



Benutzerhandbuch
Ethernet iSCSI-Adapter und
Ethernet FCoE-Adapter
QLogic BCM57xx und BCM57xxx

BC0054508-01 J



Informationen Dritter, die Ihnen von
Dell zur Verfügung gestellt wurden.

Dokumenten-Überarbeitungsverlauf	
Überarbeitung A: 18. Februar 2015	
Überarbeitung B: 29. Juli 2015	
Überarbeitung C: 24. März 2016	
Überarbeitung D: 8. April 2016	
Überarbeitung E: 2. Februar 2017	
Überarbeitung F: 25. August 2017	
Überarbeitung G: 19. Dezember 2017	
Überarbeitung H: 15. März 2018	
Überarbeitung J: 13. April 2018	
Änderungen	Betroffener Abschnitt
<p>Schritt 1 geändert.</p> <p>Unterstützung für NPIV (über die Spezifikation „Fibre Channel - Link Services“) auf Linux und Windows hinzugefügt.</p> <p>Im ersten Abschnitt Bedeutung des letzten Satzes wie folgt geklärt: „Unter Windows Server ab Version 2016 wird der <i>QLogic QLASP-Teaming</i>-Treiber nicht mehr unterstützt.“</p> <p>In der ANMERKUNG Bedeutung des letzten Satzes wie folgt geklärt: „Unter Windows Server ab Version 2016 wird der <i>QLogic QLASP-Teaming</i>-Treiber nicht mehr unterstützt.“</p> <p>Im HINWEIS die Bedeutungen des ersten und zweiten Satzes geklärt: „Die <i>statische und dynamische</i> Teamart für die Link Aggregation (<i>Switch-abhängig</i>) wird auf Ports, auf denen der NIC-Partitionsmodus (NPAR) oder iSCSI-Offload aktiviert ist, nicht unterstützt. Manche Switches unterstützen FCoE-Offload im <i>dynamischen</i> LACP Teaming-Modus.</p> <p>RHEL 6.9, 7.4, 7.5, SLES12 SP3 zur Liste der unterstützten Betriebssysteme hinzugefügt.</p> <p>ESXi 6.0 U3, ESXi 6.5 U1, ESXi 6.5 U2, ESXi 6.7 zur Liste der unterstützten Betriebssysteme hinzugefügt.</p>	<p>„Herunterladen von Dokumenten“ auf Seite xxiii</p> <p>„FCoE“ auf Seite 5</p> <p>„Konfigurieren von Teaming auf einem Windows Server“ auf Seite 8</p> <p>„QLASP Übersicht“ auf Seite 8</p> <p>„Link Aggregation (802.3ad)“ auf Seite 10</p> <p>„Linux“ auf Seite 19</p> <p>„VMware ESXi“ auf Seite 19</p>

<p>In der ANMERKUNG ESXi 6.7 hinzugefügt und angegeben, dass es eigene Treiber für alle Protokolle verwendet.</p> <p>Unter Tabelle 8-1 eine komprimierte ZIP-Treiberdatei für ESXi 6.7 hinzugefügt.</p> <p>Parameter <code>enable_live_grcdump</code> hinzugefügt.</p> <p>Unterstützung für Windows Server 2016 hinzugefügt.</p> <p>Anweisungen für die Auswahl von iSCSI als Legacy-Startprotokoll (Schritt 1 und Abbildung 10-1) hinzugefügt.</p>	<p>„VMware-Treibersoftware“ auf Seite 64</p> <p>„Verfügbare Pakete“ auf Seite 64</p> <p>„enable_live_grcdump“ auf Seite 68</p> <p>„Installieren der Treibersoftware“ auf Seite 76 (in der zweiten ANMERKUNG), „Verwenden des Installationsprogramms“ auf Seite 77 (Tabelle 9-1), „Einrichten des iSCSI-Startvorgangs für Windows Server 2012, 2012 R2 und 2016“ auf Seite 106, „Übersicht“ auf Seite 230, „FCoE-Start-Installation für Windows Server 2012, 2012 R2 und 2016“ auf Seite 245, „Data Center Bridging unter Windows Server ab Version 2012“ auf Seite 276, „Microsoft Virtualization mit Hyper-V“ auf Seite 321 (Tabelle 19-1), „Teaming-Netzwerkadapter“ auf Seite 324 (Tabelle 19-2).</p> <p>„Konfigurieren der iSCSI-Bootparameter“ auf Seite 89</p>
---	--

Inhalt

Vorwort

Zielanwender	xxi
Inhalt dieses Handbuchs	xxi
Zugehörige Materialien	xxii
Konventionen in der Dokumentation	xxii
Herunterladen von Dokumenten	xxiii
Laser-Sicherheitsinformationen	xxiv

1 Funktionen und Merkmale

Funktionsbeschreibung	1
Merkmale und Funktionen	2
iSCSI	4
FCoE	5
Energieverwaltung	5
Adaptive Interrupt-Frequenz	6
ASIC mit eingebettetem RISC-Prozessor	6
QLogic Control Suite-Befehlszeilenschnittstelle	6
Unterstützte Betriebsumgebungen	6
Netzwerkverbindung und Betriebsanzeige	7

2 Konfigurieren von Teaming auf einem Windows Server

QLASP Übersicht	8
Lastausgleich und Fehlertoleranz	9
Teamarten	9
Smart Load Balancing und Failover	10
Link Aggregation (802.3ad)	10
Allgemeines Trunking (FEC/GEC)/802,3ad-Draft Static	11
SLB (Auto-Fallback deaktiviert)	11
Einschränkungen bei den Teamarten Smart Load Balancing, Failover und SLB (Auto-Fallback deaktiviert)	12
Unterstützung für Teaming und Large Send Offload und Checksum Offload (Large-Send-Verschiebung und Prüfsummenverschiebung)	13

3	Virtuelle LANs bei Windows	
	VLAN-Überblick	14
	Hinzufügen von VLANs zu Teams	17
4	Installieren der Hardware	
	Systemanforderungen	18
	Hardwareanforderungen	18
	Anforderungen an das Betriebssystem	19
	Allgemein	19
	Microsoft Windows	19
	Linux	19
	VMware ESXi	19
	Citrix XenServer	20
	Sicherheitsvorkehrungen	20
	Vor der Installation - Checkliste	20
	Installation der zusätzlichen Netzwerkkarte	21
	Installieren der zusätzlichen Netzwerkkarte	21
	Anschließen der Netzwerkkabel	22
	Kupferdraht	23
	Lichtwellenleiter	24
5	Verwaltungsfunktionen	
	CIM	25
	Host Bus Adapter-API	26
6	Boot Agent-Treibersoftware	
	Übersicht	27
	Einrichten von MBA Agent in einer Client-Umgebung	28
	Konfigurieren des MBA-Treibers	28
	Verwenden des Comprehensive Configuration Management-Werkzeugs	29
	Verwenden von UEFI	30
	Einrichten von BIOS	33
	Einrichten von MBA Agent in einer Linux Server-Umgebung	34
7	Linux-Treibersoftware	
	Einführung	35
	Einschränkungen	36
	bnx2x-Treibereinschränkungen	36
	bnx2i-Treibereinschränkungen	36
	bnx2fc-Treibereinschränkungen	37

Verfügbare Pakete	37
Installieren der Linux-Treibersoftware	38
Installieren des Quell-RPM-Pakets	38
Installieren des KMP-Pakets	41
Erstellen des Treibers aus der Quell-TAR-Datei	41
Installieren des DKMS-Binär-RPM-Treiberpakets	42
Installieren des Binär-KMOD- und KMP-Treiberpakets	43
Laden Sie die erforderlichen iSCSI-Softwarekomponenten, und führen Sie sie aus	44
Schließen oder Entfernen des Linux-Treibers	44
Schließen oder Entfernen des Treibers aus einer RPM-Installation	44
Entfernen des Treibers aus einer TAR-Installation	45
Deinstallation QCS mit dem RPM-Paket	45
Patchen von PCI-Dateien (optional)	45
Netzwerkinstallationen	46
Einstellen der Werte für optionale Eigenschaften	47
bnx2x-Treiberparameter	47
disable_tpa	47
int_mode	47
dropless_fc	48
disable_iscsi_ooo	48
num_queues	48
pri_map	49
bnx2i-Treiberparameter	49
error_mask1 and error_mask2	49
en_tcp_dack	49
time_stamps	50
sq_size	50
rq_size	50
event_coal_div	50
last_active_tcp_port	51
ooo_enable	51
bnx2fc-Treiberparameter	51
debug_logging	51
Treiberstandardeinstellungen	52
bnx2-Treiberstandards	52
bnx2x-Treiberstandards	53

Treibermeldungen	53
bnx2x-Treibermeldungen.	53
Treiberanmeldung.	53
C-NIC-Treiberanmeldung (nur bnx2)	54
Netzwerkkarte gefunden.	54
Übertragungsrate und aktive Verbindung.	54
Nicht aktive Verbindung	54
bnx2i-Treibermeldungen	54
BNX2I-Treiberanmeldung	54
Netzwerkport zur Transportnamenbindung bei iSCSI	54
Treiber führt Handshake mit iSCSI-Offload-fähigem C-NIC-Gerät durch	54
Der Treiber erkennt, dass iSCSI-Offload auf dem C-NIC-Gerät nicht aktiviert ist.	54
Übersteigt maximal zulässige iSCSI-Offload-Obergrenze	55
Netzwerkpfad zum Zielknoten und Transportnamenbindung sind unterschiedliche Geräte	55
Ziel ist über keines der C-NIC-Geräte zu erreichen	55
Netzwerkroute ist deaktivierter Netzwerkschnittstelle zugewiesen	55
SCSI-ML leitet Host-Reset ein (Sitzungswiederherstellung) . . .	55
C-NIC erfasst iSCSI-Protokollverstoß – Schwerwiegende Fehler.	56
C-NIC Detects iSCSI Protocol Violation – Keine schwerwiegende Warnung.	57
Treiber führt Wiederherstellung einer Sitzung durch	57
Abgelehnte iSCSI-PDU vom Ziel erhalten	57
Open-iSCSI-Daemon übergibt Sitzung an Treiber	57
bnx2fc-Treibermeldungen	57
BNX2FC-Treiberanmeldung	57
Treiber führt Handshake mit FCoE-Offload-fähigem C-NIC-Gerät durch	57
Treiber führt Handshake mit iSCSI-Offload-fähigem C-NIC-Gerät nicht durch.	58
Keine gültige Lizenz, um FCoE zu starten	58
Sitzungsfehler aufgrund der Überschreitung des erlaubten FCoE-Offload-Verbindungslimits oder Arbeitsspeicherlimits . . .	58
Offload-Fehler der Sitzung	58
Upload-Fehler in der Sitzung	58
ABTS kann nicht gesendet werden	58

Aufgrund einer Zeitüberschreitung in ABTS kann die E/A unter Verwendung von ABTS nicht wiederhergestellt werden.	58
Aufgrund einer nicht abgeschlossenen Sitzung kann E/A- Anfrage (Eingabe/Ausgabe) nicht durchgeführt werden..	59
Falsche L2-Empfangsframes verwerfen.	59
Host Bus Adapter und lport-Zuweisungsfehler.	59
NPIV Port Erstellung.	59
Teaming-Funktion mit Channel Bonding	59
Statistikdaten	59
iSCSI-Verschiebung in Linux	59
Open-iSCSI-Benutzeranwendungen.	60
Benutzeranwendung - iscsiui0.	60
Verbinden Sie das iSCSI-Ziel mit dem QLogiciSCSI-Transportnamen	60
VLAN-Konfiguration für iSCSI-Offload (Linux).	61
Herstellen von Verbindungen mit iSCSI-Zielen	62
Statische Eingabe hinzufügen	62
iSCSI-Zielermittlung mithilfe von <code>sendtargets</code>	62
Anmeldung beim Ziel mit dem Befehl <code>iscsiadm</code>	62
Auflisten aller im System aktiven Laufwerke	62
Maximale Offload-iSCSI-Verbindungen.	62
Häufig gestellte Fragen zu Linux iSCSI-Offload	63

8 VMWare-Treibersoftware

Verfügbare Pakete	64
Netzwerkunterstützung, Treiber	65
Herunterladen, Installieren und Aktualisieren von Treibern.	65
Treiberparameter.	65
<code>int_mode</code>	65
<code>disable_tpa</code>	65
<code>num_queues</code>	66
<code>pri_map</code>	66
<code>droplless_fc</code>	66
RSS	67
<code>max_vfs</code>	67
<code>enable_vxlan_ofld</code>	67
<code>enable_default_queue_filters</code>	67
<code>enable_live_grcdump</code>	68
Treiberstandardeinstellungen	68

Entfernen des Treibers	68
Treibermeldungen	69
Treiberanmeldung	69
Netzwerkschnittstellenkarte erkannt	69
MSI-X erfolgreich aktiviert	69
Übertragungsrate und aktive Verbindung	69
Nicht aktive Verbindung	69
Speichereinschränkung	69
Multiqueue und NetQueue	70
Unterstützung von FCoE	70
Treiber	70
Unterstützte Distributionen	71
Aktivieren von FCoE	71
Installationsprüfung	72
Einschränkungen	73
iSCSI-Unterstützung	73
VLAN-Konfiguration für iSCSI-Offload (VMware)	73
9 Windows-Treibersoftware	
Installieren der Treibersoftware	76
Verwenden des Installationsprogramms	77
Verwenden der Hintergrundinstallation	80
Ändern der Treibersoftware	82
Reparieren oder Neuinstallieren der Treibersoftware	83
Entfernen der Gerätetreiber	83
Anzeigen oder Ändern der Adapter-Eigenschaften	84
Einstellen der Optionen zur Energieverwaltung	84
Konfigurieren des zu verwendenden Kommunikationsprotokolls über die QCC-Benutzeroberfläche, QCC PowerKit und QCS CLI	86
10 iSCSI-Protokoll	
iSCSI Boot	87
Unterstützte Betriebssysteme für iSCSI-Boot	87
Einrichten von iSCSI-Boot	88
Konfigurieren des iSCSI-Ziels	88
Konfigurieren der iSCSI-Bootparameter	89
Konfigurieren des MBA-Bootprotokolls	93
iSCSI-Boot-Konfiguration	93
Aktivieren der CHAP-Authentifizierung	100

Konfigurieren des DHCP-Servers auf Unterstützung von iSCSI-Boot	100
DHCP-Konfiguration für iSCSI-Boot bei IPv4	101
DHCP-Konfiguration für iSCSI-Boot bei IPv6	103
Konfigurieren des DHCP-Servers	104
Vorbereiten des iSCSI-Boot-Image	104
Booten	116
Weitere Hinweise zu iSCSI-Boot	116
Ändern der Einstellungen für Übertragungsrates und Duplex in Windows-Umgebungen	116
Lokal verwaltete Adresse	117
Virtuelle LANs	117
„DD“-Methode zur Erstellung eines iSCSI-Boot-Image	117
Fehlerbehebung bei iSCSI-Boot	118
iSCSI-Absturzspeicherabbild	120
iSCSI-Offload unter Windows Server	120
Konfigurieren von iSCSI-Offload	121
Installieren von QLogic-Treibern und Management-Anwendungen	121
Installieren von Microsoft iSCSI Software Initiator	121
Konfigurieren von QLogic-iSCSI mit QCC	121
Konfigurieren von Microsoft Initiator zur Verwendung von QLogic iSCSI Offload	122
Häufig gestellte Fragen zu iSCSI-Offload	130
Ereignisprotokollmeldungen für den Offload-iSCSI-(OIS)-Treiber	131

11 QLogic Teaming Services

Gesamtübersicht	139
Glossar	140
Teaming-Begriffe	141
Netzwerkadressierung	142
Teaming und Netzwerkadressen	143
Beschreibung der Teaming-Arten	143
Softwarekomponenten	149
Hardwareanforderungen	150
Repeater-Hub	150
Switching-Hub	151
Router	151
Teaming-Unterstützung nach Prozessor	151
Konfigurieren der Teaming-Funktion	152

Unterstützte Funktionen nach Teamart	152
Auswählen einer Teamart	154
Teaming-Verfahren	156
Architektur	157
Ausgehender Verkehr	158
Eingehender Verkehr (nur SLB)	159
Protokoll-Unterstützung	160
Leistung	161
Teamarten	161
Switch-unabhängig	161
Switch-abhängig	162
LiveLink	165
Attribute der mit jeder Teamart verbundenen Leistungsmerkmale	165
Für jede Teamart unterstützte Übertragungsraten	168
Teaming und andere erweiterte Netzwerkeigenschaften	168
Checksum Offload (Prüfsummenverschiebung)	170
IEEE 802.1p QoS-Markierung	170
Large Send Offload (Large Send-Verschiebung)	170
Jumbo-Rahmen	170
IEEE 802.1Q VLANs	171
Wake on LAN	171
Preboot Execution Environment	172
Allgemeine Netzwerkaspekte	172
Teaming mit Microsoft Virtual Server 2005	172
Switch-übergreifendes Teaming	173
Fehlertoleranz bei Switch-Verbindung	173
Spanning Tree-Algorithmus	177
Topology Change Notice (TCN)	178
Port Fast und Edge Port	179
Schicht-3-Routing und -Switching	179
Teaming mit Hubs (nur zur Problembhebung)	179
Verwendung von Hubs in Teaming-Netzwerkkonfigurationen	180
SLB-Teams	180
SLB-Teams mit Anschluss an einen einzelnen Hub	180
Allgemeines und Dynamisches Trunking (FEC/GEC/IEEE 802.3ad)	181
Teaming mit Microsoft Network Load Balancing	181

Anwendungsaspekte	181
Teaming und Clustering	182
Microsoft Cluster-Software	182
High-Performance Computing Cluster	184
Oracle	185
Teaming und Netzwerkbackup	186
Lastausgleich und Failover	187
Fehlertoleranz	189
Behebung von Teaming-Problemen	190
Tipps zur Teaming-Konfiguration	191
Richtlinien für die Problembehebung	192
Häufig gestellte Fragen	193
Ereignisprotokollmeldungen	197
Ereignisprotokollmeldungen unter Windows	197
Basistreiber (Physischer Adapter oder Miniport)	197
Intermediate-Treiber (Virtueller Adapter oder Team)	203
Virtual Bus Driver (VBD)	207
12 NIC-Partitionierung und Bandbreitenverwaltung	
Übersicht	211
Unterstützte Betriebssysteme für die NIC-Partitionierung	212
Konfigurieren der NIC-Partitionierung	212
13 Linux QCS Installation	
Übersicht	217
Kommunikationsprotokolle	218
Installieren von WS-MAN oder CIM-XML auf einem Linux-Server	219
Schritt 1: Installieren von OpenPegasus	219
Vom internen RPM (Nur Red Hat)	219
Von der Source (Red Hat und SUSE)	220
Schritt 2: Starten von CIM Server auf dem Server	223
Schritt 3: Konfigurieren von OpenPegasus auf dem Server	223
Aktivieren der Authentifizierung	224
Aktivieren von HTTP	224
Aktivieren von HTTPS	225
Schritt 4: Installieren des QLogic-CMPI-Providers	225
Installieren	225
Deinstallieren	225

Schritt 5: Durchführen der Linux-Firewall-Konfiguration, falls erforderlich	226
Red Hat	226
SUSE	226
Schritt 6: QCS und zugehörige Management-Anwendungen installieren	227
Installieren von WS-MAN oder CIM-XML auf einem Linux-Client	227
Konfigurieren von HTTPS auf einem Linux-Client	227
Importieren eines selbstsignierten Zertifikats auf einem Linux-Client	227
Testen der HTTPS/SSL-Verbindung von einem Linux-Client . . .	228
Installieren von QLogic Control Suite	228

14 Fibre Channel Over Ethernet

Übersicht	230
FCoE-Boot aus SAN	231
Vorbereiten des System-BIOS auf FCoE-Build und -Boot.	231
Anpassen der System-Startreihenfolge	231
Angaben des BIOS-Boot-Protokolls (falls erforderlich).	232
Vorbereiten des QLogic Multi-Boot-Agenten auf FCoE-Boot (CCM-Dienstprogramm)	232
Vorbereiten des QLogic Multi-Boot-Agenten auf FCoE-Boot (UEFI-Dienstprogramm)	237
Einrichten von Speicherzugriff im SAN	239
Vorab-Einrichtung	239
STRG+R-Methode	240
Einmalige Deaktivierung	241
FCoE-Boot-Installation mit Windows 2008 R2 und Windows Server 2008 SP2	242
FCoE-Start-Installation für Windows Server 2012, 2012 R2 und 2016	245
FCoE-Boot-Installation unter Linux	245
Installation von SLES 11 SP3 und SLES 12.	245
RHEL 6-Installation.	254
RHEL 7-Installation.	259
Linux: Hinzufügen von Boot-Pfaden	261
FCoE-Boot-Installation unter VMware ESXi	263
Konfigurieren des FCoE-Boot von SAN unter VMware	266

	Booten von SAN nach der Installation	267
	Treiberaktualisierung unter Linux-Boot von SAN-Systemen	267
	Fehler während des FCoE-Boots der SAN-Installation unter Windows	269
	Konfigurieren von FCoE	270
	N_Port-ID-Virtualisierung (NPIV)	272
15	Data Center Bridging	
	Übersicht	273
	DCB-Eigenschaften	274
	Enhanced Transmission Selection (Erweiterte Übertragungsauswahl, ETS).	274
	Priority Flow Control (PFC)	274
	Data Center Bridging eXchange (DCBX)	275
	Konfigurieren von DCB.	275
	Bedingungen für DCB	275
	Data Center Bridging unter Windows Server ab Version 2012	276
16	SR-IOV	
	Übersicht	278
	Aktivieren von SR-IOV	278
	Überprüfen der SR-IOV-Funktionsfähigkeit	282
	SR-IOV und Speicherfunktion	283
	SRSR-IOV und Jumbo-Pakete.	283
17	Spezifikationen	
	10/100/1000BASE-T- und 10GBASE-T-Kabelspezifikationen	284
	Unterstützte SFP+-Module pro NIC.	285
	Schnittstellenspezifikationen	287
	Abmessungen der Netzwerkkarte	288
	Anforderungen der Netzwerkkarte an die Stromversorgung	288
	Anforderungen von Wake on LAN an die Stromversorgung	290
	Umgebungsbedingungen	291
18	Zulassungsbestimmungen	
	Produktsicherheit	293
	AS/NZS (C-Tick).	294
	FCC-Hinweis	294
	FCC, Klasse B.	294
	FCC, Klasse A.	295

VCCI-Hinweis	296
VCCI, Klasse B	300
VCCI Class B Statement (Japan)	301
VCCI, Klasse A	301
VCCI Class A Statement (Japan)	302
CE-Hinweis	302
Konformitätserklärung für Kanada	303
Industry Canada, Class B	303
Industry Canada, Class A	303
Industry Canada, classe B.	304
Industry Canada, classe A.	304
Korea Communications Commission (KCC)-Hinweis (nur für die Republik Korea)	305
Gerät der Klasse B	305
Gerät der Klasse A	306
BSMI	308
Zulassungen für BCM95709SA0908G, BCM957710A1023G, (E02D001) und BCM957711A1123G (E03D001)	308
FCC-Hinweis	309
FCC, Klasse A	309
VCCI-Hinweis	310
Klasse A	310
VCCI Class A Statement (Japan)	311
CE-Hinweis	311
Klasse A	311
Konformitätserklärung für Kanada	311
Industry Canada, Class A.	311
Industry Canada, classe A	312
Korea Communications Commission (KCC)-Hinweis (nur für die Republik Korea)	313
Gerät der Klasse A	313

19 Fehlerbehebung

Hardware-Diagnose	315
QCS Fehler bei Diagnosetests	316
QCSFehler bei Netzwerktests	316
Überprüfen der Port-LEDs	317
Fehlerbehebung – Checkliste	317

Überprüfen der geladenen Treiber	318
Windows	318
Linux	318
Durchführen eines Kabellängentests	319
Testen der Netzwerkanbindung	319
Windows	320
Linux	320
Microsoft Virtualization mit Hyper-V	321
Einzelner Netzwerkadapter	322
Windows Server 2008	322
Windows Server 2008 R2 und 2012.	323
Teaming-Netzwerkadapter.	324
Windows Server 2008	325
Windows Server 2008 R2.	326
Konfigurieren von VMQ mit SLB-Teaming	326
Entfernen der QLogic BCM57xx und BCM57xxx Gerätetreiber	327
Aktualisieren von Windows-Betriebssystemen.	327
QLogic Boot Agent	328
QLASP	328
Linux.	330
NPAR	331
Kernel-Debugging über Ethernet	332
Sonstiges	332

Liste der Abbildungen

Abbildung	Seite	
3-1	Beispiel für die Unterstützung mehrerer markierter VLANs durch Server	15
6-1	CCM MBA Configuration Menu (MBA-Konfigurationsmenü)	29
6-2	Systemeinrichtung, Geräteeinstellungen	30
6-3	Geräteeinstellungen	31
6-4	Hauptkonfigurationsseite	32
6-5	NIC-Konfiguration	33
8-1	VM Network Properties (VM-Netzwerkeigenschaften): Beispiel 1	74
8-2	VM Network Properties (VM-Netzwerkeigenschaften): Beispiel 2	75
9-1	Eingabeaufforderung des InstallShield-Assistenten für das Verwaltungsdienstprogramm	78
9-2	Optionen zur Energieverwaltung des Geräts	85
10-1	Legacy Boot Protocol (Legacy-Startprotokoll)	89
10-2	UEFI, iSCSI-Konfiguration	90
10-3	UEFI, iSCSI-Konfiguration, allgemeine iSCSI-Parameter	91
10-4	iSCSI-Konfiguration, iSCSI-Initiatorparameter	95
10-5	iSCSI-Konfiguration, iSCSI-Parameter des ersten Ziels	97
10-6	iSCSI-Initiatoreigenschaften: Seite „Allgemein“	122
10-7	Ändern des Initiator Node Name (Initiatorknotennamens)	123
10-8	iSCSI Initiator Properties (iSCSI-Initiatoreigenschaften): Seite „Ermittlung“	124
10-9	Dialogfeld „Add Target Portal“ (Zielportal hinzufügen)	124
10-10	Erweiterte Einstellungen: General Page (Allgemeine Seite)	125
10-11	iSCSI Initiator Properties (iSCSI-Initiatoreigenschaften): Discovery Page (Seite „Ermittlung“)	126
10-12	iSCSI Initiator Properties (iSCSI-Initiatoreigenschaften): Seite „Ziele“	127
10-13	Log On to Target (Bei Ziel anmelden)	128
10-14	Advanced Settings (Erweiterte Einstellungen): Seite „Allgemein“, Lokaler Adapter	129
11-1	Auswahl einer Teamart	155
11-2	Intermediate-Treiber	157
11-3	Switch-übergreifendes Teaming ohne Verbindung zwischen den Switches	174
11-4	Switch-übergreifendes Teaming mit Schnittstelle	175
11-5	Failover-Ereignis	176
11-6	Team mit Anschluss an einen einzelnen Hub	181
11-7	Clustering mit Teaming über einen Switch	183
11-8	Clustering mit Teaming über zwei Switches	185
11-9	Netzwerkbackup ohne Teaming	186
11-10	Netzwerkbackup mit SLB-Teaming über zwei Switches	190
14-1	Öffnen des CCM-Dienstprogramms	232
14-2	CCM-Geräteliste	233
14-3	CCM-Gerätehardwarekonfiguration	233
14-4	CCM MBA Configuration Menu (MBA-Konfigurationsmenü)	234
14-5	CCM-Zielinformationen	235
14-6	CCM-Zielparameter	236

14-7	CCM-Zielinformationen (nach der Konfiguration)	236
14-8	Menü „FCoE-Boot-Konfiguration“	237
14-9	Menü „FCoE-Boot-Konfiguration“, Allgemeine FCoE-Parameter	238
14-10	FCoE-Boot	242
14-11	Installieren des EVBD-Treibers	243
14-12	Installieren des bxfcoe-Treibers	243
14-13	Auswählen der Installations-CD-Partition	244
14-14	Starten der SLES-Installation	246
14-15	Auswählen des Datenträgers zur Treiberaktualisierung	247
14-16	Laden des Treibers	247
14-17	Aktivieren des Datenträgers	248
14-18	Aktivieren von FCoE	249
14-19	Ändern der FCoE-Einstellungen	250
14-20	Konfiguration der FCoE-Schnittstelle	251
14-21	Aktivieren des Datenträgers	252
14-22	Installationseinstellungen	253
14-23	Bootlader-Gerätezuweisungstabelle	254
14-24	Hinzufügen der dd-Option	255
14-25	Auswählen eines Treiberdatenträgers	256
14-26	Hinzufügen eines FCoE SAN-Treibers	257
14-27	Konfigurieren von FCoE-Parametern	258
14-28	Bestätigen von FCoE-Treibern	258
14-29	Hinzufügen der dd-Option	259
14-30	Auswählen von Partitionierungsoptionen	261
14-31	Auswählen eines ESXi-Datenträgers	263
14-32	ESXi und VMFS gefunden	264
14-33	ESXi Installation bestätigen	264
14-34	ESXi Installation abgeschlossen	265
14-35	Auswahl des ESXi-Managementnetzwerks	265
14-36	Netzwerk-Konfiguration des VMware vSphere Client	266
14-37	Booten von SAN nach der Installation	267
14-38	Windows-Fehlermeldung zu Partition	269
14-39	Ressourcenkonfiguration – Seite	271

Tabellenliste

Tabelle	Seite	
1-1	Port-LED-Anzeige des RJ45 für Netzwerkverbindung und -betrieb	7
1-2	Port-LED-Anzeige für Netzwerkverbindung und -betrieb	7
2-1	Smart Load Balancing	12
3-1	Beispiel für eine VLAN-Netzwerktopologie	15
4-1	100/1000BASE-T und 10GBASE-T-Kabelspezifikationen	23
4-2	1000/2500BASE-X Lichtwellenleiterspezifikationen.	24
7-1	QLogic BCM57xx und BCM57xxx Linux-Treiber	35
8-1	VMware-Treiberpakete	64
9-1	Windows-Betriebssysteme und iSCSI-Absturzspeicherabbild	80
10-1	Konfigurationsoptionen	92
10-2	Definition der Parameter von „DHCP Option 17“	101
10-3	Definition der Unteroptionen von DHCP Option 43	102
10-4	Definition der Unteroptionen von DHCP Option 17	103
10-5	Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber (OIS-Treiber)	131
11-1	Glossar	140
11-2	Verfügbare Teaming-Arten	144
11-3	QLogic Teaming-Softwarekomponente	149
11-4	Vergleich der Teamarten	152
11-5	Teaming-Attribute	165
11-6	Übertragungsraten beim Teaming	168
11-7	Erweiterte Adaptereigenschaften und Teaming-Unterstützung	169
11-8	Ereignisprotokollmeldungen für Basistreiber	198
11-9	Ereignisprotokollmeldungen für Intermediate-Treiber	203
11-10	Virtual Bus Driver (VBD)-Ereignisprotokollmeldungen	207
12-1	Konfigurationsoptionen	213
12-2	Funktionsbeschreibung	214
13-1	Kommunikationsprotokolloptionen	218
13-2	Umgebungsvariablen	221
13-3	cimconfig-Befehlsoptionen	223
14-1	Unterstützte Legacy BFS und uEFI BFS	263
17-1	10/100/1000BASE-T-Kabelspezifikationen	284
17-3	BCM57710 – unterstützte Module	285
17-2	10GBASE-T – Kabelspezifikationen	285
17-4	BCM57810 – unterstützte Module	286
17-5	BCM57840 – unterstützte Module	287
17-6	10, 100, und 1000BASE-T – Leistungsspezifikationen	287
17-7	10GBASE-T – Leistungsspezifikationen	288
17-8	Abmessungen der Netzwerkkarte	288
17-9	Anforderungen der Netzwerkkarte BCM957810A1006G an die Stromversorgung	288
17-10	Anforderungen der Netzwerkkarte BCM957810A1008G an die Stromversorgung	289

17-11	Anforderungen der BCM957840A4006G Mezzanine-Karte an die Stromversorgung	289
17-12	Anforderungen der BCM957840A4007G Mezzanine-Karte an die Stromversorgung	290
17-13	BCM5709 und BCM5716 Umgebungsbedingungen	291
17-14	BCM957810A1006G Umgebungsbedingungen	291
17-15	BCM957810A1008G Umgebungsbedingungen.	292
17-16	BCM957840A4007G Umgebungsbedingungen	292
18-1	Physische Kenndaten der Netzwerktochterkarte QLogic 57800S 1GB und 10GBASE-T Rack	296
18-2	Physische Kenndaten der Netzwerktochterkarte QLogic 57800S Quad RJ-45, SFP+ oder Direct Attach Rack	297
18-3	Physische Kenndaten der PCI-e-Karte QLogic 57810S Dual 10GBASE-T	298
18-4	Physische Kenndaten der PCI-e-Karte QLogic 57810S Dual SFP+ oder Direct Attach.	298
18-5	Physische Kenndaten des Mezzanine-Adapters QLogic 57810S-K Dual KR Blade	299
18-6	Physische Kenndaten der Netzwerktochterkarte QLogic 57810S-K Dual KR Blade	299
18-7	Physische Kenndaten der Netzwerktochterkarte QLogic 57840S Quad 10GbE SFP+ oder Direct Attach Rack	300
18-8	Physische Kenndaten der Netzwerktochterkarte QLogic 57840S-K Quad KR Blade	300
19-1	Bei Netzwerkadaptern konfigurierbare Hyper-V-Funktionen	321
19-2	Bei Team-Netzwerkadaptern konfigurierbare Hyper-V-Funktionen	324

Vorwort

Dieser Abschnitt bietet Informationen zu den Zielenwendern dieses Handbuchs, zu Inhalt, Konventionen in diesem Dokument und Laser-Sicherheitsinformationen.

ANMERKUNG

QLogic® unterstützt auf allen QLogic-Adaptern nun die QConvergeConsole® (QCC)-Benutzeroberfläche als *einziges* Verwaltungstool für die Benutzeroberfläche. Die QLogic Control Suite (QCS)-Benutzeroberfläche wird auf QLogic-Adaptern, die auf Controllern der Versionen 57xx/57xxx basieren, nicht mehr unterstützt. Sie wurde durch das Verwaltungstool für die QCC-Benutzeroberfläche ersetzt. Mit der QCC-Benutzeroberfläche können Sie alle QLogic-Adapter über ein Benutzeroberflächen-Fenster verwalten.

Wenn Sie in Windows®-Umgebungen das Installationsprogramm für die QCS-Befehlszeile und die Verwaltungsagenten ausführen, werden die QCS-Benutzeroberfläche (falls auf dem System vorhanden) und alle zugehörigen Komponenten von Ihrem System deinstalliert.

Zielanwender

Dieses Handbuch ist für Personal bestimmt, das für die Installation und Wartung der Ausrüstung von Computernetzwerken verantwortlich ist.

Inhalt dieses Handbuchs

Dieses Handbuch beschreibt die Merkmale und Funktionen, die Installation und die Konfiguration der QLogic® BCM57xx und BCM57xxx Converged Network-Adapter und intelligenten Ethernet-Adapter.

Zugehörige Materialien

Weitere Informationen finden Sie im *Migrationshandbuch: QLogic/Broadcom NetXtreme I/II Adapters*, Dokumentnummer BC0054606-00. Das Migrationshandbuch gibt einen Überblick über die Übernahme bestimmter Broadcom®-Ethernet-Komponenten durch QLogic und deren Auswirkungen auf Endbenutzer. Das Handbuch wurde gemeinschaftlich von Broadcom und QLogic erstellt.

Konventionen in der Dokumentation

In diesem Handbuch werden die folgenden Konventionen verwendet:

- **ANMERKUNG** bietet zusätzliche Informationen.
- **VORSICHT!** ohne Warnsymbol weist auf eine Gefahr hin, die die Ausrüstung beschädigen oder zu Datenverlust führen könnte.
- **⚠ VORSICHT!** mit Warnsymbol weist auf eine Gefahr hin, die zu leichten bis mittelschweren Verletzungen führen könnte.
- **⚠ WARNUNG** weist auf eine Gefahr hin, die zu schweren Verletzungen oder zum Tod führen könnte.
- Text in **blauer** Schrift weist auf einen Hyperlink (eine Verknüpfung) zu einer Abbildung, einer Tabelle oder einem Abschnitt in diesem Handbuch hin, und Verknüpfungen zu Websites sind **blau unterstrichen** dargestellt. Zum Beispiel:
 - ❑ In **Tabelle 9-2** sind Probleme in Hinblick auf die Benutzeroberfläche und den Remote Agent aufgeführt.
 - ❑ Siehe „**Checkliste für die Installation**“ auf **Seite 6**.
 - ❑ Weitere Informationen finden Sie unter **www.qlogic.com**.
- **Fettgedruckter** Text weist auf Elemente der Benutzeroberfläche hin, wie z. B. Menüelemente, Schaltflächen, Kontrollkästchen oder Spaltenüberschriften. Zum Beispiel:
 - ❑ Klicken Sie auf die Schaltfläche **Start**, zeigen Sie auf **Programms** (Programme), zeigen Sie auf **Accessories** (Zubehör) und klicken Sie dann auf **Command Prompt** (Eingabeaufforderung).
 - ❑ Markieren Sie unter **Notification Options** (Benachrichtigungsoptionen) das Kontrollkästchen **Warning Alarms** (Warnalarme).

- Text in der Schriftart *Courier* weist auf einen Dateinamen, einen Verzeichnispfad oder Text in der Befehlszeile hin. Zum Beispiel:
 - ❑ Um von einem beliebigen Punkt in der Datenstruktur zum Stammverzeichnis zurückzukehren, geben Sie `cd /root` ein und drücken auf die EINGABETASTE.
 - ❑ Geben Sie den folgenden Befehl aus: `sh ./install.bin`
- Namen und Anschläge von Tasten sind in GROßBUCHSTABEN dargestellt:
 - ❑ Drücken Sie die Tasten STRG+P.
 - ❑ Drücken Sie die UP ARROW (Nach Oben)-Taste.
- *Kursiver* Text weist auf Begriffe, Hervorhebungen, Variablen oder Dokumententitel hin. Zum Beispiel:
 - ❑ Eine vollständige Liste der Lizenzen finden Sie in *QLogic Software End User License Agreement (Endbenutzer-Lizenzvereinbarung der QLogic Software)*.
 - ❑ Was sind *Tastaturbefehle*?
 - ❑ Um den Datumstyp *mm/tt/jjjj* einzugeben (wobei *mm* der Monat, *tt* der Tag und *jjjj* das Jahr ist).
- Thementitel in Anführungszeichen weisen auf miteinander verbundene Themen entweder innerhalb dieses Handbuchs oder in der Onlinehilfe hin, welche in diesem Dokument auch als *das Hilfesystem* bezeichnet wird.

Herunterladen von Dokumenten

Gehen Sie wie folgt vor, um die QLogic-Dokumente herunterzuladen, die in diesem Handbuch genannt werden:

1. Gehen Sie auf die Website www.cavium.com und klicken Sie dort auf **Downloads** oder zeigen auf **Downloads**. Klicken Sie dann in der Liste der OEMs auf **QLogic**.
2. Klicken Sie im ersten Feld auf **Converged Network Adapters** (Konvergierte Netzwerkadapter).
3. Klicken Sie im zweiten Feld auf **QLE8442**.
4. Klicken Sie im dritten Feld auf **Windows Server 2016 (x64)**.
5. Klicken Sie auf **Go** (Los).
6. Klicken Sie im Abschnitt „Documentation“ (Dokumentation) auf die entsprechende Dokumentüberschrift.

Laser-Sicherheitsinformationen

Dieses Produkt kann mit optischen Transceivern der Laserklasse 1 Daten über die Glasfaserleiter austauschen. Das Gesundheitsministerium der USA (Department of Health and Human Services, DHHS) stuft Klasse 1-Laser nicht als gefährlich ein. Die IEC-Norm 825 (Sicherheit von Lasereinrichtungen) verlangt, dass Produkte mit Klasse 1-Lasern entsprechende Aufkleber in den Sprachen Englisch, Deutsch, Finnisch und Französisch tragen. Da eine Kennzeichnung der Transceiver unzureichend ist, liegt der folgende Aufkleber diesem Handbuch bei.



1

Funktionen und Merkmale

In diesem Kapitel werden folgende Themen zu den Adaptern behandelt:

- Funktionsbeschreibung
- „Merkmale und Funktionen“ auf Seite 2
- „Unterstützte Betriebsumgebungen“ auf Seite 6
- „Netzwerkverbindung und Betriebsanzeige“ auf Seite 7

Funktionsbeschreibung

Der QLogic BCM57xx und BCM57xxx-Adapter stellt eine neue Klasse von konvergierten Netzwerkschnittstellen-Controllern (C-NIC) für Gigabit Ethernet (GbE) und 10 GbE dar. Auf einem Standard-Ethernet-Netzwerk können gleichzeitig beschleunigte Datennetzwerke und Speichernetzwerke ausgeführt werden. Der konvergierte Netzwerkschnittstellen-Controller beschleunigt gängige Protokolle, die in Datacentern verwendet werden, wie:

- TOE (TCP Offload Engine) zur Beschleunigung von TCP über 1 GbE und über 10 GbE
- iSCSI-Entlastung (Internet Small Computer Systems Interface) zur Beschleunigung des Netzwerkspeicherzugriffs mit einer zentralen Boot-Funktion (iSCSI-Boot).
- FCoE-Entlastung (Fibre Channel over Ethernet) und Beschleunigung für Fibre Channel-Blockspeicherung

ANMERKUNG

Nicht alle Adapter unterstützen jedes aufgeführte Protokoll. Lesen Sie das jeweilige Produktdatenblatt, um zu erfahren, welche Protokolle unterstützt werden.

Unternehmensnetzwerke, die verschiedene Protokolle und Netzwerkstrukturen verwenden, profitieren von der Fähigkeit der konvergierten Netzwerkschnittstellen-Controller, Datenkommunikationen, Speicher und Clustering über eine einzige Ethernet-Struktur zu kombinieren, indem die Verarbeitungsleistung der CPU und die Speicherverwendung optimiert und gleichzeitig E/A-Engpässe ausgeglichen werden.

Der QLogic BCM57xx und BCM57xxx-Adapter beinhaltet ein 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s oder 10 GBit/s Ethernet MAC mit Halb- und Vollduplexfunktionen sowie eine 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s oder 10 GBit/s physische Schicht (PHY). Der Transceiver ist vollständig mit dem IEEE-Standard 802.3 kompatibel und ermöglicht eine automatische Aushandlung der Übertragungsrates.

Mithilfe der QLogic Teaming-Software können Sie Ihr Netzwerk in virtuelle LANs (VLANs) aufteilen sowie mehrere Netzwerkadapter in Teams zusammenfassen, um die Funktionen für den Netzwerk-Lastausgleich und die Fehlertoleranz zu erhalten.

- Detaillierte Informationen zu Teaming finden Sie unter [Kapitel 2 Konfigurieren von Teaming auf einem Windows Server](#) und [Kapitel 11 QLogic Teaming Services](#).
- Eine Beschreibung von VLANs finden Sie unter [Kapitel 3 Virtuelle LANs bei Windows](#).

Merkmale und Funktionen

Im Folgenden erhalten Sie eine Liste der Leistungsmerkmale des QLogic BCM57xx und BCM57xxx-Adapters. Einige Funktionen stehen möglicherweise nicht bei allen Adaptern zur Verfügung.

- TOE (TCP Offload Engine)
- iSCSI-Offload (siehe „iSCSI“ auf Seite 4)
- FCoE (Fibre Channel over Ethernet) (siehe „FCoE“ auf Seite 5)
- NIC-Partitionierung (NPAR)
- DCB (Data Center Bridging):
 - ETS (Enhanced Transmission Selection, IEEE 802.1Qaz)
 - PFC (Priority-based Flow Control, IEEE 802.1Qbb)
 - DCBX (Data Center Bridging Capability eXchange Protocol, CEE-Version 1.01)
- Single-Chip-Lösung:
 - 100/1000/10G-MAC für dreifache Übertragungsrates

- 1G/10G-MAC für dreifache Übertragungsrate
- Serializer/Deserialize (SerDes)-Schnittstelle für optischen Transceiver-Anschluss
- PCI Express® Gen3 x8 (nur 10 GbE BCM57840)
- Hardware ohne Zwischenspeicherung
- Weitere Leistungsmerkmale:
 - TCP-, IP-, UDP-Prüfsumme
 - TCP-Segmentierung
 - Adaptive Interrupts (siehe [„Adaptive Interrupt-Frequenz“ auf Seite 6](#))
 - Receive Side Scaling (RSS)
- Verwaltungsfunktionen:
 - QLogic Control Suite (QCS) - Software-Suite für Diagnose und Konfiguration (siehe [„QLogic Control Suite-Befehlszeilenschnittstelle“ auf Seite 6](#))
 - Unterstützt die PXE 2.0 Spezifikation
 - Unterstützung für Wake on LAN (WoL)
 - UMP-Unterstützung (Universal Management Port)
 - SMBus-Controller
 - Erweiterte Konfigurations- und Energieverwaltungsschnittstelle (ACPI) 1.1a-kompatibel (mehrere Stromverbrauchsmodi) (siehe [„Energieverwaltung“ auf Seite 5](#))
 - Unterstützung für Intelligent platform management interface (Intelligente Plattformmanagement-Schnittstelle) (IPMI)
- Erweiterte Netzwerkfunktionen:
 - Jumbo-Frames (bis zu 9.600 Byte). Das Betriebssystem und der Verbindungspartner müssen Jumbo-Frames unterstützen.
 - Virtuelle LANs
 - IEEE-Standard 802.3ad-Teaming
 - Smart Load Balancing™-Teaming
 - Flusssteuerung (IEEE-Standard 802.3x)
 - LiveLink™ (wird von den 32-Bit- und 64-Bit-Windows-Betriebssystemen unterstützt)
- Logische Verbindungssteuerung (LLC) (IEEE-Standard 802.2)

- High-Speed-On-Chip Prozessoren für Rechner mit beschränktem Befehlssatz (RISC) (siehe „ASIC mit eingebettetem RISC-Prozessor“ auf Seite 6)
- Integrierter Frame-Zwischenspeicher mit einer Größe von 96 KB
- Quality of Service (QoS)
- Managementschnittstelle serielle Gigabit medienunabhängige Schnittstelle (SGMII), Gigabit medienunabhängige Schnittstelle (GMII) und medienunabhängige Schnittstelle (MII)
- 256 eindeutige MAC-Unicast-Adressen
- Unterstützung von Multicast-Adressen über 128-Bit-Hardware-Streufunktion
- Serieller NVRAM-Flash-Speicher
- Unterstützung von JTAG
- PCI Power-Management-Schnittstelle (V1.1)
- Unterstützung für 64-Bit-Basisadressregisters (BAR)
- Prozessorunterstützung von EM64T
- iSCSI und FCoE Boot-Unterstützung
- Virtualisierung:
 - Microsoft®
 - VMware®
 - Linux®
 - XenServer®
- Single Root I/O-Virtualisierung (SR-IOV)

iSCSI

Die Internet Engineering Task Force (IETF) hat einen Standard für iSCSI entwickelt. *SCSI* ist ein häufig eingesetztes Protokoll, bei dem Systeme per Blockdatenübertragung (also anhand von auf einem Speichergerät gespeicherten Adresdaten, die keine gesamte Datei darstellen) mit Speichergeräten kommunizieren können. *iSCSI* ordnet die Anwendungsprotokolle für SCSI-Anfragen/Antworten und dessen standardisierten Befehlssatz über TCP/IP-Netzwerke zu.

Da iSCSI als Transportprotokoll ausschließlich TCP verwendet, werden durch die Hardwarebeschleunigung der TCP-Verarbeitung erhebliche Vorteile erzielt. iSCSI als Layer-5-Protokoll verfügt jedoch über das TCP-Layer hinaus über weitere Verfahren. Die iSCSI-Verarbeitung kann auch entlastet werden, wodurch sich die CPU-Nutzung weiter reduziert.

Der QLogic BCM57xx und BCM57xxx-Adapter zielt auf eine optimale Systemleistung, sichert die Flexibilität des Systems für erforderliche Änderungen und unterstützt aktuelle und zukünftige Möglichkeiten der Konvergenz und Integration von Betriebssystemen. Die Architektur zur iSCSI-Entlastung des Adapters ist damit unerreichbar, was durch die Trennung von Hardware und Host-Verarbeitung deutlich wird.

FCoE

Mit FCoE können Fibre Channel-Daten über Ethernet übertragen werden. FCoE bewahrt die vorhandene Fibre Channel-Infrastruktur sowie Kapitalanlagen. Die folgenden FCoE-Funktionen werden unterstützt:

- Vollständig zustandbehaftete Hardware-FCoE-Entlastung
- Receiver-Klassifizierung von FCoE- und FCoE Initialization Protocol (FIP)-Frames. FIP wird zur Herstellung und Aufrechterhaltung von Verbindungen verwendet.
- Receiver-CRC-Verschiebung
- Transmitter-CRC-Verschiebung
- Spezielle Warteschlange für Fibre Channel-Datenverkehr
- Data Center Bridging (DCB) sorgt für verlustfreie Übertragungen mit Priority Flow Control (PFC).
- DCB weist dem FCoE-Datenverkehr per Enhanced Transmission Selection (ETS) eine bestimmte Verbindungsbandbreite zu.
- Unterstützt die Spezifikation *Fibre Channel - Link Services (FC-LS)* des Technical Committee T11, N_Port-ID-Virtualisierung (NPIV) auf Linux und Windows.

