sie können auch Netzwerkressourcenpools verwenden, für die Sie ein Bandbreitenkontingent aus der Gesamtreservierung für den Datenverkehr über virtuelle Maschinen zuweisen und dann Bandbreite aus dem Pool einzelnen virtuellen Maschinen zuteilen können.

- [Verschieben eines physischen Adapters aus dem Bereich von Network I/O Control](#)

Unter bestimmten Umständen müssen Sie evtl. physische Adapter mit geringer Kapazität aus dem Bandbreitenzuteilungsmodell von Network I/O Control Version 3 ausschließen.

- [Arbeiten mit Network I/O Control Version 2](#)

Auf einem vSphere Distributed Switch 5.x bzw. einem vSphere Distributed Switch, für das ein Upgrade auf 6.0 durchgeführt wurde und das nicht über die verbesserte Version Network I/O Control Version 3 verfügt, können Sie sicherstellen, dass der Systemdatenverkehr und die virtuellen Maschinen die erforderliche Bandbreite für ihren Betrieb erhalten, indem Sie das Ressourcenpoolmodell von Network I/O Control Version 2 verwenden.

Info zu vSphere Network I/O Control Version 3

In vSphere Network I/O Control Version 3 wird ein Mechanismus eingeführt, mit dem Bandbreite für Systemdatenverkehr basierend auf der Kapazität der physischen Adapter eines Hosts reserviert werden kann. Dadurch lassen sich die Ressourcen auf VM-Netzwerkadapterebene ähnlich detailliert steuern wie bei dem Modell, das Sie zum Zuteilen von CPU- und Arbeitsspeicherressourcen verwenden.

Version 3 von Network I/O Control bietet verbesserte Netzwerkressourcenreservierung und -zuteilung auf dem gesamten Switch.

Modelle für die Bandbreitenressourcenreservierung

Network I/O Control Version 3 unterstützt getrennte Modelle für die Ressourcenverwaltung des Systemdatenverkehrs im Zusammenhang mit Infrastrukturdiensten wie vSphere Fault Tolerance und des Datenverkehrs von virtuellen Maschinen.

Die beiden Datenverkehrskategorien sind von ihrer Art her unterschiedlich. Systemdatenverkehr ist strikt einem ESXi-Host zugeordnet. Die Netzwerkdatenverkehrsrouten ändern sich, wenn Sie eine virtuelle Maschine in einer Umgebung migrieren. Um Netzwerkressourcen hostunabhängig an eine virtuelle Maschine bereitzustellen, können Sie in Network I/O Control eine Ressourcenzuteilung für virtuelle Maschinen konfigurieren, die im Bereich des ganzen Distributed Switch gültig ist.

Bandbreitengarantie für virtuelle Maschinen

Network I/O Control Version 3 stellt Bandbreite für die Netzwerkadapter von virtuellen Maschinen bereit. Zu diesem Zweck werden Konstrukte aus Anteilen, Reservierung und Grenzwerten verwendet. Auf der Grundlage dieser Konstrukte können sich virtualisierte Arbeitslasten darauf verlassen, dass sie über die Zugangssteuerung in vSphere Distributed Switch, vSphere DRS und vSphere HA ausreichend Bandbreite erhalten. Siehe [Zugangssteuerung für Bandbreite virtueller Maschinen](#).

Network I/O Control Version 2 und Version 3 in vSphere 6.0

In vSphere 6.0 können die Versionen 2 und 3 von Network I/O Control parallel verwendet werden. Die beiden Versionen implementieren verschiedene Modelle für die Zuteilung von Bandbreite zu virtuellen Maschinen und Systemdatenverkehr. In Network I/O Control Version 2 konfigurieren Sie die Bandbreitenzuteilung für virtuelle Maschinen auf der Ebene der physischen Adapter. Mit Version 3 können Sie dagegen die Bandbreitenzuteilung für virtuelle Maschinen auf der Ebene des ganzen Distributed Switch einrichten.

Wenn Sie ein Upgrade für einen Distributed Switch durchführen, wird Network I/O Control ebenfalls auf Version 3 aktualisiert, es sei denn, Sie verwenden einige der Funktionen, die in Network I/O Control Version 3 nicht verfügbar sind, wie z. B. CoS-Tagging und benutzerdefinierte Netzwerkressourcenpools. In diesem Fall ist aufgrund des Unterschieds zwischen den Ressourcenzuteilungsmodellen von Version 2 und 3 kein unterbrechungsfreies Upgrade möglich. Sie können weiterhin Version 2 verwenden, um die Bandbreitenzuteilungseinstellungen für virtuelle Maschinen beizubehalten, oder Sie können zu Version 3 wechseln und eine Bandbreitenrichtlinie für alle Switch-Hosts erstellen.

Tabelle 11-1. Network I/O Control Version entsprechend der Version von vSphere Distributed Switch und ESXi

vSphere Network I/O Control	Version des vSphere Distributed Switch	ESXi-Version
2.0	5.1.0	<ul style="list-style-type: none"> ■ 5.1 ■ 5.5 ■ 6.0
	5.5.0	<ul style="list-style-type: none"> ■ 5.5 ■ 6.0
3.0	6.0.0	6.0

Verfügbarkeit von Funktionen

SR-IOV ist für virtuelle Maschinen, die für Network I/O Control Version 3 konfiguriert sind, nicht verfügbar.

Upgrade von Network I/O Control auf Version 3 auf einem vSphere Distributed Switch

Wenn Sie für einen vSphere Distributed Switch ein Upgrade auf Version 6.0.0 durchgeführt haben, ohne Network I/O Control auf Version 3 zu konvertieren, können Sie ein Upgrade für Network I/O Control durchführen, um das erweiterte Modell zur Bandbreitenzuteilung für Systemdatenverkehr und einzelne virtuelle Maschinen zu verwenden.

Wenn Sie für Network I/O Control, Version 2, ein Upgrade auf Version 3 durchführen, werden die Einstellungen aus allen vorhandenen System-Netzwerkressourcenpools, die in Version 2 definiert sind, in Konstrukte von Anteilen, Reservierung und Grenzwerten für Systemdatenverkehr konvertiert. Die Reservierung ist für alle konvertierten System-Datenverkehrstypen standardmäßig nicht festgelegt.

Das Upgrade eines Distributed Switch auf Version 3 ist mit Unterbrechungen verbunden. Bestimmte Funktionen sind nur in Network I/O Control, Version 2, verfügbar und werden während des Upgrades auf Version 3 entfernt.

Tabelle 11-2. Während des Upgrades auf Network I/O Control, Version 3, entfernte Funktionen

Während des Upgrades entfernte Funktionen	Beschreibung
Benutzerdefinierte Netzwerkressourcenpools einschließlich aller Verknüpfungen zwischen diesen und vorhandenen verteilten Portgruppen	Sie können bestimmte Einstellungen für die Ressourcenzuteilung beibehalten, indem Sie die Anteile von den benutzerdefinierten Netzwerkressourcenpools an Anteile für einzelne Netzwerkadapter übertragen. Vor dem Upgrade auf Network I/O Control, Version 3, sollten Sie deshalb sicherstellen, dass das Upgrade keine übermäßigen Auswirkungen auf die Bandbreitenzuteilung hat, die für virtuelle Maschinen in Network I/O Control, Version 2, konfiguriert ist.
Vorhandene Verknüpfungen zwischen Ports und benutzerdefinierten Netzwerkressourcenpools	In Network I/O Control, Version 3, kann ein einzelner verteilter Port keinem Netzwerkressourcenpool zugeordnet werden, der nicht mit dem Pool identisch ist, der der übergeordneten Portgruppe zugewiesen ist. Im Gegensatz zu Version 2 unterstützt Network I/O Control, Version 3, nicht das Außerkraftsetzen der Ressourcenzuteilungsrichtlinie auf der Portebene.
CoS-Tagging des Datenverkehrs in Zusammenhang mit einem Netzwerkressourcenpool	Das Kennzeichnen von Datenverkehr, der höhere QoS-Anforderungen hat, mit CoS-Tags wird von Network I/O Control, Version 3, nicht unterstützt. Verwenden Sie nach dem Upgrade die Netzwerkrichtlinie zum Filtern und Markieren des Datenverkehrs, um das CoS-Tagging des Datenverkehrs in Zusammenhang mit einem benutzerdefinierten Netzwerkressourcenpool wiederzustellen. Siehe Markieren des Datenverkehrs in verteilten oder Uplink-Portgruppen und Markieren des Datenverkehrs in verteilten oder Uplink-Ports .

Voraussetzungen

- Stellen Sie sicher, dass der vSphere Distributed Switch Version 6.0.0 entspricht.
- Stellen Sie sicher, dass die Network I/O Control-Funktion des Distributed Switch der Version 2 entspricht.
- Stellen Sie sicher, dass Sie für die verteilten Portgruppen auf dem Switch über das Recht **dvPort-Gruppe.Ändern** verfügen.
- Stellen Sie sicher, dass alle Hosts auf dem Switch mit vCenter Server verbunden sind.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Upgrade > Upgrade für Network I/O Control durchführen** aus.

Der Assistent **Upgrade für Network I/O Control durchführen** wird angezeigt.

- 3 (Optional) Erstellen Sie auf der Seite „Überblick“ eine Sicherungskopie der Switch-Konfiguration.
Mithilfe der Sicherungskopie können Sie die Switch-Konfiguration wiederherstellen, falls das Upgrade fehlschlägt.
- 4 Überprüfen Sie die durch das Upgrade verursachten Änderungen und klicken Sie auf **Weiter**.
- 5 Stellen Sie sicher, dass der Distributed Switch die Validierungsvoraussetzungen für das Upgrade erfüllt, und klicken Sie auf **Weiter**.

Voraussetzung	Beschreibung
Portgruppenzugriff	Sie verfügen über Rechte, um auf den Uplink und die verteilten Portgruppen auf dem Switch zuzugreifen und diese zu ändern.
Hostzustand	Alle Hosts auf dem Switch sind mit vCenter Server verbunden.
CoS-Prioritäts-Tag für Systemdatenverkehr	Der Distributed Switch weist keine Netzwerkressourcenpools auf, denen ein CoS-Tag zugewiesen ist.
Benutzerdefinierte Netzwerkressourcenpools	Der Distributed Switch enthält keine benutzerdefinierten Ressourcenpools für die Bandbreitenkontrolle virtueller Maschinen.
Außerkraftsetzung der Ressourcenzuteilungsrichtlinie	Keine verteilten Portgruppen auf dem Switch erlauben das Außerkraftsetzen der Network I/O Control-Richtlinie auf einzelnen Ports.

- 6 Falls der Distributed Switch benutzerdefinierte Ressourcenpools enthält, übertragen Sie die Anteile von den benutzerdefinierten Ressourcenpools in Version 2 an Anteile einzelner VM-Netzwerkadapter in Version 3 und klicken Sie auf **Weiter**.

Durch das Übertragen der Anteile können Sie bestimmte Einstellungen für die Bandbreitenzuteilung von virtuellen Maschinen beibehalten.

Hinweis Die Grenzwerte für benutzerdefinierte Netzwerkressourcenpools werden während der Konvertierung nicht beibehalten.

- 7 Überprüfen Sie die Upgrade-Einstellungen und klicken Sie auf **Beenden**.

Nächste Schritte

- Weisen Sie einer Gruppe von virtuellen Maschinen, die mit dem Switch verbunden sind, ein Reservierungsbandbreitenkontingent zu, indem Sie Netzwerkressourcenpools erstellen und ihnen die verteilten Portgruppen zuordnen, mit denen die virtuellen Maschinen verbunden sind. Siehe [Erstellen eines Netzwerkressourcenpools](#) und [Hinzufügen einer verteilten Portgruppe zu einem Netzwerkressourcenpool](#).

Falls Sie die ursprünglichen Anteile von Version 2 übertragen haben, werden sie erzwungen, wenn Sie Netzwerkressourcenpools die Portgruppen des Switches zuordnen.

- Teilen Sie Bandbreite aus dem Kontingent den einzelnen virtuellen Maschinen zu, indem Sie Anteile, Reservierung und Grenzwerte verwenden. Siehe [Konfigurieren der Bandbreitenzuteilung für eine virtuelle Maschine](#).

Aktivieren von Network I/O Control auf einem vSphere Distributed Switch

Aktivieren Sie die Netzwerkressourcenverwaltung auf einem vSphere Distributed Switch, um eine Mindestbandbreite für Systemdatenverkehr der vSphere-Funktionen und für Datenverkehr der virtuellen Maschinen zu garantieren.

Voraussetzungen

Stellen Sie sicher, dass der vSphere Distributed Switch Version 5.1.0 oder höher entspricht.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Einstellungen bearbeiten** aus.
- 3 Wählen Sie im Dropdown-Menü **Network I/O Control** die Option **Aktivieren** aus.
- 4 Klicken Sie auf **OK**.

Ergebnisse

Bei Aktivierung basiert das Modell, das von Network I/O Control zum Verarbeiten der Bandbreitenzuteilung für Systemdatenverkehr und Datenverkehr der virtuellen Maschinen verwendet wird, auf der Network I/O Control-Version, die auf dem Distributed Switch aktiv ist. Siehe [Info zu vSphere Network I/O Control Version 3](#).

Bandbreitenzuteilung für Systemdatenverkehr

Basierend auf Freigaben, Reservierung und Grenzwerten können Sie Network I/O Control so konfigurieren, dass eine bestimmte Bandbreitenkapazität für Datenverkehr zugeteilt wird, der von vSphere Fault Tolerance, iSCSI-Speicher, vSphere vMotion usw. generiert wird.

Mithilfe von Network I/O Control können Sie auf einem Distributed Switch die Bandbreitenzuteilung für den Datenverkehr in Zusammenhang mit den Hauptsystemfunktionen in vSphere konfigurieren:

- Management
- Fault Tolerance
- iSCSI
- NFS

- Virtual SAN
- vMotion
- vSphere Replication
- vSphere Data Protection-Sicherung
- Virtuelle Maschine

vCenter Server gibt die Zuteilung vom Distributed Switch an jeden physischen Adapter auf den mit dem Switch verbundenen Hosts weiter.

- **Bandbreitenzuteilungsparameter für Systemdatenverkehr**

Anhand von mehreren Konfigurationsparametern teilt Network I/O Control Bandbreite zu Datenverkehr von grundlegenden vSphere-Systemfunktionen zu.

- **Beispiel-Bandbreitenreservierung für Systemdatenverkehr**

Die Kapazität der physischen Adapter bestimmt die von Ihnen garantierte Bandbreite. Entsprechend dieser Kapazität können Sie einer Systemfunktion eine Mindestbandbreite garantieren, damit sie optimal funktionieren kann.

- **Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr**

Weisen Sie Bandbreite für Hostverwaltung, virtuelle Maschinen, iSCSI-Speicher, NFS-Speicher, vSphere vMotion, vSphere Fault Tolerance, Virtual SAN und vSphere Replication auf den physischen Adaptern zu, die mit einem vSphere Distributed Switch verbunden sind.

Bandbreitenzuteilungsparameter für Systemdatenverkehr

Anhand von mehreren Konfigurationsparametern teilt Network I/O Control Bandbreite zu Datenverkehr von grundlegenden vSphere-Systemfunktionen zu.

Tabelle 11-3. Zuteilungsparameter für Systemdatenverkehr

Bandbreitenzuteilungsparameter	Beschreibung
Anteile	<p>Anteile von 1 bis 100 geben die relative Priorität eines Systemdatenverkehrstyps im Vergleich zu anderen Systemdatenverkehrstypen an, die auf dem gleichen physischen Adapter aktiv sind.</p> <p>Die Menge der für den Systemdatenverkehrstyp verfügbaren Bandbreite wird durch die relativen Anteile und die Menge der Daten, die durch andere Systemfunktionen übertragen werden, bestimmt.</p> <p>Beispielsweise weisen Sie dem vSphere FT- und dem iSCSI-Datenverkehr 100 Anteile zu, während jeder der anderen Netzwerkressourcenpools 50 Anteile erhält. Ein physischer Adapter ist für das Versenden von vSphere Fault Tolerance-, iSCSI- und Verwaltungsdatenverkehr konfiguriert. Zu einem bestimmten Zeitpunkt sind vSphere Fault Tolerance und iSCSI die aktiven Datenverkehrstypen auf dem physischen Adapter und verbrauchen dessen Kapazität. Jeder Datenverkehr erhält 50 % der verfügbaren Bandbreite. Zu einem anderen Zeitpunkt ist der Adapter durch alle drei Datenverkehrstypen ausgelastet. In diesem Fall erhalten vSphere FT-Datenverkehr und iSCSI-Datenverkehr 40 % der Adapterkapazität, und vMotion erhält 20 %.</p>
Reservierung	<p>Die Mindestbandbreite in MBit/s, die auf einem einzelnen physischen Adapter garantiert sein muss. Die Gesamtbandbreite, die für alle Systemdatenverkehrstypen reserviert wird, darf 75 Prozent der Bandbreite des physischen Netzwerkadapters mit der geringsten Kapazität nicht überschreiten.</p> <p>Reservierte Bandbreite, die nicht verwendet wird, wird für andere Systemdatenverkehrstypen verfügbar. Network I/O Control verteilt jedoch die Kapazität, die nicht von Systemdatenverkehr verwendet wird, nicht an die Platzierung virtueller Maschinen weiter.</p> <p>Beispiel: Sie konfigurieren eine Reservierung von 2 GBit/s für iSCSI. Es ist möglich, dass der Distributed Switch diese Reservierung nie für einen physischen Adapter durchsetzt, weil iSCSI einen einzelnen Pfad verwendet. Die nicht verwendete Bandbreite wird nicht dem Systemdatenverkehr der virtuellen Maschine zugeteilt, sodass Network I/O Control einen potenziellen Bandbreitenbedarf für Systemdatenverkehr sicher bedienen kann, z. B. im Fall eines neuen iSCSI-Pfads, bei dem Sie Bandbreite für einen neuen VMkernel-Adapter bereitstellen müssen.</p>
Grenzwert	<p>Die maximale Bandbreite in MBit/s oder GBit/s, die ein Systemdatenverkehrstyp für einen einzelnen physischen Adapter nutzen kann.</p>

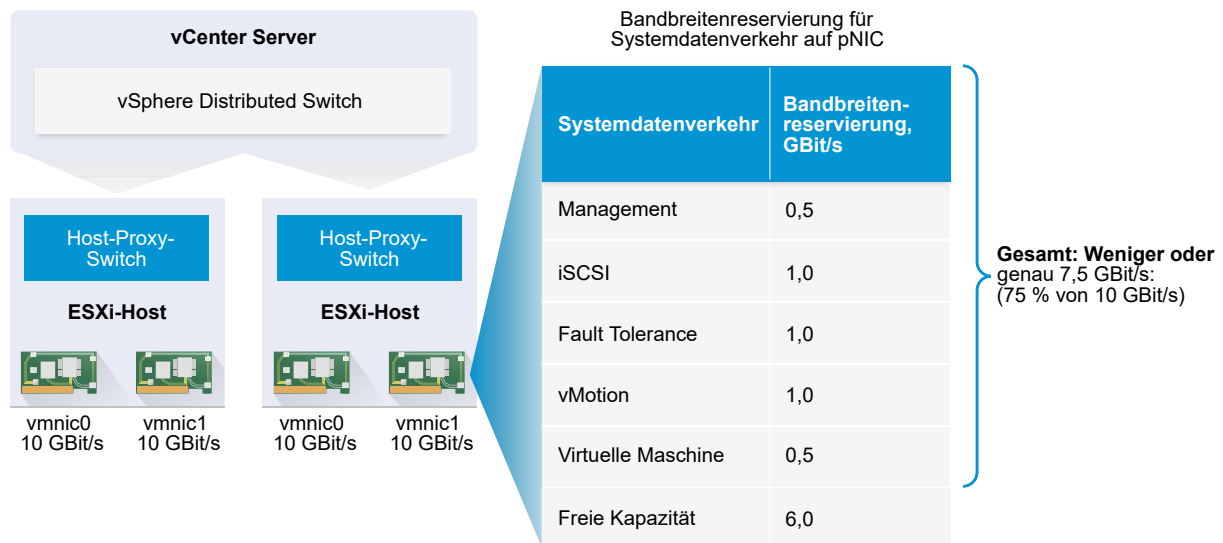
Beispiel-Bandbreitenreservierung für Systemdatenverkehr

Die Kapazität der physischen Adapter bestimmt die von Ihnen garantierte Bandbreite. Entsprechend dieser Kapazität können Sie einer Systemfunktion eine Mindestbandbreite garantieren, damit sie optimal funktionieren kann.

Beispielsweise können Sie auf einem Distributed Switch, der mit ESXi-Hosts mit 10-GbE-Netzwerkadaptern verbunden ist, eine Reservierung konfigurieren, mit der 1 GBit/s für die Verwaltung über vCenter Server, 1 GBit/s für iSCSI-Speicher, 1 GBit/s für vSphere Fault Tolerance, 1 GBit/s für vSphere vMotion-Datenverkehr und 0,5 GBit/s für Datenverkehr der virtuellen Maschinen reserviert wird. Network I/O Control teilt die angeforderte Bandbreite jedem physischen Netzwerkadapter zu. Sie können nicht mehr als 75 Prozent der Bandbreite eines physischen Netzwerkadapters reservieren, d.h. nicht mehr als 7,5 GBit/s.

Sie können weitere nicht reservierte Kapazität zurückhalten, damit der Host Bandbreite dynamisch je nach Anteilen, Grenzwerten und Verwendung zuteilen kann, und nur genügend Bandbreite für den Betrieb einer Systemfunktion reservieren.

Abbildung 11-1. Beispiel-Bandbreitenreservierung für Systemdatenverkehr auf einem physischen 10-GbE-Netzwerkadapter



Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr

Weisen Sie Bandbreite für Hostverwaltung, virtuelle Maschinen, iSCSI-Speicher, NFS-Speicher, vSphere vMotion, vSphere Fault Tolerance, Virtual SAN und vSphere Replication auf den physischen Adaptern zu, die mit einem vSphere Distributed Switch verbunden sind.

Konfigurieren Sie den Systemdatenverkehr auf virtuellen Maschinen, um die Bandbreitenzuteilung für virtuelle Maschinen mithilfe von Network I/O Control zu ermöglichen. Die Bandbreitenreservierung für Datenverkehr über virtuelle Maschinen wird auch bei der Zugangssteuerung verwendet. Wenn Sie eine virtuelle Maschine einschalten, überprüft die Zugangssteuerung, ob ausreichend Bandbreite verfügbar ist.

Voraussetzungen

- Überprüfen Sie, ob der vSphere Distributed Switch die Version 6.0.0 oder höher aufweist.
- Überprüfen Sie, ob Network I/O Control für den Switch die Version 3 aufweist.
- Überprüfen Sie, ob Network I/O Control aktiviert ist. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Ressourcenzuteilung**.
- 3 Klicken Sie auf **Systemdatenverkehr**.
Die Bandbreitenzuteilung für die Systemdatenverkehrstypen wird angezeigt.
- 4 Wählen Sie den Datenverkehrstyp gemäß der vSphere-Funktion aus, die Sie bereitstellen möchten, und klicken Sie auf **Bearbeiten**.
Die Netzwerkressourceneinstellungen für den Datenverkehrstyp werden angezeigt.
- 5 Bearbeiten Sie im Dropdown-Menü **Anteile** den Anteil des Datenverkehrs am Gesamtdatenverkehr über einen physischen Adapter.
Network I/O Control wendet die konfigurierten Anteile an, wenn ein physischer Adapter ausgelastet ist.
Sie können eine Option auswählen, um einen vordefinierten Wert festzulegen. Sie können aber auch **Benutzerdefiniert** auswählen und eine Zahl zwischen 1 und 100 eingeben, um einen anderen Anteil festzulegen.
- 6 Geben Sie im Textfeld **Reservierung** einen Wert für die Mindestbandbreite ein, die für den Datenverkehrstyp verfügbar sein muss.
Die Gesamtreservierung für Systemdatenverkehr darf 75 % der Bandbreite, die vom physischen Adapter mit der geringsten Kapazität unter allen mit dem Distributed Switch verbundenen Adaptern unterstützt wird, nicht überschreiten.
- 7 Legen Sie im Textfeld **Grenzwert** die maximale Bandbreite für Systemdatenverkehr des ausgewählten Typs fest.
- 8 Klicken Sie auf **OK**, um die Zuteilungseinstellungen anzuwenden.

Ergebnisse

vCenter Server gibt die Zuteilung vom Distributed Switch an die mit dem Switch verbundenen physischen Hostadapter weiter.

Bandbreitenzuteilung für Datenverkehr über virtuelle Maschinen

Mit Version 3 von Network I/O Control können Sie Bandbreitenanforderungen für einzelne virtuelle Maschinen konfigurieren. Sie können auch Netzwerkressourcenpools verwenden, für die Sie ein Bandbreitenkontingent aus der Gesamtreservierung für den Datenverkehr über virtuelle Maschinen zuweisen und dann Bandbreite aus dem Pool einzelnen virtuellen Maschinen zuteilen können.

Info zur Zuteilung von Bandbreite zu virtuellen Maschinen

Network I/O Control teilt Bandbreite zu virtuellen Maschinen anhand von zwei Modellen zu: Zuteilung über den gesamten vSphere Distributed Switch hinweg anhand von Netzwerkressourcenpools und Zuteilung an den physischen Adapter, der den Datenverkehr einer virtuellen Maschine überträgt.

Netzwerkressourcenpools

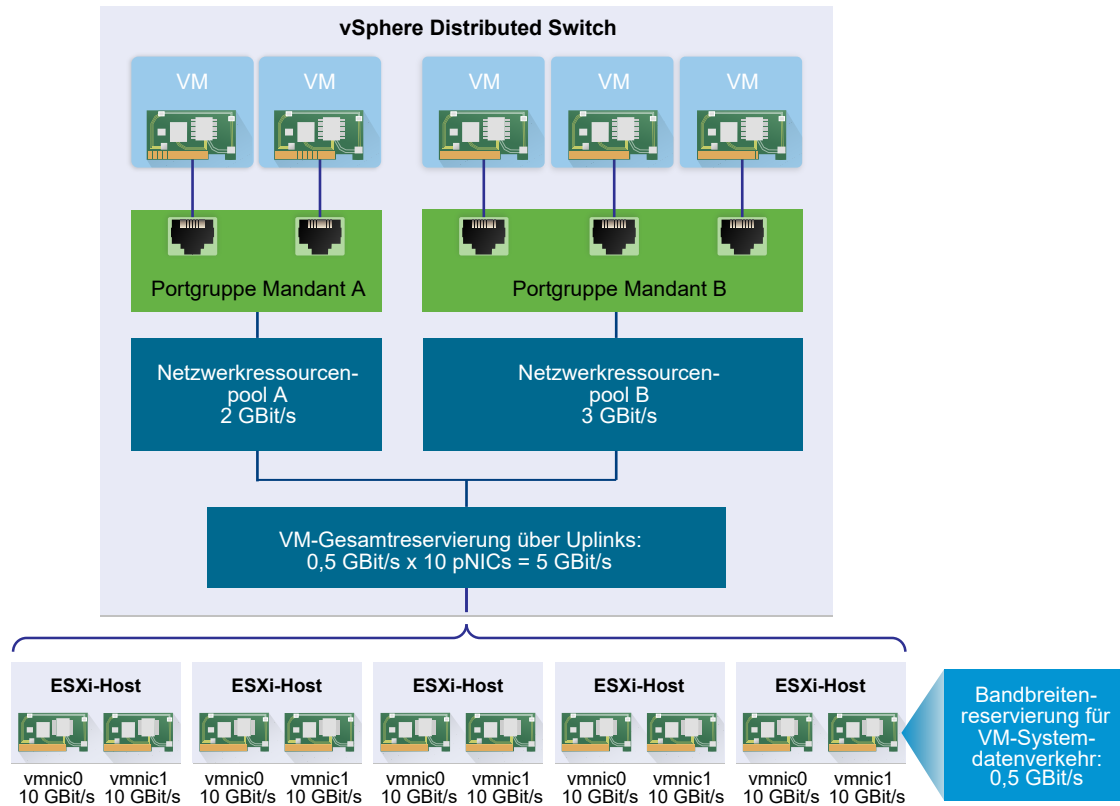
Ein Netzwerkressourcenpool stellt einen Teil der aggregierten Bandbreite dar, die für den Systemdatenverkehr der virtuellen Maschine auf allen physischen Adaptern, die mit dem Distributed Switch verbunden sind, reserviert ist.

Wenn zum Beispiel für den Systemdatenverkehr der virtuellen Maschine 0,5 GBit/s auf jedem 10 GbE-Uplink auf einem Distributed Switch mit 10 Uplinks reserviert sind, dann beträgt die gesamte aggregierte Bandbreite, die für die VM-Reservierung auf diesem Switch zur Verfügung steht, 5 GBit/s. Jeder Netzwerkressourcenpool kann ein Kontingent dieser Kapazität von 5 GBit/s reservieren.

