vSphere-Netzwerk

Update 2
Geändert am 19. APR. 2022
VMware vSphere 6.7
VMware ESXi 6.7
vCenter Server 6.7

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

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

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

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

Inhalt

Grundlegende Informationen zu vSphere-Netzwerken 11

Aktualisierte Informationen 12

1 Einführung in das vSphere-Netzwerk 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 Adaptern 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 36
  - Aufgaben für das Verwalten von Host-Netzwerken auf einem vSphere Distributed Switch 37
  - Hosts zu einem vSphere Distributed Switch hinzufügen 39
  - Konfigurieren von physischen Netzwerkadaptern auf einem vSphere Distributed Switch 41
  - Migrieren von VMkernel-Adaptern 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
  - Verwenden eines Hosts als Vorlage zur Erstellung einer einheitlichen Netzwerkkonfiguration auf einem vSphere Distributed Switch 47
  - Entfernen von Hosts aus einem vSphere Distributed Switch 49

Verwalten von Netzwerken auf Host-Proxy-Switches 50
Migrieren von Netzwerkadaptern auf einem Host zu einem vSphere Distributed Switch 50
Migrieren eines VMkernel-Adapters auf einem Host zu einem vSphere Standard-Switch 51
Zuweisen einer physischen Netzwerkkarte eines Hosts zu einem vSphere Distributed Switch 52
Entfernen einer physischen Netzwerkkarte aus einem vSphere Distributed Switch 52
Entfernen von NICs von den aktiven virtuellen Maschinen 53
Verteilte Portgruppen 54
Hinzufügen einer verteilten Portgruppe 54
Bearbeiten der allgemeinen Einstellungen von verteilten Portgruppen 59
Entfernen einer verteilten Portgruppe 60
Arbeiten mit verteilten Ports 60
Überwachen des Status von verteilten Ports 61
Konfigurieren der Einstellungen für verteilte Ports 61
Konfigurieren von Netzwerken von virtuellen Maschinen auf einem vSphere Distributed Switch 62
Migrieren von virtuellen Maschinen auf einen oder von einem vSphere Distributed Switch 62
Verbinden einer individuellen virtuellen Maschine mit einer verteilten Portgruppe 63
Topologie-Diagramme eines vSphere Distributed Switch im vSphere Web Client 63
Anzeigen der Topologie eines vSphere Distributed Switch 64
Anzeigen der Topologie eines Host-Proxy-Switch 66

4 Einrichten von VMkernel-Netzwerken 67
VMkernel-Netzwerkebene 68
Anzeigen von Informationen über VMkernel-Adapter auf einem Host 71
Erstellen eines VMkernel-Adapters auf einem vSphere Standard-Switch 71
Erstellen eines VMkernel-Adapters auf einem Host, der einem vSphere Distributed Switch zugeordnet ist 74
Bearbeiten einer VMkernel-Adapterkonfiguration 77
Außerkraftsetzen des Standard-Gateways eines VMkernel-Adapters 79
Konfigurieren des VMkernel-Adapter-Gateways mit esxcli-Befehlen 80
Anzeigen der TCP/IP-Stack-Konfiguration auf einem Host 81
Ändern der Konfiguration eines TCP/IP-Stack auf einem Host 81
Erstellen eines benutzerdefinierten TCP/IP-Stacks 82
Entfernen eines VMkernel-Adapters 83

5 LACP-Support auf einem vSphere Distributed Switch 84
Konfiguration von LACP-Teaming und -Failover für verteilte Portgruppen 87
Konfigurieren einer Linkzusammenfassungsgruppe zur Regelung des Datenverkehrs für verteilte Portgruppen 87
Linkzusammenfassungsgruppe erstellen 88

Festlegen einer Linkzusammenfassungsgruppe als Standby in der Teaming- und Failover-Reihenfolge für verteilte Portgruppen 90

Zuweisen physischer Netzwerkkarten zu den Ports der Linkzusammenfassungsgruppe 91

Festlegen einer Linkzusammenfassungsgruppe als aktiv in der Teaming- und Failover-Reihenfolge für eine verteilte Portgruppe 92

Bearbeiten einer Linkzusammenfassungsgruppe 93

Einschränkungen der LACP-Unterstützung für einen vSphere Distributed Switch 94

6 Sichern und Wiederherstellen von Netzwerkkonfigurationen 95

Sichern und Wiederherstellen einer vSphere Distributed Switch-Konfiguration 95

Exportieren von vSphere Distributed Switch-Konfigurationen 95

Importieren einer vSphere Distributed Switch-Konfiguration 96

Wiederherstellen einer vSphere Distributed Switch-Konfiguration 97

Exportieren, Importieren und Wiederherstellen der Konfigurationen für verteilte vSphere-Portgruppen 98

Exportieren der Konfigurationen für verteilte vSphere-Portgruppen 98

Importieren einer Konfiguration für verteilte vSphere-Portgruppen 99

Wiederherstellen einer Konfiguration für verteilte vSphere-Portgruppen 99

7 Rollback und Wiederherstellung des Verwaltungsnetzwerks 101

vSphere-Netzwerk-Rollback 101

Deaktivieren des Netzwerk-Rollbacks 103

Deaktivieren des Netzwerk-Rollbacks unter Verwendung der vCenter Server-Konfigurationsdatei 103

Beheben von Fehlern bei der Konfiguration des Verwaltungsnetzwerks auf einem vSphere Distributed Switch 104

8 Netzwerkrichtlinien 106

Anwenden von Netzwerkrichtlinien auf einen vSphere Standard oder Distributed Switch 107

Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene 109

Teaming- und Failover-Richtlinie 110

Verfügbare Lastausgleichsalgorithmen für virtuelle Switches 112

Konfigurieren von NIC-Gruppierung, Failover und Lastausgleich auf einem vSphere Standard-Switch oder in einer Standardportgruppe 118

Konfigurieren von NIC-Teaming, Failover und Lastausgleich in einer verteilten Portgruppe oder einem verteilten Port 120

VLAN-Richtlinie 123

Konfigurieren von VLAN-Tagging in einer verteilten Portgruppe oder einem verteilten Port 123

Konfigurieren von VLAN-Tagging auf einer Uplink-Portgruppe oder einem Uplink-Port 124

Sicherheitsrichtlinie 126

Konfigurieren der Sicherheitsrichtlinie für einen vSphere Standard-Switch oder eine Standardportgruppe 126

Konfigurieren der Sicherheitsrichtlinie für eine verteilte Portgruppe oder einen verteilten Port 127

Traffic-Shaping-Richtlinie 129
Konfigurieren von Traffic-Shaping für einen vSphere Standard-Switch oder eine Standardportgruppe 130
Bearbeiten der Traffic-Shaping-Richtlinie für eine verteilte Portgruppe oder einen verteilten Port 131
Ressourcenzuteilungsrichtlinie 133
Bearbeiten der Ressourcenzuteilungsrichtlinie für eine verteilte Portgruppe 133
Überwachungsrichtlinie 134
Aktivieren oder Deaktivieren der NetFlow-Überwachung auf einer verteilten Portgruppe oder einem verteilten Port 134
Richtlinien für das Filtern und Markieren des Datenverkehrs 135
Filtern und Markieren des Datenverkehrs in verteilten oder Uplink-Portgruppen 136
Filtern und Markieren des Datenverkehrs in verteilten oder Uplink-Ports 145
Qualifizieren des Datenverkehrs für die Filterung und Markierung 156
Verwalten von Richtlinien für mehrere Portgruppen auf einem vSphere Distributed Switch 159
Portblockierungsrichtlinien 166
Bearbeiten der Portblockierungsrichtlinie für eine verteilte Portgruppe 166
Bearbeiten der Portblockierungsrichtlinie für verteilte oder Uplink-Portgruppen 167
MAC Learning-Richtlinie 167

9 Isolieren des Netzwerkverkehrs mithilfe von VLANs 169
VLAN-Konfiguration 169
Private VLANs 170
Erstellen eines privaten VLAN 170
Entfernen eines primären privaten VLAN 171
Entfernen eines sekundären privaten VLAN 172

10 Verwalten von Netzwerkressourcen 173
DirectPath I/O 173
Aktivieren des Passthroughs für ein Netzwerkgerät auf einem Host 174
Konfigurieren eines PCI-Geräts auf einer virtuellen Maschine 175
Single Root I/O Virtualization (SR-IOV) 175
SR-IOV-Unterstützung 176
SR-IOV-Komponentenarchitektur und -Interaktion 178
Interaktion von vSphere und virtueller Funktion 180
DirectPath I/O im Vergleich zu SR-IOV 181
Konfigurieren einer virtuellen Maschine zur Verwendung von SR-IOV 181
Netzwerkoptionen für den Datenverkehr einer SR-IOV-fähigen virtuellen Maschine 185
Bewältigen des Datenverkehrs von virtuellen Maschinen mit einem SR-IOV-fähigen physischen Adapter 185
Aktivieren von SR-IOV mit Hostprofilen oder mit einem ESXCLI-Befehl 186
Eine virtuelle Maschine, die eine virtuelle SR-IOV-Funktion verwendet, kann nicht eingeschaltet werden, weil der Host den Status „Out of Interrupt Vectors“ aufweist 189

RDMA für virtuelle Maschinen 190
Unterstützung von PVRDMA 190
Konfigurieren eines ESXi-Hosts für PVRDMA 191
Zuweisen eines PVRDMA Adapters zu einer virtuellen Maschine 192
Netzwerkanforderungen für RDMA over Converged Ethernet 193
Jumbo-Frames 194
Aktivieren von Jumbo-Frames auf einem vSphere Distributed Switch 195
Aktivieren von Jumbo-Frames auf einem vSphere Standard-Switch 195
Aktivieren von Jumbo-Frames für einen VMkernel-Adapter 196
Aktivieren der Jumbo Frame-Unterstützung auf einer virtuellen Maschine 196
TCP-Segmentierungs-Offload 197
Aktivieren oder Deaktivieren von Software-TSO im VMkernel 198
Ermitteln, ob TSO auf den physischen Netzwerkadaptern eines ESXi-Hosts unterstützt wird 198
Aktivieren oder Deaktivieren von TSO auf einem ESXi-Host 198
Ermitteln, ob TSO auf einem ESXi-Host aktiviert ist 199
Aktivieren oder Deaktivieren von TSO auf einer Linux-VM 200
Aktivieren oder Deaktivieren von TSO auf einer Windows-VM 200
Large Receive Offload 201
Aktivieren von Hardware-LRO für alle VMXNET3-Adapter auf einem ESXi-Host 201
Aktivieren oder Deaktivieren von Software-LRO für alle VMXNET3-Adapter auf einem ESXi-Host 202
Ermitteln, ob LRO für VMXNET3-Adapter auf einem ESXi-Host aktiviert ist 202
Ändern der Größe des LRO-Puffers für VMXNET 3-Adapter 203
Aktivieren oder Deaktivieren von LRO für alle VMkernel-Adapter auf einem ESXi-Host 203
Ändern der Größe des LRO-Puffers für VMkernel-Adapter 203
Aktivieren oder Deaktivieren von LRO auf einem VMXNET3-Adapter auf einer Linux-VM 204
Aktivieren oder Deaktivieren von LRO auf einem VMXNET3-Adapter auf einer Windows-VM 204
Globales Aktivieren von LRO auf einer virtuellen Windows-Maschine 205
NetQueue und Netzwerkleistung 206
Aktivieren von NetQueue auf einem Host 206
Deaktivieren von NetQueue auf einem Host 207

11 vSphere Network I/O Control 208
Info zu vSphere Network I/O Control Version 3 208
Aktivieren von Network I/O Control auf einem vSphere Distributed Switch 209
Bandbreitenzuteilung für Systemdatenverkehr 210
Bandbreitenzuteilungsparameter für Systemdatenverkehr 211
Beispiel-Bandbreitenreservierung für Systemdatenverkehr 211
Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr 212
Bandbreitenzuteilung für Datenverkehr über virtuelle Maschinen 213

Info zur Zuteilung von Bandbreite zu virtuellen Maschinen 213
Bandbreitenzuteilungsparameter für Datenverkehr virtueller Maschinen 215
Zugangssteuerung für Bandbreite virtueller Maschinen 216
Erstellen eines Netzwerkressourcenpools 217
Hinzufügen einer verteilten Portgruppe zu einem Netzwerkressourcenpool 219
Konfigurieren der Bandbreitenzuteilung für eine virtuelle Maschine 219
Konfigurieren der Bandbreitenzuteilung auf mehreren virtuellen Maschinen 221
Ändern des Kontingents eines Netzwerkressourcenpools 222
Entfernen von verteilten Portgruppen aus einem Netzwerkressourcenpool 223
Löschen eines Netzwerkressourcenpools 223
Verschieben eines physischen Adapters aus dem Bereich von Network I/O Control 224

12 Verwaltung von MAC-Adressen 225
Zuweisen von MAC-Adressen in vCenter Server 225
VMware-OUI-Zuteilung 226
Zuteilen von präfixbasierten MAC-Adressen 227
Zuteilen von bereichsbasierten MAC-Adressen 227
Zuweisen von MAC-Adressen 227
Generierung von MAC-Adressen auf ESXi-Hosts 230
Festlegen einer statischen MAC-Adresse für eine virtuelle Maschine 231
VMware-OUI in statischen MAC-Adressen 231
Zuweisen einer statischen MAC-Adresse über den vSphere Web Client 232
Zuweisen von statischen MAC-Adressen in der Konfigurationsdatei der virtuellen Maschine 232

13 Konfigurieren von vSphere für IPv6 234
vSphere IPv6-Konnektivität 234
Bereitstellen von vSphere auf IPv6 236
Aktivieren von IPv6 in einer vSphere-Installation 236
Aktivieren von IPv6 in einer vSphere-Umgebung mit Upgrade 237
Aktivieren oder Deaktivieren der IPv6-Unterstützung auf einem Host 240
Einrichten von IPv6 auf einem ESXi-Host 241
Einrichten von IPv6 auf vCenter Server 241
Einrichten von IPv6 auf der vCenter Server Appliance 242
Einrichten von vCenter Server unter Windows mit IPv6 243

14 Überwachen der Netzwerkverbindung und des Netzwerkdatenverkehrs 244
Erfassung von Netzwerkpaketen unter Verwendung des PacketCapture-Dienstprogramms 244
Erfassen und Nachverfolgen von Netzwerkpaketen unter Verwendung des Dienstprogramms pktcap-uw 246
Befehlssyntax von pktcap-uw zum Erfassen von Paketen 247
Befehlssyntax von pktcap-uw zum Nachverfolgen von Paketen 251

Optionen von pktcap-uw zum Kontrollieren der Ausgabe 251
Optionen von pktcap-uw zum Filtern von Paketen 252
Erfassen von Paketen mithilfe des Dienstprogramms pktcap-uw 254
Nachverfolgen von Paketen mithilfe des Dienstprogramms pktcap-uw 265
Konfigurieren der NetFlow-Einstellungen eines vSphere Distributed Switch 267
Arbeiten mit der Portspiegelung 268
Portspiegelung - Interoperabilität 268
Erstellen einer Portspiegelungssitzung 271
Anzeigen von Details zu einer Portspiegelungssitzung 275
Bearbeiten der Details, Quellen und Ziele von Portspiegelungssitzungen 275
Überprüfung des Systemzustands des vSphere Distributed Switch 277
Aktivieren oder Deaktivieren der Überprüfung des Systemzustands des vSphere Distributed Switch 278
Anzeigen des Systemstatus von vSphere Distributed Switch 279
Switch-Discovery-Protokoll 279
Aktivieren des Cisco Discovery-Protokolls auf einem vSphere Distributed Switch 280
Aktivieren des Link Layer Discovery Protocol (LLDP) auf einem vSphere Distributed Switch 280
Anzeigen von Switch-Informationen 281
Anzeigen des Topologiediagramms eines NSX Virtual Distributed Switch 282

15 Konfigurieren von Protokollprofilen für Netzwerke virtueller Maschinen 283
Hinzufügen eines Netzwerkprotokollprofils 284
Benennen des Netzwerkprotokollprofils und Auswählen des Netzwerks 284
Festlegen der IPv4-Konfiguration des Netzwerkprotokollprofils 285
Festlegen der IPv6-Konfiguration für das Netzwerkprotokollprofil 285
Festlegen des DNS und weiterer Konfigurationseinstellungen für das Netzwerkprotokollprofil 286
Abschließen der Erstellung des Netzwerkprotokollprofils 286
Zuordnen einer Portgruppe zu einem Netzwerkprotokollprofil 287
Konfigurieren einer virtuellen Maschine oder von vApp zur Verwendung eines Netzwerkprotokollprofils 287

16 Multicast-Filter 289
Multicast-Filtermodi 289
Aktivieren von Multicast-Snooping auf einem vSphere Distributed Switch 291
Bearbeiten des Abfragezeitintervalls für Multicast-Snooping 291
Bearbeiten der Anzahl von IP-Adressen der Quelle für IGMP und MLD 292

17 Statusfreie Netzwerkbereitstellung 293

18 Optimale Vorgehensweisen für Netzwerke 296

19 Fehlerbehebung beim Netzwerk 298

Richtlinien zur Fehlerbehebung 299

Identifizieren der Symptome 299

Definieren des Problembereichs 299

Testen möglicher Lösungen 300

Fehlerbehebung mit Protokollen 301

Fehlerbehebung bei der Zuteilung von MAC-Adressen 303

Doppelte MAC-Adressen von virtuellen Maschinen im gleichen Netzwerk 303

Einschalten einer virtuellen Maschine schlägt aufgrund eines MAC-Adressenkonflikts fehl 306

Host kann nicht auf einem vSphere Distributed Switch entfernt werden 307

Für Hosts auf einem vSphere Distributed Switch wird die Verbindung zu vCenter Server getrennt 308

Für Hosts auf einem vSphere Distributed Switch 5.0 (und früher) wird die Verbindung zu vCenter Server getrennt 310

Alarm wegen des Verlusts der Netzwerkredundanz auf einem Host 311

Nach der Änderung der Failover-Reihenfolge für Uplinks einer verteilten Portgruppe wird die Verbindung zu virtuellen Maschinen getrennt 312

Physischer Adapter kann nicht zu einem vSphere Distributed Switch hinzugefügt werden 314

Fehlerbehebung bei SR-IOV-fähigen Arbeitslasten 315

SR-IOV-fähige Arbeitslast kann nach der Änderung der MAC-Adresse nicht mehr kommunizieren 315

Eine virtuelle Maschine, die einen VPN-Client ausführt, verursacht einen Denial-of-Service-Fehler für virtuelle Maschinen auf dem Host oder für einen vSphere HA-Cluster 316

Geringer Durchsatz für UDP-Arbeitslasten auf virtuellen Windows-Maschinen 318

Virtuelle Maschinen in derselben verteilten Portgruppe und auf unterschiedlichen Hosts können nicht miteinander kommunizieren 320

Der Versuch, eine migrierte vApp einzuschalten, schlägt fehl, weil das zugewiesene Protokollprofil fehlt 321

Für einen Netzwerkkonfigurationsvorgang wird ein Rollback durchgeführt und ein Host wird vom vCenter Server getrennt 323

Grundlegende Informationen zu vSphere-Netzwerken

vSphere-Netzwerk bietet Informationen zum Konfigurieren von Netzwerken für VMware vSphere®, 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.

vSphere Web Client und vSphere Client

Die Anweisungen in diesem Handbuch beziehen sich auf den vSphere Client (eine HTML5-basierte Benutzeroberfläche). Sie können die Anweisungen auch nutzen, um die Aufgaben mithilfe des vSphere Web Client (einer Flex-basierten Benutzeroberfläche) durchzuführen.

Für Aufgaben, bei denen sich der Workflow zwischen dem vSphere Client und dem vSphere Web Client erheblich unterscheidet, sind doppelte Prozeduren vorhanden. Die Schritte der einzelnen Prozeduren beziehen sich auf die jeweilige Client-Benutzeroberfläche. Im Titel der Prozeduren, die sich auf den vSphere Web Client beziehen, ist vSphere Web Client angegeben.

Hinweis In vSphere 6.7 Update 1 sind fast alle Funktionen des vSphere Web Client im vSphere Client implementiert. Eine aktuelle Liste aller nicht unterstützten Funktionen finden Sie im Handbuch für Funktions-Updates für den vSphere Client.

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
25. Jan. 2022	Es wurde ein Hinweis zu Einschränkungen bei der Auswahl von Port-Mirroring-Quellen hinzugefügt. Weitere Informationen finden Sie unter Auswählen von Port-Mirroring-Quellen.
12. APR 2021	Ein Hinweis zum Festlegen einer Failover-Richtlinie wurde hinzugefügt. Weitere Informationen finden Sie unter Konfigurieren von NIC-Teaming, Failover und Lastausgleich in einer verteilten Portgruppe oder einem verteilten Port.
04. August 2020	Wir bei VMware legen Wert auf die Verwendung neutraler Sprache. Um dieses Prinzip in unserer Kunden-, Partner- und internen Community zu fördern, ersetzen einen Teil der Terminologie in unseren Inhalten. Wir haben diesen Leitfaden aktualisiert, um Instanzen einer nicht inklusiven Sprache zu entfernen.
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.
20. FEB 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. Weitere Informationen finden Sie unter MAC-Bezeichner für Datenverkehr.
11. APR 2018	Erstversion.

Einführung in das vSphere-Netzwerk

1

Lernen Sie die grundlegenden Konzepte des vSphere-Netzwerks sowie Funktionen zum Einrichten und Konfigurieren eines Netzwerks in einer vSphere-Umgebung kennen.

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 vSphere 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.

Opakes Netzwerk

Ein Opaque-Netzwerk oder opakes Netzwerk ist ein Netzwerk, das von einer separaten Einheit außerhalb von vSphere erstellt und verwaltet wird. Von VMware NSX® erstellte und verwaltete logische Netzwerke werden beispielsweise in vCenter Server als opake Netzwerke des Typs nsx.LogicalSwitch angezeigt. Sie können ein opakes Netzwerk als Sicherung für einen VM Netzwerkadapter auswählen. Verwenden Sie zum Verwalten eines opaken Netzwerks die mit dem opaken Netzwerk verknüpften Verwaltungstools, z. B. VMware NSX® Manager oder die VMware NSX API-Verwaltungstools.

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 virtuellen 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

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. Eine Portgruppe legt Port-Konfigurationsoptionen, z. B. Bandbreitenbeschränkungen oder VLAN-Tagging-Richtlinien, für jeden Port in der Portgruppe fest.

vSphere Distributed Switch

Ein vSphere Distributed Switch agiert als einzelner Switch über alle verbundenen Hosts in einem Datencenter 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 auf alle Hosts übertragen, 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 vSAN.

IP-Speicher

Jede Form von Speicher, der die TCP/IP-Netzwerkkommunikation zugrunde liegt. iSCSI und NFS können als VM-Datenspeicher und für das direkte Mounten von `.ISO`-Dateien verwendet werden, die virtuellen Maschinen als CD-ROMs angezeigt 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 unterstützt vSphere Standard-Switches 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 *Installation und Einrichtung von vCenter Server*-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

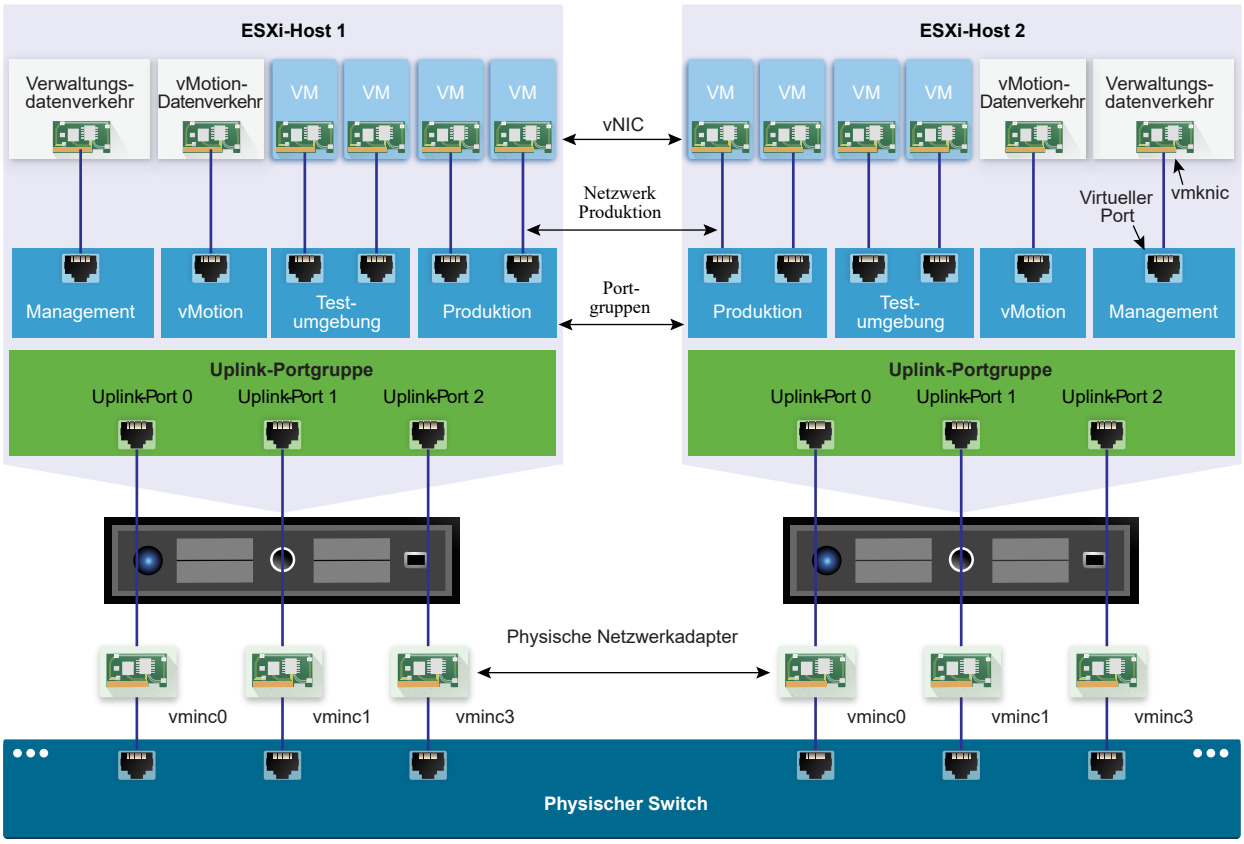
vSphere Standard-Switches

Sie können abstrakte Netzwerkgeräte erstellen, die als vSphere Standard-Switches bezeichnet werden. Mithilfe von Standard-Switches können Sie Netzwerkkonnektivität für Hosts und virtuelle Maschinen 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 Netzwerkkonnektivität für Hosts und virtuelle Maschinen 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. Die Netzwerkadapter der virtuellen Maschinen verfügen genauso wie die physischen Netzwerkkarten des Hosts am vSwitch jeweils über ihren eigenen logischen Port. Jeder logische Port auf dem Standard-Switch gehört einer einzelnen Portgruppe an. 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 Datencenter 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.

Sie können außerdem eine VLAN-ID festlegen, die den Netzwerkverkehr auf ein logisches Segment des physikalischen Netzes einschränkt. Damit Portgruppen den gleichen Datenverkehr wie der Host erhalten, der aber von mehr als einem VLAN stammt, muss die VLAN-ID auf VGT (VLAN 4095) eingestellt sein.

Anzahl der Standardports

Für eine effiziente Verwendung der Hostressourcen wird auf ESXi-Hosts 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **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 vSAN-Datenverkehr.
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	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	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 7.
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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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 Topologiediagrammtitel auf das Symbol **Einstellungen bearbeiten**.

6 Benennen Sie auf der Seite „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 auf der Seite „Sicherheit“ die Switch-Einstellungen, um Schutz vor der Imitation von MAC-Adressen und vor der Ausführung von virtuellen Maschinen im promiskuitiven Modus zu bieten.

9 Überschreiben Sie auf der Seite „Traffic-Shaping“ auf der Portgruppenebene die Größe für die Durchschnitts- und Spitzenbandbreite und für Bursts.

10 Überschreiben Sie auf der Seite „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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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 werden auf ESXi-Hosts 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.

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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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 einen MTU-Wert von mehr als 1500 festlegen. Es kann keine MTU-Größe von mehr als 9000 Byte festgelegt werden.

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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Physische Adapter** aus.

   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 in der Liste aus und klicken Sie auf das Symbol **Adaptereinstellungen 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 Adaptern 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Virtuelle Switches** aus.

3 Wählen Sie den Standard-Switch, dem Sie einen physischen Adapter hinzufügen möchten.

4 Klicken Sie auf das Symbol **Physische Netzwerkadapter, die mit dem ausgewählten Switch verbunden sind, 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Virtuelle Switches** aus.