Energieverwaltung

Die Einstellung der Adaptergeschwindigkeit orientiert sich an der konfigurierten Geschwindigkeit für WOL, wenn das System ausgeschaltet ist.

ANMERKUNG

Dell™ unterstützt WOL jeweils nur auf einem Adapter im System. Informationen zur Unterstützung von WOL auf bestimmten Systemen finden Sie in der Dokumentation zu Ihrem System.

Adaptive Interrupt-Frequenz

Der Adaptertreiber passt die Host-Interrupt-Frequenz je nach den Datenverkehrsbedingungen intelligent an, um den Gesamtdurchsatz der Anwendungen zu erhöhen. Bei geringem Datenverkehr generiert der Adaptertreiber für jedes empfangene Paket einen Interrupt auf dem Host und verringert so die Latenz. Bei hohem Datenverkehr generiert der Adapter einen Host-Interrupt für mehrere eingehende Back-to-Back-Pakete und trägt so zum Erhalt der CPU-Zyklen des Hosts bei.

ASIC mit eingebettetem RISC-Prozessor

Die Kernsteuerung für den QLogic BCM57xx und BCM57xxx-Adapter befindet sich in einem eng integrierten Hochleistungs-ASIC. Der ASIC umfasst einen RISC-Prozessor, der die notwendige Flexibilität bietet, um durch Software-Downloads neue Funktionen zur Karte hinzufügen und sie an künftige Netzwerkanforderungen anpassen zu können. Gleichzeitig wird es den Treibern des Adapters ermöglicht, die im Adapter integrierten Host-Entlastungsfunktionen zu nutzen, sobald die Host-Betriebssysteme in der Lage sind, diese Funktionen einzusetzen.

QLogic Control Suite-Befehlszeilenschnittstelle

Die QLogic Control Suite (QCS)-Befehlszeilenschnittstelle stellt nützliche Informationen über jeden der auf dem System installierten Netzwerkadapter zur Verfügung. Mit dem QCS-Dienstprogramm können Sie außerdem ausführliche Tests, Diagnosen und Analysen für jeden Adapter vornehmen sowie die Eigenschaftswerte für die einzelnen Adapter ändern und die Netzwerkstatistiken anzeigen.

Unterstützte Betriebsumgebungen

Der QLogic BCM57xx und BCM57xxx-Adapter wird von den folgenden Betriebssystemen unterstützt:

- Microsoft Windows (32-Bit- und 64-Bit-Erweiterungen)
- Linux (64-Bit extended)
- ESXi™ Server (VMware)
- Citrix® XenServer

Netzwerkverbindung und Betriebsanzeige

Bei Ethernet-Anschlüssen über Kupferdraht wird der Status der Netzwerkverbindung und des Netzwerkbetriebs wie unter [Tabelle 1-1](#) beschrieben durch die LEDs am Anschluss RJ45 angezeigt.

Tabelle 1-1. Port-LED-Anzeige des RJ45 für Netzwerkverbindung und -betrieb

Port-LED	LED-Anzeige	Netzwerkstatus
Link-LED	Aus	Keine Verbindung (Kabel abgetrennt)
	Leuchtet konstant	Verbindung
Aktivitäts-LED	Aus	Kein Netzwerkbetrieb
	Blinkend	Netzwerkbetrieb

Bei Ethernet-Anschlüssen über Lichtwellenleiter und SFP+ wird der Status der Netzwerkverbindung und des Netzwerkbetriebs, wie unter [Tabelle 1-2](#) beschrieben, durch eine LED neben dem Portanschluss angezeigt.

Tabelle 1-2. Port-LED-Anzeige für Netzwerkverbindung und -betrieb

LED-Anzeige	Netzwerkstatus
Aus	Keine Verbindung (Kabel abgetrennt)
Leuchtet konstant	Verbindung
Blinkend	Netzwerkbetrieb

QLogic Control Suite liefert darüber hinaus Informationen zum Status der Netzwerkverbindung und des Betriebs.

2 Konfigurieren von Teaming auf einem Windows Server

Die Teaming-Konfiguration in einem Microsoft Windows Server®-System umfasst einen Überblick über QLogic Advanced Server Program (QLASP), Lastausgleich und Fehlertoleranz. Windows Server ab Version 2016 bietet keine Unterstützung der QLASP-Treiber von QLogic mehr.

- [QLASP Übersicht](#)
- [„Lastausgleich und Fehlertoleranz“ auf Seite 9](#)

ANMERKUNG

Dieses Kapitel beschreibt das Teaming für Adapter bei Windows Server-Systemen. Weitere Informationen zu einer ähnlichen Technologie bei Linux-Betriebssystemen (namens „Channel Bonding“) finden Sie in der Dokumentation zu Ihrem Betriebssystem.

QLASP Übersicht

QLASP ist die QLogic-Teaming-Software für die Windows-Betriebssystemfamilie. Die QLASP-Einstellungen werden über die QLogic Control Suite (QCS)-Befehlszeilenschnittstelle konfiguriert.

QLASP bietet heterogene Unterstützung für Adapter-Teaming für Dell-BCM57xx und BCM57xxx-Adapter sowie für Dell-Geräte mit Intel Netzwerkkarten-Adaptoren und LANs auf Motherboards (LOMs).

QLASP unterstützt vier Teamarten für Schicht-2-Teaming:

- Smart Load Balancing und Failover
- Link Aggregation (802.3ad)
- Allgemeines Trunking (Generic EtherChannel [GEC] und Fast EtherChannel [FEC]) und 802.3ad-Draft Static
- SLB (Auto-Fallback deaktiviert)

Weitere Informationen zu Teamingkonzepten für Netzwerkadapter finden Sie unter [Kapitel 11 QLogic Teaming Services](#).

ANMERKUNG

Windows Server 2012 und höher bieten integrierten Teaming-Support, das *NIC-Teaming*. QLogic empfiehlt, dass Benutzer nicht QLASP gleichzeitig bei mehreren Adaptern Teams über NIC-Teaming und BASP aktivieren.

Windows Server 2016 bietet keine Unterstützung des QLASP-Teaming-Treibers von QLogic mehr.

Lastausgleich und Fehlertoleranz

Die Teaming-Funktion bietet einen Ausgleich der Datenverkehrslast sowie eine Fehlertoleranz: redundanter Adapterbetrieb bei Ausfall einer Netzwerkverbindung. Sind mehrere Gigabit Ethernet-Netzwerkadapter auf dem gleichen System installiert, können Sie diese in Teams zusammenfassen und somit einen virtuellen Adapter erstellen.

Ein Team kann aus zwei bis acht Netzwerkkarten-Schnittstellen bestehen, wobei jeder Schnittstelle der Status einer primären Schnittstelle oder einer Standby-Schnittstelle zugewiesen werden kann. (Standby-Schnittstellen können nur in einem Team der Art [Smart Load Balancing und Failover](#) verwendet werden und nur eine Standby-Schnittstelle kann pro SLB-Team bestimmt werden.) Wird bei einer der Verbindungen des Adapter-Teams kein Datenverkehr festgestellt, weil ein Adapter, ein Kabel, ein Switch-Port oder - bei Anbindung der Adapter eines Teams an unterschiedliche Switches - ein Switch ausgefallen ist, wird die Lastverteilung neu ausgewertet und den verbleibenden Teammitgliedern zugewiesen. Sollten alle Primäradapter ausfallen, wird der Hot Standby-Adapter aktiviert. Die bestehenden Sitzungen bleiben erhalten, und die Situation hat keinerlei Auswirkungen auf die Benutzer.

ANMERKUNG

Sie können zwar ein Team mit einem Adapter erstellen, jedoch empfiehlt QLogic dieses Vorgehen nicht, da dies dem eigentlichen Zweck des Teamings widerspricht. Ein aus einem Adapter bestehendes Team wird automatisch beim Einrichten von VLANs auf einem einzigen Adapter erstellt, und dies sollte das einzige Mal sein, dass ein Team mit nur einem Adapter erstellt wird.

Teamarten

Es sind folgende Teamarten für Windows-Betriebssysteme verfügbar:

- [Smart Load Balancing und Failover](#)
- [Link Aggregation \(802.3ad\)](#)
- [Allgemeines Trunking \(FEC/GEC\)/802,3ad-Draft Static](#)
- [SLB \(Auto-Fallback deaktiviert\)](#)

Smart Load Balancing und Failover

Smart Load Balancing und Failover ist das von Broadcom® implementierte Verfahren zum Lastausgleich und basiert auf dem IP-Fluss. Mit dieser Funktion kann der IP-Verkehr bidirektional über mehrere Adapter (Teammitglieder) ausgeglichen werden. Bei dieser Teamart verfügen alle Adapter des Teams über separate MAC-Adressen. Diese Teamart ermöglicht die automatische Fehlererkennung und eine dynamische Ausfallsicherung durch ein anderes Teammitglied oder ein Hot Standby-Element. Failover erfolgt unabhängig vom Schicht-3-Protokoll (IP, IPX und NetBIOS erweiterte Benutzerschnittstelle [NetBEUI]) bzw. kann in Verbindung mit vorhandenen Schicht-2- und Schicht-3-Switches verwendet werden. Für diese Teamart ist keine Switch-Konfiguration (wie Trunking oder Link Aggregation) erforderlich.

ANMERKUNG

- Wenn Sie LiveLink beim Konfigurieren von SLB-Teams nicht aktivieren, empfiehlt QLogic, das Spanning Tree Protocol (STP) am Switch oder Anschluss zu deaktivieren oder Port Fast am Switch oder Anschluss zu aktivieren. Dadurch werden die Ausfallzeiten beim Failover auf Grund der Schleifen-Berechnung nach dem Spanning Tree-Algorithmus reduziert. Probleme dieser Art werden von LiveLink entschärft.
 - TCP/IP führt einen kompletten Lastausgleich durch, und Internetwork Packet Exchange (IPX) führt nur einen Lastausgleich auf der Übertragungsseite des Teams durch. Andere Protokolle sind auf den Primäradapter beschränkt.
 - Wenn die Übertragungsrate der Verbindung bei einem Teammitglied höher ist als bei einem anderen, wird der größte Teil des Datenverkehrs von dem Teammitglied mit der höheren Verbindung bewältigt.
-

Link Aggregation (802.3ad)

Der Link Aggregation-Modus unterstützt Link Aggregation und entspricht dem IEEE-Standard 802.3ad (LACP). Mit der Konfigurationssoftware können Sie dynamisch festlegen, welche Adapter einem bestimmten Team angehören. Wenn der Verbindungspartner nicht richtig für die Verbindungskonfiguration 802,3ad konfiguriert ist, werden die Fehler erkannt und protokolliert. In diesem Modus sind alle Adapter für den Empfang von Paketen unter derselben MAC-Adresse konfiguriert. Das Lastausgleichsschema für den ausgehenden Datenverkehr wird durch den QLASP-Treiber von QLogic bestimmt. Das Lastausgleichsschema für ankommende Datenpakete wird dagegen durch den Verbindungspartner des Teams festgelegt. In diesem Modus muss mindestens einer der Verbindungspartner aktiv sein.

ANMERKUNG

Die statische und dynamische Teamart für die Link Aggregation (Switch-abhängig) wird auf Ports, auf denen der NIC-Partitionsmodus (NPAR) oder iSCSI-Offload aktiviert ist, nicht unterstützt. Manche Switches unterstützen FCoE-Offload im dynamischen LACP Teaming-Modus. Weitere Informationen erhalten Sie in Ihrer Switchdokumentation.

Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static

Die Teamart Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static ist der Teamart Link Aggregation (802.3ad) in der Hinsicht sehr ähnlich, dass alle Adapter des Teams für den Empfang von Paketen unter derselben MAC-Adresse konfiguriert werden. Die Teamart Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static bietet jedoch keine LACP- oder Marker-Protokoll-Unterstützung. Diese Teamart unterstützt eine Vielzahl von Umgebungen, in denen die Adapterverbindungspartner zur Unterstützung eines proprietären Trunking-Verfahrens statisch konfiguriert sind. Mit dieser Teamart könnte beispielsweise OpenTrunk™ von Lucent® oder Fast EtherChannel (FEC) von Cisco® unterstützt werden. Bei der Teamart Allgemeines Trunking handelt es sich im Prinzip um eine vereinfachte Version der 802.3ad Link Aggregation. Der hier zugrunde liegende Ansatz ist wesentlich einfacher, da kein formalisiertes Link Aggregation-Steuerungsprotokoll (LACP) verwendet wird. Wie bei anderen Teamarten erfolgen die Teamerstellung und die Zuordnung der physischen Adapter zu den verschiedenen Teams statisch über die Benutzerkonfigurations-Software.

Die Teamart Allgemeines Trunking (FEC/GEC/802.3ad-Draft Static) unterstützt Load Balancing (Lastausgleich) und Failover (Ausfallsicherung) für den ankommenden und abgehenden Datenverkehr.

ANMERKUNG

Die Teamart Allgemeines Trunking (FEC/GEC/802.3ad-Draft Static) wird für Ports mit aktiviertem NPAR-Modus, FCoE-Offload-Modus oder iSCSI-Offload-Modus nicht unterstützt.

SLB (Auto-Fallback deaktiviert)

Die Teamart „SLB“ (Auto-Fallback deaktiviert) ist mit den Teamarten „Smart Load Balancing“ und „Failover“ identisch, bis auf die folgende Ausnahme: Wenn das Standby-Element aktiv ist und ein primäres Mitglied die Verbindung wiederhergestellt hat, verwendet das Team weiterhin das Standby-Element, anstatt wieder auf das primäre Mitglied umzuschalten.

Alle primären Schnittstellen in einem Team sind durch das Senden und Empfangen von Teilmengen des gesamten Datenverkehrs an Lastausgleichsvorgängen beteiligt. Standby-Schnittstellen übernehmen diese Funktion, wenn die Verbindungen für alle primären Schnittstellen unterbrochen werden.

Das Failover-Teaming ermöglicht bei Ausfall einer Netzwerkverbindung einen redundanten Adapterbetrieb (Fehlertoleranz). Wenn die Verbindung des Primäradapters in einem Team aufgrund eines Adapter-, Kabel- oder Switch-Port-Ausfalls unterbrochen wird, wird das sekundäre Teammitglied aktiviert und leitet sowohl den ankommenden als auch den abgehenden Datenverkehr, der ursprünglich dem Primäradapter zugewiesen wurde, weiter. Sitzungen bleiben erhalten, und die Situation hat keinerlei Auswirkungen auf die Benutzer.

Einschränkungen bei den Teamarten Smart Load Balancing, Failover und SLB (Auto-Fallback deaktiviert)

Bei Smart Load-Balancing (SLB) handelt es sich um ein Schema für ein bestimmtes Protokoll. Der Umfang der Unterstützung für die IP wird in [Tabelle 2-1](#) aufgeführt.

Tabelle 2-1. Smart Load Balancing

Betriebssystem	Failover und Fallback: Nur Dell	Failover und Fallback: Herstellerunabhängig
Protokoll	IP	IP
Windows Server 2008	Ja	Ja
Windows Server 2008 R2	Ja	Ja
Windows Server 2012 und 2012 R2	Ja	Ja
Betriebssystem	Lastausgleich: Nur Dell	Lastausgleich: Herstellerunabhängig
Protokoll	IP	IP
Windows Server 2008	Ja	Ja
Windows Server 2008 R2	Ja	Ja
Windows Server 2012 und 2012 R2	Ja	Ja

Die Teamart Smart Load Balancing funktioniert mit allen Ethernet-Switches, ohne dass die Switch-Ports für einen bestimmten Trunking-Modus konfiguriert werden müssen. Nur IP-Verkehr wird für sowohl für den ankommenden als auch für den abgehenden Datenverkehr dem Lastausgleich unterzogen. IPX-Verkehr wird für abgehenden Datenverkehr dem Lastausgleich unterzogen. Andere Protokollpakete werden über eine primäre Schnittstelle gesendet und empfangen. Failover für Nicht-IP-Verkehr wird nur bei Verwendung von Dell-Netzwerkadaptern unterstützt. Die Teamart Allgemeines Trunking erfordert, dass der Ethernet-Switch eine Form des Port-Trunking-Modus unterstützt (z. B. den Modus Gigabit EtherChannel von Cisco oder den Modus Link Aggregation anderer Hersteller von Switches). Diese Teamart ist protokollunabhängig. Sämtlicher Datenverkehr sollte fehlertolerant sein und dem Lastausgleich unterzogen werden.

ANMERKUNG

Wenn Sie LiveLink beim Konfigurieren von SLB-Teams nicht aktivieren, empfiehlt QLogic, STP am Switch zu deaktivieren oder Port Fast am Switch zu aktivieren. Dadurch werden die Ausfallzeiten beim Failover auf Grund der Schleifen-Berechnung nach dem Spanning Tree-Algorithmus reduziert. Probleme dieser Art werden von LiveLink entschärft.

Unterstützung für Teaming und Large Send Offload und Checksum Offload (Large-Send-Verschiebung und Prüfsummenverschiebung)

Large Send Offload (LSO) und die Prüfsummenverschiebung (CO) werden nur dann für ein Team aktiviert, wenn alle Mitglieder diese Funktionen unterstützen und dafür konfiguriert wurden.

3 Virtuelle LANs bei Windows

Dieses Kapitel enthält Informationen zu VLANs für Teaming in Windows.

- [VLAN-Überblick](#)
- [„Hinzufügen von VLANs zu Teams“ auf Seite 17](#)

VLAN-Überblick

Mit virtuellen LANs (VLANs) können Sie das physische LAN logisch unterteilen, Arbeitsgruppen logisch segmentieren und für jedes logische Segment Sicherheitsrichtlinien festlegen. Jedes definierte VLAN verhält sich wie ein separates Netzwerk, dessen Datenverkehr und Broadcasts von den anderen Netzwerken getrennt sind, so dass die Bandbreiteneffizienz innerhalb der einzelnen logischen Gruppen erhöht wird. Für jeden QLogic-Adapter auf dem Server können Sie bis zu 64 VLANs (63 markierte und 1 unmarkiertes) definieren, je nachdem, wie viel Speicherplatz im System verfügbar ist.

VLANs können zu Teams hinzugefügt werden, um mehrere VLANs mit unterschiedlichen VLAN-IDs zu ermöglichen. Für jedes hinzugefügte VLAN wird ein virtueller Adapter erstellt.

VLANs werden normalerweise verwendet, um einzelne Broadcast-Domänen und separate IP-Teilnetze einzurichten. Es kann sich jedoch unter Umständen als nützlich erweisen, wenn ein Server gleichzeitig in mehreren VLANs verfügbar ist. QLogic-Adapter unterstützen mehrere VLANs auf Port- oder auf Teambasis und ermöglichen so äußerst flexible Netzwerkkonfigurationen.

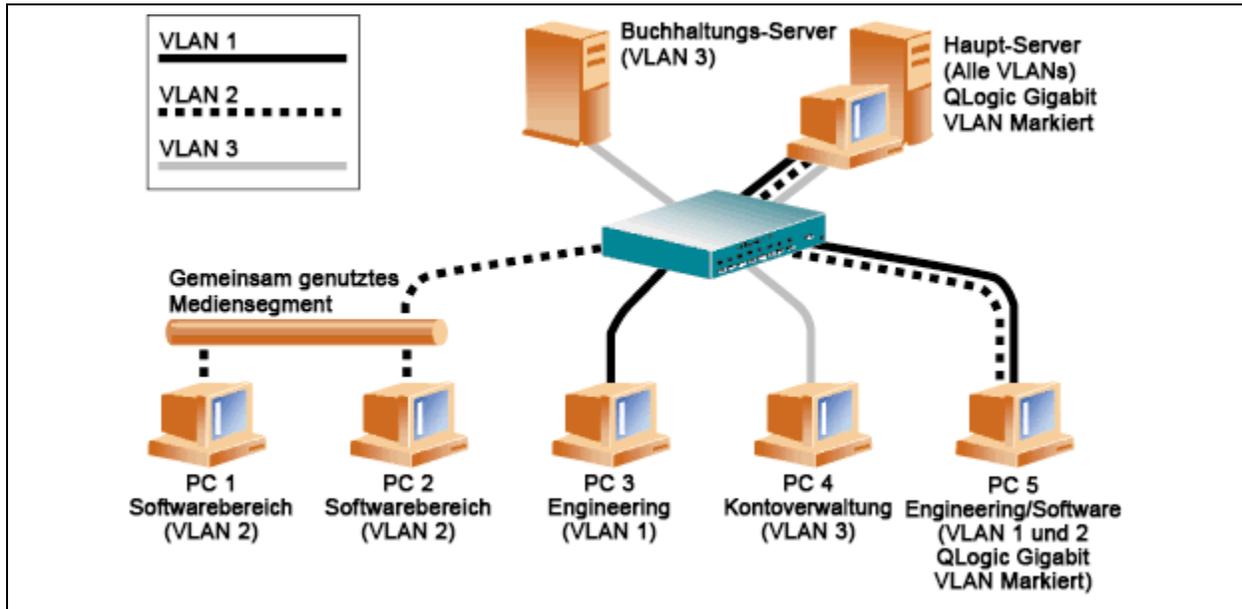


Abbildung 3-1. Beispiel für die Unterstützung mehrerer markierter VLANs durch Server

Abbildung 3-1 zeigt ein Netzwerk mit mehreren VLANs. In diesem Netzwerk besteht das physische LAN aus einem Switch, zwei Servern und fünf Clients. Das LAN ist logisch in drei verschiedene VLANs unterteilt, von denen jedes ein anderes IP-Subnetz darstellt. Die Funktionen dieses Netzwerks werden in Tabelle 3-1 beschrieben.

Tabelle 3-1. Beispiel für eine VLAN-Netzwerktopologie

Komponente	Beschreibung
VLAN 1	IP-Subnetz, das den Haupt-Server, PC 3 und PC 5 umfasst. Dieses Subnetz stellt eine Technikergruppe dar.
VLAN 2	Umfasst den Haupt-Server, PC 1 und PC 2 (über ein gemeinsam genutztes Mediensegment) sowie PC 5. Bei diesem VLAN handelt es sich um eine Software-Entwicklergruppe.
VLAN 3	Umfasst den Haupt-Server, den Buchhaltungs-Server und PC 4. Bei diesem VLAN handelt es sich um eine Buchhaltungsgruppe.

Tabelle 3-1. Beispiel für eine VLAN-Netzwerktopologie (fortgesetzt)

Komponente	Beschreibung
Primärer Name-server	Ein sehr häufig verwendeter Server, der von allen VLANs und IP-Subnetzen aus erreichbar sein muss. Auf dem Haupt-Server ist ein QLogic-Adapter installiert. Der Zugriff auf die drei IP-Teilnetze erfolgt über eine physische Adapterschnittstelle. Der Server ist mit einem Switch-Port verbunden, der für VLAN 1, 2 und 3 konfiguriert ist. Sowohl für den Adapter als auch für den verbundenen Switch-Port ist die Markierung aktiviert. Da beide Geräte in der Lage sind, VLANs zu markieren, kann der Server über alle drei IP-Subnetze in diesem Netzwerk kommunizieren, behandelt die drei Subnetze beim Broadcasting aber weiterhin als separate Einheiten.
Buchhaltungs-Server	Nur für VLAN 3 verfügbar. Der Buchhaltungs-Server ist vom gesamten Datenverkehr in VLAN 1 und VLAN 2 getrennt. Bei dem an dieses Segment angeschlossenen Switch-Port ist die Markierung deaktiviert.
PC 1 und 2	Sind an einen gemeinsam genutzten Medien-Hub angeschlossen, der wiederum mit dem Switch verbunden ist. PC 1 und PC 2 sind nur in VLAN 2 eingebunden und befinden sich logisch im gleichen IP-Teilnetz wie der Haupt-Server und PC 5. Bei dem an dieses Segment angeschlossenen Switch-Port ist die Markierung deaktiviert.
PC 3	PC 3 ist in VLAN 1 eingebunden und kann nur mit dem Haupt-Server und PC 5 kommunizieren. Bei dem Switch-Port von PC 3 ist die Markierung deaktiviert.
PC 4	PC 4 ist in VLAN 3 eingebunden und kann nur mit den Servern kommunizieren. Bei dem Switch-Port von PC 4 ist die Markierung deaktiviert.
PC 5	PC 5 ist in VLAN 1 und VLAN 2 eingebunden und verfügt über einen QLogic-Adapter. Er ist an Switch-Port 10 angeschlossen. Der Adapter und der Switch-Port sind für VLAN 1 und VLAN 2 konfiguriert, und bei beiden ist die Markierung aktiviert.

ANMERKUNG

Das Markieren von VLANs muss nur bei Switch-Ports, die Trunk-Verbindungen zu anderen Switches herstellen, oder Ports, die an markierungsfähige Endstationen (z. B. Server oder Workstations) mit QLogic-Adaptoren angeschlossen sind, aktiviert sein.

Erstellen Sie bei Hyper-V® VLANs in der vSwitch-to-VM-Verbindung statt in einem Team, damit VM-Livemigrationen möglich sind, ohne sicherstellen zu müssen, dass die VLAN-Einrichtung des Teams im zukünftigen Hostsystem diesem entspricht.

Hinzufügen von VLANs zu Teams

Jedes Team unterstützt bis zu 64 VLANs (63 markierte und 1 unmarkiertes). Zum Einrichten von Teams mit VLANs können nur QLogic-Adapter und Alteon® AceNIC-Adapter verwendet werden. Sind mehrere VLANs mit einem Adapter verbunden, können Sie einen Server in mehreren IP-Subnetzen logisch verfügbar machen. Sind mehrere VLANs in ein Team eingebunden, können Sie einen Server in mehreren IP-Subnetzen verfügbar machen und die Vorteile der Lastausgleich- und Failover-Funktionen nutzen.

ANMERKUNG

Sie können Adapter konfigurieren, die zu einem Failover-Team gehören, damit diese ebenfalls VLANs unterstützen. Intel LOMs unterstützen keine VLANs. Wenn ein Failover-Team ein Intel LOM umfasst, können Sie keine VLANs für dieses Team konfigurieren.

4 Installieren der Hardware

Dieses Kapitel bezieht sich auf die QLogic BCM57xx und BCM57xxx-Add-In-Netzwerkkarten. Die Hardware-Installation umfasst Folgendes:

- [Systemanforderungen](#)
- [„Sicherheitsvorkehrungen“ auf Seite 20](#)
- [„Vor der Installation - Checkliste“ auf Seite 20](#)
- [„Installation der zusätzlichen Netzwerkkarte“ auf Seite 21](#)

ANMERKUNG

Service Personnel (Wartungspersonal): Dieses Produkt ist nur zur Installation an einem Standort mit Zugangsbeschränkung (RAL) konzipiert.

Systemanforderungen

Bevor Sie QLogic BCM57xx und BCM57xxx-Adapter installieren, stellen Sie sicher, dass Ihr Computer die Voraussetzungen für die Hardware und das Betriebssystem erfüllt.

Hardwareanforderungen

- Ein IA32- oder EMT64-basierter Computer, der die Anforderungen an das Betriebssystem erfüllt
 - Ein geöffneter PCI Express-Steckplatz. Abhängig von der PCI Express-Unterstützung für Ihren Adapter ist der Steckplatz möglicherweise einer dieser Typen:
 - PCI Express 1.0a x1
 - PCI Express 1.0a x4
 - PCI Express Gen2 x8
 - PCI Express Gen3 x8
- Volle Dual-Port 10 GBit/s Bandbreite wird auf PCI Express Gen2 x8 oder schnelleren Steckplätzen unterstützt.
- Mindestens 128 MB RAM

Anforderungen an das Betriebssystem

ANMERKUNG

Da das *Dell Update Packages Version xx.xx.xxx User's Guide* nicht im selben Zyklus aktualisiert wird wie das Handbuch dieses Ethernet-Adapters, sind die in diesem Abschnitt aufgeführten Betriebssysteme als die aktuellsten zu betrachten.

Dieser Abschnitt beschreibt die Anforderungen für alle unterstützten Betriebssysteme.

Allgemein

Es ist folgende Host-Schnittstelle erforderlich:

- PCI Express v1.0a, ab x1 Host-Schnittstelle

Microsoft Windows

Eine der folgenden Versionen von Microsoft Windows:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows Server 2008 SP2 x64
- Windows Server 2008 SP2 x32

Linux

Eine der folgenden Versionen von Linux:

- Red Hat Enterprise Linux (RHEL) 7.5
- RHEL 7.4
- RHEL 7.3
- RHEL 7.2
- RHEL 6.9
- RHEL 6.8
- RHEL 6.7
- SUSE Linux Enterprise Server (SLES) 12 SP3
- SLES 12 SP2
- SLES 11 SP4

VMware ESXi

Eine der folgenden Versionen von vSphere® ESXi:

- VMware ESXi 6.7
- VMware ESXi 6.5

- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U1
- VMware ESXi 6.0 U3
- VMware ESXi 6.0 U2

Citrix XenServer

Die folgende Version von XenServer:

- Citrix XenServer 6.5

Sicherheitsvorkehrungen

WARNUNG

Der Adapter wird in ein System installiert, dessen Betriebsspannungen tödlich sein können. Vor dem Entfernen der Systemabdeckung müssen Sie folgende Maßnahmen zum persönlichen Schutz und zur Vermeidung von Schäden an den Systemkomponenten durchführen:

- Entfernen Sie alle Metallobjekte oder Schmuck von Händen und Handgelenken.
- Stellen Sie sicher, dass Sie ausschließlich isolierte bzw. nichtleitende Werkzeuge verwenden.
- Stellen Sie vor dem Berühren interner Komponenten sicher, dass das Gerät ausgeschaltet und der Netzstecker gezogen ist.
- Installieren oder entfernen Sie Adapter in einer Umgebung, die nicht elektrostatisch aufgeladen ist. Das Tragen einer ordnungsgemäß geerdeten Erdungsmanschette am Handgelenk und die Verwendung anderer Antistatik-Geräte sowie einer antistatischen Fußmatte wird ausdrücklich empfohlen.

Vor der Installation - Checkliste

1. Überprüfen Sie, ob Ihr Server die unter „Systemanforderungen“ auf Seite 18 aufgeführten Hardware- und Software-Anforderungen erfüllt.
2. Überprüfen Sie, ob Ihr System das neueste BIOS verwendet.

ANMERKUNG

Falls Sie die Adaptersoftware auf einem Datenträger oder über die Support-Website von Dell (<http://support.dell.com>) erhalten haben, überprüfen Sie den Pfad zu den Adaptertreiberdateien.

3. Wenn Ihr System eingeschaltet ist, fahren Sie es herunter.

4. Wenn das System vollständig heruntergefahren ist, schalten Sie es aus, und ziehen Sie den Netzstecker.
5. Entfernen Sie die Verpackung des Adapters, und legen Sie die Karte auf einer antistatischen Oberfläche ab.
6. Prüfen Sie den Adapter und insbesondere den Stiftsockel auf sichtbare Anzeichen von Schäden. Installieren Sie niemals einen beschädigten Adapter.

Installation der zusätzlichen Netzwerkkarte

Die folgenden Anweisungen gelten für die Installation der QLogic BCM57xx und BCM57xxx-Adapter (zusätzliche Netzwerkkarte) auf den meisten Systemen. Weitere Informationen, wie die Installation auf Ihrem System auszuführen ist, finden Sie in den Handbüchern, die im Lieferumfang Ihres Systems enthalten waren.

Installieren der zusätzlichen Netzwerkkarte

1. Lesen Sie nochmals die Abschnitte [Sicherheitsvorkehrungen](#) und [Vor der Installation - Checkliste](#). Stellen Sie vor dem Installieren des Adapters sicher, dass das System ausgeschaltet und der Netzstecker gezogen ist, und dass entsprechende Erdungsmaßnahmen durchgeführt wurden.
2. Öffnen Sie das Systemgehäuse, und wählen Sie den Steckplatz abhängig vom Adapter aus, wobei der Steckplatz vom Typ PCIe® 1.0a x1, PCIe 1.0a x4, PCIe Gen2 x8, PCIe Gen3 x8 oder ein anderer passender Steckplatz sein könnte. Ein schmalerer Adapter kann in einen breiteren Steckplatz gesteckt werden (x8 in einen x16), aber ein breiterer Adapter kann nicht in einen schmaleren Steckplatz gesteckt werden (x8 in einen x4). Informationen dazu, woran Sie einen PCI-Steckplatz erkennen, finden Sie in Ihrer Systemdokumentation.
3. Entfernen Sie die Abdeckplatte vom ausgewählten Steckplatz.
4. Richten Sie die Steckerleiste des Adapters am PCI Express-Steckplatz des Systems aus.

5. Drücken Sie gleichmäßig auf die beiden Ecken der Karte, und schieben Sie die Adapterkarte in den Steckplatz, bis sie fest sitzt. Wenn der Adapter ordnungsgemäß eingesetzt wurde, sind die Portanschlüsse an der Steckplatzöffnung ausgerichtet, und die Frontplatte schließt genau mit dem Systemgehäuse ab.

VORSICHT!

Beim Einsetzen der Karte sollte nicht übermäßig viel Kraft aufgewendet werden, da dies zur Beschädigung des Systems oder des Adapters führen kann. Wenn sich der Adapter nicht einsetzen lässt, nehmen Sie ihn wieder heraus, richten Sie ihn nochmals aus, und versuchen Sie es erneut.

6. Befestigen Sie den Adapter mit der Adapterklemme oder -schraube.
7. Schließen Sie das Systemgehäuse, und entfernen Sie Ihre Antistatik-Geräte.

Anschließen der Netzwerkkabel

Die QLogic BCM57xx und BCM57xxx-Adapter verfügen entweder über einen RJ45-Anschluss, über den der Rechner mit einem Ethernet-Kupferdrahtsegment verbunden werden kann, oder über einen LWL-Anschluss, über den der Rechner mit einem Ethernet-LWL-Segment verbunden werden kann.

ANMERKUNG

Dieser Abschnitt gilt nicht für Blade-Server.

Kupferdraht

Anschluss eines Kupferdrahts:

1. Wählen Sie ein geeignetes Kabel aus. [Tabelle 4-1](#) führt die Eigenschaften von Kabeln für den Anschluss an 100 und 1000BASE-T und 10GBASE-T auf:

Tabelle 4-1. 100/1000BASE-T und 10GBASE-T-Kabelspezifikationen

Porttyp	Anschluss	Speichermedien	Maximale Länge
100/1000BASE-T ^a	RJ45	UTP-KABEL DER KATEGORIE 5 ^b	100 m
10GBASE-T	RJ45	UTP-KABEL DER KATEGORIE 6 ^c UTP-Kabel der Kategorie 6A und Kategorie 7 ^c	40 m (131 ft) 100 m (328CAT-ft)

^a Bei 1000BASE-T-Signalisierung sind vier TP-Kabel der Kategorie 5 für symmetrische Verkabelung gemäß ISO/IEC 11801:2002 und ANSI/EIA/TIA-568-B erforderlich.

^b Mindestens Kategorie 5. Kategorie 5E, Kategorie 6, Kategorie 6A und Kategorie 7 werden vollständig unterstützt.

^c Bei 10GBASE-T-Signalisierung sind vier TP-Kabel der Kategorie 6 oder Kategorie 6A (erweiterte Kategorie 6) für symmetrische Verkabelung gemäß ISO/IEC 11801:2002 und ANSI/TIA/EIA-568-B erforderlich.

2. Schließen Sie ein Kabelende an den RJ45-Stecker am Adapter an.
3. Schließen Sie das andere Kabelende an den RJ45 Ethernet-Netzwerkport an.

Lichtwellenleiter

Anschluss eines Lichtwellenleiters:

1. Wählen Sie ein geeignetes Kabel aus. [Tabelle 4-2](#) führt die Eigenschaften von Lichtwellenleitern für den Anschluss an 1000 und 2500BASE-X-Ports auf: Siehe auch Tabelle unter „[Unterstützte SFP+-Module pro NIC](#)“ auf [Seite 285](#).

Tabelle 4-2. 1000/2500BASE-X Lichtwellenleiterspezifikationen

Porttyp	Anschluss	Speichermedien	Maximale Länge
1000BASE-X	Small Form Faktor (SFF) Transceiver mit LC™ Verbindungssystem (Infineon® Teilenummer V23818-K305-L57)	Multimode-Faser (MMF) System optimiert für 62,5/50 µm Grade-Index-Glasfaser	550m (1,804 ft)
2500BASE-X ^a	Small Form Faktor (SFF) Transceiver mit LC™ Verbindungssystem (Finisar® Teilenummer FTLF8542E2KNV)	Multimode-Faser (MMF) System optimiert für 62,5/50 µm Grade-Index-Glasfaser	550m (1,804 ft)

^a Elektrik wird von IEEE 802.3ae-2002 (XAUI) unterstützt. 2500BASE-X ist ein von QLogic verwendeter Begriff zur Beschreibung des 2,5 Gbit/s (3,125 GBd) Betriebs.

2. Schließen Sie ein Kabelende an den LWL-Anschluss am Adapter an.
3. Schließen Sie das andere Kabelende an den Lichtwellenleiter-Ethernet-Netzwerkport an.

5 Verwaltungsfunktionen

Die Informationen über Verwaltungsfunktionen enthalten folgende Angaben:

- [CIM](#)
- [„Host Bus Adapter-API“ auf Seite 26](#)

CIM

Beim CIM-Modell (Common Information Model; Gemeinsames Informationsmodell) handelt es sich um einen von dem Standardisierungsgremium DMTF (Distributed Management Task Force) festgelegten Industriestandard. Microsoft implementiert CIM auf Windows-Server-Plattformen. QLogic unterstützt CIM auf Windows Server- und Linux-Plattformen.

ANMERKUNG

Weitere Informationen zum Installieren eines CIM-Providers auf einem Linux-System finden Sie unter [Kapitel 13 Linux QCS Installation](#).

Durch das Implementieren von CIM stehen über CIM-Clientanwendungen verschiedene Klassen zur Informationsbereitstellung für Benutzer zur Verfügung. Beachten Sie, dass der QLogic CIM-Datenprovider nur Daten zur Verfügung stellt. Benutzer können zum Durchsuchen der vom QLogic CIM-Provider bereitgestellten Daten eine beliebige CIM-Clientsoftware verwenden.

Die Klassen, durch die vom QLogic CIM-Provider Informationen bereitgestellt werden, heißen wie folgt:

- Die `QLGC_NetworkAdapter`-Klasse bietet Netzwerkadapter-Informationen, die zu einer Gruppe von Adaptern gehören, einschließlich Controller von QLogic und anderen Herstellern.
- Die `QLGC_ExtraCapacityGroup`-Klasse ist für die Teamkonfiguration für QLASP verantwortlich. Die derzeitige Implementierung bietet Teaminformationen und Informationen zu den physischen Netzwerkadaptern im Team.

QLASP stellt Ereignisse über Ereignisprotokolle bereit. Um diese Ereignisse anzuzeigen bzw. zu überwachen, verwenden Sie entweder die Ereignisanzeige der Windows-Serverplattformen oder das CIM. Der QLogic CIM-Provider stellt außerdem Ereignisinformationen über das generische Ereignismodell von CIM bereit. Bei diesen Ereignissen handelt es sich um `__InstanceCreationEvent`, `__InstanceDeletionEvent` und `__InstanceModificationEvent`, die durch CIM festgelegt werden. Die Clientanwendung muss die Ereignisse aus der Anwendung bei CIM registrieren, damit Ereignisse erfolgreich empfangen werden können. Dies erfolgt mit Hilfe von Abfragen (siehe nachfolgende Beispiele):

```
SELECT * FROM __InstanceModificationEvent
where TargetInstance ISA "QLGC_NetworkAdapter"
SELECT * FROM __InstanceModificationEvent
where TargetInstance ISA "QLGC_ExtraCapacityGroup"
SELECT * FROM __InstanceCreationEvent
where TargetInstance ISA "QLGC_NetworkAdapter"
++SELECT * FROM __InstanceDeletionEvent
where TargetInstance ISA "QLGC_NetworkAdapter"
SELECT * FROM __InstanceCreationEvent
where TargetInstance ISA "QLGC_ActsAsSpare"
++SELECT * FROM __InstanceDeletionEvent
where TargetInstance ISA "QLGC_ActsAsSpare"
```

Detaillierte Informationen zu diesen Ereignissen finden Sie in der CIM-Dokumentation:

http://www.dmtf.org/sites/default/files/standards/documents/DSP0004V2.3_final.pdf

QLogic implementiert ebenfalls die Spezifikation SMI-S, die CIM-Verwaltungsprofile für Speichersysteme festlegt.

Host Bus Adapter-API

QLOGIC unterstützt die SNIA Common HBA API unter Windows und Linux. Die Common HBA API ist eine Programmierschnittstelle zur Verwaltung von Fibre Channel Host-Bus-Adaptern.

6 Boot Agent-Treibersoftware

In diesem Kapitel wird behandelt, wie man MBA in Client- und Serverumgebungen einrichtet:

- [Übersicht](#)
- [„Einrichten von MBA Agent in einer Client-Umgebung“ auf Seite 28](#)
- [„Einrichten von MBA Agent in einer Linux Server-Umgebung“ auf Seite 34](#)

Übersicht

QLogic BCM57xx und BCM57xxx Adapter unterstützen Preboot Execution Environment (PXE), Remote Program Load (RPL), iSCSI und Bootstrap Protocol (BootP). Multi-Boot Agent (MBA) von QLogic ist ein Softwaremodul, das es dem an das Netzwerk angeschlossenen Computer ermöglicht, mit einem von den Remote-Servern im Netzwerk zur Verfügung gestellten Betriebssystem-Images zu booten. Der QLogic MBA-Treiber entspricht der PXE-Spezifikation 2.1 und wird mit monolithischen und geteilten Binär-Images zur Verfügung gestellt. Diese Images gewährleisten Flexibilität für Benutzer in verschiedenen Umgebungen, deren Hauptplatine u. U. nicht über einen integrierten Basis-Code verfügt.

Das MBA-Modul wird in einer Client-Server-Umgebung eingesetzt. Ein Netzwerk besteht aus einem oder mehreren Boot-Servern, die Boot-Images mehreren Computern über das Netzwerk zur Verfügung stellen. Die QLogicMBA-Modul-Implementierung wurde in den folgenden Umgebungen erfolgreich getestet:

- **Linux Red Hat PXE-Server.** QLogic PXE-Clients können einen Remote-Boot durchführen, Netzwerk-Ressourcen (NFS-Bereitstellung usw.) verwenden und Linux-Installationen vornehmen. Bei einem Remote-Boot-Vorgang wird der Linux-Universaltreiber nahtlos an die QLogic Universelle Netzwerktreiber-Schnittstelle (UNDI) angebunden, wodurch der unter Linux im Fernzugriff gestarteten Client-Umgebung eine Netzwerkschnittstelle zur Verfügung steht.
- **Intel APITEST.** Der QLogic PXE-Treiber besteht alle Testprogramme für die Prüfung der API-Kompatibilität.

- **Windows Deployment Service (WDS).** (Windows-Implementierungsdienst, WDS): Um Funktionen über die grundlegenden Netzwerkanbindungen hinaus zu erweitern, wenn ein Betriebssystem über Microsoft WDS geladen wird, generieren Sie ein WinPE-Image (3.0 oder höher), das den EVBD- oder den NDIS (Network Driver Interface Specification)-Treiber anwendet.

Einrichten von MBA Agent in einer Client-Umgebung

Das Einrichten von MBA Agent in einer Client-Umgebung umfasst folgende Schritte:

1. [Konfigurieren des MBA-Treibers.](#)
2. [Einrichten von BIOS](#) für die Boot-Reihenfolge.

Konfigurieren des MBA-Treibers

Dieser Abschnitt gilt für die Konfiguration des MBA-Treibers bei zusätzlichen Netzwerkkartenmodellen der QLogic-Adapter. Informationen zur Konfiguration des MBA-Treibers bei LOM-Modellen der QLogic-Adapter finden Sie in Ihrer Systemdokumentation.

ANMERKUNG

Sie können das Comprehensive Configuration Management (CCM)-Dienstprogramm von QLogic oder das Unified Extensible Firmware Interface (UEFI)-Dienstprogramm verwenden, um den MBA-Treiber für jeweils einen Adapter wie folgt beschrieben zu konfigurieren.

Das CCM-Dienstprogramm ist nur verfügbar, wenn das System auf den Legacy-Boot-Modus gesetzt ist. Es ist nicht verfügbar, wenn die Systeme auf den UEFI-Boot-Modus gesetzt sind. Die Seiten für die UEFI-Gerätekonfiguration sind in beiden Modi verfügbar.

Verwenden des Comprehensive Configuration Management-Werkzeugs

Verwendung von CCM, um den MBA-Treiber zu konfigurieren:

1. Starten Sie das System neu.
2. Drücken Sie die Tasten STRG + S. Für diesen Vorgang stehen Ihnen nach entsprechender Aufforderung bis zu vier Sekunden Zeit zur Verfügung. Es wird eine Liste mit Adaptern angezeigt.
 - a. Wählen Sie den zu konfigurierenden Adapter aus, und drücken Sie dann ENTER (die Eingabetaste). Es wird das Hauptmenü angezeigt.
 - b. Wählen Sie **MBA Configuration** (MBA-Konfiguration) aus, um das **MBA Configuration Menu** (MBA-Konfigurationsmenü), wie in [Abbildung 6-1](#) gezeigt, zu öffnen.

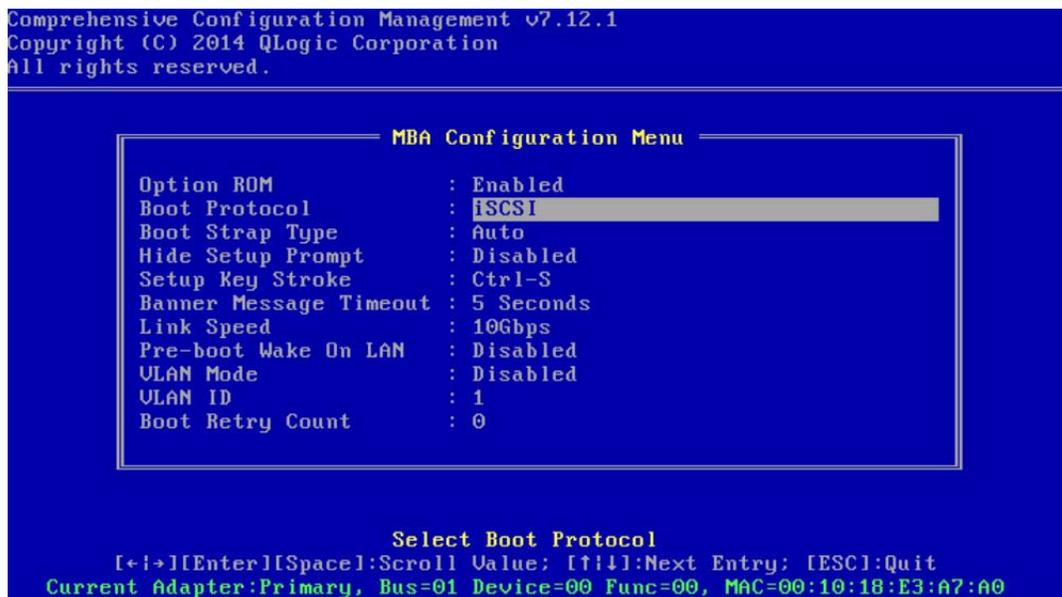


Abbildung 6-1. CCM MBA Configuration Menu (MBA-Konfigurationsmenü)

3. Um das Menüelement **Boot Protocol** (Boot-Protokoll) auszuwählen, drücken Sie auf die Tasten BILD NACH OBEN und BILD NACH UNTEN. Wenn andere Boot-Protokolle neben **Preboot Execution Environment (PXE)** verfügbar sind, drücken Sie die RIGHT ARROW (Pfeil-nach-rechts-) oder die LEFT ARROW (Pfeil-nach-links-Taste), um das gewünschte Boot-Protokoll auszuwählen: **FCoE** oder **iSCSI**.

ANMERKUNG

Legen Sie für iSCSI- und FCoE-bootfähige LOMs das Boot-Protokoll über das BIOS fest. Weitere Informationen erhalten Sie in Ihrer Systemdokumentation.

ANMERKUNG

Wenn Ihr System über mehrere Adapter verfügt und Sie unsicher sind, welchen Adapter Sie konfigurieren, drücken Sie die Tasten STRG + F6. Dies führt dazu, dass die Port-LEDs auf dem Adapter zu blinken beginnen.

4. Um bei Bedarf die Werte der anderen Menüelemente zu ändern, verwenden Sie die Taste UP ARROW (Pfeil-nach-oben), DOWN ARROW (Pfeil-nach-unten), LEFT ARROW (Pfeil-nach-links) und RIGHT ARROW (Pfeil-nach-rechts).
5. Um die Einstellungen zu speichern, drücken Sie die Taste F4.
6. Drücken Sie nach dem Speichern der Einstellungen auf ESC.

Verwenden von UEFI

Verwendung von UEFI, um den MBA-Treiber zu konfigurieren:

1. Starten Sie das System neu.
2. Rufen Sie das Konfigurationsmenü **Device Settings** (Geräteeinstellungen) des Programms **System Setup** (Systemeinrichtung) für das System-BIOS auf (siehe [Abbildung 6-2](#)).