Das Bandbreitenkontingent, das für einen Netzwerkressourcenpool reserviert ist, wird unter den verteilten Portgruppen dieses Pools verteilt. Eine virtuelle Maschine erhält Bandbreite aus dem Pool über die verteilte Portgruppe, mit der die VM verbunden ist.

Standardmäßig sind verteilte Portgruppen auf dem Switch einem Netzwerkressourcenpool mit den Namen „default“ zugewiesen, dessen Kontingent nicht konfiguriert ist.

Abbildung 11-2. Bandbreitenaggregation für Netzwerkressourcenpools für alle Uplinks eines vSphere Distributed Switch



Definieren der Bandbreitenanforderungen für eine virtuelle Maschine

Sie können Bandbreite zu einer einzelnen virtuellen Maschine ähnlich wie CPU und Arbeitsspeicherressourcen zuteilen. Network I/O Control Version 3 stellt Bandbreite an eine virtuellen Maschine entsprechend den Anteilen, der Reservierung und den Grenzwerten bereit, die für einen Netzwerkadapter in den VM-Hardwareeinstellungen definiert sind. Die Reservierung garantiert, dass der Datenverkehr der virtuellen Maschine mindestens die angegebene Bandbreite verbrauchen kann. Wenn ein physischer Adapter über mehr Kapazität verfügt, kann die virtuelle Maschine zusätzliche Bandbreite entsprechend den angegebenen Anteilen und dem Grenzwert verbrauchen.

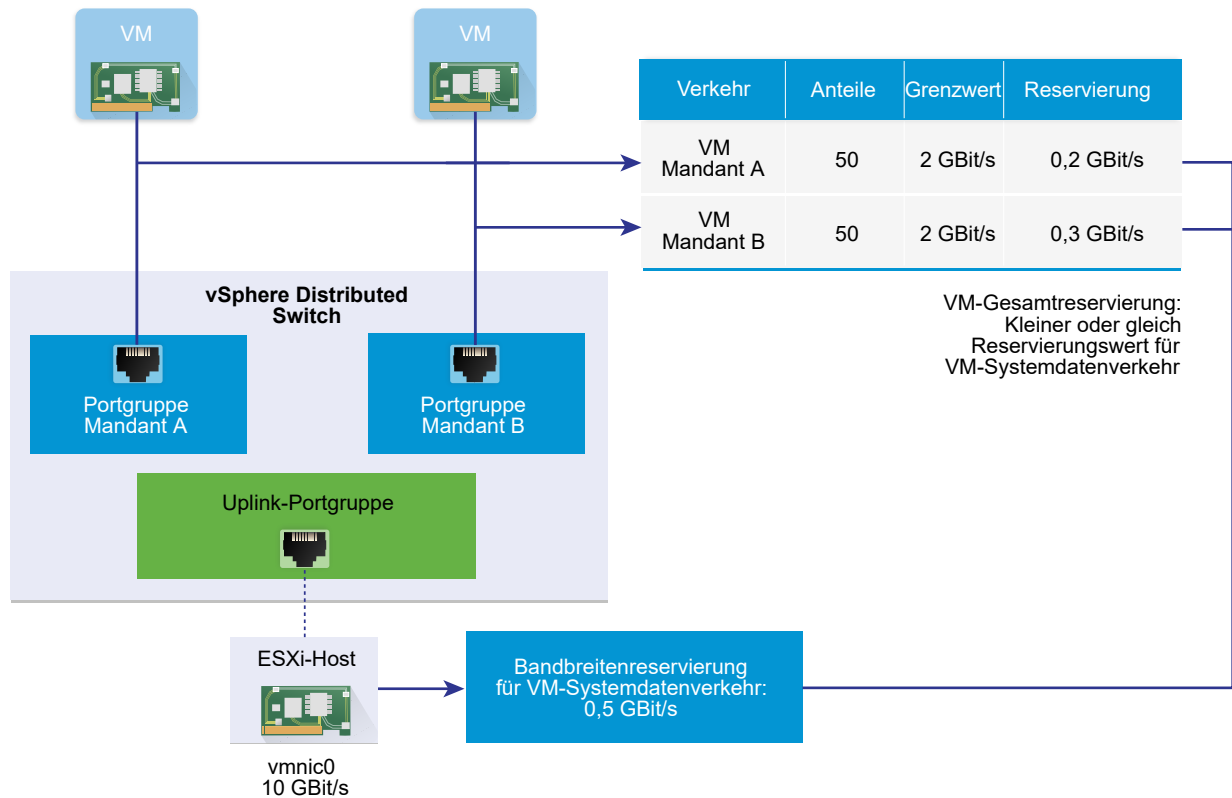
Bandbreitenbereitstellung an eine virtuelle Maschine auf dem Host

Um die Bandbreite zu garantieren, implementiert Network I/O Control eine Engine für die Datenverkehrsplatzierung, die aktiv wird, wenn für eine virtuelle Maschine eine Bandbreitenreservierung konfiguriert wird. Der Distributed Switch versucht, den Datenverkehr eines VM-Netzwerkadapters auf dem physischen Adapter zu platzieren, der die erforderliche Bandbreite liefern kann und sich im Bereich der aktiven Teaming-Richtlinie befindet.

Die gesamte Bandbreitenreservierung der virtuellen Maschinen eines Hosts darf die reservierte Bandbreite, die für den Systemdatenverkehr der virtuellen Maschine konfiguriert ist, nicht überschreiten.

Der aktuelle Grenzwert und die Reservierung hängen auch von der Traffic-Shaping-Richtlinie für die verteilte Portgruppe ab, mit der der Adapter verbunden ist. Wenn z. B. ein VM-Netzwerkadapter ein Limit von 200 MBit/s benötigt und die durchschnittliche in der Traffic-Shaping-Richtlinie konfigurierte Bandbreite 100 MBit/s beträgt, dann ist 100 MBit/s der effektive Grenzwert.

Abbildung 11-3. Konfiguration der Bandbreitenzuteilung für einzelne virtuelle Maschinen.



Bandbreitenzuteilungsparameter für Datenverkehr virtueller Maschinen

Network I/O Control Version 3 teilt Bandbreite zu einzelnen virtuellen Maschinen auf der Grundlage der in den VM-Hardwareeinstellungen konfigurierten Anteilen, Reservierungen und Grenzwerten für die Netzwerkadapter zu.

Tabelle 11-4. Bandbreitenzuteilungsparameter für einen VM-Netzwerkadapter

Bandbreitenzuteilungsparameter	Beschreibung
Anteile	Die relative Priorität von 1 bis 100 des Datenverkehrs über diesen VM-Netzwerkadapter in Bezug auf die Kapazität des physischen Adapters, der den VM-Datenverkehr an das Netzwerk überträgt.
Reservierung	Die Mindestbandbreite in MBit/s, die der VM-Netzwerkadapter auf dem physischen Adapter empfangen muss.
Grenzwert	Die maximale Bandbreite auf dem VM-Netzwerkadapter für Datenverkehr an andere virtuelle Maschinen auf dem gleichen oder auf einem anderen Host.

Zugangssteuerung für Bandbreite virtueller Maschinen

Um sicherzustellen, dass für eine virtuelle Maschine genügend Bandbreite vorhanden ist, implementiert vSphere eine Zugangssteuerung auf Host- und Clusterebene, die auf der Bandbreitenreservierung und Teaming-Richtlinie basiert.

Bandbreitenzugangssteuerung in vSphere Distributed Switch

Wenn Sie eine virtuelle Maschine einschalten, überprüft die Network I/O Control-Funktion eines Distributed Switch, ob diese Bedingungen auf dem Host erfüllt sind.

- Ein physischer Adapter auf dem Host kann die Mindestbandbreite für die VM-Netzwerkadapter entsprechend der Teaming-Richtlinie und Reservierung bereitstellen.
- Die Reservierung für einen VM-Netzwerkadapter liegt unter dem freien Kontingent im Netzwerkressourcenpool.

Wenn Sie die Reservierung für einen Netzwerkadapter einer laufenden virtuellen Maschine ändern, überprüft Network I/O Control erneut, ob der zugeordnete Netzwerkressourcenpool die neue Reservierung erfüllen kann. Wenn der Pool nicht über ausreichend freies Kontingent verfügt, wird die Änderung nicht angewendet.

Führen Sie die folgenden Aufgaben durch, um die Zugangssteuerung in vSphere Distributed Switch zu verwenden:

- Konfigurieren Sie die Bandbreitenzuteilung für den Systemdatenverkehr der virtuellen Maschine auf dem Distributed Switch.
- Konfigurieren Sie einen Netzwerkressourcenpool mit einem Reservierungskontingent aus der Bandbreite, die für den Systemdatenverkehr der virtuellen Maschine konfiguriert wurde.
- Ordnen Sie den Netzwerkressourcenpool der verteilten Portgruppe zu, die die virtuellen Maschinen mit dem Switch verbindet.
- Konfigurieren Sie die Bandbreitenanforderungen einer virtuellen Maschine, die mit der Portgruppe verbunden ist.

Bandbreitenzugangssteuerung in vSphere DRS

Wenn Sie eine virtuelle Maschine einschalten, die sich in einem Cluster befindet, platziert vSphere DRS die virtuelle Maschine auf einem Host, der genügend Kapazität hat, um die für die virtuelle Maschine reservierte Bandbreite entsprechend der aktiven Teaming-Richtlinie zu garantieren.

vSphere DRS migriert eine virtuelle Maschine zu einem anderen Host, um die Bandbreitenreservierung der virtuellen Maschine in folgenden Situationen zu erfüllen:

- Die Reservierung wird zu einen Wert geändert, die vom anfänglichen Host nicht mehr erfüllt werden kann.
- Ein physischer Adapter, der Datenverkehr von der virtuellen Maschine überträgt, ist offline.

Führen Sie die folgenden Aufgaben durch, um Zugangssteuerung in vSphere DRS zu verwenden:

- Konfigurieren Sie die Bandbreitenzuteilung für den Systemdatenverkehr der virtuellen Maschine auf dem Distributed Switch.
- Konfigurieren Sie die Bandbreitenanforderungen einer virtuellen Maschine, die mit dem Distributed Switch verbunden ist.

Weitere Informationen über die Ressourcenverwaltung entsprechend den Bandbreitenanforderungen virtueller Maschinen finden Sie in der Dokumentation *Handbuch zur vSphere-Ressourcenverwaltung*.

Bandbreitenzugangssteuerung in vSphere HA

Wenn ein Host ausfällt oder isoliert wird, schaltet vSphere HA eine virtuelle Maschine auf einem anderen Host im Cluster entsprechend der Bandbreitenreservierung und Teaming-Richtlinie ein.

Führen Sie die folgenden Aufgaben durch, um die Zugangssteuerung in vSphere HA zu verwenden:

- Teilen Sie Bandbreite für den Systemdatenverkehr auf virtuellen Maschinen zu.
- Konfigurieren Sie die Bandbreitenanforderungen einer virtuellen Maschine, die mit dem Distributed Switch verbunden ist.

Weitere Informationen dazu, wie vSphere HA Failover basierend auf den Bandbreitenanforderungen virtueller Maschinen bereitstellt, finden Sie in der Dokumentation *Handbuch zur Verfügbarkeit in vSphere*.

Erstellen eines Netzwerkressourcenpools

Erstellen Sie Netzwerkressourcenpools auf einem vSphere Distributed Switch, um Bandbreite für eine Reihe virtueller Maschinen zu reservieren.

Ein Netzwerkressourcenpool stellt virtuellen Maschinen ein Reservierungskontingent bereit. Das Kontingent stellt einen Teil der Bandbreite dar, die für den Systemdatenverkehr der virtuellen Maschinen auf den physischen Adaptern, die mit dem Distributed Switch verbunden sind, reserviert wird. Sie können Bandbreite aus dem Kontingent für die virtuellen Maschinen zurückhalten, die dem Pool zugeordnet sind. Die Reservierung durch die Netzwerkadapter eingeschalteter VMs, die dem Pool zugeordnet sind, darf das Kontingent des Pools nicht überschreiten. Siehe [Info zur Zuteilung von Bandbreite zu virtuellen Maschinen](#).

Voraussetzungen

- Überprüfen Sie, ob der vSphere Distributed Switch die Version 6.0.0 oder höher aufweist.
- Überprüfen Sie, ob Network I/O Control für den Switch die Version 3 aufweist.
- Überprüfen Sie, ob Network I/O Control aktiviert ist. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).
- Überprüfen Sie, ob für den Systemdatenverkehr auf virtuellen Maschinen eine Bandbreitenreservierung konfiguriert ist. Siehe [Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Ressourcenzuteilung**.
- 3 Klicken Sie auf **Netzwerkressourcenpools**.
- 4 Klicken Sie auf das Symbol **Add**.
- 5 (Optional) Geben Sie einen Namen und eine Beschreibung für den Netzwerkressourcenpool ein.
- 6 Geben Sie einen Wert für **Reservierungskontingent** in MBit/s aus der freien Bandbreite ein, die für den Systemdatenverkehr der virtuellen Maschinen reserviert ist.

Das maximale Kontingent, das Sie dem Pool zuweisen können, wird anhand der folgenden Formel bestimmt:

```
max reservation quota = aggregated reservation for vm system traffic - quotas of the other resource pools
```

wo

- `aggregated reservation for vm system traffic` = konfigurierte Bandbreitenreservierung für den Systemdatenverkehr der virtuellen Maschine auf jeder pNIC * Anzahl der mit dem Distributed Switch verbundenen pNICs
- `quotas of the other pools` = Summe der Reservierungskontingente der anderen Netzwerkressourcenpools

- 7 Klicken Sie auf **OK**.

Nächste Schritte

Fügen Sie dem Netzwerkressourcenpool eine oder mehrere verteilte Portgruppen hinzu, damit Sie Bandbreite zu einzelnen virtuellen Maschinen aus dem Kontingent des Pools zuteilen können. Siehe [Hinzufügen einer verteilten Portgruppe zu einem Netzwerkressourcenpool](#).

Hinzufügen einer verteilten Portgruppe zu einem Netzwerkressourcenpool

Fügen Sie eine verteilte Portgruppe zu einem Netzwerkressourcenpool hinzu, damit Sie den virtuellen Maschinen, die mit der Portgruppe verbunden sind, Bandbreite zuteilen können.

Um einen Netzwerkressourcenpool zu mehreren verteilten Portgruppen gleichzeitig zuzuweisen, können Sie die Ressourcenzuteilungsrichtlinie im Assistenten **Verteilte Portgruppen verwalten** verwenden. Siehe [Verwalten von Richtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch](#).

Network I/O Control weist den virtuellen Maschinen, die der verteilten Portgruppe zugeordnet sind, Bandbreite entsprechend dem implementierten Modell in der Network I/O Control-Version zu, die auf dem Distributed Switch aktiv ist. Siehe [Info zu vSphere Network I/O Control Version 3](#).

Voraussetzungen

- Überprüfen Sie, ob der vSphere Distributed Switch die Version 5.1 oder höher aufweist.
- Überprüfen Sie, ob Network I/O Control aktiviert ist. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).

Verfahren

- 1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**.
- 2 Wählen Sie die verteilte Portgruppe aus und klicken Sie auf **Einstellungen der verteilten Portgruppe bearbeiten**.
- 3 Klicken Sie im Dialogfeld „Einstellungen bearbeiten“ auf die Registerkarte **Allgemein**.
- 4 Wählen Sie im Dropdown-Menü **Netzwerkressourcenpool** den Netzwerkressourcenpool aus und klicken Sie auf **OK**.

Wenn der Distributed Switch keine Netzwerkressourcenpools enthält, wird nur die Option **(Standard)** im Dropdown-Menü angezeigt.

Konfigurieren der Bandbreitenzuteilung für eine virtuelle Maschine

Sie können die Bandbreitenzuteilung für einzelne virtuelle Maschinen konfigurieren, die mit einer verteilten Portgruppe verbunden sind. Verwenden Sie Anteils-, Reservierungs- und Grenzwerteinstellungen für die Bandbreite.

Voraussetzungen

- Überprüfen Sie, ob der vSphere Distributed Switch die Version 6.0.0 oder höher aufweist.
- Überprüfen Sie, ob Network I/O Control für den Switch die Version 3 aufweist.
- Überprüfen Sie, ob Network I/O Control aktiviert ist. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).
- Überprüfen Sie, ob für den Systemdatenverkehr auf virtuellen Maschinen eine Bandbreitenreservierung konfiguriert ist. Siehe [Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr](#).

Verfahren

- 1 Ermitteln Sie die virtuelle Maschine im vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus der Liste aus.
- 2 Wählen Sie auf der Registerkarte **Verwalten** der virtuellen Maschine **Einstellungen > VM-Hardware** aus.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Erweitern Sie den Abschnitt **X** des Netzwerkadapters für den VM-Netzwerkadapter.
- 5 Wenn Sie die Bandbreitenzuteilung für einen neuen VM-Netzwerkadapter konfigurieren möchten, wählen Sie im Dropdown-Menü **Neues Gerät** die Option **Netzwerk** und klicken Sie auf **Hinzufügen**.

In einem Bereich „Neues Netzwerk“ werden Optionen für die Bandbreitenzuteilung und andere Netzwerkadaptereinstellungen angezeigt.

- 6 Wenn der VM-Netzwerkadapter nicht mit der verteilten Portgruppe verbunden ist, wählen Sie die Portgruppe aus dem Dropdown-Menü neben dem Netzwerkadapter **X** oder der Bezeichnung „Neues Netzwerk“ aus.

Die Einstellungen für **Anteile**, **Reservierung** und **Grenzwert** werden für den VM-Netzwerkadapter angezeigt.

- 7 Legen Sie im Dropdown-Menü **Anteile** die relative Priorität des Datenverkehrs von dieser virtuellen Maschine als anteilige Kapazität des verbundenen physischen Adapters fest.

Network I/O Control wendet die konfigurierten Anteile an, wenn ein physischer Adapter ausgelastet ist.

Sie können eine Option auswählen, um einen vordefinierten Wert festzulegen. Sie können aber auch **Benutzerdefiniert** auswählen und eine Zahl zwischen 1 und 100 eingeben, um einen anderen Anteil festzulegen.

- 8 Reservieren Sie im Textfeld **Reservierung** die Mindestbandbreite, die für den VM-Netzwerkadapter verfügbar sein muss, wenn die virtuelle Maschine eingeschaltet ist.

Wenn Sie Bandbreite mithilfe eines Netzwerkressourcenpools bereitstellen, darf die Reservierung von den Netzwerkadaptern der eingeschalteten VMs, die dem Pool zugeordnet sind, das Kontingent des Pools nicht überschreiten.

Falls vSphere DRS aktiviert ist, müssen Sie zum Einschalten der virtuellen Maschine sicherstellen, dass die Reservierung von allen VM-Netzwerkadaptern auf dem Host nicht die Bandbreite überschreitet, die für VM-Systemdatenverkehr auf den physischen Adaptern des Hosts reserviert ist.

- 9 Legen Sie im Textfeld **Grenzwert** einen Grenzwert für die Bandbreite fest, die vom VM-Netzwerkadapter verbraucht werden kann.

- 10 Klicken Sie auf **OK**.

Ergebnisse

Netzwerk

I/O Control teilt die Bandbreite, die Sie für den Netzwerkadapter der virtuellen Maschine reserviert haben, aus dem Reservierungskontingent des Netzwerkressourcenpools zu.

Konfigurieren der Bandbreitenzuteilung auf mehreren virtuellen Maschinen

Konfigurieren Sie in einem Vorgang die Bandbreitenzuteilung für mehrere virtuelle Maschinen, die mit einem bestimmten Netzwerkressourcenpool verbunden sind, z. B. nach dem Upgrade von Network I/O Control auf Version 3.

Voraussetzungen

- Überprüfen Sie, ob der vSphere Distributed Switch die Version 6.0.0 oder höher aufweist.
- Überprüfen Sie, ob Network I/O Control für den Switch die Version 3 aufweist.
- Überprüfen Sie, ob Network I/O Control aktiviert ist. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).
- Überprüfen Sie, ob für den Systemdatenverkehr auf virtuellen Maschinen eine Bandbreitenreservierung konfiguriert ist. Siehe [Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr](#).
- Überprüfen Sie, dass die virtuellen Maschinen über die verbundenen verteilten Portgruppen einem bestimmten Netzwerkressourcenpool zugeordnet sind. Siehe [Hinzufügen einer verteilten Portgruppe zu einem Netzwerkressourcenpool](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Ressourcenzuteilung**.

3 Klicken Sie auf **Netzwerkressourcenpools**.

4 Wählen Sie einen Netzwerkressourcenpool aus.

5 Klicken Sie auf **Virtuelle Maschinen**.

Es wird eine Liste der VM-Netzwerkadapter angezeigt, die mit dem ausgewählten Netzwerkressourcenpool verbunden sind.

6 Wählen Sie die VM-Netzwerkadapter aus, deren Einstellungen Sie konfigurieren möchten, und klicken Sie auf **Bearbeiten**.

7 Legen Sie im Dropdown-Menü **Anteile** die relative Priorität des Datenverkehrs dieser virtuellen Maschinen im Bereich der physischen Adapter, die den Datenverkehr übertragen, fest.

Network I/O Control wendet die konfigurierten Anteile an, wenn ein physischer Adapter ausgelastet ist.

8 Reservieren Sie im Textfeld **Reservierung** eine minimale Bandbreite, die für jeden VM-Netzwerkadapter verfügbar sein muss, wenn die virtuellen Maschinen eingeschaltet werden.

Wenn Sie Bandbreite mithilfe eines Netzwerkressourcenpools bereitstellen, darf die Reservierung von den Netzwerkadaptern der eingeschalteten VMs, die dem Pool zugeordnet sind, das Kontingent des Pools nicht überschreiten.

9 Legen Sie im Textfeld **Grenzwert** einen Grenzwert für die Bandbreite fest, die jeder VM-Netzwerkadapter verwenden kann.

10 Klicken Sie auf **OK**.

Ändern des Kontingents eines Netzwerkressourcenpools

Sie können das Bandbreitenkontingent ändern, das für mit einem Satz verteilter Portgruppen verbundene virtuelle Maschinen reserviert werden kann.

Voraussetzungen

- Überprüfen Sie, ob der vSphere Distributed Switch die Version 6.0.0 oder höher aufweist.
- Überprüfen Sie, ob Network I/O Control für den Switch die Version 3 aufweist.
- Überprüfen Sie, ob Network I/O Control aktiviert ist. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).
- Überprüfen Sie, ob für den Systemdatenverkehr auf virtuellen Maschinen eine Bandbreitenreservierung konfiguriert ist. Siehe [Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr](#).

Verfahren

1 Navigieren Sie im vSphere Web Client zum Distributed Switch.

2 Klicken Sie auf der Registerkarte **Verwalten** auf **Ressourcenzuteilung**.

- 3 Klicken Sie auf **Netzwerkressourcenpools**.
- 4 Wählen Sie in der Liste einen Netzwerkressourcenpool aus, und klicken Sie auf **Bearbeiten**.
- 5 Geben Sie im Textfeld **Reservierungskontingent** das Bandbreitenkontingent für virtuelle Maschinen aus der Aggregation für freie Bandbreite ein, das für Systemdatenverkehr für virtuelle Maschinen auf allen physischen Adaptern des Switches reserviert ist.
- 6 Klicken Sie auf **OK**.

Entfernen von verteilten Portgruppen aus einem Netzwerkressourcenpool

Damit keine Bandbreite aus dem Reservierungskontingent eines Netzwerkressourcenpools mehr zu virtuellen Maschinen zugeteilt wird, entfernen Sie die Zuordnung zwischen der Portgruppe, über die die virtuellen Maschinen verbunden sind, und dem Pool.

Verfahren

- 1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
 - a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Verteilte Portgruppen**.
- 2 Wählen Sie die verteilte Portgruppe aus und klicken Sie auf **Einstellungen der verteilten Portgruppe bearbeiten**.
- 3 Klicken Sie im Dialogfeld „Einstellungen bearbeiten“ auf **Allgemein**.
- 4 Wählen Sie im Dropdown-Menü **Netzwerkressourcenpool** die Option **(Standard)** und klicken Sie auf **OK**.

Ergebnisse

Die verteilte Portgruppe wird dem Standard-Netzwerkressourcenpool der VM zugeordnet.

Löschen eines Netzwerkressourcenpools

Löschen Sie einen Netzwerkressourcenpool, der nicht mehr verwendet wird.

Voraussetzungen

Entkoppeln Sie den Netzwerkressourcenpool von allen verteilten Portgruppen. Siehe [Entfernen von verteilten Portgruppen aus einem Netzwerkressourcenpool](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Ressourcenzuteilung**.
- 3 Klicken Sie auf **Netzwerkressourcenpools**.

- 4 Wählen Sie einen Netzwerkressourcenpool aus und klicken Sie auf **Entfernen**.
- 5 Klicken Sie auf **Ja**, um den Ressourcenpool zu entfernen.

Verschieben eines physischen Adapters aus dem Bereich von Network I/O Control

Unter bestimmten Umständen müssen Sie evtl. physische Adapter mit geringer Kapazität aus dem Bandbreitenzuteilungsmodell von Network I/O Control Version 3 ausschließen.

Wenn z. B. die Bandbreitenzuteilung auf einem vSphere Distributed Switch auf Netzwerkkarten mit mehr als 10 GbE zugeschnitten ist, können Sie möglicherweise keine Netzwerkkarte mit 1GbE zum Switch hinzufügen, da diese die höheren Zuteilungsanforderungen der Netzwerkkarten mit 10 GbE nicht erfüllen kann.

Voraussetzungen

- Stellen Sie sicher, dass der Host ESXi 6.0 und höher ausführt.
- Überprüfen Sie, ob der vSphere Distributed Switch die Version 6.0.0 oder höher aufweist.
- Überprüfen Sie, ob Network I/O Control für den Switch die Version 3 aufweist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen**.
- 3 Erweitern Sie „System“ und klicken Sie auf **Erweiterte Systemeinstellungen**.
- 4 Legen Sie die physischen Adapter, die außerhalb des Bereichs von Network I/O Control eingesetzt werden sollen, als kommagetrennte Liste für den `Net.IOControlPnicOptOut`-Parameter fest.

Beispiel: `vmnic0,vmnic3`

- 5 Klicken Sie auf **OK**, damit die Änderungen wirksam werden.

Arbeiten mit Network I/O Control Version 2

Auf einem vSphere Distributed Switch 5.x bzw. einem vSphere Distributed Switch, für das ein Upgrade auf 6.0 durchgeführt wurde und das nicht über die verbesserte Version Network I/O Control Version 3 verfügt, können Sie sicherstellen, dass der Systemdatenverkehr und die virtuellen Maschinen die erforderliche Bandbreite für ihren Betrieb erhalten, indem Sie das Ressourcenpoolmodell von Network I/O Control Version 2 verwenden.

Netzwerkressourcenpools in Network I/O Control Version 2

In Network I/O Control Version 2 unterstützt der Distributed Switch-Datenverkehr zwei Arten von Netzwerkressourcenpools:

- **System-Netzwerkressourcenpools** Vordefinierte Pools für die Steuerung der Netzwerkbandbreite, die an die wichtigsten Systemdatenverkehrstypen bereitgestellt werden: Fault Tolerance-, iSCSI-, vMotion-, Verwaltungs-, vSphere Replication-, NFS- und VM-Datenverkehr.
- **Benutzerdefinierte Netzwerkressourcenpools** Benutzerdefinierte Pools für VM-Datenverkehr. Die Einstellungen in einem benutzerdefinierten Ressourcenpool werden auf virtuelle Maschinen angewendet, nachdem Sie einen benutzerdefinierten Ressourcenpool einer verteilten Portgruppe zugewiesen haben.

Bandbreitenzuteilungsparameter für Netzwerkressourcenpools in Network I/O Control Version 2

Bandbreitenzuteilungsparameter	Beschreibung
Anteile	<p>Wenn ein physischer Adapter ausgelastet ist, erhalten die virtuellen Maschinen bzw. die VMkernel-Adapter, die den Adapter verwenden, Bandbreite vom externen Netzwerk entsprechend den Anteilen, die im Netzwerkressourcenpool konfiguriert wurden.</p> <p>Die einem Netzwerkressourcenpool zugewiesenen Anteile physischer Adapter bestimmen den Anteil der insgesamt verfügbaren Bandbreite, der für den diesem Netzwerkressourcenpool zugewiesenen Datenverkehr garantiert ist. Der tatsächliche Anteil an Bandbreite für ausgehenden Datenverkehr für einen Netzwerkressourcenpool wird durch die Anteile des Netzwerkressourcenpools sowie dadurch bestimmt, welche anderen Netzwerkressourcenpools aktiv Daten übertragen. Beispielsweise weisen Sie dem vSphere FT- und dem iSCSI-Datenverkehr 100 Anteile zu, während jeder der anderen Netzwerkressourcenpools 50 Anteile erhält. Ein physischer Adapter ist für das Versenden von vSphere Fault Tolerance-, iSCSI- und Verwaltungsdatenverkehr konfiguriert. Zu einem bestimmten Zeitpunkt sind vSphere Fault Tolerance und iSCSI die aktiven Datenverkehrstypen auf dem physischen Adapter und verbrauchen dessen Kapazität. Jeder Datenverkehr erhält 50 % der verfügbaren Bandbreite. Zu einem anderen Zeitpunkt ist der Adapter durch alle drei Datenverkehrstypen ausgelastet. In diesem Fall erhalten vSphere FT-Datenverkehr und iSCSI-Datenverkehr 40 % der Adapterkapazität, und vMotion erhält 20 %.</p> <p>Hinweis Die Ressourcenpool-Anteile für den iSCSI-Datenverkehr gelten nicht für iSCSI-Datenverkehr auf einem abhängigen Hardware-iSCSI-Adapter.</p>
Grenzwert	Der Hostgrenzwert eines Netzwerkressourcenpools ist die maximale Bandbreite, die der dem Netzwerkressourcenpool zugeordnete Datenverkehr an einem physischen Adapter verbrauchen kann.
QoS-Tag	Durch Zuweisen eines QoS-Prioritäts-Tags zu einem Netzwerkressourcenpool wird ein 802.1p-Tag (CoS) für alle ausgehenden Pakete angewendet, die dem Netzwerkressourcenpool zugeordnet sind. So können Sie bestimmten Datenverkehr markieren, damit er von Netzwerkgeräten wie Switches mit höherer Priorität bearbeitet werden kann.