3 Wählen Sie den Standard-Switch aus der Liste aus.

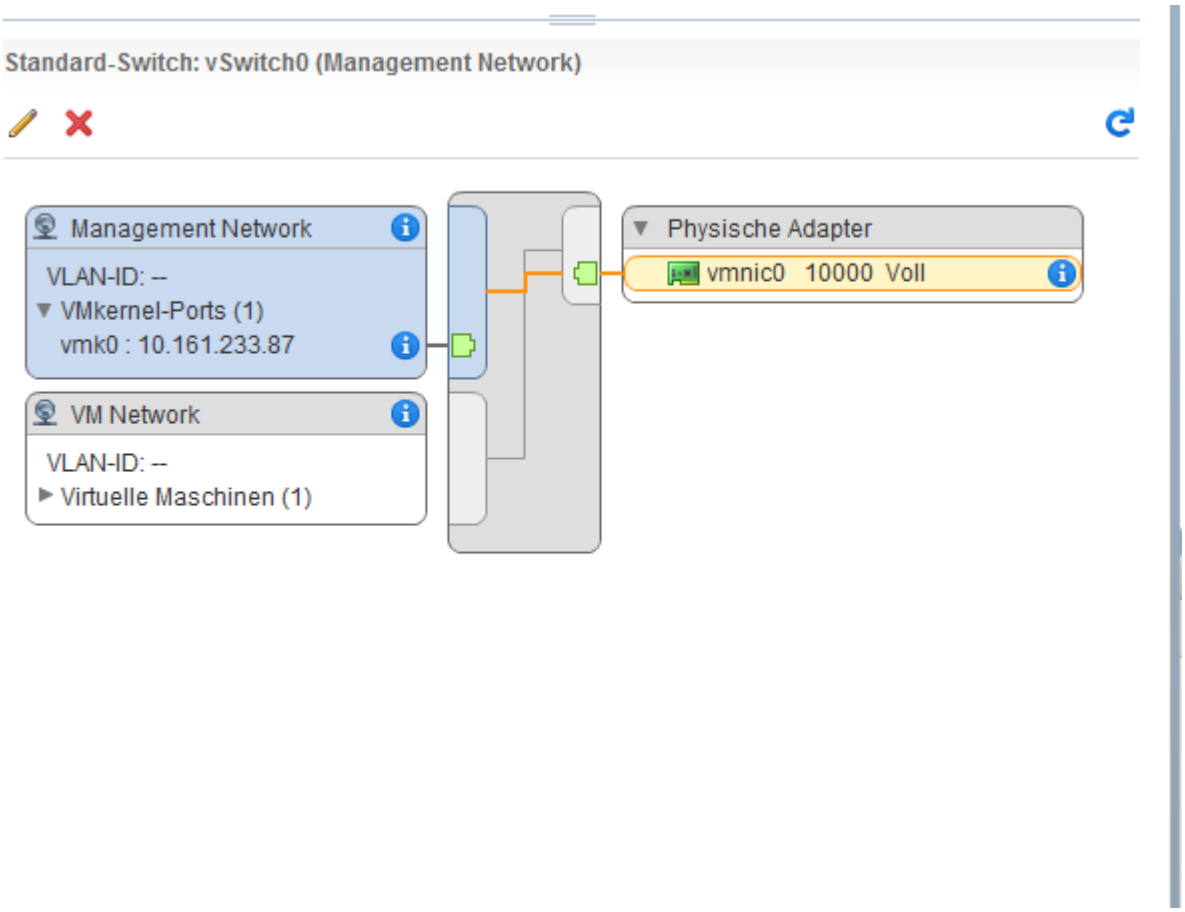
Ergebnisse

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.

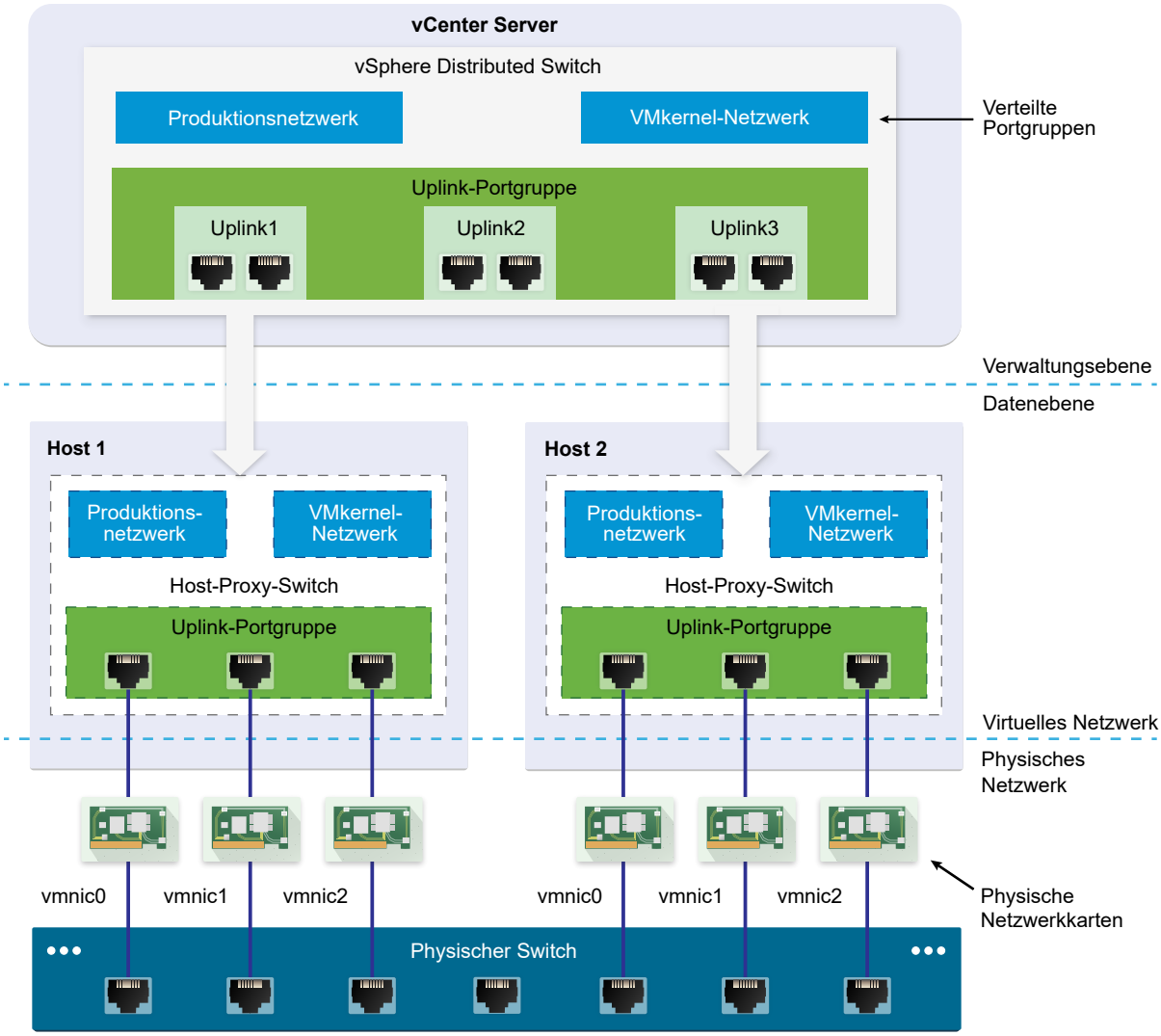
Dieses Kapitel enthält die folgenden Themen:

- 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.

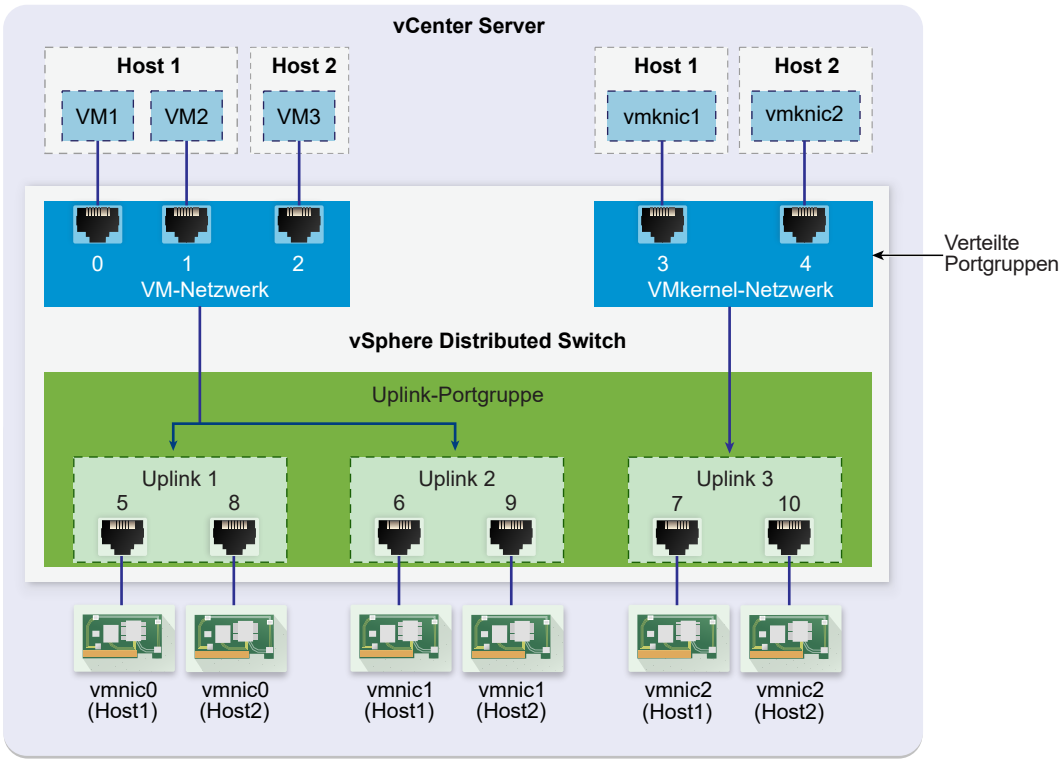
Beispiel: Angenommen, Sie erstellen einen vSphere Distributed Switch auf Ihrem Datencenter und verknüpfen zwei Hosts damit. Sie konfigurieren drei Uplinks zur Uplink-Portgruppe und schließen eine physische Netzwerkkarte von jedem Host zu einem Uplink an. Auf diese Weise werden jedem Uplink zwei physische Netzwerkkarten von jedem Host zugeordnet, zum Beispiel wird Uplink 1 mit vmnic0 von Host 1 und Host 2 konfiguriert. Dann erstellen stellen 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.

Für eine effiziente Verwendung der Hostressourcen wird 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.

Datenfluss beim vSphere Distributed Switch

Der Datenfluss von den virtuellen Maschinen und VMkernel-Adaptern 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.

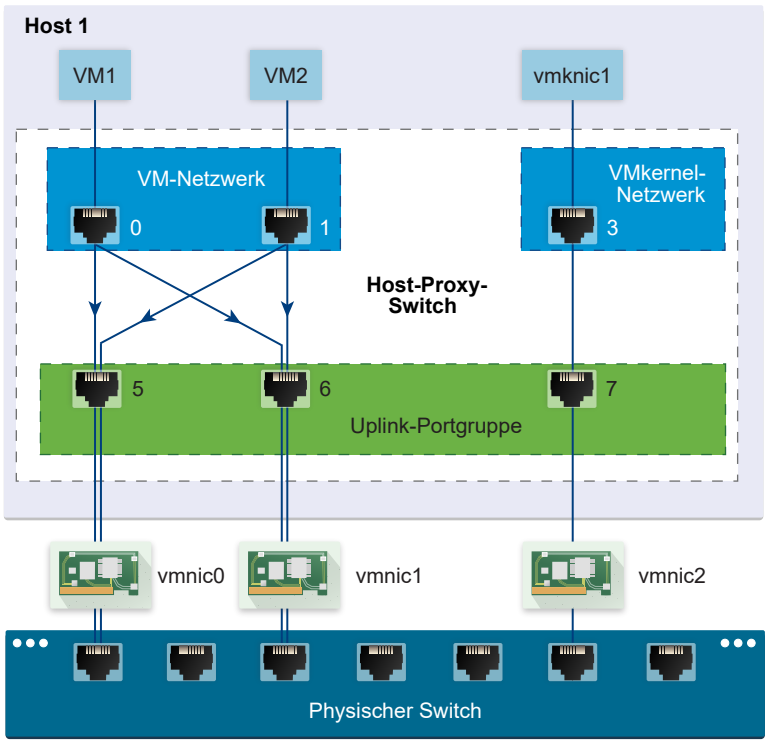
Abbildung 3-2. NIC-Gruppierung und Portzuteilung auf einem vSphere Distributed Switch



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 Datencenter, um die Netzwerkkonfiguration mehrerer Hosts gleichzeitig von einer zentralen Stelle aus zu regeln.

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 **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: 6.6.0	Kompatibel mit ESXi 6.7 und höher.
Distributed Switch: 6.5.0	Kompatibel mit ESXi Version 6.5 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Distributed Switch: 6.0.0	Kompatibel mit ESXi Version 6.0 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.

5 Konfigurieren Sie auf der Seite „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 auf der Seite „Bereit zum Abschließen“ die ausgewählten Einstellungen und klicken Sie auf **Beenden**.

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

Ergebnisse

Ein Distributed Switch wird im Datencenter 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 6.x auf eine höhere Version durchführen. Nach dem Upgrade kann der Distributed Switch Funktionen nutzen, die nur in der neueren Version verfügbar sind.

Beim Aktualisieren eines Distributed Switch kommt es auf den mit dem Switch verbundenen Hosts und virtuellen Maschinen zu kurzen Ausfallzeiten. Weitere Informationen finden Sie unter KB 52621.

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 6.7.
- Aktualisieren Sie alle Hosts, die mit dem Distributed Switch verbunden sind, auf ESXi6.7.

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 6.6.0	Kompatibel mit ESXi Version 6.7 und höher.
Version 6.5.0	Kompatibel mit ESXi Version 6.5 und höher. Erst in späteren Versionen von vSphere Distributed Switch implementierte Funktionen werden nicht unterstützt.
Version 6.0.0	Kompatibel mit ESXi Version 6.0 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.

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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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 Network I/O Control 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	■ **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	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 und vSAN 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.

- 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 Datencenter 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 Zielportgruppen 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 Zielportgruppe 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 auf der Seite „Aufgabe auswählen“ die Option **Hosts hinzufügen** aus und klicken Sie auf **Weiter**.
4. Klicken Sie auf der Seite „Hosts auswählen“ auf **Neue Hosts**, treffen Sie aus den Hosts im Datencenter eine Auswahl, klicken Sie auf **OK** und anschließend auf **Weiter**.
5. Wählen Sie auf der Seite „Netzwerkadapteraufgaben auswählen“ die Aufgaben für das Konfigurieren von Netzwerkadaptern zum verteilten Switch aus und klicken Sie auf **Weiter**.

6 Konfigurieren Sie auf der Seite „Physische Netzwerkadapter verwalten“ physische Netzwerkkarten zum verteilten 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 auf der Seite „VMkernel-Netzwerkadapter verwalten“ VMkernel-Aadapter.

   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.

   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.

10 Klicken Sie auf **Weiter**.

11 Konfigurieren Sie auf der Seite „VM-Netzwerk migrieren“ das virtuelle Maschinen-Netzwerk.

   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**.

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

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 unter **Aufgabe auswählenHostnetzwerk verwalten** aus und klicken Sie auf **Weiter**.
4. Klicken Sie unter **Hosts auswählen** auf **Angehängte Hosts...** und wählen Sie aus den Hosts aus, die mit dem Distributed Switch verknüpft sind.
5. Klicken Sie auf **Weiter**.
6. Wählen Sie unter **Netzwerkadapteraufgaben auswählen** die Option **Physische Adapter verwalten** aus und klicken Sie auf **Weiter**.
7. Wählen Sie in **Physische Netzwerkadapter verwalten** eine physische Netzwerkkarte aus der Liste „Auf anderen Switches/frei“ 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-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.

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 unter **Aufgabe auswählenHostnetzwerk verwalten** aus und klicken Sie auf **Weiter**.

4 Klicken Sie unter **Hosts auswählen** auf **Angehängte Hosts...** und wählen Sie aus den Hosts aus, die mit dem Distributed Switch verknüpft sind.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie unter **Netzwerkadapteraufgaben auswählen** die Option **VMkernel-Adapter verwalten** aus und klicken Sie auf **Weiter**.

7 Wählen Sie unter **VMkernel-Netzwerkadapter verwalten** 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 und vSAN 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 unter **Aufgabe auswählenHostnetzwerk verwalten** aus und klicken Sie auf **Weiter**.

4 Klicken Sie unter **Hosts auswählen** auf **Angehängte Hosts...** und wählen Sie aus den Hosts aus, die mit dem Distributed Switch verknüpft sind.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie unter **Netzwerkadapteraufgaben auswählen** die Option **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 unter **Zielgerät auswählen** eine verteilte Portgruppe aus und klicken Sie auf **Weiter**.

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	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	Für den Standard-TCP/IP-Stack auf dem Host können Dienste aktiviert werden. Zur Auswahl stehen die folgenden Dienste: ■ **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 Zielreplizierungssite. ■ **vSAN**. Ermöglicht den vSAN-Datenverkehr auf dem Host. Jeder Host, der Teil eines Clusters für vSAN 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 Warnungsdialogfeld 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-Adaptern 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
IPv4-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IPv4-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. Aktivieren Sie das Kontrollkästchen **Standard-Gateway für diesen Adapter überschreiben** und geben Sie eine Gateway-Adresse ein, wenn Sie ein anderes Gateway für den VMkernel-Adapter angeben möchten.

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. In ESXi 6.5 und höher ist die Router-Ankündigung standardmäßig aktiviert und unterstützt die M- und O-Flags gemäß RFC 4861.
Statische IPv6-Adressen	a Klicken Sie auf **IPv6-Adresse 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 Um das VMkernel-Standard-Gateway zu ändern, klicken Sie auf **Standard-Gateway für diesen Adapter überschreiben**. Die Adresse des Standard-Gateways für VMkernel für IPv6 wird vom ausgewählten TCP/IP-Stack bezogen.

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 unter **Aufgabe auswählenHostnetzwerk verwalten** aus und klicken Sie auf **Weiter**.

4 Klicken Sie unter **Hosts auswählen** auf **Angehängte Hosts...** und wählen Sie aus den Hosts aus, die mit dem Distributed Switch verknüpft sind.

5 Klicken Sie auf **Weiter**.

6 Wählen Sie unter **Netzwerkadapteraufgaben auswählenNetzwerk virtueller 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**.

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 Netzwerkadapteraufgaben 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**.

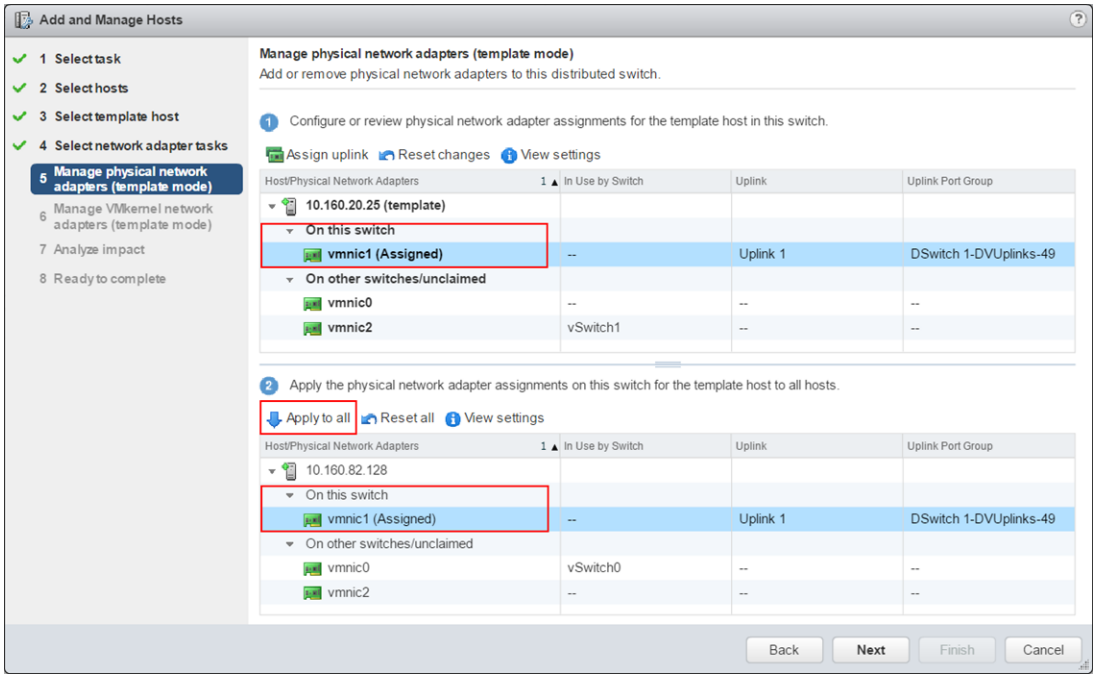
9 Klicken Sie auf der Seite „Bereit zum Abschließen“ auf **Beenden**.

Beispiel: Konfigurieren von physischen Adaptern und VMkernel-Adaptern 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 einem Uplink auf dem Vorlagenhost eine physische Netzwerkkarte zu und klicken Sie dann auf **Auf alle anwenden**, um die gleiche Konfiguration auf dem anderen Host zu erstellen.

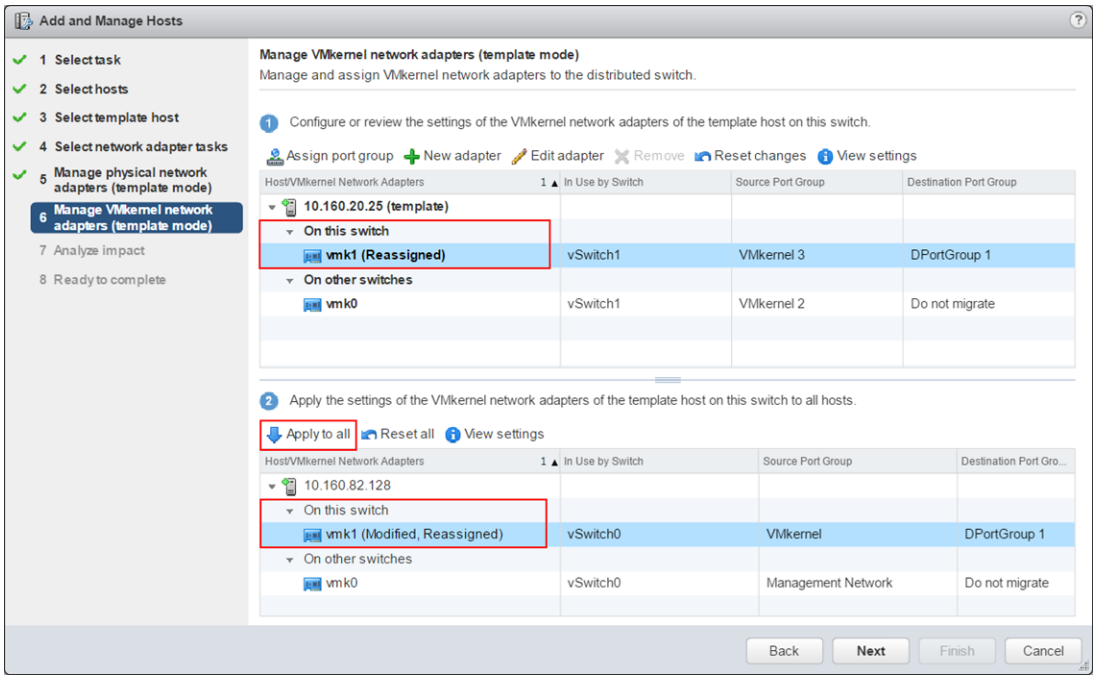
Abbildung 3-4. Anwenden der Konfiguration von physischen Netzwerkkarten auf einen vSphere Distributed Switch anhand eines Vorlagenhosts



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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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 zu diesem Distributed Switch 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-Adaptern 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Virtuelle Switches** aus.

3 Wählen Sie den Ziel-Standard-Switch aus der Liste aus.

4 Klicken Sie auf **Einen VMkernel-Netzwerkadapter auf den ausgewählten Switch 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 auf der Seite „Bereit zum Abschließen“ die Migrationsdetails 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Virtuelle Switches** aus.

3 Wählen Sie einen Distributed Switch aus der Liste aus.

4 Klicken Sie auf das Symbol **Physische Netzwerkadapter, die mit dem ausgewählten Switch verbunden sind, 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Virtuelle Switches** aus.

3 Wählen Sie den Distributed Switch aus.

4 Klicken Sie auf das Symbol **Physische Netzwerkadapter, die mit dem ausgewählten Switch verbunden sind, 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.

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	Wählen Sie aus, wann Ports virtuellen Maschinen zugewiesen werden, die mit dieser verteilten Portgruppe verbunden sind. ■ **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 Bindung**: 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	■ **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.

Einstellung	Beschreibung
VLAN	Verwenden Sie das Dropdown-Menü **VLAN-Typ**, um die VLAN-Optionen auszuwählen: ■ **Keine**: Verwenden Sie VLAN nicht. ■ **VLAN**: Geben Sie im Textfeld **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 auf der Seite „Sicherheit“ die Sicherheitsausnahmen und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Promiscuous-Modus	■ **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. Firewalls, Portscanner, Erkennungssysteme für Eindringversuche usw. müssen im promiskuitiven Modus ausgeführt werden.
MAC-Adressänderungen	■ **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. Wenn das Gastbetriebssystem die MAC-Adresse zurück ändert, empfängt die virtuelle Maschine wieder Frames. ■ **Akzeptieren**. Wenn das Gastbetriebssystem die MAC-Adresse eines Netzwerkadapters ändert, empfängt der Adapter Frames an der neuen Adresse.
Gefälschte Übertragungen	■ **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 auf der Seite „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.
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 auf der Seite „Teaming und Failover“ die Einstellungen und klicken Sie auf **Weiter**.

Einstellung	Beschreibung
Lastausgleich	Geben Sie an, wie ein Uplink ausgewählt werden soll. ■ **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-Ermittlungkriterien erfüllt. **Hinweis** Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit „EtherChannel“ konfiguriert wird. Deaktivieren Sie „EtherChannel“ bei allen anderen Optionen.
Netzwerkausfallerkennung	Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an. ■ **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. **Hinweis** Verwenden Sie die Signalprüfung nicht zusammen mit dem IP-Hash-Lastausgleich.

Einstellung	Beschreibung
Switches benachrichtigen	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, eine Benachrichtigung über das Netzwerk 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. **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.
Failback	Wählen Sie **Ja** oder **Nein**, um die Failback-Funktion zu deaktivieren bzw. zu aktivieren. 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.
Failover-Reihenfolge	Geben Sie an, wie die Arbeitslast 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: ■ **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 des aktiven Adapters nicht verfügbar ist. ■ **Nicht verwendete Uplinks**. Verwenden Sie diesen Uplink nicht. **Hinweis** Wenn Sie den IP-Hash-Lastausgleich verwenden, konfigurieren Sie keine Standby-Uplinks.

8 (Optional) Aktivieren oder deaktivieren Sie auf der Seite „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 auf der Seite „Sonstiges“ **Ja** 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 auf der Seite „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 auf der Seite „Bereit zum Abschließen“ die Einstellungen und klicken Sie auf **Beenden**.

Klicken Sie auf die Schaltfläche **Zurück**, wenn Sie eine Einstellung 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 **Netzwerke**.

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	Wählen Sie aus, wann Ports virtuellen Maschinen zugewiesen werden, die mit dieser verteilten Portgruppe verbunden sind. ■ **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	■ **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

1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.

   a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Netzwerke**.

   b Klicken Sie auf **Verteilte Portgruppen**.

2 Wählen Sie die verteilte Portgruppe aus.

3 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 **Netzwerke**.

   b Klicken Sie auf **Verteilte Portgruppen**.

2 Doppelklicken Sie auf eine verteilte Portgruppe.

3 Klicken Sie auf die Registerkarte **Ports** und wählen Sie einen Port aus der Hardwareliste aus.

4 Klicken Sie auf das Symbol **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 **Netzwerke**.

   b Klicken Sie auf **Verteilte Portgruppen**.

2 Doppelklicken Sie auf eine verteilte Portgruppe in der Liste.

3 Klicken Sie auf die Registerkarte **Ports** und wählen Sie einen verteilten Port aus der Tabelle aus.

   Am unteren Rand des Bildschirms werden Informationen zum verteilten Port angezeigt.