Abbildung 6-2. Systemeinrichtung, Geräteeinstellungen

3. Wählen Sie das Gerät aus, bei dem Sie die MBA-Einstellungen ändern möchten (siehe [Abbildung 6-3](#)).

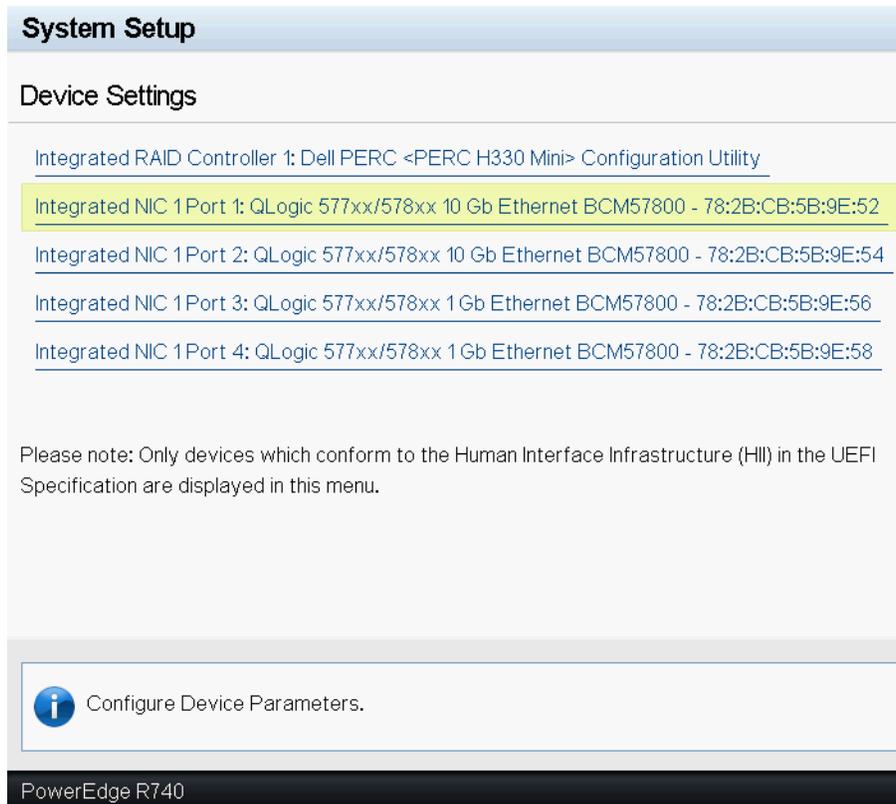


Abbildung 6-3. Geräteeinstellungen

4. Wählen Sie auf der Seite **Main Configuration** (Hauptkonfiguration) die Option **NIC Configuration** (Schnittstellenkarten-Konfiguration) aus (siehe [Abbildung 6-4](#)).

Integrated NIC 1 Port 1: QLogic 577xx/578xx 10 Gb Ethernet BCM57800 - 78:2B:CB:5B:9E:52

Main Configuration Page

Main Configuration Page

[Firmware Image Properties](#)

[Device Level Configuration](#)

[NIC Configuration](#)

[iSCSI Configuration](#)

[FCoE Configuration](#)

Blink LEDs	0
Chip Type	BCM57800 B0
PCI Device ID	168A
PCI Address	18:00:00
Link Status	Connected
MAC Address	78:2B:CB:5B:9E:52
Virtual MAC Address	78:2B:CB:5B:9E:52
iSCSI Offload MAC Address	00:00:00:00:00:00
Virtual iSCSI Offload MAC Address	00:00:00:00:00:00
FIP MAC Address	00:00:00:00:00:00
Virtual FIP MAC Address	00:00:00:00:00:00
World Wide Node Name	20:00:00:00:00:00:00:00
Virtual World Wide Node Name	20:00:00:00:00:00:00:00
World Wide Port Name	20:01:00:00:00:00:00:00
Virtual World Wide Port Name	20:01:00:00:00:00:00:00

 Firmware image information.

PowerEdge R740

Abbildung 6-4. Hauptkonfigurationsseite

5. Verwenden Sie auf der Seite „NIC Configuration“ (Netzwerkschnittstellen-Konfiguration) (siehe [Abbildung 6-5](#)) das Dropdown-Menü **Legacy Boot Protocol** (Legacy-Boot-Protokoll), um das gewünschte Boot-Protokoll auszuwählen, falls andere Boot-Protokolle als **Preboot Execution Environment (PXE)** verfügbar sind. Ist dies der Fall, gehören zu den anderen Boot-Protokollen **iSCSI** und **FCoE**. Die 1-GbE-Ports von BCM57xxx unterstützen nur PXE- und iSCSI-Remote-Boot.

Main Configuration Page > NIC Configuration

QLogic 577xx/578xx 10 Gb Ethernet BCM57800 - 78:2B:CB:5B:9E:52

Legacy Boot Protocol	None
Boot Strap Type	Auto Detect
Hide Setup Prompt	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Setup Key Stroke	<input checked="" type="radio"/> Ctrl-S <input type="radio"/> Ctrl-B
Banner Message Timeout	5
Link Speed	<input type="radio"/> 1 Gbps <input checked="" type="radio"/> 10 Gbps
Wake On LAN	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Virtual LAN Mode	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Virtual LAN ID	1
Boot Retry Count	No Retry

 Select a non-UEFI Boot Protocol to be used.

PowerEdge R740

Abbildung 6-5. NIC-Konfiguration

ANMERKUNG

Für iSCSI- und FCoE-bootfähige LOMs wird das Boot-Protokoll über das BIOS festgelegt. Weitere Informationen erhalten Sie in Ihrer Systemdokumentation.

6. Drücken Sie die Taste UP ARROW (Pfeil-nach-oben), DOWN ARROW (Pfeil-nach-unten), LEFT ARROW (Pfeil-nach-links) und RIGHT ARROW (Pfeil-nach-rechts), um bei Bedarf die Werte der anderen Menüelemente zu ändern.
7. Wählen Sie **Back** (Zurück) aus, um zum **Main Menu** (Hauptmenü) zurückzukehren.
8. Wählen Sie **Finish** (Fertig stellen) zum Speichern und Beenden aus.

Einrichten von BIOS

Legen Sie den MBA-aktivierten Adapter als erstes bootfähiges Gerät unter BIOS fest, um ein Booten mit dem MBA vom Netzwerk zu ermöglichen. Dieses Verfahren hängt von der BIOS-Implementierung des Systems ab. Weitere Informationen finden Sie im Benutzerhandbuch des Systems.

Einrichten von MBA Agent in einer Linux Server-Umgebung

Die Red Hat Enterprise Linux-Distribution unterstützt PXE-Server. Hiermit können Benutzer eine vollständige Remote-Installation unter Linux über das Netzwerk ausführen. Im Lieferumfang des Pakets sind die Boot-Images *Boot-Kernel* (*vmlinuz*) und *Initial-RAM-Disk* (*initrd*) enthalten, die sich auf der Red Hat-CD Nr. 1 befinden:

```
/images/pxeboot/vmlinuz  
/images/pxeboot/initrd.img
```

Weitere Informationen über die Installation von PXE-Servern unter Linux finden Sie in der Red Hat-Dokumentation.

Die Datei *initrd.img*, die in Red Hat Enterprise Linux enthalten ist, verfügt über keinen Linux-Netzwerktreiber für QLogicBCM57xx und BCM57xxx-Adapter. Für diese Version ist eine Treiberdiskette für Treiber erforderlich, die kein Bestandteil der Standarddistribution sind. Mit dem Image, das auf der Installations-CD enthalten ist, können Sie einen Treiberdatenträger für die QLogicBCM57xx und BCM57xxx-Adapter erstellen. Weitere Informationen dazu finden Sie in der Linux-Datei *Readme.txt*.

7 Linux-Treibersoftware

Die Informationen zur Linux-Treibersoftware enthalten folgende Angaben:

- Einführung
- „Einschränkungen“ auf Seite 36
- „Verfügbare Pakete“ auf Seite 37
- „Installieren der Linux-Treibersoftware“ auf Seite 38
- „Schließen oder Entfernen des Linux-Treibers“ auf Seite 44
- „Patching von PCI-Dateien (optional)“ auf Seite 45
- „Netzwerkinstallationen“ auf Seite 46
- „Einstellen der Werte für optionale Eigenschaften“ auf Seite 47
- „Treiberstandardeinstellungen“ auf Seite 52
- „Treibermeldungen“ auf Seite 53
- „Teaming-Funktion mit Channel Bonding“ auf Seite 59
- „Statistikdaten“ auf Seite 59
- „iSCSI-Verschiebung in Linux“ auf Seite 59

Einführung

In diesem Abschnitt werden die Linux-Treiber für die Netzwerkadapter QLogic BCM57xx und BCM57xxx behandelt, die in [Tabelle 7-1](#) aufgeführt sind.

Tabelle 7-1. QLogic BCM57xx und BCM57xxx Linux-Treiber

Linux-Treiber	Beschreibung
bnx2x	Linux-Treiber für die BCM57xx und BCM57xxx 10-GB-Netzwerkadapter. Durch diesen Treiber wird die Hardware direkt gesteuert. Er ist außerdem für das Senden und Empfangen von Ethernet-Paketen für den Linux-Hostnetzwerk-Stack verantwortlich. Der Treiber empfängt und verarbeitet darüber hinaus Geräte-Interrupts (sowohl für sich selbst (für L2-Netzwerke) als auch für die bnx2fc-Treiber (FCoE) und C-NIC-Treiber).

Tabelle 7-1. QLogic BCM57xx und BCM57xxx Linux-Treiber (fortgesetzt)

Linux-Treiber	Beschreibung
cnic	Der C-NIC-Treiber liefert die Schnittstelle zwischen den QLogic-Protokolltreibern der oberen Schicht (z. B. Speichertreibern) und den QLogicBCM57xx und BCM57xxx1-Gb- und 10-Gb-Netzwerkadaptern. Das C-NIC-Modul kann mit den bnx2- und bnx2x-Netzwerktreibern im Downstream und den bnx2fc- (FCoE-) und bnx2i- (iSCSI-) Treibern im Upstream verwendet werden.
bnx2i	Linux iSCSI-HBA-Treiber zur Aktivierung von iSCSI-Offload für die BCM57xx und BCM57xxx1-GB- und 10-GB-Netzwerkadapter.
bnx2fc	Linux FCoE-Kernel-Modultreiber, mit dem eine Übersetzungsschicht zwischen dem Linux SCSI-Stack und der Broadcom FCoE-Firmware-/Hardware bereitgestellt wird. Darüber hinaus ist der Treiber mit der Netzwerkschicht verbunden, um eingekapselte FCoE-Frames für <code>libfc/libfcoc</code> von Open-FCoE für die FIP-/Geräteerkennung zu übertragen und zu empfangen.

Einschränkungen

Die Linux-Treiber unterliegen den folgenden Einschränkungen:

- [bnx2x-Treibereinschränkungen](#)
- [bnx2i-Treibereinschränkungen](#)
- [bnx2fc-Treibereinschränkungen](#)

bnx2x-Treibereinschränkungen

Die aktuelle Version des Treibers wurde für 2.6.x-Kernel getestet, beginnend mit dem 2.6.9-Kernel. Möglicherweise lässt sich der Treiber nicht auf Kernel kompilieren, die älter als Version 2.6.9 sind. Die Testverfahren konzentrieren sich auf die Architekturen i386 und x86_64. Auf einigen anderen Architekturen wurden weniger Testverfahren durchgeführt. Auf einigen Kernen sind möglicherweise geringfügige Änderungen an bestimmten Quelldateien und an der `makefile` (Steuerdatei) erforderlich.

bnx2i-Treibereinschränkungen

Die aktuelle Version des Treibers wurde für 2.6.x-Kernel getestet, beginnend mit dem 2.6.18-Kernel. Möglicherweise lässt sich der bnx2i-Treiber nicht auf ältere Kernel kompilieren. Die Testverfahren konzentrieren sich auf i386- und x86_64-Architekturen, RHEL 6, RHEL 7 und SUSE 11 SP1 und höhere Distributionen.

bnx2fc-Treibereinschränkungen

Die aktuelle Version des Treibers wurde für 2.6.x-Kernel getestet, beginnend mit dem 2.6.32-Kernel, der in RHEL 6.1-Distributionen enthalten ist. Der bnx2fc-Treiber lässt sich evtl. nicht auf älteren Kernen kompilieren. Die Testverfahren wurden beschränkt auf i386- und x86_64-Architekturen, RHEL 6.1, RHEL 7.0 und SLES 11 SP1 und höhere Distributionen.

Verfügbare Pakete

Die Linux-Treiber sind in den folgenden Paketformaten verfügbar:

Dynamic Kernel Module Support (DKMS)-Pakete

- `netxtreme2-version.dkms.noarch.rpm`
- `netxtreme2-version.dkms.src.rpm`

Kernel-Modul-Pakete (KMP)

- SLES:
 - `netxtreme2-kmp-[kernel]-version.i586.rpm`
 - `netxtreme2-kmp-[kernel]-version.x86_64.rpm`
- Red Hat:
 - `kmod-kmp-netxtreme2-{kernel}-version.i686.rpm`
 - `kmod-kmp-netxtreme2-{kernel}-version.x86_64.rpm`

Das Befehlszeilenschnittstellen-Verwaltungsprogramm QLogic Control Suite (QCS) wird auch als RPM-Paket verteilt (`QCS-{version}.{arch}.rpm`).

Quellpakete

Sowohl das RPM- als auch das TAR-Quellpaket enthalten identische Quelldateien zum Erstellen des Treibers. Die ergänzende TAR-Datei enthält zusätzliche Elemente wie Patches und Treiberdisketten-Images für die Netzwerkinstallation.

Im Folgenden wird eine Liste der enthaltenen Dateien aufgeführt:

- `netxtreme2-version.src.rpm`: RPM-Paket mit den Treiberquellen BCM57xx und BCM57xxx bnx2, bnx2x, cnic, bnx2fc, bnx2ilibfc und libfcoe.
- `netxtreme2-version.tar.gz`: Komprimiertes TAR-Paket mit den Treiberquellen BCM57xx und BCM57xxx bnx2, bnx2x, cnic, bnx2fc, bnx2i, libfc und libfcoe.
- `iscsiuio-version.tar.gz`: Binärdatei des Verwaltungstools für den iSCSI-Benutzerbereich

Der Linux-Treiber ist abhängig von Open-FCoE-Userspace-Managementtools als Frontend zur Steuerung der FCoE-Schnittstellen. Der Paketname des Open-FCoE-Tools lautet *foe-utils* für RHEL 6.4 und *open-foe* für Legacy-Versionen.

Installieren der Linux-Treibersoftware

Das Vorgehen der Installation der Linux-Treibersoftware beinhaltet:

- [Installieren des Quell-RPM-Pakets](#)
- [Erstellen des Treibers aus der Quell-TAR-Datei](#)
- [Installieren des DKMS-Binär-RPM-Treiberpakets](#)
- [Installieren des Binär-KMOD- und KMP-Treiberpakets](#)

ANMERKUNG

Beim Laden eines bnx2/bnx2x/bnx2i-Treibers und Aktualisieren des Linux-Kernels muss das Treiber-Modul neu kompiliert werden, wenn das Treiber-Modul mit Hilfe des Quell-RPM- oder des TAR-Pakets installiert wurde. Dies gilt nicht für die DKMS-Quell-RPM.

Installieren des Quell-RPM-Pakets

Im Folgenden werden die Richtlinien zum Installieren des Quell-RPM-Treiberpakets aufgeführt.

Voraussetzungen:

- Linux-Kernel-Quelle
- C-Compiler

Installieren und Konfigurieren des Quell-RPM-Pakets:

1. Installieren Sie das RPM-Paket:

```
rpm -ivh netxtreme2-<version>.src.rpm
```
2. Wechseln Sie zum Verzeichnis des RPM-Pfads, und erstellen Sie das Binär-RPM für Ihren Kernel:

Für RHEL:

```
cd ~/rpmbuild  
rpmbuild -bb SPECS/netxtreme2.spec
```

Für SLES:

```
cd /usr/src/packages  
rpmbuild -bb SPECS/netxtreme2.spec
```

3. Installieren Sie das neu kompilierte RPM:

```
rpm -ivh RPMS/<arch>/netxtreme2-<version>.<arch>.rpm
```

Bitte beachten Sie, dass die Option `--force` bei einigen Linux-Distributionen erforderlich sein kann, wenn Konflikte gemeldet werden.

4. Für einen FCoE-Offload installieren Sie das Open-FCoE-Dienstprogramm. Gehen Sie bei RHEL 6.4 und Legacy-Versionen wie folgt vor:

```
yum install fcoe-utils-<version>.rhel.64.brcm.<subver>.<arch>.rpm
```

```
rpm -ivh fcoe-utils-<version>.rhel.64.brcm.<subver>.<arch>.rpm
```

Für RHEL 6.4 und Legacy-Versionen ist die mit Ihrer Distribution gelieferte Version von `fcoe-utils` oder `open-fcoe` ausreichend, und es werden keine sofort einsatzbereiten Aktualisierungen bereitgestellt.

Wenn verfügbar, werden Abhängigkeiten bei einer Installation mit `yum` automatisch aufgelöst. Andernfalls sind erforderliche Abhängigkeiten auf dem Installationsdatenträger Ihres Betriebssystems gespeichert.

5. Aktivieren Sie für SLES 11 SP1 die Dienste FCoE und link layer discover protocol agent daemon (`lldpad`) für einen FCoE-Offload, und für iSCSI-offload-TLV nur `lldpad`, wie im Folgenden angegeben:

```
chkconfig lldpad on
```

```
chkconfig fcoe on
```

6. Integrierte Treiber sind in allen unterstützten Betriebssystemen vorhanden. Die einfachste Methode zur Sicherstellung, dass die neu installierten Treiber geladen werden, ist ein Neustart.
7. Um einen FCoE-Offload durchzuführen, erstellen Sie nach dem Neustart Konfigurationsdateien für alle FCoE `ethX`-Schnittstellen:

```
cd /etc/fcoe
```

```
cp cfg-ethx cfg-<ethX FCoE interface name>
```

ANMERKUNG

Bitte beachten Sie, dass bei Ihrer Distribution möglicherweise ein anderes Benennungssystem für Ethernet-Geräte gilt. (d. h. `pXpX` oder `emX` anstatt `ethX`).

8. Um einen FCoE-Offload oder iSCSI-Offload-TLV durchzuführen, modifizieren Sie `/etc/fcoe/cfg-<interface>`, indem Sie `DCB_REQUIRED=yes` in `DCB_REQUIRED=no` ändern.

9. Aktivieren Sie alle ethX-Schnittstellen.

```
ifconfig <ethX> up
```

10. Konfigurieren Sie für SLES Ihre Ethernet-Schnittstellen mit YaST (ein Installations- und Konfigurationswerkzeug für openSUSE und die SUSE Linux Enterprise-Distributionen) so, dass sie beim Booten automatisch gestartet werden. Dazu legen Sie eine statische IP-Adresse fest oder aktivieren DHCP für die Schnittstelle.

11. Um einen FCoE-Offload bzw. iSCSI-Offload-TLV durchzuführen, deaktivieren Sie lldpad für QLogicConverged Network Adapter-Schnittstellen. Dies ist erforderlich, weil QLogic einen entlasteten DCBX-Client verwendet.

```
lldptool set-lldp -i <ethX> adminStatus=disabled
```

12. Um einen FCoE-Offload bzw. iSCSI-Offload durchzuführen, stellen Sie, wie unten dargestellt, sicher, dass `/var/lib/llddpad/llddpad.conf` erstellt wird und in keinem `<ethX>`-Block `adminStatus` auftritt oder falls doch, dass dafür `0` festgelegt wird (`adminStatus=0`).

```
lldp :
{
  eth5 :
  {
    tlv00000001 :
    {
      info = "04BC305B017B73";
    };
    tlv00000002 :
    {
      info = "03BC305B017B73";
    };
  };
};
```

13. Um einen FCoE-Offload bzw. iSCSI-Offload-TLV auszuführen und die neuen Einstellungen anzuwenden, starten Sie den lldpad-Dienst neu.

Für SLES11 SP1, RHEL 6.4 und Legacy-Versionen:

```
service lldpad restart
```

14. Für einen FCOE-Offload und die Anwendung der neuen Einstellungen starten Sie den FCoE-Dienst neu.

Für SLES11 SP1, RHEL 6.4 und Legacy-Versionen:

```
service fcoe restart
```

Installieren des KMP-Pakets

ANMERKUNG

Die aufgeführten Beispiele beziehen sich auf den bnx2x-Treiber, gelten aber auch für die Treiber bnx2fc und bnx2i.

So installieren Sie das KMP-Paket:

1. Installieren Sie das KMP-Paket:

```
rpm -ivh <file>
rmmod bnx2x
```
2. Laden Sie den Treiber folgendermaßen:

```
modprobe bnx2x
```

Erstellen des Treibers aus der Quell-TAR-Datei

ANMERKUNG

Die aufgeführten Beispiele beziehen sich auf den bnx2-Treiber, gelten aber auch für die Treiber bnx2xi und bnx2fc

So erstellen Sie den Treiber über die TAR-Datei:

1. Erstellen Sie ein Verzeichnis, und extrahieren Sie die TAR-Dateien in dieses Verzeichnis:

```
tar xvzf netxtreme2-version.tar.gz
```
2. Erstellen Sie den Treiber `bnx2.ko` (oder `bnx2.o`) als ladbares Modul für den ausgeführten Kernel:

```
cd netxtreme2-version
make
```
3. Testen Sie den Treiber, indem Sie ihn laden (entfernen Sie bei Bedarf zunächst den vorliegenden Gerätetreiber):

```
rmmod bnx2x (oder bnx2fc oder bnx2i)
insmod bnx2x/src/bnx2x.ko (oder bnx2fc/src/bnx2fc.ko, oder
bnx2i/src/bnx2i.ko)
```
4. Um einen iSCSI-Offload bzw. FCoE-Offload durchzuführen, laden Sie den C-NIC-Treiber (falls erforderlich):

```
insmod cnic.ko
```

5. Installieren Sie den Treiber und die Man-Page:

```
make install
```

ANMERKUNG

Entnehmen Sie die Angaben zum Speicherort des installierten Treibers den vorherigen RPM-Anweisungen.

6. Installieren Sie den Benutzer-Daemon (iscsiuio).

Anweisungen zum Laden der für die Nutzung der QLogic-Funktion zum iSCSI-Offload erforderlichen Softwarekomponenten finden Sie unter „[Laden Sie die erforderlichen iSCSI-Softwarekomponenten, und führen Sie sie aus](#)“ auf [Seite 44](#).

Schlagen Sie die Anleitungen zum Konfigurieren des Netzwerkprotokolls sowie der Netzwerkadresse nach dem Erstellen des Treibers im Handbuch zu Ihrem Betriebssystem nach.

Installieren des DKMS-Binär-RPM-Treiberpakets

Dynamic Kernel Module Support (DKMS) soll die Neuerstellung von Modulen bei jeder Aktualisierung des Kernels vereinfachen. Um den Kernel zu aktualisieren, erstellen Sie eine Umgebung, in der sich eine Kernel-abhängige Modul-Quelle befindet.

So installieren Sie das DKMS-Binär-RPM-Treiberpaket:

1. Laden Sie das DKMS-Binär-RPM-Paket (`dkms-version.noarch.rpm`) herunter:

<http://linux.dell.com/dkms/>

2. Installieren Sie das DKMS-Binär-RPM-Paket, indem Sie den folgenden Befehl ausführen:

```
rpm -ivh dkms-version.noarch.rpm
```

3. Installieren Sie das DKMS-RPM-Paket, indem Sie den folgenden Befehl ausgeben:

```
rpm -ivh netxtreme2-version dkms.noarch.rpm
```

Vergewissern Sie sich anhand des Meldungsprotokolls, dass Ihr Netzwerkadapter iSCSI unterstützt. Wenn die Meldung "bnx2i: dev eth0 does not support iSCSI" (bnx2i: dev eth0 unterstützt iSCSI nicht) im Meldungsprotokoll angezeigt wird, nachdem Sie den bnx2i-Treiber geladen haben, bietet der Adapter keine iSCSI-Unterstützung. Diese Meldung wird möglicherweise erst angezeigt, wenn die Schnittstelle geöffnet wird, wie bei:

```
ifconfig eth0 up
```

4. Informationen zur Benutzung von iSCSI finden Sie unter „Laden Sie die erforderlichen iSCSI-Softwarekomponenten, und führen Sie sie aus“ auf Seite 44. Hier können Sie die erforderlichen Softwarekomponenten laden. Weitere Informationen finden Sie unter:

<http://linux.dell.com>

Installieren des Binär-KMOD- und KMP-Treiberpakets

So installieren Sie die binären Kernelmodule (KMOD) und das KMP-Treiberpaket:

1. Installieren Sie die Treiberpakete KMOD und KMP RPM:

SUSE:

```
netxtreme2-kmp-default-<driver ver>_<kernel>-<rel>.<dist maj.min>.<arch>.rpm
```

Red Hat:

```
kmod-netxtreme2-<driver ver>.<dist maj.min>.<arch>.rpm
```

2. Vergewissern Sie sich anhand des Meldungsprotokolls, dass Ihr Netzwerkadapter iSCSI unterstützt. Wenn die Meldung `bnx2i: dev eth0 does not support iSCSI` (bnx2i: dev eth0 unterstützt iSCSI nicht) im Meldungsprotokoll angezeigt wird, nachdem Sie den bnx2i-Treiber geladen haben, bietet der Adapter keine iSCSI-Unterstützung. Diese Meldung wird möglicherweise erst angezeigt, wenn die Schnittstelle geöffnet wird, wie bei:

```
ifconfig eth0 up
```

3. Informationen zur Benutzung von iSCSI finden Sie unter „Laden Sie die erforderlichen iSCSI-Softwarekomponenten, und führen Sie sie aus“ auf Seite 44. Hier können Sie die erforderlichen Softwarekomponenten laden. Weitere Informationen finden Sie unter:

<http://linux.dell.com>

Laden Sie die erforderlichen iSCSI-Softwarekomponenten, und führen Sie sie aus

Die QLogiciSCSI Offload Software-Suite besteht aus drei Kernelmodulen und einem Benutzer-Daemon. Erforderliche Softwarekomponenten können entweder manuell oder über Systemdienste geladen werden.

1. Entfernen Sie den bestehenden Treiber, sofern erforderlich. Geben Sie bei manueller Eingabe den folgenden Befehl aus:

```
rmmod bnx2i
```

2. Laden Sie den iSCSI-Treiber. Geben Sie zum manuellen Laden einen der folgenden Befehle aus:

```
insmod bnx2i.ko
```

```
modprobe bnx2i
```

Schließen oder Entfernen des Linux-Treibers

- [Schließen oder Entfernen des Treibers aus einer RPM-Installation](#)
- [Entfernen des Treibers aus einer TAR-Installation](#)

Schließen oder Entfernen des Treibers aus einer RPM-Installation

ANMERKUNG

- Die aufgeführten Beispiele beziehen sich auf den bnx2x-Treiber, gelten aber auch für die Treiber bnx2fc und bnx2i.
 - Für 2.6-Kernel ist es nicht erforderlich, die eth#-Schnittstellen vor dem Entfernen des Treibermoduls zu schließen.
 - Wenn der C-NIC-Treiber geladen wurde, dann entfernen Sie ihn, bevor Sie den bnx2-Treiber entfernen.
 - Vor dem Entfernen des bnx2i-Treibers müssen alle aktiven iSCSI-Sitzungen und -Ziele getrennt werden.
-

Geben Sie `ifconfig` ein, um alle durch den Treiber geöffneten eth#-Schnittstellen zu schließen, und führen Sie dann den folgenden Befehl aus:

```
rmmod bnx2x
```

ANMERKUNG

Der vorherige Befehl entfernt auch das C-NIC-Modul.

Wenn der Treiber mit RPM installiert wurde, entfernen Sie ihn anhand des folgenden Befehls:

```
rpm -e netxtreme2
```

Entfernen des Treibers aus einer TAR-Installation

ANMERKUNG

Die aufgeführten Beispiele beziehen sich auf den bnx2x-Treiber, gelten aber auch für die Treiber bnx2fc und bnx2i.

Wenn der Treiber unter Verwendung von `make install` aus der TAR-Datei installiert wurde, muss die Treiberdatei `bnx2.ko` manuell aus dem Betriebssystem gelöscht werden. Unter „[Installieren des Quell-RPM-Pakets](#)“ auf [Seite 38](#) finden Sie Informationen zum Speicherort des installierten Treibers.

Deinstallation QCS mit dem RPM-Paket

Geben Sie den folgenden Befehl aus, um eine Deinstallation von QCS CLI und/oder dem zugehörigen RPC-Agenten mit dem Linux RPM-Paket durchzuführen:

```
% rpm -e <package_name>.rpm
```

Wobei `<package_name>` aus Folgendem besteht:

QCS CLI `QCS-CLI-<version>-<arch>.rpm`

RPC-Agent `qlnxremote-<version>.<arch>.rpm`

Patches von PCI-Dateien (optional)

ANMERKUNG

Die aufgeführten Beispiele beziehen sich auf den bnx2x-Treiber, gelten aber auch für die Treiber bnx2fc und bnx2i.

Wenn Sie Dienstprogramme zur Hardware-Erkennung wie Red Hat kudzu verwenden möchten, um von bnx2 unterstützte Geräte zu erkennen, müssen möglicherweise eine Reihe von Dateien mit PCI-Händler- und -Geräteinformationen aktualisiert werden. Übernehmen Sie die Aktualisierungen, indem Sie die in der ergänzenden TAR-Datei enthaltenen Skripten ausführen. Wenden Sie beispielsweise unter Red Hat Enterprise Linux die Updates mithilfe der folgenden Befehle an:

```
./patch_pcitbl.sh /usr/share/hwdata/pcitable pci.updates  
/usr/share/hwdata/pcitable.new bnx2  
./patch_pciids.sh /usr/share/hwdata/pci.ids pci.updates  
/usr/share/hwdata/pci.ids.new
```

Sichern Sie als nächstes die alten Dateien und benennen Sie die neuen zu verwendenden um.

```
cp /usr/share/hwdata/pci.ids /usr/share/hwdata/old.pci.ids  
cp /usr/share/hwdata/pci.ids.new /usr/share/hwdata/pci.ids  
cp /usr/share/hwdata/pcitable /usr/share/hwdata/old.pcitable  
cp /usr/share/hwdata/pcitable.new /usr/share/hwdata/pcitable
```

Netzwerkinstallationen

Für Netzwerkinstallationen über NFS, FTP oder HTTP (mithilfe einer Netzwerk-Bootdiskette oder PXE) ist unter Umständen ein Treiberdatenträger mit dem bnx2x-Treiber erforderlich. Die Treiberdatenträger-Images für die aktuellsten Red Hat- und SuSE-Versionen sind im Lieferumfang enthalten. Boottreiber für andere Linux-Versionen können durch Verändern der Steuerdatei `Makefile` und der make-Umgebung kompiliert werden. Weitere Informationen finden Sie auf der Website von Red Hat:

<http://www.redhat.com>

Einstellen der Werte für optionale Eigenschaften

Für die verschiedenen Treiber liegen unterschiedliche optionale Eigenschaften vor:

- [bnx2x-Treiberparameter](#)
- [bnx2i-Treiberparameter](#)
- [bnx2fc-Treiberparameter](#)

bnx2x-Treiberparameter

In den folgenden Abschnitten werden die Parameter für den Treiber bnx2x ausführlich beschrieben.

disable_tpa

Der Parameter `disable_tpa` kann als Befehlszeilenargument für das Deaktivieren der Funktion Transparent Packet Aggregation (TPA) verwendet werden. Standardmäßig bündelt der Treiber TCP-Pakete. Geben Sie `disable_tpa` ein, um die erweiterte TPA-Funktion zu deaktivieren.

Setzen Sie den Parameter `disable_tpa` wie nachstehend gezeigt auf 1. Damit wird die TPA-Funktion auf allen BCM57xx und BCM57xxx Netzwerkadaptern des Systems deaktiviert. Sie können den Parameter auch in der `modprobe.conf`-Datei setzen. Weitere Informationen erhalten Sie auf der Man-Page.

```
insmod bnx2x.ko disable_tpa=1  
oder  
modprobe bnx2x disable_tpa=1
```

int_mode

Der Parameter `int_mode` erzwingt einen Interrupt-Modus.

Setzen Sie den Parameter `int_mode` auf 1, um die Verwendung des Legacy INTx-Modus durch alle BCM57xx und BCM57xxx-Adapter des Systems zu erzwingen.

```
insmod bnx2x.ko int_mode=1  
oder  
modprobe bnx2x int_mode=1
```

Setzen Sie den Parameter `int_mode` auf 2, um die Verwendung des MSI-Modus durch alle BCM57xx und BCM57xxx-Adapter des Systems zu erzwingen.

```
insmod bnx2x.ko int_mode=2
```

oder

```
modprobe bnx2x int_mode=2
```

Setzen Sie den Parameter `int_mode` auf 3, um die Verwendung des MSI-X-Modus durch alle BCM57xx und BCM57xxx-Adapter des Systems zu erzwingen.

dropless_fc

Mit dem Parameter `dropless_fc` können Sie einen zusätzlichen Flow Control-Mechanismus in den BCM57xx und BCM57xxx-Adaptoren aktivieren. Der Standardmechanismus für Flow Control wird an PAUSE Frames gesendet, wenn der Puffer auf dem Chip (BRD) einen bestimmten Belegungsgrad erreicht hat, der ein leistungsorientierter Flow Control-Mechanismus ist. Bei Verwendung von BCM57xx und BCM57xxx-Adaptoren können Sie einen anderen Flow Control-Mechanismus zum Senden von PAUSE Frames aktivieren, wenn einer der Hostpuffer (im RSS-Modus) voll ist.

Bei `dropless_fc` handelt es sich um einen gezielten „Zero Packet Drop“ Flow Control-Mechanismus.

Setzen Sie den Parameter `dropless_fc` auf 1, um den „Dropless“ Flow Control-Mechanismus auf allen BCM57xx und BCM57xxx-Adaptoren des Systems zu aktivieren.

```
insmod bnx2x.ko dropless_fc=1
```

oder

```
modprobe bnx2x dropless_fc=1
```

disable_iscsi_ooo

Mit dem Parameter `disable_iscsi_ooo` wird die Zuweisung der iSCSI-TCP-Out-of-Order-(OoO-)Empfangsressourcen deaktiviert (insbesondere für VMware bei Systemen mit geringem Arbeitsspeicher).

num_queues

Mit dem optionalen Parameter `num_queues` können Sie die Anzahl der Warteschlangen festlegen, wenn `multi_mode` auf 1 und der Interrupt-Modus auf MSI-X gesetzt ist. Ist ein anderer Interrupt-Modus als MSI-X festgelegt (siehe [„int_mode“ auf Seite 47](#)), wird die Anzahl der Warteschlangen ungeachtet der Einstellung für diesen Parameter auf 1 gesetzt.

pri_map

Der optionale Parameter `pri_map` wird verwendet, um den VLAN-PRI-Wert oder den IP-DSCP-Wert in der Hardware auf eine andere oder dieselbe Dienstklasse zu setzen. Der Treiber wertet diesen 32-Bit-Parameter als einen 8er-Wert mit jeweils 4 Bits aus. Jedes Nibble legt die erforderliche Hardware-Warteschlangennummer für diese Priorität fest. So kann z. B. mit dem Wert „0x11110000“ für `pri_map` der Dienstklasse 0 die Priorität 0 bis 3 und der Dienstklasse 1 die Priorität 4 bis 7 zugeordnet werden.

bnx2i-Treiberparameter

Die optionalen Parameter `en_tcp_dack`, `error_mask1` und `error_mask2` können als Befehlszeilenargumente für die Befehle `insmod` oder `modprobe` für `bnx2i` bereitgestellt werden.

error_mask1 and error_mask2

Config FW iSCSI Error Mask dient dem Konfigurieren bestimmter iSCSI-Protokoll-Verstöße, sodass diese entweder als Warnung oder fataler Fehler eingestuft werden. Alle fatalen iSCSI-Protokollverstöße führen zur Sitzungswiederherstellung (ERL 0). Dies sind Bit-Masken.

Standardeinstellung: Alle Verstöße werden als Fehler behandelt.

VORSICHT!

Verwenden Sie `error_mask` nicht, wenn Sie sich bezüglich der Konsequenzen nicht völlig im Klaren sind. Diese Werte sollten unbedingt mit dem Entwicklungsteam von QLogic für jeden Einzelfall individuell abgestimmt werden. Dieser Parameter ist nur ein Mechanismus, um Probleme bei der iSCSI-Implementierung auf der Zielseite zu umgehen. Es wird dringend davon abgeraten, ohne fundierte und detaillierte Kenntnisse des iSCSI-Protokolls mit diesen Parametern zu experimentieren.

en_tcp_dack

Enable TCP Delayed ACK aktiviert bzw. deaktiviert die TCP-verzögerte ACK-Funktion (Quittierung) bei verschobenen iSCSI-Verbindungen.

Standardeinstellung: TCP-verzögerte ACK ist AKTIVIERT. Zum Beispiel:

```
insmod bnx2i.ko en_tcp_dack=0
```

oder

```
modprobe bnx2i en_tcp_dack=0
```

time_stamps

Enable TCP TimeStamps aktiviert bzw. deaktiviert die TCP-Zeitstempel-Funktion bei verschobenen iSCSI-Verbindungen.

Standardeinstellung: TCP-Zeitstempel-Funktion ist DEAKTIVIERT. Zum Beispiel:

```
insmod bnx2i.ko time_stamps=1
```

oder

```
modprobe bnx2i time_stamps=1
```

sq_size

Verwenden Sie **Configure SQ size** (SQ-Größe konfigurieren), um die Größe der Sendewarteschlange für verschobene Verbindungen festzulegen. Die SQ-Größe bestimmt die maximal zulässige Anzahl von SCSI-Befehlen in der Warteschlange. Die Größe von SQ wirkt sich auf eine Reihe von Verbindungen aus, die verschoben werden können. Mit zunehmender QP-Größe sinkt die Anzahl der unterstützten Verbindungen. Wenn Standardwerte gelten, können die BCM5708-Adapter 28 Verbindungen verschieben.

Standard: 128

Bereich: 32 bis 128

Beachten Sie, dass die QLogic-Validierung auf Werte von hoch 2 beschränkt ist; z. B. 32, 64 und 128.

rq_size

Verwenden Sie **Configure RQ size** (RQ-Größe konfigurieren), um die Größe der asynchronen Pufferwarteschlange pro verschobene Verbindung festzulegen. Die Größe von RQ muss nicht größer als 16 sein, da der Wert für die Platzierung von Nachrichten der iSCSI-Typen ASYNC/NOP/REJECT und SCSI-Wertdaten verwendet wird.

Standard: 16

Bereich: 16 bis 32

Beachten Sie, dass die QLogic-Validierung auf Werte von hoch 2 beschränkt ist; z. B. 16 oder 32.

event_coal_div

Event Coalescing Divide Factor ist ein Parameter zur Leistungsabstimmung, mit dem die Frequenz der Interrupt-Erstellung durch die iscsi-Firmware gesteuert wird.

Standard: 2

Gültige Werte: 1, 2, 4, 8

last_active_tcp_port

Last active TCP port used ist ein Statusparameter, der die TCP-Portnummer angibt, die in der iSCSI-Offload-Verbindung zuletzt verwendet wurde.

Standard: k.A.

Gültige Werte: k.A.

Anmerkung: Dieser Parameter ist schreibgeschützt.

ooo_enable

Die Funktion **Enable TCP out-of-order** (TCP außerhalb der Reihenfolge aktivieren) aktiviert bzw. deaktiviert die TCP-Out-of-Order-rx-Behandlungsfunktion bei verschobenen iSCSI-Verbindungen.

Standard: Die TCP-Out-of-Order-Funktion ist AKTIVIERT. Zum Beispiel:

```
insmod bnx2i.ko ooo_enable=1
```

oder

```
modprobe bnx2i ooo_enable=1
```

bnx2fc-Treiberparameter

Sie können die optionale Eigenschaft `debug_logging` als Befehlszeilenargument für die Befehle `insmod` oder `modprobe` für `bnx2fc` bereitstellen.

debug_logging

Die Bit-Maske zum Aktivieren der Debugprotokollierung aktiviert bzw. deaktiviert die Debugprotokollierung des Treibers.

Standard: None (Ohne). Zum Beispiel:

```
insmod bnx2fc.ko debug_logging=0xff
```

oder

```
modprobe bnx2fc debug_logging=0xff
```

Debugging auf E/A-Level = 0x1

Debugging auf Sitzungslevel = 0x2

Debugging auf HBA-Level = 0x4

ELS-Debugging = 0x8

Debugging Verschiedenes = 0x10

Max-Debugging = 0xff

Treiberstandardeinstellungen

In den folgenden Abschnitten werden die Parameter für die Treiber ausführlich beschrieben.

- [bnx2-Treiberstandards](#)
- [bnx2x-Treiberstandards](#)

bnx2-Treiberstandards

Geschwindigkeit: Die automatische Aushandlung wird für alle Übertragungsraten angekündigt.

Datenflusssteuerung: Die automatische Aushandlung wird für RX und TX angekündigt.

MTU: 1500 (Bereich von 46 bis 9000)

RX-Ringgröße: 255 (Bereich von 0 bis 4080)

RX-Jumbo-Ringgröße: 0 (Bereich von 0 bis 16320) mit Treiberanpassung auf Basis von MTU und Rx-Ringgröße

TX-Ringgröße: 255 (Bereich (MAX_SKB_FRAGS+1) bis 255).
MAX_SKB_FRAGS ändert sich je nach Kernel und Architektur. Bei einem 2.6-Kernel für x86 liegt MAX_SKB_FRAGS bei 18.

RX-Verbindung Mikrosekunden: 18 (Bereich von 0 bis 1023)

RX-Verbindung Mikrosekunden IRQ: 18 (Bereich von 0 bis 1023)

RX-Verbindung Rahmen: 6 (Bereich von 0 bis 255)

RX-Verbindung Rahmen IRQ: 6 (Bereich von 0 bis 255)

TX-Verbindung Mikrosekunden: 80 (Bereich von 0 bis 1023)

TX-Verbindung Mikrosekunden IRQ: 80 (Bereich von 0 bis 1023)

TX-Verbindung Rahmen: 20 (Bereich von 0 bis 255)

TX-Verbindung Rahmen IRQ: 20 (Bereich von 0 bis 255)

Statistikverbindung Mikrosekunden: 999936 (ungefähr 1 Sekunde) (Bereich von 0 bis 16776960 mit einer Schrittweite von 256)

MSI: Aktiviert (bei Unterstützung durch 2.6.-Kernel und Bestehen des Interrupt-Tests)

TSO: Aktiviert (auf 2.6-Kernel)

WoL: Starteinstellung auf Basis der NVRAM-Einstellung

bnx2x-Treiberstandards

Geschwindigkeit: Die automatische Aushandlung wird für alle Übertragungsraten angekündigt.

Datenflusssteuerung: Die automatische Aushandlung wird für RX und TX angekündigt.

MTU: 1500 (Bereich von 46 bis 9600)

RX-Ringgröße: 4078 (Bereich von 0 bis 4078)

TX-Ringgröße: 4078 (Bereich (MAX_SKB_FRAGS+4) bis 255). MAX_SKB_FRAGS ändert sich je nach Kernel und Architektur. Bei einem 2.6-Kernel für x86 liegt MAX_SKB_FRAGS bei 18.

RX-Verbindung Mikrosekunden: 25 (Bereich von 0 bis 3000)

TX-Verbindung Mikrosekunden: 50 (Bereich von 0 bis 12288)

Statistikverbindung Mikrosekunden: 999936 (ungefähr 1 Sekunde) (Bereich von 0 bis 16776960 mit einer Schrittweite von 256)

MSI-X: Aktiviert (bei Unterstützung durch 2.6.-Kernel und Bestehen des Interrupt-Tests)

TSO: Enabled (Aktiviert)

WoL: Disabled (Deaktiviert)

Treibermeldungen

Die nachfolgende Auflistung zeigt die gängigsten Beispielmeldungen, die in der Datei `/var/log/messages` protokolliert werden können. Geben Sie den Befehl `dmesg -n <Ebene>` aus, um die Ebene zu steuern, auf der Meldungen an der Konsole angezeigt werden. Die meisten Systeme sind standardmäßig auf die Ebene 6 eingestellt. Wenn Sie alle Meldungen sehen möchten, setzen Sie die Ebene höher fest.

- [bnx2x-Treibermeldungen](#)
- [bnx2i-Treibermeldungen](#)
- [bnx2fc-Treibermeldungen](#)

bnx2x-Treibermeldungen

Die bnx2x-Treibermeldungen enthalten folgende Angaben.

Treiberanmeldung

```
QLogic BCM57xx and BCM57xxx 10 Gigabit Ethernet Driver bnx2x  
v1.6.3c (July 23, 2007)
```

C-NIC-Treiberanmeldung (nur bnx2)

QLogic BCM57xx and BCM57xxx cnic v1.1.19 (Sep 25, 2007)

Netzwerkkarte gefunden

```
eth#: QLogic BCM57xx and BCM57xxx xGb (B1)
PCI-E x8 found at mem f6000000, IRQ 16, node addr 0010180476ae
cnic: Added CNIC device: eth0
```

Übertragungsrate und aktive Verbindung

```
bnx2x: eth# NIC Link is Up, 10000 Mbps full duplex
```

Nicht aktive Verbindung

```
bnx2x: eth# NIC Link is Down
MSI-X Enabled Successfully
bnx2x: eth0: using MSI-X
```

bnx2i-Treibermeldungen

Die bnx2xi Treibermeldungen enthalten die folgenden Angaben:

BNX2I-Treiberanmeldung

QLogic BCM57xx and BCM57xxx iSCSI Driver bnx2i v2.1.1D (May 12, 2015)

Netzwerkport zur Transportnamenbindung bei iSCSI

```
bnx2i: netif=eth2, iscsi=bcm570x-050000
bnx2i: netif=eth1, iscsi=bcm570x-030c00
```

Treiber führt Handshake mit iSCSI-Offload-fähigem C-NIC-Gerät durch

```
bnx2i [05:00.00]: ISCSI_INIT passed
```

ANMERKUNG

Diese Meldung wird nur angezeigt, wenn der Benutzer versucht, eine iSCSI-Verbindung herzustellen.

Der Treiber erkennt, dass iSCSI-Offload auf dem C-NIC-Gerät nicht aktiviert ist.

```
bnx2i: iSCSI not supported, dev=eth3
bnx2i: bnx2i: LOM is not enabled to offload iSCSI connections,
dev=eth0
bnx2i: dev eth0 does not support iSCSI
```

Übersteigt maximal zulässige iSCSI-Offload-Obergrenze

```
bnx2i: alloc_ep: unable to allocate iscsi cid
bnx2i: unable to allocate iSCSI context resources
```

Netzwerkpfad zum Zielknoten und Transportnamenbindung sind unterschiedliche Geräte

```
bnx2i: conn bind, ep=0x... ($ROUTE_HBA) does not belong to hba
$USER_CHOSEN_HBA
```

Dabei ist `ROUTE_HBA` das Netzgerät, auf das die Verbindung anhand von Routinginformationen verschoben wurde, und `USER_CHOSEN_HBA` ist der Host Bus Adapter, mit dem der Zielknoten verbunden ist (anhand des iSCSI-Transportnamens)

Ziel ist über keines der C-NIC-Geräte zu erreichen

```
bnx2i: check route, cannot connect using cnic
```

Netzwerkroute ist deaktivierter Netzwerkschnittstelle zugewiesen

```
bnx2i: check route, hba not found
```

SCSI-ML leitet Host-Reset ein (Sitzungswiederherstellung)

```
bnx2i: attempting to reset host, #3
```

C-NIC erfasst iSCSI-Protokollverstoß – Schwerwiegende Fehler

```
bnx2i: iscsi_error - wrong StatSN rcvd
bnx2i: iscsi_error - hdr digest err
bnx2i: iscsi_error - data digest err
bnx2i: iscsi_error - wrong opcode rcvd
bnx2i: iscsi_error - AHS len > 0 rcvd
bnx2i: iscsi_error - invalid ITT rcvd
bnx2i: iscsi_error - wrong StatSN rcvd
bnx2i: iscsi_error - wrong DataSN rcvd
bnx2i: iscsi_error - pend R2T violation
bnx2i: iscsi_error - ERL0, U0
bnx2i: iscsi_error - ERL0, U1
bnx2i: iscsi_error - ERL0, U2
bnx2i: iscsi_error - ERL0, U3
bnx2i: iscsi_error - ERL0, U4
bnx2i: iscsi_error - ERL0, U5
bnx2i: iscsi_error - ERL0, U
bnx2i: iscsi_error - invalid resi len
bnx2i: iscsi_error - MRDSL violation
bnx2i: iscsi_error - F-bit not set
bnx2i: iscsi_error - invalid TTT
bnx2i: iscsi_error - invalid DataSN
bnx2i: iscsi_error - burst len violation
bnx2i: iscsi_error - buf offset violation
bnx2i: iscsi_error - invalid LUN field
bnx2i: iscsi_error - invalid R2TSN field
bnx2i: iscsi_error - invalid cmd len1
bnx2i: iscsi_error - invalid cmd len2
bnx2i: iscsi_error - pend r2t exceeds MaxOutstandingR2T value
bnx2i: iscsi_error - TTT is rsvd
bnx2i: iscsi_error - MBL violation
bnx2i: iscsi_error - data seg len != 0
bnx2i: iscsi_error - reject pdu len error
bnx2i: iscsi_error - async pdu len error
bnx2i: iscsi_error - nopin pdu len error
bnx2i: iscsi_error - pend r2t in cleanup
bnx2i: iscsi_error - IP fragments rcvd
bnx2i: iscsi_error - IP options error
bnx2i: iscsi_error - urgent flag error
```

C-NIC Detects iSCSI Protocol Violation – Keine schwerwiegende Warnung

```
bnx2i: iscsi_warning - invalid TTT
bnx2i: iscsi_warning - invalid DataSN
bnx2i: iscsi_warning - invalid LUN field
```

ANMERKUNG

Der Treiber muss so konfiguriert werden, dass bestimmte Verstöße als Warnung und nicht als schwerwiegende Fehler behandelt werden.