Erstellen eines Netzwerkressourcenpools in Network I/O Control, Version 2

Erstellen Sie benutzerdefinierte Netzwerkressourcenpools, um die Bandbreitenzuteilung anzupassen, wenn der über einen physischen Netzwerkadapter übertragene Datenverkehr sehr hoch ist.

Voraussetzungen

- Überprüfen Sie, ob der vSphere Distributed Switch die Version 5.1 oder höher aufweist.
- Überprüfen Sie, ob Network I/O Control für den Distributed Switch die Version 2 aufweist.
- Aktivieren Sie Network I/O Control auf dem Distributed Switch. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Ressourcenzuteilung**.
- 3 Klicken Sie auf **Neu**.
- 4 Geben Sie einen Namen und optional eine Beschreibung für den Netzwerkressourcenpool ein.
- 5 Geben Sie im Textfeld **Grenzwert** den Bandbreitengrenzwert in MBit/s für den Netzwerkressourcenpool bezüglich der verbundenen physischen Adapter auf dem Host ein.
Standardmäßig gilt keine Beschränkung des Datenverkehrs.

- 6 Geben Sie im Dropdown-Menü **Physischer Adapter - Anteile** die Anteile der physischen Adapterkapazität ein, über die die virtuellen Maschinen oder die VMkernel-Adapter, die dem Netzwerkressourcenpool zugeordnet sind, verfügen.

Network I/O Control wendet die konfigurierten Anteile an, wenn der verbundene physische Adapter ausgelastet ist.

Sie können eine Option auswählen, um einen vordefinierten Wert festzulegen. Sie können aber auch **Benutzerdefiniert** auswählen und eine Zahl zwischen 1 und 100 eingeben, um einen anderen Anteil festzulegen.

- 7 (Optional) Wählen Sie im Dropdown-Menü **CoS-Prioritäts-Tag** den QoS-Tag zum Markieren des Datenverkehrs des Systems bzw. der virtuellen Maschine aus, der dem Netzwerkressourcenpool zugeordnet ist, und klicken Sie auf **OK**.

Das QoS-Prioritäts-Tag ist ein IEEE 802.1p (CoS)-Tag zum Definieren der Priorität des Datenverkehrs von den virtuellen Maschinen für den Ressourcenpool in Schicht 2 des Netzwerkprotokoll-Stacks.

Nächste Schritte

Ordnen Sie einen oder mehrere verteilte Portgruppen dem Netzwerkressourcenpool zu, um die Einstellungen für die Bandbreitenkontrolle auf virtuelle Maschinen anzuwenden. Siehe [Hinzufügen einer verteilten Portgruppe zu einem Netzwerkressourcenpool](#).

Bearbeiten der Einstellungen eines Netzwerkressourcenpools in Network I/O Control, Version 2

Bearbeiten Sie die Einstellungen eines System- oder benutzerdefinierten Netzwerkressourcenpools, um die Priorität des Datenverkehrs in Zusammenhang mit dem Pool in Network I/O Control, Version 2, zu ändern.

Voraussetzungen

- Überprüfen Sie, ob der vSphere Distributed Switch die Version 5.1 oder höher aufweist.
- Überprüfen Sie, ob Network I/O Control für den Distributed Switch die Version 2 aufweist.
- Aktivieren Sie Network I/O Control auf dem Distributed Switch. Siehe [Aktivieren von Network I/O Control auf einem vSphere Distributed Switch](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Ressourcenzuteilung**.
- 3 Wählen Sie in der Liste einen Netzwerkressourcenpool aus, und klicken Sie auf **Bearbeiten**.
- 4 Legen Sie im Textfeld **Grenzwert** einen Grenzwert für die Bandbreite fest, die vom VM-Netzwerkadapter verbraucht werden kann.
- 5 Geben Sie im Dropdown-Menü **Physischer Adapter - Anteile** die Anteile der physischen Adapterkapazität ein, über die die virtuellen Maschinen oder die VMkernel-Adapter, die dem Netzwerkressourcenpool zugeordnet sind, verfügen.

Network I/O Control wendet die konfigurierten Anteile an, wenn der verbundene physische Adapter ausgelastet ist.

Sie können eine Option auswählen, um einen vordefinierten Wert festzulegen. Sie können aber auch **Benutzerdefiniert** auswählen und eine Zahl zwischen 1 und 100 eingeben, um einen anderen Anteil festzulegen.

- 6 (Optional) Wählen Sie im Dropdown-Menü **CoS-Prioritäts-Tag** den QoS-Tag zum Markieren des Datenverkehrs des Systems bzw. der virtuellen Maschine aus, der dem Netzwerkressourcenpool zugeordnet ist, und klicken Sie auf **OK**.

Das QoS-Prioritäts-Tag ist ein IEEE 802.1p (CoS)-Tag zum Definieren der Priorität des Datenverkehrs von den virtuellen Maschinen für den Ressourcenpool in Schicht 2 des Netzwerkprotokoll-Stacks.

Ergebnisse

Network I/O Control, Version 2, wendet die neuen Einstellungen für die Bandbreitenkontrolle auf den VMkernel und die VM-Adapter in den verteilten Portgruppen an, die dem Netzwerkressourcenpool zugeordnet sind.

Verwaltung von MAC-Adressen

12

MAC-Adressen werden auf Schicht 2 (Sicherungsschicht) des Netzwerkprotokoll-Stacks zum Übertragen von Frames an den Empfänger verwendet. In vSphere generiert vCenter Server MAC-Adressen für Adapter der virtuellen Maschine und für VMkernel-Adapter. Sie können aber auch manuell Adressen zuweisen.

Jedem Hersteller von Netzwerkadaptern wird ein eindeutiges, drei Byte großes Präfix zugewiesen, das als OUI (Organizationally Unique Identifier, eindeutiger Bezeichner für Organisationen) genannt wird und das der Hersteller zur Generierung eindeutiger MAC-Adressen verwenden kann.

VMware unterstützt mehrere Adresszuteilungsmechanismen mit jeweils einem separaten OUI:

- Generierte MAC-Adressen
 - Von vCenter Server zugewiesen
 - Vom ESXi-Host zugewiesen
- Manuell festgelegte MAC-Adressen
- Für ältere virtuelle Maschinen generiert (wird jedoch bei ESXi nicht mehr verwendet)

Wenn Sie den Netzwerkadapter einer ausgeschalteten virtuellen Maschine neu konfigurieren, zum Beispiel durch das Ändern des automatischen MAC-Adressen-Zuteilungstyps oder durch das Festlegen einer statischen MAC-Adresse, löst vCenter Server alle MAC-Adressenkonflikte, bevor die Adapterneukonfiguration übernommen wird.

Dieses Kapitel enthält die folgenden Themen:

- [Zuweisen von MAC-Adressen in vCenter Server](#)
- [Generierung von MAC-Adressen auf ESXi-Hosts](#)
- [Festlegen einer statischen MAC-Adresse für eine virtuelle Maschine](#)

Zuweisen von MAC-Adressen in vCenter Server

In vSphere 5.1 und höher gibt es mehrere Schemata für die automatische Zuteilung von MAC-Adressen in vCenter Server. Sie können das Schema auswählen, das für Ihre Anforderungen an die Duplizierung von MAC-Adressen, OUI-Anforderungen für lokal verwaltete oder universal verwaltete Adressen usw. am besten geeignet ist.

In vCenter Server gibt es die folgenden Schemata für die Generierung von MAC-Adressen:

- VMware OUI-Zuteilung, Standardzuteilung
- Präfixbasierte Zuteilung
- Bereichsbasierte Zuteilung

Nachdem die MAC-Adresse generiert wurde, ändert sie sich nur, wenn die virtuelle Maschine einen MAC-Adressenkonflikt mit einer anderen registrierten virtuellen Maschine hat. Die MAC-Adresse wird in der Konfigurationsdatei der virtuellen Maschine gespeichert.

Hinweis Wenn Sie ungültige präfix- oder bereichsbasierte Zuteilungswerte verwenden, wird ein Fehler in der Datei `vpd.log` protokolliert. vCenter Server teilt während der Bereitstellung einer virtuellen Maschine keine MAC-Adressen zu.

Verhindern von MAC-Adressenkonflikten

Die MAC-Adresse einer ausgeschalteten virtuellen Maschine wird nicht mit MAC-Adressen ausgeführter oder angehaltener virtueller Maschinen abgeglichen.

Wenn eine virtuelle Maschine wieder eingeschaltet wird, erhält sie möglicherweise eine andere MAC-Adresse. Diese Änderung ist möglicherweise auf einen Adressenkonflikt mit einer anderen virtuellen Maschine zurückzuführen. Während diese virtuelle Maschine ausgeschaltet war, wurde ihre MAC-Adresse einer anderen virtuellen Maschine zugeteilt, als diese eingeschaltet wurde.

Wenn Sie den Netzwerkadapter einer ausgeschalteten virtuellen Maschine neu konfigurieren, zum Beispiel durch das Ändern des automatischen MAC-Adressen-Zuteilungstyps oder durch das Festlegen einer statischen MAC-Adresse, löst vCenter Server MAC-Adressenkonflikte, bevor die Adapterneukonfiguration übernommen wird.

Informationen zum Lösen von MAC-Adressenkonflikten finden Sie in der Dokumentation *vSphere-Fehlerbehebung*.

VMware-OUI-Zuteilung

Bei der VMware-Zuteilung des OUI (Organizationally Unique Identifier, eindeutiger Bezeichner für Organisationen) werden MAC-Adressen auf Grundlage des Standard-VMware-OUI `00:50:56` und der vCenter Server-ID zugeteilt.

Die VMware-Zuteilung des OUI ist das standardmäßige MAC-Adressen-Zuweisungsmodell für virtuelle Maschinen. Die Zuteilung funktioniert mit bis zu 64 vCenter Server-Instanzen, und jeder vCenter Server kann bis zu 64.000 eindeutige MAC-Adressen zuweisen. Das VMware-OUI-Zuteilungsschema ist für kleine Bereitstellungen geeignet.

MAC-Adressformat

Gemäß VMware-OUI-Zuteilungsschema hat eine MAC-Adresse das Format `00:50:56:XX:YY:ZZ`. Dabei stellt `00:50:56` den VMware-OUI dar, `XX` wird als $(80 + \text{vCenter Server-ID})$ berechnet, und `YY` und `ZZ` sind Zufallszahlen im zweistelligen Hexadezimalformat.

Die über die VMware-Zuteilung des OUI erstellten Adressen liegen im Bereich 00:50:56:80:YY:ZZ bis 00:50:56:BF:YY:ZZ.

Zuteilen von präfixbasierten MAC-Adressen

Auf ESXi-Hosts 5.1 und höher können Sie präfixbasierte Zuteilung verwenden, um eine andere OUI als den VMware-Standard 00:50:56 anzugeben oder um LAA-MAC-Adressen (Locally Administered Addresses) für einen größeren Adressraum einzugeben.

Mit der präfixbasierten MAC-Adresszuteilung werden die Einschränkungen der Standardzuteilung von VMware überwunden, um in größeren Bereitstellungen eindeutige Adressen bereitzustellen. Die Einführung eines LAA-Präfix führt zu einem sehr großen MAC-Adressraum (2^{46}), anstelle einer universell eindeutigen Adress-OUI, mit der nur 16 Millionen MAC-Adressen möglich sind.

Überprüfen Sie, dass die für die einzelnen vCenter Server-Instanzen bereitgestellten Präfixe im gleichen Netzwerk eindeutig sind. vCenter Server verlässt sich auf die Präfixe, um Duplizierungsprobleme bei MAC-Adressen zu verhindern. Informationen finden Sie in der Dokumentation *vSphere-Fehlerbehebung*.

Zuteilen von bereichsbasierten MAC-Adressen

Auf ESXi-Hosts 5.1 und höher können Sie die bereichsbasierte Zuteilung verwenden, um Bereiche von lokal verwalteten Adressen (Locally Administered Address, LAA) einzuschließen oder auszuschließen.

Legen Sie einen oder mehrere Bereiche fest, indem Sie MAC-Start- und -Endadressen eingeben (z. B. 02:50:68:00:00:02, 02:50:68:00:00:FF). MAC-Adressen werden nur in dem angegebenen Bereich generiert.

Sie können mehrere LAA-Bereiche festlegen und vCenter Server verfolgt die Anzahl der verwendeten Adressen für jeden Bereich. vCenter Server teilt MAC-Adressen vom ersten Bereich zu, in dem noch Adressen verfügbar sind. vCenter Server überprüft die MAC-Adresse auf Konflikte innerhalb des Bereiches.

Wenn Sie die bereichsbasierte Zuteilung verwenden, müssen Sie verschiedene Instanzen von vCenter Server mit Bereichen versehen, die einander nicht überlappen. vCenter Server erkennt keine Bereiche, die mit anderen vCenter Server-Instanzen kollidieren. Weitere Informationen zum Beheben von Problemen mit doppelten MAC-Adressen finden Sie in der *vSphere-Fehlerbehebung*-Dokumentation.

Zuweisen von MAC-Adressen

Verwenden Sie den vSphere Web Client, um präfixbasierte oder bereichsbasierte MAC-Adressenzuteilung zu aktivieren und die Zuteilungsparameter anzupassen.

Verwenden Sie zum Wechseln des Zuteilungstyps, z. B. von der VMware OUI-Zuteilung zur bereichsbasierten Zuteilung, den vSphere Web Client. Ist jedoch ein Schema präfixbasiert oder bereichsbasiert und Sie möchten zu einem anderen Zuteilungsschema wechseln, müssen Sie die Datei `vpzd.cfg` manuell bearbeiten und vCenter Server neu starten.

Wechseln zu oder Anpassen von bereichsbasierten oder präfixbasierten Zuteilungen

Durch den Wechsel von den standardmäßigen VMware OUI- zu bereichs- oder präfixbasierten MAC-Adressenzuteilungen über den vSphere Web Client können Sie in vSphere-Bereitstellungen Konflikte wegen doppelter MAC-Adressen vermeiden und beheben.

Ändern Sie das Zuteilungsschema von den standardmäßigen VMware OUI- in die bereichs- oder präfixbasierte Zuteilung durch Verwendung der **erweiterten Einstellungen**, die für die vCenter Server-Instanz im vSphere Web Client zur Verfügung stehen.

Bearbeiten Sie die Datei `vpzd.cfg` manuell, um von einer bereichs- oder präfixbasierten Zuteilung zurück zu einer VMware OUI-Zuteilung oder zwischen der bereichs- und der präfixbasierten Zuteilung zu wechseln. Weitere Informationen hierzu finden Sie unter [Festlegen und Ändern von Zuteilungstypen](#).

Hinweis Sie sollten die präfixbasierte MAC-Adressenzuteilung in vCenter Server 5.1- und ESXi 5.1-Hosts und höher verwenden.

Wenn eine vCenter Server 5.1-Instanz ESXi-Hosts vor der ESXi-Version 5.1 verwaltet, verwenden Sie die präfixbasierte MAC-Adressenzuteilung von VMware OUI. Virtuelle Maschinen, denen die nicht präfixbasierten MAC-Adressen von VMware OUI zugewiesen sind, können auf Hosts vor Version 5.1 nicht eingeschaltet werden. Diese Hosts überprüfen explizit, ob eine zugewiesene MAC-Adresse das VMware OUI-Präfix 00:50:56 verwendet.

Verfahren

- 1 Navigieren Sie in vSphere Web Client zu einer vCenter Server-Instanz.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und wählen Sie **Einstellungen > Erweiterte Einstellungen** aus.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Fügen Sie Parameter für den Zielzuteilungstyp hinzu bzw. bearbeiten Sie diese.

Verwenden Sie nur einen Zuteilungstyp.

- Ändern Sie die Zuteilung in die präfixbasierte Zuteilung.

Schlüssel	Beispielwert
<code>config.vpzd.macAllocScheme.prefixScheme.prefix</code>	005026
<code>config.vpzd.macAllocScheme.prefixScheme.prefixLength</code>	23

`prefix` und `prefixLength` legen den Bereich der MAC-Adressenpräfixe für neu hinzugefügte vNICs fest. `prefix` stellt die Start-OUI der MAC-Adressen im Verhältnis zur vCenter Server-Instanz dar, und `prefixLength` legt die Länge des Präfixes in Bit fest.

Beispiel: Die Einstellungen aus der Tabelle ergeben VM-NIC-MAC-Adressen, die mit 00:50:26 oder 00:50:27 beginnen.

- Ändern Sie die Zuteilung in die bereichsbasierte Zuteilung.

Schlüssel	Beispielwert
<code>config.vpxd.macAllocScheme.rangeScheme.range[X].begin</code>	005067000000
<code>config.vpxd.macAllocScheme.rangeScheme.range[X].end</code>	005067ffffff

Das `X` in `range[X]` ist die Sequenznummer des Bereichs. Beispiel: 0 in `range[0]` steht für die Zuteilungseinstellungen des ersten Bereichs der MAC-Adressenzuteilung.

- 5 Klicken Sie auf **OK**.

Festlegen und Ändern von Zuteilungstypen

Wenn Sie von bereichs- oder präfixbasierter Zuteilung auf die VMware-OUI-Zuteilung wechseln, müssen Sie den Zuteilungstyp in der `vpxd.cfg`-Datei angeben und vCenter Server neu starten.

Voraussetzungen

Entscheiden Sie sich für einen Zuteilungstyp, bevor Sie die Datei `vpxd.cfg` ändern. Hinweise zu Zuteilungstypen finden Sie unter [Zuweisen von MAC-Adressen in vCenter Server](#).

Verfahren

- 1 Navigieren Sie auf der Hostmaschine von vCenter Server zu dem Verzeichnis, in dem die Konfigurationsdatei gespeichert ist:
 - Bei einem Windows Server-Betriebssystem finden Sie dieses Verzeichnis unter `C:\ProgramData\VMware\CIS\cfg\vmware-vpx`.
 - Bei der vCenter Server Appliance finden Sie dieses Verzeichnis unter `/etc/vmware-vpx`.
- 2 Öffnen Sie die `vpxd.cfg`-Datei.

- 3 Entscheiden Sie, welchen Zuteilungstyp Sie verwenden möchten, und geben Sie den entsprechenden XML-Code in die Datei ein, um den Zuteilungstyp zu konfigurieren.

Nachstehend finden Sie Beispiele für zu benutzenden XML-Code.

Hinweis Verwenden Sie nur einen Zuteilungstyp.

◆ VMware-OUI-Zuteilung

```
<vpzd>
  <macAllocScheme>
    <VMwareOUI>true</VMwareOUI>
  </macAllocScheme>
</vpzd>
```

◆ Präfixbasierte Zuteilung

```
<vpzd>
  <macAllocScheme>
    <prefixScheme>
      <prefix>005026</prefix>
      <prefixLength>23</prefixLength>
    </prefixScheme>
  </macAllocScheme>
</vpzd>
```

◆ Bereichsbasierte Zuteilung

```
<vpzd>
  <macAllocScheme>
    <rangeScheme>
      <range id="0">
        <begin>005067000001</begin>
        <end>005067000001</end>
      </range>
    </rangeScheme>
  </macAllocScheme>
</vpzd>
```

- 4 Speichern Sie die Datei `vpzd.cfg`.
- 5 Starten Sie das vCenter Server-System neu.

Generierung von MAC-Adressen auf ESXi-Hosts

Ein ESXi-Host generiert die MAC-Adresse für einen VM-Adapter, wenn der Host nicht mit vCenter Server verbunden ist. Solche Adressen haben einen separaten VMware-OUI zur Vermeidung von Konflikten.

Der ESXi-Host generiert die MAC-Adresse für einen VM-Adapter in einem der folgenden Fälle:

- Der Host ist mit vCenter Server verbunden.

- Die Konfigurationsdatei der virtuellen Maschine enthält keine MAC-Adresse und Informationen zum Zuteilungstyp für MAC-Adressen.

MAC-Adressformat

Der Host generiert MAC-Adressen, die aus dem VMware-OUI 00:0c:29 und mindestens den letzten drei Oktetten im Hexadezimalformat der UUID der virtuellen Maschine bestehen. Die UUID der virtuellen Maschine basiert auf einem Hash, der unter Verwendung der UUID der physischen ESXi-Maschine und des Pfads zur Konfigurationsdatei (.vmx) der virtuellen Maschine berechnet wird.

Verhindern von MAC-Adressenkonflikten

Alle MAC-Adressen, die Netzwerkadaptern von ausgeführten oder angehaltenen virtuellen Maschinen auf einem bestimmten physischen Computer zugewiesen wurden, werden bezüglich Konflikten nachverfolgt.

Wenn Sie eine virtuelle Maschine mit einer hostgenerierten MAC-Adresse von einem vCenter Server zum anderen importieren, wählen Sie die Option **Ich habe sie kopiert**, wenn Sie die virtuelle Maschine einschalten, um die Adresse zu regenerieren und mögliche Konflikte auf dem Ziel-vCenter Server oder zwischen den vCenter Server-Systemen zu vermeiden.

Festlegen einer statischen MAC-Adresse für eine virtuelle Maschine

In den meisten Netzwerkbereitstellungen sind generierte MAC-Adressen ein guter Ansatz. Möglicherweise müssen Sie jedoch eine statische MAC-Adresse für einen VM-Adapter mit eindeutigem Wert festlegen.

Die folgenden Fälle verdeutlichen, in welchen Fällen Sie möglicherweise eine statische MAC-Adresse festlegen müssen:

- VM-Adapter auf unterschiedlichen physischen Hosts verwenden das gleiche Subnetz, und ihnen wurde die gleiche MAC-Adresse zugewiesen, wodurch ein Konflikt entsteht.
- Stellen Sie sicher, dass ein VM-Adapter immer die gleiche MAC-Adresse hat.

Standardmäßig verwendet VMware den OUI (Organizationally Unique Identifier, eindeutiger Bezeichner für Organisationen) 00:50:56 für manuell generierte Adressen, es werden jedoch alle eindeutigen manuell erstellten Adressen unterstützt.

Hinweis Stellen Sie sicher, dass keine anderen Nicht-VMware-Geräte Adressen verwenden, die VMware-Komponenten zugewiesen sind. Beispiel: In demselben Subnetz sind physische Server eingerichtet, die 11:11:11:11:11:11, 22:22:22:22:22:22 als statische MAC-Adressen verwenden. Die physischen Server gehören nicht zur vCenter Server-Bestandsliste und vCenter Server kann keine Adressenkollision ermitteln.

VMware-OUI in statischen MAC-Adressen

Standardmäßig tragen statische MAC-Adressen den VMware-OUI (Organizationally Unique Identifier, eindeutiger Bezeichner für Organisationen) als Präfix. Der Bereich freier Adressen, die vom VMware-OUI zur Verfügung gestellt werden, ist jedoch eingeschränkt.

Wenn Sie einen VMware-OUI verwenden möchten, wird ein Teil des Bereichs zur Verwendung durch vCenter Server, physische Host-Netzwerkkarten, virtuelle Netzwerkkarten und zur zukünftigen Verwendung reserviert.

Sie können eine statische MAC-Adresse, die das VMware-OUI-Präfix enthält, entsprechend dem folgenden Format festlegen:

```
00:50:56:XX:YY:ZZ
```

Dabei ist *XX* eine gültige hexadezimale Zahl zwischen 00 und 3F, und *YY* und *ZZ* sind gültige hexadezimale Zahlen zwischen 00 und FF. Um Konflikte mit MAC-Adressen zu vermeiden, die von vCenter Server generiert werden oder VMkernel-Adaptoren für Infrastrukturdatenverkehr zugewiesen sind, darf der Wert für *XX* 3F nicht überschreiten.

Der Höchstwert für eine manuell generierte MAC-Adresse lautet:

```
00:50:56:3F:FF:FF
```

Um Konflikte zwischen den generierten MAC-Adressen und den manuell zugewiesenen Adressen zu vermeiden, wählen Sie aus Ihren nicht veränderlichen Adressen einen eindeutigen Wert für *XX:YY:ZZ* aus.

Zuweisen einer statischen MAC-Adresse über den vSphere Web Client

Sie können statische MAC-Adressen mithilfe des vSphere Web Client der virtuellen Netzwerkkarte einer ausgeschalteten virtuellen Maschine zuweisen.

Verfahren

- 1 Ermitteln Sie die virtuelle Maschine im vSphere Web Client.
 - a Wählen Sie ein Datencenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus der Liste aus.
- 2 Schalten Sie die virtuelle Maschine aus.
- 3 Wählen Sie auf der Registerkarte **Verwalten** der virtuellen Maschine **Einstellungen > VM-Hardware** aus.
- 4 Klicken Sie auf **Bearbeiten** und klicken Sie dann auf die Registerkarte **Virtuelle Hardware**.
- 5 Erweitern Sie auf der Registerkarte **Virtuelle Hardware** den Abschnitt zum Netzwerkadapter.

- 6 Wählen Sie im Abschnitt „MAC-Adresse“ aus dem Dropdown-Menü **Manuell** aus.
- 7 Geben Sie die statische MAC-Adresse ein und klicken Sie auf **OK**.
- 8 Schalten Sie die virtuelle Maschine ein.

Zuweisen von statischen MAC-Adressen in der Konfigurationsdatei der virtuellen Maschine

Zum Festlegen einer statischen MAC-Adresse für eine virtuelle Maschine können Sie die Konfigurationsdatei der virtuellen Maschine mit dem vSphere Web Client bearbeiten.

Verfahren

- 1 Ermitteln Sie die virtuelle Maschine im vSphere Web Client.
 - a Wählen Sie ein Datacenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **Verwandte Objekte**.
 - b Klicken Sie auf **Virtuelle Maschinen** und wählen Sie die virtuelle Maschine aus der Liste aus.
- 2 Schalten Sie die virtuelle Maschine aus.
- 3 Wählen Sie auf der Registerkarte **Verwalten** der virtuellen Maschine die Option **Einstellungen** aus.
- 4 Erweitern Sie auf der Registerkarte **VM-Optionen** die Option **Erweitert**.
- 5 Klicken Sie auf **Konfiguration bearbeiten**.
- 6 Um eine statische MAC-Adresse zuzuweisen, müssen Sie die Parameter nach Bedarf hinzufügen oder bearbeiten.

Parameter	Wert
<code>ethernet X.addressType</code>	statisch
<code>ethernet X.address</code>	<i>MAC_address_of_the_virtual_NIC</i>

Das *X* neben `ethernet` steht für die fortlaufende Nummer der virtuellen Netzwerkkarte in der virtuellen Maschine.

Beispielsweise steht `0` in `ethernet0` für die Einstellungen der ersten virtuellen Netzwerkkarte, die der virtuellen Maschine hinzugefügt wurde.

- 7 Klicken Sie auf **OK**.
- 8 Schalten Sie die virtuelle Maschine ein.

Konfigurieren von vSphere für IPv6

13

Konfigurieren Sie ESXi-Hosts und vCenter Server für den Betrieb in einer reinen IPv6-Umgebung, um einen größeren Adressraum und verbesserte Adresszuweisung zu erhalten.

IPv6 ist von der Internet Engineering Task Force (IETF) als Nachfolger von IPv4 bestimmt und bietet die folgenden Vorteile:

- **Erweiterte Adresslänge.** Die Erweiterung des Adressraums löst das Problem der Adressknappheit und macht die Netzwerkadressübersetzung überflüssig. IPv6 verwendet 128-Bit-Adressen statt der 32-Bit-Adressen, die IPv4 verwendet.
- **Die automatische Adresskonfiguration der Knoten wurde verbessert.**

Dieses Kapitel enthält die folgenden Themen:

- [vSphere IPv6-Konnektivität](#)
- [Bereitstellen von vSphere auf IPv6](#)
- [Aktivieren oder Deaktivieren der IPv6-Unterstützung auf einem Host](#)
- [Einrichten von IPv6 auf einem ESXi-Host](#)
- [Einrichten von IPv6 auf vCenter Server](#)

vSphere IPv6-Konnektivität

In einer auf vSphere 6.0 und höher basierten Umgebung können Knoten und Funktionen transparent über IPv6 kommunizieren. Die statische und automatische Adresskonfiguration wird unterstützt.