4 Klicken Sie auf das Symbol **Einstellungen des verteilten Ports bearbeiten**.

5 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 Netzwerkadapter mit verteilten Portgruppen verbinden. Dies kann entweder für eine individuelle virtuelle Maschine durch Ändern der Konfiguration des Netzwerkadapters 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 **VMs 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 Netzwerkadapter 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 Datencenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **VMs**.

b Klicken Sie auf **Virtuelle Maschinen** und doppelklicken Sie auf die virtuelle Maschine aus der Liste.

2 Erweitern Sie auf der Registerkarte **Konfigurieren** der virtuellen Maschine **Einstellungen** und wählen Sie **VM-Hardware**.

3 Klicken Sie auf **Bearbeiten**.

4 Erweitern Sie den Abschnitt **Netzwerkadapter** und wählen Sie **Weitere Netzwerke anzeigen** aus dem Dropdown-Menü **Netzwerkadapter** aus.

5 Wählen Sie im Dialogfeld zur Netzwerkauswahl eine verteilte Portgruppe aus und klicken Sie auf **OK**.

6 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-Adaptern, VMkernel-Adaptern und physischen Adaptern 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. Erweitern Sie auf der Registerkarte **Konfigurieren** die **Einstellungen** und wählen Sie **Topologie**.

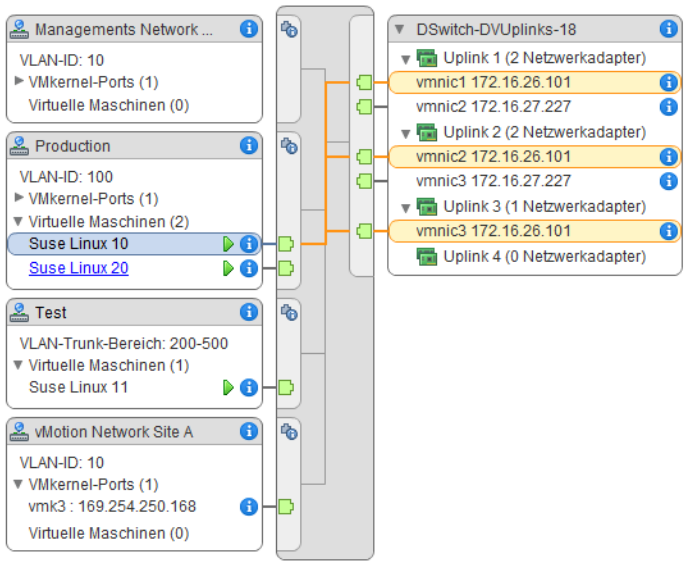
Ergebnisse

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 Domänennamen 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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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, vSAN usw. aufzunehmen.

- VMkernel-Netzwerkebene

  Die VMkernel-Netzwerkschicht bietet Verbindung zu Hosts und verarbeitet den Standard-Systemdatenverkehr von vSphere vMotion, IP-Speicher, Fault Tolerance, vSAN usw. 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, vSAN 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, vSAN 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.

- Außerkraftsetzen des Standard-Gateways eines VMkernel-Adapters

  Unter Umständen müssen Sie das Standard-Gateway für einen VMkernel-Netzwerkadapter überschreiben, um ein anderes Gateway für vSphere vMotion bereitzustellen.

- Konfigurieren des VMkernel-Adapter-Gateways mit esxcli-Befehlen

  Sie können das Standard-Gateway eines VMkernel-Adapters mithilfe von esxcli-Befehlen überschreiben, um ein anderes Gateway für vSphere vMotion anzugeben.

- 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-Netzwerkschicht bietet Verbindung zu Hosts und verarbeitet den Standard-Systemdatenverkehr von vSphere vMotion, IP-Speicher, Fault Tolerance, vSAN usw. 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 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 für die Verarbeitung des NFC-Datenverkehrs bei vMotion für große Entfernungen verwenden. NFC stellt einen dateispezifischen FTP-Dienst für vSphere bereit. ESXi verwendet NFC für das 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 *vSphere-Installation und -Einrichtung*.

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. Konfigurieren Sie die VMkernel-Adapter für vMotion so, dass sie 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 NFS 3 und 4.1. Zum Konfigurieren eines Fibre Channel über Ethernet (FCoE)-Softwareadapters müssen Sie über einen dedizierten VMkernel-Adapter verfügen. 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 Zielreplizierungssite.

vSAN-Datenverkehr

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

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 die Registerkarte **Konfigurieren** und erweitern Sie das Menü **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, vSAN 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **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 Standard-Switch**.

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 **Adapter hinzufügen** und wählen Sie die benötigten physischen Netzwerkkarten 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	Für den Standard-TCP/IP-Stack auf dem Host können Dienste aktiviert werden. Zur Auswahl stehen die folgenden Dienste: ■ **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 Zielreplizierungssite. ■ **vSAN**. Ermöglicht den vSAN-Datenverkehr auf dem Host. Jeder Host, der Teil eines vSAN-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 Warnungsdialogfeld 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-Adaptern 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
IPv4-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IPv4-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. Aktivieren Sie das Kontrollkästchen **Standard-Gateway für diesen Adapter überschreiben** und geben Sie eine Gateway-Adresse ein, wenn Sie ein anderes Gateway für den VMkernel-Adapter angeben möchten.

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. In ESXi 6.5 und höher ist die Router-Ankündigung standardmäßig aktiviert und unterstützt die M- und O-Flags gemäß RFC 4861.
Statische IPv6-Adressen	a Klicken Sie auf **IPv6-Adresse 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 Um das VMkernel-Standard-Gateway zu ändern, klicken Sie auf **Standard-Gateway für diesen Adapter überschreiben**. Die Adresse des Standard-Gateways für VMkernel für IPv6 wird vom ausgewählten TCP/IP-Stack bezogen.

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, vSAN 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **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	Für den Standard-TCP/IP-Stack auf dem Host können Dienste aktiviert werden. Zur Auswahl stehen die folgenden Dienste: ■ **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 Zielreplizierungssite. ■ **vSAN**. Ermöglicht den vSAN-Datenverkehr auf dem Host. Jeder Host, der Teil eines Clusters für vSAN 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 Warnungsdialogfeld 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-Adaptern 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
IPv4-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IPv4-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. Aktivieren Sie das Kontrollkästchen **Standard-Gateway für diesen Adapter überschreiben** und geben Sie eine Gateway-Adresse ein, wenn Sie ein anderes Gateway für den VMkernel-Adapter angeben möchten.

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. In ESXi 6.5 und höher ist die Router-Ankündigung standardmäßig aktiviert und unterstützt die M- und O-Flags gemäß RFC 4861.
Statische IPv6-Adressen	a Klicken Sie auf **IPv6-Adresse 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 Um das VMkernel-Standard-Gateway zu ändern, klicken Sie auf **Standard-Gateway für diesen Adapter überschreiben**. Die Adresse des Standard-Gateways für VMkernel für IPv6 wird vom ausgewählten TCP/IP-Stack bezogen.

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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **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 Zielreplizierungssite.
vSAN	Aktiviert den vSAN-Datenverkehr auf dem Host. Jeder Host, der Teil eines vSAN-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
IPv4-Einstellungen automatisch abrufen	DHCP zum Beziehen der IP-Einstellungen verwenden. Ein DHCP-Server muss im Netzwerk vorhanden sein.
Statische IPv4-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. Aktivieren Sie das Kontrollkästchen **Standard-Gateway für diesen Adapter überschreiben** und geben Sie eine Gateway-Adresse ein, wenn Sie ein anderes Gateway für den VMkernel-Adapter angeben möchten.

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. In ESXi 6.5 und höher ist die Router-Ankündigung standardmäßig aktiviert und unterstützt die M- und O-Flags gemäß RFC 4861.
Statische IPv6-Adressen	a Klicken Sie auf **IPv6-Adresse 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 Um das VMkernel-Standard-Gateway zu ändern, klicken Sie auf **Standard-Gateway für diesen Adapter überschreiben**. Die Adresse des Standard-Gateways für VMkernel für IPv6 wird vom ausgewählten TCP/IP-Stack bezogen.

Klicken Sie auf der Seite „IPv6-Einstellungen“ auf „Erweiterte Einstellungen“, um IPv6-Adressen zu 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 „Auswirkungen analysieren“ sicher, dass die am VMKernel-Adapter vorgenommenen Änderungen andere Vorgänge nicht stören.

9 Klicken Sie auf **OK**.

Außerkraftsetzen des Standard-Gateways eines VMkernel-Adapters

Unter Umständen müssen Sie das Standard-Gateway für einen VMkernel-Netzwerkadapter überschreiben, um ein anderes Gateway für vSphere vMotion bereitzustellen.

Jeder TCP/IP-Stack auf einem Host kann nur einen Standard-Gateway aufweisen. Dieser Standard-Gateway ist Bestandteil der Routing-Tabelle und er wird von allen auf dem TCP/IP-Stack betriebenen Dienste verwendet.

Die VMkernel-Adapter vmk0 und vmk1 können beispielsweise auf einem Host konfiguriert werden.

- vmk0 wird für Verwaltungsdatenverkehr im Subnetz 10.162.10.0/24 mit dem Standard-Gateway 10.162.10.1 verwendet.
- vmk1 wird für Datenverkehr von vMotion im Subnetz 172.16.1.0/24 verwendet.

Wenn Sie 172.16.1.1 als Standard-Gateway für vmk1 festlegen, verwendet vMotion vmk1 als Egress-Schnittstelle mit dem Gateway 172.16.1.1. Der Gateway 172.16.1.1 ist Bestandteil der vmk1-Konfiguration und nicht in der Routing-Tabelle enthalten. Nur diejenigen Dienste, die vmk1 als Egress-Schnittstelle festlegen, verwenden diesen Gateway. Dadurch können für Dienste, die mehrere Gateways benötigen, zusätzliche Schicht 3-Verbindungen bereitgestellt werden.

Sie können den vSphere Web Client oder einen ESXCLI-Befehl verwenden, um den Standard-Gateway eines VMkernel-Adapters zu konfigurieren.

Siehe Erstellen eines VMkernel-Adapters auf einem vSphere Standard-Switch, Erstellen eines VMkernel-Adapters auf einem Host, der einem vSphere Distributed Switch zugeordnet ist und Konfigurieren des VMkernel-Adapter-Gateways mit esxcli-Befehlen.

Konfigurieren des VMkernel-Adapter-Gateways mit esxcli-Befehlen

Sie können das Standard-Gateway eines VMkernel-Adapters mithilfe von esxcli-Befehlen überschreiben, um ein anderes Gateway für vSphere vMotion anzugeben.

Verfahren

1 Stellen Sie eine SSH-Verbindung mit dem Host her.

2 Melden Sie sich als Root-Benutzer an.

3 Führen Sie den folgenden Befehl aus.

Option	Beschreibung
IPv4	`esxcli network ip interface ipv4 set -i vmknic -t static -g IPv4-Gateway -I IPv4-Adresse -N Maske`

IPv6	**Wichtig** Sie müssen DHCPv6 oder Router-Werbung deaktivieren, bevor Sie das IPv6 vmknic-Gateway festlegen können.
	`esxcli network ip interface ipv6 set -i vmknic -d off -r off`
	So fügen Sie eine statische IPv6-Adresse hinzu:
	`esxcli network ip interface ipv6 address add -i vmknic -I IPv6-Adresse`
	So richten Sie das IPv6-vmknic-Gateway ein:
	`esxcli network ip interface ipv6 set -i vmknic -g IPv6-Gateway`

Dabei ist *vmknic* der Name des VMkernel-Adapters, *gateway* ist die IP-Adresse des Gateways, *IP address* ist die Adresse des VMkernel-Adapters und *mask* ist die Netzwerkmaske.

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. Erweitern Sie **Netzwerk** auf der Registerkarte **Konfigurieren** 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.

Hinweis Sie können nur die DNS- und Standard-Gateway-Konfiguration auf dem Standard-TCP/IP-Stack ändern. Das Ändern der DNS- und Standard-Gateway-Konfiguration auf benutzerdefinierten TCP/IP-Stacks wird nicht unterstützt.

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	Wählen Sie eine Methode zum Abrufen des DNS-Server aus. ■ 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. a Bearbeiten Sie den Hostnamen. b Bearbeiten Sie den Domänennamen. 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 Domänennamen verwendet werden.
Routing	Bearbeiten Sie die VMkernel-Gatewayinformationen. **Hinweis** Durch Entfernen des Standard-Gateways kann die Verbindung zwischen Client und Host getrennt werden.
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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **VMkernel-Adapter** aus.
3. Wählen Sie einen VMkernel-Adapter aus der Liste aus und klicken Sie auf das Symbol **Ausgewählten Netzwerkadapter entfernen**.
4. Klicken Sie im Bestätigungsdialogfeld 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“.

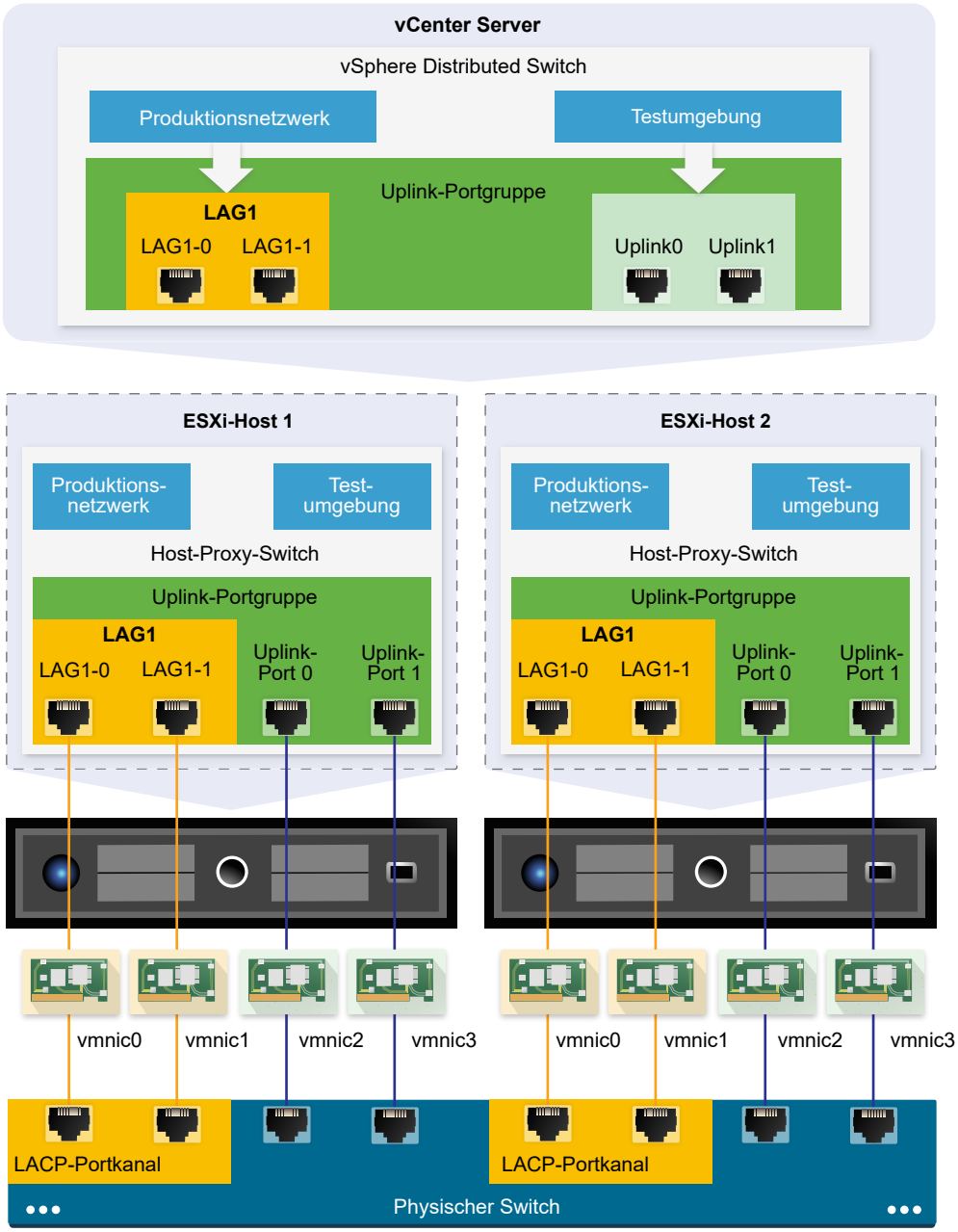
6. Klicken Sie auf **OK**.

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 Linkzusammenfassungsgruppe mit zwei oder mehr Ports und verbinden physische Netzwerkkarten mit den Ports. Ports von Linkzusammenfassungsgruppen werden innerhalb der Linkzusammenfassungsgruppe gruppiert und für den Lastausgleich des Netzwerkdatenverkehrs zwischen den Ports wird ein LACP-Hashing-Algorithmus verwendet. Mithilfe einer Linkzusammenfassungsgruppe 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:

- Konfiguration von LACP-Teaming und -Failover für verteilte Portgruppen
- Konfigurieren einer Linkzusammenfassungsgruppe zur Regelung des Datenverkehrs für verteilte Portgruppen
- Bearbeiten einer Linkzusammenfassungsgruppe

- Einschränkungen der LACP-Unterstützung für einen vSphere Distributed Switch

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 6.0 oder höher 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Einstellungen** und wählen Sie **LACP** aus.

3 Klicken Sie auf das Symbol **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 einzelnem 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 Portgruppe > 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 Portgruppe > 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**.

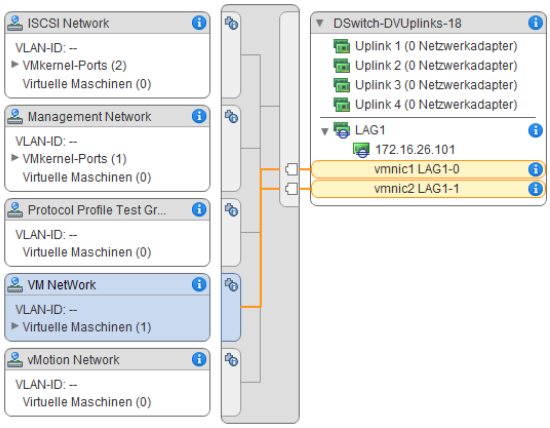
Ergebnisse

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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Einstellungen** und wählen Sie **LACP** aus.

3 Klicken Sie auf das Symbol **Neue Linkzusammenfassungsgruppe**.

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**.

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.

- LACP wird nicht mit Software-iSCSI-Port-Bindung unterstützt. iSCSI-Multipathing über LAG wird unterstützt, wenn keine Port-Bindung verwendet wird.
- 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 Linkzusammenfassungsgruppe geregelt wird.

Sichern und Wiederherstellen von Netzwerkkonfigurationen

6

vSphere ermöglicht die Sicherung und Wiederherstellung der Konfiguration von vSphere Distributed Switches sowie verteilten und Uplink-Portgruppen im Fall von ungültigen Änderungen oder Übertragungen an 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.

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** aus.
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. Weitere Informationen hierzu finden Sie unter Importieren einer vSphere Distributed Switch-Konfiguration.
- Überschreiben Sie die Einstellungen eines vorhandenen Distributed Switch. Weitere Informationen hierzu finden Sie unter Wiederherstellen einer vSphere Distributed Switch-Konfiguration.

Sie können auch nur Portgruppenkonfigurationen exportieren, importieren und wiederherstellen. Weitere Informationen hierzu finden Sie unter 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.

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.

Verfahren

1. Navigieren Sie im vSphere Web Client zu einem Datencenter.
2. Klicken Sie mit der rechten Maustaste auf das Datencenter 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.

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.

Verfahren

1 Suchen Sie eine verteilte Portgruppe im vSphere Web Client.

a Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Netzwerke**.

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.

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.

Verfahren

1. Suchen Sie eine verteilte Portgruppe im vSphere Web Client.
   a. Wählen Sie einen Distributed Switch aus und klicken Sie auf die Registerkarte **Netzwerke**.
   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

Sie können 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.

Die Rollback-Funktion ist im vSphere-Netzwerk 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. Weitere Informationen hierzu finden Sie unter Wiederherstellen einer Konfiguration für verteilte vSphere-Portgruppen.

Deaktivieren des Netzwerk-Rollbacks

Rollback ist in vSphere 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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Einstellungen** und wählen Sie **Erweiterte Einstellungen** aus.
3. 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

Rollback ist in vSphere 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

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

Wenn 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.

Netzwerkrichtlinien

8

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_0bjobp2b)

- 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 Lastaustgleichsalgorithmen 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 einem vSphere Distributed Switch 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.

- MAC Learning-Richtlinie

  MAC Learning bietet Netzwerkkonnektivität zu Bereitstellungen, bei denen mehrere MAC-Adressen von einer vNIC verwendet werden.

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 **Netzwerke**.

   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 Lastaustgleichsalgorithmen 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 Signalpakete. 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 Zugriffssschnittstellen oder den PortfFast-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.

Bei der Methode „Anhand des ursprünglichen virtuellen Ports routen“ handelt es sich um die Standardmethode für den Lastausgleich auf dem vSphere Standard-Switch und dem vSphere Distributed Switch.

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, solang 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	■ 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	■ 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	■ 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	■ 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 und 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. 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	■ 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	■ 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	■ 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	■ 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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	a Wählen Sie den Switch aus der Liste aus. b Klicken Sie auf **Einstellungen bearbeiten** und wählen Sie **Teaming und Failover** aus.
Standard-Portgruppe	a Wählen Sie den Switch aus, bei dem sich die Portgruppe befindet. b Wählen Sie im Switch-Topologiediagramm die Standardportgruppe aus und klicken Sie auf **Einstellungen bearbeiten**. c Wählen Sie **Teaming und Failover** aus. d 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.
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 **Netzwerkausfallerkennung** 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 Signalpakete. 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 hierzu 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.

Hinweis Das Festlegen einer Failback-Option wird in Verbindung mit der Teaming-Richtlinie **Anhand der physischen Netzwerkkartenauslastung routen** nicht unterstützt.

Voraussetzungen

Um eine Richtlinie auf der Ebene der verteilten Ports außer Kraft zu setzen, aktivieren Sie die Außerkraftsetzungen auf Portebene für diese Richtlinie. Weitere Informationen hierzu finden Sie unter 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	a Wählen Sie im Menü **Aktionen** die Option **Verteilte Portgruppe > Verteilte Portgruppen verwalten** aus. b Wählen Sie **Teaming und Failover** aus. c Wählen Sie die Portgruppe aus und klicken Sie auf **Weiter**.
Verteilter Port	a Klicken Sie auf der Registerkarte **Netzwerke** auf **Verteilte Portgruppen** und doppelklicken Sie auf eine verteilte Portgruppe. b Wählen Sie auf der Registerkarte **Ports** einen Port aus und klicken Sie auf **Einstellungen des verteilten Ports bearbeiten**. c Wählen Sie **Teaming und Failover** aus. d 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. **Hinweis** Die Auswahl von **Anhand der physischen Netzwerkkartenauslastung routen** hindert Sie daran, eine Failback-Option für eine verteilte Portgruppe festzulegen.
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 **Netzwerkausfallerkennung** 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 Signalpakete. 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 Netzwerkumgebung 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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien 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	a Wählen Sie im Menü **Aktionen** die Option **Verteilte Portgruppe > Verteilte Portgruppen verwalten** aus. b Wählen Sie **VLAN** aus und klicken Sie auf **Weiter**. c Wählen Sie die Portgruppe aus und klicken Sie auf **Weiter**.
Verteilter Port	a Klicken Sie auf der Registerkarte **Netzwerke** auf **Verteilte Portgruppen** und doppelklicken Sie auf eine verteilte Portgruppe. b Wählen Sie auf der Registerkarte **Ports** einen Port aus und klicken Sie auf das Symbol **Einstellungen des verteilten Ports bearbeiten**. c Wählen Sie **VLAN**. d Wählen Sie neben den außer Kraft zu setzenden Eigenschaften **Außer Kraft setzen** aus.

3 Wählen Sie im Dropdown-Menü **VLAN-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. Beispiel: `1702-1705, 1848-1849`. 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 verwerfen 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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene.

Verfahren

1 Wechseln Sie im vSphere Web Client zu einem Distributed Switch.

2 Klicken Sie auf der Registerkarte **Netzwerke** auf **Uplink-Portgruppen**.

3 Navigieren Sie zur VLAN-Richtlinie für die Uplink-Portgruppe oder den Port.

Option	Aktion
Uplink-Portgruppe	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	a Doppelklicken Sie auf eine Uplink-Portgruppe. b Wählen Sie in der Registerkarte **Ports** einen Port aus und klicken Sie auf die Registerkarte **Einstellungen des verteilten Ports bearbeiten**. c 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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
3. Navigieren Sie zur Sicherheitsrichtlinie für den Standard-Switch oder die 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 **Sicherheit** 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 **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	■ **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. **Hinweis** Der Promiscuous-Modus ist ein unsicherer Betriebsmodus. Firewalls, Portscanner und Erkennungssysteme für Eindringversuche müssen im Promiscuous-Modus ausgeführt werden.
MAC-Adressänderungen	■ **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 `.vmx`-Konfigurationsdatei), unterbindet der Switch alle eingehenden Frames zum Adapter. Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine wieder zur MAC-Adresse des VM-Netzwerkadapters ändert, empfängt die virtuelle Maschine wieder Frames. ■ **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	■ **Ablehnen**. Der Switch verwirft alle ausgehenden Frames von einem Adapter einer virtuellen Maschine 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.

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. Weitere Informationen hierzu finden Sie unter 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	a Wählen Sie im Menü **Aktionen** die Option **Verteilte Portgruppe > Verteilte Portgruppen verwalten** aus. b Wählen Sie **Sicherheit** aus. c Wählen Sie die Portgruppe aus und klicken Sie auf **Weiter**.
Verteilter Port	a Klicken Sie auf der Registerkarte **Netzwerke** auf **Verteilte Portgruppen** und doppelklicken Sie auf eine verteilte Portgruppe. b Wählen Sie auf der Registerkarte **Ports** einen Port aus und klicken Sie auf das Symbol **Einstellungen des verteilten Ports bearbeiten**. c Wählen Sie **Sicherheit** aus. d 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	■ **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. **Hinweis** Der Promiscuous-Modus ist ein unsicherer Betriebsmodus. Firewalls, Portscanner und Erkennungssysteme für Eindringversuche müssen im Promiscuous-Modus ausgeführt werden.
MAC-Adressänderungen	■ **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 `.vmx`-Konfigurationsdatei), unterbindet der Switch alle eingehenden Frames zum Adapter. Wenn das Gastbetriebssystem die effektive MAC-Adresse der virtuellen Maschine wieder zur MAC-Adresse des VM-Netzwerkadapters ändert, empfängt die virtuelle Maschine wieder Frames. ■ **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	■ **Ablehnen**. Der Switch verwirft alle ausgehenden Frames von einem Adapter einer virtuellen Maschine 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.

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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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. Weitere Informationen hierzu finden Sie unter 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	a Wählen Sie im Menü **Aktionen** die Option **Verteilte Portgruppe > Verteilte Portgruppen verwalten** aus. b Wählen Sie **Traffic-Shaping** aus. c Wählen Sie die Portgruppe aus und klicken Sie auf **Weiter**.
Verteilter Port	a Klicken Sie auf der Registerkarte **Netzwerke** auf **Verteilte Portgruppen** und doppelklicken Sie auf eine verteilte Portgruppe. b Wählen Sie auf der Registerkarte **Ports** einen Port aus und klicken Sie auf das Symbol **Einstellungen des verteilten Ports bearbeiten**. c Wählen Sie **Traffic-Shaping** aus. d 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/sendet 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. Weitere Informationen hierzu finden Sie unter Aktivieren von Network I/O Control auf einem vSphere Distributed Switch.
- Erstellen und konfigurieren Sie Netzwerkressourcenpools. Weitere Informationen hierzu finden Sie unter 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.

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. Weitere Informationen hierzu finden Sie unter 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	a Wählen Sie im Menü **Aktionen** die Option **Verteilte Portgruppe** > **Verteilte Portgruppen verwalten** aus. b Wählen Sie **Überwachen** aus. c Wählen Sie die Portgruppe aus und klicken Sie auf **Weiter**.
Verteilter Port	a Klicken Sie auf der Registerkarte **Netzwerke** auf **Verteilte Portgruppen** und doppelklicken Sie auf eine verteilte Portgruppe. b Wählen Sie auf der Registerkarte **Ports** einen Port aus und klicken Sie auf das Symbol **Einstellungen des verteilten Ports bearbeiten**. c Wählen Sie **Überwachen** aus. d Wählen Sie neben den außer Kraft zu setzenden Eigenschaften **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 einem vSphere Distributed Switch 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 **Netzwerke**.
   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 **Netzwerke**.
   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 das 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 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 **Netzwerke**.
   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 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 **Netzwerke**.
   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 Datenverkehrbezeichner-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 **Netzwerke**.
   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 **Netzwerke**.
   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 **Netzwerke**.
   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 **Netzwerke**.
   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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene.