Treiber führt Wiederherstellung einer Sitzung durch

```
conn_err - hostno 3 conn 03fbcd00, iscsi_cid 2 cid a1800
```

Abgelehnte iSCSI-PDU vom Ziel erhalten

```
bnx2i - printing rejected PDU contents
[0]: 1 fffffffa1 0 0 0 0 20 0
[8]: 0 7 0 0 0 0 0 0
[10]: 0 0 40 24 0 0 fffffff80 0
[18]: 0 0 3 fffffff88 0 0 3 4b
[20]: 2a 0 0 2 fffffffc8 14 0 0
[28]: 40 0 0 0 0 0 0 0
```

Open-iSCSI-Daemon übergibt Sitzung an Treiber

```
bnx2i: conn update - MBL 0x800 FBL 0x800MRDSL_I 0x800 MRDSL_T
0x2000
```

bnx2fc-Treibermeldungen

Die bnx2xi-Treibermeldungen enthalten die folgende Angaben:

BNX2FC-Treiberanmeldung

```
QLogic FCoE Driver bnx2fc v0.8.7 (Mar 25, 2011)
```

Treiber führt Handshake mit FCoE-Offload-fähigem C-NIC-Gerät durch

```
bnx2fc [04:00.00]: FCOE_INIT passed
```

Treiber führt Handshake mit iSCSI-Offload-fähigem C-NIC-Gerät nicht durch

```
bnx2fc: init_failure due to invalid opcode
bnx2fc: init_failure due to context allocation failure
bnx2fc: init_failure due to NIC error
bnx2fc: init_failure due to completion status error
bnx2fc: init_failure due to HSI mismatch
```

Keine gültige Lizenz, um FCoE zu starten

```
bnx2fc: FCoE function not enabled <ethX>
bnx2fc: FCoE not supported on <ethX>
```

Sitzungsfehler aufgrund der Überschreitung des erlaubten FCoE-Offload-Verbindungslimits oder Arbeitsspeicherlimits

```
bnx2fc: Failed to allocate conn id for port_id <remote port id>
bnx2fc: exceeded max sessions..logoff this tgt
bnx2fc: Failed to allocate resources
```

Offload-Fehler der Sitzung

```
bnx2fc: bnx2fc_offload_session - Offload error
<rport> not FCP type. not offloading
<rport> not FCP_TARGET. not offloading
```

Upload-Fehler in der Sitzung

```
bnx2fc: ERROR!! destroy timed out
bnx2fc: Disable request timed out. destroy not set to FW
bnx2fc: Disable failed with completion status <Status>
bnx2fc: Destroy failed with completion status <Status>
```

ABTS kann nicht gesendet werden

```
bnx2fc: initiate_abts: tgt not offloaded
bnx2fc: initiate_abts: rport not ready
bnx2fc: initiate_abts: link is not ready
bnx2fc: abort failed, xid = <xid>
```

Aufgrund einer Zeitüberschreitung in ABTS kann die E/A unter Verwendung von ABTS nicht wiederhergestellt werden.

```
bnx2fc: Relogin to the target
```

Aufgrund einer nicht abgeschlossenen Sitzung kann E/A-Anfrage (Eingabe/Ausgabe) nicht durchgeführt werden.

```
bnx2fc: Unable to post io_req
```

Falsche L2-Empfangsframes verwerfen

```
bnx2fc: FPMA mismatch... drop packet  
bnx2fc: dropping frame with CRC error
```

Host Bus Adapter und lport-Zuweisungsfehler

```
bnx2fc: Unable to allocate hba  
bnx2fc: Unable to allocate scsi host
```

NPIV Port Erstellung

```
bnx2fc: Setting vport names, <WWNN>, <WWPN>
```

Teaming-Funktion mit Channel Bonding

Mit den Linux-Treibern können Sie Adapter in einem Team gruppieren, indem Sie Bonding-Kernel-Module und eine Channel Bonding-Schnittstelle verwenden. Weitere Informationen finden Sie unter den Channel Bonding-Informationen in der Dokumentation Ihres Betriebssystems.

Statistikdaten

Detaillierte Statistikdaten und Konfigurationsinformationen können über das ethtool-Dienstprogramm angezeigt werden. Weitere Informationen erhalten Sie auf der Man-Page für ethtool.

iSCSI-Verschiebung in Linux

Die Informationen zum iSCSI-Offload in Linux enthalten die folgenden Angaben:

- [Open-iSCSI-Benutzeranwendungen](#)
- [Benutzeranwendung - iscsiui0](#)
- [Verbinden Sie das iSCSI-Ziel mit dem QLogiciSCSI-Transportnamen](#)
- [VLAN-Konfiguration für iSCSI-Offload \(Linux\)](#)
- [Herstellen von Verbindungen mit iSCSI-Zielen](#)
- [Maximale Offload-iSCSI-Verbindungen](#)
- [Häufig gestellte Fragen zu Linux iSCSI-Offload](#)

Open-iSCSI-Benutzeranwendungen

Installieren Sie die integrierten open-iscsi-Initiator-Programme von der DVD, und führen Sie sie aus. Weitere Details finden Sie unter [„Verfügbare Pakete“](#) auf [Seite 37](#).

Benutzeranwendung - iscsiui0

Installieren Sie den iscsiui0-Daemon, bevor Sie iSCSI-Verbindungen erstellen, und führen Sie ihn aus. Der Treiber kann ohne den Daemon keine Verbindungen zum iSCSI-Ziel herstellen.

Installieren Sie den iscsiui0-Daemon:

1. Installieren Sie das Quell-Paket iscsiui0 wie folgt:

```
# tar -xvzf iscsiui0-<version>.tar.gz
```
2. Wechsel zum Verzeichnis, in das iscsiui0 extrahiert wird

```
# cd iscsiui0-<version>
```
3. Kompilieren und installieren Sie wie folgt:

```
# ./configure  
# make  
# make install
```
4. Stellen Sie sicher, dass die Iscsiui0-Version mit dem Quell-Paket wie folgt übereinstimmt:

```
# iscsiui0 -v
```
5. Starten sie iscsiui0 wie folgt:

```
# iscsiui0
```

Verbinden Sie das iSCSI-Ziel mit dem QLogiciSCSI-Transportnamen

Standardmäßig stellt der Open-iscsi-Daemon eine Verbindung zu erfassten Zielen mit dem Softwareinitiator (`transport name = 'tcp'`) her. Benutzer, die die iSCSI-Verbindung auf ein C-NIC-Gerät verschieben wollen, sollten die Transportbindung explizit über iSCSI iface ändern. Dies kann mithilfe des CLI-Dienstprogramms `iscsiadm` folgendermaßen vorgenommen werden,

```
iscsiadm -m iface -I <iface_file_name> -n iface.transport_name -v  
bnx2i -o update
```

Hierbei enthält die `iface`-Datei die folgenden Informationen für SLES 11 SP1:

```
iface.net_ifacename = ethX
iface.iscsi_ifacename = <name of the iface file>
iface.hwaddress = xx:xx:xx:xx:xx:xx
iface.ipaddress = XX.XX.XX.XX
iface.transport_name = bnx2i
```

Achten Sie darauf, dass der Wert für `iface.hwaddress` in Kleinbuchstaben angegeben wird.

Wenn Sie wieder auf den Software-Initiator zurückgreifen möchten, geben Sie Folgendes ein:

```
iscsiadm -m iface -I <iface_file_name> -n iface.transport_name -v
tcp -o update
```

Wobei die `iface`-Datei die folgenden Informationen enthält:

```
iface.net_ifacename = ethX
iface.iscsi_ifacename = <name of the iface file>
iface.transport_name = tcp
```

VLAN-Konfiguration für iSCSI-Offload (Linux)

iSCSI-Datenverkehr im Netzwerk kann in einem VLAN isoliert werden, um ihn von anderem Datenverkehr zu trennen. In so einem Fall muss die iSCSI-Schnittstelle auf dem Adapter Teil des VLAN sein.

Um das iSCSI-VLAN zu konfigurieren, fügen Sie die VLAN-ID in der `iface`-Datei für iSCSI hinzu. Im folgenden Beispiel ist die VLAN-ID auf 100 festgelegt.

```
#Begin Record 6.2.0-873.2.el6
Iface.iscsi_ifacefile name = <>
Iface.ipaddress = 0.0.0.0
Iface.hwaddress = <>
Iface.trasport_name = bnx2i
Iface.vlan_id = 100
Iface.vlan_priority = 0
Iface.iface_num = 100
Iface.mtu = 0
Iface.port = 0
#END Record
```

ANMERKUNG

Obwohl es nicht zwingend erforderlich ist, empfiehlt QLogic, die gleiche VLAN-ID im Feld `iface.iface_num` zur Identifikation der `iface`-Datei zu konfigurieren.

Herstellen von Verbindungen mit iSCSI-Zielen

In der Dokumentation zu `open-scsi` finden Sie eine umfassende Liste der `iscsiadm`-Befehle. Es folgt eine Beispielliste für Befehle für die Zielerkennung und für das Erstellen von `iscsi`-Verbindungen mit einem Ziel.

Statische Eingabe hinzufügen

```
iscsiadm -m node -p <ipaddr[:port]> -T  
iqn.2007-05.com.qlogic:target1 -o new -I <iface_file_name>
```

iSCSI-Zielermittlung mithilfe von `sendtargets`

```
iscsiadm -m discovery --type sendtargets -p <ipaddr[:port]> -I  
<iface_file_name>
```

Anmeldung beim Ziel mit dem Befehl `iscsiadm`

```
iscsiadm --mode node --targetname <iqn.targetname> --portal  
<ipaddr[:port]> --login
```

Auflisten aller im System aktiven Laufwerke

```
fdisk -l
```

Maximale Offload-iSCSI-Verbindungen

Wenn für die Treiberparameter Standardwerte festgelegt wurden, was 128 ausstehende Befehle umfasst, kann `bnx2i` 128 Verbindungen auf QLogic BCM5771x-Adapter verschieben.

Diese Anzahl ist keine feste Obergrenze, sondern basiert auf einer einfachen vom Chip durchgeführten Ressourcenzuweisungsberechnung. `bnx2i` kann mehr Verbindungen verschieben, indem die Größe der gemeinsamen Warteschlange verringert wird, was wiederum die maximale Anzahl ausstehender Aufgaben in einer Verbindung verringert. Siehe „[Einstellen der Werte für optionale Eigenschaften](#)“ auf Seite 47 für Informationen zu `sq_size` und `rq_size`. Wenn die maximal zulässige Offload-Obergrenze erreicht wurde, gibt der Treiber die folgende Meldung im `syslog` (Systemprotokoll) aus:

```
bnx2i: unable to allocate iSCSI context resources
```

Häufig gestellte Fragen zu Linux iSCSI-Offload

- Nicht alle QLogic BCM57xx und BCM57xxx-Adapter unterstützen iSCSI-Offload.
- Die iSCSI-Sitzung wird nach Hot-Remove und Hot-Plug nicht wiederhergestellt.
- Damit Microsoft Multipfad-E/A (MPIO) ordnungsgemäß funktioniert, müssen Sie iSCSI `noopout` in jeder iSCSI-Sitzung aktivieren. Die Vorgänge für das Einrichten von Werten für `noop_out_interval` und `noop_out_timeout` finden Sie in der Open-iSCSI-Dokumentation.
- In einem Szenario, in dem sich mehrere C-NIC-Geräte im System befinden und das System über die QLogic iSCSI-Bootlösung gebootet wird, ist sicherzustellen, dass der `iscsi`-Knoten unter `/etc/iscsi/nodes` für das Boot-Ziel mit der NIC verbunden ist, die für den Bootvorgang verwendet wird.

8

VMware-Treibersoftware

In diesem Kapitel werden folgende Themen zur VMware-Treibersoftware behandelt:

- [Verfügbare Pakete](#)
- [Netzwerkunterstützung, Treiber](#)
- [„Unterstützung von FCoE“ auf Seite 70](#)
- [„iSCSI-Unterstützung“ auf Seite 73](#)

ANMERKUNG

Informationen in diesem Kapitel beziehen sich hauptsächlich auf die aktuell unterstützten VMware-Versionen: ESXi 6.0 U2, ESXi 6.5 und ESXi 6.7. ESXi 6.7 verwendet eigene Treiber für alle Protokolle.

Verfügbare Pakete

Der VMware-Treiber ist in den in [Tabelle 8-1](#) aufgeführten Paketformaten verfügbar.

Tabelle 8-1. VMware-Treiberpakete

Merkmal	Treiber
Komprimierte Zip-Datei	QLG-NetXtremeIIversion.zip (ESXi 6.0, ESXi 6.5)
Komprimierte Zip-Datei	QLG-qcnic-offline_bundle.zip (ESXi 6.7)

Netzwerkunterstützung, Treiber

In diesem Abschnitt wird der VMware ESXi-Treiber `bnx2x` für QLogic BCM57xx und BCM57xxx PCIe 10 GbE-Netzwerkadapter beschrieben. Er enthält folgende Informationen: Herunterladen, Installieren und Aktualisieren von VMware-Treibern sowie Entladen und Entfernen von Treibern, Erklärungen der Treiberparameter, Standardeinstellungen und Treibermeldungen.

Herunterladen, Installieren und Aktualisieren von Treibern

Informationen zum Herunterladen, Installieren und Aktualisieren des VMware ESXi-Treibers für BCM57xx und BCM57xxx 10 GbE-Netzwerkadapter finden Sie unter <http://www.vmware.com/support>. Das Paket ist doppelt gezippt. Entzippen Sie das Paket, bevor Sie es in den ESXi-Host kopieren.

Treiberparameter

Sie können mehrere optionale Parameter als Befehlszeilenargument für den Befehl `vmkload_mod` angeben. Stellen Sie diese Parameter ein, indem Sie den Befehl `esxcfg-module` ausgeben. Für weitere Informationen führen Sie den folgenden Befehl aus: `esxcfg-module -h`.

`int_mode`

Verwenden Sie den optionalen Parameter `int_mode`, um die Verwendung eines anderen Interrupt-Modus als MSI-X zu erzwingen. Der Treiber versucht standardmäßig, MSI-X zu aktivieren, wenn dieser Modus vom Kernel unterstützt wird. Wenn MSI-X nicht verfügbar ist, versucht der Treiber, MSI zu aktivieren, wenn es vom Kernel unterstützt wird. Wenn MSI nicht verfügbar ist, verwendet der Treiber den Legacy-Modus INTx.

Um die Verwendung von Legacy-Modus INTx auf allen Netzwerkadaptern BCM57xx und BCM57xxx des Systems zu erzwingen, setzen Sie den Parameter `int_mode` auf 1 (siehe unten):

```
vmkload_mod bnx2x int_mode=1
```

Um die Verwendung des MSI-Modus auf allen BCM57xx und BCM57xxx-Netzwerkadaptern des Systems zu erzwingen, setzen Sie den Parameter `int_mode` auf 2 (siehe unten):

```
vmkload_mod bnx2x int_mode=2
```

`disable_tpa`

Verwenden Sie den optionalen Parameter `disable_tpa`, um die Funktion „Transparent Packet Aggregation“ (TPA) zu deaktivieren. Standardmäßig bündelt der Treiber TCP-Pakete.

Um die TPA-Funktion auf allen BCM57xx und BCM57xxx-Netzwerkadaptern des Systems zu deaktivieren, setzen Sie den Parameter `disable_tpa` auf 1 (siehe unten):

```
vmkload_mod bnx2x disable_tpa=1
```

Verwenden Sie `ethtool`, um TPA (LRO) für einen bestimmten Netzwerkadapter zu deaktivieren.

num_queues

Legen Sie mit dem Parameter `num_queues` die Anzahl der Warteschlangen fest (standardmäßig ist die Anzahl der CPUs eingestellt).

pri_map

Verwenden Sie den optionalen Parameter `pri_map`, um den VLAN-PRI-Wert oder den IP-DSCP-Wert in der Hardware auf eine andere oder dieselbe Dienstklasse zu setzen. Der Treiber wertet diesen 32-Bit-Parameter als 8 Werte mit jeweils 4 Bits aus. Jedes Nibble legt die erforderliche Hardware-Warteschlangennummer für diese Priorität fest.

Wenn Sie für den Parameter `pri_map` beispielsweise den Wert `0x22221100` festlegen, wird der Dienstklasse 0 die Priorität 0 und 1, der Dienstklasse 1 die Priorität 2 und 3 und der Dienstklasse 2 die Priorität 4 bis 7 zugeordnet. Wenn Sie in einem anderen Beispiel für den Parameter `pri_map` den Wert `0x11110000` festlegen, wird der Dienstklasse 0 die Priorität 0 bis 3 und der Dienstklasse 1 die Priorität 4 bis 7 zugeordnet.

dropless_fc

Mit dem optionalen Parameter `dropless_fc` können Sie einen zusätzlichen Mechanismus zur Durchflusssteuerung in den QLogic-Netzwerkadaptern aktivieren. Der Standardmechanismus zur Datenflusssteuerung sendet PAUSE Frames, wenn der Puffer auf dem Chip (BRD) einen bestimmten Belegungsgrad erreicht hat. Diese Belegung ist eine leistungsorientierte Datenflusssteuerung. Bei Verwendung von QLogic-Netzwerkadaptern können Sie einen anderen Mechanismus zur Datenflusssteuerung zum Senden von PAUSE Frames aktivieren, wenn einer der Hostpuffer (im RSS-Modus) voll ist. Die PAUSE Frames bieten einen gezielten „Zero Packet Drop“-Mechanismus zur Datenflusssteuerung.

Setzen Sie, um den „Dropless“-Mechanismus zur Datenflusssteuerung auf allen QLogic-Netzwerkadaptern des Systems zu aktivieren, den Parameter `dropless_fc` auf 1 (siehe unten):

```
vmkload_mod bnx2x int_mode=1
```

RSS

Verwenden Sie den optionalen Parameter `RSS`, um die Anzahl der Warteschlangen für die empfangsseitige Skalierung zu bestimmen. Bei VMware ESXi 6.0 U2 und 6.5 können die `RSS`-Werte 2 bis 4 sein; `RSS=1` deaktiviert die RSS-Warteschlangen.

max_vfs

Verwenden Sie den optionalen Parameter `max_vfs`, um eine bestimmte Menge an virtuellen Funktionen zu aktivieren. Werte für `max_vfs` können 1 bis 64 sein oder setzen Sie `max_vfs=0` (Standard), um alle virtuellen Funktionen zu deaktivieren.

enable_vxlan_ofld

Verwenden Sie den optionalen Parameter `enable_vxlan_ofld`, um VXLAN-Taskabladungen mit TX TSO und TX CSO zu aktivieren. Bei VMware ESXi 6.0 U2 und 6.5 aktiviert `enable_vxlan_ofld=1` (Standard) VXLAN-Taskabladungen, und `enable_vxlan_ofld=0` deaktiviert VXLAN-Taskabladungen.

enable_default_queue_filters

Verwenden Sie den optionalen Parameter `enable_default_queue_filters`, um die Klassifizierungsfiler in der Warteschlange zu aktivieren. Die Hardware unterstützt insgesamt 512 Klassifizierungsfiler, die gleichmäßig auf die Ports eines Adapters aufgeteilt werden. Ein Quad-Port-Adapter hat z. B. 128 Filter pro Port. Bei einer NPAR-Konfiguration werden die Filter auf die Standardwarteschlange angewendet, damit der Datenverkehr zwischen den Partitionen desselben physischen Ports umgeleitet werden kann.

Überschreitet die Menge der Filter die Hardwaregrenzen, wird in den vmkernel-Protokollen die Meldung `Rx filters on NetQ Rx Queue 0 exhausted` (Rx-Filter in NetQ Rx-Warteschlange 0 erschöpft) angezeigt. Diese Meldung teilt mit, dass das Hardware-Filterlimit erreicht wurde und keine weiteren Einträge hinzugefügt werden können. Sie können Filter für die Standardwarteschlange deaktivieren, indem Sie den Parameter `enable_default_queue_filters` auf 0 einstellen. Dadurch wird die Umleitung des Datenverkehrs auf andere Partitionen deaktiviert.

enable_live_grcdump

Verwenden Sie den Parameter `enable_live_grcdump`, um anzuzeigen, welcher Firmware-Dump für die Fehlerbehebung erfasst wird. Gültige Werte:

Wert	Beschreibung
-------------	---------------------

0x0	Live Global Register Controller (GRC)-Dump deaktivieren
0x1	Parität/Live GRC-Dump (Standard) aktivieren
0x2	Sende-Zeitüberschreitung für GRC-Dump aktivieren
0x4	Statistik-Zeitüberschreitung für GRC-Dump aktivieren

Die Standardeinstellung eignet sich in den meisten Situationen. Ändern Sie den Standardwert nur nach Aufforderung durch das Support-Team.

Treiberstandardeinstellungen

Standardeinstellungen für VMware ESXi-Treiber `bnx2x` lauten wie folgt:

Geschwindigkeit: Die automatische Aushandlung wird für alle Übertragungsraten angekündigt.

Datenflusssteuerung: Die automatische Aushandlung wird für RX und TX angekündigt.

MTU: 1500 (Bereich 46-9600)

Rx-Ringgröße: 4078 (Bereich 0-4078)

Tx-Ringgröße: 4078 (Bereich (MAX_SKB_FRAGS+4) - 4078).

MAX_SKB_FRAGS ändert sich je nach Kernel und Architektur. Bei einem 2.6-Kernel für x86 liegt MAX_SKB_FRAGS bei 18.

RX-Verbindung Mikrosekunden: 25 (Bereich 0-3000)

TX-Verbindung Mikrosekunden: 50 (Bereich 0-12288)

MSI-X: Aktiviert (bei Unterstützung durch 2.6-Kernel)

TSO: Enabled (Aktiviert)

WoL: Disabled (Deaktiviert)

Entfernen des Treibers

Geben Sie zum Entladen des VMware ESXi-Treibers `bnx2x` den folgenden Befehl aus:

```
vmkload_mod -u bnx2x
```

Treibermeldungen

Die nachfolgende Auflistung zeigt die gängigsten Beispielmeldungen des VMware ESXi-Treibers `bnx2x`, die in der Datei `/var/log/vmkernel.log` protokolliert werden können. Geben Sie den Befehl `dmesg -n <level>` aus, um die Ebene zu steuern, auf der Meldungen an der Konsole angezeigt werden. Die meisten Systeme sind standardmäßig auf die Ebene 6 eingestellt. Wenn Sie alle Meldungen sehen möchten, setzen Sie die Ebene höher fest.

Treiberanmeldung

```
QLogic BCM57xxx 10Gigabit Ethernet Driver  
bnx2x 0.40.15 ($DateTime: 2015/11/22 05:32:40 $)
```

Netzwerkschnittstellenkarte erkannt

```
bnx2x: msix capability found  
bnx2x: part number 0-0-0-0  
PCI: driver bnx2x claimed device 0000:01:00.0
```

MSI-X erfolgreich aktiviert

```
bnx2x 0000:01:00.0: vmnic0: using MSI-X  IRQs: sp 16  fp[0] 28 ...  
fp[7] 35
```

Übertragungsrate und aktive Verbindung

```
bnx2x 0000:01:00.0: vmnic0: NIC Link is Up, 10000 Mbps full duplex,  
Flow control: ON - receive & transmit
```

Nicht aktive Verbindung

```
bnx2x 0000:01:00.1: vmnic0: NIC Link is Down
```

Speichereinschränkung

Die folgenden Meldungen in der Protokolldatei weisen darauf hin, dass der ESXi-Host stark überlastet ist. Deaktivieren Sie `NetQueue`, um diese Belastung zu reduzieren.

```
Dec  2 18:24:20 ESX4 vmkernel: 0:00:00:32.342 cpu2:4142)WARNING:  
Heap: 1435: Heap bnx2x already at its maximumSize. Cannot expand.  
Dec  2 18:24:20 ESX4 vmkernel: 0:00:00:32.342 cpu2:4142)WARNING:  
Heap: 1645: Heap_Align(bnx2x, 4096/4096 bytes, 4096 align) failed.  
caller: 0x41800187d654  
Dec  2 18:24:20 ESX4 vmkernel: 0:00:00:32.342 cpu2:4142)WARNING:  
vmklinux26: alloc_pages: Out of memory
```

Um NetQueue über das manuelle Laden des bnx2x VMkernel-Moduls zu deaktivieren, führen Sie den folgenden Befehl aus:

```
vmkload_mod bnx2x num_queues=1
```

Sie können die Einstellungen auch nach Neustarts mit dem folgenden Befehl beibehalten:

```
esxcfg-module -s num_queues =1 bnx2x
```

Starten Sie das Gerät neu, damit die Einstellungen in Kraft treten.

Multiqueue und NetQueue

Verwenden Sie den optionalen Parameter `num_queues`, um die Anzahl der Rx- und Tx-Warteschlangen festzulegen, wenn `multi_mode` auf 1 und der Interrupt-Modus auf MSI-X gesetzt ist. Ist ein anderer Interrupt-Modus als MSI-X festgelegt (siehe Parameter „`int_mode`“ auf Seite 65), wird die Anzahl der Rx- und Tx-Warteschlangen ungeachtet der Einstellung für diesen Parameter auf 1 gesetzt.

Wenn Sie mehr als eine Warteschlange verwenden möchten, legen Sie die Anzahl der zu verwendenden NetQueues fest, indem Sie den folgenden Befehl ausgeben:

```
esxcfg-module -s "num_queues=<num of queues>" bnx2x
```

Lassen Sie andernfalls mit dem folgenden Befehl zu, dass der bnx2x-Treiber die Anzahl der zu verwendenden NetQueues auswählt:

```
esxcfg-module -s "num_queues=0" bnx2x
```

Am besten entspricht die Anzahl der NetQueues der Anzahl der CPUs am Gerät.

Unterstützung von FCoE

In diesem Abschnitt werden die Inhalte und Installationsverfahren des VMware-Softwarepakets für die Unterstützung von QLogic FCoE C-NICs beschrieben.

Treiber

Der QLogic BCM57xx und BCM57xxx FCoE-Treiber umfasst bnx2x und bnx2fc.

- Dieser **bnx2x**-Treiber verwaltet alle PCI-Geräteressourcen (Register, Hostschnittstellen-Warteschlangen usw.) und dient außerdem als Schicht-2-VMware-Netzwerktreiber der unteren Ebene für das QLogic BCM57xx und BCM57xxx-10G-Gerät. Durch diesen Treiber wird die Hardware direkt gesteuert. Er ist außerdem für das Senden und Empfangen

von Ethernet-Paketen für den VMware-Hostnetzwerk-Stack verantwortlich. Der bnx2x-Treiber empfängt und verarbeitet darüber hinaus Geräte-Interrupts, sowohl für sich selbst (für L2-Netzwerke) als auch für die bnx2fc-Treiber (FCoE-Protokoll) und C-NIC-Treiber.

- Der **bnx2fc** QLogic VMware FCoE-Treiber ist ein Kernel-Modultreiber, mit dem eine Übersetzungsschicht zwischen dem VMware SCSI-Stack und der QLogic FCoE-Firmware und -Hardware bereitgestellt wird. Darüber hinaus ist der Treiber mit der Netzwerkschicht verbunden, um eingekapselte FCoE-Frames für libfc und libfcOE von Open-FCoE für die FIP-/Geräteerkennung zu übertragen und zu empfangen.

Unterstützte Distributionen

Die FCoE und DCB-Funktionen werden unter VMware ESXi 6.0 und höheren Versionen unterstützt.

Aktivieren von FCoE

So aktivieren Sie die FCoE-Hardwareabladung auf dem C-NIC:

1. Bestimmen Sie die FCoE-fähigen Ports, indem Sie den folgenden Befehl ausgeben:

```
# esxcli fcoe nic list
```

Ausgabebeispiel:

```
vmnic4
User Priority: 3
Source MAC: FF:FF:FF:FF:FF:FF
Active: false
Priority Settable: false
Source MAC Settable: false
VLAN Range Settable: false
VN2VN Mode Enabled: false
```

2. Aktivieren Sie die FCoE-Schnittstelle wie folgt:

```
# esxcli fcoe nic discover -n vmnicX
```

Dabei steht **x** für die Schnittstellenummer, die in [Schritt 1](#) bestimmt wurde.

3. Stellen Sie sicher, dass die Schnittstelle folgendermaßen funktioniert:

```
# esxcli fcoe adapter list
```

Ausgabebeispiel:

```
vmhba34
Source MAC: bc:30:5b:01:82:39
FCF MAC: 00:05:73:cf:2c:ea
VNPort MAC: 0e:fc:00:47:04:04
Physical NIC: vmn7
User Priority: 3
VLAN id: 2008
VN2VN Mode Enabled: false
```

Die Ausgabe dieses Befehls muss eine gültige FCoE-Weiterleitung (FCF) MAC, VNPort MAC, Priorität und VLAN-ID für die Fabric, die mit dem C-NIC verbunden ist, anzeigen.

Sie können auch mit dem folgenden Befehl überprüfen, ob die Schnittstelle ordnungsgemäß funktioniert:

```
# esxcfg-scsidevs -a
```

Ausgabebeispiel:

```
vmhba34 bnx2fc link-up fcoe.1000<mac address>:2000<mac address>
vmhba35 bnx2fc link-up fcoe.1000<mac address>:2000<mac address>
```

ANMERKUNG

Die Bezeichnung `Software FCoE` ist ein VMware-Begriff, mit dem Initiatoren beschrieben werden, die von den Posteingangs-FCoE-Bibliotheken und -Dienstprogrammen abhängen. Die FCoE-Lösung von QLogic stellt eine vollständig zustandsbehaftete, verbundungs-basierte Hardware-Entlastungslösung dar, mit der die CPU-Belastung durch einen Non-Offload-Softwareinitiator erheblich reduziert wird.

Installationsprüfung

Führen Sie die nachfolgend beschriebenen Schritte aus, um die richtige Installation des Treibers zu überprüfen und sicherzustellen, dass der Hostport für den Switch sichtbar ist.

So überprüfen Sie die richtige Installation des Treibers:

1. Prüfen Sie mit einem der folgenden Befehle, ob der Hostport in der Datenbank des Fabric Login (FLOGI) des Switch angezeigt wird:

```
show flogi database (bei Cisco FCF)
```

```
fcoe -loginshow (bei Brocade FCF)
```

2. Wenn der Host-WWPN nicht in der FLOGI-Datenbank angezeigt wird, prüfen Sie die Treiberprotokollmeldungen.

Einschränkungen

Folgende Einschränkungen gelten für FCoE-Support:

- NPIV wird zurzeit aufgrund von Abhängigkeiten von unterstützenden Komponenten (libfc, libfcoe) und Modulen nicht auf ESXi mit abhängigen Hardwarelösungen unterstützt.
- Non-Offload-FCoE wird bei Offload-fähigen QLogic-Geräten nicht unterstützt. Nur der vollständige Hardware-Offload-Pfad wird unterstützt.

iSCSI-Unterstützung

QLogic stellt den bnx2i-Treiber zur Unterstützung von iSCSI bereit. Der QLogic BCM57xx und BCM57xxx iSCSI-Treiber, bnx2i, ist ein QLogic VMware iSCSI Host Bus Adapter-Treiber. Ähnlich wie bnx2fc ist bnx2i ebenfalls ein Kernel-Modultreiber, mit dem eine Übersetzungsschicht zwischen dem VMware SCSI-Stack und der QLogic iSCSI-Firmware und -Hardware bereitgestellt wird. bnx2i funktioniert unter Open-iSCSI-Framework.

VLAN-Konfiguration für iSCSI-Offload (VMware)

iSCSI-Datenverkehr im Netzwerk kann in einem VLAN isoliert werden, um ihn von anderem Datenverkehr zu trennen. In so einem Fall muss die iSCSI-Schnittstelle auf dem Adapter Teil des VLAN sein.

So konfigurieren Sie das VLAN mit dem vSphere-Client (GUI):

1. Wählen Sie ESXi-Host.
2. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration).
3. Klicken Sie auf der Seite „Configuration“ (Konfiguration) auf den Link **Networking** (Netzwerkbetrieb) und anschließend auf **Properties** (Eigenschaften).
4. Klicken Sie auf der ausgewählten Seite „vSwitch Properties“ (vSwitch-Eigenschaften), „Ports“ (Ports) auf die virtuellen Switch- oder Port-Gruppen und anschließend auf **Edit** (Bearbeiten).
5. (Optional) Weisen Sie auf der Seite „VM Network Properties“ (VM-Netzwerkeigenschaften), „General“ (Allgemein) eine VLAN-Nummer im Feld **VLAN ID** (VLAN-ID) zu. [Abbildung 8-1](#) und [Abbildung 8-2](#) zeigen Beispiele.

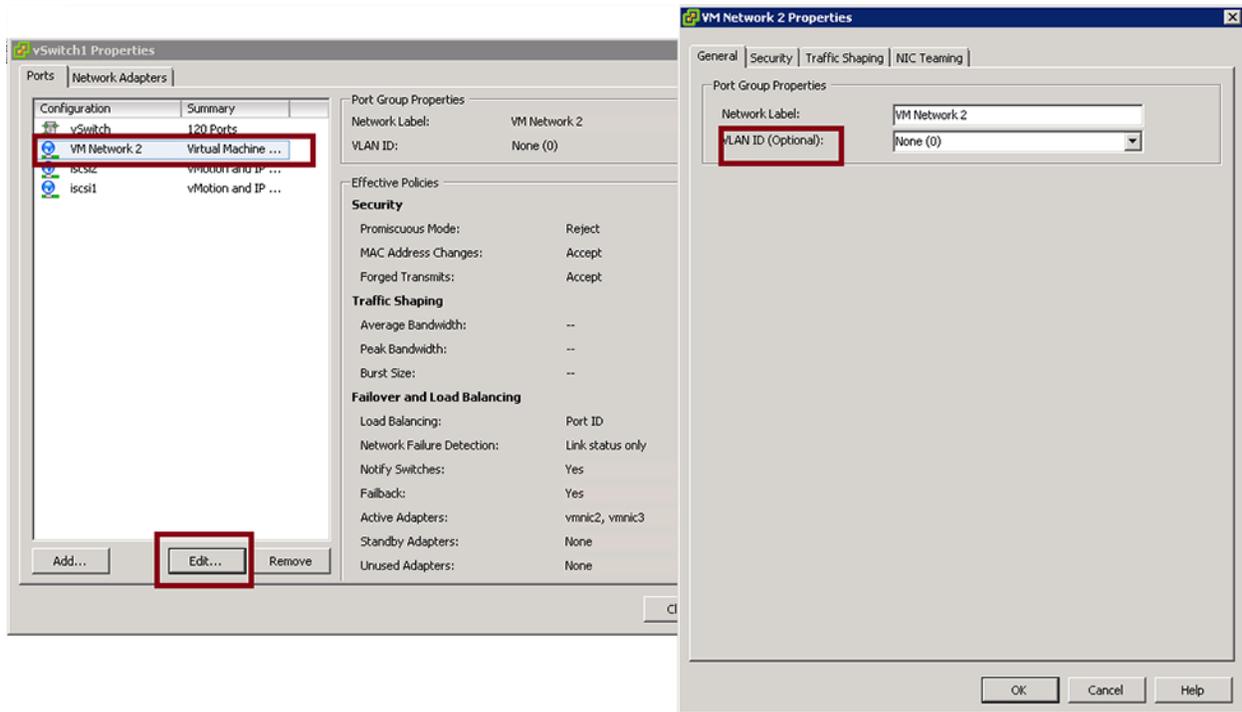


Abbildung 8-1. VM Network Properties (VM-Netzwerkeigenschaften): Beispiel 1

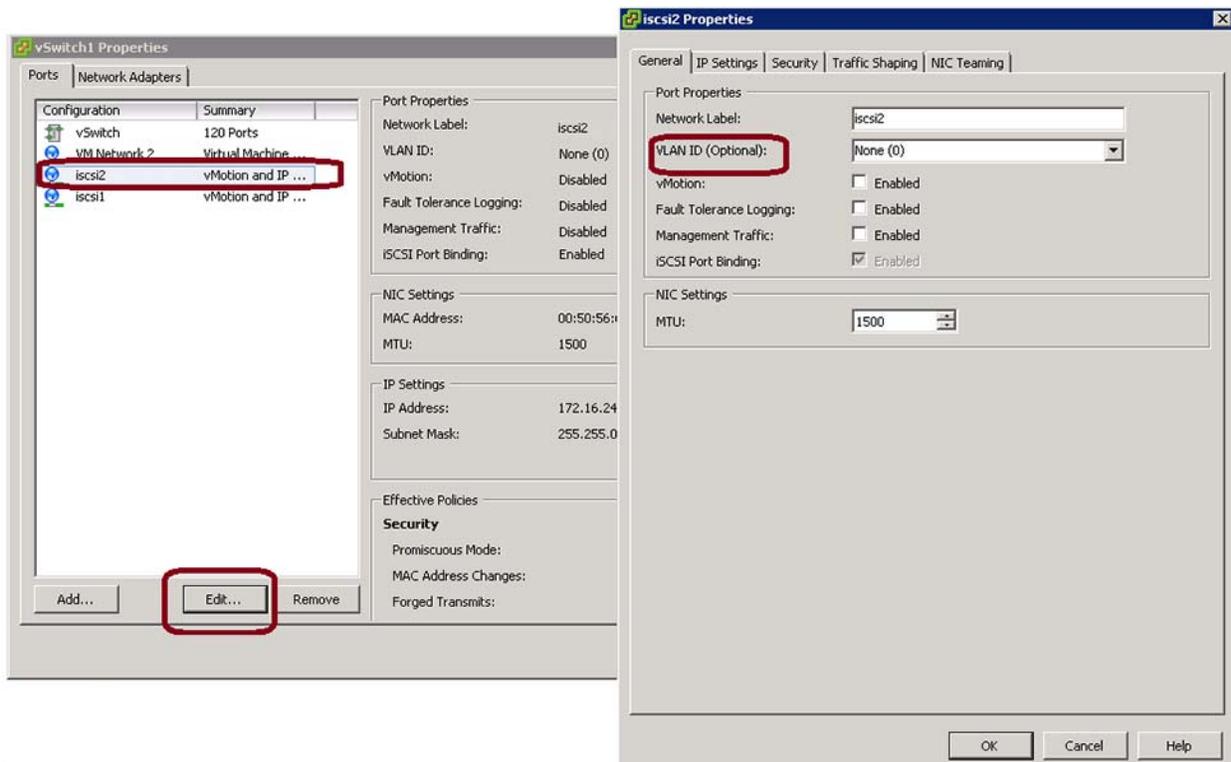


Abbildung 8-2. VM Network Properties (VM-Netzwerkeigenschaften): Beispiel 2

6. Konfigurieren Sie das VLAN über VMkernel.

9

Windows-Treibersoftware

Die Informationen zur Windows-Treibersoftware enthalten folgende Angaben:

- [Installieren der Treibersoftware](#)
- [„Ändern der Treibersoftware“ auf Seite 82](#)
- [„Reparieren oder Neuinstallieren der Treibersoftware“ auf Seite 83](#)
- [„Entfernen der Gerätetreiber“ auf Seite 83](#)
- [„Anzeigen oder Ändern der Adapter-Eigenschaften“ auf Seite 84](#)
- [„Einstellen der Optionen zur Energieverwaltung“ auf Seite 84](#)
- [„Konfigurieren des zu verwendenden Kommunikationsprotokolls über die QCC-Benutzeroberfläche, QCC PowerKit und QCS CLI“ auf Seite 86](#)

Installieren der Treibersoftware

ANMERKUNG

Diese Anweisungen basieren auf der Annahme, dass der QLogic BCM57xx und BCM57xxx-Adapter nicht werksseitig installiert wurde. Wenn der Controller werksseitig installiert wurde, ist auch die Treibersoftware installiert worden.

Wenn Windows das erste Mal nach der Installation eines Hardware-Geräts (wie beispielsweise eines QLogic BCM57xx und BCM57xxx-Adapters) bzw. nach dem Entfernen eines bereits vorhandenen Gerätetreibers gestartet wird, erkennt das Betriebssystem automatisch die Hardware und fordert Sie auf, die Treibersoftware für dieses Gerät zu installieren.

Die folgenden zwei Methoden sind für die Treiberinstallation verfügbar:

- [Grafischer interaktiver Installationsmodus \(siehe „Verwenden des Installationsprogramms“ auf Seite 77\)](#)
- [Befehlszeilenmodus für die Hintergrundinstallation \(siehe „Verwenden der Hintergrundinstallation“ auf Seite 80\)](#)

ANMERKUNG

- Prüfen Sie vor dem Installieren der Treibersoftware, dass Ihr Windows-Betriebssystem mit dem neuesten Service Pack auf die aktuelle Version aufgerüstet ist.
- Stellen Sie sicher, dass vor der Verwendung der QLogicBCM57xx und BCM57xxx-Controller ein Netzwerkgerätetreiber auf Ihrem Windows-Betriebssystem installiert wurde. Diese Treiber befinden sich auf der Installations-CD.
- Zur Verwendung von TCP/IP Offload Engine (TOE) ist Windows Server 2008, Windows Server 2008 R2 oder Windows Server 2012 oder Windows Server 2016 erforderlich. Außerdem muss ein Lizenzschlüssel auf dem Motherboard (für LOMs) installiert sein. Der Lizenzschlüssel für zusätzliche Netzwerkkarten ist in der Hardware vorprogrammiert.
- QCS wird bei Verwendung der Installationsoption „Server Core“ für Microsoft Windows Server 2008 R2 nicht unterstützt.

Verwenden des Installationsprogramms

Neben den QLogic-Gerätetreibern installiert das Installationsprogramm auch die Management-Anwendungen. Folgende Anwendungen werden installiert, wenn das Installationsprogramm ausgeführt wird:

- **QLogic Device Drivers** Installiert die QLogic-Gerätetreiber.
- **Control Suite** ist QLogic Control Suite (QCS CLI).
- **QCC** ist die Benutzeroberfläche der QConverge-Konsole.
- **QLASP** installiert das QLogic Advanced Server Program¹.
- **SNMP** installiert den SNMP-Subagent.
- **CIM Provider** installiert den Common Information Model Provider.
- **iSCSI Crash Dump Driver** installiert den Treiber für das iSCSI-Absturzspeicherabbild-Dienstprogramm.
- **FCoE Crash Dump Driver** installiert den Treiber für das FCoE-Absturzspeicherabbild-Dienstprogramm.
- **FastLinQ HBA Device Mgmt Agent** installiert den Agenten für die Geräteverwaltung.

¹ QLASP wird von Windows Server 2016 und höher nicht unterstützt. Diese Option ist für die Installation nicht verfügbar.

So installieren Sie die QLogic BCM57xx und BCM57xxx-Treiber und Managementanwendungen:

1. Wenn das Fenster **Found New Hardware Wizard** (Assistent für das Suchen neuer Hardware) angezeigt wird, klicken Sie auf **Cancel** (Abbrechen).
2. Auf dem Quelldatenträger mit dem Treiber oder an dem Speicherort, zu dem Sie das Paket mit den Software-Treibern heruntergeladen haben, können Sie Folgendes machen:
 - a. Öffnen Sie den Ordner für das Betriebssystem.
 - b. Öffnen Sie den `MUPS` -Ordner und extrahieren Sie dann den entsprechenden Ordner gemäß der Konfiguration Ihres Betriebssystems.
 - c. Doppelklicken Sie auf die Datei `Setup.exe`.Der InstallShield-Assistent für QLogic-Treiber und Managementanwendungen wird im Begrüßungsfenster geöffnet.
3. Wählen Sie nach Aufforderung des InstallShield-Assistenten ([Abbildung 9-1](#)) das gewünschte Dienstprogramm für die Adapterverwaltung:
 - Klicken Sie auf **Ja**, um QConvergeConsole GUI zu verwenden.
 - Klicken Sie auf **Nein**, um QLogic Control Suite zu verwenden.

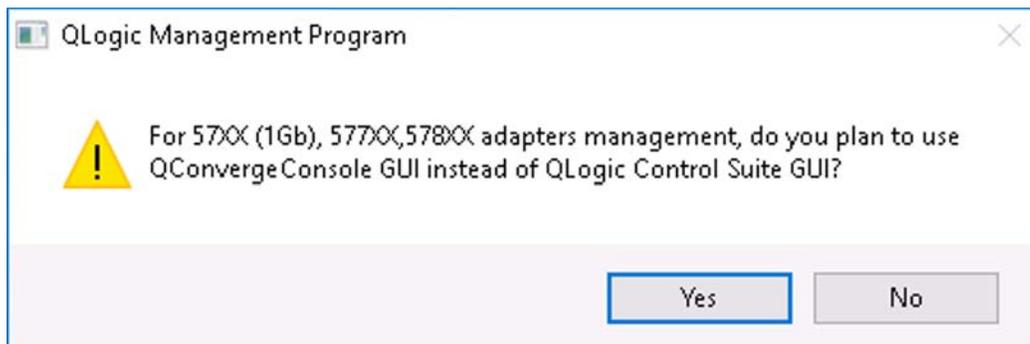


Abbildung 9-1. Eingabeaufforderung des InstallShield-Assistenten für das Verwaltungsdienstprogramm

4. Wählen Sie nach der Aufforderung „Möchten Sie die WMI-Installation überspringen?“ des InstallShield-Assistenten eine der folgenden Optionen:
 - Klicken Sie auf **Yes**, um die Installation der Windows Management Instrumentation (WMI)-Initiative zu verschieben.
 - Klicken Sie auf **No**, um WMI zu installieren.

5. Klicken Sie im InstallShield-Begrüßungsfenster auf **Next** (Weiter), um fortzufahren.
6. Nachdem Sie den Lizenzvertrag gelesen haben, klicken Sie auf **I accept the terms in the license agreement** (Ich stimme den Bedingungen der Lizenzvereinbarung zu) und dann auf **Next** (Weiter).
7. Wählen Sie die Funktionen aus, die Sie installieren möchten.
8. Klicken Sie auf **Install** (Installieren).
9. Klicken Sie zum Schließen des Assistenten auf **Finish** (Fertig stellen).
10. Das Installationsprogramm bestimmt, ob ein Neustart des Systems nötig ist. Befolgen Sie die Anweisungen auf dem Bildschirm.

So installieren Sie den Microsoft iSCSI Software Initiator für das iSCSI-Absturzspeicherabbild:

Wenn das QLogic-Dienstprogramm für das iSCSI-Absturzspeicherabbild unterstützt wird und Sie es verwenden möchten, muss die Installationsreihenfolge unbedingt eingehalten werden:

1. Führen Sie das Installationsprogramm aus.
2. Installieren Sie Microsoft iSCSI Software Initiator zusammen mit dem Patch (MS KB939875).

ANMERKUNG

Wenn Sie über das Installationsprogramm eine Aktualisierung der Gerätetreiber vornehmen, aktivieren Sie **iSCSI Crash Dump** (iSCSI-Absturzspeicherabbild) im Abschnitt **Advanced** (Erweitert) der Konfigurationsseite der QCC-Benutzeroberfläche erneut.

So installieren Sie die Gerätetreiber (nachdem Sie das Installationsprogramm ausgeführt haben):

1. Installieren Sie Microsoft iSCSI Software Initiator (Version 2.06 oder höher), wenn dieser nicht bereits in Ihrem Betriebssystem enthalten ist. Informationen dazu, wie Sie herausfinden können, in welchen Fällen Microsoft iSCSI Software Initiator installiert werden muss, finden Sie unter [Tabelle 9-1](#). Um den Microsoft iSCSI Software Initiator herunterzuladen, gehen Sie zu:
<http://www.microsoft.com/downloads/en/details.aspx?familyid=12cb3c1a-15d6-4585-b385-befd1319f825&displaylang=en>.
2. Installieren Sie, falls erforderlich, den Microsoft-Patch für die Erstellung der iSCSI-Absturzspeicherabbilddatei (Microsoft KB939875)
<http://support.microsoft.com/kb/939875>

Informationen dazu, wie Sie herausfinden können, ob Sie den Microsoft-Patch installieren müssen, finden Sie unter [Tabelle 9-1](#).