IPv6 in der Kommunikation zwischen vSphere-Knoten

Die Knoten in einer vSphere-Bereitstellung können über IPv6 kommunizieren und zugewiesene Adressen entsprechend der Netzwerkkonfiguration akzeptieren.

Tabelle 13-1. IPv6-Support der Knoten in einer vSphere-Umgebung

Verbindungstyp	IPv6-Unterstützung	Adresskonfiguration auf vSphere-Knoten
ESXi zu ESXi	Ja	<ul style="list-style-type: none"> ■ Statisch ■ Automatisch: DHCPv6
vCenter Server-Maschine zu ESXi	Ja	<ul style="list-style-type: none"> ■ Statisch ■ Automatisch: DHCPv6
vCenter Server-Maschine zu vSphere Web Client-Maschine	Ja	<ul style="list-style-type: none"> ■ Statisch ■ Automatisch: DHCPv6
ESXi- zu vSphere Client-Maschine	Ja	<ul style="list-style-type: none"> ■ Statisch ■ Automatisch: DHCPv6
Virtuelle Maschine zu virtueller Maschine	Ja	<ul style="list-style-type: none"> ■ Statisch ■ Automatisch: DHCPv6
ESXi zu iSCSI-Speicher	Ja	<ul style="list-style-type: none"> ■ Statisch ■ Automatisch: DHCPv6
ESXi zu NFS-Speicher	Ja	<ul style="list-style-type: none"> ■ Statisch ■ Automatisch: DHCPv6
ESXi zu Active Directory	Nein Verwenden Sie LDAP über vCenter Server zur Verbindung von ESXi mit der Active Directory-Datenbank	–
vCenter Server Appliance zu Active Directory	Nein Verwenden Sie LDAP zur Verbindung der vCenter Server Appliance mit der Active Directory-Datenbank	–

IPv6-Konnektivität von vSphere-Funktionen

Bestimmte vSphere-Funktionen unterstützen IPv6 nicht:

- Auto Deploy
IPv6 wird von Auto Deploy nur teilweise unterstützt. Der PXE-Startvorgang ist nur über IPv4 möglich. Die weitere Kommunikation zwischen dem Auto Deploy-Server und ESXi-Hosts oder vCenter Server ist jedoch in einer reinen IPv6-Umgebung möglich.
- vSphere DPM über Intelligent Platform Management Interface (IPMI) und Hewlett-Packard Integrated Lights-Out (iLO). vSphere 6.0 unterstützt nur Wake-On-LAN (WOL), um einen Host aus dem Standby-Modus herauszubringen.
- Virtual Volumes
- Virtual SAN
- Authentication Proxy
- NFS 4.1-Speicher mit Kerberos

Verwenden Sie NFS 4.1 mit AUTH_SYS.

- vSphere Management Assistant und vSphere Command-Line Interface mit Active Directory verbunden.

Verwenden Sie LDAP, um vSphere Management Assistant oder vSphere Command-Line Interface mit der Active Directory-Datenbank zu verbinden.

IPv6-Konnektivität von virtuellen Maschinen

Virtuelle Maschinen können Daten im Netzwerk über IPv6 austauschen. vSphere unterstützt sowohl die statische als auch die automatische Zuweisung von IPv6-Adressen für virtuelle Maschinen.

Es können auch eine oder mehrere IPv6-Adressen konfiguriert werden, wenn Sie das Gastbetriebssystem einer virtuellen Maschine konfigurieren.

FQDNs und IPv6-Adressen

In vSphere sollten vollständig qualifizierte Domännennamen (FQDNs) verwendet werden, die IPv6-Adressen auf dem DNS-Server zugeordnet sind. Sie können IPv6-Adressen verwenden, wenn diese über einen gültigen FQDN auf dem DNS-Server für Reverse-Lookup verfügen.

Um vCenter Server in einer reinen IPv6-Umgebung bereitzustellen, dürfen Sie nur FQDNs verwenden.

Bereitstellen von vSphere auf IPv6

Führen Sie vSphere in einer reinen IPv6-Umgebung aus, um einen erweiterten Adressraum und flexible Adresszuweisung zu verwenden.

Wenn Sie vCenter Server und ESXi-Hosts in einem IPv6-Netzwerk bereitstellen möchten, müssen Sie zusätzliche Schritte durchführen.

- [Aktivieren von IPv6 in einer vSphere-Installation](#)

Wenn Sie eine Greenfield-Bereitstellung von vSphere 6.0 in einem IPv6-Netzwerk haben, konfigurieren Sie ESXi und vCenter Server für eine reine IPv6-Verwaltungsverbindung, indem Sie IPv6 auf den Bereitstellungsknoten konfigurieren und diese verbinden.

- [Aktivieren von IPv6 in einer vSphere-Umgebung mit Upgrade](#)

In einer IPv4-Bereitstellung von vSphere 6.5, die aus einem installierten oder aktualisierten vCenter Server und aktualisierten ESXi besteht, konfigurieren Sie ESXi und vCenter Server für eine reine IPv6-Verwaltungsverbindung, indem Sie IPv6 auf den bereitgestellten Knoten aktivieren und diese erneut verbinden.

Aktivieren von IPv6 in einer vSphere-Installation

Wenn Sie eine Greenfield-Bereitstellung von vSphere 6.0 in einem IPv6-Netzwerk haben, konfigurieren Sie ESXi und vCenter Server für eine reine IPv6-Verwaltungsverbindung, indem Sie IPv6 auf den Bereitstellungsknoten konfigurieren und diese verbinden.

Voraussetzungen

- Überprüfen Sie, dass die IPv6-Adressen für vCenter Server, die ESXi-Hosts und die externe Datenbank (falls verwendet) vollständig qualifizierten Domännennamen (FQDNs) auf dem DNS-Server zugewiesen sind.
- Überprüfen Sie, dass die Netzwerkinfrastruktur IPv6-Konnektivität für die ESXi-Hosts, vCenter Server und ggf. die externe Datenbank bereitstellt.
- Überprüfen Sie, ob Sie Version 6.0 von vCenter Server mit einem FQDN installiert haben, der einer IPv6-Adresse zugeordnet ist. Informationen finden Sie in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere*.
- Überprüfen Sie, ob auf den Hosts ESXi 6.0 installiert ist. Informationen finden Sie in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere*.

Verfahren

- 1 Konfigurieren Sie in der Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) jeden ESXi-Host als reinen IPv6-Knoten.
 - a Drücken Sie in der DCUI die Taste F2 und melden Sie sich beim Host an.
 - b Wählen Sie im Menü **Verwaltungsnetzwerk konfigurieren** die Option **IPv6-Konfiguration** und drücken Sie die Eingabetaste.
 - c Weisen Sie dem Host eine IPv6-Adresse zu.

Adresszuweisungsoption	Beschreibung
Automatische Adresszuweisung mit DHCPv6	1 Wählen Sie die Option Dynamische IPv6-Adresse und Netzwerkkonfiguration verwenden und wählen Sie DHCPv6 verwenden .
	2 Drücken Sie die Eingabetaste, um die Änderungen zu speichern.
Statische Adresszuweisung	1 Wählen Sie die Option Statische IPv6-Adresse und Netzwerkkonfiguration festlegen aus und geben Sie die IPv6-Adresse des Hosts und des Standardgateways ein.
	2 Drücken Sie die Eingabetaste, um die Änderungen zu speichern.

- d Wählen Sie im Menü **Verwaltungsnetzwerk konfigurieren** die Option **IPv4-Konfiguration** aus und drücken Sie die Eingabetaste.
 - e Wählen Sie **IPv4-Konfiguration für Verwaltungsnetzwerk deaktivieren** aus und drücken Sie die Eingabetaste.
- 2 Fügen Sie im vSphere Web Client die Hosts zur Bestandsliste hinzu.

Aktivieren von IPv6 in einer vSphere-Umgebung mit Upgrade

In einer IPv4-Bereitstellung von vSphere 6.5, die aus einem installierten oder aktualisierten vCenter Server und aktualisierten ESXi besteht, konfigurieren Sie ESXi und vCenter Server für eine reine IPv6-Verwaltungsverbindung, indem Sie IPv6 auf den bereitgestellten Knoten aktivieren und diese erneut verbinden.

Voraussetzungen

- Überprüfen Sie, dass die Netzwerkinfrastruktur IPv6-Konnektivität für die ESXi-Hosts, vCenter Server und ggf. die externe Datenbank bereitstellt.
- Überprüfen Sie, dass die IPv6-Adressen für vCenter Server, die ESXi-Hosts und die externe Datenbank (falls verwendet) vollständig qualifizierten Domännennamen (FQDNs) auf dem DNS-Server zugewiesen sind.
- Vergewissern Sie sich, dass Sie Version 6.x von vCenter Server installiert oder ein Upgrade darauf durchgeführt haben. Weitere Hinweise finden Sie in der Dokumentation *Installations- und Einrichtungshandbuch für vSphere* und *vSphere-Upgrade*.
- Vergewissern Sie sich, dass für alle ESXi-Hosts ein Upgrade auf Version 6.x durchgeführt wurde. Informationen hierzu finden Sie in der *vSphere-Upgrade*-Dokumentation.

Verfahren

- 1 Trennen Sie im vSphere Web Client die Hosts vom vCenter Server.

2 Konfigurieren Sie jeden ESXi-Host als reinen IPv6-Knoten.

- a Öffnen Sie eine SSH-Verbindung und melden Sie sich beim ESXi-Host an.
- b Führen Sie den folgenden Befehl aus:

```
esxcli network ip interface ipv6 set -i vmk0 -e true
```

- c Weisen Sie dem Verwaltungsnetzwerk eine IPv6-Adresse zu.

Adresszuweisungsoption	Beschreibung
Statische Adresszuweisung	<ol style="list-style-type: none"> Öffnen Sie eine SSH-Verbindung und melden Sie sich beim ESXi-Host an. Legen Sie eine statische IPv6-Adresse für das Verwaltungsnetzwerk vmk0 fest, indem Sie den folgenden Befehl ausführen: <pre>esxcli network ip interface ipv6 address add -I IPv6_address -i vmk0</pre> Legen Sie das Standard-Gateway für das Verwaltungsnetzwerk vmk0 fest, indem Sie den folgenden Befehl ausführen: <pre>esxcli network ip interface ipv6 set -i vmk0 -g default_gateway_IPv6_address</pre> Fügen Sie einen DNS-Server hinzu, indem Sie den folgenden Befehl ausführen: <pre>esxcli network ip dns server add -s DNS_server_IPv6_address</pre>
Automatische Adresszuweisung mit DHCPv6	<ol style="list-style-type: none"> Öffnen Sie eine SSH-Verbindung und melden Sie sich beim ESXi-Host an. Aktivieren Sie DHCPv6 für das Verwaltungsnetzwerk vmk0, indem Sie den folgenden Befehl ausführen: <pre>esxcli network ip interface ipv6 -i vmk0 -enable-dhcpv6 = true</pre> Aktivieren Sie „IPv6-Router angekündigt“ für das Verwaltungsnetzwerk vmk0, indem Sie den folgenden Befehl ausführen: <pre>esxcli network ip interface ipv6 set -i vmk0 -enable-router-adv =true</pre> Fügen Sie einen DNS-Server hinzu oder verwenden Sie die durch DHCPv6 veröffentlichte DNS-Einstellung, indem Sie einen der folgenden Befehle ausführen: <pre>esxcli network ip dns server add -s DNS_server_IPv6_address</pre> <pre>esxcli network ip interface ipv6 set -i vmk0 --peer-dns=true</pre>

- 3 Deaktivieren der IPv4-Konfiguration für das Verwaltungsnetzwerk
 - a Öffnen Sie eine SSH-Verbindung und melden Sie sich beim ESXi-Host an.
 - b Führen Sie den folgenden Befehl aus:

```
esxcli network ip interface ipv4 set -i vmk0 --type=none
```

- 4 Wenn vCenter Server eine externe Datenbank verwendet, konfigurieren Sie die Datenbank als IPv6-Knoten.
- 5 Konfigurieren Sie vCenter Server als reinen IPv6-Knoten und starten Sie ihn neu.
- 6 Deaktivieren Sie IPv4 auf dem Datenbankserver.
- 7 Fügen Sie im vSphere Web Client die Hosts zur Bestandsliste hinzu.
- 8 Deaktivieren Sie IPv4 in der Netzwerkinfrastruktur.

Aktivieren oder Deaktivieren der IPv6-Unterstützung auf einem Host

Über die IPv6-Unterstützung in vSphere können Hosts in einem IPv6-Netzwerk betrieben werden, das einen großen Adressbereich, verbessertes Multicasting, vereinfachtes Routing und andere Vorteile bietet.

In ESXi 5.1 und neueren Versionen ist IPv6 standardmäßig aktiviert.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerk** und wählen Sie **Erweitert**.
- 3 Klicken Sie auf **Bearbeiten**.
- 4 Aktivieren oder deaktivieren Sie im Dropdown-Menü **IPv6-Unterstützung** die IPv6-Unterstützung.
- 5 Klicken Sie auf **OK**.
- 6 Starten Sie den Host neu, damit die Änderungen an der IPv6-Unterstützung wirksam werden.

Nächste Schritte

Konfigurieren Sie die IPv6-Einstellungen der VMkernel-Adapter auf dem Host, beispielsweise des Verwaltungsnetzwerks. Siehe [Einrichten von IPv6 auf einem ESXi-Host](#).

Einrichten von IPv6 auf einem ESXi-Host

Um einen ESXi-Host über IPv6 mit dem Verwaltungsnetzwerk, vSphere vMotion, gemeinsam genutztem Speicher, vSphere Fault Tolerance usw. zu verbinden, bearbeiten Sie die IPv6-Einstellungen der VMkernel-Adapter auf dem Host.

Voraussetzungen

Vergewissern Sie sich, dass IPv6 auf dem ESXi-Host aktiviert ist. Siehe [Aktivieren oder Deaktivieren der IPv6-Unterstützung auf einem Host](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Wählen Sie unter **Verwalten** die Option **Netzwerk** und dann **VMkernel-Adapter** aus.
- 3 Wählen Sie den VMkernel-Adapter auf dem Ziel-Distributed Switch oder Ziel-Standard-Switch aus und klicken Sie auf **Bearbeiten**.
- 4 Klicken Sie im Dialogfeld „Einstellungen bearbeiten“ auf **IPv6-Einstellungen**.
- 5 Konfigurieren Sie die Adresszuweisung des VMkernel-Adapters.

IPv6-Adressoption	Beschreibung
IPv6-Adresse automatisch mittels DHCP abrufen	Empfängt eine IPv6-Adresse für den VMkernel-Adapter von einem DHCPv6-Server.
IPv6-Adresse automatisch mittels Router-Ankündigung abrufen	Empfängt eine IPv6-Adresse für den VMkernel-Adapter von einem Router über Router-Ankündigung.
Statische IPv6-Adressen	Legen Sie eine oder mehrere Adressen fest. Geben Sie für jeden Adresseintrag die IPv6-Adresse des Adapters, die Subnetz-Präfixlänge und die IPv6-Adresse des Standardgateways ein.

Abhängig von der Konfiguration Ihres Netzwerks können Sie mehrere Zuweisungsoptionen auswählen.

- 6 (Optional) Entfernen Sie im Abschnitt „Erweiterte Einstellungen“ auf der Seite der IPv6-Einstellungen bestimmte IPv6-Adressen, die über Router-Ankündigung zugewiesen werden.
 Sie können bestimmte IPv6-Adressen löschen, die der Host über Router-Ankündigung erhalten hat, um die Kommunikation mit diesen Adressen zu stoppen. Sie können alle automatisch zugewiesenen Adressen löschen, um die konfigurierte statische Adresse auf dem VMkernel zu erzwingen.
- 7 Klicken Sie auf **OK**, damit die Änderungen auf dem VMkernel-Adapter wirksam werden.

Einrichten von IPv6 auf vCenter Server

Konfigurieren Sie vCenter Server für den Datenaustausch mit ESXi-Hosts und mit vSphere Web Client in einem IPv6-Netzwerk.

Einrichten von IPv6 auf der vCenter Server Appliance

Verwenden Sie den vSphere Web Client, um die vCenter Server Appliance für die Kommunikation mit ESXi-Hosts in einem IPv6-Netzwerk zu konfigurieren.

Verfahren

- 1 Klicken Sie auf der Startseite des vSphere Web Client auf **Systemkonfiguration**.

- 2 Klicken Sie unter „Systemkonfiguration“ auf **Knoten**.
- 3 Wählen Sie unter „Knoten“ einen Knoten aus und klicken Sie auf die Registerkarte **Verwalten**.
- 4 Wählen Sie unter „Allgemein“ die Option **Netzwerk** aus und klicken Sie auf **Bearbeiten**.
- 5 Erweitern Sie den Namen der Netzwerkschnittstelle, um die IP-Adresseinstellungen zu bearbeiten.
- 6 Bearbeiten Sie die IPv6-Einstellungen.

Option	Beschreibung
IPv6-Adressen automatisch mittels DHCP abrufen	Weist der Appliance mithilfe von DHCP automatisch IPv6-Adressen vom Netzwerk zu.
IPv6-Einstellungen automatisch mittels Router-Ankündigung abrufen	Weist der Appliance mithilfe von Router-Ankündigung automatisch IPv6-Adressen vom Netzwerk zu.
Statische IPv6-Adressen	Verwendet statische IPv6-Adressen, die Sie manuell eingerichtet haben. <ol style="list-style-type: none"> 1 Klicken Sie auf das Symbol Add. 2 Geben Sie die IPv6-Adresse und die Länge des Subnetzpräfixes ein. 3 Klicken Sie auf OK. 4 (Optional) Bearbeiten Sie das Standard-Gateway.

Sie können die Appliance so konfigurieren, dass die IPv6-Einstellungen sowohl über DHCP als auch über die Router-Ankündigung automatisch abgerufen werden. Sie können gleichzeitig eine statische IPv6-Adresse zuweisen.

- 7 (Optional) Um die IPv6-Adressen zu entfernen, die automatisch über Router-Ankündigung zugewiesen wurden, klicken Sie auf **Adressen entfernen** und löschen Sie die Adressen.

Sie können bestimmte IPv6-Adressen löschen, die die vCenter Server Appliance über Router-Ankündigung erhalten hat, um die Kommunikation an diesen Adressen anzuhalten und die konfigurierten statischen Adressen zu erzwingen.

Nächste Schritte

Verbinden Sie die ESXi-Hosts über IPv6 mit vCenter Server, indem Sie deren FQDNs verwenden.

Einrichten von vCenter Server unter Windows mit IPv6

Um ESXi-Hosts oder den vSphere Web Client über IPv6 mit vCenter Server zu verbinden, der auf einer Windows-Hostmaschine ausgeführt wird, konfigurieren Sie die IPv6-Adresseinstellungen in Windows.

Verfahren

- ◆ Konfigurieren Sie im Ordner „Netzwerk- und Freigabecenter“ der Windows-Systemsteuerung die IPv6-Adresseinstellungen des Hosts für die LAN-Verbindung.

Nächste Schritte

Verbinden Sie die ESXi-Hosts über IPv6 mit vCenter Server, indem Sie deren FQDNs verwenden.

Überwachen der Netzwerkverbindung und des Netzwerkdatenverkehrs

14

Überwachen Sie die durch die Ports eines vSphere Standard-Switch oder eines vSphere Distributed Switch geleiteten Netzwerkverbindungen und -pakete, um den Datenverkehr zwischen virtuellen Maschinen und Hosts zu analysieren.

Dieses Kapitel enthält die folgenden Themen:

- Erfassen und Nachverfolgen von Netzwerkpaketen unter Verwendung des Dienstprogramms `pktcap-uw`
- Konfigurieren der NetFlow-Einstellungen eines vSphere Distributed Switch
- Arbeiten mit der Portspiegelung
- Überprüfung des Systemzustands des vSphere Distributed Switch
- Switch-Discovery-Protokoll

Erfassen und Nachverfolgen von Netzwerkpaketen unter Verwendung des Dienstprogramms `pktcap-uw`

Überwachen Sie den Datenverkehr, der durch physische Netzwerkadapter, VMkernel-Adapter und VM-Adapter fließt, und analysieren Sie die Paketinformationen unter Verwendung der grafischen Benutzeroberfläche von Netzwerkanalysetools wie Wireshark.

In vSphere 5.5 oder höher können Sie Pakete auf einem Host mit dem Konsolendienstprogramm `pktcap-uw` überwachen. Sie können das Dienstprogramm ohne zusätzliche Installation auf einem ESXi-Host verwenden. `pktcap-uw` bietet viele Punkte im Host-Netzwerkstapel, an denen Sie Datenverkehr überwachen können.

Um eine detaillierte Analyse der erfassten Pakete vorzunehmen, speichern Sie den Paketinhalt aus dem Dienstprogramm `pktcap-uw` in Dateien im PCAP- oder PCAPNG-Format und öffnen Sie diese in Wireshark. Sie können auch eine Fehlerbehebung für verloren gegangene Pakete durchführen und den Pfad eines Pakets im Netzwerkstapel verfolgen.

Hinweis Das Dienstprogramm `pktcap-uw` wird zur Abwärtskompatibilität über die vSphere-Versionen hinweg nicht vollständig unterstützt. Die Optionen des Dienstprogramms können zukünftig geändert werden.

Befehlssyntax von `pktcap-uw` zum Erfassen von Paketen

Verwenden Sie das Dienstprogramm `pktcap-uw`, um die Inhalte von Paketen zu untersuchen, während sie den Netzwerk-Stack auf einem ESXi-Host durchlaufen.

Syntax von `pktcap-uw` zum Erfassen von Paketen

Der Befehl `pktcap-uw` hat die folgende Syntax zum Erfassen von Paketen an einer bestimmten Stelle im Netzwerk-Stack:

```
pktcap-uw  
  switch_port_arguments  
  capture_point_options  
  filter_options  
  output_control_options
```

Hinweis Bestimmte Optionen des Dienstprogramms `pktcap-uw` sind ausschließlich zur VMware-internen Verwendung bestimmt und sollten nur auf Anweisung des technischen Supports von VMware verwendet werden. Diese Optionen werden im Handbuch *vSphere-Netzwerk* nicht beschrieben.

Tabelle 14-1. Argumente von pktcap-uw zum Erfassen von Paketen

Argumentengruppe	Argument	Beschreibung
<i>Switch-Port-Argumente</i>	<code>--uplink vmnicX</code>	<p>Erfasst Pakete im Zusammenhang mit einem physikalischen Adapter. Sie können die Optionen <code>--uplink</code> und <code>--capture</code> kombinieren, um Pakete an einer bestimmten Stelle auf dem Pfad zwischen dem physikalischen Adapter und dem virtuellen Switch zu überwachen.</p> <p>Weitere Informationen hierzu finden Sie unter Erfassen von Paketen, die beim physikalischen Adapter ankommen.</p>
	<code>--vmk vmkX</code>	<p>Erfasst Pakete im Zusammenhang mit einem VMKernel-Adapter. Sie können die Optionen <code>vmk</code> und <code>--capture</code> kombinieren, um Pakete an einer bestimmten Stelle auf dem Pfad zwischen dem VMkernel-Adapter und dem virtuellen Switch zu überwachen.</p> <p>Weitere Informationen hierzu finden Sie unter Erfassen von Paketen für einen VMkernel-Adapter.</p>

Tabelle 14-1. Argumente von pktcap-uw zum Erfassen von Paketen (Fortsetzung)

Argumentengruppe	Argument	Beschreibung
	<code>--switchport {VMXNET3-Port-ID VMkernel-Adapter-Port-ID}</code>	<p>Erfasst Pakete im Zusammenhang mit einem VMXNET3-Adapter einer virtuellen Maschine oder einem an einen bestimmten Port eines virtuellen Switches angeschlossenen VMkernel-Adapter. Sie können die ID des Ports im Netzwerkfenster des Dienstprogramms <code>esxtop</code> anzeigen.</p> <p>Sie können die Optionen <code>switchport</code> und <code>capture</code> kombinieren, um Pakete an einer bestimmten Stelle auf dem Pfad zwischen dem VMXNET3- oder VMkernel-Adapter und dem virtuellen Switch zu überwachen.</p> <p>Weitere Informationen hierzu finden Sie unter Erfassen von Paketen für einen VMXNET3-VM-Adapter.</p>
	<code>--lifID LIF-ID</code>	<p>Erfasst Pakete im Zusammenhang mit der logischen Schnittstelle eines verteilten Routers. Weitere Informationen hierzu finden Sie in der <i>VMware NSX</i>-Dokumentation.</p>
<i>Erfassungspunktoptionen</i>	<code>--capture Erfassungspunkt</code>	<p>Erfasst Pakete an einer bestimmten Stelle im Netzwerk-Stack. Sie können z. B. Pakete unmittelbar nach deren Ankunft von einem physikalischen Adapter überwachen.</p>
	<code>--dir {0 1}</code>	<p>Erfasst Pakete entsprechend der Flussrichtung bezogen auf den virtuellen Switch.</p> <p>0 steht für eingehenden Datenverkehr und 1 für ausgehenden Datenverkehr.</p> <p>Standardmäßig erfasst das Dienstprogramm <code>pktcap-uw</code> Ingress-Datenverkehr.</p> <p>Verwenden Sie die Option <code>--dir</code> zusammen mit der Option <code>--uplink</code>, <code>--vmk</code> oder <code>--switchport</code>.</p>

Tabelle 14-1. Argumente von `pktcap-uw` zum Erfassen von Paketen (Fortsetzung)

Argumentengruppe	Argument	Beschreibung
	<code>--stage {0 1}</code>	Erfasst die Pakete näher an Quelle oder Ziel. Verwenden Sie diese Option, um zu untersuchen, wie ein Paket sich verändert, während es die Punkte im Stack durchläuft. 0 steht für Datenverkehr näher an der Quelle und 1 für Datenverkehr näher am Ziel. Verwenden Sie die Option <code>--stage</code> zusammen mit der Option <code>--uplink</code> , <code>--vmk</code> , <code>--switchport</code> oder <code>--dvfilter</code> .
	<code>--dvfilter Filtername --capture PreDVFilter PostDVFilter</code>	Erfasst Pakete, bevor oder nachdem diese von vSphere Network Appliance (DVFilter) abgefangen werden. Weitere Informationen hierzu finden Sie unter Erfassen von Paketen auf DVFilter-Ebene .
	<code>-A --availpoints</code>	Zeigt alle vom Dienstprogramm <code>pktcap-uw</code> unterstützten Erfassungspunkte an.
	Details zu den Erfassungspunkten des Dienstprogramms <code>pktcap-uw</code> finden Sie unter Erfassungspunkte des Dienstprogramms pktcap-uw .	
<i>Filteroptionen</i>	Filtert erfasste Pakete nach Quell- oder Zieladresse, VLAN-ID, VXLAN-ID, Schicht 3-Protokoll und TCP-Port. Weitere Informationen hierzu finden Sie unter Optionen von pktcap-uw zum Filtern von Paketen .	
<i>Ausgabesteuerungsoptionen</i>	Speichert die Inhalte eines Pakets in einer Datei, erfasst nur eine bestimmte Anzahl von Paketen, erfasst eine bestimmte Anzahl von Bytes am Paketanfang, usw. Weitere Informationen hierzu finden Sie unter Optionen von pktcap-uw zum Kontrollieren der Ausgabe .	

Die vertikalen Linien | stehen zwischen alternativen Werten und die mit vertikalen Linien verwendeten geschweiften Klammern { } geben eine Liste von Auswahlmöglichkeiten für ein Argument oder eine Option an.

Befehlssyntax von `pktcap-uw` zum Nachverfolgen von Paketen

Verwenden Sie das Dienstprogramm `pktcap-uw`, um den Pfad eines Pakets im Netzwerkstapel auf einem ESXi-Host zur Latenzanalyse anzuzeigen.

Syntax von pktcap-uw zum Nachverfolgen von Paketen

Der Befehl des Dienstprogramms `pktcap-uw` hat die folgende Syntax zum Nachverfolgen von Paketen im Netzwerkstapel:

```
pktcap-uw --trace filter_options output_control_options
```

Optionen für das Dienstprogramm pktcap-uw zum Nachverfolgen von Paketen

Das Dienstprogramm `pktcap-uw` unterstützt die folgenden Optionen zum Nachverfolgen von Paketen:

Tabelle 14-2. Optionen von pktcap-uw zum Nachverfolgen von Paketen

Argument	Beschreibung
<i>Filteroptionen</i>	Filtert nachverfolgte Paketen nach Quell- oder Zieladresse, VLAN-ID, VXLAN-ID, Schicht 3-Protokoll und TCP-Port. Weitere Informationen hierzu finden Sie unter Optionen von pktcap-uw zum Filtern von Paketen .
<i>Ausgabesteuerungsoptionen</i>	Speichert den Inhalt eines Pakets in einer Datei und führt die Nachverfolgung nur für eine bestimmte Anzahl von Paketen aus. Weitere Informationen hierzu finden Sie unter Optionen von pktcap-uw zum Kontrollieren der Ausgabe .