Verfahren

1. Navigieren Sie zu einem Distributed Switch und anschließend zu einem verteiltem Port oder Uplink-Port.
   - Zum Navigieren zu den verteilten Ports des Switches klicken Sie auf **Netzwerke > Verteilte Portgruppen**, doppelklicken Sie auf eine verteilte Portgruppe in der Liste und klicken Sie anschließend auf die Registerkarte **Ports**.
   - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Netzwerke > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken auf die Registerkarte **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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene.

Verfahren

1. Navigieren Sie zu einem Distributed Switch und anschließend zu einem verteiltem Port oder Uplink-Port.
   - Zum Navigieren zu den verteilten Ports des Switches klicken Sie auf **Netzwerke > Verteilte Portgruppen**, doppelklicken Sie auf eine verteilte Portgruppe in der Liste und klicken Sie anschließend auf die Registerkarte **Ports**.
   - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Netzwerke > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken auf die Registerkarte **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 das 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 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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene.

Verfahren

1 Navigieren Sie zu einem Distributed Switch und anschließend zu einem verteiltem Port oder Uplink-Port.

   - Zum Navigieren zu den verteilten Ports des Switches klicken Sie auf **Netzwerke > Verteilte Portgruppen**, doppelklicken Sie auf eine verteilte Portgruppe in der Liste und klicken Sie anschließend auf die Registerkarte **Ports**.
   - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Netzwerke > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken auf die Registerkarte **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 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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene.

Verfahren

1. Navigieren Sie zu einem Distributed Switch und anschließend zu einem verteiltem Port oder Uplink-Port.
   - Zum Navigieren zu den verteilten Ports des Switches klicken Sie auf **Netzwerke > Verteilte Portgruppen**, doppelklicken Sie auf eine verteilte Portgruppe in der Liste und klicken Sie anschließend auf die Registerkarte **Ports**.
   - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Netzwerke > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken auf die Registerkarte **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 Datenverkehrbezeichner-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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene.

Verfahren

1 Navigieren Sie zu einem Distributed Switch und anschließend zu einem verteiltem Port oder Uplink-Port.

   - Zum Navigieren zu den verteilten Ports des Switches klicken Sie auf **Netzwerke > Verteilte Portgruppen**, doppelklicken Sie auf eine verteilte Portgruppe in der Liste und klicken Sie anschließend auf die Registerkarte **Ports**.
   - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Netzwerke > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken auf die Registerkarte **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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene.

Verfahren

1. Navigieren Sie zu einem Distributed Switch und anschließend zu einem verteiltem Port oder Uplink-Port.
   - Zum Navigieren zu den verteilten Ports des Switches klicken Sie auf **Netzwerke > Verteilte Portgruppen**, doppelklicken Sie auf eine verteilte Portgruppe in der Liste und klicken Sie anschließend auf die Registerkarte **Ports**.
   - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Netzwerke > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken auf die Registerkarte **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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene.

Verfahren

1 Navigieren Sie zu einem Distributed Switch und anschließend zu einem verteiltem Port oder Uplink-Port.

   - Zum Navigieren zu den verteilten Ports des Switches klicken Sie auf **Netzwerke > Verteilte Portgruppen**, doppelklicken Sie auf eine verteilte Portgruppe in der Liste und klicken Sie anschließend auf die Registerkarte **Ports**.
   - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Netzwerke > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken auf die Registerkarte **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. Weitere Informationen hierzu finden Sie unter Konfigurieren von überschreibenden Netzwerkrichtlinien auf Portebene.

Verfahren

1 Navigieren Sie zu einem Distributed Switch und anschließend zu einem verteiltem Port oder Uplink-Port.

   - Zum Navigieren zu den verteilten Ports des Switches klicken Sie auf **Netzwerke > Verteilte Portgruppen**, doppelklicken Sie auf eine verteilte Portgruppe in der Liste und klicken Sie anschließend auf die Registerkarte **Ports**.
   - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Netzwerke > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken auf die Registerkarte **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 (Sicherungsschicht) 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.
Überwachen	Aktivieren oder deaktivieren Sie NetFlow auf den ausgewählten Portgruppen.

Option	Beschreibung
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.
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	■ **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	■ **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 `.vmx`-Konfigurationsdatei angegeben ist, werden alle eingehenden Frames verworfen. Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der `.vmx`-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	■ **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).
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	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. ■ **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.
Netzwerkausfallerkennung	Wählen Sie die Verfahrensweise zur Verwendung der Failover-Erkennung aus. ■ **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	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 Netzwerklastausgleich (NLB) von Microsoft im Unicast-Modus verwenden. 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.

Option	Beschreibung
Failback	Wählen Sie **Ja** oder **Nein**, um die Failback-Funktion zu deaktivieren bzw. zu aktivieren. Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. ■ **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	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. ■ **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-Lastausgleich 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	■ **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	Legt fest, ob die Regel für eingehenden, ausgehenden oder ein- und ausgehenden Datenverkehr gilt. Die Datenverkehrsrichtung beeinflusst auch, wie Sie Datenverkehrsquelle und -Ziel identifizieren.
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	Qualifiziert den Datenverkehr für die Regel anhand des Layer 2-Headers. ■ **Protokolltyp**. Legt das Nächste-Schicht-Protokoll fest (IPv4, IPv6 usw.), das die Nutzlast verarbeitet. Dieses Attribut entspricht dem Feld „EtherType“ in Ethernet-Frames. Sie können ein Protokoll aus dem Dropdown-Menü auswählen oder seine Hexadezimalzahl eingeben. Um beispielsweise nach Datenverkehr für das LLDP-Protokoll (Link Layer Discovery Protocol) zu suchen, geben Sie **88CC** ein. ■ **VLAN-ID**. Sucht Datenverkehr anhand des VLAN. Der VLAN-ID-Bezeichner in einer verteilten Portgruppe funktioniert mit Virtual Guest Tagging (VGT). 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. ■ **Quelladresse**. Legt eine einzelne MAC-Adresse oder ein einzelnes MAC-Netzwerk zum Abgleichen von Paketen anhand der Quelladresse fest. 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. 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. ■ **Zieladresse**. 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	Qualifiziert den Datenverkehr für die Regel anhand des Layer 3-Headers. ■ **Protokoll**. Legt das Nächste-Schicht-Protokoll fest (TCP, UDP usw.), das die Nutzlast verarbeitet. Wählen Sie im Dropdown-Menü ein Protokoll aus oder geben Sie die entsprechende Dezimalzahl gemäß *RFC 1700, Assigned Numbers* ein. Beim TCP- und UDP-Protokoll können Sie auch den Quell- und Zielport festlegen. ■ **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
	■ **Quelladresse**. 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. ■ **Zieladresse**. 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 Objektnavigator 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 Distributed Switch und anschließend zu einem verteiltem Port oder Uplink-Port.
   - Zum Navigieren zu den verteilten Ports des Switches klicken Sie auf **Netzwerke > Verteilte Portgruppen**, doppelklicken Sie auf eine verteilte Portgruppe in der Liste und klicken Sie anschließend auf die Registerkarte **Ports**.
   - Zum Navigieren zu den Uplink-Ports einer Uplink-Portgruppe klicken Sie auf **Netzwerke > Uplink-Portgruppen**, doppelklicken Sie auf eine Uplink-Portgruppe in der Liste und klicken auf die Registerkarte **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**.

MAC Learning-Richtlinie

MAC Learning bietet Netzwerkkonnektivität zu Bereitstellungen, bei denen mehrere MAC-Adressen von einer vNIC verwendet werden.

Beispielsweise in einer geschachtelten Hypervisor-Bereitstellung, bei der eine ESXi-VM auf einem ESXi-Host ausgeführt wird und mehrere VMs innerhalb der ESXi VM ausgeführt werden. Ohne MAC Learning enthält sie, wenn die vNIC der ESXi-VM eine Verbindung mit einem Switch-Port herstellt, nur eine statische MAC-Adresse. VMs, die innerhalb der ESXi-VM ausgeführt werden, verfügen über keine Netzwerkkonnektivität, da ihre Pakete über unterschiedliche MAC-Quelladressen verfügen. Beim MAC Learning überprüft vSwitch die MAC-Quelladresse jedes von der vNIC kommenden Pakets, erlernt die MAC-Adresse und lässt die Weiterleitung des Pakets zu. Wird eine erlernte MAC-Adresse eine bestimmte Zeit lang nicht verwendet, wird sie entfernt.

MAC Learning unterstützt auch unbekanntes Unicast Flooding. Wenn ein Paket, das von einem Port empfangen wird, eine unbekannte MAC-Zieladresse aufweist, wird das Paket normalerweise verworfen. Bei aktiviertem Flooding des Datenverkehrs vom Typ „Unbekannter Unicast“ leitet der Port diesen Datenverkehr an jeden Port auf dem Switch weiter, für den MAC Learning und unbekanntes Unicast-Flooding aktiviert wurden. Diese Eigenschaft ist standardmäßig aktiviert, wenn MAC Learning aktiviert ist.

Die Anzahl erlernbarer MAC-Adressen ist konfigurierbar. Der Maximalwert beträgt 4096 pro Port. Dies ist die Standardeinstellung. Sie können auch die Richtlinie für den Fall festlegen, dass der Grenzwert erreicht wird. Folgende Optionen sind verfügbar:

- Verwerfen – Pakete von einer unbekannten MAC-Quelladresse werden verworfen. Pakete, die bei dieser MAC-Adresse eingehen, werden als unbekannte Unicast-Objekte behandelt. Der Port empfängt die Pakete nur dann, wenn unbekanntes Unicast-Flooding aktiviert ist.
- Zulassen – Pakete von einer unbekannten MAC-Quelladresse werden weitergeleitet, obwohl die Adresse nicht erlernt wird. Pakete, die bei dieser MAC-Adresse eingehen, werden als unbekannte Unicast-Objekte behandelt. Der Port empfängt die Pakete nur dann, wenn unbekanntes Unicast-Flooding aktiviert ist.

In vSphere 6.7 und höher kann MAC Learning auf einer verteilten virtuellen Portgruppe mithilfe der vSphere API aktiviert werden. Sie können die MAC Learning-Richtlinie auf vSphere Distributed Switch, der verteilten virtuellen Portgruppe und dem verteilten virtuellen Port konfigurieren. Wenn keine MAC Learning-Richtlinie für die verteilte virtuelle Portgruppe festgelegt ist, wird sie von vSphere Distributed Switch übernommen. Wenn sie auf dem DVport nicht aktiviert ist, wird sie von der verteilten virtuellen Portgruppe übernommen. Weitere Informationen finden Sie in der *vSphere Web Services-API-Referenz*.

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	■ 4095 für Standard-Switch ■ VLAN-Bereich und einzelne VLANs für verteilten Switch	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. 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. **Hinweis** Für VGT muss ein 802.1Q-VLAN-Trunking-Treiber auf dem Gastbetriebssystem der virtuellen Maschine installiert sein.

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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Einstellungen** und wählen Sie **Privates VLAN** aus.
3. 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. Weitere Informationen hierzu finden Sie unter 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. Erweitern Sie auf der Registerkarte **Konfigurieren** den Abschnitt **Einstellungen** und wählen Sie **Privates VLAN**.
3. 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 Erweitern Sie auf der Registerkarte **Konfigurieren** den Abschnitt **Einstellungen** und wählen Sie **Privates VLAN**.

3 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)
- RDMA für virtuelle Maschinen
- 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
- Hochverfügbarkeit
- DRS (eingeschränkte Verfügbarkeit. Die virtuelle Maschine kann Teil eines Clusters sein, kann aber nicht über Hosts hinweg migriert werden.)

- Snapshots
- 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 Netwzerkgerät 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 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 Netwzerkgerät 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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Hardware** und klicken Sie auf **PCI-Geräte**.
3. 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.

4. 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.
5. 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 Datencenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **VMs**.
   b. Klicken Sie auf **Virtuelle Maschinen** und doppelklicken Sie auf die virtuelle Maschine aus der Liste.
2. Schalten Sie die virtuelle Maschine aus.
3. Erweitern Sie auf der Registerkarte **Konfigurieren** der virtuellen Maschine **Einstellungen** und wählen Sie **VM-Hardware**.
4. Klicken Sie auf **Bearbeiten** und wählen Sie die Registerkarte **Virtuelle Hardware** in dem Dialogfeld aus, in dem die Einstellungen angezeigt werden.
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.

Single Root I/O Virtualization (SR-IOV)

vSphere unterstützt 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 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 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 zu verwenden, muss Ihre Umgebung verschiedene Konfigurationsanforderungen erfüllen:

Tabelle 10-1. Unterstützte Konfigurationen für die Verwendung von SR-IOV

Komponente	Anforderungen
Physischer Host	■ Muss mit der ESXi-Version kompatibel sein. ■ Muss über einen Intel- oder AMD-Prozessor verfügen. ■ 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	■ 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	■ 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	■ 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.

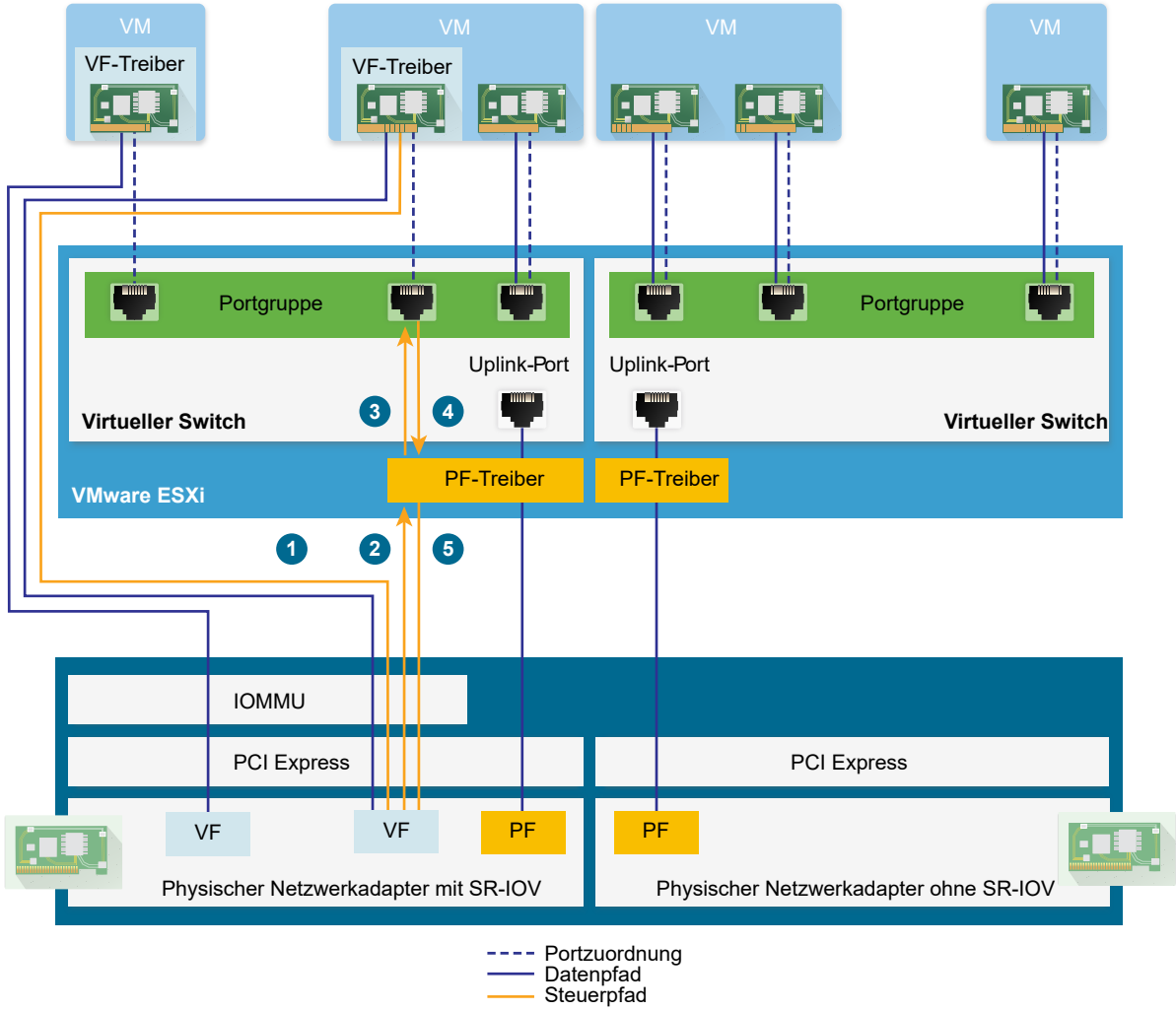
SR-IOV-Komponentenarchitektur und -Interaktion

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-Adaptern 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 instanziieren 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 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.
- 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 Netzwerkrichtlinien 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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.

   Der Wert 0 bedeutet, dass SR-IOV für diese physische Funktion nicht aktiviert ist.

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 Datencenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **VMs**.

   b Klicken Sie auf **Virtuelle Maschinen** und doppelklicken Sie auf die virtuelle Maschine aus der Liste.

2 Schalten Sie die virtuelle Maschine aus.

3 Erweitern Sie auf der Registerkarte **Konfigurieren** der virtuellen Maschine **Einstellungen** und wählen Sie **VM-Hardware**.

4 Klicken Sie auf **Bearbeiten** und wählen Sie die Registerkarte **Virtuelle Hardware** in dem Dialogfeld aus, in dem die Einstellungen angezeigt werden.

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 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	■ Wenn das Gastbetriebssystem die anfänglich festgelegte MAC-Adresse eines Netzwerkadapters 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 Netzwerkadapter 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 können die physischen Funktionen (PF) 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. Ein SR-IOV-fähiger physischer Adapter im gemischten Modus wird mit dem 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“ und wird mit dem Symbol  angezeigt.

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 *Installation und Einrichtung von vCenter Server*.

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 des vSphere Web Client auf **Hostprofile**.
2. Wählen Sie das Hostprofil aus der Liste aus und klicken Sie auf die Registerkarte **Konfigurieren**.
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, legen Sie den Wert auf `x,y` fest, 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-Netzwerkadaptertyp einer virtuellen Maschine zu. Weitere Informationen hierzu finden Sie unter 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 virtuelle 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.

RDMA für virtuelle Maschinen

vSphere 6.5 und höher unterstützt die Kommunikation über RDMA (Remote Direct Memory Access, Remote-Direktzugriff auf den Speicher) zwischen virtuellen Maschinen mit paravirtualisiertem RDMA (PVRDMA) Netzwerkadapter.

Übersicht über RDMA

RDMA ermöglicht ohne Hinzuziehung des Betriebssystems oder der CPU den direkten Zugriff auf den Speicher eines Computers vom Speicher eines anderen Computers aus. Die Übertragung des Speichers wird auf den RDMA-fähigen Hostkanaladapter (HCA) ausgelagert. Ein PVRDMA-Netzwerkadapter bietet den Remote-Direktzugriff auf den Speicher in einer virtuellen Umgebung.

Verwenden von PVRDMA in vSphere

In vSphere kann eine virtuelle Maschine einen PVRDMA-Netzwerkadapter zum Kommunizieren mit anderen virtuellen Maschinen mit PVRDMA-Geräten verwenden. Die virtuellen Maschinen müssen mit demselben vSphere Distributed Switch verbunden sein.

Das PVRDMA-Gerät wählt automatisch die Kommunikationsmethode zwischen den virtuellen Maschinen. Bei virtuellen Maschinen, die auf demselben ESXi-Host mit oder ohne physisches RDMA-Gerät ausgeführt werden, handelt es sich bei der Datenübertragung zwischen den beiden virtuellen Maschinen um die Ausführung der memcpy-Funktion. In diesem Fall wird die physische RDMA-Hardware nicht verwendet.

Bei virtuellen Maschinen, die sich auf unterschiedlichen ESXi-Hosts mit einer physischen RDMA-Verbindung befinden, müssen die physischen RDMA-Geräte Uplinks auf dem Distributed Switch sein. In diesem Fall werden für die Kommunikation zwischen den virtuellen Maschinen über PVRDMA die zugrunde liegenden physischen RDMA-Geräte verwendet.

Bei zwei virtuellen Maschinen, die auf unterschiedlichen ESXi-Hosts ausgeführt werden, wird für die Kommunikation ein TCP-basierter Kanal verwendet, was die Leistung beeinträchtigt, wenn mindestens einer der Hosts nicht über ein physisches RDMA-Gerät verfügt.

Unterstützung von PVRDMA

vSphere 6.5 und höher unterstützt PVRDMA nur in Umgebungen mit einer bestimmten Konfiguration.

Unterstützte Konfigurationen

Um PVRDMA unter vSphere 6.5 zu verwenden, muss Ihre Umgebung mehrere Konfigurationsanforderungen erfüllen:

Tabelle 10-3. Unterstützte Konfigurationen für die Verwendung von PVRDMA

Komponente	Anforderungen
vSphere	■ ESXi-Host 6.5 oder höher. ■ vCenter Server oder vCenter Server Appliance 6.5 oder höher. ■ vSphere Distributed Switch
Physischer Host	■ Muss mit der ESXi-Version kompatibel sein.
Hostkanaladapter (HCA)	■ Muss mit der ESXi-Version kompatibel sein. **Hinweis** Für virtuelle Maschinen, die sich auf verschiedenen ESXi-Hosts befinden, ist ein Hostkanaladapter (HCA) für die Verwendung von RDMA erforderlich. Sie müssen den Hostkanaladapter als Uplink für den vSphere Distributed Switch zuweisen. PVRDMA unterstützt die NIC-Gruppierung nicht. Der Hostkanaladapter muss der einzige Uplink auf dem vSphere Distributed Switch sein. Für virtuelle Maschinen auf denselben ESXi-Hosts oder virtuellen Maschinen mit TCP-basiertem Fallback ist der Hostkanaladapter nicht erforderlich.
Virtuelle Maschine	■ Virtuelle Hardwareversion 13 oder höher.
Gastbetriebssystem	■ Linux (64-Bit)

Informationen über das Verifizieren der Kompatibilität der physischen Hosts und Hostkanaladapter mit ESXi-Versionen finden Sie im *VMware-Kompatibilitätshandbuch*.

Hinweis Versuche, in vSphere Web Client nicht unterstützte Funktionen mit PVRDMA zu aktivieren oder zu konfigurieren, führen möglicherweise zu unerwartetem Verhalten in Ihrer Umgebung.

Konfigurieren eines ESXi-Hosts für PVRDMA

Konfigurieren Sie den VMkernel-Adapter und die Firewallregel eines ESXi-Hosts für die PVRDMA-Kommunikation.

Voraussetzungen

Vergewissern Sie sich, dass der ESXi-Host die Anforderungen für PVRDMA erfüllt. Weitere Informationen hierzu finden Sie unter Unterstützung von PVRDMA.

- Kennzeichnen eines VMkernel-Adapters für PVRDMA

  Wählen Sie einen VMkernel-Adapter aus und aktivieren Sie für ihn die PVRDMA-Kommunikation.

- Aktivieren der Firewall-Regel für PVRDMA

  Aktivieren Sie die Firewall-Regel für PVRDMA im Sicherheitsprofil des ESXi-Hosts.

Kennzeichnen eines VMkernel-Adapters für PVRDMA

Wählen Sie einen VMkernel-Adapter aus und aktivieren Sie für ihn die PVRDMA-Kommunikation.

Verfahren

1. Navigieren Sie im vSphere Web Client zum Host.
2. Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.
3. Klicken Sie auf **Erweiterte Systemeinstellungen**.
4. Suchen Sie nach `Net.PVRDMAVmknic` und klicken Sie auf **Bearbeiten**.
5. Geben Sie die Bezeichnung des VMkernel-Adapters ein, den Sie verwenden möchten, z. B. vmk0, und klicken Sie auf **OK**.

Aktivieren der Firewall-Regel für PVRDMA

Aktivieren Sie die Firewall-Regel für PVRDMA im Sicherheitsprofil des ESXi-Hosts.

Verfahren

1. Navigieren Sie im vSphere Web Client zum Host.
2. Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.
3. Klicken Sie auf **Sicherheitsprofil**.
4. Klicken Sie im Abschnitt „Firewall“ auf **Bearbeiten**.
5. Führen Sie einen Bildlauf zur PVRDMA-Regel durch und aktivieren Sie das entsprechende Kontrollkästchen.
6. Klicken Sie auf **OK**.

Zuweisen eines PVRDMA Adapters zu einer virtuellen Maschine

Um eine virtuelle Maschine für den Austausch von Daten unter Verwendung von RDMA zu aktivieren, müssen Sie die virtuelle Maschine mit einem PVRDMA-Netzwerkadapter verknüpfen.

Voraussetzungen

- Stellen Sie sicher, dass der Host, auf dem die virtuelle Maschine ausgeführt wird, für RDMA konfiguriert ist. Weitere Informationen hierzu finden Sie unter Konfigurieren eines ESXi-Hosts für PVRDMA.
- Überprüfen Sie, ob der Host mit einem vSphere Distributed Switch verbunden ist
- Stellen Sie sicher, dass die virtuelle Maschine die virtuelle Hardwareversion 13 verwendet.
- Vergewissern Sie sich, dass es sich bei dem Gastbetriebssystem um eine Linux 64-Bit-Verteilung handelt.

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 **VMs**.
   b. Klicken Sie auf **Virtuelle Maschinen** und doppelklicken Sie auf die virtuelle Maschine aus der Liste.
2. Schalten Sie die virtuelle Maschine aus.
3. Erweitern Sie auf der Registerkarte **Konfigurieren** der virtuellen Maschine **Einstellungen** und wählen Sie **VM-Hardware**.
4. Klicken Sie auf **Bearbeiten** und wählen Sie die Registerkarte **Virtuelle Hardware** in dem Dialogfeld aus, in dem die Einstellungen angezeigt werden.
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 verteilten Portgruppe.
7. Wählen Sie im Dropdown-Menü **Adaptertyp** die Option „PVRDMA“.
8. Erweitern Sie den Bereich **Arbeitsspeicher**, wählen Sie **Gesamten Gastarbeitsspeicher reservieren (Alle gesperrt)** und klicken Sie auf **OK**.
9. Schalten Sie die virtuelle Maschine ein.

Netzwerkanforderungen für RDMA over Converged Ethernet

RDMA over Converged Ethernet gewährleistet eine leichte RDMA-Kommunikation mit geringer Latenz und hohem Durchsatz über ein Ethernet-Netzwerk. RoCE benötigt ein für einen verlustfreien Datenverkehr auf Schicht 2 oder auf Schicht 2 und 3 konfiguriertes Netzwerk.

RDMA over Converged Ethernet (RoCE) ist ein Netzwerkprotokoll, das RDMA für eine schnellere Datenübertragung netzwerkintensiver Anwendungen verwendet. RoCE ermöglicht eine direkte Speicherübertragung zwischen Hosts, ohne dass die CPUs der Hosts dabei belastet werden.

Vom RoCE-Protokoll gibt es zwei Versionen: RoCE v1 arbeitet auf der Link-Netzwerkschicht (Schicht 2). RoCE v2 arbeitet auf der Internet-Netzwerkschicht (Schicht 3). Sowohl für RoCE v1 als auch für RoCE v2 ist eine verlustfreie Netzwerkkonfiguration erforderlich. Für RoCE v1 ist ein verlustfreies Netzwerk auf Schicht 2 erforderlich und für RoCE v2 müssen sowohl Schicht 2 als auch Schicht 3 für den verlustfreien Betrieb konfiguriert sein.

Verlustfreies Netzwerk auf Schicht 2

Zur Gewährleistung einer verlustfreien Umgebung auf Schicht 2 müssen Sie in der Lage sein, den Datenverkehr zu steuern. Die Flusssteuerung wird durch Aktivieren einer globalen Pause im gesamten Netzwerk oder durch Verwenden des von der Data Center Bridging-Gruppe (DCB) definierten Priority Flow Control (PFC)-Protokolls erreicht. PFC ist ein Protokoll der Schicht 2, das das Class of Services-Feld des VLAN-Tags 802.1Q verwendet, um einzelne Verkehrsprioritäten festzulegen. Es unterbricht die Übertragung von Paketen zu einem Empfänger entsprechend den einzelnen Class of Service-Prioritäten. Auf diese Weise erfolgt auf einem einzigen Link sowohl verlustfreier RoCE-Verkehr als auch verlustbehafteter Mindestverkehr. Wichtiger verlustbehafteter Verkehr kann jedoch im Falle eines Staus des Verkehrsflusses beeinträchtigt werden. Um unterschiedliche Flüsse voneinander zu isolieren, verwenden Sie RoCE in einem VLAN, in dem PFC als Priorität aktiviert ist.