Tabelle 9-1. Windows-Betriebssysteme und iSCSI-Absturzspeicherabbild

Betriebssystem	Microsoft iSCSI Software Initiator erforderlich?	Microsoft-Patch (MS KB939875) erforderlich?
NDIS		
Windows Server 2008	Ja (im Betriebssystem enthalten)	Nein
Windows Server 2008 R2	Ja (im Betriebssystem enthalten)	Nein
Windows Server ab Version 2012	Ja (im Betriebssystem enthalten)	Nein
Offload-iSCSI (OIS)		
Windows Server 2008	Nein	Nein
Windows Server 2008 R2	Nein	Nein
Windows Server ab Version 2012	Nein	Nein

Verwenden der Hintergrundinstallation

ANMERKUNG

- Bei allen Befehlen muss die Groß-/Kleinschreibung beachtet werden.
- Ausführliche Anleitungen und Informationen zur unbeaufsichtigten Installation finden Sie in der Datei `silent.txt` im Ordner `Driver_Management_Apps_Installer`.

So führen Sie im Hintergrund eine Installation aus dem Quellordner des Installationsprogramms heraus durch:

Geben Sie den folgenden Befehl aus:

```
setup /s /v/qn
```

So führen Sie im Hintergrund ein Upgrade aus dem Quellordner des Installationsprogramms heraus durch:

Geben Sie den folgenden Befehl aus:

```
setup /s /v/qn
```

So führen Sie im Hintergrund eine Neuinstallation desselben Installationsprogramms durch:

Geben Sie den folgenden Befehl aus:

```
setup /s /v"/qn REINSTALL=ALL"
```

ANMERKUNG

Der Switch REINSTALL darf nur verwendet werden, wenn dasselbe Installationsprogramm bereits auf dem System installiert ist. Wenn Sie ein Upgrade auf eine frühere Version des Installationsprogramms durchführen, geben Sie, wie oben angegeben, `setup /s /v/qn` ein.

So führen Sie im Hintergrund eine Installation einzelner Elemente durch:

Verwenden Sie ADDSOURCE, um beliebige der nachfolgend aufgeführten Elemente in die Installation einzubeziehen.

Geben Sie entsprechend der Plattform den folgenden Befehl aus:

IA32-Plattformen:

```
setup /s /v"/qn ADDSOURCE=Driversi32,BACSi32,BASPi32,SNMPi32,CIMi32"
```

AMD/EM64T-Plattformen:

```
setup /s /v"/qn ADDSOURCE=Driversa64,BACSa64,BASPa64,SNMPa64,CIMa64"
```

Über folgende Befehlszeileingabe werden nur die QLogic-Treiber entsprechend der Plattform installiert:

IA32-Plattformen:

```
setup /s /v"/qn ADDSOURCE=Driversi32"
```

AMD64-Plattformen:

```
setup /s /v"/qn ADDSOURCE=Driversa64"
```

ANMERKUNG

Die QLogic-Gerätetreiber gehören zu den erforderlichen Elementen und werden immer installiert, auch wenn Sie nicht ADDSOURCE angeben.

So führen Sie eine Hintergrundinstallation von einer Batch-Datei aus durch:

Um eine Hintergrundinstallation von einer Batch-Datei aus durchzuführen und zu warten bis die Installation vollständig abgeschlossen ist, bevor Sie mit der nächsten Befehlszeile fortfahren, geben Sie folgenden Befehl aus:

```
start /wait setup /s /w /v/qn
```

Ändern der Treibersoftware

So ändern Sie die Treibersoftware:

1. Doppelklicken Sie in der Systemsteuerung auf **Add or Remove Programs** (Programme hinzufügen oder entfernen).
2. Klicken Sie auf **QLogic Drivers and Management Applications** (QLogic-Treiber und Managementanwendungen), und klicken Sie auf **Change** (Ändern).
3. Klicken Sie auf **Next** (Weiter), um fortzufahren.
4. Klicken Sie auf **Modify, Add, or Remove** (Ändern, Hinzufügen oder Entfernen), um Programmelemente zu ändern.

ANMERKUNG

Mit dieser Option werden keine Treiber für neue Adapter installiert. Informationen zum Installieren von Treibern für neue Adapter finden Sie unter „[Reparieren oder Neuinstallieren der Treibersoftware](#)“ auf [Seite 83](#).

5. Klicken Sie auf **Next** (Weiter), um fortzufahren.
6. Klicken Sie auf ein Symbol, um die Installationsweise für ein Element zu ändern.
7. Klicken Sie auf **Next** (Weiter).
8. Klicken Sie auf **Install** (Installieren).
9. Klicken Sie zum Schließen des Assistenten auf **Finish** (Fertig stellen).
10. Das Installationsprogramm bestimmt, ob ein Neustart des Systems nötig ist. Befolgen Sie die Anweisungen auf dem Bildschirm.

Reparieren oder Neuinstallieren der Treibersoftware

So reparieren oder installieren Sie die Treibersoftware neu:

1. Doppelklicken Sie in der Systemsteuerung auf **Add or Remove Programs** (Software).
2. Klicken Sie auf **QLogic Drivers and Management Applications** (QLogic-Treiber und Managementanwendungen), und klicken Sie auf **Change** (Ändern).
3. Klicken Sie auf **Next** (Weiter), um fortzufahren.
4. Klicken Sie auf **Repair or Reinstall** (Reparieren oder Neu installieren), um Fehler zu beheben oder Treiber für neue Adapter zu installieren.
5. Klicken Sie auf **Next** (Weiter), um fortzufahren.
6. Klicken Sie auf **Install** (Installieren).
7. Klicken Sie zum Schließen des Assistenten auf **Finish** (Fertig stellen).
8. Das Installationsprogramm bestimmt, ob ein Neustart des Systems nötig ist. Befolgen Sie die Anweisungen auf dem Bildschirm.

Entfernen der Gerätetreiber

Wenn Sie die Gerätetreiber entfernen, werden alle installierten Management-Anwendungen ebenfalls entfernt.

ANMERKUNG

Windows Server 2008 und Windows Server 2008 R2 verfügen über die Rollback-Funktion für Gerätetreiber, um einen Gerätetreiber durch einen bereits installierten Treiber zu ersetzen. Die komplexe Softwarearchitektur des BCM57xx und BCM57xxx-Geräts stellt jedoch möglicherweise ein Problem dar, wenn die Rollback-Funktion für eine der einzelnen Komponenten verwendet wird. Daher empfiehlt Ihnen QLogic, Änderungen an Treiberversionen nur über ein Treiberinstallationsprogramm vorzunehmen.

So entfernen Sie Gerätetreiber:

1. Doppelklicken Sie in der Systemsteuerung auf **Add or Remove Programs** (Programme hinzufügen oder entfernen).
2. Klicken Sie auf **QLogic Drivers and Management Applications** (QLogic-Treiber und Managementanwendungen), und klicken Sie auf **Remove** (Entfernen). Befolgen Sie die Anweisungen auf dem Bildschirm.

3. Starten Sie Ihr System neu, um die Treiber vollständig zu entfernen. Wenn Sie das System nicht neu starten, können Sie die Treiber nicht erfolgreich installieren.

Anzeigen oder Ändern der Adapter-Eigenschaften

So zeigen Sie die Eigenschaften eines QLogic-Netzwerkadapters an bzw. ändern sie:

1. Klicken Sie in der Systemsteuerung auf **QLogicControl Suite**.
2. Klicken Sie auf der Seite „Configurations“ (Konfigurationen) auf den Abschnitt **Advanced** (Erweitert).

Einstellen der Optionen zur Energieverwaltung

Sie können die Optionen zur Energieverwaltung so einstellen, dass das Betriebssystem den Controller abschalten kann, um Energie zu sparen, bzw. dass der Controller den Computer reaktivieren kann. Wenn das Gerät gerade einen Vorgang (z. B. Abwicklung einer Verbindung) ausführt, schaltet das Betriebssystem das Gerät jedoch nicht ab. Das Betriebssystem versucht nur dann, alle möglichen Geräte herunterzufahren, wenn der Computer in den Ruhezustand wechseln will.

So lassen Sie den Controller jederzeit eingeschaltet:

Deaktivieren Sie unter „Adapter Properties“ (Adaptoreigenschaften) auf der Seite „Power Management“ (Energieverwaltung) das Kontrollkästchen **Allow the computer to turn off the device to save power** (Computer kann Gerät ausschalten, um Energie zu sparen), wie in [Abbildung 9-2](#) gezeigt.

ANMERKUNG

Auf Blade-Servern stehen Optionen zur Energieverwaltung nicht zur Verfügung.

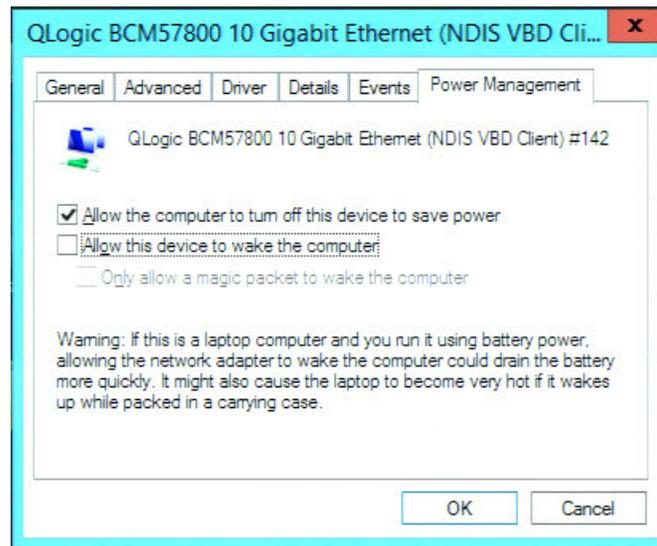


Abbildung 9-2. Optionen zur Energieverwaltung des Geräts

ANMERKUNG

- Die Seite „Power Management“ (Energieverwaltung) ist nur bei Servern verfügbar, die Energieverwaltung unterstützen.
- Aktivieren Sie das Kontrollkästchen **Allow the device to wake the computer** (Gerät kann den Computer aus dem Ruhezustand aktivieren), um die Funktion „Wake-on LAN“ (WOL) im Standby-Modus zu aktivieren.
- Wenn Sie das Kontrollkästchen **Only allow a magic packet to wake the computer** (Nur Magic Packet kann Computer aus dem Ruhezustand aktivieren) aktivieren, kann *nur* Magic Packet den Standby-Modus des Computers aufheben.

VORSICHT!

Aktivieren Sie für keinen Adapter, der Mitglied eines Teams ist, das Kontrollkästchen **Allow the computer to turn off this device to save power** (Computer kann Gerät ausschalten, um Energie zu sparen).

Konfigurieren des zu verwendenden Kommunikationsprotokolls über die QCC-Benutzeroberfläche, QCC PowerKit und QCS CLI

Es gibt zwei Hauptkomponenten der Verwaltungsanwendungen für die QCC-Benutzeroberfläche, QCC PowerKit und die QCS-Befehlszeilenschnittstelle: den RPC-Agenten und die Clientsoftware. Ein RPC-Agent wird auf einem Server oder Managed Host installiert, der ein oder mehrere konvergierte Netzwerkadapter (CNA) enthält. Der RPC-Agent sammelt Informationen über die CNAs und stellt sie für den Abruf von einem Management-PC bereit, auf dem die Clientsoftware installiert ist. Die Clientsoftware ermöglicht die Anzeige von Informationen des RPC-Agenten und der Konfiguration der konvertierten Netzwerkadapter (CNAs). Die Verwaltungssoftware enthält eine QCC-Benutzeroberfläche und eine QCS-Befehlszeilenschnittstelle.

Ein Kommunikationsprotokoll ermöglicht die Kommunikation zwischen dem RPC-Agenten und der Clientsoftware. Abhängig von der Mischung an Betriebssystemen (Linux, Windows oder beides) auf den Clients und Managed Hosts in Ihrem Netzwerk können Sie ein passendes Dienstprogramm auswählen, das verwendet werden soll.

Weitere Installationsanweisungen für diese Verwaltungsanwendungen finden Sie in den folgenden Dokumenten:

- *User's Guide, QLogic Control Suite CLI* (Teilenummer BC0054511-00)
- *User's Guide, PowerShell* (Teilenummer BC0054518-00)
- *Installation Guide, QConvergeConsole GUI* (Teilenummer SN0051105-00)

Hinweise zum Speicherort dieser Dokumente finden Sie unter „[Herunterladen von Dokumenten](#)“ auf Seite xxiii.

10 iSCSI-Protokoll

Dieses Kapitel enthält folgende Informationen zum iSCSI-Protokoll:

- [iSCSI Boot](#)
- [„iSCSI-Absturzspeicherabbild“ auf Seite 120](#)
- [„iSCSI-Offload unter Windows Server“ auf Seite 120](#)

iSCSI Boot

QLogic BCM57xx und BCM57xxx Gigabit Ethernet (GbE)-Adapter der Reihe 4xxxx unterstützen die iSCSI-Startfunktion zur Aktivierung des Netzwerkstarts von Betriebssystemen auf Systemen ohne Festplatte. Die iSCSI-Startfunktion ermöglicht den Remote-Betriebssystemstart in Windows-, Linux- oder VMware-Umgebungen über eine iSCSI-Zielmaschine über ein Standard-IP-Netzwerk.

Bei Windows- und Linux-Betriebssystemen kann iSCSI-Boot mit zwei verschiedenen Pfaden konfiguriert werden: Non-Offload (auch als Microsoft/Open-iSCSI-Initiator bekannt) und Offload (der Offload-iSCSI-Treiber von QLogic oder Host Bus Adapter). Die Konfiguration des Pfads wird im iSCSI-Konfigurationsprogramm auf der Seite Allgemeine Parameter über die Option **HBA Boot Mode** (HBA Boot-Modus) festgelegt. Weitere Informationen zu allen Konfigurationsoptionen auf der Seite „General Parameters“ (Allgemeine Parameter) finden Sie unter [Tabelle 10-1 auf Seite 92](#).

ANMERKUNG

Wenn Sie iSCSI-Boot auf BCM57xxx-basierten Designs verwenden, muss SR-IOV im System deaktiviert sein, bevor eine Aktualisierung von Version 7.2.x oder niedriger auf Version 7.4.x oder höher vorgenommen wird.

Unterstützte Betriebssysteme für iSCSI-Boot

iSCSI-Boot wird von den QLogicBCM57xx und BCM57xxx Gigabit Ethernet-Adaptoren für die folgenden Betriebssysteme unterstützt:

- Windows Server 2008 und höher, 32 Bit und 64 Bit (unterstützt Offload- und Non-Offload-Pfade)

- Linux RHEL 6 und höhere Versionen, und SLES 11.1 und höhere Versionen (unterstützt Offload- und Non-Offload-Pfade)
- SLES 10.x und SLES 11 (unterstützen nur den Non-Offload-Pfad)
- VMware ESXi 5.0 und höher für IPv4 (unterstützt nur den Non-Offload-Pfad), und ESXi 6.0 und höher für IPv6.
- VMware ESX in Schicht-2-Pfad

Darüber hinaus unterstützen die Adapter iSCSI-Boot für unbekannte Pfadtypen auf SLES 11 SP3 sowie SLES12.0 und höher, außerdem auf RHEL 6.5, 6.6, 7, 7.1 und höher, Windows 2012, Windows 2012 R2 und höher sowie ESXi 6.0 U2, 6.5 und höher.

Einrichten von iSCSI-Boot

Das Einrichten von iSCSI-Boot umfasst:

- [Konfigurieren des iSCSI-Ziels](#)
- [Konfigurieren der iSCSI-Bootparameter](#)
- [Vorbereiten des iSCSI-Boot-Image](#)
- [Booten](#)

Konfigurieren des iSCSI-Ziels

Das Konfigurieren des iSCSI-Ziels erfolgt bei den Zielen der verschiedensten Hersteller auf unterschiedliche Weise. Informationen über das Konfigurieren des iSCSI-Ziels finden Sie in der vom Hersteller mitgelieferten Dokumentation. Die allgemeinen Schritte sind:

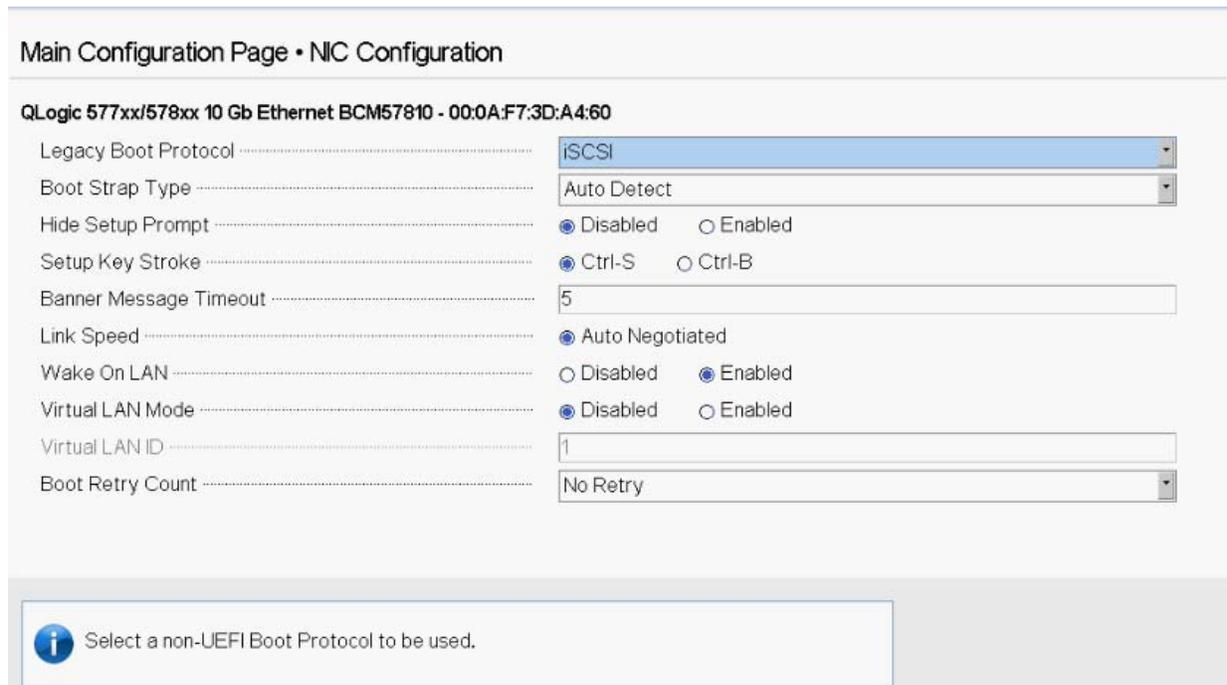
1. Einrichten eines iSCSI-Ziels.
2. Einrichten eines virtuellen Laufwerks
3. Zuweisen des virtuellen Laufwerks an das in [Schritt 1](#) eingerichtete virtuelle Laufwerk.
4. Verknüpfen eines iSCSI-Initiators mit dem iSCSI-Ziel
5. Notieren des Namens des iSCSI-Ziels, der TCP-Portnummer, der iSCSI-LUN, des Internet Qualified Name (IQN) des Ziels und der Einzelheiten zur CHAP-Authentifizierung.
6. Nach dem Konfigurieren des iSCSI-Ziels verfügen Sie über die folgenden Informationen:
 - IQN des Ziels
 - Ziel-IP-Adresse
 - TCP-Portnummer des Ziels
 - LUN des Ziels

- IQN des Initiators
- CHAP-ID und CHAP-Kennwort

Konfigurieren der iSCSI-Bootparameter

So konfigurieren Sie die iSCSI-Startparameter:

1. Klicken Sie auf der Seite „NIC Configuration“ (NIC-Konfiguration) im Drop-Down-Menü **Legacy Boot Protocol** (Legacy-Startprotokoll) auf **iSCSI** (siehe [Abbildung 10-1](#)).



Main Configuration Page • NIC Configuration

QLogic 577xx/578xx 10 Gb Ethernet BCM57810 - 00:0A:F7:3D:A4:60

Legacy Boot Protocol	iSCSI
Boot Strap Type	Auto Detect
Hide Setup Prompt	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Setup Key Stroke	<input checked="" type="radio"/> Ctrl-S <input type="radio"/> Ctrl-B
Banner Message Timeout	5
Link Speed	<input checked="" type="radio"/> Auto Negotiated
Wake On LAN	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Virtual LAN Mode	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
Virtual LAN ID	1
Boot Retry Count	No Retry

i Select a non-UEFI Boot Protocol to be used.

Abbildung 10-1. Legacy Boot Protocol (Legacy-Startprotokoll)

Gemäß [Abbildung 10-1](#) wird UEFI für das iSCSI-Protokoll für die BCM57xx und BCM57xxx-Adapter nicht unterstützt.

2. Konfigurieren Sie die QLogic iSCSI-Boot-Software für die statische oder die dynamische Konfiguration entweder über das CCM-Dienstprogramm, über das UEFI-Dienstprogramm (siehe [Abbildung 10-2](#)), über die QCC-Benutzeroberfläche oder die QCS-Befehlszeilenschnittstelle.

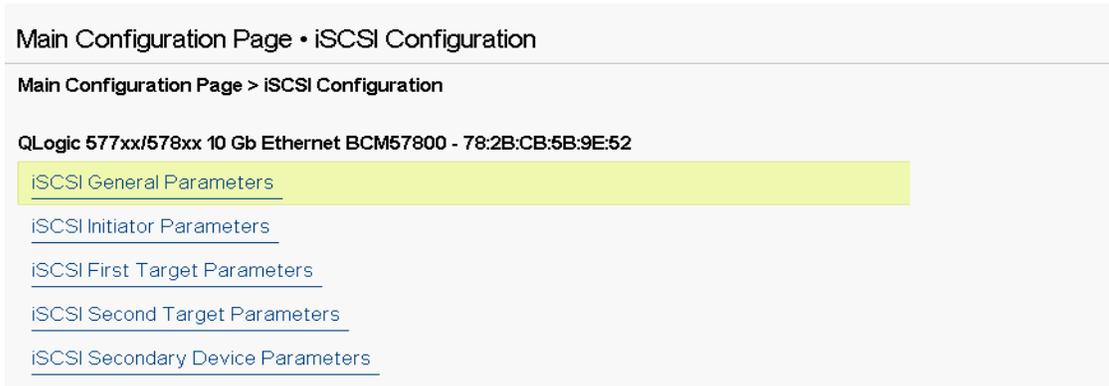


Abbildung 10-2. UEFI, iSCSI-Konfiguration

Die Konfigurationsoptionen im Fenster „General Parameters“ (Allgemeine Parameter, siehe [Abbildung 10-3](#)) werden in [Tabelle 10-1](#) aufgeführt.

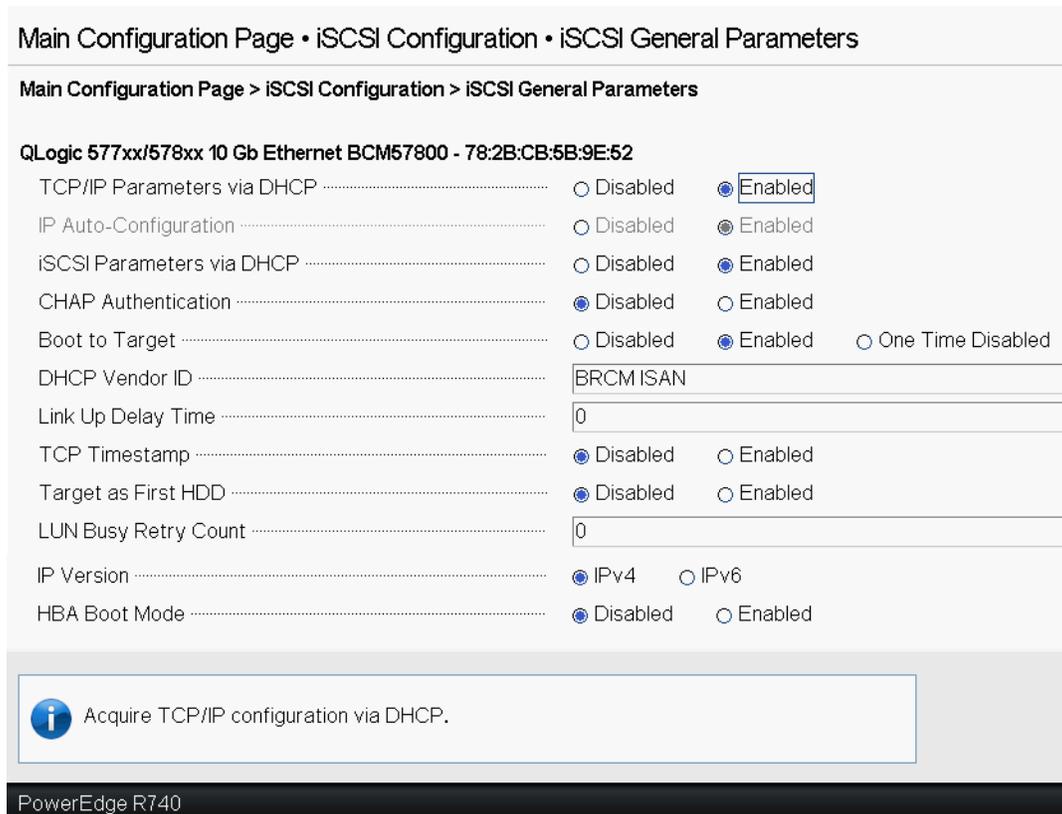


Abbildung 10-3. UEFI, iSCSI-Konfiguration, allgemeine iSCSI-Parameter

[Tabelle 10-1](#) enthält sowohl Parameter für IPv4 als auch für IPv6. Parameter, die nur für IPv4 bzw. IPv6 gelten, sind entsprechend gekennzeichnet.

ANMERKUNG

Die Verfügbarkeit von iSCSI-Boot für IPv6 ist plattform- und geräteabhängig.

Table 10-1. Konfigurationsoptionen

Option	Beschreibung
TCP/IP parameters through (DHCPTCP/IP-Parameter über DHCP)	Diese Option gilt nur für IPv4. legt fest, ob die iSCSI-Boothost-Software die IP-Adresse über DHCP erhält (aktiviert) oder eine statische IP-Konfiguration verwendet (deaktiviert)
IP Autoconfiguration (IP-Autokonfiguration)	Diese Option gilt nur für IPv6. Sie legt fest, ob die iSCSI-Boothost-Software eine zustandslose link-local-Adresse und/oder eine zustandbehaftete Adresse konfigurieren soll, wenn DHCPv6 vorhanden und in Verwendung ist („Aktiviert“). Router-Solicitation-Pakete werden bis zu dreimal in einem Abstand von 4 Sekunden zwischen den einzelnen Wiederholungen gesendet. Sie können aber auch eine statische IP-Konfiguration verwenden („Deaktivieren“).
iSCSI Parameters via DHCP (iSCSI-Parameter über DHCP)	legt fest, ob die iSCSI-Boothost-Software die Parameter des iSCSI-Ziels über DHCP (aktiviert) oder über eine statische Konfiguration (deaktiviert) erhält. Die statischen Informationen werden im Konfigurationsfenster „iSCSI Initiator Parameters Configuration“ (Konfigurieren der Parameter für iSCSI-Initiator) eingegeben.
CHAP Authentication (CHAP-Authentifizierung)	legt fest, ob die iSCSI-Boothost-Software eine CHAP-Authentifizierung für den Verbindungsaufbau zum iSCSI-Ziel verwendet. Wenn CHAP-Authentifizierung aktiviert ist, werden CHAP-ID und CHAP-Kennwort im Fenster „iSCSI Initiator Parameters Configuration“ (Konfigurieren der Parameter für iSCSI-Initiator) eingegeben.
Boot to Target (Start über Ziel)	<p>Beim ersten Verbindungsaufbau steuert diese Option, ob:</p> <ul style="list-style-type: none"> ■ Nicht von der designierten iSCSI-LUN gestartet wird (Disabled (Deaktiviert)) ■ Immer von der designierten iSCSI-LUN gestartet wird (Activated (Aktiviert)) ■ Nicht von der designierten iSCSI-LUN gestartet wird. <p>Nach einem Neustart muss diese Option auf „Enabled“ (Aktiviert) gesetzt werden und der Start muss immer diese Option erfolgen (One Time Disabled (Einmalige Deaktivierung)).</p> <p>Mit dieser Option kann das Startbetriebssystem auf der angeschlossenen LUN installiert werden. Dieser Schritt muss bei der ersten Einrichtung des Systems erfolgen. Anschließend kann dieses System eine Verbindung zu diesem installierten Betriebssystem-Image herstellen und von diesem Image starten, sobald diese Option auf „Enabled“ (Aktiviert) gesetzt ist.</p>

Tabelle 10-1. Konfigurationsoptionen (fortgesetzt)

Option	Beschreibung
DHCP Vendor ID	legt fest, wie die iSCSI-Boothost-Software bei DHCP das Feld „Vendor Class ID“ interpretiert. Wenn das Feld „Vendor Class ID“ im DHCP Offer Packet dem Wert in diesem Feld entspricht, sucht die iSCSI-Boothost-Software in den Feldern „DHCP Option 43“ nach den angeforderten iSCSI-Boot-Erweiterungen. Bei deaktiviertem DHCP muss kein Wert festgelegt werden.
Link Up Delay Time (Verzögerung nach Verbindungsaufbau)	legt die Wartezeit (in Sekunden) für die iSCSI-Boothost-Software zwischen dem Aufbau einer Ethernet-Verbindung und dem Senden von Daten über das Netzwerk fest. Die gültigen Werte liegen im Bereich zwischen 0 und 255. Ein Benutzer muss z. B. möglicherweise einen Wert für diese Option festlegen, wenn ein Netzwerkprotokoll, wie z. B. Spanning Tree, an der Switch-Schnittstelle zum Client-System aktiviert ist.
TCP Timestamp (TCP-Zeitstempel)	aktiviert bzw. deaktiviert die Option „TCP-Zeitstempel“
Target as First HDD (Ziel als erstes HDD)	legt fest, dass das iSCSI-Ziellaufwerk als erste Festplatte im System erscheint
LUN Busy Retry Count (Anzahl Wiederholungen bei „LUN besetzt“)	Legt die Anzahl der Wiederholungen des Verbindungsaufbaus durch den iSCSI-Boot-Initiator bei nicht erreichbarer iSCSI-Ziel-LUN fest.
IP Version (IP-Version)	Diese Option gilt nur für IPv6. Schaltet zwischen dem IPv4- und dem IPv6-Protokoll um. Wenn Sie von einer Protokollversion zur anderen wechseln, gehen alle IP-Einstellungen verloren.
HBA Boot Mode (HBA Boot-Modus)	Wird auf disable (deaktivieren) gesetzt, wenn das Host-Betriebssystem auf „software initiator mode“ (Softwareinitiatormodus) konfiguriert ist, und auf enable (aktivieren), wenn das Host-Betriebssystem auf den HBA- (oder iSCSI-Offload)-Modus konfiguriert ist. Diese Option steht für BCM57xx und BCM57xxx-Adapter zur Verfügung. (Hinweis: Dieser Parameter kann nicht geändert werden, wenn der Adapter sich im Multifunktionsmodus befindet.

Konfigurieren des MBA-Bootprotokolls

Weitere Informationen zum Konfigurieren des Boot-Protokolls finden Sie unter [Kapitel 6 Boot Agent-Treibersoftware](#):

iSCSI-Boot-Konfiguration

- [Konfigurieren einer statischen iSCSI-Boot-Konfiguration](#)
- [Konfigurieren einer dynamischen iSCSI-Boot-Konfiguration](#)

Konfigurieren einer statischen iSCSI-Boot-Konfiguration

Bei einer statischen Konfiguration müssen Sie die IP-Adresse des Systems, den Initiator-IQN des Systems und die unter „Konfigurieren des iSCSI-Ziels“ auf [Seite 88](#) erhaltenen Parameter des Ziels eingeben. Informationen über Konfigurationsoptionen finden Sie unter [Tabelle 10-1 auf Seite 92](#).

So konfigurieren Sie die iSCSI-Boot-Parameter in einer statischen Konfiguration:

1. Nehmen Sie auf der Menüseite „General Parameters“ (Allgemeine Parameter) die folgenden Einstellungen vor:
 - TCP/IP parameters via DHCP** (TCP/IP-Parameter via DHCP): Disabled (Deaktiviert, für IPv4)
 - IP Autoconfiguration** (IP-Autokonfiguration): Disabled (Deaktiviert, für IPv6, kein Offload)
 - iSCSI parameters via DHCP** (iSCSI-Parameter via DHCP): Disabled (Deaktiviert)
 - CHAP Authentication** (CHAP-Authentifizierung): Disabled (Deaktiviert)
 - Boot from Target** (Booten von Ziel): siehe [ANMERKUNG](#)
 - DHCP Vendor ID** (DHCP-Anbieter-ID): QLGC ISAN
 - Link Up Delay Time** (Verzögerung nach Verbindungsaufbau): 0
 - Use TCP Timestamp** (TCP-Zeitstempel verwenden): Enabled (Aktiviert) (bei einigen Zielen, wie dem Dell oder EMC AX100i, muss **Use TCP Timestamp** (TCP-Zeitstempel verwenden) aktiviert sein).
 - Target as First HDD** (Ziel als erstes HDD): Disabled (Deaktiviert)
 - LUN Busy Retry Count** (Anzahl an Wiederholungen bei „LUN besetzt“): 0
 - IP Version** (IP-Version): IPv6 (für IPv6, kein Offload)
 - HBA Boot Mode** (HBA-Boot-Modus): Disabled (Deaktiviert) (**ANMERKUNG:** Dieser Parameter kann nicht geändert werden, wenn der Adapter sich im Multifunktionsmodus befindet.)

ANMERKUNG

Für die Erstinstallation des Betriebssystems auf einer freien iSCSI Ziel-LUN von einer CD/DVD-ROM oder einem gemounteten, startfähigen Betriebssysteminstallationsabbild setzen Sie **Boot from Target** (Booten vom Zielsystem) auf **One Time Disabled** (Einmalige Deaktivierung). Diese Einstellung sorgt dafür, dass das System nach erfolgreichem Login und Verbindungsaufbau nicht vom konfigurierten iSCSI-Ziel bootet. Diese Einstellung wird nach dem nächsten Systemneustart automatisch auf **Enabled** (Aktiviert) gesetzt. **Enabled** (Aktiviert) bedeutet das Verbinden mit einem iSCSI-Ziel und den Versuch, von diesem zu booten. **Disabled** (Deaktiviert) bedeutet das Verbinden mit einem iSCSI-Ziel und kein Booten von diesem Gerät; stattdessen wird der Boot-Vektor an das nächste bootfähige Gerät der Startfolge abgegeben.

2. Drücken Sie die Taste ESC, um zum **Main** menu (Hauptmenü) zurückzukehren.
3. Wählen Sie im **Main** menu (Hauptmenü) die Option **iSCSI Initiator Parameters** (iSCSI-Initiatorparameter).

Daraufhin wird das Fenster „iSCSI Initiator Parameters“ (iSCSI-Initiatorparameter) angezeigt (siehe [Abbildung 10-4](#)).

Main Configuration Page • iSCSI Configuration • iSCSI Initiator Parameters

Main Configuration Page > iSCSI Configuration > iSCSI Initiator Parameters

QLogic 577xx/578xx 10 Gb Ethernet BCM57800 - 78:2B:CB:5B:9E:52

IP Address	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="0.0.0.0"/>
Subnet Mask Prefix	<input type="text" value="64"/>
Default Gateway	<input type="text" value="0.0.0.0"/>
Primary DNS	<input type="text" value="0.0.0.0"/>
Secondary DNS	<input type="text" value="0.0.0.0"/>
iSCSI Name	<input type="text" value="iqn.1995-05.com.broadcom.iscsiboot"/>
CHAP ID	<input type="text"/>
CHAP Secret	<input type="text"/>

Abbildung 10-4. iSCSI-Konfiguration, iSCSI-Initiatorparameter

4. Geben Sie im Fenster „iSCSI Initiator Parameters“ (iSCSI-Initiatorparameter) ([Abbildung 10-4](#)) Werte für Folgendes ein:
- IP Address (IP-Adresse) (nicht angegebene IPv4- und IPv6-Adressen sollten jeweils 0.0.0.0 und :: lauten)

ANMERKUNG

Geben Sie die IP-Adresse ein. Achten Sie dabei auf die korrekte Eingabe. Die IP-Adresse wird nicht auf Fehler im Hinblick auf Dopplungen oder falsche Zuweisungen zu einem Segment oder Netzwerk geprüft.

- Subnet Mask (Teilnetzmaske)
 - Submnet Mask Prefix (Präfix für Subnetzmaske)
 - Default Gateway (Standard-Gateway)
 - Primary DNS (Primärer DNS)
 - Secondary DNS (Sekundärer DNS)
 - iSCSI Name (iSCSI-Name) (entspricht dem vom Client-System zu verwendenden Namen des iSCSI-Initiators)
 - CHAP ID (CHAP-ID)
 - CHAP Secret (CHAP-Geheimschlüssel)
5. Drücken Sie die Taste ESC, um zum **Main** menu (Hauptmenü) zurückzukehren.
6. Wählen Sie im **Main** menu (Hauptmenü) **iSCSI First Target Parameters** (iSCSI-Parameter des ersten Ziels) aus.
- Daraufhin wird das Fenster „iSCSI First Target Parameters“ (iSCSI-Parameter des ersten Ziels) angezeigt (siehe [Abbildung 10-5](#)).

Main Configuration Page • iSCSI Configuration • iSCSI First Target Parameters

Main Configuration Page > iSCSI Configuration > iSCSI First Target Parameters

QLogic 577xx/578xx 10 Gb Ethernet BCM57800 - 78:2B:CB:5B:9E:52

Connect	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled
IP Address	0.0.0.0
TCP Port	3260
Boot LUN	0
iSCSI Name	
CHAP ID	
CHAP Secret	

Abbildung 10-5. iSCSI-Konfiguration, iSCSI-Parameter des ersten Ziels

7. Führen Sie im Fenster „iSCSI First Target Parameters“ (iSCSI-Parameter des ersten Ziels) die folgenden Aktivitäten aus ([Abbildung 10-5](#)):
 - a. Aktivieren Sie **Connect** (Verbinden), um eine Verbindung zum iSCSI-Ziel herzustellen.
 - b. Geben Sie die folgenden Werte ein, die auch beim Konfigurieren des iSCSI-Ziels verwendet wurden:
 - IP Address (IP-Adresse)
 - TCP Port (TCP-Port)
 - Boot LUN (Boot-LUN)
 - iSCSI Name (iSCSI-Name)
 - CHAP ID (CHAP-ID)
 - CHAP Secret (CHAP-Geheimschlüssel)
8. Drücken Sie ESC, um zum **Main** menu (Hauptmenü) zurückzukehren.
9. (Optional) Konfigurieren Sie ein zweites iSCSI-Ziel, indem Sie die Schritte im Fenster „iSCSI Second Target Parameter“ (iSCSI-Parameter für zweites Ziel) wiederholen.
10. Drücken Sie ESC und wählen Sie die Option **Exit and Save Configuration** (Beenden und Konfiguration speichern) aus.
11. Drücken Sie die Taste F4, um die MBA-Konfiguration zu speichern.

Konfigurieren einer dynamischen iSCSI-Boot-Konfiguration

Bei einer dynamischen Konfiguration müssen Sie lediglich vorgeben, dass die IP-Adresse des Systems und die Daten für Ziel/Initiator über DHCP bereitgestellt werden sollen (siehe Konfiguration von IPv4 und IPv6 unter [„Konfigurieren des DHCP-Servers auf Unterstützung von iSCSI-Boot“ auf Seite 100](#)). Bei IPv4 werden mit Ausnahme des Initiator-iSCSI-Namens sämtliche Einstellungen in den Fenstern für die Parameter des Initiators, die Parameter des ersten Ziels und die des zweiten Ziels ignoriert und müssen daher nicht gelöscht werden. Bei IPv6 werden mit Ausnahme von CHAP-ID und CHAP-Kennwort sämtliche Einstellungen in den Fenstern für die Parameter des Initiators, die Parameter des ersten Ziels und die des zweiten Ziels ignoriert und müssen daher nicht gelöscht werden. Informationen über Konfigurationsoptionen finden Sie unter [Tabelle 10-1 auf Seite 92](#).

ANMERKUNG

Bei Verwendung eines DHCP-Servers werden die Einträge des DNS-Servers durch die vom DHCP-Server bereitgestellten Werte überschrieben. Dieses Überschreiben tritt selbst dann auf, wenn die lokal bereitgestellten Werte gültig sind und der DHCP-Server keine Daten über den DNS-Server zur Verfügung stellt. Wenn der DHCP-Server keine Daten über den DNS-Server zur Verfügung stellt, werden die Werte sowohl für den primären als auch für den sekundären DNS-Server auf 0.0.0.0 eingestellt. Wenn das Betriebssystem Windows die Steuerung übernimmt, fragt der Microsoft iSCSI Initiator die Parameter des iSCSI Initiators ab und konfiguriert die entsprechenden Register statisch. Dabei werden die zuvor konfigurierten Werte immer überschrieben. Da der DHCP-Daemon in der Umgebung von Windows als Benutzerprozess ausgeführt wird, müssen alle TCP/IP-Parameter statisch festgelegt werden, bevor der Stack in der iSCSI-Boot-Umgebung aufgebaut wird.

Bei Verwendung von „DHCP Option 17“ werden die Daten über das Ziel vom DHCP-Server bereitgestellt, und als Initiator-iSCSI-Name wird der im Fenster „Initiator Parameters“ (Initiator-Parameter) eingegebene Name verwendet. Wenn kein Wert ausgewählt wird, nimmt der Controller standardmäßig folgenden Namen an:

```
iqn.1995-05.com.qlogic.<11.22.33.44.55.66>.iscsiboot
```

Wobei die Zeichenfolge 11.22.33.44.55.66 der MAC-Adresse des Controllers entspricht.

Bei Verwendung von „DHCP Option 43“ (nur IPv4) werden sämtliche Einstellungen in den Fenstern für die Parameter des Initiators, die Parameter des ersten Ziels und die des zweiten Ziels ignoriert und müssen daher nicht gelöscht werden.

So konfigurieren Sie die iSCSI-Boot-Parameter mithilfe einer dynamischen Konfiguration:

1. Nehmen Sie im Menüfenster „General Parameters“ (Allgemeine Parameter) die folgenden Einstellungen vor:
 - TCP/IP parameters via DHCP** (TCP/IP-Parameter via DHCP): Enabled (Aktiviert) (Für IPv4.)
 - IP Autoconfiguration** (IP-Autokonfiguration): Enabled (Aktiviert) (Für IPv6, Non-Offload.)
 - iSCSI parameters via DHCP** (iSCSI-Parameter via DHCP): Enabled (Aktiviert)
 - CHAP Authentication** (CHAP-Authentifizierung): Disabled (Deaktiviert)
 - Boot from Target** (Booten vom Ziel): siehe [ANMERKUNG](#)
 - DHCP Vendor ID** (DHCP-Anbieter-ID): QLGC ISAN
 - Link Up Delay Time** (Verzögerung nach Verbindungsaufbau): 0
 - Use TCP Timestamp** (TCP-Zeitstempel verwenden): Enabled (Aktiviert) (bei einigen Zielen, wie dem Dell oder EMC AX100i, muss **Use TCP Timestamp** (TCP-Zeitstempel verwenden) aktiviert sein).
 - Target as First HDD** (Ziel als erstes HDD): Disabled (Deaktiviert)
 - LUN Busy Retry Count** (Anzahl an Wiederholungen bei „LUN besetzt“): 0
 - IP Version** (IP-Version): IPv6. (Für IPv6, Kein Offload)
 - HBA Boot Mode** (HBA-Boot-Modus): Disabled. (**Hinweis:** Dieser Parameter kann nicht geändert werden, wenn der Adapter sich im Multifunktionsmodus befindet.
2. Drücken Sie die Taste ESC, um zum **Main** menu (Hauptmenü) zurückzukehren.

ANMERKUNG

Die Daten in den Fenstern „Initiator Parameters“ (Initiator-Parameter) und Parameter des ersten Ziels werden ignoriert; ein Löschen dieser Daten ist nicht erforderlich.

3. Wählen Sie **Exit and Save Configurations** (Beenden und Konfigurationen speichern) aus.

Aktivieren der CHAP-Authentifizierung

Stellen Sie sicher, dass die CHAP-Authentifizierung auf dem Ziel und dem Initiator aktiviert wurde.

So aktivieren Sie die CHAP-Authentifizierung:

1. Setzen Sie im Fenster „iSCSI General Parameters“ (Allgemeine iSCSI-Parameter) die Option **CHAP Authentication** (CHAP-Authentifizierung) auf **Enabled** (Aktiviert).
2. Geben Sie im Fenster „iSCSI Initiator Parameters“ (iSCSI-Initiatorparameter) Werte für Folgendes ein:
 - CHAP ID (CHAP-ID) (bis zu 128 Byte)
 - CHAP Secret (CHAP-Kennwort) (wenn eine Authentifizierung erforderlich ist, muss aus mindestens 12 Zeichen bestehen)
3. Drücken Sie die Taste ESC, um zum **Main** menu (Hauptmenü) zurückzukehren.
4. Geben Sie im Fenster „iSCSI First Target Parameters“ (iSCSI-Parameter des ersten Ziels) die folgenden Werte ein, die auch beim Konfigurieren des iSCSI-Ziels verwendet wurden:
 - CHAP ID (CHAP-ID) (optional, bei Zweiweg-CHAP)
 - CHAP Secret (CHAP-Kennwort) (optional, bei Zweiweg-CHAP, muss aus mindestens 12 Zeichen bestehen)
5. Drücken Sie ESC, um zum **Main** menu (Hauptmenü) zurückzukehren.
6. (optional) Fügen Sie „CHAP“ zum Menü „iSCSI Second Target Parameters“ (iSCSI-Parameter für das zweite Ziel) hinzu.
7. Drücken Sie ESC und wählen Sie die Option **Exit and Save Configuration** (Beenden und Konfiguration speichern) aus.

Konfigurieren des DHCP-Servers auf Unterstützung von iSCSI-Boot

Bei dem DHCP-Server handelt es sich um eine optionale Komponente, die nur benötigt wird, wenn Sie eine Konfiguration für dynamisches iSCSI-Boot einrichten (siehe „[Konfigurieren einer dynamischen iSCSI-Boot-Konfiguration](#)“ auf Seite 98).

Die Konfiguration des DHCP-Servers zur Unterstützung von iSCSI-Boot ist für IPv4 und IPv6 unterschiedlich.

- [DHCP-Konfiguration für iSCSI-Boot bei IPv4](#)
- [DHCP-Konfiguration für iSCSI-Boot bei IPv6](#)

DHCP-Konfiguration für iSCSI-Boot bei IPv4

Das DHCP-Protokoll beinhaltet eine Anzahl von Optionen, die Konfigurationsinformationen an den DHCP-Client übermitteln. Die QLogic-Adapter unterstützen die folgenden DHCP-Konfigurationen für iSCSI-Boot:

- [DHCP Option 17, Root Path](#)
- [DHCP Option 43, Herstellerspezifische Informationen](#)

DHCP Option 17, Root Path

Mit Hilfe von Option 17 werden Informationen über das iSCSI-Ziel an den iSCSI-Client übermittelt.

Das Format für das Wurzelverzeichnis ist in IETF RFC 4173 definiert und lautet:

```
"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
```

[Tabelle 10-2](#) enthält eine Auflistung der Parameter und Definitionen.

Tabelle 10-2. Definition der Parameter von „DHCP Option 17“

Parameter	Definition
"iscsi:"	eine festgelegte Zeichenfolge
<servername>	die IP-Adresse oder FQDN des iSCSI-Ziels
":"	Trennzeichen
<protocol>	IP-Protokoll für den Zugriff auf das iSCSI-Ziel. Zurzeit wird ausschließlich TCP unterstützt, das Protokoll lautet daher „6“.
<port>	Dem Protokoll zugeordnete Portnummer. Die Standardportnummer für iSCSI lautet 3260.
<LUN>	Die für das iSCSI-Ziel zu verwendende LUN. Der Wert der LUN muss im hexadezimalen Format angegeben sein. Konfigurieren einer LUN mit einer ID OF 64 im Parameter zu „Option 17“ des DHCP-Servers als 40.
<targetname>	Name des Ziels, entweder im IQN-Format oder im EUI-Format (Details zu den Formaten IQN und EUI finden Sie in RFC 3720). Ein Beispiel für einen IQN-Namen ist <code>iqn.1995-05.com.QLogic:iscsi-target</code> .

DHCP Option 43, Herstellerspezifische Informationen

DHCP Option 43 (herstellerspezifische Informationen) stellt dem iSCSI-Client mehr Konfigurationsoptionen zur Verfügung als DHCP Option 17. In dieser Konfiguration werden drei zusätzliche Unteroptionen angeboten, die den Initiator-IQN dem iSCSI-Boot-Client zuweisen und zusätzlich zwei iSCSI-Ziel-IQN bereitstellen, die zum Booten verwendet werden können. Das Format des iSCSI-Ziel-IQN ist mit dem Format von DHCP Option 17 identisch, beim iSCSI-Initiator-IQN handelt es sich einfach um den IQN des Initiators.

ANMERKUNG

DHCP Option 43 wird nur bei IPv4 unterstützt.

Tabelle 10-3 enthält eine Auflistung der Unteroptionen.