Optionen von pktcap-uw zum Kontrollieren der Ausgabe

Verwenden Sie zum Kontrollieren der Ausgabe das Dienstprogramm `pktcap-uw`, um Paketinhalte in eine Datei zu speichern, höchstens eine bestimmte Anzahl von Bytes aus jedem Paket zu erfassen und die Anzahl der erfassten Pakete einzugrenzen.

Optionen von pktcap-uw zum Kontrollieren der Ausgabe

Die Optionen des Dienstprogramms `pktcap-uw` zum Kontrollieren der Ausgabe sind gültig, wenn Sie Pakete erfassen und verfolgen. Zu Informationen bezüglich der Befehlssyntax des Dienstprogramms `pktcap-uw`, siehe [Befehlssyntax von pktcap-uw zum Erfassen von Paketen](#) und [Befehlssyntax von pktcap-uw zum Nachverfolgen von Paketen](#).

Tabelle 14-3. Optionen zum Kontrollieren der Ausgabe, die vom Dienstprogramm pktcap-uw unterstützt werden

Option	Beschreibung
<code>{-o --outfile} pcap_file</code>	Speichern Sie erfasste oder verfolgte Pakete im Paket-Speicherformat (PCAP) in einer Datei. Verwenden Sie diese Option, um Pakete in einem visuellen Analysetool, beispielsweise Wireshark, zu überprüfen.
<code>-P --ng</code>	Speichern Sie den Paketinhalt im PCAPNG-Dateiformat. Verwenden Sie diese Option in Verbindung mit der Option <code>-o</code> oder <code>--outfile</code> .

Tabelle 14-3. Optionen zum Kontrollieren der Ausgabe, die vom Dienstprogramm `pktcap-uw` unterstützt werden (Fortsetzung)

Option	Beschreibung
<code>--console</code>	Schreiben Sie Paketangaben und -inhalte in die Konsolenausgabe. Standardmäßig zeigt das Dienstprogramm <code>pktcap-uw</code> Paketinformationen in der Konsolenausgabe an.
<code>{-c --count} number_of_packets</code>	Erfassen Sie die ersten <i>number_of_packets</i> Pakete.
<code>{-s --snaplen} snapshot_length</code>	<p>Erfassen Sie nur die ersten <i>snapshot_length</i> Bytes von jedem Paket. Ist der Datenverkehr auf dem Host stark, verwenden Sie diese Option, um die CPU- und Speicherauslastung zu verringern.</p> <p>Um die Größe von gespeicherten Inhalten zu beschränken, wählen Sie einen Wert größer als 24.</p> <p>Um das vollständige Paket zu speichern, setzen Sie diese Option auf 0.</p>
<code>-h</code>	Zum Dienstprogramm <code>pktcap-uw</code> schauen Sie unter Hilfe.

Die vertikalen Linien | stehen zwischen alternativen Werten und die mit vertikalen Linien verwendeten geschweiften Klammern { } geben eine Liste von Auswahlmöglichkeiten für ein Argument oder eine Option an.

Optionen von `pktcap-uw` zum Filtern von Paketen

Grenzen Sie den Bereich der Pakete, die Sie überwachen, ein, indem Sie das Dienstprogramm `pktcap-uw` verwenden, um Filteroptionen für die Quell- und Zieladresse, VLAN, VXLAN und das Nächste-Schicht-Protokoll anzuwenden, das die Nutzlast des Pakets verarbeitet.

Filteroptionen

Die Filteroptionen für `pktcap-uw` sind gültig für die Erfassung und Nachverfolgung von Paketen. Für Informationen zur Befehlssyntax des Dienstprogramms `pktcap-uw` siehe [Befehlssyntax von `pktcap-uw` zum Erfassen von Paketen](#) und [Befehlssyntax von `pktcap-uw` zum Nachverfolgen von Paketen](#).

Tabelle 14-4. Filteroptionen des Dienstprogramms `pktcap-uw`

Option	Beschreibung
<code>--srcmac mac_address</code>	Erfassen oder verfolgen Sie Pakete, die eine bestimmte MAC-Quelladresse haben. Trennen Sie die Oktette durch Doppelpunkte.
<code>--dstmac mac_address</code>	Erfassen oder verfolgen Sie Pakete, die eine bestimmte MAC-Zieladresse haben. Trennen Sie die Oktette durch Doppelpunkte.
<code>--mac mac_address</code>	Erfassen oder verfolgen Sie Pakete, die eine bestimmte MAC-Quell- oder Zieladresse haben. Trennen Sie die Oktette durch Doppelpunkte.

Tabelle 14-4. Filteroptionen des Dienstprogramms pktcap-uw (Fortsetzung)

Option	Beschreibung
<code>--ethtype 0xEtherType</code>	Erfassen oder verfolgen Sie Pakete auf Schicht 2 entsprechend dem Nächste-Schicht-Protokoll, das die Nutzlast des Pakets verarbeitet. <i>EtherType</i> entspricht dem Feld EtherType in den Ethernet-Frames. Es stellt den Typ des Nächste-Schicht-Protokolls dar, das die Rahmennutzlast verbraucht. Um beispielsweise Datenverkehr für das Link Layer Discovery Protocol (LLDP) zu überwachen, geben Sie <code>--ethtype 0x88CC</code> ein.
<code>--vlan VLAN_ID</code>	Erfassen oder verfolgen Sie Pakete, die zu einem VLAN gehören.
<code>--srcip IP_address IP_address/subnet_range</code>	Erfassen oder verfolgen Sie Pakete, die eine bestimmte IPv4-Quell- oder Subnetzadresse haben.
<code>--dstip IP_address IP_address/subnet_range</code>	Erfassen oder verfolgen Sie Pakete, die eine bestimmte IPv4-Ziel- oder Subnetzadresse haben.
<code>--ip IP_address</code>	Erfassen oder verfolgen Sie Pakete, die eine bestimmte Quell- oder IPv4-Zieladresse haben.
<code>--proto 0xIP_protocol_number</code>	Erfassen oder verfolgen Sie Pakete auf Schicht 3 entsprechend dem Nächste-Schicht-Protokoll, das die Nutzlast verarbeitet. Um beispielsweise Datenverkehr für das UDP-Protokoll zu überwachen, geben Sie <code>--proto 0x11</code> ein.
<code>--srcport source_port</code>	Erfassen oder verfolgen Sie Pakete ihrem Quell-TCP-Port entsprechend.
<code>--dstport destination_port</code>	Erfassen oder verfolgen Sie Pakete ihrem Ziel-TCP-Port entsprechend.
<code>--tcpport TCP_port</code>	Erfassen oder verfolgen Sie Pakete ihrem Quell- oder Ziel-TCP-Port entsprechend.
<code>--vxlan VXLAN_ID</code>	Erfassen oder verfolgen Sie Pakete, die zu einem VXLAN gehören.

Die vertikalen Balken | stellen alternative Werte dar.

Erfassen von Paketen mithilfe des Dienstprogramms pktcap-uw

Erfassen Sie Pakete mit dem Dienstprogramm `pktcap-uw` auf dem Pfad zwischen einem virtuellen Switch und den physikalischen Adaptern, VMkernel-Adaptern und VM-Adaptern, um Fehler bei Datenübertragungen im Netzwerk-Stack auf einem ESXi-Host zu beheben.

Erfassen von Paketen, die beim physikalischen Adapter ankommen

Überprüfen Sie den Host-Datenverkehr in ein externes Netzwerk, indem Sie Pakete an bestimmten Punkten zwischen vSphere Standard Switch oder vSphere Distributed Switch und einem physikalischen Adapter erfassen.

Sie können einen bestimmten Erfassungspunkt im Datenpfad zwischen einem virtuellen Switch und einem physikalischen Adapter festlegen oder einen Erfassungspunkt durch die Richtung des Datenverkehrs im Hinblick auf den Switch und die Nähe zur Paketquelle oder zum Paketziel bestimmen. Informationen zu unterstützten Erfassungspunkten finden Sie unter [Erfassungspunkte des Dienstprogramms pktcap-uw](#).

Verfahren

- 1 (Optional) Sie finden den Namen des physikalischen Adapters, den Sie überprüfen wollen, in der Host-Adapter-Liste.
 - Klicken Sie im vSphere Web Client unter der Registerkarte **Verwalten** für den Host auf **Netzwerke** und wählen Sie **Physikalische Adapter**.
 - Starten Sie für die Listenansicht der physikalische Adapter und für die Überprüfung ihres Status in der ESXi Shell für den Host den folgenden ESXCLI-Befehl:

```
esxcli network nic list
```

Jeder physikalische Adapter wird dargestellt als `vmnicX`. *X* ist die Nummer, die ESXi dem physikalischen Adapterport zugeordnet hat.

- 2 Starten Sie in der ESXi Shell an den Host den Befehl `pktcap-uw` mit dem Argument `--uplink vmnicX` und mit Optionen, die Pakete an einem bestimmten Punkt zu überwachen, erfasste Pakete zu filtern und das Ergebnis in einer Datei zu speichern.

```
pktcap-uw
  --uplink vmnicX [--capturecapture_point|--dir 0|1] [filter_options]
  [--outfilepcap_file_path [--ng]] [--countnumber_of_packets]
```

Die Optionen des Befehls `pktcap-uw--uplink vmnicX` stehen in eckigen Klammern `[]` und die vertikalen Balken `|` stellen die alternativen Werte dar.

Wenn Sie den Befehl `pktcap-uw--uplink vmnicX` ohne Optionen starten, erhalten Sie den Inhalt von Paketen, die am Standard-Switch oder Distributed Switch in der Konsolenausgabe eingehen, wenn sie umgeschaltet werden.

- a Verwenden Sie die Option `--capture`, um Pakete an einem anderen Erfassungspunkt oder die Option `--dir` in einer anderen Richtung des Datenverkehrs zu überprüfen.

Befehlsoption <code>pktcap-uw</code>	Ziel
<code>--capture UplinkSnd</code>	Überwacht Pakete, unmittelbar bevor sie in den physikalischen Adapter eingehen.
<code>--capture UplinkRcv</code>	Überwacht Pakete, unmittelbar nachdem sie in die Netzwerkkarten des physikalischen Adapters eingehen.
<code>--dir 1</code>	Überwacht Pakete, die den virtuellen Switch verlassen.
<code>--dir 0</code>	Überwacht Pakete, die in den virtuellen Switch eingehen.

- b Verwenden Sie *Filteroptionen*, um Pakete nach Quell- und Zieladresse, VLAN ID, VXLAN ID, Schicht 3-Protokoll und TCP-Port zu filtern.

Zum Überwachen der Pakete von einem Quellsystem – beispielsweise mit der IP-Adresse 192.168.25.113 – verwenden Sie z. B. die Filteroption `--srcip 192.168.25.113`.

- c Verwenden Sie Optionen zum Speichern der Inhalte jedes Pakets oder einer bestimmten Anzahl von Paketen in eine `.pcap`- oder `.pcapng`-Datei.

- Um Pakete in eine `.pcap`-Datei zu speichern, verwenden Sie die Option `--outfile`.
- Um Pakete in eine `.pcapng`-Datei zu speichern, verwenden Sie die Optionen `--ng` und `--outfile`.

Sie können die Datei in einem Netzwerkanalyssetool wie Wireshark öffnen.

Standardmäßig speichert das Dienstprogramm `pktcap-uw` die Paketdateien im Root-Ordner des ESXi-Dateisystems.

- d Verwenden Sie die Option `--count`, um nur eine bestimmte Anzahl von Paketen zu überwachen.

- 3 Wenn Sie die Anzahl der Pakete nicht mit der Option `--count` beschränkt haben, drücken Sie STRG+C, um die Erfassung oder Nachverfolgung von Paketen zu beenden.

Beispiel: Pakete erfassen, die bei `vmnic0` von einer IP-Adresse 192.168.25.113 eingehen

Um die ersten 60 Pakete von einem Quellsystem zu erfassen, dem die IP-Adresse 192.168.25.113 bei `vmnic0` zugewiesen ist, und sie in einer Datei mit der Bezeichnung `vmnic0_rcv_srcip.pcap` zu speichern, starten Sie den Befehl `pktcap-uw`:

```
pktcap-uw --uplink vmnic0 --capture UplinkRcv --srcip 192.168.25.113 --outfile
vmnic0_rcv_srcip.pcap --count 60
```

Nächste Schritte

Wenn der Inhalt des Pakets in eine Datei gespeichert wird, kopieren Sie die Datei vom ESXi-Host auf das System, auf dem ein grafisches Analysetool wie Wireshark ausgeführt wird, und öffnen Sie es in diesem Tool, um die Paketdetails zu untersuchen.

Erfassen von Paketen für einen VMXNET3-VM-Adapter

Überwachung des Datenverkehrs, zwischen einem virtuellen Switch und einem VMXNET3 Adapter der virtuellen Maschine durch Verwendung des Dienstprogramms `pktcap-uw`.

Sie können einen bestimmten Erfassungspunkt im Datenpfad zwischen einem virtuellen Switch und einem Adapter der virtuellen Maschine festlegen. Außerdem können Sie einen Erfassungspunkt durch die Richtung des Datenverkehrs im Hinblick auf den Switch und die Nähe zur Paketquelle oder zum Paketziel festlegen. Informationen zu unterstützten Erfassungspunkten finden Sie unter [Erfassungspunkte des Dienstprogramms pktcap-uw](#).

Voraussetzungen

Vergewissern Sie sich, dass es sich um einen Adapter der virtuellen Maschine des Typs VMXNET3 handelt.

Verfahren

- Finden Sie auf dem Host die Port-ID des Adapters der virtuellen Maschine mithilfe des Dienstprogramms `esxtop` heraus.

- Starten Sie das Dienstprogramm im ESXi Shell an den Host mithilfe von `esxtop`.
- Klicken Sie auf N, um zum Netzwerkfenster des Dienstprogramms zu wechseln.
- Suchen Sie in der Spalte VERWENDET VON den Adapter der virtuellen Maschine und schreiben Sie den PORT-ID-Wert dafür auf.

Das Feld VERWENDET VON enthält den Namen der virtuellen Maschine und den Port, mit dem der Adapter der virtuellen Maschine verbunden ist.

- Zum Verlassen von `esxtop` klicken Sie auf Q.

- Führen Sie in der ESXi Shell für den Host `pktcap-uw --switchport port_ID` aus.

`port_ID` ist die ID, die das Dienstprogramm `esxtop` für den Adapter der virtuellen Maschine in der Spalte PORT-ID anzeigt.

- Führen Sie in der ESXi Shell für den Host den Befehl `pktcap-uw` mit dem Argument `--switchport port_ID` und mit Optionen aus, um Pakete an einem bestimmten Punkt zu überwachen, erfasste Pakete zu filtern und das Ergebnis in einer Datei zu speichern.

```
pktcap-uw --switchport port_ID [--capture capture_point|--dir 0|1 --stage 0|1]
[filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

Die Optionen des Befehls `pktcap-uw --switchport port_ID` stehen in eckigen Klammern [], und die vertikalen Balken | stellen die alternativen Werte dar.

Wenn Sie den Befehl `pktcap-uw --switchport port_ID` ohne Optionen ausführen, erhalten Sie den Inhalt von Paketen, die am Standard-Switch oder Distributed Switch in der Konsolenausgabe eingehen, an der Stelle, an der sie umgeschaltet werden.

- a Um die Pakete an einem anderen Erfassungspunkt oder in einer anderen Richtung des Pfades zwischen dem Gastbetriebssystem und dem virtuellen Switch zu überprüfen, verwenden Sie die Option `--capture` oder verbinden Sie die Werte der Optionen `--dir` und `--stage`.

pktcap-uw Befehlsoptionen	Ziel
<code>--capture VnicTx</code>	Überwachen Sie Pakete, wenn Sie von der virtuellen Maschine an den Switch weitergegeben werden.
<code>--capture VnicRx</code>	Überwachen Sie Pakete, wenn sie in der virtuellen Maschine eingehen.
<code>--dir 1 --stage 0</code>	Überwacht Pakete, unmittelbar nachdem sie den virtuellen Switch verlassen.
<code>--dir 1</code>	Überwachen Sie Pakete, unmittelbar bevor sie in der virtuellen Maschine eingehen.
<code>--dir 0 --stage 1</code>	Überwachen Sie Pakete, unmittelbar nachdem sie in der virtuellen Maschine eingegangen sind.

- b Verwenden Sie *Filteroptionen*, um Pakete nach Quell- und Zieladresse, VLAN ID, VXLAN ID, Schicht 3-Protokoll und TCP-Port zu filtern.

Zum Überwachen der Pakete von einem Quellsystem – beispielsweise mit der IP-Adresse 192.168.25.113 – verwenden Sie z. B. die Filteroption `--srcip 192.168.25.113`.

- c Verwenden Sie Optionen zum Speichern der Inhalte jedes Pakets oder einer bestimmten Anzahl von Paketen in eine `.pcap`- oder `.pcapng`-Datei.

- Um Pakete in eine `.pcap`-Datei zu speichern, verwenden Sie die Option `--outfile`.
- Um Pakete in eine `.pcapng`-Datei zu speichern, verwenden Sie die Optionen `--ng` und `--outfile`.

Sie können die Datei in einem Netzwerkanalysetool wie Wireshark öffnen.

Standardmäßig speichert das Dienstprogramm `pktcap-uw` die Paketdateien im Root-Ordner des ESXi-Dateisystems.

- d Verwenden Sie die Option `--count`, um nur eine bestimmte Anzahl von Paketen zu überwachen.

- 4 Wenn Sie die Anzahl der Pakete nicht mit der Option `--count` beschränkt haben, drücken Sie STRG+C, um die Erfassung oder Nachverfolgung von Paketen zu beenden.

Beispiel: Erfassen Sie Pakete, die bei einer virtuellen Maschine von einer IP-Adresse 192.168.25.113 eingehen

Um die ersten 60 Pakete von einer Quelle zu erfassen, der die IP-Adresse 192.168.25.113 zugewiesen ist, wenn sie bei einem Adapter einer virtuellen Maschine mit der Port-ID 33554481 eingehen und sie in einer Datei mit der Bezeichnung `vmxnet3_rcv_srcip.pcap` zu speichern, starten Sie den folgenden `pktcap-uw`-Befehl:

```
pktcap-uw --switchport 33554481 --capture VnicRx --srcip 192.168.25.113 --outfile
vmxnet3_rcv_srcip.pcap --count 60
```

Nächste Schritte

Wenn der Inhalt des Pakets in eine Datei gespeichert wird, kopieren Sie die Datei vom ESXi-Host auf das System, auf dem ein grafisches Analysetool wie Wireshark ausgeführt wird, und öffnen Sie es in diesem Tool, um die Paketdetails zu untersuchen.

Erfassen von Paketen für einen VMkernel-Adapter

Überprüfen von Paketen, die zwischen einem VMkernel-Adapter und einem virtuellen Switch ausgetauscht werden, mithilfe des Dienstprogramms `pktcap-uw`.

Sie können Pakete an einem bestimmten Erfassungspunkt im Flow zwischen einem virtuellen Switch und einem VMkernel-Adapter erfassen. Außerdem können Sie einen Erfassungspunkt durch die Richtung des Datenverkehrs im Hinblick auf den Switch und die Nähe zur Paketquelle oder zum Paketziel festlegen. Informationen zu unterstützten Erfassungspunkten finden Sie unter [Erfassungspunkte des Dienstprogramms pktcap-uw](#).

Verfahren

- 1 (Optional) Den Namen des VMkernel-Adapters, den Sie überprüfen wollen, finden Sie in der VMkernel-Adapter-Liste.
 - Wählen Sie im vSphere Web Client aus der Networking-Liste unter der Registerkarte **Manage** für den Host **VMkernel-Adapter**.
 - Starten Sie für die Listenansicht der physikalischen Adapter im ESXi Shell für den Host den folgenden Befehl:

```
esxcli network ip interface list
```

Jeder VMkernel-Adapter wird als `vmkX` angezeigt, wobei *X* die Sequenznummer ist, die ESXi dem Adapter zugeteilt hat.

- 2 Starten Sie im ESXi Shell an den Host den Befehl `pktcap-uw` mit dem Argument `-vmkvmkX` und mit Optionen, die Pakete an einem bestimmten Punkt zu überwachen, erfasste Pakete zu filtern und das Ergebnis in eine Datei zu speichern.

```
pktcap-uw
--vmk vmkX [--capturecapture_point|--dir 0|1 --stage 0|1] [filter_options]
[--outfilepcap_file_path [--ng]] [--countnumber_of_packets]
```

Die Optionen des Befehls `pktcap-uw--vmk vmkX` stehen in eckigen Klammern `[]` und die vertikalen Balken `|` stellen die alternativen Werte dar.

Sie können die Option `--vmk vmkX` durch `--switchportvmkernel_adapter_port_ID` ersetzen, wenn `vmkernel_adapter_port_ID` der PORT-ID-Wert ist, den das Netzwerkfenster des Dienstprogramms `esxtop` für den Adapter anzeigt.

Wenn Sie den Befehl `pktcap-uw--vmk vmkX` ohne Optionen ausführen, erhalten Sie die Paketinhalte, die den VMkernel-Adapter verlassen.

- a Um die übertragenen oder erhaltenen Pakete an einem bestimmten Standort oder in einer bestimmten Richtung zu überprüfen, verwenden Sie die Option `--capture` oder verbinden Sie die Werte der Optionen `--dir` und `--stage`.

pktcap-uw Befehlsoptionen	Ziel
<code>--dir 1 --stage 0</code>	Überwacht Pakete, unmittelbar nachdem sie den virtuellen Switch verlassen.
<code>--dir 1</code>	Überwacht Pakete, unmittelbar bevor sie in den VMkernel-Adapter eingehen.
<code>--dir 0 --stage 1</code>	Überwacht Pakete, unmittelbar bevor sie in den virtuellen Switch eingehen.

- b Verwenden Sie *Filteroptionen*, um Pakete nach Quell- und Zieladresse, VLAN ID, VXLAN ID, Schicht 3-Protokoll und TCP-Port zu filtern.

Zum Überwachen der Pakete von einem Quellsystem – beispielsweise mit der IP-Adresse 192.168.25.113 – verwenden Sie z. B. die Filteroption `--srcip 192.168.25.113`.

- c Verwenden Sie Optionen zum Speichern der Inhalte jedes Pakets oder einer bestimmten Anzahl von Paketen in eine `.pcap`- oder `.pcapng`-Datei.
 - Um Pakete in eine `.pcap`-Datei zu speichern, verwenden Sie die Option `--outfile`.
 - Um Pakete in eine `.pcapng`-Datei zu speichern, verwenden Sie die Optionen `--ng` und `--outfile`.

Sie können die Datei in einem Netzwerkanalysetool wie Wireshark öffnen.

Standardmäßig speichert das Dienstprogramm `pktcap-uw` die Paketdateien im Root-Ordner des ESXi-Dateisystems.

- d Verwenden Sie die Option `--count`, um nur eine bestimmte Anzahl von Paketen zu überwachen.
- 3 Wenn Sie die Anzahl der Pakete nicht mit der Option `--count` beschränkt haben, drücken Sie STRG+C, um die Erfassung oder Nachverfolgung von Paketen zu beenden.

Nächste Schritte

Wenn der Inhalt des Pakets in eine Datei gespeichert wird, kopieren Sie die Datei vom ESXi-Host auf das System, auf dem ein grafisches Analysetool wie Wireshark ausgeführt wird, und öffnen Sie es in diesem Tool, um die Paketdetails zu untersuchen.

Erfassen von verworfenen Paketen

Fehlerbehebung bei unterbrochener Konnektivität durch Erfassen verloren gegangener Pakete mit dem Dienstprogramm `pktcap-uw`.

Ein Paket kann aus vielen Gründen innerhalb des Netzwerkdatenstroms verloren gehen, z. B. Firewallregeln, Filterung in IOChain und DVfilter, fehlender VLAN-Übereinstimmung, Fehlfunktionen eines physikalischen Adapters, Prüfsummenfehler usw. Mit dem Dienstprogramm `pktcap-uw` können Sie untersuchen, wo die Pakete verloren gehen und was der Grund hierfür ist.

Verfahren

- 1 Führen Sie in der ESXi Shell für den Host den Befehl `pktcap-uw --capture Drop` mit Optionen zum Überwachen von Paketen an einem bestimmten Punkt, zum Filtern erfasster Pakete und zum Speichern der Ergebnisse in einer Datei aus.

```
pktcap-uw --capture Drop [filter_options] [--outfile pcap_file_path [--ng]] [--count
number_of_packets]
```

wobei die Optionen des Befehls `pktcap-uw--capture Drop` in eckigen Klammern [] angegeben sind und die vertikale Linie | für alternative Werte steht.

- a Verwenden Sie *Filteroptionen*, um Pakete nach Quell- und Zieladresse, VLAN ID, VXLAN ID, Schicht 3-Protokoll und TCP-Port zu filtern.

Zum Überwachen der Pakete von einem Quellsystem – beispielsweise mit der IP-Adresse 192.168.25.113 – verwenden Sie z. B. die Filteroption `--srcip 192.168.25.113`.

- b Verwenden Sie Optionen zum Speichern der Inhalte jedes Pakets oder einer bestimmten Anzahl von Paketen in eine `.pcap`- oder `.pcapng`-Datei.
 - Um Pakete in eine `.pcap`-Datei zu speichern, verwenden Sie die Option `--outfile`.
 - Um Pakete in eine `.pcapng`-Datei zu speichern, verwenden Sie die Optionen `--ng` und `--outfile`.

Sie können die Datei in einem Netzwerkanalyssetool wie Wireshark öffnen.

Standardmäßig speichert das Dienstprogramm `pktcap-uw` die Paketdateien im Root-Ordner des ESXi-Dateisystems.

Hinweis Sie können den Grund und die Stelle, an der das Paket verloren geht, nur anzeigen, wenn Sie Pakete erfassen und an die Konsole ausgeben. Das Dienstprogramm `pktcap-uw` speichert nur die Inhalte von Paketen in einer `.pcap`- oder `.pcapng`-Datei.

- c Verwenden Sie die Option `--count`, um nur eine bestimmte Anzahl von Paketen zu überwachen.
- 2 Wenn Sie die Anzahl der Pakete nicht mit der Option `--count` beschränkt haben, drücken Sie STRG+C, um die Erfassung oder Nachverfolgung von Paketen zu beenden.

Ergebnisse

Neben den Inhalten der verloren gegangenen Pakete werden in der Ausgabe des Dienstprogramms `pktcap-uw` der Grund für den Verlust und die Funktion im Netzwerk-Stack, der das Paket zuletzt verarbeitet hat, angezeigt.

Nächste Schritte

Wenn der Inhalt des Pakets in eine Datei gespeichert wird, kopieren Sie die Datei vom ESXi-Host auf das System, auf dem ein grafisches Analysetool wie Wireshark ausgeführt wird, und öffnen Sie es in diesem Tool, um die Paketdetails zu untersuchen.

Erfassen von Paketen auf DVFilter-Ebene

Untersuchen Sie, wie Pakete sich ändern, wenn sie durch eine vSphere Network Appliance (DVFilter) geleitet werden.

DVFilter sind Agenten, die sich im Datenstrom zwischen einem VM-Adapter und einem virtuellen Switch befinden. Sie fangen Pakete ab, um virtuelle Maschinen vor Angriffen auf die Sicherheit und unerwünschtem Datenverkehr zu schützen.

Verfahren

- 1 (Optional) Um den Namen des DVFilter zu finden, den Sie überwachen möchten, führen Sie in der ESXi Shell den Befehl `summarize-dvfilter` aus.

Die Ausgabe des Befehls enthält den Fast-Path- und den Slow-Path-Agent der auf dem Host bereitgestellten DVFilter.

- 2 Führen Sie das Dienstprogramm `pktcap-uw` mit dem Argument `--dvfilterDVFilter-Name` und Optionen zum Überwachen von Paketen an bestimmten Punkten, zum Filtern erfasster Pakete und zum Speichern des Ergebnisses in einer Datei aus.