Verlustfreies Netzwerk auf Schicht 3

Für RoCE v2 muss die verlustfreie Datenübertragung auf Routing-Geräten der Schicht 3 erhalten bleiben. Um die Übertragung von verlustfreien PFC-Prioritäten der Schicht 2 über Router der Schicht 3 zu aktivieren, konfigurieren Sie den Router so, dass die empfangene Prioritätseinstellung eines Pakets der entsprechenden Differentiated Serviced Code Point (DSCP)-QoS-Einstellung zugeordnet wird, die auf Schicht 3 arbeitet. Die übertragenen RDMA-Pakete werden mit DSCP der Schicht 3, Priority Code Points (PCP) der Schicht 2 oder beiden markiert. Router verwenden DSCP oder PCP zum Extrahieren von Prioritätsinformationen aus dem Paket. Bei Verwendung von PCP muss das Paket mit VLAN gekennzeichnet sein und der Router muss die PCP-Bits des Tags kopieren und an das nächste Netzwerk weiterleiten. Wenn das Paket mit DSCP markiert ist, muss der Router die DSCP-Bits unverändert beibehalten.

Wie RoCE v1 muss auch RoCE v2 auf einem VLAN, in dem PFC als Priorität aktiviert ist, ausgeführt werden.

Hinweis Gruppieren Sie keine RoCE-Netzwerkkarten, wenn Sie beabsichtigen, RDMA auf diesen Netzwerkkarten zu verwenden.

Anbieterspezifische Konfigurationsinformationen finden Sie in der offiziellen Dokumentation des jeweiligen Geräte- oder Switch-Anbieters.

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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **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 Datencenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **VMs**.

b Klicken Sie auf **Virtuelle Maschinen** und doppelklicken Sie auf die virtuelle Maschine aus der Liste.

2 Erweitern Sie auf der Registerkarte **Konfigurieren** der virtuellen Maschine **Einstellungen** und wählen Sie **VM-Hardware**.

3 Klicken Sie auf **Bearbeiten** und wählen Sie die Registerkarte **Virtuelle Hardware** in dem Dialogfeld aus, in dem die Einstellungen angezeigt werden.

4 Erweitern Sie den Bereich **Netzwerkadapter**. Notieren Sie sich die Netzwerkeinstellungen und die MAC-Adresse des Netzwerkadapters.

5 Klicken Sie auf **Entfernen**, 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 physichen 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 vmnicXesxcli network nic software set
    --ipv6tso=1 -n vmnicX
    ```

  - Deaktivieren Sie die Softwaresimulation von TSO im VMkernel.

    ```
    esxcli network nic software set --ipv4tso=0 -n vmnicXesxcli network nic software set
    --ipv6tso=0 -n vmnicX
    ```

  Wobei *X* in vmnic*X* 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 folgenden Konsolenbefehl 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 Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.

3 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 Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.

3 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

- Überprüfen Sie, ob ESXi 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 VXMNET3-Netzwerkadaptern aktiviert. Aus Leistungsgründen können Sie TSO deaktivieren.

Voraussetzungen

- Überprüfen Sie, ob ESXi 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-Adaptern 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 VXMNET3-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 Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.

3 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-Adaptern die Netzwerkleistung von virtuellen Maschinen.

vSphere unterstützt Software-LRO für IPv4- und IPv6-Pakete.

Voraussetzungen

Verfahren

1. Navigieren Sie im vSphere Web Client zum Host.
2. Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.
3. 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. Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.
3. 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. Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.
3. 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. Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.
3. 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. Erweitern Sie auf der Registerkarte **KonfigurierenSystem**.

3 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.

Der NetQueue-Lastausgleichsdienst in ESXi verwendet Lastausgleichsalgorithmen zur effektiven Nutzung von Rx-Warteschlangen in den physischen NICs durch die Verwaltung von vNIC- und VMkernel-Adapterfiltern.

Sie haben die Möglichkeit, verschiedene Typen von Rx-Warteschlangen zu aktivieren oder zu deaktivieren. Weitere Informationen finden Sie unter dem Befehl `esxcli network nic queue loadbalancer set` in der *Referenz zur vSphere Command-Line Interface*-Dokumentation.

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.
- 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

  Sie können Network I/O Control so konfigurieren, dass eine bestimmte Bandbreitenkapazität für Datenverkehr zugeteilt wird, der von vSphere Fault Tolerance, 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.

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 Konstruke 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. Weitere Informationen hierzu finden Sie unter Zugangssteuerung für Bandbreite virtueller Maschinen.

Verfügbarkeit von Funktionen

SR-IOV ist für virtuelle Maschinen, die für Network I/O Control Version 3 konfiguriert sind, nicht verfügbar.

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.

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. Weitere Informationen hierzu finden Sie unter Info zu vSphere Network I/O Control Version 3.

Bandbreitenzuteilung für Systemdatenverkehr

Sie können Network I/O Control so konfigurieren, dass eine bestimmte Bandbreitenkapazität für Datenverkehr zugeteilt wird, der von vSphere Fault Tolerance, 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 Hauptfunktionen in vSphere konfigurieren:

- Management
- Fault Tolerance
- NFS
- vSAN
- 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, NFS-Speicher, vSphere vMotion, vSphere Fault Tolerance, vSAN 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 11-1. Zuteilungsparameter für Systemdatenverkehr

Bandbreitenzuteilungsparameter	Beschreibung
Anteile	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. 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.
Reservierung	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. 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.
Grenzwert	Die maximale Bandbreite in MBit/s oder GBit/s, die ein Systemdatenverkehrstyp für einen einzelnen physischen Adapter nutzen kann.

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 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.

Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr

Weisen Sie Bandbreite für Hostverwaltung, virtuelle Maschinen, NFS-Speicher, vSphere vMotion, vSphere Fault Tolerance, vSAN 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. Weitere Informationen hierzu finden Sie unter Aktivieren von Network I/O Control auf einem vSphere Distributed Switch.

Verfahren

1. Navigieren Sie im vSphere Web Client zum Distributed Switch.
2. Erweitern Sie auf der Registerkarte **KonfigurierenRessourcenzuteilung**.
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

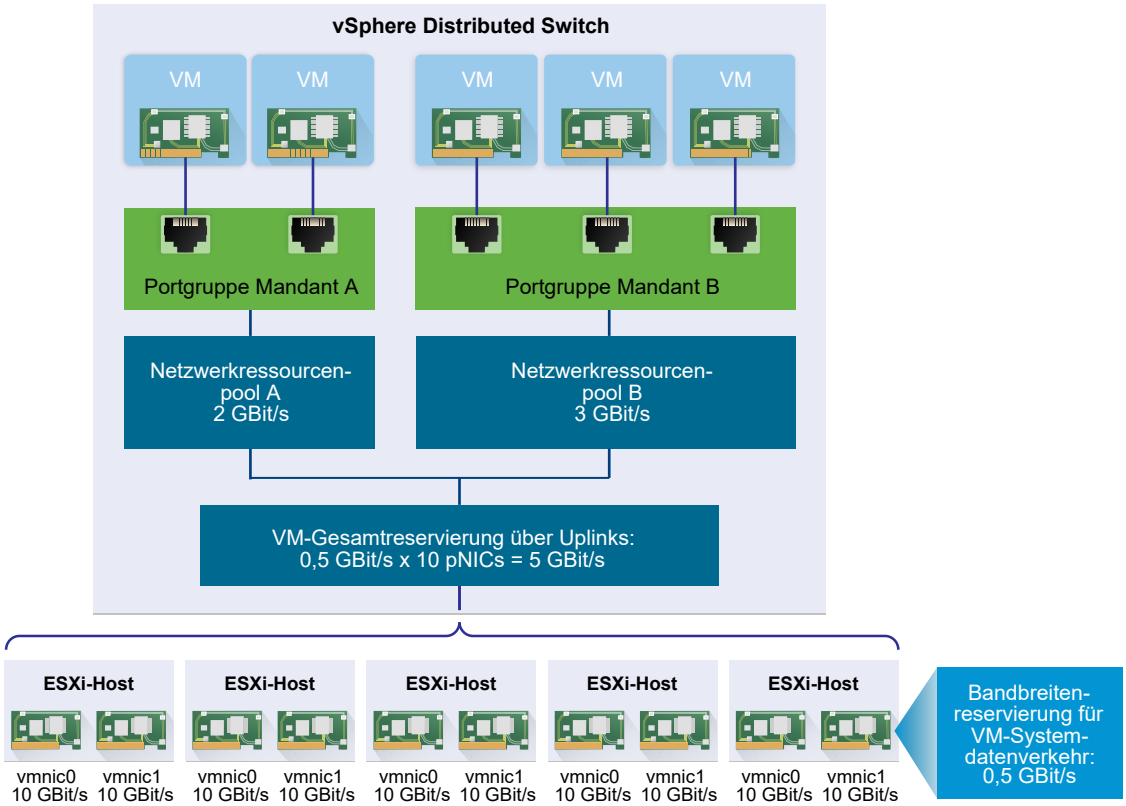
Ein Netzwerkressourcenpool stellt einen Teil der aggregierten Bandbreite dar, die für den Systemdatenverkehr der virtuellen Maschine auf allen physischen Adaptern, die mit dem Distributed Switch verbunden sind, reseriviert ist.

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 11-1. 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.

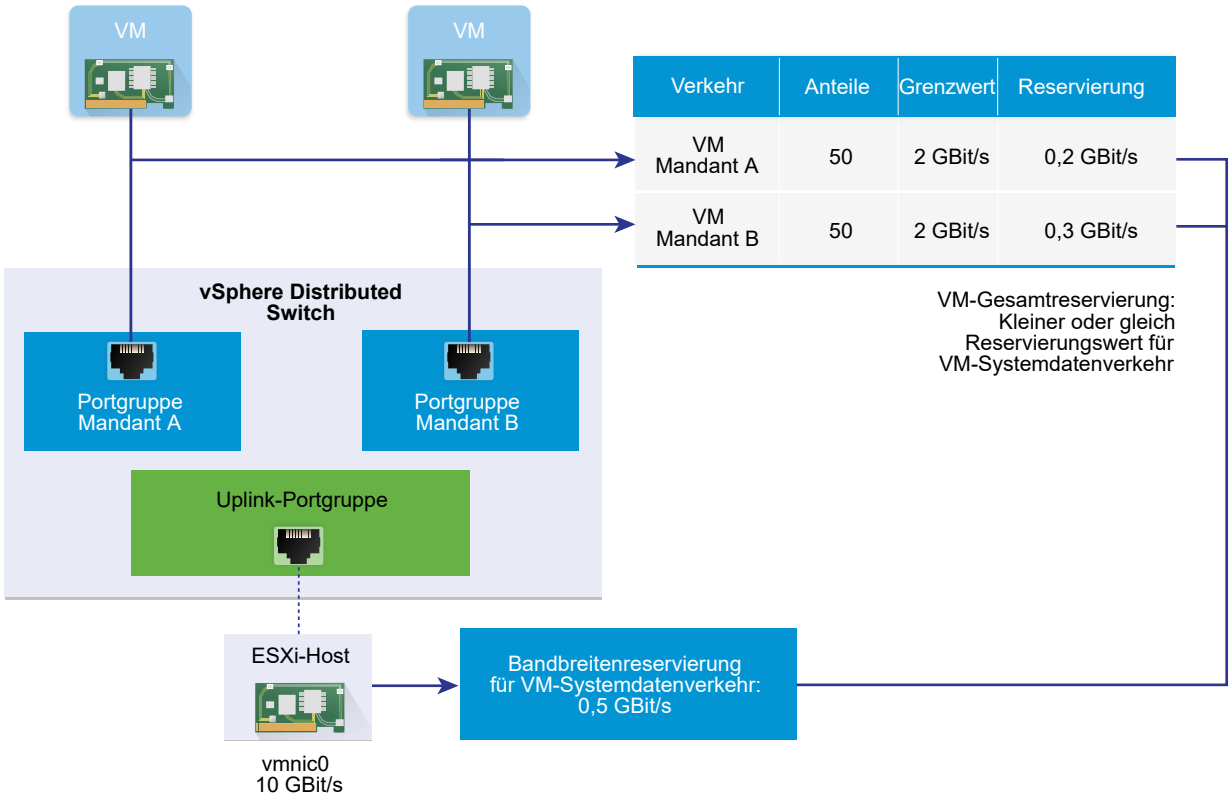
Bandbreitenbereitstellung an eine virtuelle Maschine auf dem Host

Um die Bandbreite zu garantieren, implementiert Network I/O Control eine Engine für die Datenverkehrplatzierung, 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 11-2. 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 11-2. Bandbreitenzuteilungsparameter für einem 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. Weitere Informationen hierzu finden Sie unter Aktivieren von Network I/O Control auf einem vSphere Distributed Switch.
- Überprüfen Sie, ob für den Systemdatenverkehr auf virtuellen Maschinen eine Bandbreitenreservierung konfiguriert ist. Weitere Informationen hierzu finden Sie unter Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr.

Verfahren

1. Navigieren Sie im vSphere Web Client zum Distributed Switch.
2. Erweitern Sie auf der Registerkarte **KonfigurierenRessourcenzuteilung**.
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. Weitere Informationen hierzu finden Sie unter 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. Weitere Informationen hierzu finden Sie unter Info zu vSphere Network I/O Control Version 3.

Voraussetzungen

- Überprüfen Sie, ob Network I/O Control aktiviert ist. Weitere Informationen hierzu finden Sie unter 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 **Netzwerke**.
   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. Weitere Informationen hierzu finden Sie unter Aktivieren von Network I/O Control auf einem vSphere Distributed Switch.
- Überprüfen Sie, ob für den Systemdatenverkehr auf virtuellen Maschinen eine Bandbreitenreservierung konfiguriert ist. Weitere Informationen hierzu finden Sie unter Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr.

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 **VMs**.

   b Klicken Sie auf **Virtuelle Maschinen** und doppelklicken Sie auf die virtuelle Maschine aus der Liste.

2 Erweitern Sie auf der Registerkarte **Konfigurieren** der virtuellen Maschine **Einstellungen** und wählen Sie **VM-Hardware**.

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. Weitere Informationen hierzu finden Sie unter Aktivieren von Network I/O Control auf einem vSphere Distributed Switch.
- Überprüfen Sie, ob für den Systemdatenverkehr auf virtuellen Maschinen eine Bandbreitenreservierung konfiguriert ist. Weitere Informationen hierzu finden Sie unter 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 Erweitern Sie auf der Registerkarte **KonfigurierenRessourcenzuteilung**.

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. Weitere Informationen hierzu finden Sie unter Aktivieren von Network I/O Control auf einem vSphere Distributed Switch.
- Überprüfen Sie, ob für den Systemdatenverkehr auf virtuellen Maschinen eine Bandbreitenreservierung konfiguriert ist. Weitere Informationen hierzu finden Sie unter Konfigurieren der Bandbreitenzuteilung für Systemdatenverkehr.

Verfahren

1 Navigieren Sie im vSphere Web Client zum Distributed Switch.

2 Erweitern Sie auf der Registerkarte **KonfigurierenRessourcenzuteilung**.

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 **Netzwerke**.

   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 Erweitern Sie auf der Registerkarte **KonfigurierenRessourcenzuteilung**.

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 Erweitern Sie auf der Registerkarte **KonfigurierenEinstellungen** und wählen Sie **Erweiterte Systemeinstellungen** aus.

3 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`**

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

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 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 `vpxd.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 + 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

Sie können die 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 hoch 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

Sie können 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 angeben, und vCenter Server verfolgt die Anzahl der verwendeten Adressen für jeden Bereich. vCenter Server weist MAC-Adressen aus dem ersten Bereich zu, für den noch Adressen verfügbar sind. vCenter Server prüft auf MAC-Adressenkonflikte innerhalb der zugehörigen Bereiche.

Bei Verwendung der bereichsbasierten Zuteilung müssen Sie verschiedene Instanzen von vCenter Server mit Bereichen bereitstellen, die sich nicht überlappen. vCenter Server erkennt keine Bereiche, die möglicherweise mit anderen vCenter Server-Instanzen in Konflikt stehen. Weitere Informationen zum Beheben von Problemen mit doppelten MAC-Adressen finden Sie in der *vSphere-Fehlerbehebung*-Dokumentation.

Hinweis Die Einstellungen für die bereichsbasierte MAC-Adresszuteilung gehen verloren, wenn Sie ein Upgrade auf eine neue Version von vCenter Server durchführen. Sie müssen die Einstellungen für die bereichsbasierte MAC-Adresszuteilung nach dem Upgrade manuell neu erstellen.

Zuweisen von MAC-Adressen

Verwenden Sie den vSphere Web Client, um präfixbasierte oder bereichsbasierte MAC-Adressenzuteilung zu aktivieren und die Zuteilungsparameter anzupassen.

Verwenden Sie den vSphere Web Client zum Wechseln des Zuteilungstyps, z. B. von der VMware OUI-Zuteilung zur bereichsbasierten Zuteilung. Ist jedoch ein Schema präfixbasiert oder bereichsbasiert und Sie möchten zu einem anderen Zuteilungsschema wechseln, müssen Sie die Datei `vpxd.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 `vpxd.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.

Verfahren

1. Navigieren Sie im vSphere Web Client zu einer vCenter Server-Instanz.
2. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Einstellungen** und wählen Sie **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
`config.vpxd.macAllocScheme.prefixScheme.prefix`	005026
`config.vpxd.macAllocScheme.prefixScheme.prefixLength`	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
`config.vpxd.macAllocScheme.rangeScheme.range[X].begin`	005067000000
`config.vpxd.macAllocScheme.rangeScheme.range[X].end`	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 Datei `vpxd.cfg` 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

```
<vpxd>
   <macAllocScheme>
      <VMwareOUI>true</VMwareOUI>
   </macAllocScheme>
</vpxd>
```

- Präfixbasierte Zuteilung

```
 <vpxd>
    <macAllocScheme>
      <prefixScheme>
         <prefix>005026</prefix>
```

```
         <prefixLength>23</prefixLength>
      </prefixScheme>
   </macAllocScheme>
</vpxd>
```

- Bereichsbasierte Zuteilung

```
<vpxd>
   <macAllocScheme>
       <rangeScheme>
          <range id="0">
             <begin>005067000001</begin>
             <end>005067000001</end>
          </range>
       </rangeScheme>
   </macAllocScheme>
</vpxd>
```

4 Speichern Sie die Datei `vpxd.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-Adaptern 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 **VMs**.
   b. Klicken Sie auf **Virtuelle Maschinen** und doppelklicken Sie auf die virtuelle Maschine aus der Liste.
2. Schalten Sie die virtuelle Maschine aus.
3. Erweitern Sie auf der Registerkarte **Konfigurieren** der virtuellen Maschine **Einstellungen** und wählen Sie **VM-Hardware**.
4. Klicken Sie auf **Bearbeiten** und wählen Sie die Registerkarte **Virtuelle Hardware** in dem Dialogfeld aus, in dem die Einstellungen angezeigt werden.
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 Datencenter, einen Ordner, einen Cluster, einen Ressourcenpool oder einen Host aus und klicken Sie auf die Registerkarte **VMs**.

   b Klicken Sie auf **Virtuelle Maschinen** und doppelklicken Sie auf die virtuelle Maschine aus der Liste.

2 Schalten Sie die virtuelle Maschine aus.

3 Erweitern Sie auf der Registerkarte **Konfigurieren** der virtuellen Maschine **Einstellungen** und wählen Sie **VM-Optionen**.

4 Klicken Sie auf **Bearbeiten** und erweitern Sie im Dialogfeld, in dem die Einstellungen angezeigt werden, auf der Registerkarte **VM-OptionenErweitert**.

5 Klicken Sie auf **Konfiguration bearbeiten**.

6 Um eine statische MAC-Adresse zuzuweisen, müssen Sie die Parameter nach Bedarf hinzufügen oder bearbeiten.

Parameter	Wert
`ethernet`*X*`.addressType`	**`statisch`**
`ethernet`*X*`.address`	*MAC_address_of_the_virtual_NIC*

   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	■ Statisch ■ Automatisch: AUTOCONF/ DHCPv6
vCenter Server-Maschine zu ESXi	Ja	■ Statisch ■ Automatisch: AUTOCONF/ DHCPv6
vCenter Server-Maschine zu vSphere Web Client-Maschine	Ja	■ Statisch ■ Automatisch: AUTOCONF/ DHCPv6
ESXi- zu vSphere Client-Maschine	Ja	■ Statisch ■ Automatisch: AUTOCONF/ DHCPv6
Virtuelle Maschine zu virtueller Maschine	Ja	■ Statisch ■ Automatisch: AUTOCONF/ DHCPv6
ESXi zu iSCSI-Speicher	Ja	■ Statisch ■ Automatisch: AUTOCONF/ DHCPv6
ESXi zu NFS-Speicher	Ja	■ Statisch ■ Automatisch: AUTOCONF/ 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:

- vSphere DPM über Intelligent Platform Management Interface (IPMI) und Hewlett-Packard Integrated Lights-Out (iLO). vSphere 6.5 unterstützt nur Wake-On-LAN (WOL), um einen Host aus dem Standby-Modus zu reaktivieren.
- vSAN
- Authentication Proxy
- 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 Domänennamen (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 eine Greenfield-Bereitstellung von vSphere 6.5 in einem IPv6-Netzwerk vorhanden ist, 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 eine Greenfield-Bereitstellung von vSphere 6.5 in einem IPv6-Netzwerk vorhanden ist, 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 Domänennamen (FQDNs) auf dem DNS-Server zugewiesen sind.
- Überprüfen Sie, dass die Netzwerkinfrastruktur Pv6-Konnektivität für die ESXi-Hosts, vCenter Server und ggf. die externe Datenbank bereitstellt.
- Überprüfen Sie, ob Sie Version 6.5 von vCenter Server mit einem FQDN installiert haben, der einer IPv6-Adresse zugeordnet ist. Informationen finden Sie in der Dokumentation *Installation und Einrichtung von vCenter Server*.
- Überprüfen Sie, ob auf den Hosts ESXi 6.5 installiert ist. Informationen finden Sie in der Dokumentation *Installation und Einrichtung von vCenter Server*.

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 Pv6-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 Domänennamen (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 *Installation und Einrichtung von vCenter Server* und *vCenter Server-Upgrade*.
- Vergewissern Sie sich, dass für alle ESXi-Hosts ein Upgrade auf Version 6.x durchgeführt wurde. Informationen hierzu finden Sie in der *VMware ESXi-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	1 Öffnen Sie eine SSH-Verbindung und melden Sie sich beim ESXi-Host an.
	2 Legen Sie eine statische IPv6-Adresse für das Verwaltungsnetzwerk vmk0 fest, indem Sie den folgenden Befehl ausführen:
	`esxcli network ip interface ipv6 address add -I IPv6_address -i vmk0`
	3 Legen Sie das Standard-Gateway für das Verwaltungsnetzwerk vmk0 fest, indem Sie den folgenden Befehl ausführen:
	`esxcli network ip interface ipv6 set -i vmk0 -g default_gateway_IPv6_address`
	4 Fügen Sie einen DNS-Server hinzu, indem Sie den folgenden Befehl ausführen:
	`esxcli network ip dns server add -s DNS_server_IPv6_address`

Automatische Adresszuweisung mit DHCPv6	1 Öffnen Sie eine SSH-Verbindung und melden Sie sich beim ESXi-Host an.
	2 Aktivieren Sie DHCPv6 für das Verwaltungsnetzwerk vmk0, indem Sie den folgenden Befehl ausführen:
	`esxcli network ip interface ipv6 -i vmk0 -enable-dhcpv6 = true`
	3 Aktivieren Sie „IPv6-Router angekündigt“ für das Verwaltungsnetzwerk vmk0, indem Sie den folgenden Befehl ausführen:
	`esxcli network ip interface ipv6 set -i vmk0 -enable-router-adv =true`
	4 Fügen Sie einen DNS-Server hinzu oder verwenden Sie die durch DHCPv6 veröffentlichte DNS-Einstellung, indem Sie einen der folgenden Befehle ausführen:
	`esxcli network ip dns server add -s DNS_server_IPv6_address`
	`esxcli network ip interface ipv6 set -i vmk0 --peer-dns=true`

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 6.0 und neueren Versionen ist IPv6 standardmäßig aktiviert.

Verfahren

1 Navigieren Sie im vSphere Web Client zum Host.

2 Erweitern Sie auf der Registerkarte **KonfigurierenNetzwerk** und wählen Sie **Erweitert** aus.

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. Weitere Informationen hierzu finden Sie unter 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **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. Halten Sie auf der Hauptseite von vSphere Web Client den Mauszeiger über das Symbol **Startseite**, klicken Sie auf **Startseite** und wählen Sie **Systemkonfiguration** aus.
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. 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:

- Erfassung von Netzwerkpaketen unter Verwendung des PacketCapture-Dienstprogramms
- 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
- Anzeigen des Topologiediagramms eines NSX Virtual Distributed Switch

Erfassung von Netzwerkpaketen unter Verwendung des PacketCapture-Dienstprogramms

Verwenden Sie das PacketCapture-Dienstprogramm zum Diagnostizieren von Netzwerkproblemen wie langsamen Verbindungen, verlorenen Paketen und Konnektivitätsproblemen.

PacketCapture ist ein Lightweight-tcpdump-Dienstprogramm, das nur die Mindestmenge an Daten, die für die Diagnose des Netzwerkproblems erforderlich sind, erfasst und speichert. PacketCapture ist in den rhttpproxy-Dienst von ESXi und der vCenter Server Appliance integriert. Sie starten und beenden PacketCapture, indem Sie die XML-Konfigurationsdatei des rhttpproxy-Diensts bearbeiten.

Verfahren

1 Beginnen Sie mit dem Erfassen von Paketen.

a Öffnen Sie eine SSH-Verbindung und melden Sie sich beim ESXi-Host oder bei der vCenter Server Appliance an.

b Öffnen Sie die Datei `config.xml` zum Bearbeiten.

vSphere-Komponente	Dateispeicherort
ESXi	`/etc/vmware/rhttpproxy/config.xml`
vCenter Server Appliance	`/etc/vmware-rhttpproxy/config.xml`

c Nehmen Sie die folgenden Änderungen vor.

```
<config>
  <packetCapture>
    <enabled>true</enabled>
```

d (Optional) Konfigurieren Sie PacketCapture-Optionen.

Option und Standardwert	Beschreibung
`<validity>72</validity>`	Löschen Sie beim Start alle `pcap`- und `pcap.gz`-Dateien, die vor dem angegebenen Stundenzeitraum zuletzt bearbeitet wurden und nicht Teil des aktuellen Prozesses sind.
`<directory>/directory_path</directory>`	Das Verzeichnis, in dem `pcap`- und `pcap.gz`-Dateien gespeichert sind. Das Verzeichnis muss vorhanden sein und es muss der Zugriff darauf möglich sein.
`<maxDataInPcapFile>52428800</maxDataInPcapFile>`	Die Menge an erfassten Daten in Byte, die jede `pcap`- und `pcap.gz`-Datei speichern kann, bevor zur nächsten Datei gewechselt wird. Die Mindestgröße beträgt 5 MB für die vCenter Server Appliance und 2,5 MB für ESXi. **Hinweis** Das Speichern von 50 MB erfasster Daten in einer `pcap`-Datei erfordert eine `pcap`-Datei mit einer Größe von ca. 67,5 MB.
`<maxPcapFilesCount>5</maxPcapFilesCount>`	Die Anzahl von `pcap`- oder `pcap.gz`-Dateien für die Rotation. Die Mindestanzahl beträgt 2.

e Speichern und schließen Sie die Datei `config.xml`.

f Laden Sie die Datei `config.xml` neu, indem Sie den folgenden Befehl ausführen.

```
kill -SIGHUP `pidof rhttpproxy`
```

2 Beenden Sie das Erfassen von Paketen.

a Öffnen Sie eine SSH-Verbindung und melden Sie sich beim ESXi-Host oder bei der vCenter Server Appliance an.

b Öffnen Sie die Datei `config.xml` zum Bearbeiten.

c Nehmen Sie die folgenden Änderungen vor.

```
<config>
  <packetCapture>
    <enabled>false</enabled>
```

d Speichern und schließen Sie die Datei `config.xml`.

e Laden Sie die Datei `config.xml` neu, indem Sie den folgenden Befehl ausführen.

```
kill -SIGHUP `pidof rhttpproxy`
```

3 Sammeln Sie die erfassten Daten.

Die `pcap`- oder `pcap.gz`-Dateien werden in den folgenden Standardverzeichnissen gespeichert.

vSphere-Komponente	Dateispeicherort
ESXi	`/var/run/log`
vCenter Server Appliance	`/var/log/vmware/rhttpproxy`

Nächste Schritte

Kopieren Sie die Dateien `pcap` und `pcap.gz` in ein System, in dem ein Netzwerkanalysetool ausgeführt wird, wie z. B. Wireshark, und überprüfen Sie die Paketdetails.