Tabelle 10-3. Definition der Unteroptionen von DHCP Option 43

Unteroption	Definition
201	Informationen über das erste iSCSI-Ziel im Standardformat für das Wurzelverzeichnis "iscsi:"<servername>":"<protocol>":"<port>":"<LUN>": "<targetname>"

Bei Verwendung der DHCP Option 43 sind umfangreichere Konfigurationsschritte vorzunehmen als bei DHCP Option 17, die Umgebung ist jedoch reichhaltiger und es stehen mehr Konfigurationsoptionen zur Verfügung. QLogic empfiehlt beim Ausführen einer dynamischen iSCSI-Boot-Konfiguration die Verwendung von DHCP Option 43.

Konfigurieren des DHCP-Servers

Konfigurieren Sie den DHCP-Server so, dass er Option 17 oder Option 43 unterstützt.

ANMERKUNG

Bei Verwendung von Option 43 muss zusätzlich Option 60 konfiguriert werden. Der Wert von Option 60 muss dem Wert von **DHCP Vendor ID** entsprechen. Der Wert von **DHCP Vendor ID** lautet „QLGC ISAN“, wie im Abschnitt **General Parameters** (Allgemeine Parameter) des Menüs **iSCSI Boot Configuration** (iSCSI-Boot-Konfiguration) angezeigt.

DHCP-Konfiguration für iSCSI-Boot bei IPv6

Der DHCPv6-Server stellt eine Anzahl von Optionen zur Verfügung, darunter eine zustandslose oder zustandbehaftete IP-Konfiguration sowie Informationen für den DHCPv6-Client. Die QLogic-Adapter unterstützen die folgenden DHCP-Konfigurationen für iSCSI-Boot:

- [DHCPv6 Option 16, Vendor Class-Option](#)
- [DHCPv6 Option 17, Herstellerspezifische Informationen](#)

ANMERKUNG

Die DHCPv6-Standardoption „Root Path“ ist noch nicht verfügbar. QLogic empfiehlt für die Unterstützung von dynamischem iSCSI-Boot bei IPv6 die Verwendung von Option 16 oder Option 17.

DHCPv6 Option 16, Vendor Class-Option

DHCPv6 Option 16 (Vendor Class-Option) muss vorhanden sein und eine Zeichenfolge enthalten, die mit dem Parameter **DHCP Vendor ID** übereinstimmt. Der Wert von **DHCP Vendor ID** lautet **QLGC ISAN**, wie im Bildschirm **General Parameters** (Allgemeine Parameter) des Menüs **iSCSI Boot Configuration** (-Boot-Konfiguration) angezeigt.

Der Inhalt von Option 16 sollte `<2-byte length> <DHCP Vendor ID>` sein.

DHCPv6 Option 17, Herstellerspezifische Informationen

DHCPv6 Option 17 (herstellerspezifische Informationen) stellt dem iSCSI-Client weitere Konfigurationsoptionen zur Verfügung. In dieser Konfiguration werden drei zusätzliche Unteroptionen angeboten, die den Initiator-IQN dem iSCSI-Boot-Client zuweisen und zusätzlich zwei iSCSI-Ziel-IQN bereitstellen, die zum Booten verwendet werden können.

[Tabelle 10-4](#) enthält eine Auflistung der Unteroptionen.

Tabelle 10-4. Definition der Unteroptionen von DHCP Option 17

Unteroption	Definition
201	Informationen über das erste iSCSI-Ziel im Standardformat für das Wurzelverzeichnis "iscsi:"[<servername>]":"<protocol>":"<port>": "<LUN>":"<targetname>"

ANMERKUNG

Die Klammern [] in [Tabelle 10-4](#) sind für IPv6-Adressen erforderlich.

Der Inhalt von Option 17 sollte `<2-byte Option Number 201|202|203>`
`<2-byte length> <data>` sein.

Konfigurieren des DHCP-Servers

Konfigurieren Sie den DHCP-Server so, dass er Option 16 und Option 17 unterstützt.

ANMERKUNG

Die Formate der DHCPv6-Option 16 und der Option 17 sind in RFC 3315 vollständig definiert.

Vorbereiten des iSCSI-Boot-Image

- [Einrichten von iSCSI-Boot für Windows Server 2008 R2 und SP2](#)
- [Einrichten des iSCSI-Startvorgangs für Windows Server 2012, 2012 R2 und 2016](#)
- [Einrichten von iSCSI-Boot für Linux](#)
- [Workaround für die dezentrale DVD-Installation bei SUSE 11.1](#)
- [Entfernen von integrierten Treibern vom Windows-Image](#)
- [Einfügen \(Slipstreaming\) der QLogic-Treiber in die Windows-Imagedateien](#)

Einrichten von iSCSI-Boot für Windows Server 2008 R2 und SP2

Windows Server 2008 R2 und Windows Server 2008 SP2 unterstützen das Booten und Installieren in den Offload- und den Non-Offload-Pfaden.

Mit dem folgenden Verfahren wird das Image auf das Booten im Offload- oder Non-Offload-Pfad vorbereitet. Das Verfahren bezieht sich auf Windows Server 2008 R2, ist aber auch für Windows Server 2008 SP2 gängig.

Erforderliches CD oder ISO-Image:

- Windows Server 2008 R2 x64 mit eingefügten QLogic-Treibern (siehe [„Einfügen \(Slipstreaming\) der QLogic-Treiber in die Windows-Imagedateien“ auf Seite 113](#)). Weitere Informationen finden Sie auch im Microsoft Knowledge Base-Artikel KB974072 unter support.microsoft.com.

ANMERKUNG

- Das Verfahren von Microsoft fügt nur die 10GbE Virtual Bus Driver (EVBD) und NDIS-Treiber hinzu. QLogic empfiehlt, dass alle Treiber (EVBD, VBD, BXND, OIS, FCoE und NDIS) hinzugefügt werden.
- Weitere Informationen zur Extrahierung der einzelnen Windows BCM57xx und BCM57xxx-Treiber finden Sie in der Datei `silent.txt` für das spezifische Treiberinstallationsprogramm.

Sonstige erforderliche Software:

- `Bindview.exe` (nur Windows Server 2008 R2; siehe KB976042)

Einrichten von iSCSI-Boot für Windows Server 2008 R2 und SP2:

1. Entfernen Sie alle lokalen Festplatten auf dem zu bootenden System (dem „Remote-System“).
2. Laden Sie die aktuellsten QLogic MBA- und iSCSI-Boot-Images auf den NVRAM des Adapters.
3. Konfigurieren Sie BIOS auf dem Remote-System so, dass das QLogic MBA das erste bootfähige Gerät und das CD-ROM-Laufwerk das zweite bootfähige Gerät ist.
4. Konfigurieren Sie das iSCSI-Ziel, um eine Verbindung vom Remote-Gerät zuzulassen. Vergewissern Sie sich, dass das Ziel über ausreichend Speicherplatz für die neue Betriebssysteminstallation verfügt.
5. Booten Sie das Remote-System. Wenn das Preboot Execution Environment (PXE)-Banner angezeigt wird, drücken Sie die Tasten STRG + S, um das PXE-Menü aufzurufen.
6. Legen Sie im PXE-Menü für **Boot Protocok** (Bootprotokoll) **iSCSI** fest.
7. Geben Sie die Parameter für das iSCSI-Ziel ein.
8. Setzen Sie **HBA Boot Mode** (HBA-Boot-Modus) auf **Enabled** (Aktiviert) oder **Disabled** (Deaktiviert). (**Hinweis:** Dieser Parameter kann nicht geändert werden, wenn der Adapter sich im Multifunktionsmodus befindet).
9. Speichern Sie die Einstellungen, und starten Sie das System neu.
Das Remote-System sollte eine Verbindung zum iSCSI-Ziel herstellen und dann vom DVDROM-Gerät booten.
10. Booten Sie von der DVD, und starten Sie die Installation.
11. Beantworten Sie alle Installationsfragen entsprechend (geben Sie das zu installierende Betriebssystem an, akzeptieren Sie die Lizenzbedingungen usw.).

Wenn das Fenster **Where do you want to install Windows?** (Wo soll Windows installiert werden) angezeigt wird, sollte das Ziellaufwerk angezeigt werden. Dies ist ein Laufwerk, das über das iSCSI-Boot-Protokoll angeschlossen ist und sich im externen iSCSI-Ziel befindet.

12. Wählen Sie **Next** (Weiter) aus, um mit der Windows Server 2008 R2-Installation fortzufahren.

Nach einigen Minuten wird der Installationsvorgang von der Windows Server 2008 R2-DVD gestartet, und anschließend wird das System neu gestartet. Nach dem Neustart sollte die Windows Server 2008 R2-Installation fortgesetzt und die Installation abgeschlossen werden.

13. Überprüfen Sie nach einem erneuten Systemneustart, ob das Remote-System vom Desktop gebootet werden kann.
14. Laden Sie nach dem Booten von Windows Server 2008 R2 alle Treiber, und führen Sie die Datei `Bindview.exe` aus.
 - a. Wählen Sie **All Services** (Alle Dienste) aus.
 - b. Unter **WFP Lightweight-Filter** sollten für die AUT **Binding paths** (Bindungspfade) angezeigt werden. Klicken Sie mit der rechten Maustaste darauf, und deaktivieren Sie sie. Schließen Sie dann die Anwendung.
15. Stellen Sie sicher, dass das Betriebssystem und das System funktionsfähig sind und Daten übertragen können, indem Sie die IP eines externen Systems anpingen usw.

Einrichten des iSCSI-Startvorgangs für Windows Server 2012, 2012 R2 und 2016

Windows Server 2012/2012 R2 und 2016 unterstützen das Starten und Installieren in den Offload- und den Non-Offload-Pfaden. QLogic erfordert die Verwendung einer „Slipstream“-DVD mit den neuesten QLogic-Treibern (siehe [„Einfügen \(Slipstreaming\) der QLogic-Treiber in die Windows-Imagedateien“ auf Seite 113](#)). Weitere Informationen finden Sie auch im Microsoft Knowledge Base-Artikel KB974072 unter support.microsoft.com.

ANMERKUNG

Das Verfahren von Microsoft fügt nur die EVBD- und NDIS-Treiber hinzu. QLogic empfiehlt, dass alle Treiber (EVBD, VBD, BXND, OIS, FCoE und NDIS) hinzugefügt werden.

Vorbereitung des Image auf das Booten im Offload- oder Non-Offload-Pfad:

1. Entfernen Sie alle lokalen Festplatten auf dem zu bootenden System (dem „Remote-System“).
2. Laden Sie die aktuellsten QLogic MBA- und iSCSI-Boot-Images auf den NVRAM des Adapters.
3. Konfigurieren Sie BIOS auf dem Remote-System so, dass das QLogic MBA das erste bootfähige Gerät und das CD-ROM-Laufwerk das zweite bootfähige Gerät ist.
4. Konfigurieren Sie das iSCSI-Ziel, um eine Verbindung vom Remote-Gerät zuzulassen. Vergewissern Sie sich, dass das Ziel über ausreichend Speicherplatz für die neue Betriebssysteminstallation verfügt.
5. Booten Sie das Remote-System. Wenn das Preboot Execution Environment (PXE)-Banner angezeigt wird, drücken Sie die Tasten STRG + S, um das PXE-Menü aufzurufen.
6. Legen Sie im PXE-Menü für **Boot Protocok** (Bootprotokoll) **iSCSI** fest.
7. Geben Sie die Parameter für das iSCSI-Ziel ein.
8. Setzen Sie **HBA Boot Mode** (HBA-Boot-Modus) auf **Enabled** (Aktiviert) oder **Disabled** (Deaktiviert). (**Hinweis:** Dieser Parameter kann nicht geändert werden, wenn der Adapter sich im Multifunktionsmodus befindet.)
9. Speichern Sie die Einstellungen, und starten Sie das System neu.
Das Remote-System sollte eine Verbindung zum iSCSI-Ziel herstellen und dann vom DVDROM-Gerät booten.
10. Booten Sie von der DVD, und starten Sie die Installation.
11. Beantworten Sie alle Installationsfragen entsprechend (geben Sie das zu installierende Betriebssystem an, akzeptieren Sie die Lizenzbedingungen usw.).
Wenn das Fenster **Where do you want to install Windows?** (Wo soll Windows installiert werden) angezeigt wird, sollte das Ziellaufwerk angezeigt werden. Das Ziellaufwerk, das über das iSCSI-Boot-Protokoll angeschlossen ist und sich im externen iSCSI-Ziel befindet.
12. Wählen Sie **Next** (Weiter) aus, um mit der Installation von Windows Server 2012 oder 2016 fortzufahren.
Nach einigen Minuten wird der Installationsvorgang von der Windows Server 2012- oder 2016-DVD gestartet, und anschließend wird das System neu gestartet. Nach dem Neustart sollte die Windows Server 2012- oder 2016-Installation fortgesetzt und die Installation abgeschlossen werden.
13. Überprüfen Sie nach einem erneuten Systemneustart, ob das Remote-System vom Desktop gebootet werden kann.

14. Nachdem Windows Server 2012 das Betriebssystem gebootet hat, empfiehlt QLogic, das Treiberinstallationsprogramm auszuführen, um die Installation von QLogic-Treibern und -Anwendungen abzuschließen.

Einrichten von iSCSI-Boot für Linux

iSCSI-Boot für Linux wird von Red Hat Enterprise Linux 5.5 und höher sowie von SUSE Linux Enterprise Server 11 (SLES 11) SP1 und höher sowohl in den Offload- als auch in den Non-Offload-Pfaden unterstützt. Beachten Sie, dass SLES 10.x und SLES 11 nur den Non-Offload-Pfad unterstützen.

Einrichten von iSCSI-Boot für Linux:

1. Um den Treiber zu aktualisieren, besorgen Sie die aktuelle QLogic Linux-Treiber-CD.
2. Konfigurieren Sie die iSCSI-Boot-Parameter für die direkte Installation in das Zielsystem von DVD, indem Sie die Option zum Booten vom Zielsystem auf dem Netzwerkadapter deaktivieren.
3. Konfigurieren Sie die Installation über den Non-Offload-Pfad, indem Sie **HBA Boot Mode** (HBA-Boot-Modus) in der NVRAM-Konfiguration auf **Disabled** (Deaktiviert) setzen. (**Hinweis:** (Dieser Parameter kann nicht geändert werden, wenn der Adapter sich im Multifunktionsmodus befindet.) Beachten Sie, dass für RHEL 6.2 die Installation über den Offload-Pfad unterstützt wird. Legen Sie in diesem Fall den **HBA Boot Mode** (HBA-Bootmodus) in der NVRAM-Konfiguration auf **Enabled** (Aktiviert) fest.
4. Ändern Sie die Boot-Reihenfolge wie folgt:
 - a. Booten vom Netzwerkadapter.
 - b. Booten von CD oder DVD-Treiber.
5. Starten Sie Ihr System neu.

Das System stellt eine Verbindung zum iSCSI-Ziel her und bootet anschließend vom CD- oder DVD-Laufwerk.
6. Für SUSE 11.x wählen Sie **installation** (Installation) und geben als Boot-Option **iscsi=1 netsetup=1** ein. Wenn ein Treiber-Update erforderlich ist, wählen Sie für die F6-Treiberoption **YES** (JA) aus.
7. Wählen Sie bei der Aufforderung `networking device` (Netzwerkgerät) den erforderlichen Netzwerkadapterport aus, und drücken Sie **OK**.
8. Konfigurieren Sie bei Anzeige von `configure TCP/IP` (TCP/IP konfigurieren) die Art der IP-Adresszuweisung des Systems, und klicken Sie anschließend auf **OK**.
9. Wenn Sie eine statische IP auswählen, müssen Sie IP-Informationen für den iscsi-Initiator eingeben.
10. (RHEL) Überspringen Sie den Medientest.

11. Setzen Sie die Installation nach Bedarf fort. Zu diesem Zeitpunkt steht ein Laufwerk zur Verfügung. Entnehmen Sie nach Abschluss des Kopiervorgangs die CD oder DVD, und starten Sie das System neu.
12. Aktivieren Sie beim Systemneustart die Option zum Booten vom Zielsystem in den iSCSI-Boot-Parametern, und schließen Sie die Installation ab.

Zu diesem Zeitpunkt ist die Erstinstallationsphase abgeschlossen.

Erstellung eines neuen benutzerdefinierten initrd-Image für jedes neue Komponenten-Update:

1. Aktualisieren Sie wenn erforderlich den iSCSI-Initiator. Sie müssen zunächst den vorhandenen Initiator mit `rpm -e` entfernen.
2. Stellen Sie sicher, dass alle Ausführungsebenen des Netzwerkdiensts aktiviert sind:

```
chkconfig network on
```
3. Stellen Sie sicher, dass die Ausführungsebenen 2, 3 und 5 des iSCSI-Diensts aktiviert sind:

```
chkconfig -level 235 iscsi on
```
4. Stellen Sie bei Red Hat 6.0 sicher, dass der Network Manager-Dienst beendet und deaktiviert ist.
5. (Optional) Installieren Sie `iscsiuio` (für SUSE 10 nicht erforderlich).
6. (Optional) Installieren Sie das `linux-nx2`-Paket.
7. Installieren Sie das `bibt`-Paket.
8. Entfernen Sie `ifcfg-eth*`.
9. Führen Sie einen Neustart durch.
10. Befolgen Sie bei SUSE 11.1 im nächsten Abschnitt gezeigten Workaround für die dezentrale DVD-Installation.
11. Melden Sie sich nach dem Systemneustart an, ändern Sie den Ordner in `/opt/bcm/bibt`, und führen Sie das Skript `iscsi_setup.sh` zum Erstellen von Offload- und Non-Offload-initrd-Images aus.
12. Kopieren Sie das/die initrd-Image(s), Offload und Non-Offload in das `/boot`-Verzeichnis.
13. Ändern Sie das `grub`-Menü so, dass auf das neue initrd-Image gezeigt wird.
14. Zum Aktivieren von CHAP ist eine Änderung von `iscsid.conf` erforderlich (nur Red Hat).
15. Führen Sie einen Neustart durch.
16. (Optional) Ändern der CHAP-Parameter.

17. Setzen Sie das Booten in das iSCSI-Boot-Image fort, und wählen Sie eines der erstellten Images aus (Non-Offload oder Offload). Sie müssen dabei Ihre Auswahl im Abschnitt zu den **iSCSI Boot parameters** (iSCSI-Boot-Parametern) berücksichtigen. Wenn **HBA Boot Mode** (HBA Boot-Modus) im Abschnitt **iSCSI Boot Parameters** (iSCSI-Boot-Parameter) aktiviert wurde, müssen Sie das Offload-Image booten.

ANMERKUNG

QLogic unterstützt Starten des Host Bus Adapter (Offload) in SLES 11 SP1 und höher.

QLogic unterstützt iSCSI-Boot *nicht* in Host Bus Adapter (Offload)-Modus für SLES 10.x und SLES 11.

18. Für IPv6 können Sie nun in der NVRAM-Konfiguration die gewünschte IPv6-Adresse sowohl für den Initiator als auch für das Ziel festlegen.

Workaround für die dezentrale DVD-Installation bei SUSE 11.1

1. Erstellen Sie eine neue Datei mit dem Namen `boot.open-iscsi` und dem in [Schritt 2](#) dargestellten Inhalt.
2. Kopieren Sie die erstellte Datei in den Ordner `/etc/init.d/`, und überschreiben Sie die vorhandene Datei.

Inhalt der neuen `boot.open-iscsi`-Datei:

```
#!/bin/bash
#
# /etc/init.d/iscsi
#
### BEGIN INIT INFO
# Provides:          iscsiboot
# Required-Start:
# Should-Start:      boot.multipath
# Required-Stop:
# Should-Stop:       $null
# Default-Start:     B
# Default-Stop:
# Short-Description: iSCSI initiator daemon root-fs support
# Description:       Starts the iSCSI initiator daemon if the
#                    root-filesystem is on an iSCSI device
#
### END INIT INFO

ISCSIADM=/sbin/iscsiadm
```

```
ISCSIUIO=/sbin/iscsiuio
CONFIG_FILE=/etc/iscsid.conf
DAEMON=/sbin/iscsid
ARGS="-c $CONFIG_FILE"

# Source LSB init functions
. /etc/rc.status

#
# This service is run right after booting. So all targets activated
# during mkinitrd run should not be removed when the open-iscsi
# service is stopped.
#
iscsi_load_iscsiuio()
{
    TRANSPORT=`$ISCSIADM -m session 2> /dev/null | grep "bnx2i"`
    if [ "$TRANSPORT" ] ; then
        echo -n "Launch iscsiuio "
        startproc $ISCSIUIO
    fi
}

iscsi_mark_root_nodes()
{
    $ISCSIADM -m session 2> /dev/null | while read t num i target ;
do
    ip=${i%:*}
    STARTUP=`$ISCSIADM -m node -p $ip -T $target 2> /dev/null |
grep "node.conn\[0\].startup" | cut -d' ' -f3`
    if [ "$STARTUP" -a "$STARTUP" != "onboot" ] ; then
        $ISCSIADM -m node -p $ip -T $target -o update -n
node.conn[0].startup -v onboot
    fi
done
}

# Reset status of this service
rc_reset

# We only need to start this for root on iSCSI
if ! grep -q iscsi_tcp /proc/modules ; then
    if ! grep -q bnx2i /proc/modules ; then
```

```
        rc_failed 6
        rc_exit
    fi
fi
case "$1" in
    start)
        echo -n "Starting iSCSI initiator for the root device: "
        iscsi_load_iscsiuio
        startproc $DAEMON $ARGS
        rc_status -v
        iscsi_mark_root_nodes
        ;;
    stop|restart|reload)
        rc_failed 0
        ;;
    status)
        echo -n "Checking for iSCSI initiator service: "
        if checkproc $DAEMON ; then
            rc_status -v
        else
            rc_failed 3
            rc_status -v
        fi
        ;;
    *)
        echo "Usage: $0 {start|stop|status|restart|reload}"
        exit 1
        ;;
esac
rc_exit
```

Entfernen von integrierten Treibern vom Windows-Image

1. Erstellen Sie einen temporären Ordner, wie `D:\temp`.
2. Erstellen Sie die folgenden zwei Unterordner im temporären Ordner:
 - `Win2008R2Copy`
 - `Win2008R2Mod`
3. Kopieren Sie den gesamten Inhalt aus dem DVD-Installationsmedium in den Ordner `Win2008R2Copy`.

4. Öffnen Sie die Windows Automated Installation Kit (AIK)-Eingabeaufforderung im erweiterten Modus aus „All program“ (Alle Programme), und geben Sie dann den folgenden Befehl aus:

```
attrib -r D:\Temp\Win2008R2Copy\sources\boot.wim
```

5. Geben Sie den folgenden Befehl aus, um das `boot.wim`-Abbild zu mounten:

```
dism /Mount-WIM  
/WimFile:D:\Temp\Win2008R2Copy\sources\boot.wim /index:1 /  
MountDir:D:\Temp\Win2008R2Mod
```

6. Das `boot.wim`-Image wurde im Ordner `Win2008R2Mod` gemountet. Suchen Sie alle Instanzen der unten aufgeführten Dateien in den Unterordnern des Ordners `Win2008R2Mod`, und löschen Sie diese:

- `netevbda.inf`
- `netevbda.pnf`
- `evbda.sys`
- `netbxnda.inf`
- `netbxnda.pnf`
- `bxnd60a.sys`
- `bxvbda.sys`
- `netbvbdad.inf`
- `netbvbdad.pnf`

Geben Sie den folgenden Befehl aus, um alle Instanzen der zu löschenden Dateien leicht zu finden:

```
dir /s D:\Temp\Win2008R2Mod\filename
```

7. Geben Sie den folgenden Befehl aus, um das `boot.wim`-Image zu unmounten:

```
dism /unmount-wim /Mountdir:D:\Temp\Win2008R2Mod /commit
```

8. Wiederholen Sie die Schritte 5 bis 7 und setzen Sie den `index = 2` für den Befehl in [Schritt 5](#).

In diesem Beispiel wird `index 2` für die Standardedition verwendet. Ändern Sie den Index entsprechend für andere Editionen.

Einfügen (Slipstreaming) der QLogic-Treiber in die Windows-Imagedateien

Siehe diese Anweisungen im FCoE-Artikel.

Um die QLogic-Treiber in die Windows-Imagedateien einzufügen, müssen Sie die Treiberinstallationspakete für die entsprechende Windows Server-Version (2008 R2, 2008 SP2, 2012 oder 2012 R2) verwenden.

Legen Sie diese Treiberpakete in ein Arbeitsverzeichnis. Kopieren Sie zum Beispiel alle Treiberpakete und Dateien, die auf Ihrer Windows Server-Version verwendet werden können, an den Beispiel-Speicherort des Ordners in Schritt 3:

■ `C:\Temp\drivers`

Als letztes fügen Sie diese Treiber in die Windows-Image (WIM)-Dateien ein und installieren die entsprechende Windows Server-Version von den aktualisierten Images.

Einfügen der QLogic-Treiber in die Windows-Imagedateien:

1. Installieren Sie bei Windows Server 2008 R2 und SP2 das Windows Automated Installation Kit (AIK).

Oder installieren Sie bei Windows Server 2012 und 2012 R2 das Windows Assessment and Deployment Kit (ADK).

2. Geben Sie die folgenden Befehle aus, um einen temporären Ordner zu erstellen, und stellen Sie ihn als den aktuellen Ordner für alle späteren Schritte ein:

```
md C:\Temp
cd /d C:\Temp
```

3. Geben Sie die folgenden Befehle aus, um zwei Unterordner in `C:\temp` zu erstellen:

```
md src
md mnt
md drivers (md Treiber)
```

4. Geben Sie den folgenden Befehl aus, um die Original-DVD in den Unterordner `src` zu kopieren.

```
xcopy N:\ .\src /e /c /i /f /h /k /y /q
```

Beachten Sie, dass sich in diesem Beispiel die Installations-DVD im Laufwerk `N:` befindet. ein.

5. Öffnen Sie eine Eingabeaufforderung zur Bereitstellung und für die Bildverarbeitungstools im erweiterten (Administrator)-Modus. Legen Sie anschließend `c:\Temp` als aktuellen Ordner fest.

Beachten Sie, dass dieses Eingabeaufforderungsfenster in allen folgenden Schritten verwendet wird.

6. Geben Sie die folgenden Befehle aus:

```
attrib -r .\src\sources\boot.wim
attrib -r .\src\sources\install.wim
```

7. Geben Sie den folgenden Befehl aus, um das `boot.wim`-Image zu mounten:

```
dism /mount-wim /wimfile:.\src\sources\boot.wim /index:2  
/mountdir:.\mnt
```

Hinweis: Sie müssen für den Indexwert immer „2“ verwenden.

8. Geben Sie die folgenden Befehle aus, um die folgenden Treiber zum derzeit gemounteten Image hinzuzufügen:

```
dism /image:.\mnt /add-driver /driver:C:\Temp\drivers /Recurse /ForceUnsigned
```

9. Geben Sie den folgenden Befehl aus, um das `boot.wim`-Image zu unmounten:

```
dism /unmount-wim /mountdir:.\mnt /commit
```

10. Geben Sie den folgenden Befehl aus, um den Index des gewünschten SKU im `install.wim`-Image zu ermitteln:

```
dism /get-wiminfo /wimfile:.\src\sources\install.wim
```

Unter Windows Server 2012 wird Index 2 z. B. als „Windows Server 2012 SERVERSTANDARD“ identifiziert.

11. Geben Sie den folgenden Befehl aus, um das `install.wim`-Image zu mounten:

```
dism /mount-wim /wimfile:.\src\sources\install.wim /index:X  
/mountdir:.\mnt
```

Hinweis: `X` ist ein Platzhalter für den Indexwert, den Sie im vorhergehenden Schritt erhalten haben.

12. Geben Sie die folgenden Befehle aus, um diese Treiber zum derzeit gemounteten Image hinzuzufügen:

```
dism /image:.\mnt /add-driver /driver:C:\Temp\drivers /Recurse /ForceUnsigned
```

13. Geben Sie den folgenden Befehl aus, um das `install.wim`-Image zu unmounten:

```
dism /unmount-wim /mountdir:.\mnt /commit
```

14. Bereiten Sie die ISO-Erstellung vor, indem Sie die Startdateien in `C:\temp` kopieren:

```
copy "<AIK or ADK path>..\etfsboot.com" C:\Temp  
copy "<AIK or ADK path>..\efisys.bin" C:\Temp
```

15. Geben Sie den folgenden Befehl aus, um eine `.iso`-Datei zu erstellen:

```
oscdimg -m -o -u2 -udfver102 -lslipstream -bootdata:2#p0,e,b"C:\Temp\  
etfsboot.com"#pEF,e,b"C:\Temp\efisys.bin" c:\temp\src c:\temp\Win20xxMOD.iso
```

Beachten Sie, dass `xx` in den Dateinamen ein Platzhalter für die Windows Server-Betriebssystemversion (2012, 2008 R2 oder 2008 SP2.) ist.

16. Brennen Sie mit einem DVD-Brennprogramm die von Ihnen erstellte `.iso`-Datei auf eine DVD.
17. Verwenden Sie die DVD, die Sie im vorhergehenden Schritt erstellt haben, um die passende Windows Server-Version zu installieren.

Booten

Nachdem das System für ein iSCSI-Booten vorbereitet wurde und sich das Betriebssystem auf dem iSCSI-Ziel befindet, wird in einem letzten Schritt der tatsächliche Bootvorgang ausgeführt. Das System bootet Windows oder Linux über das Netzwerk und verhält sich so, als würde sich das Betriebssystem auf der lokalen Festplatte befinden.

1. Booten Sie den Server neu.
2. Drücken Sie die Tasten STRG+S.
3. Setzen Sie den **HBA Boot Mode** (HBA Boot-Modus) für das Booten über einen Offload-Pfad auf **Enabled** (Aktiviert).
Setzen Sie den **HBA Boot Mode** (HBA Boot-Modus) für das Booten über einen Non-Offload-Pfad auf **Disabled** (Deaktiviert). (Dieser Parameter kann nicht geändert werden, wenn der Adapter sich im Multifunktionsmodus befindet.)

Wenn eine CHAP-Authentifizierung erforderlich ist, aktivieren Sie die CHAP-Authentifizierung, nachdem Sie festgestellt haben, dass der Bootvorgang ordnungsgemäß erfolgt (siehe „[Aktivieren der CHAP-Authentifizierung](#)“ auf [Seite 100](#)).

Weitere Hinweise zu iSCSI-Boot

Beachten Sie diese zusätzlichen Faktoren bei der Konfiguration eines Systems für iSCSI-Booten.

Ändern der Einstellungen für Übertragungsrate und Duplex in Windows-Umgebungen

Das Ändern der Einstellungen für Übertragungsrate und Duplex am Boot-Port mithilfe des Windows Device Manager während des iSCSI-Boots über den Offload-Pfad wird nicht unterstützt. Das Booten über den NDIS-Pfad wird unterstützt. Die Einstellungen für Übertragungsrate und Duplex können mithilfe des Dienstprogramms QCS für den iSCSI-Boot über die Offload- und NDIS-Pfade geändert werden.

Lokal verwaltete Adresse

Für iSCSI-bootfähige Geräte wird eine auf der QCS-Konfigurationsseite im Bereich **Advanced** (Erweitert) anhand der Eigenschaft **Locally Administered Address** (Lokal verwaltete Adresse) zugewiesene benutzerdefinierte MAC-Adresse nicht unterstützt.

Virtuelle LANs

VLAN-Markierung (virtuelles LAN) wird für iSCSI-Boot mit dem Microsoft iSCSI Software Initiator nicht unterstützt.

„DD“-Methode zur Erstellung eines iSCSI-Boot-Image

Wenn die Installation direkt in einem Remote-iSCSI-Ziel nicht möglich ist, verwenden Sie alternativ zur Erstellung eines solchen Image die „DD“-Methode. Für diese Methode ist das Installieren des Image direkt auf einer lokalen Festplatte notwendig, dann wird ein iSCSI-Boot-Image für den nachfolgenden Systemstart erstellt:

Erstellen eines iSCSI-Boot-Image mit „DD“:

1. Installieren Sie das Linux-Betriebssystem auf Ihrer lokalen Festplatte, und stellen Sie sicher, dass der Open-iSCSI-Initiator auf dem aktuellsten Stand ist.
2. Stellen Sie sicher, dass alle Ausführungsebenen des Netzwerkdiensts aktiviert sind.
3. Stellen Sie sicher, dass die Ausführungsebenen 2, 3 und 5 des iSCSI-Diensts aktiviert sind.
4. Aktualisieren Sie `iscsiuio`. Das `iscsiuio`-Paket wird auf der QLogic-CD bereitgestellt. Dieser Schritt ist für SUSE 10 nicht erforderlich.
5. Installieren Sie das `linux-nx2`-Paket auf Ihrem Linux-System. Dieses Paket wird auf der QLogic-CD bereitgestellt.
6. Installieren Sie das `bibt`-Paket auf Ihrem Linux-System. Dieses Paket wird auf der QLogic-CD bereitgestellt.
7. Löschen Sie alle `ifcfg-eth*`-Dateien.
8. Konfigurieren Sie einen Port des Netzwerkadapters für die Verbindung mit dem iSCSI-Ziel (Anweisungen finden Sie unter [„Konfigurieren des iSCSI-Ziels“ auf Seite 88](#)).
9. Stellen Sie eine Verbindung zum iSCSI-Ziel her.
10. Kopieren Sie die lokale Festplatte per `DD`-Befehl in das iSCSI-Ziel.
11. Geben Sie nach Abschluss des `DD`-Vorgangs den `sync`-Befehl einige Male aus, melden Sie sich vom iSCSI-Ziel ab und anschließend wieder an.

12. Führen Sie auf allen auf dem iSCSI-Ziel erstellten Partitionen den `fsck`-Befehl aus.
13. Wechseln Sie zum Ordner `/OPT/bcm/bibt`, und führen Sie das Skript `iscsi_setup.sh` zum Erstellen der `initrd`-Images aus. Option 0 erzeugt ein Non-Offload-Image und Option 1 ein Offload-Image. Das Skript `Iscsi_script.sh` erstellt unter SUSE 10 nur das Non-Offload-Image, da Offload von SUSE 10 nicht unterstützt wird.
14. Mounten Sie die `/boot`-Partition auf dem iSCSI-Ziel.
15. Kopieren Sie die `initrd`-Images, die Sie in [Schritt 13](#) von Ihrer lokalen Festplatte erstellt haben, auf die in [Schritt 14](#) gemountete Partition.
16. Bearbeiten Sie auf der in [Schritt 14](#) gemounteten Partition das `grub`-Menü so, dass auf die neuen `initrd`-Images gezeigt wird.
17. Unmounten Sie die `/boot`-Partition auf dem iSCSI-Ziel.
18. (Nur Red Hat) Um CHAP zu aktivieren, müssen Sie den CHAP-Abschnitt der `iscsid.conf`-Datei auf dem iSCSI-Ziel anpassen. Bearbeiten Sie die `iscsid.conf`-Datei nach Bedarf mit Ein- oder Zweiweg-CHAP-Daten.
19. Fahren Sie das System herunter, und trennen Sie die Verbindung zur lokalen Festplatte.

Sie können jetzt iSCSI in das iSCSI-Ziel booten.
20. (Optional) Konfigurieren Sie die iSCSI-Boot-Parameter, z. B. CHAP-Parameter (siehe [„Konfigurieren des iSCSI-Ziels“](#) auf [Seite 88](#)).
21. Setzen Sie das Booten in das iSCSI-Boot-Image fort, und wählen Sie eines der erstellten Images aus (Non-Offload oder Offload). Sie sollten dabei Ihre Auswahl im Abschnitt zu den **iSCSI Boot Parameters** (iSCSI-Boot-Parametern) berücksichtigen. Wenn **HBA Boot Mode** (HBA Boot-Modus) im Abschnitt **iSCSI Boot Parameters** (iSCSI-Boot-Parameter) aktiviert wurde, müssen Sie das Offload-Image booten. Bei SUSE 10.x und SLES 11 wird kein Offload unterstützt.

Fehlerbehebung bei iSCSI-Boot

Im Folgenden finden Sie einige nützliche Tipps für die Problembehandlung bei iSCSI-Boot.

Problem: Beim Starten von Windows Server 2008 R2 mit iSCSI über den NDIS-Pfad des Adapters kommt es zu einem Systemabsturz, wenn der Initiator mit einer link-local-IPv6-Adresse und das Ziel mit einer routerkonfigurierten IPv6-Adresse konfiguriert ist.

Lösung: Dies ist ein bekanntes Windows-TCP/IP-Stack-Problem.

Problem: Das iSCSI-Absturzspeicherabbild-Dienstprogramm von QLogic kann ein Speicherabbild nicht richtig erfassen, wenn die Verbindungsgeschwindigkeit für iSCSI-Boot auf 10 MBit/s oder 100 MBit/s festgelegt ist.

Lösung: Das iSCSI-Absturzspeicherabbild-Dienstprogramm wird unterstützt, wenn die Verbindungsgeschwindigkeit für iSCSI-Boot auf 1 GBit/s oder 10 GBit/s festgelegt ist. 10 Mbit/s und 100 Mbit/s werden nicht unterstützt.

Problem: Ein iSCSI-Ziel wird nicht als Installationsziel erkannt, wenn Windows Server 2008 über eine IPv6-Verbindung installiert wird.

Lösung: Dies ist ein bekanntes Problem, das durch ein Drittanbieterprodukt verursacht wird. Weitere Informationen finden Sie in der Microsoft Knowledge Base KB 971443 unter <http://support.microsoft.com/kb/971443>.

Problem: Wenn Sie iSCSI-Boot vom Microsoft-Standardpfad auf QLogic iSCSI Offload verschieben, kann der Boot-Vorgang nicht abgeschlossen werden.

Lösung: Installieren oder aktualisieren Sie den QLogic-VBD-Treiber (Virtual Bus Device) zusammen mit dem OIS-Treiber auf die aktuelle Version, bevor Sie den iSCSI-Boot-Pfad verschieben.

Problem: Das iSCSI-Konfigurationsprogramm kann nicht gestartet werden.

Lösung: Stellen Sie sicher, dass die iSCSI-Boot-Firmware im NVRAM installiert ist.

Problem: Beim Installieren der QLogic-Treiber mittels Windows Plug-and-Play (PnP) kommt es zu einem Systemabsturz.

Lösung: Installieren Sie die Treiber mithilfe des Setup-Programms.

Problem: Wenn Sie bei statischer IP-Konfiguration von iSCSI-Boot (Layer 2) zum QLogic iSCSI-Host Bus Adapter wechseln, entsteht ein IP-Adressenkonflikt.

Lösung: Ändern Sie die IP-Adresse im Betriebssystem.

Problem: Nachdem die iSCSI-Boot-LUN auf den Wert 255 festgelegt wurde, kommt es bei der Ausführung von iSCSI-Boot zu einem Systemabsturz.

Lösung: Zwar unterstützt die iSCSI-Lösung von QLogic einen LUN-Bereich von 0 bis 255; dies ist jedoch beim Microsoft iSCSI Software Initiator nicht der Fall. Legen Sie für die LUN einen Wert zwischen 0 und 254 fest.

Problem: NDIS-Miniports mit Code 31 Yellow-Bang nach Layer 2 iSCSI-Boot-Installation.

Lösung: Führen Sie die aktuelle Version des Treiberinstallationsprogramms aus.

Problem: Posteingangstreiber kann nicht aktualisiert werden, wenn eine Hardware-ID ohne Posteingang vorhanden ist.

Lösung: Erstellen Sie ein eigenes Slipstream-DVD-Image mit unterstützten Treibern, die auf den Installationsmedien vorhanden sind.

Problem: Unter Windows Server 2012 kann das Umschalten zwischen dem iSCSI Host Bus Adapter-Offload-Modus und dem Software-Initiator für iSCSI-Boot dafür sorgen, dass die Maschine in einem Status läuft, in dem der Host Bus Adapter-Offload-Miniport „bxois“ nicht geladen wird.

Lösung: Ändern Sie manuell die Zeile

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\bxois\StartOverride] von 3 in 0. Modifizieren Sie den Registrierungsschlüssel, bevor Sie in CCM vom NDIS- zum Hot Bus Adapter-Pfad wechseln.

ANMERKUNG

Microsoft empfiehlt diese Methode nicht. Das Umschalten des Boot-Pfads von NDIS zu Hot Bus Adapter oder umgekehrt nach dem Abschluss der Installation wird nicht empfohlen.

Problem: Mit Windows Server 2008 oder höher lässt sich keine Verbindung zu einem EqualLogic-Ziel herstellen.

Lösung: Lassen Sie durch Hinzufügen einer Ausnahme zu Ihrer Firewall ICMP-Echoanfragen zu.

Problem: Die Installation von Windows auf einem iSCSI-Ziel über iSCSI-Boot schlägt fehl, wenn eine Verbindung mit einem 1 GBit/s-Switch-Port hergestellt wird.

Lösung: Dieser Fehler ist eine Limitierung hinsichtlich der Adapter, die SFP+ als physische Verbindung verwenden. Standardmäßig wird SFP+ mit 10 Gbit/s betrieben, und es unterstützt keine automatische Aushandlung.

iSCSI-Absturzspeicherabbild

Wenn Sie das QLogic iSCSI Crash Dump utility (QLogic-Dienstprogramm) für das iSCSI-Absturzspeicherabbild verwenden, müssen Sie den iSCSI-Absturzspeicherabbild-Treiber installieren. Weitere Informationen finden Sie unter [„Verwenden des Installationsprogramms“ auf Seite 77](#).

iSCSI-Offload unter Windows Server

iSCSI-Offload ist eine Technologie, mit der die rechenintensiven Aufgaben bei der Verarbeitung des iSCSI-Protokolls von den Hostprozessoren zu deren Entlastung auf den iSCSI-Hostbus-Adapter verlagert werden und so bei gleichzeitiger Erhöhung der Netzwerkleistung und des Durchsatzes eine optimale Nutzung der Serverprozessoren erreicht wird.

In diesem Abschnitt wird die iSCSI-Offload-Funktion von QLogic für die Netzwerkadapterfamilie BCM57xx und BCM57xxx bei Windows Server-Systemen behandelt. Informationen zu iSCSI-Offload für Linux finden Sie unter [„iSCSI-Verschiebung in Linux“ auf Seite 59](#).

Konfigurieren von iSCSI-Offload

Mit der entsprechenden iSCSI-Offload-Lizenz können Sie Ihren iSCSI-fähigen Netzwerkadapter BCM57xx und BCM57xxx so konfigurieren, dass er die iSCSI-Verarbeitung vom Hostprozessor weg verschiebt. Mithilfe der folgenden Schritte können Sie Ihr System so einrichten, dass es die Vorteile der iSCSI-Offload-Funktion von QLogic nutzen kann.

- [Installieren von QLogic-Treibern und Management-Anwendungen](#)
- [Installieren von Microsoft iSCSI Software Initiator](#)
- [Konfigurieren von QLogic-iSCSI mit QCC](#)
- [Konfigurieren von Microsoft Initiator zur Verwendung von QLogic iSCSI Offload](#)

Installieren von QLogic-Treibern und Management-Anwendungen

Installieren Sie die Windows-Treiber und Management-Anwendungen.

Installieren von Microsoft iSCSI Software Initiator

Bei Windows Server 2008 und höheren Versionen ist der iSCSI-Initiator bereits enthalten. Wenn Sie den iSCSI-Initiator von Microsoft herunterladen möchten (er also nicht bereits installiert ist), klicken Sie auf den passenden Link für Ihr System:

<http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=18986>

Konfigurieren von QLogic-iSCSI mit QCC

Mit der QConvergeConsole-Benutzeroberfläche (QCC) können alle Netzwerkadapter von QLogic sowie erweiterte Funktionen verwaltet werden. Weitere Informationen finden Sie in der Onlinehilfe zu QCC GUI.

1. Öffnen Sie die QCC-Benutzeroberfläche.
2. Wählen Sie den QLogic BCM57xx und BCM57xxx C-NIC-iSCSI-Adapter aus. Wenn der C-NIC-iSCSI-Adapter nicht angezeigt wird, wählen Sie das VBD-Gerät aus und aktivieren iSCSI-Offload. Wählen Sie dazu auf der Seite „Konfiguration“ im Abschnitt **Resource Reservations** (Ressourcenreservierungen) die Option **iSCSI Offload Engine** (iSCSI-Offload-Engine) aus.
3. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration).
4. DHCP ist das Standardverfahren für die Zuweisung von IP-Adressen. Sie können aber auch eine statische IP-Adressenzuweisung verwenden, wenn Sie diese Methode für die Zuweisung von IP-Adressen bevorzugen.

ANMERKUNG

Die Methode für die Zuweisung von IP-Adressen kann nicht geändert werden, wenn der Adapter zum Booten verwendet wurde.

5. Klicken Sie auf **Apply** (Übernehmen), und schließen Sie die QCC-Benutzeroberfläche.

Konfigurieren von Microsoft Initiator zur Verwendung von QLogic iSCSI Offload

Nachdem Sie die IP-Adresse für den iSCSI-Adapter konfiguriert haben, müssen Sie Microsoft Initiator verwenden, um eine Verbindung mit dem iSCSI-Ziel unter Verwendung des iSCSI-Adapters von QLogic hinzuzufügen und zu konfigurieren. Weitere Informationen zu Microsoft Initiator finden Sie im entsprechenden Benutzerhandbuch von Microsoft.

1. Öffnen Sie Microsoft Initiator.
2. Konfigurieren Sie den IQN-Namen für den Initiator entsprechend Ihrem Setup. Klicken Sie auf Eigenschaften des iSCSI-Initiators, Seite General (Allgemein) (siehe [Abbildung 10-6](#)) und dann auf **Change** (Ändern).

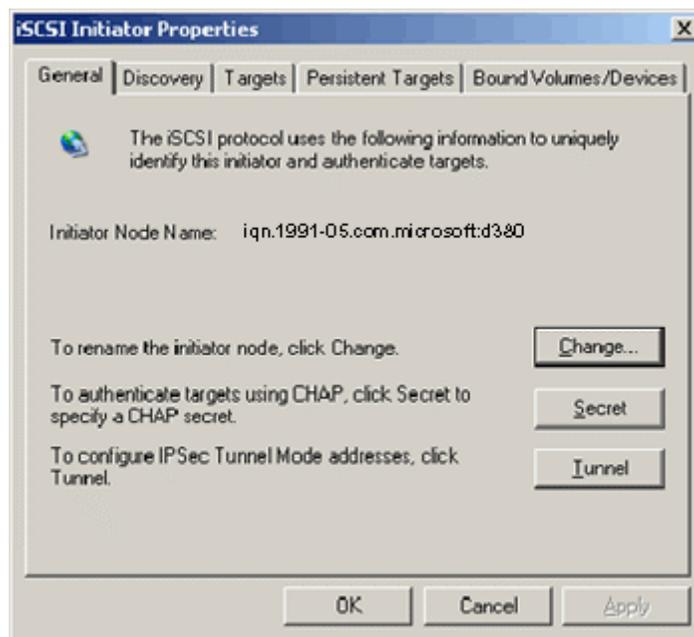


Abbildung 10-6. iSCSI-Initiatoreigenschaften: Seite „Allgemein“

3. Geben Sie im Dialogfeld „Initiator Node Name Change“ (Namensänderung Initiator-knoten) (siehe [Abbildung 10-7](#)) den IQN-Namen des Initiators ein und klicken Sie anschließend auf **OK**.

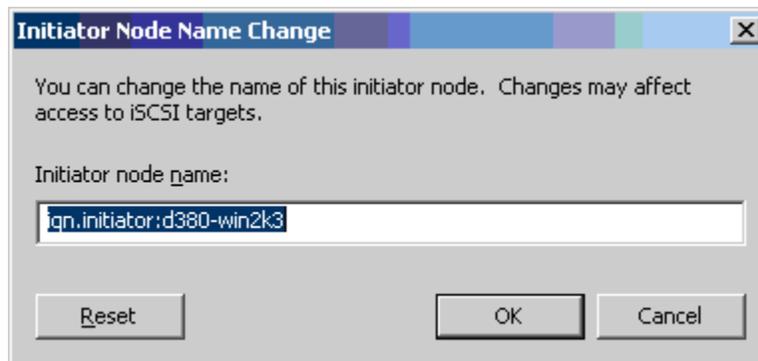
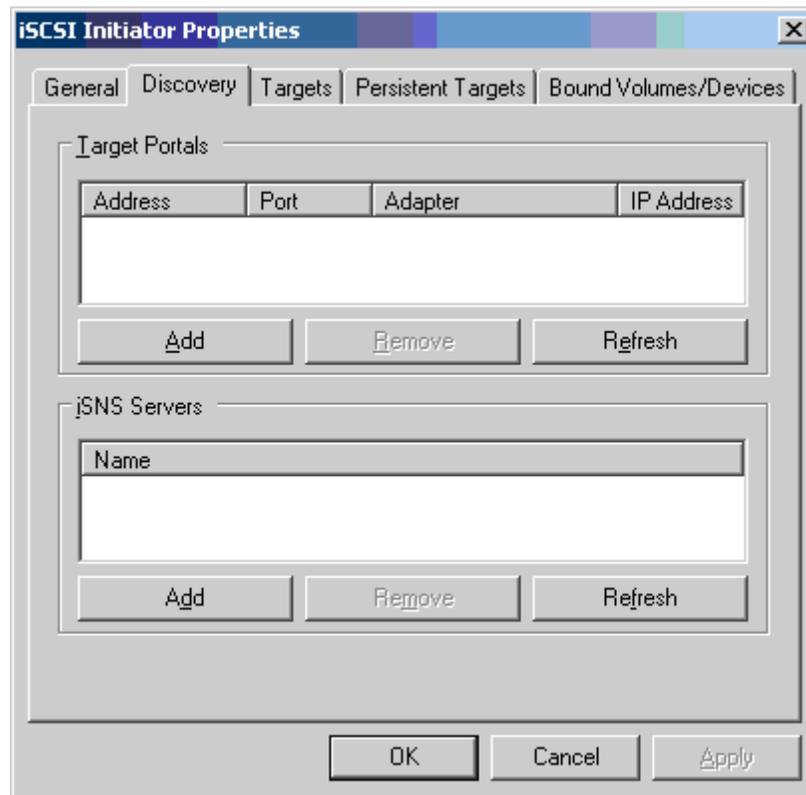


Abbildung 10-7. Ändern des Initiator Node Name (Initiatorknotennamens)

4. Klicken Sie unter Eigenschaften des iSCSI-Initiators ([Abbildung 10-8](#)) auf die Registerkarte **Discovery** (Ermittlung) und dann unter **Target Portals** (Zielportale) auf **Add** (Hinzufügen).