```
pktcap-uw
--dvFilter
dvfilter_name
--capture PreDVFilter|PostDVFilter [filter_options] [--outfilepcap_file_path
[--ng]] [--countnumber_of_packets]
```

wobei die optionalen Elemente des Befehls `pktcap-uw--dvFilter vmnicX` in eckigen Klammern `[]` angegeben sind und die vertikale Linie `|` für alternative Werte steht.

- a Verwenden Sie die Option `--capture` zum Überwachen von Paketen, bevor oder nachdem sie vom DVFilter abgefangen werden.

Befehlsoption <code>pktcap-uw</code>	Ziel
<code>--capture PreDVFilter</code>	Erfasst Pakete, bevor sie den DVFilter durchlaufen.
<code>--capture PostDVFilter</code>	Erfasst Pakete, nachdem sie den DVFilter verlassen.

- b Verwenden Sie *Filteroptionen*, um Pakete nach Quell- und Zieladresse, VLAN ID, VXLAN ID, Schicht 3-Protokoll und TCP-Port zu filtern.

Zum Überwachen der Pakete von einem Quellsystem – beispielsweise mit der IP-Adresse 192.168.25.113 – verwenden Sie z. B. die Filteroption `--srcip 192.168.25.113`.

- c Verwenden Sie Optionen zum Speichern der Inhalte jedes Pakets oder einer bestimmten Anzahl von Paketen in eine `.pcap`- oder `.pcapng`-Datei.

- Um Pakete in eine `.pcap`-Datei zu speichern, verwenden Sie die Option `--outfile`.
- Um Pakete in eine `.pcapng`-Datei zu speichern, verwenden Sie die Optionen `--ng` und `--outfile`.

Sie können die Datei in einem Netzwerkanalysetool wie Wireshark öffnen.

Standardmäßig speichert das Dienstprogramm `pktcap-uw` die Paketdateien im Root-Ordner des ESXi-Dateisystems.

- d Verwenden Sie die Option `--count`, um nur eine bestimmte Anzahl von Paketen zu überwachen.

- 3 Wenn Sie die Anzahl der Pakete nicht mit der Option `--count` beschränkt haben, drücken Sie STRG+C, um die Erfassung oder Nachverfolgung von Paketen zu beenden.

Nächste Schritte

Wenn der Inhalt des Pakets in eine Datei gespeichert wird, kopieren Sie die Datei vom ESXi-Host auf das System, auf dem ein grafisches Analysetool wie Wireshark ausgeführt wird, und öffnen Sie es in diesem Tool, um die Paketdetails zu untersuchen.

Verwenden der Erfassungspunkte des Dienstprogramms `pktcap-uw`

Sie können die Erfassungspunkte des Dienstprogramms `pktcap-uw` verwenden, um Pakete zu überwachen, wenn eine Funktion sie an einer bestimmten Stelle in der Netzwerkkarte auf einem Host verwendet.

Übersicht über Erfassungspunkte

Ein Erfassungspunkt im Dienstprogramm `pktcap-uw` stellt eine Stelle im Pfad zwischen einem virtuellen Switch auf der einen und einem physikalischen Adapter, einem VMkernel-Adapter oder einem Adapter einer virtuellen Maschine auf der anderen Seite dar.

Sie können bestimmte Erfassungspunkte in Verbindung mit einer Adapteroption verwenden. Verwenden Sie beispielsweise den UplinkRcv-Punkt, wenn Sie Uplink-Datenverkehr erfassen. Sie können andere Punkte eigenständig wählen. Verwenden Sie beispielsweise den Drop-Point, um alle nicht übermittelten Pakete zu überprüfen.

Hinweis Bestimmte Erfassungspunkte des Dienstprogramms `pktcap-uw` wurden nur für die interne Nutzung in VMware entwickelt. Sie sollten Sie nur unter Aufsicht des technischen Supports von VMware verwenden. Diese Erfassungspunkte werden nicht im *vSphere-Netzwerk* Handbuch beschrieben.

Nutzungsmöglichkeiten der Erfassungspunkte des Dienstprogramms `pktcap-uw`

Um einen Paketstatus oder Inhalt an einem Erfassungspunkt zu überprüfen, fügen Sie die Option `--capture capture_point` zum Dienstprogramm `pktcap-uw` hinzu.

Automatische Auswahl eines Erfassungspunktes

Für Verkehr in Verbindung mit einem physikalischen, VMkernel- oder VMXNET3-Adapter können Sie zwischen den Erfassungspunkten automatisch wählen und wechseln, indem Sie die `--dir` und `--stage` Optionen verbinden, um zu überprüfen, wie sich ein Paket vor und nach einem Punkt ändert.

Erfassungspunkte des Dienstprogramms `pktcap-uw`

Das Dienstprogramm `pktcap-uw` unterstützt Erfassungspunkte, die nur bei der Überwachung von Uplink-, VMkernel- oder VM-Datenverkehr verwendet werden können, sowie Erfassungspunkte, die bestimmte Stellen in einem Stack repräsentieren, die nicht mit dem Adaptertyp in Zusammenhang stehen.

Erfassungspunkte, die für Datenverkehr auf dem physischen Adapter relevant sind

Der Befehl `pktcap-uw --uplink vmnicX` unterstützt Erfassungspunkte für Funktionen zum Verarbeiten von Datenverkehr an einem bestimmten Ort und mit einer bestimmten Richtung im Pfad zwischen dem physischen Adapter und dem virtuellen Switch.

Erfassungspunkt	Beschreibung
UplinkRcv	Die Funktion, die Pakete vom physischen Adapter empfängt.
UplinkSnd	Die Funktion, die Pakete an den physischen Adapter sendet.
PortInput	Die Funktion, die eine Liste von Paketen von UplinkRcv an einen Port auf dem virtuellen Switch übergibt.
PortOutput	Die Funktion, die eine Liste von Paketen von einem Port auf dem virtuellen Switch an den UplinkSnd-Punkt übergibt.

Erfassungspunkte, die für Datenverkehr auf der virtuellen Maschine relevant sind

Der Befehl `pktcap-uw --switchport vmxnet3_port_ID` unterstützt Erfassungspunkte für Funktionen zum Verarbeiten von Datenverkehrspaketen an einem bestimmten Ort und mit einer bestimmten Richtung im Pfad zwischen einem VMXNET3-Adapter und einem virtuellen Switch.

Erfassungspunkt	Beschreibung
VnicRx	Die Funktion im NIC-Backend der virtuellen Maschine, die Pakete vom virtuellen Switch empfängt.
VnicTx	Die Funktion im NIC-Backend der virtuellen Maschine, die Pakete von der virtuellen Maschine an den virtuellen Switch sendet.
PortOutput	Die Funktion, die eine Liste von Paketen von einem Port auf dem virtuellen Switch an Vmxnet3Rx übergibt.
PortInput	Die Funktion, die eine Liste von Paketen von Vmxnet3Tx an einen Port auf dem virtuellen Switch übergibt. Standarderfassungspunkt für Datenverkehr im Zusammenhang mit einem VMXNET3-Adapter.

Erfassungspunkte, die für Datenverkehr auf dem VMkernel-Adapter relevant sind

Die Befehle `pktcap-uw --vmk vmkX` und `pktcap-uw --switchport vmkernel_adapter_port_ID` unterstützen Erfassungspunkte, die Funktionen an einem bestimmten Ort und mit einer bestimmten Richtung im Pfad zwischen einem VMkernel-Adapter und einem virtuellen Switch darstellen.

Erfassungspunkt	Beschreibung
PortOutput	Die Funktion, die eine Liste von Paketen von einem Port auf dem virtuellen Switch an den VMkernel-Adapter übergibt.
PortInput	Die Funktion, die eine Liste von Paketen vom VMkernel-Adapter an einen Port auf dem virtuellen Switch übergibt. Standarderfassungspunkt für Datenverkehr im Zusammenhang mit einem VMkernel-Adapter.

Erfassungspunkte, die für verteilte virtuelle Filter relevant sind

Der Befehl `pktcap-uw --dvfilter divfilter_name` erfordert einen Erfassungspunkt, der angibt, ob Pakete, die den DVFilter durchlaufen, erfasst werden oder nicht.

Erfassungspunkt	Beschreibung
PreDVFilter	Der Punkt, bevor ein DVFilter ein Paket abfängt.
PostDVFilter	Der Punkt, nachdem ein DVFilter ein Paket abfängt.

Eigenständige Erfassungspunkte

Bestimmte Erfassungspunkte werden nicht einem physischen, VMkernel- oder VMXNET3-Adapter, sondern dem Netzwerk-Stack direkt zugeordnet.

Erfassungspunkt	Beschreibung
Verwerfen	Erfasst verloren gegangene Pakete und zeigt an, an welcher Stelle sie verloren gegangen sind.
TcpipDispatch	Erfasst Pakete an der Funktion, die Datenverkehr vom virtuellen Switch an den TCP/IP-Stack des VMkernel sendet, und umgekehrt.
PktFree	Erfasst Pakete unmittelbar vor deren Freigabe.
VdrRxLeaf	Erfasst Pakete an der E/A-Kette des Empfangsblatts eines dynamischen Routers in VMware NSX. Verwenden Sie diesen Erfassungspunkt zusammen mit der Option <code>--lifID</code> .
VdrRxTerminal	Erfasst Pakete an der E/A-Kette des Empfangsterminals eines dynamischen Routers in VMware NSX. Verwenden Sie diesen Erfassungspunkt zusammen mit der Option <code>--lifID</code> .
VdrTxLeaf	Erfasst Pakete an der E/A-Kette des Übertragungsblatts eines dynamischen Routers in VMware NSX. Verwenden Sie diesen Erfassungspunkt zusammen mit der Option <code>--lifID</code> .
VdrTxTerminal	Erfasst Pakete an der E/A-Kette des Übertragungsterminals eines dynamischen Routers in VMware NSX. Verwenden Sie diesen Erfassungspunkt zusammen mit der Option <code>--lifID</code> .

Weitere Informationen zu dynamischen Routern finden Sie in der *VMware NSX*-Dokumentation.

Auflisten der Erfassungspunkte des Dienstprogramms `pktcap-uw`

Lassen Sie sich alle Erfassungspunkte des Dienstprogramms `pktcap-uw` anzeigen, um den Namen des Erfassungspunktes zur Überwachung von Datenverkehr an einer bestimmten Stelle in den Netzwerkkarten auf dem Host ESXi zu suchen.

Für Informationen zu den Erfassungspunkten des Dienstprogramms `pktcap-uw`, siehe [Erfassungspunkte des Dienstprogramms `pktcap-uw`](#).

Verfahren

- ◆ Starten Sie den Befehl `pktcap-uw -A` in ESXi Shell an den Host, um alle Erfassungspunkte anzeigen zu lassen, die das Dienstprogramm `pktcap-uw` unterstützt.

Nachverfolgen von Paketen mithilfe des Dienstprogramms `pktcap-uw`

Verfolgen Sie mithilfe des Dienstprogramms `pktcap-uw` den Pfad nach, den die Pakete im Netzwerk-Stack durchlaufen, um eine Latenzanalyse durchzuführen und den Punkt zu ermitteln, an dem das Paket beschädigt worden oder verloren gegangen ist.

Das Dienstprogramm `pktcap-uw` zeigt den Pfad der Pakete und den jeweiligen Zeitstempel der Verarbeitung eines Pakets durch eine Netzwerkfunktion auf ESXi an. Das Dienstprogramm gibt den Pfad eines Pakets unmittelbar vor dessen Freigabe aus dem Stack aus.

Um die vollständigen Pfadinformationen für ein Paket anzuzeigen, müssen Sie das Ergebnis des Dienstprogramms `pktcap-uw` in die Konsolenausgabe drucken oder in einer PCAPNG-Datei speichern.

Verfahren

- 1 Führen Sie in der ESXi Shell für den Host den Befehl `pktcap-uw--trace` aus und verwenden Sie Optionen zum Filtern nachverfolgter Pakete, zum Speichern der Ergebnisse in einer Datei und zum Begrenzen der Anzahl nachverfolgter Pakete.