Verwenden Sie vor dem Analysieren der Datei `pcap` und `pcap.gz`, die aus einem ESXi-Host erfasst wurden, das TraceWrangler-Dienstprogramm zum Korrigieren der Metadaten der Frame-Größen. Weitere Informationen finden Sie unter https://kb.vmware.com/kb/52843

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 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
switch_port_arguments	`--uplink vmnicX`	Erfasst Pakete im Zusammenhang mit einem physischen Adapter. Sie können die Optionen `--uplink` und `--capture` kombinieren, um Pakete an einer bestimmten Stelle auf dem Pfad zwischen dem physischen Adapter und dem virtuellen Switch zu überwachen. Weitere Informationen hierzu finden Sie unter Erfassen von Paketen, die beim physikalischen Adapter ankommen.
	`--vmk vmkX`	Erfasst Pakete im Zusammenhang mit einem VMKernel-Adapter. Sie können die Optionen `vmk` und `--capture` kombinieren, um Pakete an einer bestimmten Stelle auf dem Pfad zwischen dem VMkernel-Adapter und dem virtuellen Switch zu überwachen. Weitere Informationen hierzu finden Sie unter Erfassen von Paketen für einen VMkernel-Adapter.

Tabelle 14-1. Argumente von pktcap-uw zum Erfassen von Paketen (Fortsetzung)

Argumentengruppe	Argument	Beschreibung
	`--switchport {vmxnet3_port_ID | vmkernel_adapter_port_ID}`	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 `esxtop` anzeigen. Sie können die Optionen `switchport` und `capture` kombinieren, um Pakete an einer bestimmten Stelle auf dem Pfad zwischen dem VMXNET3- oder VMkernel-Adapter und dem virtuellen Switch zu überwachen. Weitere Informationen hierzu finden Sie unter Erfassen von Paketen für einen VMXNET3-VM-Adapter.
	`--lifID lif_ID`	Erfasst Pakete im Zusammenhang mit der logischen Schnittstelle eines verteilten Routers. Weitere Informationen hierzu finden Sie in der *VMware NSX*-Dokumentation.
capture_point_options	`--capture capture_point`	Erfasst Pakete an einer bestimmten Stelle im Netzwerk-Stack. Sie können z. B. Pakete unmittelbar nach deren Ankunft von einem physischen Adapter überwachen.

Tabelle 14-1. Argumente von pktcap-uw zum Erfassen von Paketen (Fortsetzung)

Argumentengruppe	Argument	Beschreibung
	`--dir {0|1|2}`	Erfasst Pakete entsprechend der Flussrichtung bezogen auf den virtuellen Switch. 0 steht für eingehenden Datenverkehr, 1 für ausgehenden Datenverkehr und 2 für bidirektionalen Datenverkehr. Standardmäßig erfasst das Dienstprogramm `pktcap-uw` Ingress-Datenverkehr. Verwenden Sie die Option `--dir` zusammen mit der Option `--uplink`, `--vmk` oder `--switchport`.
	`--stage {0|1}`	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 `--stage` zusammen mit der Option `--uplink`, `--vmk` , `--switchport` oder `--dvfilter`.
	`--dvfilter` *`filter_name`* `--capture PreDVFilter|PostDVFilter`	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.
	`-A | --availpoints`	Zeigt alle vom Dienstprogramm `pktcap-uw` unterstützten Erfassungspunkte an.
	Details zu den Erfassungspunkten des Dienstprogramms `pktcap-uw` finden Sie unter Erfassungspunkte des Dienstprogramms pktcap-uw.	
filter_ options	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.	
output_ control_ options	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_optionsoutput_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
Filteroptionen	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.
Ausgabesteuerungsoptionen	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
`{-o | --outfile} pcap_file`	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.
`-P | --ng`	Speichern Sie den Paketinhalt im PCAPNG-Dateiformat. Verwenden Sie diese Option in Verbindung mit der Option `-o` oder `--outfile`.
`--console`	Schreiben Sie Paketangaben und -inhalte in die Konsolenausgabe. Standardmäßig zeigt das Dienstprogramm `pktcap-uw` Paketinformationen in der Konsolenausgabe an.
`{-c | --count} number_of_packets`	Erfassen Sie die ersten *number_of_packets* Pakete.
`{-s | --snaplen} snapshot_length`	Erfassen Sie nur die ersten *snapshot_length* Bytes von jedem Paket. Ist der Datenverkehr auf dem Host stark, verwenden Sie diese Option, um die CPU- und Speicherauslastung zu verringern. Um die Größe von gespeicherten Inhalten zu beschränken, wählen Sie einen Wert größer als 24. Um das vollständige Paket zu speichern, setzen Sie diese Option auf 0.
`-h`	Zum Dienstprogramm `pktcap-uw` 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
`--srcmac mac_address`	Erfassen oder verfolgen Sie Pakete, die eine bestimmte MAC-Quelladresse haben. Trennen Sie die Oktette durch Doppelpunkte.
`--dstmac mac_address`	Erfassen oder verfolgen Sie Pakete, die eine bestimmte MAC-Zieladresse haben. Trennen Sie die Oktette durch Doppelpunkte.
`--mac mac_address`	Erfassen oder verfolgen Sie Pakete, die eine bestimmte MAC-Quell- oder Zieladresse haben. Trennen Sie die Oktette durch Doppelpunkte.
`--ethtype 0xEthertype`	Erfassen oder verfolgen Sie Pakete auf Schicht 2 entsprechend dem Nächste-Schicht-Protokoll, das die Nutzlast des Pakets verarbeitet. *EtherType* 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 **`--ethtype 0x88CC`** ein.
`--vlan VLAN_ID`	Erfassen oder verfolgen Sie Pakete, die zu einem VLAN gehören.
`--srcip IP_addess|IP_address/subnet_range`	Erfassen oder verfolgen Sie Pakete, die eine bestimmte IPv4-Quell- oder Subnetzadresse haben.
`--dstip IP_addess|IP_address/subnet_range`	Erfassen oder verfolgen Sie Pakete, die eine bestimmte IPv4-Ziel- oder Subnetzadresse haben.
`--ip IP_addess`	Erfassen oder verfolgen Sie Pakete, die eine bestimmte Quell- oder IPv4-Zieladresse haben.
`--proto 0xIP_protocol_number`	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 **`--proto 0x11`** ein.
`--srcport source_port`	Erfassen oder verfolgen Sie Pakete ihrem Quell-TCP-Port entsprechend.
`--dstport destination_port`	Erfassen oder verfolgen Sie Pakete ihrem Ziel-TCP-Port entsprechend.
`--tcpport TCP_port`	Erfassen oder verfolgen Sie Pakete ihrem Quell- oder Ziel-TCP-Port entsprechend.
`--vxlan VXLAN_ID`	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.

   - Erweitern Sie im vSphere Web Client auf der Registerkarte **Konfigurieren** für den Host die Option **Netzwerk** und wählen Sie **Physische Adapter** aus.
   - 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 physische Adapter wird als `vmnic`*X* dargestellt. *X* ist die Nummer, die ESXi dem physikalischen Adapterport zugeordnet hat.

2 Führen Sie in der ESXi Shell für den Host den Befehl `pktcap-uw` mit dem Argument `--uplink vmnic`*X* 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
   --uplink vmnicX [--capturecapture_point|--dir 0|1]  [filter_options]
[--outfilepcap_file_path [--ng]] [--countnumber_of_packets]
   ```

   Die Optionen des Befehls `pktcap-uw--uplink vmnic`*X* stehen in eckigen Klammern [] und die vertikalen Balken | stellen die alternativen Werte dar.

Wenn Sie den Befehl `pktcap-uw--uplink vmnicX` 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 Verwenden Sie die Option `--capture`, um Pakete an einem anderen Erfassungspunkt oder die Option `--dir` in einer anderen Richtung des Datenverkehrs zu überprüfen.

Befehlsoption pktcap-uw	Ziel
`--capture UplinkSnd`	Überwacht Pakete, unmittelbar bevor sie in den physikalischen Adapter eingehen.
`--capture UplinkRcv`	Überwacht Pakete, unmittelbar nachdem sie in die Netzwerkkarten des physikalischen Adapters eingehen.
`--dir 1`	Überwacht Pakete, die den virtuellen Switch verlassen.
`--dir 0`	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 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.

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

1. Finden Sie auf dem Host die Port-ID des Adapters der virtuellen Maschine mithilfe des Dienstprogramms `esxtop` heraus.
   a. Starten Sie das Dienstprogramm im ESXi Shell an den Host mithilfe von `esxtop`.
   b. Um zum Netzwerkfenster des Dienstprogramms zu wechseln, drücken Sie n.
   c. 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.
   d. Zum Verlassen von `esxtop` klicken Sie auf Q.
2. Führen Sie in der ESXi Shell den Befehl `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.
3. Führen Sie in der ESXi Shell 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
`--capture VnicTx`	Überwachen Sie Pakete, wenn Sie von der virtuellen Maschine an den Switch weitergegeben werden.
`--capture VnicRx`	Überwachen Sie Pakete, wenn sie in der virtuellen Maschine eingehen.
`--dir 1 --stage 0`	Überwacht Pakete, unmittelbar nachdem sie den virtuellen Switch verlassen.
`--dir 1`	Überwachen Sie Pakete, unmittelbar bevor sie in der virtuellen Maschine eingehen.
`--dir 0 --stage 1`	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.

   - Erweitern Sie im vSphere Web Client die Option **Netzwerk** auf der Registerkarte **Konfigurieren** des Hosts und wählen Sie **VMkernel-Adapter** aus.
   - 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 `vmk`*X* angezeigt, wobei *X* die Sequenznummer ist, die ESXi dem Adapter zugeteilt hat.

2 Führen Sie in der ESXi Shell für den Host den Befehl `pktcap-uw` mit dem Argument `--vmk vmkX` 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
            --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 `--switchport`*vmkernel_adapter_port_ID* ersetzen, wobei *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 den Inhalt der Pakete, 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
`--dir` 1 `--stage` 0	Überwacht Pakete, unmittelbar nachdem sie den virtuellen Switch verlassen.
`--dir` 1	Überwacht Pakete, unmittelbar bevor sie in den VMkernel-Adapter eingehen.
`--dir` 0 `--stage` 1	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 Netzwerkanalysetool 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 überwachten 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 `--dvfilter`*`DVFilter-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 vmnic`*`X`* 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 pktcap-uw	Ziel
`--capture PreDVFilter`	Erfasst Pakete, bevor sie den DVFilter durchlaufen.
`--capture PostDVFilter`	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 Datenverkehrpaketen 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, das Pakete vom virtuellen Switch empfängt.
VnicTx	Die Funktion im NIC-Backend der virtuellen Maschine, das 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 `--lifID`.
VdrRxTerminal	Erfasst Pakete an der E/A-Kette des Empfangsterminals eines dynamischen Routers in VMware NSX. Verwenden Sie diesen Erfassungspunkt zusammen mit der Option `--lifID`.
VdrTxLeaf	Erfasst Pakete an der E/A-Kette des Übertragungsblatts eines dynamischen Routers in VMware NSX. Verwenden Sie diesen Erfassungspunkt zusammen mit der Option `--lifID`.
VdrTxTerminal	Erfasst Pakete an der E/A-Kette des Übertragungsterminals eines dynamischen Routers in VMware NSX. Verwenden Sie diesen Erfassungspunkt zusammen mit der Option `--lifID`.

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.

vSphere Distributed Switch unterstützt 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** aus.
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. Weitere Informationen hierzu finden Sie unter 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 - 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 14-5. 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 Zielport von Host A auf Host B verschoben.

Tabelle 14-5. 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 Port-Mirroring-Quellen

Um mit dem Erstellen einer Port-Mirroring-Sitzung fortzufahren, wählen Sie Quellen und die Datenverkehrsrichtung für die neue Port-Mirroring-Sitzung.

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 **Konfigurieren** und erweitern Sie **Einstellungen**.

3 Wählen Sie die Option **Portspiegelung** aus und 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 eines Remoteagenten. Der Datenverkehr der virtuellen Maschine wird auf einem entfernen 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

1 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 Sitzungsnamen 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 Port-Mirroring-Quellen

Um mit dem Erstellen einer Port-Mirroring-Sitzung fortzufahren, wählen Sie Quellen und die Datenverkehrsrichtung für die neue Port-Mirroring-Sitzung.

Sie können eine Port-Mirroring-Sitzung ohne Einstellen der Quelle und des Ziels erstellen. Wenn eine Quelle und ein Ziel nicht eingestellt sind, wird eine Port-Mirroring-Sitzung ohne den Spiegelpfad erstellt. Damit erhalten Sie die Möglichkeit, eine Port-Mirroring-Sitzung mit den richtigen Eigenschaftseinstellungen zu erstellen. Nachdem die Eigenschaften eingestellt wurden, können Sie die Port-Mirroring-Sitzung bearbeiten, um die Quellen und Zielinformationen hinzuzufügen.

Hinweis Beachten Sie bei der Auswahl von Port-Mirroring-Quellen die folgenden Einschränkungen.

- Ein Quellspiegelport kann nur in einer Spiegelungssitzung verwendet werden.
- Ein Port kann nicht gleichzeitig als Spiegelungsquelle und als Spiegelungsziel in derselben oder in unterschiedlichen Spiegelungssitzungen verwendet werden.

Verfahren

1 Wählen Sie die Quelle des Datenverkehrs, der gespiegelt werden soll, und die Datenverkehrsrichtung.

Abhängig vom Typ der ausgewählten Port-Mirroring-Sitzung stehen verschiedene Optionen für die Konfiguration zur Verfügung.

Option	Beschreibung
Fügen Sie vorhandene Ports aus einer Liste hinzu.	Klicken Sie auf **Verteilte Ports auswählen**. In einem Dialogfeld wird eine Liste der vorhandenen Ports angezeigt. 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 Zielport 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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Einstellungen** und klicken Sie auf **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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Einstellungen** und klicken Sie auf **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 Sitzungsnamen 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.

Option	Beschreibung
Kapselungs-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 Abwärtspfeil 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

Die Überprüfung des Systemzustands unterstützt Sie dabei, Konfigurationsfehler in einem vSphere Distributed Switch zu erkennen und zu beheben.

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 Netzwerkumgebung entsprechend der Netzwerkrichtlinie 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 Zugriffsports des physischen Switch, die an einem EtherChannel beteiligt sind, mit den verteilten Ports gekoppelt sind, deren Teaming-Richtlinie auf IP-Hash festgelegt ist.	Mindestens zwei aktive physische Netzkarten 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

Verwenden Sie die Überprüfung des Systemzustands des vSphere Distributed Switch, um Konfigurationen für verteilte Switches zu überwachen und Netzwerkprobleme zu identifizieren und zu beheben.

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.

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** imn 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.

5 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.

6 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

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 **Link Layer Discovery Protocol (LLDP)** aus.

5 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Physische Adapter** aus.

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.

Anzeigen des Topologiediagramms eines NSX Virtual Distributed Switch

Sie können die Struktur und die Komponenten eines NSX Virtual Distributed Switch (N-VDS) untersuchen, indem Sie das zugehörige Topologiediagramm öffnen.

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

Voraussetzungen

Das Topologiediagramm eines N-VDS bietet eine visuelle Darstellung der Adapter und Portgruppen, die mit dem Switch verbunden sind.

Verfahren

1. Navigieren Sie im vSphere Client zum Host.
2. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Netzwerk** und wählen Sie **Virtuelle Switches** aus.
3. Wählen Sie den N-VDS in der Liste aus.

Ergebnisse

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

Nächste Schritte

Mithilfe des Topologiediagramms 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.

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 Datencenters 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 abruft, in ein anderes Datencenter verschieben, müssen Sie der verbundenen Portgruppe auf dem Ziel-Datencenter 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 Datencenter verschieben, müssen Sie der verbundenen Portgruppe auf dem Ziel-Datencenter zum Einschalten der vApp bzw. virtuellen Maschine ein Protokollprofil zuweisen.

Verfahren

1. Navigieren Sie zu einem Datencenter, das mit der vApp verknüpft ist, und klicken Sie auf die Registerkarte **Konfigurieren**.
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 Datencenter. Der vSphere Web Client zeigt verteilte Portgruppen unter dem übergeordneten Distributed Switch-Objekt an.

2. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **Mehr** und klicken Sie auf **Netzwerkprotokollprofile**.
3. Klicken Sie auf die Schaltfläche **Profil eines Netzwerkprotokolls mit dem ausgewählten Netzwerk verknüpfen** in der oberen rechten Ecke.
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 die Einstellung **Statisch - IP-Pool** wählen, wird beim ersten Einschalten der virtuellen Maschine oder vApp eine IP-Adresse zugewiesen. Die zugewiesene IP-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.

Multicast-Filter

16

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.

- Aktivieren von Multicast-Snooping auf einem vSphere Distributed Switch

  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.

Aktivieren von Multicast-Snooping auf einem vSphere Distributed Switch

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 6.5.0 oder höher aufweist.

Verfahren

1. Klicken Sie auf der Startseite des vSphere Client auf **Netzwerk** und navigieren Sie 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. Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **System** 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 Erweitern Sie auf der Registerkarte **Konfigurieren** die Option **System** 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 die Distributed Switch-Mitgliedschaft festlegt, fügt vCenter Server den ESXi-Host zu VMware Distributed Switches 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
- 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-Netzwerkadaptereinstellungen (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.

Fehlerbehebung beim Netzwerk 19

In den Themen zur Fehlerbehebung beim Netzwerk finden Sie Lösungen für potenzielle Probleme, die bei der Konnektivität von ESXi-Hosts, vCenter Server und virtuellen Maschinen auftreten können.

Dieses Kapitel enthält die folgenden Themen:

- Richtlinien zur Fehlerbehebung
- Fehlerbehebung bei der Zuteilung von MAC-Adressen
- Host kann nicht auf einem vSphere Distributed Switch entfernt werden
- Für Hosts auf einem vSphere Distributed Switch wird die Verbindung zu vCenter Server getrennt
- Für Hosts auf einem vSphere Distributed Switch 5.0 (und früher) wird die Verbindung zu vCenter Server getrennt
- Alarm wegen des Verlusts der Netzwerkredundanz auf einem Host
- Nach der Änderung der Failover-Reihenfolge für Uplinks einer verteilten Portgruppe wird die Verbindung zu virtuellen Maschinen getrennt
- Einem vSphere Distributed Switch mit aktiviertem Network I/O Control kann kein physischer Adapter hinzugefügt werden
- Fehlerbehebung bei SR-IOV-fähigen Arbeitslasten
- Eine virtuelle Maschine, die einen VPN-Client ausführt, verursacht einen Denial-of-Service-Fehler für virtuelle Maschinen auf dem Host oder für einen vSphere HA-Cluster
- Geringer Durchsatz für UDP-Arbeitslasten auf virtuellen Windows-Maschinen
- Virtuelle Maschinen in derselben verteilten Portgruppe und auf unterschiedlichen Hosts können nicht miteinander kommunizieren
- Der Versuch, eine migrierte vApp einzuschalten, schlägt fehl, weil das zugewiesene Protokollprofil fehlt
- Für einen Netzwerkkonfigurationsvorgang wird ein Rollback durchgeführt und ein Host wird vom vCenter Server getrennt

Richtlinien zur Fehlerbehebung

Für die Fehlerbehebung Ihrer vSphere-Implementierung identifizieren Sie die Symptome des Problems, bestimmen Sie die betroffenen Komponenten und testen Sie mögliche Lösungen.

Identifizieren der Symptome

Eine Reihe potenzieller Ursachen kann zur Leistungsminderung oder zum Leistungsausfall der Implementierung führen. Der erste Schritt für eine effiziente Fehlerbehebung ist die genaue Identifizierung des Problems.

Definieren des Problembereichs

Nachdem Sie die Symptome des Problems isoliert haben, müssen Sie den Problembereich definieren. Identifizieren Sie die betroffenen Software- oder Hardwarekomponenten, durch die das Problem möglicherweise verursacht wird, sowie die nicht betroffenen Software- oder Hardwarekomponenten.

Testen möglicher Lösungen

Wenn Sie die Symptome des Problems und die betroffenen Komponenten kennen, können Sie die Lösungen solange systematisch testen, bis das Problem behoben ist.

Allgemeines zur Fehlerbehebung
(https://vmwaretv.vmware.com/media/t/1_8riyfo25)

Identifizieren der Symptome

Bevor Sie versuchen, ein Problem in Ihrer Implementierung zu beheben, müssen Sie die genauen Fehlersymptome identifizieren.

Der erste Schritt bei der Fehlerbehebung ist das Erfassen von Informationen zu den genauen Symptomen. Sie können sich beim Erfassen dieser Informationen die folgende Fragen stellen:

- Welche Aufgabe wird nicht ausgeführt bzw. welches Verhalten ist nicht vorhanden?
- Kann die betroffene Aufgabe in Unteraufgaben unterteilt werden, die Sie separat auswerten können?
- Endet die Aufgabe mit einem Fehler? Ist eine Fehlermeldung damit verbunden?
- Wird die Aufgabe zwar ausgeführt, dauert aber unzumutbar lange?
- Tritt der Fehler kontinuierlich oder sporadisch auf?
- Welche Änderungen gab es in letzter Zeit bei Software oder Hardware, die in Zusammenhang mit dem Fehler stehen könnten?

Definieren des Problembereichs

Nachdem Sie die Symptome des Problems identifiziert haben, bestimmen Sie die betroffenen Komponenten, die Komponenten, die das Problem verursachen, sowie die nicht beteiligten Komponenten.

Bei der Definition des Problembereichs in einer vSphere-Implementierung müssen Sie die vorhandenen Komponenten berücksichtigen. Neben VMware-Software sollten Sie auf die verwendete Drittanbietersoftware und die mit der virtuellen VMware-Hardware verwendete Hardware achten.

Wenn Sie die Merkmale der Software- und Hardwarekomponenten und deren Auswirkungen auf das Problem kennen, können Sie allgemeine Probleme analysieren, die die Symptome verursachen.

- Fehlkonfiguration der Softwareeinstellungen
- Fehler bei der physischen Hardware
- Inkompatibilität der Komponenten

Schlüsseln Sie den Vorgang auf und erstellen Sie eine separate Analyse jeder Komponente und der Wahrscheinlichkeit, dass die jeweilige Komponente die Ursache sein könnte. Beispielsweise hat ein Problem in Zusammenhang mit einer virtuellen Festplatte im lokalen Speicher wahrscheinlich nichts mit der Konfiguration des Drittanbieterrouters zu tun. Allerdings könnte dieses Problem durch eine Einstellung für den lokalen Festplatten-Controller verursacht werden. Wenn eine Komponente nichts mit den spezifischen Symptomen zu tun hat, können Sie sie wahrscheinlich als Kandidat für Lösungstests eliminieren.

Überlegen Sie sich, was zuletzt an der Konfiguration geändert wurde, bevor die Probleme auftauchten. Suchen Sie nach Gemeinsamkeiten bei einem Problem. Wenn mehrere Probleme gleichzeitig auftauchten, sind wahrscheinlich alle Probleme auf dieselbe Ursache zurückzuführen.

Testen möglicher Lösungen

Wenn Sie die Symptome des Problems und die höchstwahrscheinlich betroffenen Software- oder Hardwarekomponenten kennen, können Sie die Lösungen solange systematisch testen, bis das Problem behoben ist.

Anhand der ermittelten Informationen zu den Symptomen und betroffenen Komponenten können Sie Tests entwickeln, um das Problem ausfindig zu machen und zu beheben. Mithilfe der folgenden Tipps wird dieser Vorgang möglicherweise effektiver ausgeführt.

- Generieren Sie Ideen für möglichst viele potenzielle Lösungen.
- Stellen Sie sicher, dass jede Lösung unmissverständlich bestimmt, ob das Problem behoben wurde. Testen Sie jede potenzielle Lösung, aber fahren Sie unverzüglich fort, falls das Problem durch die Fehlerkorrektur nicht behoben wird.
- Entwickeln und verfolgen Sie eine Hierarchie potenzieller Lösungen auf der Grundlage der Wahrscheinlichkeit. Eliminieren Sie systematisch jedes potenzielle Problem ausgehend von der wahrscheinlichsten Ursache bis hin zur unwahrscheinlichsten Ursache, bis die Symptome verschwinden.
- Ändern Sie beim Testen potenzieller Lösungen immer nur einen Faktor. Wenn das System funktioniert, nachdem Sie viele Faktoren gleichzeitig geändert haben, lässt sich möglicherweise nicht feststellen, auf welche Änderung dies zurückzuführen ist.

- Wenn das Problem durch die für eine Lösung vorgenommenen Änderungen nicht behoben werden kann, setzen Sie die Implementierung auf den vorherigen Status zurück. Für den Fall, dass Sie die Implementierung nicht auf den vorherigen Status zurücksetzen, könnten neue Fehler verursacht werden.
- Suchen Sie eine ähnliche, funktionierende Implementierung und testen Sie sie parallel zu der fehlerhaften Implementierung. Nehmen Sie an beiden Systemen gleichzeitig Änderungen vor, bis nur noch wenige Unterschiede vorhanden sind oder nur noch ein Unterschied vorhanden ist.

Fehlerbehebung mit Protokollen

Die Protokolle der verschiedenen Dienste und Agenten, die von Ihrer Implementierung verwendet werden, liefern oft hilfreiche Fehlerbehebungsinformationen.

Die meisten Protokolle sind unter `C:\ProgramData\VMware\vCenterServer\logs` für Windows-Bereitstellungen oder `/var/log/` für Linux-Bereitstellungen gespeichert. Gemeinsame Protokolle sind in allen Implementierungen verfügbar. Andere Protokolle gelten speziell für bestimmte Bereitstellungsoptionen (Verwaltungsknoten oder Platform Services Controller).

Gemeinsame Protokolle

Die folgenden Protokolle werden gemeinsam von allen Bereitstellungen unter Windows oder Linux verwendet.

Tabelle 19-1. Gemeinsame Protokollverzeichnisse

Protokollverzeichnis	Beschreibung
applmgmt	VMware Appliance Management Service
cloudvm	Protokolle für die Zuteilung und Verteilung von Ressourcen zwischen Diensten
cm	VMware Component Manager
firstboot	Speicherort der Protokolle für den erstmaligen Start
rhttpproxy	Reverse Web Proxy
sca	VMware Service Control Agent
statsmonitor	Vmware Appliance-Überwachungsdienst (nur Linux)
vapi	VMware-vAPI-Endpoint
vmaffd	VMware Authentication Framework-Daemon
vmdird	VMware Directory Service-Daemon
vmon	VMware Service Lifecycle Manager

Protokolle des Verwaltungsknotens

Die folgenden Protokolle sind verfügbar, wenn eine Verwaltungsknotenbereitstellung gewählt wird.

Tabelle 19-2. Protokollverzeichnisse des Verwaltungsknotens

Protokollverzeichnis	Beschreibung
autodeploy	VMware vSphere Auto Deploy Waiter
content-library	VMware Content Library Service
eam	VMware ESX Agent Manager
invsvc	VMware Inventory-Dienst
mbcs	VMware-Meldungs-Bus-Konfigurationsdienst
netdump	VMware vSphere ESXi Dump Collector
perfcharts	VMware-Leistungsdiagramme
vmcam	VMware vSphere Authentication Proxy
vmdird	VMware Directory Service-Daemon
vmsyslog collector	vSphere Syslog Collector (nur Windows)
vmware-sps	VMware vSphere Profile-Driven Storage Service
vmware-vpx	VMware VirtualCenter Server
vpostgres	vFabric Postgres-Datenbankdienst
mbcs	VMware-Meldungs-Bus-Konfigurationsdienst
vsphere-client	VMware vSphere Web Client
vcha	VMware High Availability-Dienst (nur Linux)

Protokolle des Platform Services Controller

Sie analysieren die folgenden Protokolle, wenn eine Platform Services Controller-Knotenbereitstellung gewählt wird.

Tabelle 19-3. Protokollverzeichnisse des Platform Services Controller-Knotens

Protokollverzeichnis	Beschreibung
cis-license	VMware-Lizenzierungsdienst
sso	VMware Secure Token Service
vmcad	VMware Certificate Authority-Daemon
vmdird	VMware Directory Service

Für Platform Services Controller-Knotenbereitstellungen befinden sich zusätzliche Laufzeitprotokolle unter `C:\ProgramData\VMware\CIS\runtime\VMwareSTSService\logs`.

Fehlerbehebung bei der Zuteilung von MAC-Adressen

In vSphere können bestimmte Einschränkungen bezüglich des MAC-Adressbereichs, der virtuellen Maschinen zugewiesen werden kann, dazu führen, dass die Verbindung getrennt wird oder Arbeitslasten nicht eingeschaltet werden können.

Doppelte MAC-Adressen von virtuellen Maschinen im gleichen Netzwerk

Paket- und Konnektivitätsverluste treten auf, da für virtuelle Maschinen von vCenter Server doppelte MAC-Adressen generiert werden.

Problem

Die MAC-Adressen von virtuellen Maschinen in derselben Broadcast-Domäne oder im selben IP-Subnetz verursachen Konflikte, oder aber vCenter Server generiert eine doppelte MAC-Adresse für eine neu erstellte virtuelle Maschine.

Eine virtuelle Maschine wird eingeschaltet und funktioniert ordnungsgemäß, verwendet aber eine MAC-Adresse gemeinsam mit einer anderen virtuellen Maschine. Dadurch können Paketverluste und sonstige Probleme verursacht werden.

Ursache

Es gibt mehrere Ursachen für doppelte MAC-Adressen bei virtuellen Maschinen.

- Zwei vCenter Server-Instanzen mit identischen IDs generieren für VM-Netzwerkadapter überlappende MAC-Adressen.

  Jede vCenter Server-Instanz weist eine ID zwischen 0 und 63 auf, die bei der Installation nach dem Zufallsprinzip erzeugt wird, aber nach der Installation neu konfiguriert werden kann. vCenter Server verwendet die Instanz-ID zum Generieren von MAC-Adressen für die Netzwerkadapter der Maschine.
- Eine virtuelle Maschine wurde in ausgeschaltetem Zustand von einer vCenter Server-Instanz an eine andere Instanz im selben Netzwerk übertragen, beispielsweise mithilfe von gemeinsam genutzten Speicher, und ein neuer VM-Netzwerkadapter in der ersten vCenter Server-Instanz erhält die freigegebene MAC-Adresse.

Lösung

- Ändern Sie die MAC-Adresse eines VM-Netzwerkadapters manuell.

  Wenn eine virtuelle Maschine mit einem MAC-Adressenkonflikt vorhanden ist, müssen Sie in den Einstellungen für **Virtuelle Hardware** eine eindeutige MAC-Adresse eingeben.

  - Schalten Sie die virtuelle Maschine aus, konfigurieren Sie für den Adapter die Verwendung einer manuellen MAC-Adresse und geben Sie die neue Adresse ein.

- Falls Sie die virtuelle Maschine nicht für die Konfiguration ausschalten können, erstellen Sie mit aktivierter manueller MAC-Adresszuweisung den Netzwerkadapter neu, der den Konflikt verursacht, und geben Sie die neue Adresse ein. Legen Sie im Gastbetriebssystem wie zuvor dieselbe statische IP-Adresse für den neu hinzugefügten Adapter fest.

Weitere Informationen zum Konfigurieren der Netzwerkadapter von virtuellen Maschinen finden Sie in der Dokumentation *vSphere-Netzwerk* und *vSphere-Administratorhandbuch für virtuelle Maschinen*.

- Falls die vCenter Server-Instanz die MAC-Adressen von virtuellen Maschinen gemäß der Standardzuteilung (VMware OUI) generiert, ändern Sie die vCenter Server-Instanz-ID oder verwenden Sie eine andere Zuteilungsmethode zum Beheben von Konflikten.

Hinweis Durch die Änderung der vCenter Server-Instanz-ID oder den Wechsel zu einem anderen Zuteilungsschema werden MAC-Adressenkonflikte bei vorhandenen virtuellen Maschinen nicht behoben. Nur nach der Änderung erstellte virtuelle Maschinen oder hinzugefügte Netzwerkadapter erhalten Adressen gemäß dem neuen Schema.

Weitere Informationen zu Zuteilungsschemen von MAC-Adressen und zur Konfiguration von MAC-Adressen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Lösung	Beschreibung
Ändern der vCenter Server-ID	Sie können das VMware-OUI-Zuteilungsschema verwenden, wenn Ihre Bereitstellung nur wenige vCenter Server-Instanzen enthält. Gemäß diesem Schema weisen MAC-Adressen das folgende Format auf: `00:50:56:XX:YY:ZZ` Dabei stellt `00:50:56` den VMware-OUI dar, *XX* wird als (80 + vCenter Server-ID) berechnet, und *YY:ZZ* ist eine Zufallszahl. Zum Ändern der vCenter Server-ID konfigurieren Sie die Option **Eindeutige vCenter Server-ID** im Abschnitt **Laufzeiteinstellungen** der Einstellungen **Allgemein** der vCenter Server-Instanz und starten die Instanz neu. Die VMware-OUI-Zuteilung funktioniert mit bis zu 64 vCenter Server-Instanzen und ist für kleine Bereitstellungen geeignet.
Wechseln zur präfixbasierten Zuteilung	Sie können einen benutzerdefinierten OUI verwenden. Beispielsweise haben für den lokal verwalteten Adressbereich `02:12:34` die MAC-Adressen das Format `02:12:34:XX:YY:ZZ`. Sie können das vierte Oktett *XX* zum Aufteilen des OUI-Adressraums auf die vCenter Server-Instanzen verwenden. Diese Struktur ergibt 255 Adresscluster, wobei jeder Cluster von einer vCenter Server-Instanz verwaltet wird, und etwa 65000 MAC-Adressen pro vCenter Server. Beispielsweise `02:12:34:01:YY:ZZ` für vCenter Server A, `02:12:34:02:YY:ZZ` für vCenter Server B usw. Die präfixbasierte Zuteilung ist für größere Bereitstellungen geeignet. Für global eindeutige MAC-Adressen muss der OUI in IEEE registriert werden.

a Konfigurieren Sie die MAC-Adressenzuteilung.

b Wenden Sie das neue Zuteilungsschema für MAC-Adressen auf eine vorhandene virtuelle Maschine in den Einstellungen für **Virtuelle Hardware** an.

- Schalten Sie eine virtuelle Maschine aus, konfigurieren Sie für den Adapter die Verwendung einer manuellen MAC-Adresse, setzen Sie auf die automatische MAC-Adressenzuteilung zurück und schalten Sie die virtuelle Maschine ein.
- Angenommen, die virtuelle Maschine wird gerade verwendet und kann deshalb nicht für die Konfiguration ausgeschaltet werden. Nachdem Sie die vCenter Server-ID oder das Zuteilungsschema für MAC-Adressen geändert haben, erstellen Sie mit aktivierter automatischer MAC-Adresszuweisung den Netzwerkadapter neu, der den Konflikt verursacht. Legen Sie im Gastbetriebssystem wie zuvor dieselbe statische IP-Adresse für den neu hinzugefügten Adapter fest.

- Erzwingen Sie die Neugenerierung von MAC-Adressen, wenn Sie eine virtuelle Maschine zwischen vCenter Server-Instanzen übertragen, indem Sie die Dateien der virtuellen Maschine aus einem Datenspeicher verwenden.

  a Schalten Sie eine virtuelle Maschine aus, entfernen Sie sie aus der Bestandsliste und legen Sie in der Konfigurationsdatei (`.vmx`) den Parameter `ethernetX.addressType` auf **`generated`** fest.

  Das `X` neben `ethernet` steht für die fortlaufende Nummer der virtuellen Netzwerkkarte in der virtuellen Maschine.

  b Importieren Sie die virtuelle Maschine aus einem vCenter Server-System in ein anderes System, indem Sie die virtuelle Maschine aus einem Datenspeicher in der vCenter Server-Zielinstanz registrieren.

  Die Dateien der virtuellen Maschine können sich in einem Datenspeicher befinden, der von den beiden vCenter Server-Instanzen gemeinsam genutzt wird. Sie können aber auch in einen Datenspeicher hochgeladen werden, auf den nur vom vCenter Server-Zielsystem aus zugegriffen werden kann.

  Weitere Informationen zum Registrieren einer virtuellen Maschine über einen Datenspeicher finden Sie unter *vSphere-Administratorhandbuch für virtuelle Maschinen*.

  c Schalten Sie die virtuellen Maschinen zum ersten Mal ein.

  Während die virtuelle Maschine gestartet wird, wird im vSphere Web Client ein Informationssymbol für die virtuelle Maschine angezeigt.

  d Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie **Gastbetriebssystem > Frage beantworten** aus.

  e Wählen Sie die Option **Ich habe sie kopiert** aus.

  Das vCenter Server-Zielsystem erstellt die MAC-Adresse der virtuellen Maschine neu. Die neue MAC-Adresse beginnt mit dem VMware-OUI `00:0c:29` und basiert auf der BIOS-UUID der virtuellen Maschine. Die BIOS-UUID der virtuellen Maschine wird anhand der BIOS-UUID des Hosts berechnet.

- Falls vCenter Server und Hosts die Version 6.0 und höher aufweisen und die vCenter Server-Instanzen im erweiterten verknüpften Modus miteinander verbunden sind, migrieren Sie virtuelle Maschinen mithilfe von vMotion zwischen vCenter Server-Systemen.

  Bei der Migration einer virtuellen Maschine zwischen vCenter Server-Systemen fügt die vCenter Server-Quellinstanz die MAC-Adresse der virtuellen Maschine zu einer Sperrliste hinzu und weist sie keinen anderen virtuellen Maschinen zu.

Einschalten einer virtuellen Maschine schlägt aufgrund eines MAC-Adressenkonflikts fehl

Nachdem Sie eine statische MAC-Adresse für einen virtuellen Maschinenadapter festgelegt haben, lässt sich die virtuelle Maschine nicht mehr einschalten.

Problem

Nachdem Sie einer virtuellen Maschine eine MAC-Adresse im Bereich von `00:50:56:40:YY:ZZ` – `00:50:56:7F:YY:ZZ` zugewiesen haben, schlägt im vSphere Web Client jeder Einschaltversuch fehl. Eine Statusmeldung weist auf einen Konflikt bei der MAC-Adresse hin.