**Abbildung 10-8. iSCSI Initiator Properties (iSCSI-Initiatoreigenschaften):
Seite „Ermittlung“**

5. Geben Sie im Dialogfeld „Add Target Portal“ (Zielportal hinzufügen) (Abbildung 10-9) die IP-Adresse des Ziels ein, und klicken Sie auf **Advanced** (Erweitert).

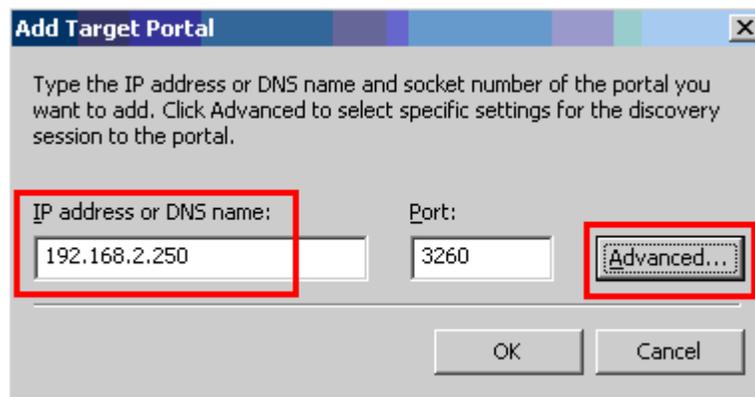


Abbildung 10-9. Dialogfeld „Add Target Portal“ (Zielportal hinzufügen)

6. Vervollständigen Sie die Seite „General“ (Allgemein) im Dialogfeld „Advanced Settings“ (Erweiterte Einstellungen) folgendermaßen:
 - a. Wählen Sie für **Local adapter** (Lokaler Adapter) den QLogic BCM57xx und BCM57xxx iSCSI-AdapterC-NIC aus.
 - b. Wählen Sie unter **Source IP** (Quell-IP) die IP-Adresse des Adapters aus.
 - c. Um das Dialogfeld „Advanced Settings“ (Erweiterte Einstellungen) zu schließen und Ihre Änderungen zu speichern, klicken Sie auf **OK**.

Abbildung 10-10 zeigt ein Beispiel.

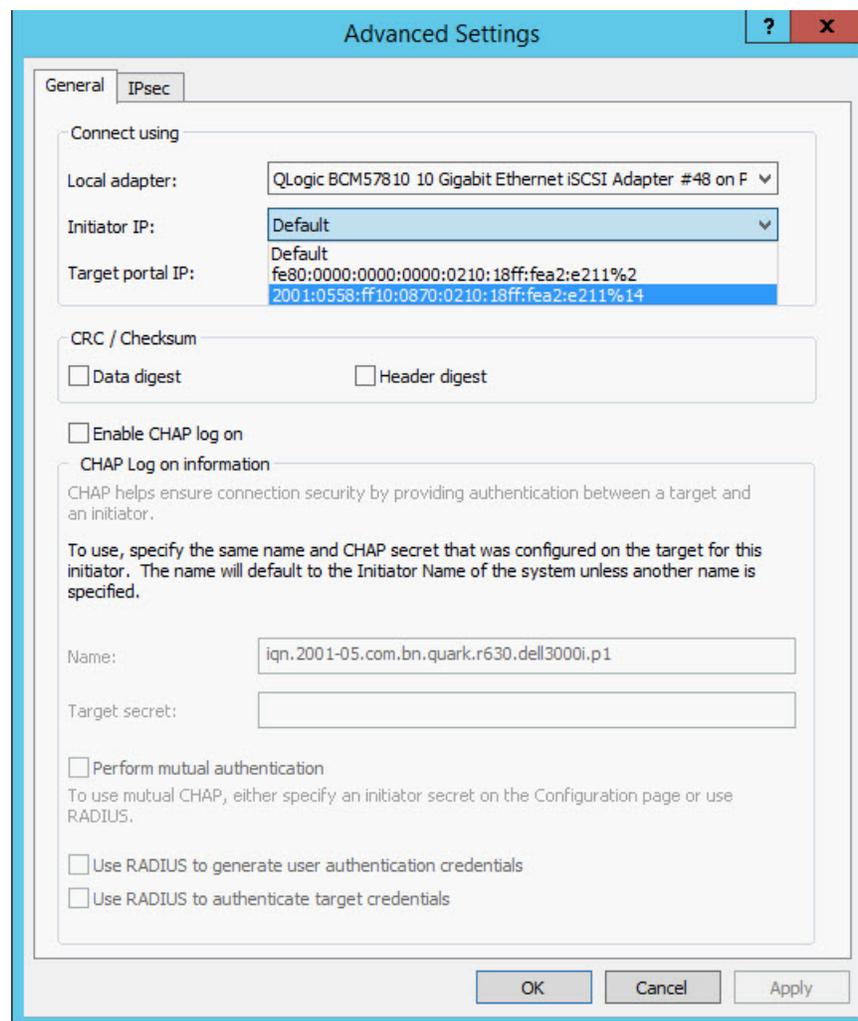
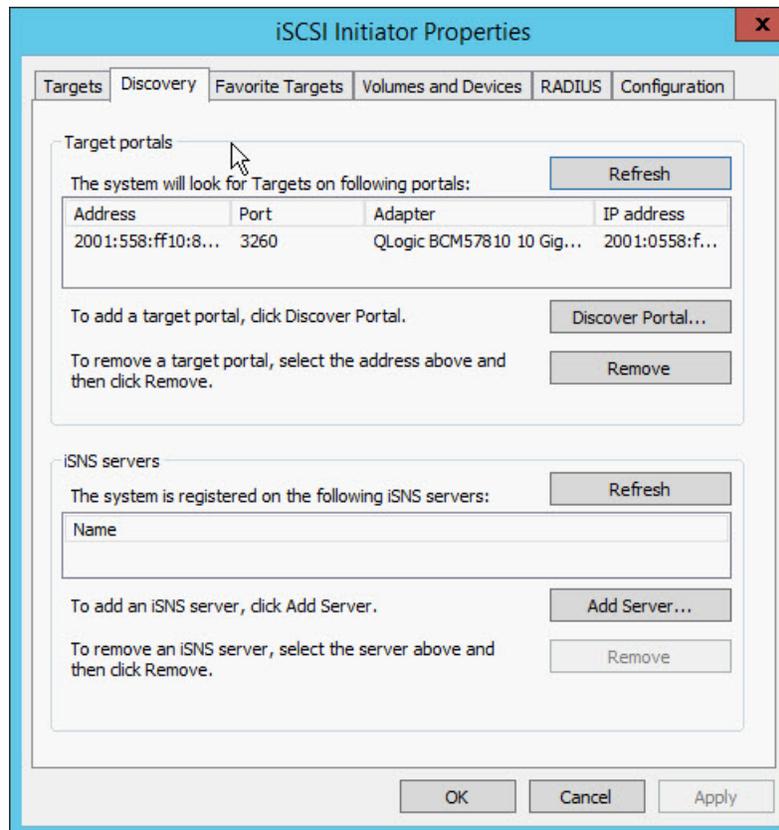


Abbildung 10-10. Erweiterte Einstellungen: General Page (Allgemeine Seite)

7. Klicken Sie unter Eigenschaften des iSCSI-Initiators auf die Registerkarte **Discovery** (Ermittlung) und dann auf der Seite „Discovery“ (Ermittlung) auf **OK**, um das Zielportal hinzuzufügen. [Abbildung 10-11](#) zeigt ein Beispiel.



**Abbildung 10-11. iSCSI Initiator Properties (iSCSI-Initiatoreigenschaften):
Discovery Page (Seite „Ermittlung“)**

8. Klicken Sie unter Eigenschaften des iSCSI-Initiators auf die Registerkarte **Targets** (Ziele).

- Wählen Sie auf der Seite „Targets“ (Ziele) das Ziel aus, und klicken Sie auf **Log on** (Anmelden), um sich unter Verwendung des iSCSI-Adapters von QLogic bei Ihrem iSCSI-Ziel anzumelden. [Abbildung 10-12](#) zeigt ein Beispiel.

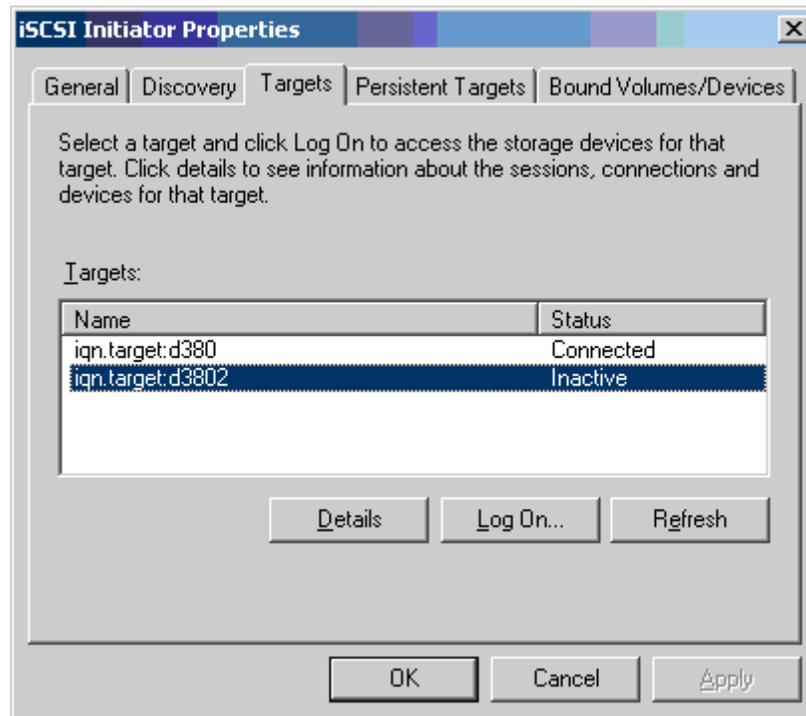


Abbildung 10-12. iSCSI Initiator Properties (iSCSI-Initiatoreigenschaften): Seite „Ziele“

- Klicken Sie im Dialogfeld „Log On To Target“ (Bei Ziel anmelden) ([Abbildung 10-13](#)) auf **Advanced** (Erweitert).

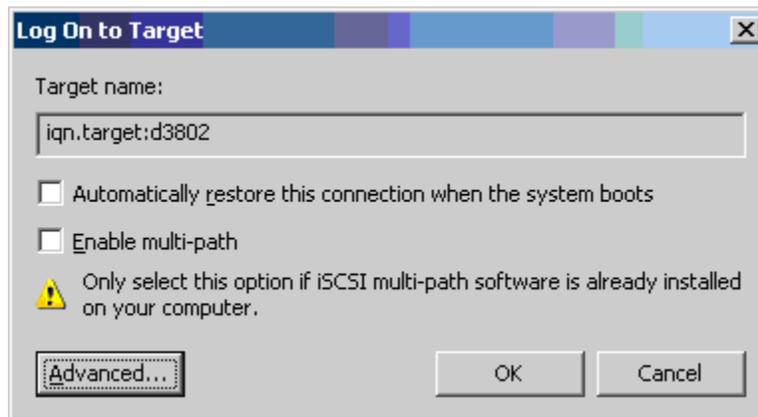


Abbildung 10-13. Log On to Target (Bei Ziel anmelden)

11. Wählen Sie im Dialogfeld „Advanced Settings“ (Erweiterte Einstellungen) auf der Seite „General“ (Allgemein) die QLogic BCM57xx und BCM57xxxC-NIC iSCSI-Adapter als **Local Adapter** (lokalen Adapter) aus und klicken dann auf **OK**. [Abbildung 10-14](#) zeigt ein Beispiel.

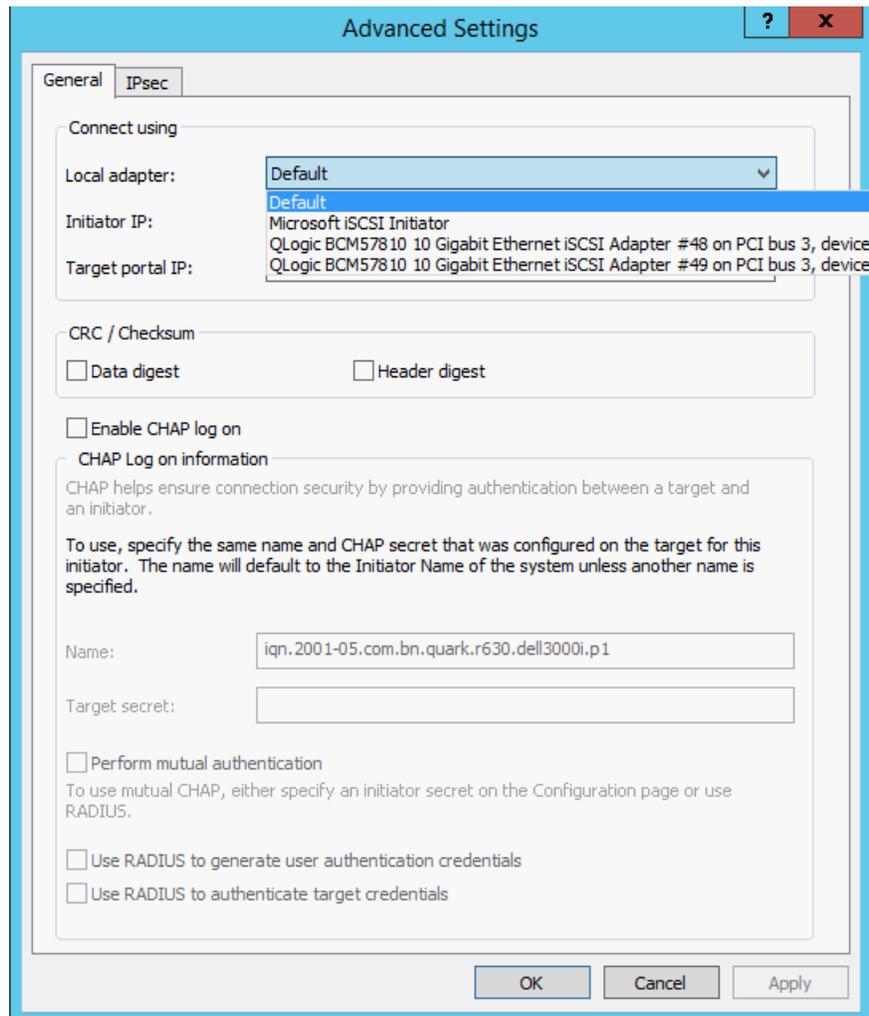


Abbildung 10-14. Advanced Settings (Erweiterte Einstellungen): Seite „Allgemein“, Lokaler Adapter

12. Klicken Sie auf **OK**, um Microsoft Initiator zu schließen.
13. Zur Formatierung Ihrer iSCSI-Partition verwenden Sie die Datenträgerverwaltung.

ANMERKUNG

- Teaming unterstützt keine iSCSI-Adapter.
 - Teaming unterstützt keine NDIS-Adapter, die sich im Boot-Pfad befinden.
 - Teaming unterstützt NDIS-Adapter, die sich nicht im iSCSI-Boot-Pfad befinden, jedoch nur für die SLB-Teamart.
-

Häufig gestellte Fragen zu iSCSI-Offload

Frage: Wie weise ich eine IP-Adresse für iSCSI-Offload zu?

Antwort: Verwenden Sie in QLogic Control Suite (QCS) die Registerkarte „Configurations“ (Konfigurationen).

Frage: Welche Werkzeuge soll ich verwenden, um die Verbindung mit dem Ziel herzustellen?

Antwort: Verwenden Sie Microsoft iSCSI Software Initiator (ab Version 2.08).

Frage: Woher weiß ich, dass sich die Verbindung im Offload-Modus befindet?

Antwort: Verwenden Sie Microsoft iSCSI Software Initiator. Geben Sie in einer Befehlszeile `iscsicli sessionlist` ein. Bei Verbindungen im iSCSI-Offload-Modus wird unter **Initiator Name** (Initiatorname) ein Eintrag angezeigt, der mit „B06BDRV...“ beginnt. Bei einer Verbindung ohne Offload wird ein Eintrag angezeigt, der mit „Root...“ beginnt.

Frage: Welche Konfigurationen sollte ich vermeiden?

Antwort: Die IP-Adresse darf nicht dieselbe sein wie für das LAN.

Frage: Warum misslingt die Installation, wenn man versucht, mit Adaptern für das Windows Server-BS für BCM57xx und BCM57xxx eine iSCSI-Offload-Installation durchzuführen?

Antwort: Es gibt einen Konflikt mit dem internen Posteingangstreiber.

Ereignisprotokollmeldungen für den Offload-iSCSI-(OIS)-Treiber

In [Tabelle 10-5](#) werden die Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber aufgelistet.

Tabelle 10-5. Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber (OIS-Treiber)

Meldungsnummer	Schweregrad	Meldung
1	Fehler	Initiator failed to connect to the target. (Der Initiator hat keine Verbindung zum Ziel hergestellt.) Target IP address and TCP Port number are specific in dump data. (Ziel-IP-Adresse und TCP-Portnummer sind spezifisch in Speicherabbildaten.)
2	Fehler	The initiator could not allocate resources for an iSCSI session. (Der Initiator konnte keine Ressourcen für eine iSCSI-Sitzung zuordnen.)
3	Fehler	Maximum command sequence number is not serially greater than expected command sequence number in login response. (Die maximale Befehlssequenznummer ist seriell nicht größer als die erwartete Befehlssequenznummer in der Anmeldeantwort.) Dump data contains Expected Command Sequence number followed by Maximum Command Sequence number. (Speicherabbildaten enthalten die erwartete Befehlssequenznummer und danach die maximale Befehlssequenznummer.)
4	Fehler	MaxBurstLength is not serially greater than FirstBurstLength. (MaxBurstLength ist seriell nicht größer als FirstBurstLength.) Dump data contains FirstBurstLength followed by MaxBurstLength. (Speicherabbildaten enthalten FirstBurstLength und danach MaxBurstLength.C)
5	Fehler	Failed to setup initiator portal. (Initiatorportal wurde nicht eingerichtet.) Error status is specified in the dump data. (Der Fehlerstatus ist in den Speicherabbildaten angegeben.)
6	Fehler	The initiator could not allocate resources for an iSCSI connection. (Der Initiator konnte keine Ressourcen für eine iSCSI-Verbindung zuordnen.)
7	Fehler	The initiator could not send an iSCSI PDU. (Der Initiator konnte keine iSCSI PDU senden.) Error status is specified in the dump data. (Der Fehlerstatus ist in den Speicherabbildaten angegeben.)

Tabelle 10-5. Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber (OIS-Treiber) (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung
8	Fehler	Target or discovery service did not respond in time for an iSCSI request sent by the initiator. iSCSI Function code is specified in the dump data. (Der Ziel- oder Erkennungsdienst antwortete nicht rechtzeitig für eine vom Initiator versandte iSCSI-Anfrage. Der iSCSI-Funktionscode wird in den Speicherabbilddaten definiert.) For details about iSCSI Function code, refer to the iSCSI user's guide. (Details über den iSCSI-Funktionscode finden Sie im iSCSI-Benutzerhandbuch.)
9	Fehler	Target did not respond in time for a SCSI request. (Das Ziel antwortete nicht rechtzeitig für eine SCSI-Anfrage.) The CDB is specified in the dump data. (Der CBD ist in den Speicherabbilddaten angegeben.)
10	Fehler	Login request failed. (Anmeldeanforderung fehlgeschlagen.) The login response packet is specified in the dump data. (Das Anmeldeantwortpaket ist in den Speicherabbilddaten angegeben.)
11	Fehler	Target returned an invalid login response packet. (Das Ziel hat ein ungültiges Anmeldeantwortpaket zurückgegeben.) The login response packet is specified in the dump data. (Das Anmeldeantwortpaket ist in den Speicherabbilddaten angegeben.)
12	Fehler	Target provided invalid data for login redirect. (Das Ziel hat ungültige Daten für die Anmeldeumleitung bereitgestellt.) Dump data contains the data returned by the target. (Die Speicherabbilddaten enthalten die vom Ziel zurückgegebenen Daten.)
13	Fehler	Target offered an unknown AuthMethod. (Das Ziel hat eine unbekannte AuthMethod angeboten.) Dump data contains the data returned by the target. (Die Speicherabbilddaten enthalten die vom Ziel zurückgegebenen Daten.)
14	Fehler	Target offered an unknown digest algorithm for CHAP. (Das Ziel hat einen unbekanntes Digest-Algorithmus für CHAP angeboten.) Dump data contains the data returned by the target. (Die Speicherabbilddaten enthalten die vom Ziel zurückgegebenen Daten.)
15	Fehler	CHAP challenge specified by the target contains invalid characters. (Die vom Ziel angegebene CHAP-Herausforderung enthält ungültige Zeichen.) Dump data contains the specified challenge. (Die Speicherabbilddaten enthalten die angegebene Herausforderung.)
16	Fehler	An invalid key was received during CHAP negotiation. (Während der CHAP-Verhandlung wurde ein ungültiger Schlüssel empfangen.) The key=value pair is specified in the dump data. (Das Schlüssel=Wert-Paar ist in den Speicherabbilddaten angegeben.)

Tabelle 10-5. Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber (OIS-Treiber) (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung
17	Fehler	CHAP Response specified by the target did not match the expected one. (Die vom Ziel angegebene CHAP-Antwort stimmte nicht mit der erwarteten überein.) Dump data contains the CHAP response. (Die Speicherabbilddaten enthalten die CHAP-Antwort.)
18	Fehler	Header Digest is required by the initiator, but target did not offer it. (Header Digest ist für den Initiator erforderlich, aber das Ziel hat es nicht angeboten.)
19	Fehler	Data Digest is required by the initiator, but target did not offer it. (Data Digest ist für den Initiator erforderlich, aber das Ziel hat es nicht angeboten.)
20	Fehler	Connection to the target was lost. (Die Verbindung mit dem Ziel wurde verloren.) The initiator will attempt to retry the connection. (Der Initiator wird versuchen, die Verbindung erneut herzustellen.)
21	Fehler	Data Segment Length specified in the header exceeds <code>MaxRecvDataSegmentLength</code> declared by the target. (Die im Kopfteil angegebene Datensegmentlänge ist größer als die vom Ziel erklärte <code>s MaxRecvDataSegmentLength</code> .)
22	Fehler	Header digest error was detected for the specified PDU. (Der Kopfteil-Digest-Fehler wurde für die angegebene PDU entdeckt.) Dump data contains the header and digest. (Speicherabbilddaten enthalten Kopfteil und Digest.)
23	Fehler	Target sent an invalid iSCSI PDU. (Das Ziel sandte eine ungültige iSCSI PDU.) Dump data contains the entire iSCSI header. (Die Speicherabbilddaten enthalten den ganzen iSCSI-Kopfteil.)
24	Fehler	Target sent an iSCSI PDU with an invalid opcode. (Das Ziel sandte eine iSCSI PDU mit einem ungültigen Opcode.) Dump data contains the entire iSCSI header. (Die Speicherabbilddaten enthalten den ganzen iSCSI-Kopfteil.)
25	Fehler	Data digest error was detected. (Daten-Digest-Fehler wurde entdeckt.) Dump data contains the calculated checksum followed by the specified checksum. (Die Speicherabbilddaten enthalten die berechnete Prüfsumme und danach die angegebene Prüfsumme.)
26	Fehler	Target trying to send more data than requested by the initiator. (Das Ziel versucht, mehr Daten zu versenden, als vom Initiator angefordert wurden.)

Tabelle 10-5. Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber (OIS-Treiber) (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung
27	Fehler	Initiator could not find a match for the initiator task tag in the received PDU. (Der Initiator konnte keine Übereinstimmung für die Initiator-Task-Kennnummer in der empfangenen PDU finden.) Dump data contains the entire iSCSI header. (Die Speicherabbilddaten enthalten den ganzen iSCSI-Kopfteil.)
28	Fehler	Initiator received an invalid R2T packet. (Der Initiator empfing ein ungültiges R2T-Paket.) Dump data contains the entire iSCSI header. (Die Speicherabbilddaten enthalten den ganzen iSCSI-Kopfteil.)
29	Fehler	Target rejected an iSCSI PDU sent by the initiator. (Das Ziel wies eine vom Initiator gesandte iSCSI PDU zurück.) Dump data contains the rejected PDU. (Die Speicherabbilddaten enthalten die zurückgewiesene PDU.)
30	Fehler	Initiator could not allocate a work item for processing a request. (Der Initiator konnte kein Arbeitselement für die Verarbeitung einer Anfrage zuordnen.)
31	Fehler	Initiator could not allocate resource for processing a request. (Der Initiator konnte keine Ressource für die Verarbeitung einer Anfrage zuordnen.)
32	„Information“ (Informationen)	Initiator received an asynchronous logout message. (Der Initiator empfing eine asynchrone Abmeldemeldung.) The Target name is specified in the dump data. (Der Zielname ist in den Speicherabbilddaten angegeben.)
33	Fehler	Challenge size specified by the target exceeds the maximum specified in iSCSI specification. (Die von Ziel angegebene Herausforderungsgröße überschreitet das in den iSCSI-Spezifikationen angegebene Maximum.)
34	„Information“ (Informationen)	A connection to the target was lost, but Initiator successfully reconnected to the target. (Eine Verbindung mit dem Ziel ging verloren, aber der Initiator hat die Verbindung mit dem Ziel erfolgreich wiederhergestellt.) Dump data contains the target name. (Die Speicherabbilddaten enthalten den Zielnamen.)
35	Fehler	Target CHAP secret is smaller than the minimum size (12 bytes) required by the specification. (Das Ziel-CHAP-Geheimnis ist kleiner als die Mindestgröße (12 Byte), die von den Angaben erfordert werden.)

Tabelle 10-5. Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber (OIS-Treiber) (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung
36	Fehler	Initiator CHAP secret is smaller than the minimum size (12 bytes) required by the specification. (Das Initiator-CHAP-Geheimnis ist kleiner als die von den Angaben erforderte Mindestgröße (12 Byte).) Dump data contains the specified CHAP secret. (Die Speicherabbilddaten enthalten das angegebene CHAP-Geheimnis.)
37	Fehler	FIPS service could not be initialized. (Der FIPS-Dienst konnte nicht initialisiert werden.) Persistent logons will not be processed. (Persistente Anmeldungen werden nicht verarbeitet.)
38	Fehler	Initiator requires CHAP for logon authentication, but target did not offer CHAP. (Der Initiator erfordert CHAP für die Anmeldeauthentifizierung, aber das Ziel hat CHAP nicht angeboten.)
39	Fehler	Initiator sent a task management command to reset the target. (Der Initiator hat einen Befehl zur Aufgabenverwaltung geschickt, um das Ziel neu einzustellen.) The target name is specified in the dump data. (Der Zielname ist in den Speicherabbilddaten angegeben.)
40	Fehler	Target requires logon authentication through CHAP, but Initiator is not configured to perform CHAP. (Das Ziel erfordert die Anmeldeauthentifizierung durch CHAP, aber der Initiator ist nicht für die Ausführung von CHAP konfiguriert.)
41	Fehler	Target did not send AuthMethod key during security negotiation phase. (Das Ziel hat während der Sicherheitsverhandlungsphase keinen AuthMethod-Schlüssel gesandt.)
42	Fehler	Target sent an invalid status sequence number for a connection. (Das Ziel hat eine ungültige Statussequenznummer für eine Verbindung gesandt.) Dump data contains Expected Status Sequence number followed by the specified status sequence number. (Die Speicherabbilddaten enthalten die Sequenznummer „Erwarteter Status“ und danach die Sequenznummer des angegebenen Status.)
43	Fehler	Target failed to respond in time for a login request. (Das Ziel hat nicht rechtzeitig für eine Anmeldeanforderung geantwortet.)
44	Fehler	Target failed to respond in time for a logout request. (Das Ziel hat nicht rechtzeitig für eine Abmeldeanforderung geantwortet.)
45	Fehler	Target failed to respond in time for a login request. (Das Ziel hat nicht rechtzeitig für eine Anmeldeanforderung geantwortet.) This login request was for adding a new connection to a session. (Diese Anmeldeanforderung diente dazu, einer Sitzung eine neue Verbindung hinzuzufügen.)

Tabelle 10-5. Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber (OIS-Treiber) (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung
46	Fehler	Target failed to respond in time for a SendTargets command. (Das Ziel hat nicht rechtzeitig für einen SendTargets-Befehl geantwortet.)
47	Fehler	Target failed to respond in time for a SCSI command sent through a WMI request. (Das Ziel hat nicht rechtzeitig für einen durch eine WMI-Anfrage gesandten SCSI-Befehl geantwortet.)
48	Fehler	Target failed to respond in time to a NOP request. (Das Ziel hat nicht rechtzeitig für eine NOP-Anfrage geantwortet.)
49	Fehler	Target failed to respond in time to a Task Management request. (Das Ziel hat nicht rechtzeitig für eine Task Management-Anfrage geantwortet.)
50	Fehler	Target failed to respond in time to a Text Command sent to renegotiate iSCSI parameters. (Das Ziel hat nicht rechtzeitig auf einen Textbefehl geantwortet, der zur Neuverhandlung von iSCSI-Parametern gesandt wurde.)
51	Fehler	Target failed to respond in time to a logout request sent in response to an asynchronous message from the target. (Das Ziel hat nicht rechtzeitig auf eine Abmeldeanfrage geantwortet, die als Antwort auf eine asynchrone Meldung vom Ziel versandt wurde.)
52	Fehler	Initiator Service failed to respond in time to a request to configure IPsec resources for an iSCSI connection. (Der Initiator-Dienst hat nicht rechtzeitig auf eine Anfrage zur Konfigurierung von IPsec-Ressourcen für eine iSCSI-Verbindung geantwortet.)
53	Fehler	Initiator Service failed to respond in time to a request to release IPsec resources allocated for an iSCSI connection. (Der Initiator-Dienst hat nicht rechtzeitig auf eine Anfrage zur Herausgabe von IPsec-Ressourcen geantwortet, die einer iSCSI-Verbindung zugeordnet sind.)
54	Fehler	Initiator Service failed to respond in time to a request to encrypt or decrypt data. (Der Initiator-Dienst hat nicht rechtzeitig auf eine Anfrage zur Verschlüsselung oder Entschlüsselung von Daten geantwortet.)
55	Fehler	Initiator failed to allocate resources to send data to target. (Der Initiator hat keine Ressourcen zum Versand von Daten ans Ziel zugeordnet.)
56	Fehler	Initiator could not map an user virtual address to kernel virtual address resulting in I/O failure. (Der Initiator konnte der virtuellen Kernadresse keine virtuelle Benutzeradresse zuordnen, was zu einem E/A-Ausfall führte.)

Tabelle 10-5. Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber (OIS-Treiber) (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung
57	Fehler	Initiator could not allocate required resources for processing a request resulting in I/O failure. (Der Initiator konnte die erforderlichen Ressourcen zur Verarbeitung einer Anfrage nicht zuordnen, was zu einem E/A-Ausfall führte.)
58	Fehler	Initiator could not allocate a tag for processing a request resulting in I/O failure. (Der Initiator konnte keine Tag-Nummer zur Verarbeitung einer Anfrage zuordnen, was zu einem E/A-Ausfall führte.)
59	Fehler	Target dropped the connection before the initiator could transition to Full Feature Phase. (Das Ziel verlor die Verbindung, bevor der Initiator in die Full Feature-Phase übergehen konnte.)
60	Fehler	Target sent data in SCSI Response PDU instead of Data_IN PDU. (Das Ziel sandte Daten in die SCSI Response PDU anstatt die Data_IN PDU.) Only Sense Data can be sent in SCSI Response. (Nur Sense-Daten können in die SCSI Response gesandt werden.)
61	Fehler	Target set DataPduInOrder to NO when initiator requested YES. (Das Ziel stellte DataPduInOrder auf NO (NEIN) ein, während der Initiator YES (JA) anforderte.) Login will be failed. (Die Anmeldung wird fehlschlagen.)
62	Fehler	Target set DataSequenceInOrder to NO when initiator requested YES. (Das Ziel stellte DataSequenceInOrder auf NO (NEIN) ein, während der Initiator YES (JA) anforderte.) Login will be failed. (Die Anmeldung wird fehlschlagen.)
63	Fehler	Cannot reset the target or LUN. (Das Ziel oder LUN kann nicht neu eingestellt werden.) Will attempt session recovery. (Es wird versucht, die Sitzung wiederherzustellen.)
64	„Information“ (Informationen)	Attempt to bootstrap Windows using iSCSI NIC Boot (iBF). (Versuch, Bootstrap von Windows mithilfe von iSCSI NIC Boot (iBF) auszuführen.)
65	Fehler	Booting from iSCSI, but could not set any NIC in Paging Path. (Booten von iSCSI aus, aber es konnte keine NIC im Paging-Pfad eingestellt werden.)
66	Fehler	Attempt to disable the Nagle Algorithm for iSCSI connection failed. (Ein Versuch, den Nagle-Algorithmus für die iSCSI-Verbindung zu deaktivieren, ist fehlgeschlagen.)

Tabelle 10-5. Ereignisprotokollmeldungen für den Offload-iSCSI-Treiber (OIS-Treiber) (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung
67	„Information“ (Informationen)	If Digest support selected for iSCSI Session, will use Processor support for Digest computation. (Falls der Digest-Support für die iSCSI-Sitzung ausgewählt wurde, wird Prozessor-Support für die Digest-Berechnung verwendet.)
68	Fehler	After receiving an async logout from the target, attempt to relogin the session failed. (Nach Empfang einer async-Abmeldung vom Ziel ist ein neuer Anmeldeversuch bei der Sitzung fehlgeschlagen.) Error status is specified in the dump data. (Der Fehlerstatus ist in den Speicherabbilddaten angegeben.)
69	Fehler	Attempt to recover an unexpected terminated session failed. (Der Versuch, eine unerwartet abgebrochene Sitzung wiederherzustellen, ist fehlgeschlagen.) Error status is specified in the dump data. (Der Fehlerstatus ist in den Speicherabbilddaten angegeben.)
70	Fehler	Error occurred when processing iSCSI logon request. (Bei der Verarbeitung einer iSCSI-Anmeldeanfrage ist ein Fehler aufgetreten.) The request was not retried. (Die Anfrage wurde nicht erneut versucht.) Error status is specified in the dump data. (Der Fehlerstatus ist in den Speicherabbilddaten angegeben.)
71	„Information“ (Informationen)	Initiator did not start a session recovery upon receiving the request. (Der Initiator startete bei Empfang der Anfrage keine Sitzungswiederherstellung.) Dump data contains the error status. (Die Speicherabbilddaten enthalten den Fehlerstatus.)
72	Fehler	Unexpected target portal IP types. (Unerwartete Zielportal-IP-Arten.) Dump data contains the expected IP type. (Die Speicherabbilddaten enthalten die erwartete IP-Art.)

11 QLogic Teaming Services

Dieses Kapitel beschreibt das Teaming für Adapter in Windows Server-Systemen (ausgenommen Windows Server 2016 und höher). Weitere Informationen zu ähnlichen Technologien bei anderen Betriebssystemen (z. B. Linux Channel Bonding) finden Sie in der Dokumentation zu Ihrem Betriebssystem.

- [Gesamtübersicht](#)
- [„Teaming-Verfahren“ auf Seite 156](#)
- [„Teaming und andere erweiterte Netzwerkeigenschaften“ auf Seite 168](#)
- [„Allgemeine Netzwerkaspekte“ auf Seite 172](#)
- [„Anwendungsaspekte“ auf Seite 181](#)
- [„Behebung von Teaming-Problemen“ auf Seite 190](#)
- [„Häufig gestellte Fragen“ auf Seite 193](#)
- [„Ereignisprotokollmeldungen“ auf Seite 197](#)

Gesamtübersicht

QLogic Teaming-Dienste sind in den folgenden Abschnitten zusammengefasst:

- [Glossar](#)
- [Teaming-Begriffe](#)
- [Softwarekomponenten](#)
- [Hardwareanforderungen](#)
- [Teaming-Unterstützung nach Prozessor](#)
- [Konfigurieren der Teaming-Funktion](#)
- [Unterstützte Funktionen nach Teamart](#)
- [Auswählen einer Teamart](#)

In diesem Abschnitt finden Sie eine Beschreibung der Technologie und Überlegungen zur Implementierung beim Einsatz der Netzwerk-Teaming-Dienste, die über die im Lieferumfang der Server- und Speicherprodukte von Dell enthaltenen QLogic-Software bereitgestellt werden. Das Ziel der QLogic Teaming-Dienste ist es, Fehlertoleranz und Link Aggregation in einem Team aus zwei oder mehr Adaptern zu gewährleisten. Die Informationen in diesem Dokument sollen IT-Experten bei der Bereitstellung von Systemanwendungen unterstützen, die Netzwerkfehlertoleranz und Lastausgleich erfordern, und sie enthalten auch Hinweise für die Problembekämpfung.

Glossar

[Tabelle 11-1](#) definiert die im Teaming verwendete Terminologie.

Tabelle 11-1. Glossar

Begriff	Definition
ARP	Address Resolution Protocol
QCS	QLogic Control Suite
QLASP	QLogic Advanced Server Program (Intermediate-Treiber)
DNS	Domain Name Service
G-ARP	Gratuitous Address Resolution Protocol
Allgemeines Trunking (FEC/GEC)/802,3ad-Draft Static	Switch-abhängige Teamart für Lastausgleich und Failover, bei der der Intermediate-Treiber ausgehenden Datenverkehr und der Switch eingehenden Datenverkehr verwaltet
HSRP	Hot Standby Router Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IPv6	Version 6 des IP
iSCSI	Internet Small Computer Systems Interface
Schicht 2	Netzwerkverkehr, der nicht entlastet wird, und wo die Hardware nur Schicht-2-Vorgänge für den Datenverkehr durchführt. Schicht 3- (IP) und Schicht 4- (TCP) Protokolle werden in der Software verarbeitet.
Schicht 4	Netzwerkverkehr, der stark auf die Hardware entlastet wird, wo ein großer Teil der Verarbeitung auf Schicht 3 (IP) und Schicht 4 (TCP) zur Verbesserung der Leistungsfähigkeit in der Hardware erfolgt.

Tabelle 11-1. Glossar (fortgesetzt)

Begriff	Definition
LACP	Link Aggregation Control Protocol
Link Aggregation (802.3ad)	Switch-abhängige Teamart mit LACP für Lastausgleich und Failover, bei der der Intermediate-Treiber ausgehenden Datenverkehr und der Switch eingehenden Datenverkehr verwaltet
LOM	LAN on Motherboard (LOM)
NDIS	Network Driver Interface Specification
PXE	Umgebung vor der Ausführung
RAID	Redundant Array of Inexpensive Disks
Smart Load Ausgleich und Failover	Switch-unabhängige Teamart für Failover, bei der das primäre Teammitglied sämtlichen eingehenden und ausgehenden Datenverkehr bewältigt, während das Standby-Element inaktiv ist, bis ein Failover-Ereignis (z. B. ein Verbindungsverlust) eintritt. Der Intermediate-Treiber (QLASP) verwaltet eingehenden und ausgehenden Datenverkehr.
Smart Load Balancing (Intelligenter Lastausgleich, SLB)	Switch-unabhängige Teamart für Lastausgleich und Failover, bei der der Intermediate-Treiber ausgehenden/eingehenden Verkehr verwaltet.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WINS	Windows Internet Name Service

Teaming-Begriffe

Das Konzept der Gruppierung mehrerer physischer Geräte zur Gewährleistung von Fehlertoleranz und Lastausgleich ist nicht neu. Es wurde bereits vor mehreren Jahren entwickelt. Speichergeräte verwenden RAID-Technologie zum Zusammenfassen individueller Festplatten. Switch-Ports können mithilfe von Technologien wie Cisco Gigabit EtherChannel, IEEE 802.3ad Link Aggregation, Bay Networks Multilink Trunking und Extreme Network Load Sharing zusammengefasst werden. Netzwerkschnittstellen auf Dell-Servern können in einem Team aus physischen Ports zusammengefasst werden, das als virtueller Adapter bezeichnet wird.

Dieser Abschnitt enthält folgende Informationen zu Teaming-Begriffen:

- [Netzwerkadressierung](#)
- [Teaming und Netzwerkadressen](#)
- [Beschreibung der Teaming-Arten](#)

Netzwerkadressierung

Zum besseren Verständnis der Teaming-Funktion ist es wichtig nachzuvollziehen, wie die Kommunikation zwischen Knoten in einem Ethernet-Netzwerk funktioniert. In diesem Dokument wird davon ausgegangen, dass der Leser mit den Grundlagen der Kommunikation in IP- und Ethernet-Netzwerken vertraut ist.

Die folgenden Informationen geben einen allgemeinen Überblick über die Grundbegriffe der Netzwerkadressierung in einem Ethernet-Netzwerk. Jede Ethernet-Netzwerkschnittstelle in einer Host-Plattform wie einem Computersystem benötigt eine global eindeutige Schicht-2-Adresse und mindestens eine global eindeutige Schicht-3-Adresse. Schicht 2 ist die Verbindungsebene, und Schicht 3 ist die Netzwerkebene, wie im OSI-Modell definiert. Die Schicht-2-Adresse wird der Hardware zugewiesen und häufig als MAC-Adresse oder physische Adresse bezeichnet. Diese Adresse wird werkseitig vorprogrammiert und in ein NVRAM (Non-Volatile RAM) auf einer Netzwerkkarte oder dem Mainboard des Systems für eine eingebettete LAN-Schnittstelle gespeichert. Die Schicht-3-Adressen werden als Protokolladressen oder logische Adressen bezeichnet, die dem Software-Stack zugewiesen werden. IP und IPX sind Beispiele für Schicht-3-Protokolle. Außerdem verwendet Schicht 4 (die Transportschicht) Portnummern für jedes höhere Kommunikationsprotokoll wie Telnet oder FTP. Diese Portnummern dienen zur Differenzierung des Verkehrsflusses über mehrere Anwendungen hinweg. Schicht-4-Protokolle wie TCP oder UDP werden in den heutigen Netzwerken am häufigsten verwendet. Die Kombination aus IP-Adresse und TCP-Portnummer wird als Socket bezeichnet.

Ethernet-Geräte kommunizieren mit anderen Ethernet-Geräten nicht über die IP-Adresse, sondern über die MAC-Adresse. Die meisten Anwendungen arbeiten jedoch mit einem Host-Namen, der mittels Namensauflösung, z. B. mit Windows Internet Name Service (WINS) oder DNS, in eine IP-Adresse übersetzt wird. Daher ist ein Verfahren zur Identifizierung der MAC-Adresse, die der IP-Adresse zugewiesen wurde, erforderlich. Das Address Resolution Protocol für ein IP-Netzwerk bietet ein solches Verfahren. Bei IPX ist die MAC-Adresse Teil der Netzwerkadresse; hier ist ARP nicht erforderlich. ARP wird mithilfe einer ARP-Anforderung und eines Frame für die ARP-Antwort implementiert. ARP-Anforderungen werden üblicherweise an eine Broadcast-Adresse gesendet, während die ARP-Antwort normalerweise als Unicast-Verkehr übermittelt wird. Eine Unicast-Adresse entspricht einer einzelnen MAC- oder IP-Adresse. Eine Broadcast-Adresse wird an alle Geräte in einem Netzwerk gesendet.

Teaming und Netzwerkadressen

Ein Team von Adaptern funktioniert wie eine einzelne virtuelle Netzwerkschnittstelle und wird von anderen Netzwerkgeräten genauso betrachtet wie ein Adapter, der nicht Bestandteil eines Teams ist. Ein virtueller Netzwerkadapter kündigt eine einzelne Schicht-2- und eine oder mehrere Schicht-3-Adressen an. Wenn der Teaming-Treiber initialisiert wird, wählt er eine MAC-Adresse von einem der physischen Adapter im Team aus, die als MAC-Adresse des Teams fungieren soll. Diese Adresse stammt normalerweise vom ersten Adapter, der vom Treiber initialisiert wird. Wenn das System, das als Host für das Team fungiert, eine ARP-Anforderung empfängt, wählt es eine MAC-Adresse unter den physischen Adaptern im Team aus, die als die Quell-MAC-Adresse in der ARP-Antwort verwendet werden soll. In Windows-Betriebssystemen zeigt der Befehl `IPCONFIG /all` die IP- und MAC-Adresse des virtuellen Adapters, nicht die des individuellen physischen Adapters. Die Protokoll-IP-Adresse ist der virtuellen Netzwerkschnittstelle zugewiesen, nicht den individuellen physischen Adaptern.

Bei Switch-unabhängigen Teaming-Modi müssen alle physischen Adapter, die einen virtuellen Adapter bilden, die eindeutige MAC-Adresse verwenden, die ihnen bei der Datenübertragung zugewiesen wird. Das heißt, die Rahmen, die von jedem der physischen Adapter im Team gesendet werden, müssen eine eindeutige MAC-Adresse verwenden, um IEEE-kompatibel zu sein. Beachten Sie, dass ARP-Cache-Einträge nicht aus empfangenen Rahmen entnommen werden, sondern ausschließlich aus ARP-Anforderungen und ARP-Antworten.

Beschreibung der Teaming-Arten

In diesem Abschnitt werden die folgenden Teaming-Arten beschrieben:

- [Smart Load Balancing und Failover](#)
- [Allgemeines Trunking](#)
- [Link Aggregation \(IEEE 802.3ad LACP\)](#)
- [SLB \(Auto-Fallback deaktiviert\)](#)

Die drei Verfahren zur Klassifizierung von unterstützten Teaming-Arten hängen von Folgendem ab:

- ob die Konfiguration des Switch-Ports der Adapter-Teaming-Art entsprechen muss.
- der Funktion des Teams, also davon, ob das Team Lastausgleich und Failover oder nur Failover unterstützt.
- ob das Link Aggregation Control Protocol (LCAP) verwendet wird oder nicht.

Tabelle 11-2 zeigt eine Übersicht der Teaming-Arten und ihrer Klassifizierung.

Tabelle 11-2. Verfügbare Teaming-Arten

Teaming-Art	Switch-abhängig ^a	Unterstützung für LACP ist auf dem Switch erforderlich	Lastausgleich	Failover
„Smart Load Balance“ und „Failover“ (mit zwei bis acht Lastausgleich-Teammitgliedern)			✓	✓
SLB (Auto-Fallback deaktiviert)			✓	✓
Link Aggregation (802.3ad)	✓	✓	✓	✓
Allgemeines Trunking (FEC/GEC)/802,3ad-Draft Static	✓		✓	✓

^a Switch muss bestimmte Teamart unterstützen.

Smart Load Balancing und Failover

Die Teamart Smart Load Balancing und Failover ermöglicht bei Konfiguration für den Lastausgleich sowohl Lastausgleich als auch Ausfallsicherung, bei Konfiguration für die Fehlertoleranz dagegen nur Ausfallsicherung. Diese Teamart funktioniert mit jedem Ethernet-Switch und erfordert keine Konfiguration für Trunking auf dem Switch. Das Team kündigt mehrere MAC-Adressen und eine oder mehrere IP-Adressen an (bei Verwendung von sekundären IP-Adressen). Die MAC-Adresse des Teams wird aus der Liste der Lastausgleichsmitglieder ausgewählt. Empfängt das System eine ARP-Anforderung, sendet der Software-Netzwerkstapel stets eine ARP-Antwort mit der MAC-Adresse des Teams. Um den Lastausgleich zu starten, modifiziert der Teaming-Treiber diese ARP-Antwort, indem er die Quell-MAC-Adresse so ändert, dass sie einem der physischen Adapter entspricht.

Smart Load Balancing ermöglicht Lastausgleich beim Senden (Transmit Load Balancing, TLB) und Empfangen (Receive Load Balancing, RLB) auf Basis der Schicht-3- und Schicht-4-IP-Adressen und der TCP/UDP-Portnummer. Mit anderen Worten: Der Lastausgleich erfolgt nicht auf Byte- oder Rahmenebene, sondern auf Basis der TCP/UDP-Sitzung. Durch dieses Verfahren wird die Übermittlung von Rahmen, die zur selben Socket-Konversation gehören, in der korrekten Reihenfolge gewährleistet. Lastausgleich wird an zwei bis acht Ports unterstützt. Dies gilt auch für Ports in einer beliebigen Kombination aus zusätzlichen Adaptern und LOM-Geräten (LAN on Motherboard).