```
pktcap-uw
--trace [filter_options] [--outfilepcap_file_path [--ng]]
[--countnumber_of_packets]
```

wobei die optionalen Elemente des Befehls `pktcap-uw --trace` in eckigen Klammern `[]` angegeben sind und die vertikale Linie `|` für alternative Werte steht.

- a Verwenden Sie *Filteroptionen*, um Pakete nach Quell- und Zieladresse, VLAN ID, VXLAN ID, Schicht 3-Protokoll und TCP-Port zu filtern.

Zum Überwachen der Pakete von einem Quellsystem – beispielsweise mit der IP-Adresse 192.168.25.113 – verwenden Sie z. B. die Filteroption `--srcip 192.168.25.113`.

- b Verwenden Sie Optionen zum Speichern der Inhalte jedes Pakets oder einer bestimmten Anzahl von Paketen in eine `.pcap`- oder `.pcapng`-Datei.
 - Um Pakete in eine `.pcap`-Datei zu speichern, verwenden Sie die Option `--outfile`.
 - Um Pakete in eine `.pcapng`-Datei zu speichern, verwenden Sie die Optionen `--ng` und `--outfile`.

Sie können die Datei in einem Netzwerkanalysetool wie Wireshark öffnen.

Standardmäßig speichert das Dienstprogramm `pktcap-uw` die Paketdateien im Root-Ordner des ESXi-Dateisystems.

Hinweis Eine `.pcap`-Datei enthält nur die Inhalte nachverfolgter Pakete. Um zusätzlich zu Paketinhalten auch Paketpfade zu erfassen, speichern Sie die Ausgabe in einer `.pcapng`-Datei.

- c Verwenden Sie die Option `--count`, um nur eine bestimmte Anzahl von Paketen zu überwachen.
- 2 Wenn Sie die Anzahl der Pakete nicht mit der Option `--count` beschränkt haben, drücken Sie STRG+C, um die Erfassung oder Nachverfolgung von Paketen zu beenden.

Nächste Schritte

Wenn der Inhalt des Pakets in eine Datei gespeichert wird, kopieren Sie die Datei vom ESXi-Host auf das System, auf dem ein grafisches Analysetool wie Wireshark ausgeführt wird, und öffnen Sie es in diesem Tool, um die Paketdetails zu untersuchen.

Konfigurieren der NetFlow-Einstellungen eines vSphere Distributed Switch

Analysieren Sie den IP-Datenverkehr der virtuellen Maschine, der über den vSphere Distributed Switch geleitet wird, indem Sie Berichte an einen NetFlow-Collector senden.

Version 5.1 und spätere Versionen von vSphere Distributed Switch unterstützen IPFIX (NetFlow Version 10).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Einstellungen > NetFlow bearbeiten**.
- 3 Geben Sie die **IP-Adresse des Collectors** und den **Collector-Port** des NetFlow-Collectors ein. Sie können den NetFlow-Collector per IPv4- oder IPv6-Adresse kontaktieren.
- 4 Legen Sie eine **Beobachtungsdomänen-ID** fest, die die Informationen bezüglich des Switch identifiziert.
- 5 Um die Informationen vom Distributed Switch im NetFlow-Collector unter einem einzigen Netzwerkgerät anstatt eines getrennten Geräts für jeden Host auf dem Switch anzuzeigen, geben Sie eine IPv4-Adresse in das Textfeld **IP-Adresse des Switches** ein.
- 6 (Optional) Legen Sie in den Textfeldern **Zeitüberschreitung bei aktivem Flow-Export** und **Zeitüberschreitung bei Flow-Export im Leerlauf** die Uhrzeit in Sekunden fest, die gewartet wird, bevor nach dem Initiieren des Flows Informationen gesendet werden.
- 7 (Optional) Um den Teil der Daten zu ändern, die vom Switch erfasst werden, konfigurieren Sie die **Sampling-Rate**.

Die Sampling-Rate repräsentiert die Anzahl der Pakete, die NetFlow nach jedem erfassten Paket löscht. Eine Sampling-Rate von x ist eine Anweisung an NetFlow, Pakete in einem Verhältnis *erfasste Pakete* : *gelöschte Pakete* von 1 : x zu löschen. Liegt die Rate bei 0, erfasst NetFlow alle Pakete, d. h., ein Paket wird erfasst und keine werden gelöscht. Liegt die Rate bei 1, erfasst NetFlow ein Paket und löscht das nächste usw.

- 8 (Optional) Wenn Daten nur bei Netzwerkaktivität zwischen virtuellen Maschinen auf demselben Host erfasst werden sollen, aktivieren Sie die Option **Nur interne Flows verarbeiten**.

Erfassen Sie interne Flows nur, wenn NetFlow auf dem physischen Netzwerkgerät aktiviert ist, um zu vermeiden, dass duplizierte Informationen vom Distributed Switch und dem physischen Netzwerkgerät gesendet werden.

9 Klicken Sie auf **OK**.

Nächste Schritte

Aktivieren Sie NetFlow-Berichte für Netzwerkdatenverkehr von virtuellen Maschinen, die mit einer verteilten Portgruppe oder einem Port verbunden sind. Siehe [Aktivieren oder Deaktivieren der NetFlow-Überwachung auf einer verteilten Portgruppe oder einem verteilten Port](#).

Arbeiten mit der Portspiegelung

Die Portspiegelung ermöglicht Ihnen, den Datenverkehr von einem verteilten Port an andere verteilte Ports oder bestimmte physische Switch-Ports zu spiegeln.

Die Portspiegelungsfunktion wird auf einem Switch verwendet, um eine Kopie von Paketen, die auf einem Switch-Port (oder einem kompletten VLAN) angezeigt werden, an einen überwachenden Anschluss an einem anderen Switch-Port zu senden. Die Portspiegelungsfunktion verwendet, um Daten zu analysieren und zu reparieren oder Fehler in einem Netzwerk zu diagnostizieren.

Portspiegelung - Versionskompatibilität

Bestimmte Portspiegelungsfunktionen in vSphere 5.1 und höher sind abhängig von der Version von vCenter Server, dem vSphere Distributed Switch und dem Host, die Sie einsetzen, sowie davon, wie Sie diese Aspekte von vSphere zusammen verwenden.

Tabelle 14-5. Portspiegelungskompatibilität

vCenter Server-Version	Version des vSphere Distributed Switch	Hostversion	vSphere 5.1-Portspiegelungsfunktionalität
vSphere 5.1 und höher	vSphere 5.1 und höher	vSphere 5.1 und höher	Die Portspiegelung von vSphere 5.1 kann verwendet werden. Funktionen für die Portspiegelung von vSphere 5.0 und vorherigen Versionen stehen nicht zur Verfügung.
vSphere 5.1 und höher	vSphere 5.1 und höher	vSphere 5.0 und früher	vSphere 5.0 und frühere Hosts können zu vSphere 5.1 vCenter Server hinzugefügt werden, zu Distributed Switches der Version 5.1 und höher können sie jedoch nicht hinzugefügt werden.
vSphere 5.1 und höher	vSphere 5.0	vSphere 5.0	vSphere vCenter Server 5.1 und höher kann die Portspiegelung auf einem vSphere 5.0 Distributed Switch konfigurieren.

Tabelle 14-5. Portspiegelungskompatibilität (Fortsetzung)

vCenter Server-Version	Version des vSphere Distributed Switch	Hostversion	vSphere 5.1-Portspiegelungsfunktionalität
vSphere 5.1 und höher	vSphere 5.0	vSphere 5.1 und höher	Hosts, auf denen vSphere 5.1 ausgeführt wird, können zu vSphere 5.0 Distributed Switches hinzugefügt werden und die vSphere 5.0 Portspiegelung unterstützen.
vSphere 5.1 und höher	Vor vSphere 5.0	vSphere 5.5 und früher	Portspiegelung wird nicht unterstützt.
vSphere 5.0 und früher	vSphere 5.0 und früher	vSphere 5.1	Ein vSphere 5.1-Host kann nicht zu vCenter Server 5.0 und früher hinzugefügt werden.

Wenn Sie ein Hostprofil mit Portspiegelungseinstellungen verwenden, muss das Hostprofil an die neue Version der Portspiegelung in vSphere 5.1 und höher angepasst werden.

Portspiegelung - Interoperabilität

Bei Verwendung der vSphere-Portspiegelung zusammen mit anderen Funktionen von vSphere sind einige Interoperabilitätsprobleme zu berücksichtigen.

vMotion

Je nachdem, welchen Typ von vSphere-Portspiegelungssitzung Sie auswählen, funktioniert vMotion unterschiedlich. Während eines vMotion-Vorgangs kann ein Spiegelungspfad vorübergehend ungültig werden. Dieser Pfad wird jedoch wiederhergestellt, sobald der vMotion-Vorgang abgeschlossen ist.

Tabelle 14-6. Interoperabilität der Portspiegelung mit vMotion

Typ der Portspiegelungssitzung	Quelle und Ziel	Interoperabilität mit vMotion	Funktionalität
Spiegelung verteilter Ports	Quelle und Ziel eines verteilten Nicht-Uplink-Ports	Ja	Die Portspiegelung zwischen verteilten Ports kann nur lokal sein. Wenn sich aufgrund von vMotion die Quelle und das Ziel auf unterschiedlichen Hosts befinden, funktioniert die Spiegelung zwischen ihnen nicht. Wenn jedoch die Quelle und das Ziel auf denselben Host verschoben werden, funktioniert die Portspiegelung.
Remotespiegelungsquelle	Quelle eines verteilten Nicht-Uplink-Ports	Ja	Wenn ein verteilter Port, der als Quelle dient, von Host A auf Host B verschoben wird, wird der ursprüngliche Spiegelungspfad vom Quellport zum Uplink von Host A auf Host A entfernt und ein neuer Spiegelungspfad vom Quellport zum Uplink von Host B wird auf Host B erstellt. Der Uplink, der schließlich verwendet wird, wird vom in der Sitzung angegebenen Uplink-Namen bestimmt.
	Uplink-Port-Ziele	Nein	Uplinks können nicht von vMotion verschoben werden.
Remotespiegelungsziel	VLAN-Quelle	Nein	
	Ziel eines verteilten Nicht-Uplink-Ports	Ja	Wenn ein verteilter Port, der als Ziel dient, von Host A auf Host B verschoben wird, werden alle ursprünglichen Spiegelungspfade von Quell-VLANs zum Zielpport von Host A auf Host B verschoben.

Tabelle 14-6. Interoperabilität der Portspiegelung mit vMotion (Fortsetzung)

Typ der Portspiegelungssitzung	Quelle und Ziel	Interoperabilität mit vMotion	Funktionalität
Gekapselte Remotespiegelungsquelle (L3)	Quelle eines verteilten Nicht-Uplink-Ports	Ja	Wenn ein verteilter Port, der als Quelle dient, von Host A auf Host B verschoben wird, werden alle ursprünglichen Spiegelungspfade vom Quellport auf die Ziel-IP-Adressen von Host A auf Host B verschoben.
	IP-Ziel	Nein	
Spiegelung verteilter Ports (Legacy)	IP-Quelle	Nein	
	Ziel eines verteilten Nicht-Uplink-Ports	Nein	Wenn ein verteilter Port, der als Ziel dient, von Host A auf Host B verschoben wird, sind alle ursprünglichen Spiegelungspfade von den Quell-IP-Adressen auf den Zielport ungültig, da die Quelle der Portspiegelungssitzung nach wie vor das Ziel auf Host A sieht.

TSO und LRO

TSO (TCP Segmentation Offload) und LRO (Large Receive Offload) sorgen möglicherweise dafür, dass die Anzahl der Spiegelungspakete nicht mit der Anzahl der gespiegelten Pakete übereinstimmt.

Wenn TSO auf einer vNIC aktiviert ist, sendet die vNIC möglicherweise ein umfangreiches Paket an einen Distributed Switch. Wenn LRO auf einer vNIC aktiviert ist, werden kleine Pakete, die an die vNIC gesendet werden, möglicherweise in einem großen Paket zusammengefasst.

Quelle	Ziel	Beschreibung
TSO	LRO	Pakete von der Quell-vNIC sind möglicherweise große Pakete. Ob sie aufgeteilt werden, hängt davon ab, ob ihre Größen den LRO-Grenzwert der Ziel-vNIC überschreiten.
TSO	Beliebiges Ziel	Pakete von der Quell-vNIC sind möglicherweise große Pakete und werden an der Ziel-vNIC in Standardpakete aufgeteilt.
Beliebige Quelle	LRO	Pakete von der Quell-vNIC sind Standardpakete und werden möglicherweise an der Ziel-vNIC in größere Pakete zusammengefasst.

Erstellen einer Portspiegelungssitzung

Erstellen Sie mit dem vSphere Web Client eine Portspiegelungssitzung, um den Datenverkehr eines vSphere Distributed Switch auf Ports, Uplinks und Remote-IP-Adressen zu spiegeln.

Voraussetzungen

Stellen Sie sicher, dass der vSphere Distributed Switch die Version 5.0.0 oder höher aufweist.

Verfahren

1 Auswählen eines Typs der Portspiegelungssitzung

Um eine Portspiegelungssitzung zu beginnen, müssen Sie den Typ der Portspiegelungssitzung angeben.

2 Festlegen des Portspiegelungsnamens und von Sitzungsdetails

Um mit dem Erstellen einer Portspiegelungssitzung fortzufahren, geben Sie Namen, Beschreibung und Sitzungsdetails für die neue Portspiegelungssitzung ein.

3 Auswählen von Portspiegelungsquellen

Um mit dem Erstellen einer Portspiegelungssitzung fortzufahren, wählen Sie Quellen und die Datenverkehrsrichtung für die neue Portspiegelungssitzung.

4 Auswählen von Portspiegelungszielen und Überprüfen von Einstellungen

Um die Erstellung einer Portspiegelung abzuschließen, wählen Sie Ports oder Uplinks als Ziele für die Portspiegelungssitzung aus.

Auswählen eines Typs der Portspiegelungssitzung

Um eine Portspiegelungssitzung zu beginnen, müssen Sie den Typ der Portspiegelungssitzung angeben.

Verfahren

- 1 Navigieren Sie zu einem Distributed Switch im Navigator von vSphere Web Client.
- 2 Klicken Sie auf die Registerkarte **Verwalten**, und wählen Sie **Einstellungen > Portspiegelung**.
- 3 Klicken Sie auf **Neu**.
- 4 Wählen Sie den Sitzungstyp für die Portspiegelungssitzung.

Option	Beschreibung
Spiegelung verteilter Ports	Spiegeln Sie Pakete von mehreren verteilten Ports an andere verteilte Ports auf demselben Host. Wenn Quelle und Ziel auf verschiedenen Hosts liegen, funktioniert dieser Sitzungstyp nicht.
Remotespiegelungsquelle	Spiegeln Sie Pakete von mehreren verteilten Ports an bestimmte Uplink-Ports auf dem entsprechenden Host.
Remotespiegelungsziel	Spiegeln Sie Pakete von mehreren VLANs an verteilte Ports.

Option	Beschreibung
Gekapselte Remotespiegelungsquelle (L3)	Spiegeln Sie Pakete von mehreren verteilten Ports an die IP-Adressen des Remoteagenten. Der Datenverkehr der virtuellen Maschine wird auf einem entfernten physischen Remoteziel über einen IP-Tunnel gespiegelt.
Spiegelung verteilter Ports (Legacy)	Spiegeln Sie Pakete von mehreren verteilten Ports an mehrere verteilte Ports und/oder Uplink-Ports auf dem entsprechenden Host.

5 Klicken Sie auf **Weiter**.

Festlegen des Portspiegelungsnamens und von Sitzungsdetails

Um mit dem Erstellen einer Portspiegelungssitzung fortzufahren, geben Sie Namen, Beschreibung und Sitzungsdetails für die neue Portspiegelungssitzung ein.

Verfahren

- Legen Sie die Sitzungseigenschaften fest. Je nach dem ausgewählten Sitzungstyp sind verschiedene Optionen für die Konfiguration verfügbar.

Option	Beschreibung
Name	Sie können einen eindeutigen Namen für die Portspiegelungssitzung eingeben oder den automatisch generierten Sitzungsamen übernehmen.
Status	Verwenden Sie das Dropdown-Menü zum Aktivieren oder Deaktivieren der Sitzung.
Sitzungstyp	Zeigt den ausgewählten Sitzungstyp an.
Normal-E/A auf Zielports	Verwenden Sie das Dropdown-Menü, um normale E/A-Vorgänge auf Zielports zuzulassen oder nicht zuzulassen. Diese Eigenschaft ist nur für Uplink-Portziele und verteilte Portziele verfügbar. Wenn Sie diese Option sperren, wird ausgehender gespiegelter Datenverkehr auf den Zielports zugelassen, aber eingehender Datenverkehr nicht.
Länge des gespiegelten Pakets (in Byte)	Verwenden Sie das Kontrollkästchen, um die Länge des gespiegelten Pakets in Byte zu aktivieren. Es wird ein Grenzwert für die Größe von gespiegelten Frames festgelegt. Wenn diese Option ausgewählt ist, werden alle gespiegelten Frames auf die angegebene Länge gekürzt.
Sampling-Rate	Wählen Sie die Rate, mit der Pakete gesampelt werden. Dies wird standardmäßig für alle Portspiegelungssitzungen mit Ausnahme von Legacy-Sitzungen aktiviert.
Beschreibung	Sie können eine Beschreibung für die Konfiguration der Portspiegelungssitzung eingeben.

2 Klicken Sie auf **Weiter**.

Auswählen von Portspiegelungsquellen

Um mit dem Erstellen einer Portspiegelungssitzung fortzufahren, wählen Sie Quellen und die Datenverkehrsrichtung für die neue Portspiegelungssitzung.

Sie können eine Portspiegelungssitzung ohne Einstellen der Quelle und des Ziels erstellen. Wenn eine Quelle und ein Ziel nicht eingestellt sind, wird eine Portspiegelungssitzung ohne den Spiegelpfad erstellt. Damit erhalten Sie die Möglichkeit, eine Portspiegelungssitzung mit den richtigen Eigenschaftseinstellungen zu erstellen. Nachdem die Eigenschaften eingestellt wurden, können Sie die Portspiegelungssitzung bearbeiten, um die Quellen und Zielinformationen hinzuzufügen.

Verfahren

- 1 Wählen Sie die Quelle des Datenverkehrs, der gespiegelt werden soll, und die Datenverkehrsrichtung.

Abhängig vom Typ der ausgewählten Portspiegelungssitzung stehen verschiedene Optionen für die Konfiguration zur Verfügung.

Option	Beschreibung
Fügen Sie vorhandene Ports aus einer Liste hinzu.	Klicken Sie auf Verteilte Ports auswählen . Ein Dialogfeld zeigt eine Liste von bestehenden Ports an. Aktivieren Sie das Kontrollkästchen neben dem verteilten Port, und klicken Sie auf OK . Sie können mehr als einen verteilten Port auswählen.
Vorhandene Ports nach Portnummer hinzufügen	Klicken Sie auf Verteilte Ports hinzufügen , geben Sie die Portnummer ein und klicken Sie auf OK .
Datenverkehrsrichtung festlegen	Wählen Sie nach dem Hinzufügen der Ports in der Liste den Port aus, und klicken Sie auf die Schaltfläche „Ingress“, „Egress“ oder „Ingress/Egress“. Ihre Auswahl wird in der Spalte „Datenverkehrsrichtung“ angezeigt.
Quell-VLAN angeben	Wenn Sie einen Sitzungstyp mit Remotespiegelungsziel ausgewählt haben, müssen Sie das Quell-VLAN angeben. Klicken Sie auf Hinzufügen , um eine VLAN-ID hinzuzufügen. Bearbeiten Sie die ID mit den Pfeilen nach oben und nach unten, oder klicken Sie in das Feld und geben Sie die VLAN-ID manuell ein.

- 2 Klicken Sie auf **Weiter**.

Auswählen von Portspiegelungszielen und Überprüfen von Einstellungen

Um die Erstellung einer Portspiegelung abzuschließen, wählen Sie Ports oder Uplinks als Ziele für die Portspiegelungssitzung aus.

Sie können eine Portspiegelungssitzung ohne Einstellen der Quelle und des Ziels erstellen. Wenn eine Quelle und ein Ziel nicht eingestellt sind, wird eine Portspiegelungssitzung ohne den Spiegelpfad erstellt. Damit erhalten Sie die Möglichkeit, eine Portspiegelungssitzung mit den richtigen Eigenschaftseinstellungen zu erstellen. Nachdem die Eigenschaften eingestellt wurden, können Sie die Portspiegelungssitzung bearbeiten, um die Quellen und Zielinformationen hinzuzufügen.

Die Portspiegelung wird anhand der VLAN-Weiterleitungsrichtlinie überprüft. Wenn das VLAN der ursprünglichen Frames nicht gleich dem Zielpport ist oder von ihm getrunkt wird, werden die Frames nicht gespiegelt.

Verfahren

- 1 Wählen Sie das Ziel für die Portspiegelungssitzung aus.

Abhängig vom ausgewählten Sitzungstyp sind verschiedene Optionen verfügbar.

Option	Beschreibung
Verteilten Zielport auswählen	Klicken Sie auf Verteilte Ports auswählen , um Ports aus einer Liste auszuwählen, oder klicken Sie auf Verteilte Ports hinzufügen , um Ports nach Portnummern hinzuzufügen. Sie können mehr als einen verteilten Port hinzufügen.
Auswählen eines Uplinks	Wählen Sie in der Liste einen verfügbaren Uplink aus, und klicken Sie auf Hinzufügen , um den Uplink der Portspiegelungssitzung hinzuzufügen. Sie können mehr als einen Uplink auswählen.
Ports oder Uplinks auswählen	Klicken Sie auf Verteilte Ports auswählen , um Ports aus einer Liste auszuwählen, oder klicken Sie auf Verteilte Ports hinzufügen , um Ports nach Portnummern hinzuzufügen. Sie können mehr als einen verteilten Port hinzufügen. Klicken Sie auf Uplinks hinzufügen , um dem Ziel Uplinks hinzuzufügen. Wählen Sie Uplinks in der Liste aus, und klicken Sie auf OK .
IP-Adresse angeben	Klicken Sie auf Hinzufügen . Ein neuer Listeneintrag wird erstellt. Wählen Sie den Eintrag und klicken Sie auf Bearbeiten , um die IP-Adressen einzugeben, oder klicken Sie direkt in das IP-Adressenfeld und geben Sie die IP-Adresse ein. Wenn die IP-Adresse ungültig ist, erscheint eine Warnung.

- 2 Klicken Sie auf **Weiter**.
- 3 Prüfen Sie die Informationen, die Sie für die Portspiegelungssitzung eingegeben haben, auf der Seite **Bereit zum Abschließen**.
- 4 (Optional) Bearbeiten Sie die Informationen mit der Schaltfläche **Zurück**.
- 5 Klicken Sie auf **Beenden**.

Ergebnisse

Die neue Portspiegelungssitzung wird im Abschnitt „Portspiegelung“ auf der Registerkarte **Einstellungen** angezeigt.

Anzeigen von Details zu einer Portspiegelungssitzung

Zeigen Sie Details zu einer Portspiegelungssitzung an, wie Status, Quellen und Ziele.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie auf der Registerkarte **Verwalten** die Option **Einstellungen > Portspiegelung**.
- 3 Wählen Sie eine Portspiegelungssitzung aus der Liste aus, um unten am Bildschirm die zugehörigen Details anzuzeigen. Mittels der Registerkarten können Sie die Konfigurationsdetails überprüfen.

- 4 (Optional) Klicken Sie auf **Neu**, um eine neue Portspiegelungssitzung hinzuzufügen.
- 5 (Optional) Klicken Sie auf **Bearbeiten**, um die Details der ausgewählten Portspiegelungssitzung zu bearbeiten.
- 6 (Optional) Klicken Sie auf **Entfernen**, um die ausgewählte Portspiegelungssitzung zu löschen.

Bearbeiten der Details, Quellen und Ziele von Portspiegelungssitzungen

Bearbeiten Sie die Details einer Portspiegelungssitzung, z. B. Name, Beschreibung, Status, Quellen und Ziele.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf die Registerkarte **Verwalten**, und wählen Sie **Einstellungen > Portspiegelung**.
- 3 Wählen Sie in der Liste eine Portspiegelungssitzung aus, und klicken Sie auf **Bearbeiten**.
- 4 Bearbeiten Sie auf der Seite **Eigenschaften** die Sitzungseigenschaften.

Je nach Typ der bearbeiteten Portspiegelungssitzung sind unterschiedliche Optionen für die Konfiguration verfügbar.

Option	Beschreibung
Name	Sie können einen eindeutigen Namen für die Portspiegelungssitzung eingeben oder den automatisch generierten Sitzungsamen übernehmen.
Status	Verwenden Sie das Dropdown-Menü, um die Sitzung zu aktivieren oder zu deaktivieren.
Normal-E/A auf Zielports	Verwenden Sie das Dropdown-Menü, um normale E/A-Vorgänge auf Zielports zuzulassen oder nicht zuzulassen. Diese Eigenschaft ist nur für Uplink-Portziele und verteilte Portziele verfügbar. Wenn Sie diese Option nicht auswählen, wird ausgehender gespiegelter Datenverkehr auf den Zielports zugelassen, aber eingehender Datenverkehr nicht.
Gekapselte VLAN-ID	Geben Sie eine gültige VLAN-ID in das Feld ein. Diese Informationen sind für Portspiegelungssitzungen mit Remotespiegelungsquelle erforderlich. Aktivieren Sie das Kontrollkästchen neben Ursprüngliches VLAN beibehalten , um eine VLAN-ID zu erstellen, in der alle Frames auf den Zielports gekapselt sind. Falls die ursprünglichen Frames über ein VLAN verfügen und die Option „Ursprüngliches VLAN beibehalten“ nicht aktiviert ist, wird das ursprüngliche VLAN durch das Kapselungs-VLAN ersetzt.
Länge des gespiegelten Pakets (in Byte)	Verwenden Sie das Kontrollkästchen, um die Länge des gespiegelten Pakets in Byte zu aktivieren. Es wird ein Grenzwert für die Größe von gespiegelten Frames festgelegt. Wenn diese Option ausgewählt ist, werden alle gespiegelten Frames auf die angegebene Länge gekürzt.
Beschreibung	Sie können eine Beschreibung für die Konfiguration der Portspiegelungssitzung eingeben.

5 Bearbeiten Sie auf der Seite **Quellen** die Quellen für die Portspiegelungssitzung.

Je nach Typ der bearbeiteten Portspiegelungssitzung sind unterschiedliche Optionen für die Konfiguration verfügbar.

Option	Beschreibung
Fügen Sie vorhandene Ports aus einer Liste hinzu.	Klicken Sie auf die Schaltfläche Verteilte Ports auswählen.... Es wird ein Dialogfeld mit einer Liste der vorhandenen Ports geöffnet. Aktivieren Sie das Kontrollkästchen neben dem verteilten Port, und klicken Sie auf OK . Sie können mehr als einen verteilten Port auswählen.
Vorhandene Ports nach Portnummer hinzufügen	Klicken Sie auf die Schaltfläche Verteilte Ports hinzufügen.... , geben Sie die Portnummer ein, und klicken Sie auf OK .
Datenverkehrsrichtung festlegen	Wählen Sie nach dem Hinzufügen der Ports in der Liste den Port aus, und klicken Sie auf die Schaltfläche „Ingress“, „Egress“ oder „Ingress/Egress“. Ihre Auswahl wird in der Spalte „Datenverkehrsrichtung“ angezeigt.
Quell-VLAN angeben	Wenn Sie einen Sitzungstyp mit Remotespiegelungsziel ausgewählt haben, müssen Sie das Quell-VLAN angeben. Klicken Sie auf die Schaltfläche Hinzufügen , um eine VLAN-ID hinzuzufügen. Bearbeiten Sie die ID, indem Sie entweder den Aufwärts- oder Abwärtspeil verwenden oder in das Feld klicken und die VLAN-ID manuell eingeben.

6 Bearbeiten Sie im Abschnitt **Ziele** die Ziele für die Portspiegelungssitzung.

Je nach Typ der bearbeiteten Portspiegelungssitzung sind unterschiedliche Optionen für die Konfiguration verfügbar.

Option	Beschreibung
Verteilten Zielport auswählen	Klicken Sie auf die Schaltfläche Verteilte Ports auswählen.... , um Ports in der Liste auszuwählen, oder klicken Sie auf die Schaltfläche Verteilte Ports hinzufügen.... , um Ports nach der Portnummer hinzuzufügen. Sie können mehr als einen verteilten Port hinzufügen.
Uplink auswählen	Wählen Sie in der Liste einen verfügbaren Uplink aus, und klicken Sie auf Hinzufügen > , um den Uplink der Portspiegelungssitzung hinzuzufügen. Sie können mehr als einen Uplink auswählen.
Ports oder Uplinks auswählen	Klicken Sie auf die Schaltfläche Verteilte Ports auswählen.... , um Ports in der Liste auszuwählen, oder klicken Sie auf die Schaltfläche Verteilte Ports hinzufügen.... , um Ports nach der Portnummer hinzuzufügen. Sie können mehr als einen verteilten Port hinzufügen. Klicken Sie auf die Schaltfläche Uplinks hinzufügen.... , um Uplinks als Ziel hinzuzufügen. Wählen Sie Uplinks in der Liste aus, und klicken Sie auf OK .
IP-Adresse angeben	Klicken Sie auf die Schaltfläche Hinzufügen . Ein neuer Listeneintrag wird erstellt. Markieren Sie den Eintrag, und klicken Sie entweder auf die Schaltfläche „Bearbeiten“, um die IP-Adresse einzugeben, oder klicken Sie direkt in das Feld „IP-Adresse“, und geben Sie die IP-Adresse ein. Wenn die IP-Adresse ungültig ist, wird ein Dialogfeld mit einer Warnung angezeigt.

7 Klicken Sie auf **OK**.

Überprüfung des Systemzustands des vSphere Distributed Switch

Durch die Unterstützung der Systemstatusprüfung in vSphere Distributed Switch 5.1 und höher können Konfigurationsfehler eines vSphere Distributed Switch leichter identifiziert und behoben werden.

Verwenden Sie die Überprüfung des Systemzustands des vSphere Distributed Switch, um bestimmte Einstellungen auf verteilten Switches und physischen Switches zu prüfen und häufige Fehler in der Netzwerkkonfiguration Ihrer Umgebung zu identifizieren. Das Standardintervall zwischen zwei Systemstatusprüfungen beträgt 1 Minute.

Wichtig Verwenden Sie die Überprüfung des Systemzustands, um Netzwerkprobleme zu beheben, und deaktivieren Sie sie, nachdem Sie das Problem identifiziert und behoben haben. Nachdem die Überprüfung des Systemzustands des vSphere Distributed Switch deaktiviert wurde, erreichen die generierten MAC-Adressen das Ende ihrer Lebensdauer in der physischen Netzwerkkonfiguration entsprechend der Netzwerkkonfiguration erreicht. Weitere Informationen finden Sie im Knowledgebase-Artikel [KB 2034795](#).

Konfigurationsfehler	Systemstatusprüfung	Erforderliche Konfiguration auf dem Distributed Switch
Die VLAN-Trunk-Bereiche, die auf dem Distributed Switch konfiguriert sind, stimmen nicht mit den Trunk-Bereichen auf dem physischen Switch überein.	Es wird überprüft, ob die VLAN-Einstellungen auf dem Distributed Switch mit der Trunk-Portkonfiguration auf den verbundenen physischen Switch-Ports übereinstimmen.	Mindestens zwei aktive physische Netzwerkkarten
Die MTU-Einstellungen der physischen Netzwerkadapter, des Distributed Switch und der physischen Switch-Ports stimmen nicht überein.	Überprüft, ob die MTU Jumbo-Frame-Einstellung für den Switchport für den physischen Zugriff pro VLAN mit der MTU-Einstellung des vSphere Distributed Switches übereinstimmt.	Mindestens zwei aktive physische Netzwerkkarten
Die für die Portgruppen konfigurierte Teaming-Richtlinie stimmt nicht mit der Richtlinie des Port-Channel des physischen Switch überein.	Es wird geprüft, ob die verbundenen Zugriffssports des physischen Switch, der an einem EtherChannel beteiligt ist, mit den verteilten Ports gepaart sind, deren Teaming-Richtlinie IP-Hash ist.	Mindestens zwei aktive physische Netzwerkkarten und zwei Hosts

Die Systemzustandsprüfung beschränkt sich auf den Switchport für den Zugriff, mit dem der Uplink des Distributed Switches eine Verbindung herstellt.

Aktivieren oder Deaktivieren der Überprüfung des Systemzustands des vSphere Distributed Switch

Die Systemstatusprüfung überwacht Änderungen an den vSphere Distributed Switch-Konfigurationen. Sie müssen die Systemstatusprüfung für vSphere Distributed Switch aktivieren, um Überprüfungen der Distributed Switch-Konfigurationen durchzuführen.

Die Überprüfung des Systemzustands des vSphere Distributed Switch hilft Ihnen dabei, Konfigurationsprobleme mit vSphere Distributed Switch (VDS) und nicht übereinstimmenden Konfigurationen zwischen dem VDS und dem physischen Netzwerk Ihrer Umgebung zu ermitteln und zu beheben. Die Überprüfung des Systemzustands ist standardmäßig deaktiviert. Sie können die Überprüfung des Systemzustands aktivieren, um mögliche Netzwerkprobleme zu identifizieren und zu beheben. Je nachdem, welche Optionen Sie auswählen, kann die Überprüfung des Systemzustands des vSphere Distributed Switch zahlreiche MAC-Adressen zum Testen der Teaming-Richtlinie, der MTU-Größe und der VLAN-Konfiguration generieren. Diese MAC-Adressen führen zu zusätzlichem Netzwerkdatenverkehr, was sich auf die Netzwerkleistung auswirken kann.

Wichtig Verwenden Sie die Überprüfung des Systemzustands, um Netzwerkprobleme zu beheben, und deaktivieren Sie sie, nachdem Sie das Problem identifiziert und behoben haben. Nachdem die Überprüfung des Systemzustands des vSphere Distributed Switch deaktiviert wurde, erreichen die generierten MAC-Adressen das Ende ihrer Lebensdauer in der physischen Netzwerkumgebung entsprechend der Netzwerkrichtlinie erreicht. Weitere Informationen finden Sie im Knowledgebase-Artikel [KB 2034795](#).

Voraussetzungen

Überprüfen Sie, ob der vSphere Distributed Switch die Version 5.1 oder höher aufweist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Einstellungen > Systemstatusprüfung bearbeiten** aus.
- 3 Aktivieren oder deaktivieren Sie über die Dropdown-Menüs die Optionen für den Systemzustand.

Option	Beschreibung
VLAN und MTU	Meldet den Status der verteilten Uplink-Ports und VLAN-Bereiche.
Teaming und Failover	Überprüft auf beliebige Konfigurationskonflikte zwischen dem ESXi-Host und dem physischen Switch, der in der Teaming-Richtlinie verwendet wird.

- 4 Klicken Sie auf **OK**.

Nächste Schritte

Wenn Sie die Konfiguration eines vSphere Distributed Switch ändern, können Sie Informationen über die Änderung auf der Registerkarte **Überwachen** im vSphere Web Client anzeigen. Weitere Informationen hierzu finden Sie unter [Anzeigen des Systemstatus von vSphere Distributed Switch](#).

Anzeigen des Systemstatus von vSphere Distributed Switch

Nachdem Sie die Systemstatusprüfung eines vSphere Distributed Switch aktiviert haben, können Sie den Netzwerksystemstatus der in vSphere Web Client verbundenen Hosts anzeigen.

Voraussetzungen

Überprüfen Sie, ob die Systemstatusprüfung für VLAN und MTU sowie für die Teaming-Richtlinie auf dem vSphere Distributed Switch aktiviert ist. Siehe [Aktivieren oder Deaktivieren der Überprüfung des Systemzustands des vSphere Distributed Switch](#).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Klicken Sie auf der Registerkarte **Überwachen** auf **Status**.
- 3 Prüfen Sie im Abschnitt „Details zum Systemstatus“ den Gesamtstatus, den VLAN-, den MTU- und den Teaming-Status der mit dem Switch verbundenen Hosts.

Switch-Discovery-Protokoll

Switch-Discovery-Protokolle helfen vSphere-Administratoren zu ermitteln, welcher Port des physischen Switch mit einem vSphere Standard-Switch oder vSphere Distributed Switch verbunden ist.

vSphere 5.0 und höher unterstützt das Cisco Discovery Protocol (CDP) und das Link Layer Discovery Protocol (LLDP). CDP ist verfügbar für vSphere Standard-Switches und vSphere Distributed Switches, die mit physischen Cisco-Switches verbunden sind. LLDP ist verfügbar für vSphere Distributed Switches der Version 5.0.0 und höher.

Wenn CDP oder LLDP für einen bestimmten vSphere Distributed Switch oder vSphere Standard-Switch aktiviert ist, können Sie die Eigenschaften des physischen Peer-Switches wie z. B. Geräte-ID, Softwareversion und Zeitüberschreitung vom vSphere Web Client aus anzeigen.

Aktivieren des Cisco Discovery-Protokolls auf einem vSphere Distributed Switch

Cisco Discovery-Protokolle (CDP) ermöglichen es vSphere-Administratoren, zu ermitteln, welcher Port eines physischen Cisco-Switches mit einem vSphere Standard-Switch oder vSphere Distributed Switch verbunden ist. Wenn CDP für einen vSphere Distributed Switch aktiviert ist, können Sie die Eigenschaften des Cisco-Switches anzeigen (z. B. Geräte-ID, Softwareversion und Zeitüberschreitung).

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Einstellungen > Einstellungen bearbeiten** aus.
- 3 Klicken Sie im Dialogfeld „Einstellungen bearbeiten“ auf **Erweitert**.
- 4 Wählen Sie im Abschnitt „Discovery-Protokoll“ im Dropdown-Menü **Typ** die Option **Cisco Discovery-Protokoll** aus.

- Wählen Sie im Dropdown-Menü **Vorgang** den Betriebsmodus der mit dem Switch verbundenen ESXi-Hosts aus.