```
00:50:56:XX:YY:ZZ ist keine gültige statische Ethernet-Adresse. Es besteht ein Konflikt mit
für VMware reservierten MACs zur anderweitigen Nutzung.
```

Ursache

Sie versuchen, eine MAC-Adresse zuzuweisen, die mit dem VMware OUI-Präfix `00:50:56` beginnt und sich innerhalb des Adressbereichs für Host-VMkernel-Adapter im vCenter Server-System befindet.

Lösung

Wenn Sie das VMware OUI-Präfix beibehalten möchten, legen Sie eine statische MAC-Adresse im Bereich zwischen `00:50:56:00:00:00` und `00:50:56:3F:FF:FF` fest. Andernfalls bestimmen Sie eine willkürliche MAC-Adresse mit einem anderen Präfix als VMware OUI. Informationen über die verfügbaren Bereiche für statische MAC-Adressen mit dem VMware OUI-Präfix erhalten Sie in der Dokumentation zu *vSphere-Netzwerk*.

Host kann nicht auf einem vSphere Distributed Switch entfernt werden

Unter bestimmten Bedingungen kann ein Host möglicherweise nicht auf einem vSphere Distributed Switch entfernt werden.

Problem

- Versuche, einen Host von einem vSphere Distributed Switch zu entfernen, schlagen fehl. Außerdem werden Sie informiert, dass Ressourcen weiterhin verwendet werden. Diese Benachrichtigung kann wie folgt aussehen:

  ```
  Die Ressource '16' ist in Gebrauch. vDS DSwitch-Port 16 ist noch auf dem Host 10.23.112.2
  verbunden mit MyVM nic=4000 type=vmVnic
  ```

- Versuche, einen Host-Proxy-Switch zu entfernen, der noch aus einer vorherigen Netzwerkkonfiguration auf dem Host vorhanden ist, schlagen fehl. Angenommen, Sie haben den Host in ein anderes Datencenter oder vCenter Server-System verschoben, ein Upgrade der ESXi- und vCenter Server-Software durchgeführt und eine neue Netzwerkkonfiguration erstellt. Der Versuch, den Host-Proxy-Switch zu entfernen, schlägt fehl, da Ressourcen auf dem Proxy-Switch weiterhin verwendet werden.

Ursache

Aus folgenden Gründen ist es nicht möglich, den Host vom Distributed Switch zu entfernen oder den Host-Proxy-Switch zu löschen.

- Auf dem Switch sind VMkernel-Adapter vorhanden, die verwendet werden.
- Netzwerkadapter der virtuellen Maschine sind mit dem Switch verbunden.

Lösung

Problem	Lösung
Host kann nicht auf einem Distributed Switch entfernt werden	1 Navigieren Sie im vSphere Web Client zum Distributed Switch. 2 Wählen Sie auf der Registerkarte **KonfigurierenMehr > Ports** aus. 3 Suchen Sie alle Ports, die noch verwendet werden, und überprüfen Sie, welche VMkernel- oder VM-Netzwerkadapter auf dem Host noch mit den Ports verbunden sind. 4 Migrieren oder löschen Sie die VMkernel- und VM-Netzwerkadapter, die noch mit dem Switch verbunden sind. 5 Verwenden Sie den Assistenten **Hosts hinzufügen und verwalten** im vSphere Web Client, um den Host vom Switch zu entfernen. Nachdem der Host entfernt wurde, wird der Host-Proxy-Switch automatisch gelöscht.
Host-Proxy-Switch kann nicht entfernt werden	1 Navigieren Sie im vSphere Web Client zum Host. 2 Löschen oder migrieren Sie VMkernel- oder VM-Netzwerkadapter, die noch mit dem Host-Proxy-Switch verbunden sind. 3 Löschen Sie den Host-Proxy-Switch in der Netzwerkansicht auf dem Host.

Für Hosts auf einem vSphere Distributed Switch wird die Verbindung zu vCenter Server getrennt

Hosts auf einem vSphere Distributed Switch können nach der Konfiguration einer Portgruppe keine Verbindung zu vCenter Server herstellen.

Problem

Nach der Änderung der Netzwerkkonfiguration einer Portgruppe auf einem vSphere Distributed Switch, der die VMkernel-Adapter für das Verwaltungsnetzwerk enthält, wird für Hosts auf dem Switch die Verbindung zu vCenter Server getrennt. Im vSphere Web Client wird als Status angezeigt, dass die Hosts nicht reagieren.

Ursache

Auf einem vSphere Distributed Switch in vCenter Server mit deaktiviertem Netzwerk-Rollback ist die Portgruppe mit den VMkernel-Adaptern für das Verwaltungsnetzwerk in vCenter Server falsch konfiguriert, und die ungültige Konfiguration wird an die Hosts auf dem Switch weitergegeben.

Hinweis Die Rollback-Funktion ist im vSphere-Netzwerk standardmäßig aktiviert. Allerdings können Sie Rollbacks auf vCenter Server-Ebene aktivieren bzw. deaktivieren. Weitere Informationen finden Sie in der Dokumentation *vSphere-Netzwerk*.

Lösung

1 Konfigurieren Sie über die Benutzerschnittstelle der direkten Konsole (Direct Console User Interface, DCUI) für einen betroffenen Host mithilfe der Option **vDS wiederherstellen** im Menü **Optionen der Netzwerkwiederherstellung** die Uplinks und die ID des VLAN für das Verwaltungsnetzwerk.

   Die DCUI erstellt einen lokalen flüchtigen Port und wendet die VLAN und die Uplink-Konfiguration auf den Port an. Die DCUI ändert den VMkernel-Adapter für das Verwaltungsnetzwerk, sodass der neue lokale Host-Port verwendet wird, um die Konnektivität mit vCenter Server wiederherzustellen.

   Nachdem der Host erneut eine Verbindung zu vCenter Server hergestellt hat, zeigt der vSphere Web Client eine Warnung an, dass einige Hosts auf dem Switch eine andere als die im vSphere Distributed Switch gespeicherte Netzwerkkonfiguration aufweisen.

2 Konfigurieren Sie im vSphere Web Client die verteilte Portgruppe mit den richtigen Einstellungen für das Verwaltungsnetzwerk.

Situation	Lösung
Sie haben die Konfiguration der Portgruppe nur einmal geändert	Für die Konfiguration der Portgruppe können Sie ein Rollback um einen Schritt durchführen. Klicken Sie mit der rechten Maustaste auf die Portgruppe, klicken Sie auf **Konfiguration wiederherstellen** und wählen Sie **Auf frühere Konfiguration zurücksetzen** aus.
Sie haben eine gültige Konfiguration der Portgruppe gesichert	Mithilfe der Sicherungsdatei können Sie die Konfiguration der Portgruppe wiederherstellen. Klicken Sie mit der rechten Maustaste auf die Portgruppe, klicken Sie auf **Konfiguration wiederherstellen** und wählen Sie **Konfiguration aus einer Datei wiederherstellen** aus. Sie können auch die Konfiguration für den gesamten Switch, einschließlich der Portgruppe, mithilfe einer Sicherungsdatei für den Switch wiederherstellen.
Sie haben mehrere Konfigurationsschritte ausgeführt und verfügen nicht über eine Sicherungsdatei	Sie müssen gültige Einstellungen für die Portgruppe manuell eingeben.

   Weitere Informationen zum Netzwerk-Rollback und zur Wiederherstellung finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

3 Migrieren Sie mit dem Assistenten **Hosts hinzufügen und verwalten** den VMkernel-Adapter für das Verwaltungsnetzwerk vom lokalen flüchtigen Port des Hosts auf einen verteilten Port des Switches.

   Im Gegensatz zu verteilten Ports weist der lokale flüchtige Port des VMkernel eine nicht-numerische ID auf.

   Weitere Informationen zum Umgang mit VMkernel-Adaptern mithilfe des Assistenten **Hosts hinzufügen und verwalten** finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

4 Wenden Sie die Konfiguration der verteilten Portgruppe und den VMkernel-Adapter von vCenter Server auf den Host an.

- Übertragen Sie die richtige Konfiguration der verteilten Portgruppe und den VMkernel-Adapter von vCenter Server an den Host.
  a Navigieren Sie im vSphere Web Client zum Host.
  b Klicken Sie auf der Registerkarte **Konfigurieren** auf **Netzwerk**.
  c Wählen Sie aus der Liste **Virtuelle Switches** den Distributed Switch aus und klicken Sie auf **Zustand des ausgewählten Distributed Switch auf dem Host berichtigen**.
- Warten Sie, bis vCenter Server die Einstellungen innerhalb der nächsten 24 Stunden anwendet.

Für Hosts auf einem vSphere Distributed Switch 5.0 (und früher) wird die Verbindung zu vCenter Server getrennt

Hosts auf einem vSphere Distributed Switch 5.0 (und früher) können nach der Konfiguration einer Portgruppe keine Verbindung zu vCenter Server herstellen.

Problem

Nach der Änderung der Netzwerkkonfiguration einer Portgruppe auf einem vSphere Distributed Switch 5.0 (und früher), der die VMkernel-Adapter für das Verwaltungsnetzwerk enthält, wird für Hosts auf dem Switch die Verbindung zu vCenter Server getrennt. Im vSphere Web Client wird als Status angezeigt, dass die Hosts nicht reagieren.

Ursache

Auf einem vSphere Distributed Switch 5.0 (und früher) in vCenter Server ist die Portgruppe mit den VMkernel-Adaptern für das Verwaltungsnetzwerk in vCenter Server falsch konfiguriert und die ungültige Konfiguration wird an die Hosts auf dem Switch weitergegeben.

Lösung

1 Stellen Sie über den vSphere Client eine Verbindung zu einem betroffenen Host her.

2 Wählen Sie unter **Konfiguration** die Option **Netzwerk** aus.

3 Erstellen Sie in der Ansicht „vSphere Standard-Switch“ einen neuen Standard-Switch, falls der Host keinen geeigneten Standard-Switch für das Verwaltungsnetzwerk aufweist.
   a Klicken Sie auf **Netzwerk hinzufügen (Add Networking)**.
   b Wählen Sie im **Assistenten zum Hinzufügen von Netzwerken** unter „Verbindungstypen“ die Option **Virtuelle Maschine** aus und klicken Sie auf **Weiter**.
   c Wählen Sie **vSphere Standard-Switch erstellen**.

d Wählen Sie im Abschnitt **vSphere Standard-Switch erstellen** einen oder mehrere freie physische Adapter auf dem Host für die Übertragung des Verwaltungsdatenverkehrs aus und klicken Sie auf **Weiter**.

Falls bereits alle physischen Adapter mit Datenverkehr von anderen Switches belegt sind, erstellen Sie den Switch ohne verbundenen physischen Netzwerkadapter. Später entfernen Sie den physischen Adapter für das Verwaltungsnetzwerk im Proxy-Switch des Distributed Switch und fügen ihn zu diesem Standard-Switch hinzu.

e Geben Sie im Abschnitt „Portgruppeneigenschaften“ eine Netzwerkbezeichnung für die zu erstellende Portgruppe und optional eine VLAN-ID ein.

f Klicken Sie auf **Beenden**.

4 Migrieren Sie in der Ansicht „vSphere Distributed Switch“ den VMkernel-Adapter für das Netzwerk auf einen Standard-Switch.

a Wählen Sie die Ansicht „vSphere Distributed Switch“ aus und klicken Sie für den Distributed Switch auf **Virtuelle Adapter verwalten**.

b Wählen Sie im Assistenten **Virtuelle Adapter verwalten** den VMkernel-Adapter aus der Liste aus und klicken Sie auf **Migrieren**.

c Wählen Sie den neu erstellten oder einen anderen Standard-Switch aus, auf den der Adapter migriert werden soll, und klicken Sie auf **Weiter**.

d Geben Sie eine Netzwerkbezeichnung, die im Bereich des Hosts eindeutig ist, und optional eine VLAN-ID für das Verwaltungsnetzwerk ein und klicken Sie auf **Weiter**.

e Überprüfen Sie die Einstellungen im Ziel-Standard-Switch und klicken Sie auf **Beenden**.

5 Konfigurieren Sie im vSphere Web Client die verteilte Portgruppe mit den richtigen Einstellungen für das Verwaltungsnetzwerk.

6 Migrieren Sie mit dem Assistenten **Hosts hinzufügen und verwalten** den VMkernel-Adapter für das Verwaltungsnetzwerk vom Standard-Switch auf einen Port des Distributed Switch.

Weitere Informationen zum Assistenten **Hosts hinzufügen und verwalten**finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

7 Falls Sie den physischen Adapter vom Proxy-Switch auf den Standard-Switch verschoben haben, können Sie ihn mit dem Assistenten **Hosts hinzufügen und verwalten** erneut zum Distributed Switch hinzufügen.

Alarm wegen des Verlusts der Netzwerkredundanz auf einem Host

Ein Alarm meldet für einen Host den Verlust der Uplink-Redundanz auf einem vSphere Standard-Switch oder einem Distributed Switch.

Problem

Für einen Host sind keine redundanten physischen Netzwerkkarten mit einem bestimmten Standard-Switch oder Distributed Switch verbunden und der folgende Alarm wird angezeigt:

```
        Hostname oder IP-Adresse     Netzwerk-Uplink-Redundanz verloren
```

Ursache

Nur eine physische Netzwerkkarte auf dem Host ist mit einem bestimmten Standard-Switch oder Distributed Switch verbunden. Die redundanten physischen Netzwerkkarten sind entweder nicht betriebsbereit oder nicht dem Switch zugewiesen.

Angenommen, ein Host in Ihrer Umgebung weist die physischen Netzwerkkarten *vmnic0* und *vmnic1* auf, die mit *vSwitch0* verbunden sind. Die physische Netzwerkkarte *vmnic1* wird offline geschaltet, sodass nur *vmnic0* mit *vSwitch0* verbunden ist. Die Uplink-Redundanz für *vSwitch0* geht deshalb auf dem Host verloren.

Lösung

Überprüfen Sie, für welchen Switch die Uplink-Redundanz auf dem Host verloren geht. Verbinden Sie mindestens eine zusätzliche physische Netzwerkkarte auf dem Host mit diesem Switch und setzen Sie den Alarm auf Grün zurück. Sie können dazu den vSphere Web Client oder die ESXi Shell verwenden.

Wenn eine physische Netzwerkkarte nicht betriebsbereit ist, versuchen Sie mithilfe der ESXi Shell auf dem Host deren Betriebsbereitschaft wiederherzustellen.

Weitere Informationen zur Verwendung der Netzwerkbefehle in der ESXi Shell finden Sie unter *Referenz zur vSphere Command-Line Interface*. Weitere Informationen zum Konfigurieren von Netzwerkeinstellungen auf einem Host im vSphere Web Client finden Sie unter *vSphere-Netzwerk*.

Nach der Änderung der Failover-Reihenfolge für Uplinks einer verteilten Portgruppe wird die Verbindung zu virtuellen Maschinen getrennt

Durch Änderungen bei der Failover-Reihenfolge für die Netzwerkkarte in einer verteilten Portgruppe werden die virtuellen Maschinen, die der Gruppe zugeordnet sind, vom externen Netzwerk getrennt.

Problem

Nachdem Sie die Uplinks in den Failover-Gruppen für eine verteilte Portgruppe in vCenter Server, beispielsweise mit dem vSphere Web Client geändert haben, können einige virtuelle Maschinen in der Portgruppe nicht mehr auf das externe Netzwerk zugreifen.

Ursache

Nach der Änderung der Failover-Reihenfolge gibt es viele Gründe, weshalb die Verbindung von virtuellen Maschinen zum externen Netzwerk getrennt wird.

- Für den Host, auf dem die virtuellen Maschinen ausgeführt werden, sind den Uplinks keine physischen Netzwerkkarten zugeordnet, die auf „Aktiv“ oder „Standby“ festgelegt sind. Alle Uplinks, denen physische Netzwerkkarten vom Host für die Portgruppe zugeordnet sind, werden nach „Nicht verwendet“ verschoben.
- Eine Linkzusammenfassungsgruppe ohne physische Netzwerkkarten vom Host wird gemäß den Anforderungen für die Verwendung von LACP in vSphere als einziger aktiver Uplink festgelegt.
- Falls der Datenverkehr der virtuellen Maschine auf VLANs verteilt ist, sind die physischen Adapter des Hosts für die aktiven Uplinks möglicherweise mit Trunk-Ports auf dem physischen Switch verbunden, die keinen Datenverkehr von diesen VLANs verarbeiten.
- Falls die Portgruppe über eine IP-Hash-Lastausgleichsrichtlinie konfiguriert wurde, wird ein aktiver Uplink-Adapter mit einem physischen Switch-Port verbunden, der sich möglicherweise nicht in einem „EtherChannel“ befindet.

Mit dem zentralen Topologie-Diagramm des Distributed Switch oder mit dem Proxy-Switch-Diagramm für den Host können Sie die Konnektivität der virtuellen Maschinen in der Portgruppe mit zugehörigen Host-Uplinks und Uplink-Adaptern analysieren.

Lösung

- Stellen Sie die Failover-Reihenfolge mit dem Uplink, der einer einzelnen physischen Netzwerkkarte auf dem Host zugeordnet ist, wieder als aktiv her.
- Erstellen Sie eine Portgruppe mit identischen Einstellungen, legen Sie die Verwendung der gültigen Uplink-Nummer für den Host fest und migrieren Sie das Netzwerk der virtuellen Maschine zur Portgruppe.
- Verschieben Sie die Netzwerkkarte in einen Uplink, der an der aktiven Failover-Gruppe beteiligt ist.

  Mit dem vSphere Web Client können Sie die physische Netzwerkkarte des Hosts in einen anderen Uplink verschieben.

  - Verwenden Sie den Assistenten **Hosts hinzufügen und verwalten** auf dem Distributed Switch.

    a Navigieren Sie zum Distributed Switch im vSphere Web Client.

    b Wählen Sie aus dem Menü **AktionenHosts hinzufügen und verwalten** aus.

    c Wählen Sie auf der Seite **Aufgabe auswählen** die Option **Hostnetzwerk verwalten** und anschließend den Host aus.

d Um die Netzwerkkarte des Hosts einem aktiven Uplink zuzuweisen, navigieren Sie zur Seite **Physische Netzwerkadapter verwalten** und ordnen Sie die Netzwerkkarte dem Switch-Uplink zu.

- Verschieben Sie die Netzwerkkarte auf der Hostebene.
  a Navigieren Sie zum Host im vSphere Web Client und erweitern Sie auf der Registerkarte **Konfigurieren** das Menü **Netzwerk**.
  b Wählen Sie **Virtuelle Switches** und dann den Distributed Switch-Proxy aus.
  c Klicken Sie auf **Physische Netzwerkadapter, die mit dem ausgewählten Switch verbunden sind, verwalten** und verschieben Sie die Netzwerkkarte zum aktiven Uplink.

Einem vSphere Distributed Switch mit aktiviertem Network I/O Control kann kein physischer Adapter hinzugefügt werden

Es kann sein, dass Sie einem vSphere Distributed Switch mit konfiguriertem vSphere Network I/O Control Version 3 keinen physischen Adapter mit geringer Geschwindigkeit (z. B. 1 GBit/s) hinzufügen können.

Problem

Sie versuchen, einem vSphere Distributed Switch, der mit physischen Adaptern mit hoher Geschwindigkeit (z. B. 10 GBit/s) verbunden ist, einen physischen Adapter mit geringer Geschwindigkeit (z. B. 1 GBit/s) hinzuzufügen. Network I/O Control Version 3 ist auf dem Switch aktiviert und es sind Bandbreitenreservierungen für mindestens einen Systemdatenverkehrstyp vorhanden, z. B. für vSphere-Verwaltungsdatenverkehr, vSphere vMotion-Datenverkehr, vSphere-NFS-Datenverkehr usw. Das Hinzufügen des physischen Adapters schlägt fehl und es wird eine Statusmeldung mit dem Hinweis angezeigt, dass ein Parameter falsch ist.

```
Ein angegebener Parameter war nicht korrekt: spec.host[].backing.pnicSpec[]
```

Ursache

Network I/O Control richtet die zur Reservierung verfügbare Bandbreite an der 10-GBit/s-Geschwindigkeit der einzelnen physischen Adapter aus, die bereits mit dem Distributed Switch verbunden sind. Nachdem Sie einen Teil dieser Bandbreite reserviert haben, reicht ein Adapter mit weniger als 10 GBit/s für die Anforderungen eines Systemdatenverkehrstyps möglicherweise nicht mehr aus.

Informationen zu Network I/O Control Version 3 finden Sie in der Dokumentation zu *vSphere-Netzwerk*.

Lösung

1 Navigieren Sie im vSphere Web Client zum Host.

2 Erweitern Sie auf der Registerkarte **Konfigurieren** die Gruppe der Einstellungen für **System**.

3 Wählen Sie **Erweiterte Systemeinstellungen** aus und klicken Sie auf **Bearbeiten**.

4 Geben Sie die physischen Adapter, die außerhalb des Bereichs von Network I/O Control eingesetzt werden sollen, als kommagetrennte Liste für den `Net.IOControlPnicOptOut`-Parameter ein.

   Beispiel: **`vmnic2,vmnic3`**

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

6 Fügen Sie in vSphere Web Client den physischen Adapter zum verteilten Switch hinzu.

Fehlerbehebung bei SR-IOV-fähigen Arbeitslasten

Unter bestimmten Bedingungen können bei virtuellen Maschinen, die mithilfe von SR-IOV Daten an physische Netzwerkadapter senden, Konnektivitäts- oder Einschaltprobleme auftreten.

SR-IOV-fähige Arbeitslast kann nach der Änderung der MAC-Adresse nicht mehr kommunizieren

Nach dem Ändern der MAC-Adresse im Gastbetriebssystem einer SR-IOV-fähigen virtuellen Maschine wird die Verbindung der virtuellen Maschine unterbrochen.

Problem

Wenn Sie den Netzwerkadapter einer virtuellen Maschine mit einer virtuellen SR-IOV-Funktion (VF) verbinden, erstellen Sie einen Passthrough-Netzwerkadapter für die virtuelle Maschine. Nachdem der (VF-) Treiber im Gastbetriebssystem die MAC-Adresse für den Passthrough-Netzwerkadapter modifiziert hat, zeigt das Gastbetriebssystem an, dass die Änderung erfolgreich war, aber die Verbindung des VM-Netzwerkadapters geht verloren. Obwohl das Gastbetriebssystem anzeigt, dass die neue MAC-Adresse aktiviert ist, weist eine Protokollnachricht in der Datei `/var/log/vmkernel.log` darauf hin, dass die Operation fehlgeschlagen ist.

```
Angeforderte Änderung der MAC-Adresse auf neue MAC-Adresse auf Port Portnummer der VM-Netzwerkkarte wegen vSwitch-Richtlinie unzulässig.
```

wo

- *neue MAC-Adresse* ist die MAC-Adresse im Gastbetriebssystem.
- *Portnummer der VM-Netzwerkkarte* ist die Portnummer des VM-Netzwerkadapters im Hexadezimalformat.

Ursache

Die Standardsicherheitsrichtlinie auf der Portgruppe, mit der der Passthrough-Netzwerkadapter verbunden ist, erlaubt keine Änderungen der MAC-Adresse im Gastbetriebssystem. Deshalb kann die Netzwerkschnittstelle im Gastbetriebssystem keine IP-Adresse erhalten und ihre Verbindung geht verloren.

Lösung

- Setzen Sie im Gastbetriebssystem die Schnittstelle zurück, damit der Passthrough-Netzwerkadapter wieder seine gültige MAC-Adresse erhält. Wenn die Schnittstelle für die Verwendung von DHCP für die Adressenzuweisung konfiguriert ist, ruft die Schnittstelle automatisch eine IP-Adresse ab.

  Beispiel: Führen Sie auf einer virtuellen Linux-Maschine den Konsolenbefehl `ifconfig` aus.

  ```
  ifconfig ethX down
  ifconfig ethX up
  ```

  dabei stellt *X* in `ethX` die Sequenznummer des Netzwerkadapters der virtuellen Maschine im Gastbetriebssystem dar.

Eine virtuelle Maschine, die einen VPN-Client ausführt, verursacht einen Denial-of-Service-Fehler für virtuelle Maschinen auf dem Host oder für einen vSphere HA-Cluster

Eine virtuelle Maschine, die BPDU-Frames (Bridge Protocol Data Unit) sendet (z. B. ein VPN-Client), bewirkt, dass bei virtuellen Maschinen, die mit derselben Portgruppe verbunden sind, die Verbindung getrennt wird. Die Übertragung von BPDU-Frames kann auch die Verbindung des Hosts oder des übergeordneten vSphere HA-Clusters trennen.

Problem

Eine virtuelle Maschine, die BPDU-Frames senden soll, bewirkt, dass der Datenverkehr zum externen Netzwerk der virtuellen Maschinen in derselben Portgruppe blockiert wird.

Falls die virtuelle Maschine auf einem Host ausgeführt wird, der Bestandteil eines vSphere HA-Clusters ist, und falls der Host unter bestimmten Bedingungen vom Netzwerk isoliert wird, treten Denial-of-Service-Fehler (DoS) auf den Hosts im Cluster auf.

Ursache

Es empfiehlt sich, für einen physischen Switch-Port, der mit einem ESXi-Host verbunden ist, Port-Fast und BPDU-Guard zu aktivieren, um die Begrenzung des Spanning-Tree-Protokolls (STP) zu erzwingen. STP wird von einem Standard-Switch oder Distributed Switch nicht unterstützt, und es werden keine BPDU-Frames an den Switch-Port gesendet. Wenn jedoch ein BPDU-Frame von einer manipulierten virtuellen Maschine an einem physischen Switch-Port eintrifft, der auf einen ESXi-Host verweist, deaktiviert die BPDU-Guard-Funktion den Port, um eine Beeinträchtigung der Spanning-Tree-Topologie des Netzwerks durch die Frames zu verhindern.

In bestimmen Fällen soll eine virtuelle Maschine BPDU-Frames senden, beispielsweise beim Bereitstellen eines VPN, das über ein Windows-Bridge-Gerät oder über eine Bridge-Funktion verbunden ist. Wenn für die Kombination aus physischem Switch-Port und physischem Adapter, von der der Datenverkehr dieser virtuellen Maschine verarbeitet wird, BPDU-Guard aktiviert ist, ist der Port aufgrund eines Fehlers deaktiviert. Die virtuellen Maschinen und die VMkernel-Adapter, die den physischen Adapter des Hosts verwenden, können nicht mehr mit dem externen Netzwerk kommunizieren.

Falls die Teaming- und Failover-Richtlinie der Portgruppe mehr aktive Uplinks enthält, wird der BPDU-Datenverkehr auf den Adapter für den nächsten aktiven Uplink verschoben. Der neue physische Switch-Port wird deaktiviert, weshalb für weitere Arbeitslasten keine Pakete mit dem Netzwerk ausgetauscht werden können. Schließlich sind fast alle Entitäten auf dem ESXi-Host nicht mehr erreichbar.

Falls die virtuelle Maschine auf einem Host ausgeführt wird, der Bestandteil eines vSphere HA-Clusters ist, und falls der Host vom Netzwerk isoliert wird, da die meisten verbundenen physischen Switch-Ports deaktiviert sind, verschiebt der aktive primäre Host im Cluster die virtuelle Maschine des BPDU-Absenders auf einen anderen Host. Die virtuelle Maschine beginnt mit dem Deaktivieren der physischen Switch-Ports, die mit dem neuen Host verbunden sind. Die Migration im vSphere HA-Cluster führt letztlich zu einer Häufung von DoS-Fehlern im gesamten Cluster.

Lösung

- Falls die VPN-Software noch auf der virtuellen Maschine verwendet werden muss, lassen Sie den ausgehenden Datenverkehr für die virtuelle Maschine zu und konfigurieren Sie den physischen Switch-Port so, dass die BPDU-Frames übertragen werden.

Netzwerkgerät	Konfiguration
Distributed Switch oder Standard-Switch	Legen Sie die Sicherheitseigenschaft „Gefälschte Übertragungen“ in der Portgruppe auf **Akzeptieren** fest, damit BPDU-Frames aus dem Host übertragen werden und den physischen Switch-Port erreichen. Sie können die Einstellungen und den physischen Adapter für den VPN-Datenverkehr isolieren, indem Sie die virtuelle Maschine einer separaten Portgruppe hinzufügen und den physischen Adapter der Gruppe zuweisen. **Vorsicht** Die Festlegung der Sicherheitseigenschaft „Gefälschte Übertragungen“ auf **Akzeptieren**, damit BPDU-Frames von einem Host gesendet werden können, beinhaltet ein Sicherheitsrisiko, da eine manipulierte virtuelle Maschine Spoofing-Angriffe ausführen kann.
Physischer Switch	■ Lassen Sie Port-Fast aktiviert. ■ Aktivieren Sie den BPDU-Filter für den betreffenden Port. Wenn ein BPDU-Frame am Port eintrifft, wird er herausgefiltert. **Hinweis** Aktivieren Sie den BPDU-Filter nicht global. Wenn der BPDU-Filter global aktiviert wird, wird der Port-Fast-Modus deaktiviert und alle physischen Switch-Ports führen den kompletten STP-Funktionssatz aus.

- Um ein Bridge-Gerät zwischen zwei VM-Netzwerkkarten bereitzustellen, die mit demselben Layer 2-Netzwerk verbunden sind, lassen Sie den ausgehenden BPDU-Datenverkehr für die virtuellen Maschinen zu und deaktivieren Sie Port-Fast und die Verhinderung von BPDU-Schleifen.

Netzwerkgerät	Konfiguration
Distributed Switch oder Standard-Switch	Legen Sie die Eigenschaft „Gefälschte Übertragungen“ der Sicherheitsrichtlinie in den Portgruppen auf **Akzeptieren** fest, damit BPDU-Frames aus dem Host übertragen werden und den physischen Switch-Port erreichen. Sie können die Einstellungen und einen oder mehrere physische Adapter für den Bridge-Datenverkehr isolieren, indem Sie die virtuelle Maschine einer separaten Portgruppe hinzufügen und die physischen Adapter der Gruppe zuweisen. **Vorsicht** Die Festlegung der Sicherheitseigenschaft „Gefälschte Übertragungen“ auf **Akzeptieren**, um die Bridge-Bereitstellung zu ermöglichen, beinhaltet ein Sicherheitsrisiko, da eine manipulierte virtuelle Maschine Spoofing-Angriffe ausführen kann.
Physischer Switch	■ Deaktivieren Sie Port-Fast auf den Ports zum virtuellen Bridge-Gerät, um STP darauf auszuführen. ■ Deaktivieren Sie BPDU-Guard und filtern Sie nach den Ports, die auf das Bridge-Gerät verweisen.

- Schützen Sie die Umgebung auf jeden Fall vor DoS-Angriffen, indem Sie den BPDU-Filter auf dem ESXi-Host oder dem physischen Switch aktivieren.
  - Aktivieren Sie auf einem Host, für den der Gast-BPDU-Filter nicht implementiert ist, den BPDU-Filter auf dem physischen Switch-Port zum virtuellen Bridge-Gerät.

Netzwerkgerät	Konfiguration
Distributed Switch oder Standard-Switch	Setzen Sie die Eigenschaft „Gefälschte Übertragungen“ der Sicherheitsrichtlinie in der Portgruppe auf **Ablehnen**.
Physischer Switch	■ Behalten Sie die Port-Fast-Konfiguration bei. ■ Aktivieren Sie den BPDU-Filter für den betreffenden physischen Switch-Port. Wenn ein BPDU-Frame am physischen Port eintrifft, wird er herausgefiltert. **Hinweis** Aktivieren Sie den BPDU-Filter nicht global. Wenn der BPDU-Filter global aktiviert wird, wird der Port-Fast-Modus deaktiviert und alle physischen Switch-Ports führen den kompletten STP-Funktionssatz aus.

Geringer Durchsatz für UDP-Arbeitslasten auf virtuellen Windows-Maschinen

Wenn eine virtuelle Windows-Maschine in vSphere große UDP-Pakete überträgt, ist der Durchsatz geringer als erwartet oder schwankt, auch wenn anderer Datenverkehr zu vernachlässigen ist.

Problem

Wenn eine virtuelle Windows-Maschine UDP-Pakete größer als 1024 Byte überträgt, ist der Durchsatz geringer als erwartet oder schwankt, auch wenn anderer Datenverkehr zu vernachlässigen ist. Im Falle eines Video-Streaming-Servers hält die Video-Wiedergabe an.

Ursache

Für jedes UDP-Paket größer als 1024 Byte wartet der Windows-Netzwerkstapel auf einen Übertragungsabschluss-Interrupt, bevor das nächste Paket gesendet wird. vSphere bietet keine transparente Umgehung der Situation.

Lösung

- Erhöhen Sie den Schwellenwert in Byte, bei dem Windows sein Verhalten in Bezug auf UDP-Pakete ändert, indem Sie die Registrierung des Windows-Gastbetriebssystems ändern.
  a Suchen Sie den Registrierungsschlüssel `HKLM\System\CurrentControlSet\Services\Afd\Parameters`.
  b Fügen Sie einen Wert mit dem Namen `FastSendDatagramThreshold` vom Typ DWORD gleich 1500 hinzu.

  Weitere Informationen zum Beheben dieses Problems in der Windows-Registrierung finden Sie auf http://support.microsoft.com/kb/235257.
- Ändern Sie die Vereinigungseinstellungen der Netzwerkkarte der virtuellen Maschine.

  Wenn die virtuelle Windows-Maschine über einen VMXNET3 vNIC-Adapter verfügt, konfigurieren Sie einen der folgenden Parameter in der `.vmx`-Datei der virtuellen Maschine. Verwenden Sie den vSphere Web Client oder ändern Sie direkt die `.vmx`-Datei.

Aktion	Parameter	Wert
Erhöhen Sie die Interrupt-Rate der virtuellen Maschine auf eine höhere Rate als die erwartete Paketrate. Wenn die erwartete Paketrate beispielsweise 15000 Interrupts pro Sekunde entspricht, legen Sie die Interrupt-Rate auf 16000 Interrupts pro Sekunde fest. Setzen Sie den Parameter `ethernetX.coalescingScheme` auf **`rbc`** und den Parameter `ethernetX.coalescingParams` auf **`16000`**. Die Standard-Interrupt-Rate beträgt 4000 Interrupts pro Sekunde.	`ethernetX.coalescingScheme` `ethernetX.coalescingParams`	rbc 16000
Deaktivieren Sie die Vereinigung für geringen Durchsatz oder latenzempfindliche Arbeitslasten. Informationen zum Konfigurieren von Arbeitslasten mit niedriger Latenz finden Sie unter Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs.	`ethernetX.coalescingScheme`	Deaktiviert
Stellen Sie den Vereinigungsalgorithmus früherer ESXi-Versionen wieder her. **Hinweis** In höheren vSphere-Versionen kann ein früherer Algorithmus nicht wiederhergestellt werden.	`ethernetX.coalescingScheme`	kalibrieren

  Das *X* neben `ethernet` steht für die fortlaufende Nummer der vNIC in der virtuellen Maschine.

  Weitere Informationen zum Konfigurieren von Parametern in der `.vmx`-Datei finden Sie in der *vSphere-Administratorhandbuch für virtuelle Maschinen*-Dokumentation.

- Ändern Sie die Vereinigungseinstellungen des ESXi-Hosts.

  Dieser Ansatz betrifft alle virtuellen Maschinen und alle Netzwerkkarten virtueller Maschinen auf dem Host.

  Sie können die Liste „Erweiterte Systemeinstellungen“ für den Host im vSphere Web Client oder mithilfe eines vCLI-Konsolenbefehls auf dem Host aus der ESXi Shell bearbeiten.

Aktion	Parameter im vSphere Web Client	Parameter für den Befehl `esxcli system settings sdvanced set`	Wert
Legen Sie eine Standard-Interrupt-Rate fest, die höher als die erwartete Paketrate ist. Legen Sie beispielsweise die Interrupt-Rate auf 16000 fest, wenn 15.000 Interrupts pro Sekunde erwartet werden.	`Net.CoalesceScheme` `Net.CoalesceParams`	`/Net/CoalesceScheme` `/Net/CoalesceParams`	rbc 16000
Deaktivieren Sie die Vereinigung für geringen Durchsatz oder latenzempfindliche Arbeitslasten. Informationen zum Konfigurieren von Arbeitslasten mit niedriger Latenz finden Sie unter Best Practices for Performance Tuning of Latency-Sensitive Workloads in vSphere VMs.	`Net.CoalesceDefaultOn`	`/Net/CoalesceDefaultOn`	0
Stellen Sie das Vereinigungsschema früherer ESXi-Versionen wieder her. **Hinweis** In höheren vSphere-Versionen kann ein früherer Algorithmus nicht wiederhergestellt werden.	`Net.CoalesceScheme`	`/Net/CoalesceScheme`	kalibrieren

  Weitere Informationen zum Konfigurieren eines Hosts aus dem vSphere Web Client finden Sie in der *vCenter Server und Hostverwaltung*-Dokumentation. Weitere Informationen zum Festlegen von Hosteigenschaften mithilfe eines vCLI-Befehls finden Sie in der *Referenz zur vSphere Command-Line Interface*-Dokumentation.

Virtuelle Maschinen in derselben verteilten Portgruppe und auf unterschiedlichen Hosts können nicht miteinander kommunizieren

Unter bestimmten Bedingungen können die virtuellen Maschinen, die sich in derselben verteilten Portgruppe, aber auf unterschiedlichen Hosts befinden, nicht miteinander kommunizieren.

Problem

Virtuelle Maschinen, die sich auf unterschiedlichen Hosts und in derselben Portgruppe befinden, können nicht miteinander kommunizieren. Die Ausführung von Ping-Befehlen zwischen virtuellen Maschinen zeigt keine Wirkung. Sie können die virtuellen Maschinen nicht mithilfe von vMotion zwischen den Hosts migrieren.

Ursache

- Auf einigen Hosts sind aktiven oder Standby-Uplinks in der Teaming- und Failover-Reihenfolge der verteilten Portgruppe keine physischen Netzwerkkarten zugewiesen.
- Die physischen Netzwerkkarten auf den Hosts, die den aktiven oder Standby-Uplinks zugewiesen sind, befinden sich in unterschiedlichen VLANs auf dem physischen Switch. Die physischen Netzwerkkarten in unterschiedlichen VLANs erkennen die jeweils anderen Netzwerkkarten nicht und können deshalb nicht miteinander kommunizieren.

Lösung

- Überprüfen Sie in der Topologie des Distributed Switch, welchem Host keine physischen Netzwerkkarten zu einem aktiven oder Standby-Uplink in der verteilten Portgruppe zugewiesen sind. Weisen Sie mindestens eine physische Netzwerkkarte auf diesem Host einem aktiven Uplink in der Portgruppe zu.
- Überprüfen Sie in der Topologie des Distributed Switch die VLAN-IDs der physischen Netzwerkkarten, die den aktiven Uplinks in der verteilten Portgruppe zugewiesen sind. Weisen Sie auf allen Hosts physische Netzwerkkarten desselben VLAN einem aktiven Uplink in der verteilten Portgruppe zu.
- Um sicherzustellen, dass auf der physischen Ebene kein Problem vorliegt, migrieren Sie die virtuellen Maschinen zum selben Host und überprüfen Sie die Kommunikation zwischen ihnen. Stellen Sie sicher, dass eingehender und ausgehender ICMP-Datenverkehr im Gastbetriebssystem aktiviert sind. Standardmäßig ist ICMP-Datenverkehr in Windows Server 2008 und Windows Server 2012 deaktiviert.

Der Versuch, eine migrierte vApp einzuschalten, schlägt fehl, weil das zugewiesene Protokollprofil fehlt

Sie können keine vApp oder virtuelle Maschine einschalten, die Sie an ein Datencenter oder ein vCenter Server-System übertragen haben, weil ein Netzwerkprotokollprofil fehlt.

Problem

Nach der Cold-Migration einer vApp oder einer virtuellen Maschine zu einem anderen Datacenter oder vCenter Server-System schlägt das Einschalten der vApp bzw. der virtuellen Maschine fehl. Eine Fehlermeldung gibt an, dass eine Eigenschaft nicht initialisiert oder zugewiesen werden kann, weil das Netzwerk der vApp oder virtuellen Maschine kein zugewiesenes Netzwerkprotokollprofil besitzt.

```
Eigenschaft 'property' kann nicht initialisiert werden. Netzwerk 'port group' besitzt kein
zugewiesenes Netzwerkprotokollprofil.
```

```
IP-Adresse für Eigenschaft 'property' kann nicht zugewiesen werden. Netzwerk 'port group'
besitzt kein zugewiesenes Netzwerkprotokollprofil.
```

Ursache

Mithilfe der OVF-Umgebung ruft die vApp oder virtuelle Maschine die Netzwerkeinstellungen von einem Netzwerkprotokollprofil ab, das mit der Portgruppe der vApp oder virtuellen Maschine verknüpft ist.

Der vCenter Server schafft ein solches Netzwerkprotokollprofil für Sie, wenn Sie das OVF einer vApp installieren, und ordnet das Profil mit der Portgruppe zu, das Sie während der Installation angeben.

Die Zuordnung zwischen dem Protokollprofil und der Portgruppe ist nur im Bereich eines Datencenters zulässig. Wenn Sie vApp verschieben, wird das Protokollprofil aus folgenden Gründen nicht an das Zieldatencenter übertragen:

- Die Netzwerkeinstellungen des Protokollprofils sind möglicherweise in der Netzwerkumgebung des Zieldatencenters nicht zulässig.
- Eine Portgruppe, die den gleichen Namen hat und einem anderen Protokollprofil zugeordnet ist, existiert möglicherweise bereits im Zieldatencenter und vApps und virtuelle Maschinen sind möglicherweise mit dieser Gruppe verbunden. Durch das Ersetzen der Protokollprofile für die Portgruppe kann die Konnektivität dieser vApp und virtuellen Maschinen beeinflusst werden.

Lösung

- Erstellen Sie mit den erforderlichen Netzwerkeinstellungen ein Netzwerkprotokollprofil im Zieldatencenter oder vCenter Server-System und ordnen Sie das Protokollprofil der Portgruppe zu, mit der vApp oder die virtuelle Maschine verbunden ist. Dieser Ansatz ist beispielsweise geeignet, wenn vApp oder die virtuelle Maschine eine vCenter Server-Erweiterung ist, die den vCenter-Erweiterungs-vService nutzt.

  Für Informationen zur Bereitstellung von Netzwerkeinstellungen für vApp oder eine virtuelle Maschine durch ein Netzwerkprotokollprofil, siehe *vSphere-Netzwerk* Dokumentation.
- Verwenden Sie den vSphere Web Client, um die OVF-Datei von vApp oder der virtuellen Maschine vom Quelldatencenter oder vCenter Server-System zu exportieren und im Zieldatencenter oder vCenter Server-System bereitzustellen.

  Wenn Sie vSphere Web Client verwenden, um die OVF-Datei bereitzustellen, erstellt das vCenter Server-System das Netzwerkprotokollprofil für vApp.

  Für Informationen zur Verwaltung von OVF-Dateien im vSphere Web Client, siehe *vSphere-Administratorhandbuch für virtuelle Maschinen* Dokumentation.

Für einen Netzwerkkonfigurationsvorgang wird ein Rollback durchgeführt und ein Host wird vom vCenter Server getrennt

Wenn Sie versuchen, Netzwerke auf einem vSphere Distributed Switch auf einem Host hinzuzufügen oder zu konfigurieren, wird für den Vorgang ein Rollback durchgeführt und die Verbindung zwischen Host und vCenter Server wird getrennt.

Problem

Ein Versuch, einen Netzwerkkonfigurationsvorgang für einen vSphere Distributed Switch auf einem Host durchzuführen, z. B. Erstellen eines VM-Adapters oder einer Portgruppe, führt dazu, dass die Verbindung zwischen Host und vCenter Server getrennt und die Fehlermeldung `Für die Transaktion wurde auf dem Host ein Rollback durchgeführt` angezeigt wird.

Ursache

Bei hoher Belastung des Hosts, d. h., wenn viele gleichzeitige Netzwerkvorgänge sich begrenzte Ressourcen teilen müssen, überschreitet die Ausführungsdauer einiger der Vorgänge möglicherweise das Standardzeitlimit für das Rollback von Netzwerkkonfigurationsvorgängen auf dem Distributed Switch. Infolgedessen wird für diese Vorgänge ein Rollback durchgeführt.

Solch eine Bedingung kann beispielsweise eintreten, wenn Sie einen VMkernel-Adapter auf einem Host erstellen, der eine große Zahl von Switch-Ports oder virtuellen Adaptern aufweist, die alle Systemressourcen auf dem Host verbrauchen.

Das Standardzeitlimit für das Rollback eines Vorgangs beträgt 30 Sekunden.

Lösung

- Verwenden Sie den vSphere Web Client, um die Zeitüberschreitung für das Rollback auf dem vCenter Server zu erhöhen.

  Falls dasselbe Problem erneut auftritt, erhöhen Sie die Zeitüberschreitung für das Rollback schrittweise um jeweils 60 Sekunden, bis die Zeit ausreicht, um den Vorgang erfolgreich auszuführen.

  a Erweitern Sie auf der Registerkarte **Konfigurieren** einer vCenter Server-Instanz die Option **Einstellungen**.

  b Wählen Sie **Erweiterte Einstellungen** aus und klicken Sie auf **Bearbeiten**.

  c Wenn die Eigenschaft nicht existiert, fügen Sie den Parameter `config.vpxd.network.rollbackTimeout` zu den Einstellungen hinzu.

  d Geben Sie für den Parameter `config.vpxd.network.rollbackTimeout` einen neuen Wert (in Sekunden) ein.

  e Klicken Sie auf **OK**.

  f Starten Sie das vCenter Server-System neu, um die Änderungen anzuwenden.

- Erhöhen Sie die Zeitüberschreitung für das Rollback durch Bearbeiten der `vpxd.cfg`-Konfigurationsdatei.

  Falls dasselbe Problem erneut auftritt, erhöhen Sie die Zeitüberschreitung für das Rollback schrittweise um jeweils 60 Sekunden, bis die Zeit ausreicht, um den Vorgang erfolgreich auszuführen.

  a Navigieren Sie auf einer vCenter Server-Instanz in das Verzeichnis, das die `vpxd.cfg`-Konfigurationsdatei enthält.

    - Navigieren Sie in einem Windows Server-Betriebssystem zu *`vCenter Server-Stammverzeichnis`*`\Application Data\VMware\VMware VirtualCenter`.
    - Navigieren Sie auf der vCenter Server-Appliance zu `/etc/vmware-vpx`.

  b Öffnen Sie die Datei `vpxd.cfg` zur Bearbeitung.

  c Erhöhen Sie im Abschnitt `<network>` für das Element `<rollbackTimeout>` die Zeitüberschreitung.

```
<config>
  <vpxd>
    <network>
      <rollbackTimeout>60</rollbackTimeout>
    </network>
  </vpxd>
</config>
```

  d Speichern und schließen Sie die Datei.

  e Starten Sie das vCenter Server-System neu, um die Änderungen anzuwenden.