Option	Beschreibung
Überwachen	ESXi erkennt und zeigt Informationen zum verknüpften Cisco-Switchport an, jedoch stehen dem Administrator des Cisco-Switches keine Informationen über den vSphere Distributed Switch zur Verfügung.
Werben	ESXi stellt dem Cisco-Switch-Administrator Informationen zum vSphere Distributed Switch zur Verfügung, ohne jedoch Informationen zum Cisco-Switch zu erkennen und anzuzeigen.
Beide	ESXi erkennt und zeigt Informationen zum verknüpften Cisco-Switch an und stellt dem Administrator des Cisco-Switches Informationen über den vSphere Distributed Switch zur Verfügung.

- Klicken Sie auf **OK**.

Aktivieren des Link Layer Discovery Protocol (LLDP) auf einem vSphere Distributed Switch

vSphere-Administratoren können mit dem Link Layer Discovery Protocol (LLDP) den physischen Switch-Port ermitteln, mit dem ein angegebener vSphere Distributed Switch verbunden ist. Wenn LLDP für einen bestimmten Distributed Switch aktiviert ist, können Sie die Eigenschaften des physischen Switch, z. B. Chassis-ID, Systemname und -beschreibung sowie Gerätefunktionen, vom vSphere Web Client aus anzeigen.

Verfahren

- Navigieren Sie im vSphere Web Client zum Distributed Switch.
- Wählen Sie im Menü **Aktionen** die Option **Einstellungen > Einstellungen bearbeiten** aus.
- Klicken Sie im Dialogfeld „Einstellungen bearbeiten“ auf **Erweitert**.
- Wählen Sie im Abschnitt „Discovery-Protokoll“ im Dropdown-Menü **Typ** die Option **Link Layer Discovery Protocol (LLDP)** aus.
- Wählen Sie im Dropdown-Menü **Vorgang** den Betriebsmodus der mit dem Switch verbundenen ESXi-Hosts aus.

Vorgang	Beschreibung
Überwachen	ESXi erkennt und zeigt Informationen zum verknüpften physischen Switch-Port an, jedoch stehen dem Switch-Administrator keine Informationen zum vSphere Distributed Switch zur Verfügung.
Werben	ESXi stellt dem Switch-Administrator Informationen zum vSphere Distributed Switch zur Verfügung, ohne jedoch Informationen zum physischen Switch zu erkennen oder anzuzeigen.
Beide	ESXi erkennt und zeigt Informationen zum verknüpften physischen Switch an und stellt dem Switch-Administrator Informationen zum vSphere Distributed Switch zur Verfügung.

- 6 Klicken Sie auf **OK**.

Anzeigen von Switch-Informationen

Wenn Cisco Discovery Protocol (CDP) oder Link Layer Discovery Protocol (LLDP) auf dem Distributed Switch aktiviert ist und die mit dem Switch verbundenen Hosts sich im Betriebsmodus „Überwachen“ oder „Beides“ befinden, können Sie Informationen zum physischen Switch in vSphere Web Client anzeigen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf die Registerkarte **Verwalten** und anschließend auf **Netzwerk > Physische Adapter**.
- 3 Wählen Sie einen physischen Adapter aus der Liste aus, um detaillierte Informationen anzuzeigen.

Ergebnisse

Entsprechend dem aktivierten Switch-Discovery-Protokoll werden die Eigenschaften des Switches auf der Registerkarte **CDP** oder **LLDP** angezeigt. Wenn die Informationen im Netzwerk verfügbar sind, können Sie die Systemfunktionalitäten des Switches unter „Funktionalität des Peer-Geräts“ prüfen.

Konfigurieren von Protokollprofilen für Netzwerke virtueller Maschinen

15

Ein Netzwerkprotokollprofil enthält einen Pool an IPv4- und IPv6-Adressen, die vCenter Server vApps oder virtuellen Maschinen mit vApp-Funktionalität zuweist, die mit den Portgruppen des Profils verbunden sind.

Netzwerkprotokollprofile enthalten auch Einstellungen für das IP-Subnetz, das DNS und den HTTP-Proxy-Server.

Führen Sie die folgenden Schritte aus, um die Netzwerkeinstellungen virtueller Maschinen mithilfe von Netzwerkprotokollprofilen zu konfigurieren:

- Erstellen Sie Netzwerkprofile auf der Ebene eines Datacenters oder eines vSphere Distributed Switch.
- Ordnen Sie ein Protokollprofil der Portgruppe einer virtuellen vApp-Maschine zu.
- Aktivieren Sie die vorübergehende oder statische IP-Zuteilungsrichtlinie in den vApp-Einstellungen oder in den vApp-Optionen einer virtuellen Maschine.

Hinweis Wenn Sie eine vApp oder eine virtuelle Maschine, die ihre Netzwerkeinstellungen aus einem Protokollprofil abrufen, in ein anderes Datacenter verschieben, müssen Sie der verbundenen Portgruppe auf dem Ziel-Datacenter ein Protokollprofil zuordnen, um die vApp oder virtuelle Maschine einzuschalten.

- **Hinzufügen eines Netzwerkprotokollprofils**

Ein Netzwerkprotokollprofil enthält einen Pool mit IPv4- und IPv6-Adressen. vCenter Server weist diese Ressourcen vApps oder virtuellen Maschinen mit vApp-Funktionalität zu, die mit Portgruppen verbunden sind, welche mit dem Profil verknüpft sind.

- **Zuordnen einer Portgruppe zu einem Netzwerkprotokollprofil**

Um den IP-Adressbereich eines Netzwerkprotokollprofils auf eine virtuelle Maschine anzuwenden, die Teil einer vApp ist oder auf der die vApp-Funktionalität aktiviert ist, ordnen Sie das Profil einer Portgruppe zu, die das Netzwerk der virtuellen Maschine steuert.

■ Konfigurieren einer virtuellen Maschine oder von vApp zur Verwendung eines Netzwerkprotokollprofils

Nachdem Sie einer Portgruppe eines Standard-Switches oder eines Distributed Switch ein Protokollprofil zugewiesen haben, aktivieren Sie die Profilverwendung auf einer virtuellen Maschine, die mit der Portgruppe verbunden ist und mit einer vApp verknüpft ist oder bei der die vApp-Optionen aktiviert wurden.

Hinzufügen eines Netzwerkprotokollprofils

Ein Netzwerkprotokollprofil enthält einen Pool mit IPv4- und IPv6-Adressen. vCenter Server weist diese Ressourcen vApps oder virtuellen Maschinen mit vApp-Funktionalität zu, die mit Portgruppen verbunden sind, welche mit dem Profil verknüpft sind.

Netzwerkprotokollprofile enthalten auch Einstellungen für das IP-Subnetz, das DNS und den HTTP-Proxy-Server.

Hinweis Wenn Sie eine vApp oder eine virtuelle Maschine, die ihre Netzwerkeinstellungen von einem Protokollprofil abruft, in ein anderes Datacenter verschieben, müssen Sie der verbundenen Portgruppe auf dem Ziel-Datacenter zum Einschalten der vApp bzw. virtuellen Maschine ein Protokollprofil zuweisen.

Verfahren

- 1 Navigieren Sie zu einem Datacenter, das mit der vApp verknüpft ist, und klicken Sie auf die Registerkarte **Verwalten**.
- 2 Klicken Sie auf **Netzwerkprotokollprofile**
Es werden vorhandene Netzwerkprotokollprofile aufgelistet.
- 3 Klicken Sie auf das Symbol „Hinzufügen“ (+), um ein neues Netzwerkprotokollprofil hinzuzufügen.

Benennen des Netzwerkprotokollprofils und Auswählen des Netzwerks

Benennen Sie das Netzwerkprotokollprofil und wählen Sie das Netzwerk, das es benutzen soll.

Verfahren

- 1 Geben Sie den Namen des Netzwerkprotokollprofils ein.
- 2 Wählen Sie die Netzwerke aus, die dieses Netzwerkprotokollprofil verwenden.
Ein Netzwerk kann nur einem Netzwerkprotokollprofil auf einmal zugewiesen werden.
- 3 Klicken Sie auf **Weiter**.

Festlegen der IPv4-Konfiguration des Netzwerkprotokollprofils

Ein Netzwerkprotokollprofil enthält einen Pool der von vApps verwendeten IPv4- und IPv6-Adressen. Beim Erstellen eines Netzwerkprotokollprofils legen Sie dessen IPv4-Konfiguration fest.

Sie können Adressbereiche von Netzwerkprotokollprofilen für IPv4, IPv6 oder beides konfigurieren. Diese Bereiche werden von vCenter Server für die dynamische Zuweisung von IP-Adressen zu virtuellen Maschinen verwendet, wenn eine vApp für die Verwendung von vorübergehender IP-Reservierung eingerichtet ist.

Verfahren

- 1 Geben Sie das **IP-Subnetz** und das **Gateway** in die entsprechenden Felder ein.
- 2 Wählen Sie **DHCP vorhanden** aus, um anzugeben, dass der DHCP-Server auf diesem Netzwerk zur Verfügung steht.
- 3 Geben Sie die DNS Server-Informationen ein.
Geben Sie die Server durch IP-Adressen an, die durch ein Komma, Semikolon oder Leerzeichen getrennt sind.
- 4 Aktivieren Sie das Kontrollkästchen **IP-Pool aktivieren**, um einen IP-Pool-Bereich anzugeben.
- 5 Wenn Sie IP-Pools aktivieren, geben Sie in das Feld **IP-Pool-Bereich** eine kommagetrennte Liste mit Hostadressbereichen ein.
Ein Bereich besteht aus einer IP-Adresse, einer Raute (#) und einer Zahl, die die Länge des Bereichs angibt.
Das Gateway und die Bereiche müssen sich innerhalb des Subnetzes befinden. Die Bereiche, die Sie in das Feld **IP-Pool-Bereich** eingeben, dürfen nicht die Gateway-Adresse beinhalten.
Beispielsweise zeigt **10.20.60.4#10**, **10.20.61.0#2** an, dass die IPv4-Adressen im Bereich von „10.20.60.4“ bis „10.20.60.13“ und „10.20.61.0“ bis „10.20.61.1“ liegen können.
- 6 Klicken Sie auf **Weiter**.

Festlegen der IPv6-Konfiguration für das Netzwerkprotokollprofil

Ein Netzwerkprotokollprofil enthält einen Pool der von vApps verwendeten IPv4- und IPv6-Adressen. Wenn Sie ein Netzwerkprotokollprofil erstellen, legen Sie seine IPv6-Konfiguration fest.

Sie können Netzwerkprotokollprofilbereiche für IPv4, IPv6 oder beides konfigurieren. vCenter Server verwendet diese Bereiche für die dynamische Zuteilung von IP-Adressen zu virtuellen Maschinen, wenn eine vApp für die Verwendung der vorübergehenden IP-Zuteilung konfiguriert ist.

Verfahren

- 1 Geben Sie das **IP-Subnetz** und das **Gateway** in die entsprechenden Felder ein.
- 2 Wählen Sie **DHCP vorhanden** aus, um anzugeben, dass der DHCP-Server auf diesem Netzwerk zur Verfügung steht.

- 3 Geben Sie die DNS Server-Informationen ein.

Geben Sie die Server durch IP-Adressen an, die durch ein Komma, Semikolon oder Leerzeichen getrennt sind.

- 4 Aktivieren Sie das Kontrollkästchen **IP-Pool aktivieren**, um einen IP-Pool-Bereich anzugeben.

- 5 Wenn Sie IP-Pools aktivieren, geben Sie in das Feld **IP-Pool-Bereich** eine kommagetrennte Liste mit Hostadressbereichen ein.

Ein Bereich besteht aus einer IP-Adresse, einer Raute (#) und einer Zahl, die die Länge des Bereichs angibt. Nehmen Sie beispielsweise an, dass Sie den folgenden IP-Pool-Bereich angeben:

fe80:0:0:0:2bff:fe59:5a:2b#10,fe80:0:0:0:2bff:fe59:5f:b1#2

Dann befinden sich die Adressen in diesem Bereich:

fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34

und

fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2

Das Gateway und die Bereiche müssen sich innerhalb des Subnetzes befinden. Die Bereiche, die Sie in das Feld **IP-Pool-Bereich** eingeben, dürfen nicht die Gateway-Adressen einschließen.

- 6 Klicken Sie auf **Weiter**.

Festlegen des DNS und weiterer Konfigurationseinstellungen für das Netzwerkprotokollprofil

Wenn Sie ein Netzwerkprotokollprofil erstellen, können Sie die DNS-Domäne, den DNS-Suchpfad, einen Hostpräfix und einen HTTP-Proxy festlegen.

Verfahren

- 1 Geben Sie die DNS-Domäne ein.
- 2 Geben Sie den Hostpräfix ein.
- 3 Geben Sie den DNS-Suchpfad ein.

Die Suchpfade werden als Liste von DNS-Domänen angegeben, die durch Kommas, Semikolons oder Leerzeichen getrennt sind.

- 4 Geben Sie den Servernamen und die Portnummer für den Proxy-Server ein.

Der Servername kann einen Doppelpunkt und eine Portnummer enthalten.

Beispielsweise ist `web-proxy:3912` ein gültiger Proxy-Server.

- 5 Klicken Sie auf **Weiter**.

Abschließen der Erstellung des Netzwerkprotokollprofils

Verfahren

- ◆ Überprüfen Sie die Einstellungen und klicken Sie auf **Beenden**, um das Hinzufügen des Profils des Netzwerkprotokolls abzuschließen.

Zuordnen einer Portgruppe zu einem Netzwerkprotokollprofil

Um den IP-Adressbereich eines Netzwerkprotokollprofils auf eine virtuelle Maschine anzuwenden, die Teil einer vApp ist oder auf der die vApp-Funktionalität aktiviert ist, ordnen Sie das Profil einer Portgruppe zu, die das Netzwerk der virtuellen Maschine steuert.

Sie können einer Portgruppe eines Standard-Switches oder einer verteilten Portgruppe eines Distributed Switch ein Netzwerkprotokollprofil unter Verwendung der Einstellungen der Gruppe zuordnen.

Verfahren

- 1 Navigieren Sie zu einer verteilten Portgruppe eines vSphere Distributed Switch oder zu einer Portgruppe eines vSphere Standard-Switches in der Netzwerkansicht des vSphere Web Client.

Die Portgruppen von Standard-Switches befinden sich unter dem Datacenter. Der vSphere Web Client zeigt verteilte Portgruppen unter dem übergeordneten Distributed Switch-Objekt an.

- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Netzwerkprotokollprofile**.
- 3 Klicken Sie auf **Profil eines Netzwerkprotokolls mit dem ausgewählten Netzwerk verknüpfen**.
- 4 Wählen Sie auf der Seite „Zuordnungstyp festlegen“ im Assistenten **Netzwerkprotokollprofil zuordnen** die Option **Vorhandenes Netzwerkprotokollprofil verwenden** aus, und klicken Sie auf **Weiter**.

Wenn die vorhandenen Netzwerkprotokollprofile keine geeigneten Einstellungen für die vApp-VMs in der Portgruppe enthalten, müssen Sie ein neues Profil erstellen.

- 5 Wählen Sie das Netzwerkprotokollprofil aus, und klicken Sie auf **Weiter**.
- 6 Überprüfen Sie die Zuordnung und die Einstellungen des Netzwerkprotokollprofils und klicken Sie auf **Beenden**.

Konfigurieren einer virtuellen Maschine oder von vApp zur Verwendung eines Netzwerkprotokollprofils

Nachdem Sie einer Portgruppe eines Standard-Switches oder eines Distributed Switch ein Protokollprofil zugewiesen haben, aktivieren Sie die Profilverwendung auf einer virtuellen Maschine, die mit der Portgruppe verbunden ist und mit einer vApp verknüpft ist oder bei der die vApp-Optionen aktiviert wurden.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Maschine mit einer Portgruppe verbunden ist, die mit dem Netzwerkprotokollprofil verknüpft ist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zur virtuellen Maschine oder vApp.
- 2 Öffnen Sie die Einstellungen der vApp oder die Registerkarte **vApp-Optionen** der virtuellen Maschine.
 - Klicken Sie mit der rechten Maustaste auf eine vApp und wählen Sie **Einstellungen bearbeiten**.
 - Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine, wählen Sie **Einstellungen bearbeiten** aus und klicken Sie im Dialogfeld „Einstellungen bearbeiten“ auf die Registerkarte **vApp-Optionen**.

- 3 Klicken Sie auf **vApp-Optionen aktivieren**.

- 4 Erweitern Sie unter „Erstellen“ die Option **IP-Zuteilung** und setzen Sie das IP-Zuteilungsschema auf **OVF-Umgebung**.

- 5 Erweitern Sie unter „Bereitstellung“ die Option **IP-Zuteilung** und legen Sie für die **IP-Zuteilung** die Einstellung **Vorübergehend - IP-Pool** oder **Statisch - IP-Pool** fest.

Sowohl bei der Option **Statisch - IP-Pool** als auch bei **Vorübergehend - IP-Pool** wird eine IP-Adresse aus dem Bereich im Netzwerkprotokollprofil zugeteilt, das mit der Portgruppe verknüpft ist. Wenn Sie **Statisch - IP-Pool** wählen, wird die IP-Adresse beim ersten Einschalten der virtuellen Maschine oder der vApp zugewiesen, und die Adresse bleibt bei jedem Neustart erhalten. Wenn Sie die Einstellung **Vorübergehend - IP-Pool** wählen, wird bei jedem Einschalten der virtuellen Maschine oder vApp eine IP-Adresse zugewiesen.

- 6 Klicken Sie auf **OK**.

Ergebnisse

Wenn die virtuelle Maschine eingeschaltet ist, erhalten die Adapter, die mit der Portgruppe verbunden sind, IP-Adressen aus dem Bereich im Protokollprofil. Wenn die virtuelle Maschine ausgeschaltet ist, werden die IP-Adressen wieder freigegeben.

In vSphere 6.0 und höher unterstützt vSphere Distributed Switch grundlegende und Snooping-Modelle zum Filtern von Multicast-Paketen, die mit einzelnen Multicast-Gruppen in Verbindung stehen. Wählen Sie ein Modell entsprechend der Anzahl der Multicast-Gruppen aus, bei denen die virtuellen Maschinen auf dem Switch abonniert sind.

- **Multicast-Filtermodi**

Zusätzlich zum Standard-Basismodus für das Filtern von Multicast-Datenverkehr unterstützen vSphere Distributed Switch 6.0.0 und höhere Versionen Multicast-Snooping, mit dem Multicast-Datenverkehr auf präzisere Weise basierend auf den IGMP-Meldungen (Internet Group Management Protocol) bzw. den MLD-Meldungen (Multicast Listener Discovery) der virtuellen Maschinen weitergeleitet wird.

- **Multicast-Snooping auf einem vSphere Distributed Switch aktivieren**

Verwenden Sie Multicast-Snooping auf einem vSphere Distributed Switch, um Datenverkehr präzise entsprechend IGMP- oder MLD-Mitgliedschaftsinformationen (Internet Group Management Protocol bzw. Multicast Listener Discovery) weiterzuleiten, die von virtuellen Maschinen gesendet werden, um Multicast-Datenverkehr zu abonnieren.

- **Bearbeiten des Abfragezeitintervalls für Multicast-Snooping**

Wenn IGMP- oder MLD-Multicast-Snooping auf einem vSphere Distributed Switch 6.0 aktiviert ist, sendet der Switch allgemeine Abfragen über die Mitgliedschaft von virtuellen Maschinen, wenn ein Snooping-Abfrager nicht auf dem physischen Switch konfiguriert ist. Auf ESXi 6.0-Hosts, die mit dem Distributed Switch verbunden sind, können Sie das Zeitintervall bearbeiten, in dem der Switch allgemeine Abfragen sendet.

- **Bearbeiten der Anzahl von IP-Adressen der Quelle für IGMP und MLD**

Wenn Sie IGMP- oder MLD-Multicast-Snooping auf einem vSphere Distributed Switch 6.0 aktivieren, können Sie die maximale Anzahl der IP-Quellen bearbeiten, aus denen die Mitglieder einer Multicast-Gruppe Pakete empfangen.

Multicast-Filtermodi

Zusätzlich zum Standard-Basismodus für das Filtern von Multicast-Datenverkehr unterstützen vSphere Distributed Switch 6.0.0 und höhere Versionen Multicast-Snooping, mit dem Multicast-Datenverkehr auf präzisere Weise basierend auf den IGMP-Meldungen (Internet Group

Management Protocol) bzw. den MLD-Meldungen (Multicast Listener Discovery) der virtuellen Maschinen weitergeleitet wird.

Multicast-Filterung im Basismodus

Im Basismodus der Multicast-Filterung leitet ein vSphere Standard-Switch oder vSphere Distributed Switch Multicast-Datenverkehr für virtuelle Maschinen entsprechend den MAC-Zieladressen der Multicast-Gruppe weiter. Beim Beitritt zu einer Multicast-Gruppe verschiebt das Gastbetriebssystem die Multicast-MAC-Adresse der Gruppe durch den Switch zum Netzwerk. Der Switch speichert die Zuordnung zwischen dem Port und der Multicast-MAC-Zieladresse in einer lokalen Weiterleitungstabelle.

Der Switch interpretiert die IGMP-Meldungen nicht, die von einer virtuellen Maschine zum Beitritt oder Verlassen einer Gruppe gesendet werden. Der Switch sendet sie direkt an den lokalen Multicast-Router, der sie interpretiert und die virtuelle Maschine in die Gruppe aufnimmt bzw. daraus entfernt.

Der Basismodus weist die folgenden Einschränkungen auf:

- Eine virtuelle Maschine kann Pakete von Gruppen erhalten, für die sie nicht abonniert ist, weil der Switch Pakete entsprechend der MAC-Zieladresse einer Multicast-Gruppe weiterleitet, die potenziell bis zu 32 IP-Multicast-Gruppen zugeordnet sein kann.
- Eine virtuelle Maschine, die Datenverkehr für mehr als 32 Multicast-MAC-Adressen abonniert hat, erhält Pakete, die sie nicht abonniert hat, aufgrund einer Einschränkung des Weiterleitungsmodells.
- Der Switch filtert keine Pakete entsprechend der Quelladresse wie in IGMP Version 3 definiert.

Multicast-Snooping

Im Multicast-Snooping-Modus stellt ein vSphere Distributed Switch IGMP- und MLD-Snooping entsprechend RFC 4541 bereit. Der Switch bearbeitet Multicast-Datenverkehr präziser, indem IP-Adressen verwendet werden. Dieser Modus unterstützt IGMPv1, IGMPv2 und IGMPv3 für IPv4-Multicast-Gruppenadressen und MLDv1 und MLDv2 für IPv6-Multicast-Gruppenadressen.

Der Switch erkennt die Mitgliedschaft einer virtuellen Maschine dynamisch. Wenn eine virtuelle Maschine ein Paket mit IGMP- oder MLD-Mitgliedschaftsinformationen über einen Switch-Port sendet, erstellt der Switch einen Datensatz über die IP-Zieladresse der Gruppe, und im Fall von IGMPv3 über eine IP-Quelladresse, von der die virtuelle Maschine vorzugsweise Datenverkehr erhalten möchte. Wenn eine virtuelle Maschine ihre Gruppenmitgliedschaft nicht in einem bestimmten Zeitraum verlängert, entfernt der Switch den Eintrag für die Gruppe aus den Lookup-Datensätzen.

Im Multicast-Snooping-Modus eines Distributed Switch kann eine virtuelle Maschine Multicast-Datenverkehr an einem einzelnen Switch-Port von bis zu 256 Gruppen und 10 Quellen erhalten.

Multicast-Snooping auf einem vSphere Distributed Switch aktivieren

Verwenden Sie Multicast-Snooping auf einem vSphere Distributed Switch, um Datenverkehr präzise entsprechend IGMP- oder MLD-Mitgliedschaftsinformationen (Internet Group Management Protocol bzw. Multicast Listener Discovery) weiterzuleiten, die von virtuellen Maschinen gesendet werden, um Multicast-Datenverkehr zu abonnieren.

Verwenden Sie Multicast-Snooping, wenn die virtualisierten Arbeitslasten auf dem Switch mehr als 32 Multicast-Gruppen abonniert haben oder Sie Datenverkehr von bestimmten Quellknoten empfangen müssen. Informationen über die Multicast-Filtermodi von vSphere Distributed Switch finden Sie unter [Multicast-Filtermodi](#).

Voraussetzungen

Überprüfen Sie, ob der vSphere Distributed Switch die Version 6.0.0 oder höher aufweist.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Distributed Switch.
- 2 Wählen Sie im Menü **Aktionen** die Option **Einstellungen > Einstellungen bearbeiten** aus.
- 3 Klicken Sie im Dialogfeld, das die Switch-Einstellungen anzeigt, auf **Erweitert**.
- 4 Wählen Sie im Dropdown-Menü **Multicast-Filtermodus** die Option **IGMP/MLD-Snooping** aus und klicken Sie auf **OK**.

Ergebnisse

Multicast-Snooping wird auf Hosts aktiv, die ESXi 6.0 oder höher ausführen.

Bearbeiten des Abfragezeitintervalls für Multicast-Snooping

Wenn IGMP- oder MLD-Multicast-Snooping auf einem vSphere Distributed Switch 6.0 aktiviert ist, sendet der Switch allgemeine Abfragen über die Mitgliedschaft von virtuellen Maschinen, wenn ein Snooping-Abfrager nicht auf dem physischen Switch konfiguriert ist. Auf ESXi 6.0-Hosts, die mit dem Distributed Switch verbunden sind, können Sie das Zeitintervall bearbeiten, in dem der Switch allgemeine Abfragen sendet.

Das Standardzeitintervall für das Senden von Snooping-Abfragen beträgt 125 Sekunden.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen** und wählen Sie **Erweiterte Systemeinstellungen** aus.
- 3 Suchen Sie die Systemeinstellung `Net.IGMPQueryInterval`.

- 4 Klicken Sie auf **Bearbeiten** und geben Sie einen neuen Wert in Sekunden für die Einstellung ein.

Bearbeiten der Anzahl von IP-Adressen der Quelle für IGMP und MLD

Wenn Sie IGMP- oder MLD-Multicast-Snooping auf einem vSphere Distributed Switch 6.0 aktivieren, können Sie die maximale Anzahl der IP-Quellen bearbeiten, aus denen die Mitglieder einer Multicast-Gruppe Pakete empfangen.

Verfahren

- 1 Navigieren Sie im vSphere Web Client zum Host.
- 2 Klicken Sie auf der Registerkarte **Verwalten** auf **Einstellungen** und wählen Sie **Erweiterte Systemeinstellungen** aus.
- 3 Um die Anzahl der Quell-IP-Adressen zu bearbeiten, suchen Sie nach der Systemeinstellung `Net.IGMPV3MaxSrcIPNum` oder `Net.MLDV2MaxSrcIPNum`.
- 4 Klicken Sie auf **Bearbeiten** und geben Sie einen neuen Wert zwischen 1 und 32 für die Einstellung ein.
- 5 Klicken Sie auf **OK**.

Statusfreie Netzwerkbereitstellung

17

Die statusfreie Netzwerkbereitstellung ist ein Ausführungsmodus für ESXi-Hosts ohne lokalen Speicher, in dem früher die Konfiguration oder der Status gespeichert wurde. Die Konfigurationen werden in ein Hostprofil abstrahiert. Dabei handelt es sich um eine Vorlage, die auf eine Klasse von Maschinen angewendet wird. Die statusfreie Konfiguration ermöglicht ein problemloses Austauschen, Entfernen und Hinzufügen von fehlerhafter Hardware. Außerdem wird damit die Skalierung einer Hardwarebereitstellung vereinfacht.

Jeder statusfreie ESXi-Start ist wie ein erster Startvorgang. Der ESXi-Host startet mit Netzwerkkonnektivität zum vCenter Server über den integrierten Standard-Switch. Wenn das Hostprofil eine Distributed Switch-Mitgliedschaft festlegt, fügt der vCenter Server den ESXi-Host den VMware Distributed Switches oder einer Switch-Lösung eines Drittanbieters hinzu.

Bei der Planung der Netzwerkeinrichtung für statusfreie ESXi-Hosts sollten Sie die Konfiguration so allgemein wie möglich halten und hostspezifische Elemente vermeiden. Derzeit sieht das Design keine Hooks vor, um die physischen Switches neu zu konfigurieren, wenn ein neuer Host bereitgestellt wird. Für solche Anforderungen ist eine spezielle Behandlung erforderlich.

Wenn Sie eine statusfreie Bereitstellung einrichten, muss ein ESXi-Host mit der Standardmethode installiert werden. Danach suchen Sie die nachstehenden netzwerkbezogenen Informationen, um sie im Hostprofil zu speichern:

- vSphere Standard Switch-Instanzen und -Einstellungen (Portgruppen, Uplinks, MTU usw.)
- Distributed Switch-Instanzen (VMware und Lösungen von Drittanbietern)
- Auswahlregeln für Uplinks und Uplink-Port oder Portgruppen
- vNIC-Informationen:
 - Adresseninformationen (IPv4 oder IPv6, statisch oder DHCP, Gateway)
 - Portgruppen und verteilte Portgruppen, die dem physischen Netzwerkadapter (`vmknic`) zugewiesen sind
 - Wenn Distributed Switches vorhanden sind, notieren Sie das VLAN, die physischen Netzwerkkarten, die an `vmknic` gebunden sind, und notieren Sie, ob `Etherchannel` konfiguriert ist.

Die aufgezeichneten Informationen werden als Vorlage für das Hostprofil verwendet. Nachdem die Informationen des virtuellen Switches für das Hostprofil extrahiert und in das Hostprofil eingelesen wurden, können Sie jede Information ändern. Die Änderungen können in diesen Abschnitten für Standard-Switches und Distributed Switches durchgeführt werden: Uplink-Auswahlrichtlinie, basierend auf dem vmnic-Namen oder der Gerätenummer, und Auto Discovery basierend auf der VLAN-ID. Die (möglicherweise geänderten) Informationen werden von der statusfreien Start-Infrastruktur gespeichert und beim nächsten Start auf einen statusfreien ESXi-Host angewendet. Während der Netzwerkinitialisierung interpretiert ein allgemeines Netzwerk-Plug-In die aufgezeichneten Hostprofil-Einstellungen und führt Folgendes durch:

- Es lädt die geeigneten physischen Netzwerkkartentreiber.
- Es erstellt alle Standard-Switch-Instanzen mit den Portgruppen. Es wählt Uplinks basierend auf einer Richtlinie aus. Wenn die Richtlinie auf der VLAN-ID beruht, ist ein Prüfungsprozess vorhanden, um relevante Informationen zu beziehen.
- Für VMkernel-Netzwerkadapter, die mit dem Standard-Switch verbunden sind, erstellt es VMkernel-Netzwerkadapter und verbindet sie mit Portgruppen.
- Für jeden VMkernel-Netzwerkadapter, der mit einem Distributed Switch verbunden ist, erstellt es einen temporären Standard-Switch (wenn erforderlich) mit Uplinks, die an den VMkernel-Netzwerkadapter gebunden sind. Es erstellt eine temporäre Portgruppe mit VLAN und Gruppierungsrichtlinien, die auf aufgezeichneten Informationen basieren. Insbesondere wird IP-Hash verwendet, wenn Etherchannel im Distributed Switch verwendet wurde.
- Es konfiguriert alle VMkernel-Netzwerkadaptoreinstellungen (Adressenzuweisung, Gateway, MTU, usw.).

Die grundlegende Konnektivität funktioniert und das Netzwerk-Setup ist vollständig, wenn kein Distributed Switch vorhanden ist.

Wenn ein Distributed Switch vorhanden ist, bleibt das System im Wartungsmodus, bis die Distributed Switch-Standardisierung abgeschlossen ist. Zu diesem Zeitpunkt werden keine virtuellen Maschinen gestartet. Da vCenter Server für Distributed Switches erforderlich ist, läuft der Startprozess, bis die vCenter Server-Konnektivität hergestellt ist und vCenter Server erkennt, dass der Host Teil eines Distributed Switch sein soll. Es veranlasst den Beitritt des Hosts zum Distributed Switch, indem es einen Distributed Switch Proxy-Standard-Switch auf dem Host erstellt, wählt die geeigneten Uplinks aus und migriert den vmknic vom Standard-Switch auf den Distributed Switch. Wenn dieser Vorgang abgeschlossen ist, löscht es den temporären Standard-Switch und die Portgruppen.

Am Ende des Standardisierungsprozesses wird der ESXi-Host aus dem Wartungsmodus geholt. HA oder DRS können auf dem Host virtuelle Maschinen starten.

Wenn kein Hostprofil vorhanden ist, wird ein temporärer Standard Switch mit „Standardnetzwerkeinstellungen“-Logik erstellt, der einen Verwaltungsnetzwerk-Switch (mit „no VLAN“-Tag) einrichtet, dessen Uplink der mit PXE startenden vNIC entspricht. Ein vmknic wird für die Verwaltungsnetzwerk-Portgruppe mit derselben MAC-Adresse wie die mit PXE startende vNIC erstellt. Diese Logik wurde früher für den Start mit PXE verwendet. Wenn ein Hostprofil

vorhanden, aber das Netzwerk-Hostprofil deaktiviert oder unvollständig ist, nutzt vCenter Server die Standard-Netzwerkverarbeitung, damit der ESXi-Host remote verwaltet werden kann. Damit wird ein Übereinstimmungsfehler ausgelöst, sodass vCenter Server Maßnahmen zur Wiederherstellung einleitet.

Optimale Vorgehensweisen für Netzwerke

18

Ziehen Sie folgende optimale Vorgehensweisen für die Konfiguration Ihres Netzwerks in Betracht.

- Um eine stabile Verbindung zwischen vCenter Server, ESXi und anderen Produkten und Diensten zu gewährleisten, legen Sie keine Verbindungsgrenzwerte und Zeitüberschreitungen zwischen den Produkten fest. Grenzwerte und Zeitüberschreitungen können sich auf den Paketfluss auswirken und zu Dienstunterbrechungen führen.
- Zur höheren Sicherheit und besseren Leistung isolieren Sie die Netzwerke für Hostverwaltung, vSphere vMotion, vSphere FT usw. voneinander.
- Reservieren Sie eine getrennte physische Netzwerkkarte für eine Gruppe virtueller Maschinen oder verwenden Sie Network I/O Control und Traffic-Shaping, um Bandbreite für die virtuellen Maschinen zu garantieren. Durch diese Trennung kann auch ein Teil der gesamten Netzwerk-Arbeitslast über mehrere CPUs verteilt werden. Die isolierten virtuellen Maschinen sind dann beispielsweise besser in der Lage, den Anwendungsdatenverkehr von einem Webclient zu verarbeiten.
- Um Netzwerkdienste physisch zu trennen und eine bestimmte Gruppe von Netzwerkkarten einem bestimmten Netzwerkdienst zuzuweisen, erstellen Sie einen vSphere Standard-Switch oder vSphere Distributed Switch für jeden Dienst. Wenn das nicht möglich ist, können Netzwerkdienste auf einem einzelnen Switch voneinander getrennt werden, indem sie Portgruppen mit unterschiedlichen VLAN-IDs zugeordnet werden. In jedem Fall sollte der Netzwerkadministrator bestätigen, dass die gewählten Netzwerke oder VLANs vom Rest der Umgebung isoliert sind, d. h. dass keine Router daran angeschlossen sind.
- Richten Sie die vSphere vMotion-Verbindung auf einem separaten Netzwerk ein. Bei der Migration mit vMotion wird der Inhalt des Arbeitsspeichers des Gastbetriebssystems über das Netzwerk übertragen. Diese Empfehlungen können entweder durch die Verwendung von VLANs zur Aufteilung eines physischen Netzwerks in Segmente oder durch die Verwendung getrennter physischer Netzwerke umgesetzt werden (die zweite Variante ist dabei zu bevorzugen).

Für die Migration über IP-Subnetze hinweg und zur Verwendung von getrennten Puffer- und Socket-Pools platzieren Sie Datenverkehr für vMotion in den vMotion TCP/IP-Stack und Datenverkehr für die Migration ausgeschalteter virtueller Maschinen und Klone auf den Bereitstellungs-TIPC/IP-Stack. Weitere Informationen hierzu finden Sie unter [VMkernel-Netzwerkebene](#).

- Sie können Netzwerkkarten zu einem Standard-Switch oder Distributed Switch hinzufügen oder davon entfernen, ohne dass die virtuelle Maschinen oder die Netzwerkdienste hinter diesem Switch beeinflusst werden. Wenn Sie die gesamte ausgeführte Hardware entfernen, können die virtuelle Maschinen weiter untereinander kommunizieren. Wenn Sie eine Netzwerkkarte intakt lassen, können alle virtuelle Maschinen weiterhin auf das physische Netzwerk zugreifen.
- Um die empfindlichsten virtuelle Maschinen zu schützen, installieren Sie Firewalls auf virtuelle Maschinen, die den Datenverkehr zwischen virtuellen Netzwerken mit Uplinks zu physischen Netzwerken und reinen virtuellen Netzwerken ohne Uplinks weiterleiten.
- Verwenden Sie virtuelle VMXNET 3-Netzwerkkarten, um eine bestmögliche Leistung zu erzielen.
- Jede mit demselben vSphere Standard-Switch oder vSphere Distributed Switch verbundene physische Netzwerkkarte sollte ebenfalls mit demselben physischen Netzwerk verbunden sein.
- Konfigurieren Sie dieselbe MTU für alle VMkernel-Netzwerkadapter in einem vSphere Distributed Switch. Wenn mehrere VMkernel-Netzwerkadapter mit vSphere Distributed Switches verbunden sind, aber unterschiedliche MTUs konfiguriert wurden, treten möglicherweise Netzwerkverbindungsprobleme auf.