TLB wird durch Erstellen einer Hash-Tabelle mit den Quell- und Ziel-IP-Adressen sowie TCP/UDP-Portnummern herbeigeführt. Die gleiche Kombination aus Quell- und Ziel-IP-Adressen sowie TCP/UDP-Portnummern ergibt im Allgemeinen denselben Hash-Index und verweist daher auf denselben Port im Team. Bei Auswahl eines Ports für den Transport aller Rahmen eines bestimmten Sockets wird die eindeutige MAC-Adresse des physischen Adapters in den Rahmen einbezogen, nicht die MAC-Adresse des Teams. Diese Einbeziehung ist zur Einhaltung des IEEE-Standards 802.3 erforderlich. Wenn zwei Adapter bei der Übertragung dieselbe MAC-Adresse verwenden, würde dies zu einer doppelten MAC-Adresse führen – eine Situation, die der Switch nicht bewältigen kann.

ANMERKUNG

SLB führt einen Lastausgleich für IPv6-adressierten Datenverkehr durch, da ARP keine IPv6-Funktion ist.

Der Lastausgleich beim Empfangen (Receive Load Balancing) erfolgt durch einen Intermediate-Treiber, der unangeforderte ARPs (G-ARPs) von Client zu Client sendet und dabei die Unicast-Adresse der einzelnen Clients als Zieladresse der ARP-Anforderung verwendet (auch als gerichtetes ARP bezeichnet). Dieser Vorgang wird nicht als Ausgleich der Traffic Load Balancing (Datenverkehrslast), sondern als Client Load Balancing (Client-Lastausgleich) betrachtet. Wenn der Intermediate-Treiber ein erhebliches Lastungleichgewicht zwischen den physischen Adaptern in einem SLB-Team erkennt, generiert er G-ARPs, um damit eingehende Rahmen umzuverteilen. Der Intermediate-Treiber (QLASP) beantwortet keine ARP-Anforderungen; nur der Protokollstapel der Software liefert die erforderliche ARP-Antwort. Der Lastausgleich beim Empfangen ist eine Funktion der Anzahl der Clients, die über die Team-Schnittstelle eine Verbindung zum System herstellen.

Beim Lastausgleich beim Empfangen mit SLB wird versucht, eingehenden Datenverkehr für Client-Geräte über physische Ports im Team auszugleichen. Mit einem veränderten unangeforderten ARP wird eine andere MAC-Adresse für die IP-Adresse des Teams in der physischen und der Protokolladresse des Absenders angekündigt. Das G-ARP wird als Unicast mit der MAC- und IP-Adresse eines Client-Geräts in der physischen Zieladresse bzw. der Ziel-Protokolladresse gesendet. Der Ziel-Client aktualisiert daraufhin seinen ARP-Cache mit der neuen MAC-Adresse, die der IP-Adresse des Teams zugeordnet wird. G-ARPs werden nicht als Broadcasts gesendet, da sonst alle Clients ihren Datenverkehr an denselben Port senden würden. Dadurch würden die Vorteile des Client-Lastausgleichs aufgehoben, und es könnte zu einer Rahmenübermittlung in ungeordneter Reihenfolge kommen. Dieses Schema für den Lastausgleich beim Empfangen funktioniert, solange alle Clients und das Team-System sich im selben Subnetz oder derselben Broadcast-Domäne befinden.

Wenn sich die Clients und das System in verschiedenen Subnetzen befinden und eingehender Datenverkehr einen Router durchlaufen muss, wird der empfangene, für das System bestimmte Datenverkehr keinem Lastausgleich unterzogen. Der physische Adapter, der vom Intermediate-Treiber für den Transport des IP-Flusses ausgewählt wurde, befördert den gesamten Datenverkehr. Wenn der Router einen Rahmen an die IP-Adresse des Teams sendet, überträgt er eine ARP-Anforderung (falls nicht im ARP-Cache vorhanden). Der Server-Softwarestack generiert eine ARP-Antwort mit der MAC-Adresse des Teams, diese wird jedoch vom Intermediate-Treiber modifiziert und über einen bestimmten physischen Adapter gesendet; damit wird der Fluss für diese Sitzung hergestellt.

Dies liegt daran, dass ARP kein routbares Protokoll ist. Es verfügt nicht über eine IP-Kopfzeile, und daher wird es nicht an den Router oder an das Standard-Gateway gesendet. ARP ist lediglich ein lokales Subnetzprotokoll. Da es sich bei G-ARP nicht um ein Broadcast-Paket handelt, wird es vom Router nicht verarbeitet, und der Router aktualisiert sein ARP-Cache nicht.

Der Router würde ein ARP, das für ein anderes Netzwerkgerät bestimmt ist, nur dann verarbeiten, wenn Proxy-ARP aktiviert wäre und der Host keinen Standard-Gateway hätte. Dieser Fall tritt äußerst selten ein und wird für die meisten Anwendungen nicht empfohlen.

Über einen Router gesendeter Verkehr wird ausgeglichen, da der Lastausgleich beim Senden auf der Quell- und Ziel-IP-Adresse sowie der TCP/UDP-Portnummer basiert. Da Router die Quell- und Ziel-IP-Adresse nicht verändern, funktioniert der Lastausgleichsalgorithmus wie vorgesehen.

Durch Konfigurieren von Routern für das Hot Standby Routing Protocol (HSRP) kann im Adapter-Team kein Lastausgleich beim Empfangen ausgeführt werden. Im Allgemeinen ermöglicht es HSRP, dass zwei Router als ein Router fungieren, der eine virtuelle IP- und eine virtuelle MAC-Adresse ankündigt. Ein physischer Router ist die aktive Schnittstelle, während der andere als Standby-Router dient. Obwohl durch HSRP auch die Last von Knoten (über verschiedene Standard-Gateways auf den Host-Knoten) über mehrere Router in HSRP-Gruppen aufgeteilt werden kann, verweist es stets auf die primäre MAC-Adresse des Teams.

Allgemeines Trunking

„Allgemeines Trunking“ ist ein Switch-unterstützter Teaming-Modus, bei dem die Ports an beiden Enden einer Verbindung konfiguriert werden müssen: die Serverschnittstellen und die Switch-Ports. Diese Port-Konfiguration wird häufig als Cisco Fast EtherChannel oder Gigabit EtherChannel bezeichnet. Allgemeines Trunking unterstützt darüber hinaus ähnliche Implementierungen durch andere Switch-OEMs wie Extreme Networks Load Sharing und Bay Networks oder IEEE 802.3ad Link Aggregation im statischen Modus. In diesem Modus kündigt das Team eine MAC-Adresse und eine IP-Adresse an, wenn der Protokollstapel auf die ARP-Anforderungen antwortet. Des Weiteren verwendet jeder physische Adapter im Team bei der Übertragung von Rahmen dieselbe Team-MAC-Adresse. Die Verwendung der Adresse ist möglich, da der Switch am anderen Ende der Verbindung den Teaming-Modus kennt und die Verwendung einer einzigen MAC-Adresse durch jeden Port im Team gewährleistet. In der Weiterleitungstabelle im Switch wird der Trunk als ein einziger virtueller Port aufgeführt.

Bei diesem Teaming-Modus steuert der Intermediate-Treiber Lastausgleich und Failover nur für ausgehenden Datenverkehr, während eingehender Verkehr von der Switch-Firmware und -Hardware gesteuert wird. Wie beim Smart Load Balancing verwendet der QLASP-Intermediate-Treiber die IP/TCP- und UDP-Quelladressen und -Zieladressen, um den vom Server gesendeten Datenverkehr auszugleichen. Die meisten Switches implementieren XOR-Hashing der Quell- und Ziel-MAC-Adresse.

ANMERKUNG

Allgemeines Trunking wird von iSCSI-Offload-Adaptoren nicht unterstützt.

Link Aggregation (IEEE 802.3ad LACP)

Link Aggregation funktioniert ähnlich wie Allgemeines Trunking, außer dass das Link Aggregation Control Protocol (LACP) für das Aushandeln der Ports verwendet wird, aus denen sich das Team zusammensetzt. An beiden Enden der Verbindung muss LACP aktiviert sein, andernfalls ist das Team nicht funktionsfähig. Ist LACP nicht an beiden Enden der Verbindung verfügbar, bietet 802.3ad eine manuelle Bündelung. Hierfür ist es lediglich erforderlich, dass beide Enden verbunden sind. Da bei manueller Bündelung die Aktivierung einer Mitgliedsverbindung ohne den LACP-Austausch vollzogen wird, ist eine solche Verbindung weniger verlässlich und robust als eine durch LACP ausgehandelte Verbindung. LACP bestimmt automatisch, welche Mitgliedsverbindungen gebündelt werden können, und führt die Bündelung dann aus. Es gewährleistet das geregelte Hinzufügen und Entfernen von physischen Verbindungen für die Link Aggregation, so dass keine Rahmen verloren gehen oder dupliziert werden. Gebündelte Verbindungsmitglieder werden durch das Marker-Protokoll entfernt, das wahlweise für Verbindungen mit Aggregation Control Protocol (LACP) aktiviert werden kann.

Die Link Aggregation-Gruppe kündigt eine einzelne MAC-Adresse für alle Ports im Trunk an. Die MAC-Adresse des Aggregators kann die MAC-Adresse eines der MACs sein, aus denen die Gruppe besteht. LACP und Marker-Protokolle verwenden eine Multicast-Zieladresse.

Die Link Aggregation-Steuerungsfunktion bestimmt, welche Verbindungen gebündelt werden können, bindet dann die Ports an eine Bündelungsfunktion im System und überwacht den Zustand, um zu bestimmen, ob eine Änderung in der Aggregation-Gruppe erforderlich ist. Bei der Link Aggregation werden die Leistungen einzelner Verbindungen in einer hochleistungsfähigen virtuellen Verbindung kombiniert. Der Ausfall oder Ersatz einer Verbindung in einem LACP-Trunk hat keinen Verbindungsverlust zur Folge. Der Datenverkehr wird dank Failover einfach von den übrigen Verbindungen im Trunk übernommen.

SLB (Auto-Fallback deaktiviert)

Diese Teamart ist mit der Teamart „Smart Load Balance“ und „Failover“ bis auf eine Ausnahme identisch: Wenn das Standby-Element aktiv ist und ein primäres Mitglied die Verbindung wiederhergestellt hat, verwendet das Team weiterhin das Standby-Element, anstatt wieder auf das primäre Mitglied umzuschalten. Diese Teamart wird nur verwendet, wenn das Netzkabel getrennt und wieder mit dem Netzwerkadapter verbunden wurde. Sie wird nicht unterstützt, wenn der Adapter mithilfe des Geräte-Managers oder über Hot-Plug PCI entfernt bzw. installiert wird.

Wird ein primärer Adapter, der einem Team zugewiesen ist, deaktiviert, fungiert das Team als ein Team der Art „Smart Load Balancing“ und „Failover“, in dem Auto-Fallback auftritt.

Softwarekomponenten

Teaming wird im Windows-Betriebssystem über einen NDIS Intermediate-Treiber implementiert. Diese Softwarekomponente wirkt mit dem Miniport-Treiber, der NDIS-Schicht und dem Protokollstapel zusammen und ermöglicht so die Teaming-Architektur (siehe [Abbildung 11-2 auf Seite 157](#)). Der Miniport-Treiber steuert den Host-LAN-Controller direkt und ermöglicht so Funktionen wie Senden, Empfangen und Unterbrechen der Verarbeitung. Der Intermediate-Treiber befindet sich zwischen Miniport-Treiber und Protokollschicht, ermöglicht das Multiplexing mehrerer Miniport-Treiberinstanzen und erstellt einen virtuellen Adapter, der von der NDIS-Schicht als einzelner Adapter wahrgenommen wird. NDIS bietet eine Reihe von Bibliotheksfunktionen und ermöglicht so die Kommunikation zwischen Miniport-Treibern oder zwischen Intermediate-Treibern und dem Protokollstapel. Der Protokollstapel implementiert IP, IPX und ARP. Jeder Miniport-Geräteinstanz wird eine Protokolladresse (z. B. eine IP-Adresse) zugewiesen. Ist jedoch ein Intermediate-Treiber installiert, wird die Protokolladresse dem virtuellen Team-Adapter zugewiesen, und nicht den individuellen Miniport-Geräten, aus denen das Team besteht.

Der von QLogic bereitgestellte Teaming-Support wird durch drei individuelle Softwarekomponenten gewährleistet, die gemeinsam arbeiten und als Paket unterstützt werden. Wird eine Komponente aktualisiert, müssen auch alle anderen Komponenten auf die unterstützten Versionen aktualisiert werden.

[Tabelle 11-3](#) beschreibt die vier Softwarekomponenten und die dazugehörigen Dateien für die unterstützten Betriebssysteme.

Tabelle 11-3. QLogic Teaming-Softwarekomponente

Softwarekomponente	QLogic Name	Netzwerkadapter oder Betriebssystem	Systemarchitektur	Windows-Dateiname
–	Virtueller Bustreiber (VBD)	BCM57xx	32-Bit	bxvbdx.sys
		BCM57xx	64-Bit	bxvbda.sys
		BCM5771x, BCM578xx	32-Bit	evbdx.sys
		BCM5771x, BCM578xx	64-Bit	evbda.sys
Miniport-Treiber	QLogic Basistreiber	Windows Server 2008 (NDIS 6.0)	32-Bit	bxnd60x.sys
		Windows Server 2008 (NDIS 6.0)	64-Bit	bxnd60a.sys
		Windows Server 2008 R2 (NDIS 6.0)	64-Bit	bxnd60a.sys
		Windows Server 2012, 2012 R2	64-Bit	bxnd60a.sys

Tabelle 11-3. QLogic Teaming-Softwarekomponente (fortgesetzt)

Softwarekomponente	QLogic Name	Netzwerkadapter oder Betriebssystem	Systemarchitektur	Windows-Dateiname
Intermediate-Treiber	QLASP	Windows Server 2008	32-Bit und 64-Bit	qlasp.sys
		Windows Server 2008 R2	64-Bit	qlasp.sys
		Windows Server 2012, 2012 R2	64-Bit	qlasp.sys
Konfigurationsbenutzer-schnittstelle	QLogic Control Suite (QCS)	Windows Server 2008	–	qcs.exe
		Windows Server 2008 R2	–	qcs.exe
		Windows Server 2012, 2012 R2	–	qcs.exe

Hardwareanforderungen

Die Hardwareanforderungen für das Teaming umfassen Folgendes:

- [Repeater-Hub](#)
- [Switching-Hub](#)
- [Router](#)

Durch die verschiedenen in diesem Dokument beschriebenen Teaming-Modi gelten für die Netzwerkgeräte, die zur Verbindung von Clients mit Team-Systemen verwendet werden, gewisse Einschränkungen. Jede Art von Netzwerkverbindungstechnologie hat Auswirkungen auf das Teaming, die in den folgenden Abschnitten beschrieben werden.

Repeater-Hub

Ein Repeater-Hub ermöglicht es dem Netzwerkadministrator, ein Ethernet-Netzwerk über die Grenzen eines einzelnen Segments hinaus auszuweiten. Der Repeater regeneriert das Eingangssignal, das an einem Port empfangen wird, an allen anderen verbundenen Ports und bildet so eine Kollisionsdomäne. Diese Domäne bedeutet, dass wenn eine an einen Repeater angeschlossene Station einen Ethernet-Rahmen an eine andere Station sendet, auch alle anderen Stationen innerhalb derselben Kollisionsdomäne diese Nachricht empfangen. Wenn zwei Stationen gleichzeitig mit der Übertragung beginnen, kommt es zu einer Kollision, und jede übertragende Station muss ihre Daten nach einer willkürlich festgelegten Wartezeit erneut senden.

Bei Verwendung eines Repeaters muss jede Station innerhalb der Kollisionsdomäne im Halbduplex-Modus betrieben werden. Der Halbduplex-Modus wird zwar für Gigabit Ethernet (GbE)-Adapter nach dem IEEE 802.3-Standard unterstützt, nicht jedoch von der Mehrheit der Hersteller von GbE-Adaptern. Daher wird der Halbduplex-Modus hier außer Acht gelassen.

Teaming über mehrere Hubs wird ausschließlich für SLB-Teams zu Problemlösungszwecken (z. B. Anschluss eines Netzwerkanalysators) unterstützt.

Switching-Hub

Anders als bei einem Repeater-Hub ist es mit einem Switching-Hub (oder einfacher einem Switch) möglich, ein Ethernet in mehrere Kollisionsdomänen zu unterteilen. Der Switch ist für die Weiterleitung von Ethernet-Paketen zwischen Hosts allein auf der Grundlage von Ethernet MAC-Adressen verantwortlich. Ein physischer Netzwerkadapter, der mit einem Switch verbunden ist, kann im Halbduplex- oder Vollduplex-Modus betrieben werden.

Für die Unterstützung von Allgemeinem Trunking und 802.3ad Link Aggregation muss ein Switch speziell diese Funktion unterstützen. Sollte der Switch diese Protokolle nicht unterstützen, kann er immer noch für Smart Load Balancing verwendet werden.

ANMERKUNG

Alle Netzwerk-Teaming-Modi werden über Switches hinweg unterstützt, wenn diese als stapelbare Switches betrieben werden.

Router

Ein Router dient zur Weiterleitung von Netzwerkverkehr auf der Basis von Schicht-3-Protokollen (oder höher), arbeitet jedoch häufig auch als Schicht-2-Gerät mit Switching-Funktion. Das Teaming von direkt mit einem Router verbundenen Ports wird nicht unterstützt.

Teaming-Unterstützung nach Prozessor

Alle Teamarten werden von den Prozessoren IA-32 und EM64T unterstützt.

Konfigurieren der Teaming-Funktion

Das Dienstprogramm QLogic Control Suite (QCS) wird für die Teaming-Konfiguration in den unterstützten Betriebssystemen verwendet.

QCS ist für 32-Bit- und 64-Bit-Windows-Betriebssysteme ausgelegt. Verwenden Sie QCS, um VLANs und Lastausgleich und Fehlertoleranz-Teaming zu konfigurieren. Daneben werden auch die MAC-Adresse, die Treiberversion und Statusinformationen über die einzelnen Netzwerkkadapters angezeigt. QCS umfasst außerdem eine Reihe von Diagnose-Tools, z. B. für Hardware-Diagnose, einen Kabeltest und einen Netzwerktopologietest.

Unterstützte Funktionen nach Teamart

[Tabelle 11-4](#) bietet einen Vergleich der Funktionen der verschiedenen Teamarten, die von Dell unterstützt werden. Anhand dieser Tabelle können Sie bestimmen, welche Teamart am besten für Ihre Anwendung geeignet ist. Die Teaming-Software unterstützt maximal acht Ports in einem Team und bis zu 16 Teams in einem System. In diesen Teams können die unterstützten Teamarten beliebig kombiniert werden, allerdings muss sich jedes Team in einem separaten Netzwerk oder Subnetz befinden.

Tabelle 11-4. Vergleich der Teamarten

Teamart	Fehlertoleranz	Lastausgleich	Switch-abhängiges Static Trunking	Switch-unabhängig Dynamic Link Aggregation (IEEE 802.3ad)
Funktion	SLB mit Standby ^a	SLB	Allgemeines Trunking	Link Aggregation
Anzahl an Ports pro Team (gleiche Broadcast-Domäne)	2-16	2-16	2-16	2-16
Anzahl der Teams	16	16	16	16
Adapter-Fehlertoleranz	Ja	Ja	Ja	Ja
Fehlertoleranz bei Switch-Verbindung (gleiche Broadcast-Domäne)	Ja	Ja	Switch-abhängig	Switch-abhängig
TX-Lastausgleich	Nein	Ja	Ja	Ja
RX-Lastausgleich	Nein	Ja	Ja (vom Switch ausgeführt)	Ja (vom Switch ausgeführt)

Tabelle 11-4. Vergleich der Teamarten (fortgesetzt)

Teamart	Fehler-toleranz	Lastaus-gleich	Switch-abhängiges Static Trunking	Switch-unabhängig Dynamic Link Aggregation (IEEE 802.3ad)
Funktion	SLB mit Standby ^a	SLB	Allgemeines Trunking	Link Aggregation
Erfordert kompatiblen Switch	Nein	Nein	Ja	Ja
Heartbeats zum Testen der Konnektivität	Nein	Nein	Nein	Nein
Gemischte Medien (Adapter mit verschiedenen Medien)	Ja	Ja	Ja (Switch-abhängig)	Ja
Verschiedene Raten (Adapter, die keine gemeinsame Übertragungsrate unterstützen, sondern bei verschiedenen Raten betrieben werden können)	Ja	Ja	Nein	Nein
Verschiedene Raten (Adapter, die eine gemeinsame Übertragungsrate unterstützen, jedoch bei verschiedenen Raten betrieben werden können)	Ja	Ja	Nein (Raten müssen identisch sein)	Ja
Lastausgleich TCP/IP	Nein	Ja	Ja	Ja
Teaming mit Geräten verschiedener Hersteller	Ja ^b	Ja ^b	Ja ^b	Ja ^b
Lastausgleich für Nicht-IP-Verkehr	Nein	Ja (nur ausgehender IPX-Verkehr)	Ja	Ja

Tabelle 11-4. Vergleich der Teamarten (fortgesetzt)

Teamart	Fehler-toleranz	Lastaus-gleich	Switch-abhängiges Static Trunking	Switch-unabhängig Dynamic Link Aggregation (IEEE 802.3ad)
Funktion	SLB mit Standby ^a	SLB	Allgemeines Trunking	Link Aggregation
Gleiche MAC-Adresse für alle Teammitglieder	Nein	Nein	Ja	Ja
Gleiche IP-Adresse für alle Teammitglieder	Ja	Ja	Ja	Ja
Lastausgleich nach IP-Adresse	Nein	Ja	Ja	Ja
Lastausgleich nach MAC-Adresse	Nein	Ja (verwendet für Nicht-IP-/IPX-Verkehr)	Ja	Ja

^a SLB mit einem primären und einem Standby-Element.

^b Es muss mindestens ein QLogic-Adapter im Team vorhanden sein.

Auswählen einer Teamart

Das folgende Flussdiagramm zeigt den Entscheidungsprozess bei der Planung des Schicht-2-Teamings. Das wichtigste Argument für Teaming ist der Bedarf an zusätzlicher Netzwerkbandbreite und Fehlertoleranz. Teaming bietet Link Aggregation und Fehlertoleranz und erfüllt damit beide Kriterien.

Präferenz-Teaming sollte in der folgenden Reihenfolge ausgewählt werden:

- Erste Wahl: Link Aggregation
- Zweite Wahl: Allgemeines Trunking
- Dritte Wahl: SLB, bei Verwendung von Switches, die die beiden ersten Optionen nicht unterstützen, oder wenn nicht verwaltete Switches verwendet werden. Sollte Switch-Fehlertoleranz erforderlich sein, ist SLB die einzige Möglichkeit.

Abbildung 11-1 zeigt ein Flussdiagramm zur Bestimmung der Teamart.

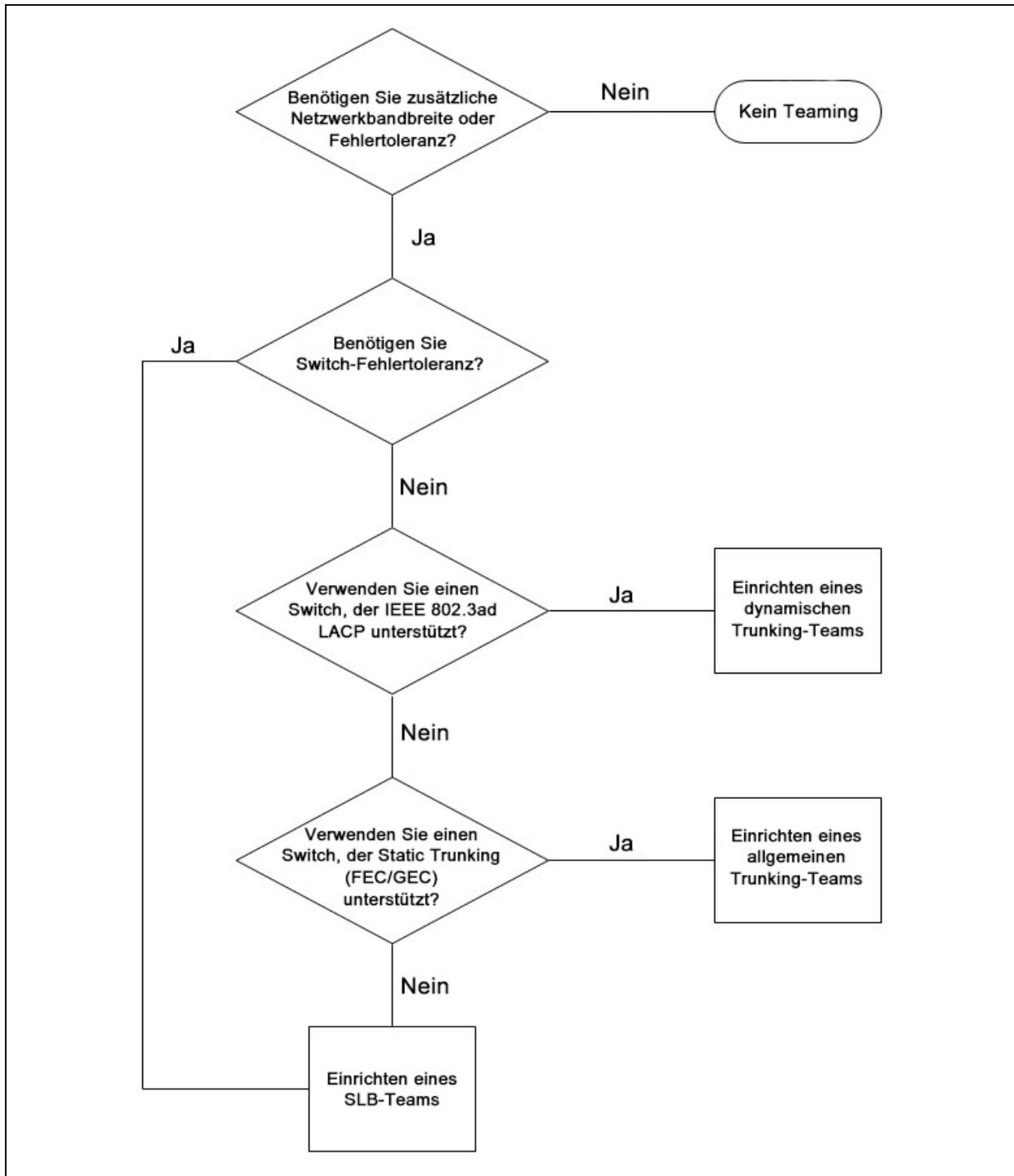


Abbildung 11-1. Auswahl einer Teamart

Teaming-Verfahren

Dieser Abschnitt enthält folgende Informationen zu Teaming-Verfahren:

- [Architektur](#)
- [Teamarten](#)
- [Attribute der mit jeder Teamart verbundenen Leistungsmerkmale](#)
- [Für jede Teamart unterstützte Übertragungsraten](#)

Architektur

QLASP ist als NDIS Intermediate-Treiber implementiert (siehe [Abbildung 11-2](#)). Es wird unterhalb von Protokollstapeln wie TCP/IP und IPX betrieben und als virtueller Adapter angezeigt. Dieser virtuelle Adapter übernimmt die MAC-Adresse des ersten im Team initialisierten Ports. Für den virtuellen Adapter muss außerdem eine Schicht-3-Adresse konfiguriert werden. Die Hauptfunktion von QLASP besteht im Ausgleich des eingehenden (für SLB) und ausgehenden (für alle Teaming-Modi) Verkehrs zwischen den im System installierten physischen Adapters, die für Teaming ausgewählt wurden. Die Algorithmen für eingehenden und ausgehenden Verkehr sind voneinander unabhängig und operieren orthogonal zueinander. Der ausgehende Verkehr und der entsprechende eingehende Verkehr für eine bestimmte Sitzung können verschiedenen Ports zugewiesen werden.

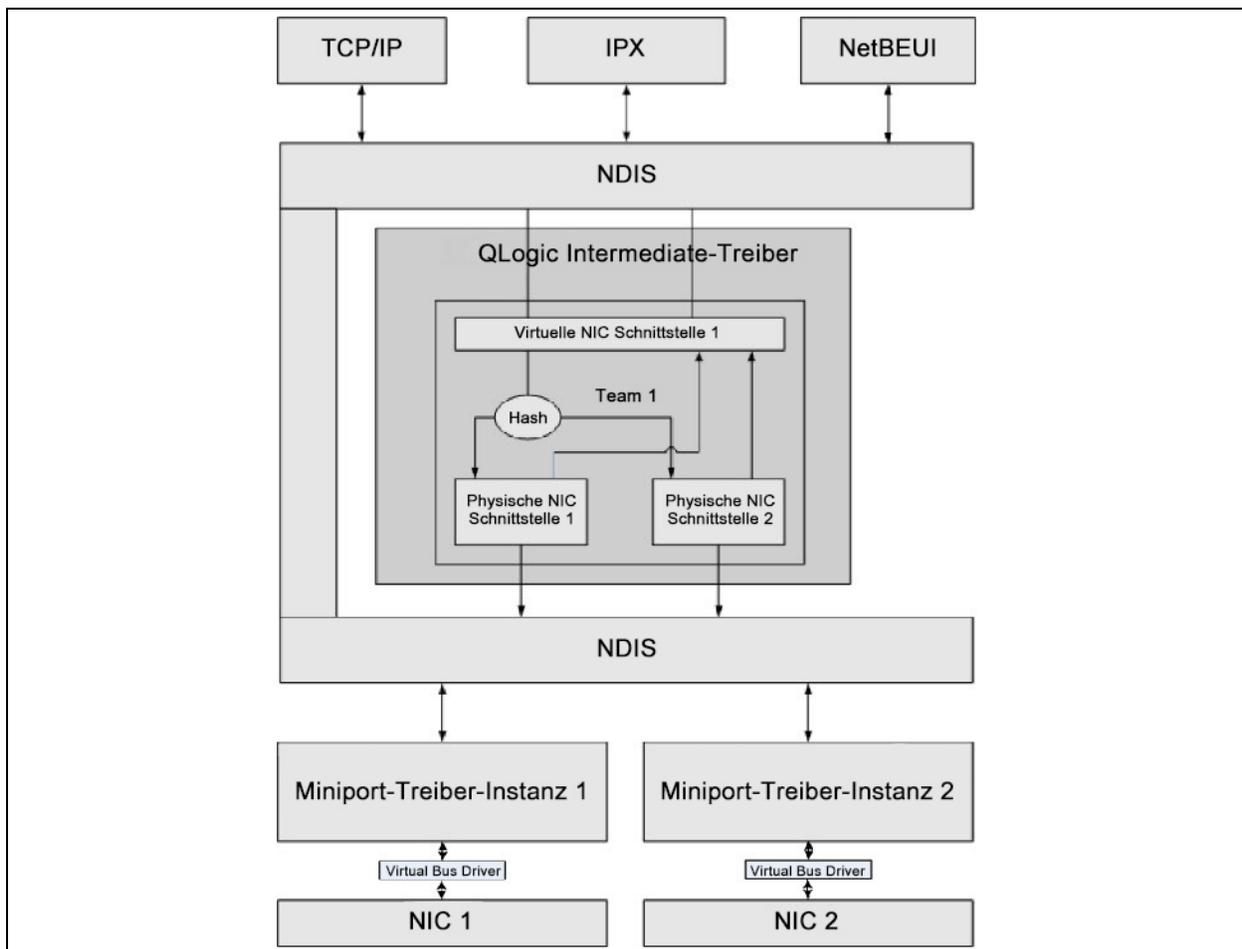


Abbildung 11-2. Intermediate-Treiber

Ausgehender Verkehr

Der QLogic Intermediate-Treiber verwaltet den ausgehenden Verkehrsfluss für alle Teaming-Modi. Für den ausgehenden Verkehr wird jedes Paket zunächst einem Fluss zugeteilt und dann an die ausgewählten physischen Adapter zur Übertragung verteilt. Die Zuteilung zu einem Fluss erfolgt mittels einer effizienten Hash-Berechnung anhand bekannter Protokollfelder. Der daraus resultierende Hash-Wert wird verwendet, um eine Outbound-Flow-Hash-Tabelle zu indizieren. Der ausgewählte Outbound-Flow-Hash-Eintrag enthält den Index des ausgewählten physischen Adapters, der für die Übertragung dieses Flusses zuständig ist. Die Quell-MAC-Adresse der Pakete wird dann in die MAC-Adresse des ausgewählten physischen Adapters geändert. Das modifizierte Paket wird anschließend an den ausgewählten physischen Adapter zur Übertragung weitergegeben.

Die ausgehenden TCP- und UDP-Pakete werden mithilfe der Kopfzeileninformationen aus Schicht 3 und Schicht 4 klassifiziert. Dieses Schema verbessert die Lastverteilung für häufig verwendete Internet-Protokoll-Dienste, die mit bekannten Ports wie HTTP und FTP arbeiten. Daher sorgt QLASP für Lastausgleich auf Basis einer TCP-Sitzung, nicht auf Paket-Basis.

In den Outbound Flow Hash-Einträgen werden außerdem Statistikkähler nach der Klassifizierung aktualisiert. Das Lastausgleichsmodul verwendet diese Zähler dann, um die Datenflüsse regelmäßig über die Ports im Team zu verteilen. Der Codepfad für den Ausgangsfluss ist so ausgelegt, dass optimale Zeitgleichheit erreicht wird, wenn gleichzeitig mehrere Zugriffe auf die Outbound Flow Hash-Tabelle zulässig sind.

Bei allen anderen Protokollen außer TCP/IP wird stets der erste physische Adapter für ausgehende Pakete ausgewählt. Eine Ausnahme bildet das Address Resolution Protocol (ARP), das anders gehandhabt wird, um Lastausgleich für eingehenden Verkehr zu erreichen.

Eingehender Verkehr (nur SLB)

Der QLogic Intermediate-Treiber verwaltet den Fluss des eingehenden Verkehrs für den Teaming-Modus SLB. Im Gegensatz zum Lastausgleich für ausgehenden Verkehr kann Lastausgleich für eingehenden Verkehr nur auf IP-Adressen angewendet werden, die sich im selben Subnetz befinden wie der Lastausgleichsserver. Beim Lastausgleich für eingehenden Verkehr wird eine einmalige Besonderheit des Address Resolution Protocol (RFC0826) genutzt: Jeder IP-Host verwendet seinen eigenen ARP-Cache zur Einkapselung des IP-Datagramms in einen Ethernet-Rahmen. QLASP manipuliert die ARP-Antwort sorgfältig, sodass jeder IP-Host angewiesen wird, das eingehende IP-Paket an den gewünschten physischen Adapter zu senden. Daher handelt es sich beim Lastausgleich für eingehenden Verkehr um ein vorausplanendes Schema, das auf dem statistischen Verlauf der eingehenden Datenflüsse basiert. Neue Verbindungen von einem Client zum System werden stets über den primären physischen Adapter hergestellt (da die vom Betriebssystem-Protokollstapel generierte ARP-Antwort die logische IP-Adresse stets der MAC-Adresse des primären physischen Adapters zuordnet).

Wie im Fall des ausgehenden Verkehrs gibt es auch hier eine Hash-Tabelle: die Inbound Flow Head Hash-Tabelle. Für jeden Eintrag in dieser Tabelle gibt es eine einfach verkettete Liste, und jede Verkettung (Inbound Flow-Einträge) stellt einen IP-Host im selben Subnetz dar.

Beim Empfang eines eingehenden IP-Datagramms wird der entsprechende Inbound Flow Head-Eintrag durch Hashing der Quell-IP-Adresse des IP-Datagramms lokalisiert. Außerdem werden zwei im ausgewählten Eintrag gespeicherte Statistikzähler aktualisiert. Diese Zähler werden vom Lastausgleichsmodul auf dieselbe Weise verwendet wie die Ausgangszähler: zur regelmäßigen Neuzuweisung der Datenflüsse an den physischen Adapter.

Die Inbound Flow Head Hash-Tabelle im Codepfad für den Eingangsfluss ist ebenfalls für gleichzeitigen Zugriff ausgelegt. Auf die Verbindungslisten der Inbound Flow-Einträge wird nur im Fall der Verarbeitung von ARP-Paketen und periodischem Lastausgleich Bezug genommen. Es gibt keinen Verweis pro Paket auf die Inbound Flow-Einträge. Obgleich die Verbindungslisten nicht beschränkt sind, ist der Overhead bei der Verarbeitung jedes Nicht-ARP-Pakets stets eine Konstante. Die Verarbeitung der ein- und ausgehenden ARP-Pakete hängt jedoch von der Anzahl der Verbindungen innerhalb der entsprechenden Verbindungsliste ab.

Im Verarbeitungspfad für eingehende Pakete werden auch Filter eingesetzt, um zu verhindern, dass Broadcast-Pakete in einer Schleife von anderen physischen Adapter durch das System zurückgeleitet werden.

Protokoll-Unterstützung

ARP- und IP/TCP/UDP-Datenflüsse werden einem Lastausgleich unterzogen. Handelt es sich bei dem Paket nur um ein IP-Protokoll wie ICMP oder IGMP, werden alle Daten, die an eine bestimmte IP-Adresse fließen, durch denselben physischen Adapter geleitet. Wenn das Paket TCP oder UDP für das Schicht-4-Protokoll verwendet, wird die Portnummer dem Hashing-Algorithmus hinzugefügt, sodass zwei separate Schicht-4-Flüsse durch zwei separate physische Adapter an dieselbe IP-Adresse geleitet werden können.

Beispiel: Der Client hat die IP-Adresse 10.0.0.1. Sämtlicher IGMP- und ICMP-Verkehr wird durch denselben physischen Adapter geleitet, da nur die IP-Adresse für den Hash verwendet wird. Der Fluss würde in etwa so aussehen:

```
IGMP -----> PhysAdapter1 -----> 10.0.0.1  
ICMP -----> PhysAdapter1 -----> 10.0.0.1
```

Wenn der Server also einen TCP- und UDP-Fluss an dieselbe 10.0.0.1-Adresse sendet, kann hierfür derselbe physische Adapter wie bei IGMP und ICMP verwendet werden, oder es können vollkommen verschiedene physische Adapter zum Einsatz kommen. Der Fluss würde in etwa so aussehen:

```
IGMP -----> PhysAdapter1 -----> 10.0.0.1  
ICMP -----> PhysAdapter1 -----> 10.0.0.1  
TCP -----> PhysAdapter1 -----> 10.0.0.1  
UDP -----> PhysAdatper1 -----> 10.0.0.1
```

Die Ströme könnten auch so aussehen:

```
IGMP -----> PhysAdapter1 -----> 10.0.0.1  
ICMP -----> PhysAdapter1 -----> 10.0.0.1  
TCP -----> PhysAdapter2 -----> 10.0.0.1  
UDP -----> PhysAdatper3 -----> 10.0.0.1
```

Die eigentliche Zuweisung zwischen Adaptern kann sich im Laufe der Zeit ändern; jedes Protokoll, das nicht auf TCP/UDP basiert, wird jedoch über denselben physischen Adapter geleitet, da nur die IP-Adresse im Hash verwendet wird.

Leistung

Moderne Netzwerkkarten bieten zahlreiche Hardwarefunktionen, mit denen die CPU-Nutzung durch Entlastung bestimmter CPU-intensiver Vorgänge reduziert werden kann (siehe „[Teaming und andere erweiterte Netzwerkeigenschaften](#)“ auf [Seite 168](#)). Der QLASP Intermediate-Treiber ist dagegen eine reine Softwarefunktion, die jedes von den Protokollstapeln empfangene Paket untersucht und auf dessen Inhalt reagieren muss, bevor das Paket über eine bestimmte physische Schnittstelle gesendet wird. Obgleich der QLASP-Treiber jedes ausgehende Paket nahezu gleich schnell verarbeiten kann, können einige Anwendungen, die bereits an die CPU gebunden sind, beeinträchtigt werden, wenn sie über eine Schnittstelle in einem Team betrieben werden. Für eine solche Anwendung ist es unter Umständen günstiger, die Failover-Funktionen des Intermediate-Treibers statt der Lastausgleichsfunktionen zu nutzen. Ebenfalls wäre es möglich, dass sie über einen einzelnen physischen Adapter mit einer bestimmten Hardwarefunktion, wie Large Send Offload (Large Send-Verschiebung), effizienter arbeitet.

Teamarten

Zu den Teamarten zählen Switch-abhängig, Switch-unabhängig und LiveLink.

Switch-unabhängig

Die Teamart Smart Load Balancing von QLogic ermöglicht den Betrieb von zwei bis acht physischen Adaptern als einziger virtueller Adapter. Der größte Vorteil der Teamart SLB besteht darin, dass sie auf jedem IEEE-kompatiblen Switch eingesetzt werden kann und keine besondere Konfiguration erfordert.

Smart Load Balancing und Failover

SLB ermöglicht Switch-unabhängiges, bidirektionales fehlertolerantes Teaming und Lastausgleich. Switch-unabhängig bedeutet, dass der Switch diese Funktion nicht speziell unterstützen muss. Damit ist SLB mit allen Switches kompatibel. Mit SLB haben alle Adapter im Team individuelle MAC-Adressen. Der Lastausgleichsalgorithmus operiert an Schicht-3-Adressen der Quell- und Zielknoten, wodurch SLB sowohl eingehenden als auch ausgehenden Verkehr einem Lastausgleich unterziehen kann.

Der QLASP Intermediate-Treiber überwacht die physischen Ports in einem Team kontinuierlich auf Verbindungsverluste. Im Fall eines Verbindungsverlusts an einem der Ports wird der Verkehr automatisch an andere Ports im Team umgeleitet. Der Teaming-Modus SLB unterstützt Switch-Fehlertoleranz, indem er das Teaming über verschiedene Switches hinweg ermöglicht, vorausgesetzt, die Switches befinden sich in demselben physischen Netzwerk oder derselben Broadcast-Domäne.

Netzwerkkommunikation

Zu den wichtigsten Merkmalen von SLB zählen:

- Failover-Verfahren – Erkennen von Verbindungsverlust.
- Lastausgleichsalgorithmus – Eingehender und ausgehender Verkehr wird durch ein QLogic-eigenes Verfahren auf der Basis der Schicht-4-Datenflüsse ausgeglichen.
- Lastausgleich für ausgehenden Datenverkehr über MAC-Adresse: Nein
- Lastausgleich für ausgehenden Datenverkehr über IP-Adresse: Ja
- Herstellerunabhängiges Teaming wird unterstützt (bei mindestens einem Teammitglied muss es sich um einen QLogic Ethernet-Adapter handeln).

Anwendungen

Der SLB-Algorithmus eignet sich am besten für den Einsatz im Privatbereich und in kleineren Unternehmen, in denen die Kosten möglichst niedrig gehalten werden sollen oder handelsübliche Switching-Geräte verwendet werden. SLB-Teaming funktioniert mit nicht verwalteten Schicht-2-Switches und bietet eine kostengünstige Möglichkeit, Redundanz und Link Aggregation auf dem Server zu erreichen. SLB unterstützt außerdem das Teaming physischer Adapter mit unterschiedlichen Verbindungsfähigkeiten. Des Weiteren eignet sich SLB, wenn Switch-Fehlertoleranz mit Teaming erforderlich ist.

Konfigurationsempfehlungen

SLB unterstützt den Anschluss der Ports im Team an Hubs und Switches, vorausgesetzt, sie befinden sich in derselben Broadcast-Domäne. Die Verbindung mit einem Router oder Schicht-3-Switch wird dagegen nicht unterstützt, da die Ports sich im selben Subnetz befinden müssen.

Switch-abhängig

Allgemeines Static Trunking

Dieser Modus unterstützt eine Vielzahl von Umgebungen, bei denen die Adapter-Verbindungspartner zur Unterstützung eines proprietären Trunking-Verfahrens statisch konfiguriert sind. Dieser Modus kann in Verbindung mit Open Trunk von Lucent, Fast EtherChannel (FEC) von Cisco und Gigabit EtherChannel (GEC) von Cisco eingesetzt werden. Im statischen Modus (wie bei der allgemeinen Link Aggregation) muss der Switch-Administrator dem Team die Ports zuweisen. Diese Zuweisung kann durch QLASP nicht geändert werden, da es keinen Austausch des LACP-Rahmens (Link Aggregation Control Protocol) gibt.

In diesem Modus sind alle Adapter für den Empfang von Paketen unter derselben MAC-Adresse konfiguriert. Trunking wird an Schicht-2-Adressen eingesetzt und unterstützt Lastausgleich und Failover für eingehenden und ausgehenden Verkehr. Der QLASP-Treiber bestimmt das Lastausgleichsschema für ausgehende Datenpakete mithilfe der zuvor behandelten Schicht-4-Protokolle. Das Lastausgleichsschema für eingehende Datenpakete wird dagegen durch den Verbindungspartner des Teams festgelegt.

Der angeschlossene Switch muss das entsprechende Trunking-Schema für diesen Betriebsmodus unterstützen. QLASP und Switch überwachen ihre Ports kontinuierlich auf Verbindungsverluste. Im Fall eines Verbindungsverlusts an einem der Ports wird der Verkehr automatisch an andere Ports im Team umgeleitet.

Netzwerkkommunikation

Im Folgenden werden die wichtigsten Merkmale von Allgemeinem Static Trunking aufgeführt:

- Failover-Verfahren – Erkennen von Verbindungsverlust
- Lastausgleichsalgorithmus – Ausgehender Verkehr wird durch ein QLogic-eigenes Verfahren auf der Basis der Schicht-4-Datenflüsse ausgeglichen. Eingehender Datenverkehr wird entsprechend einem Switch-spezifischen Verfahren ausgeglichen.
- Lastausgleich für ausgehenden Datenverkehr über MAC-Adresse: Nein
- Lastausgleich für ausgehenden Datenverkehr über IP-Adresse: Ja
- Herstellerunabhängiges Teaming wird unterstützt (bei mindestens einem Teammitglied muss es sich um einen QLogic Ethernet-Adapter handeln).

Anwendungen

Allgemeines Trunking funktioniert mit Switches, die Cisco Fast EtherChannel, Cisco Gigabit EtherChannel, Extreme Networks Load Sharing und Bay Networks oder IEEE 802.3ad Link Aggregation im statischen Modus unterstützen. Da Lastausgleich an Schicht-2-Adressen implementiert wird, werden alle höheren Protokolle wie IP, IPX und NetBEUI unterstützt. Daher wird dieser Teaming-Modus empfohlen, wenn der Switch allgemeine Trunking-Modi über SLB unterstützt.

Konfigurationsempfehlungen

Statisches Trunking bietet Unterstützung für die Verbindung der Team-Ports mit Switches, wenn sie sich in derselben Broadcast-Domäne befinden und allgemeines Trunking unterstützen. Die Verbindung mit einem Router oder Schicht-3-Switch wird dagegen nicht unterstützt, da die Ports sich im selben Subnetz befinden müssen.

Dynamisches Trunking (IEEE 802.3ad Link Aggregation)

In diesem Modus wird Link Aggregation durch statische und dynamische Konfiguration über das Link Aggregation Control Protocol (LACP) unterstützt. In diesem Modus sind alle Adapter für den Empfang von Paketen unter derselben MAC-Adresse konfiguriert. Hier wird die MAC-Adresse des ersten Adapters im Team verwendet. Diese Adresse kann nicht durch eine andere MAC-Adresse ersetzt werden. Der QLASP-Treiber bestimmt das Lastausgleichsschema für ausgehende Datenpakete mithilfe der zuvor behandelten Schicht-4-Protokolle. Das Lastausgleichsschema für eingehende Datenpakete wird dagegen durch den Verbindungspartner des Teams festgelegt. Da der Lastausgleich an Schicht-2-Adressen implementiert wird, werden alle höheren Protokolle wie IP, IPX und NetBEUI unterstützt. Der verbundene Switch muss den Link Aggregation-Standard 802.3ad für diesen Betriebsmodus unterstützen. Der Switch verwaltet den eingehenden Datenverkehr an den Adapter, während QLASP für den ausgehenden Verkehr zuständig ist. QLASP und Switch überwachen ihre Ports kontinuierlich auf Verbindungsverluste. Im Fall eines Verbindungsverlusts an einem der Ports wird der Verkehr automatisch an andere Ports im Team umgeleitet.

Netzwerkkommunikation

Im Folgenden werden die wichtigsten Merkmale von Dynamischem Trunking aufgeführt:

- Failover-Verfahren – Erkennen von Verbindungsverlust
- Lastausgleichsalgorithmus – Ausgehender Verkehr wird durch ein QLogic-eigenes Verfahren auf der Basis der Schicht-4-Datenflüsse ausgeglichen. Eingehender Datenverkehr wird entsprechend einem Switch-spezifischen Verfahren ausgeglichen.
- Lastausgleich für ausgehenden Datenverkehr über MAC-Adresse: Nein
- Lastausgleich für ausgehenden Datenverkehr über IP-Adresse: Ja
- Herstellerunabhängiges Teaming wird unterstützt (bei mindestens einem Teammitglied muss es sich um einen QLogic Ethernet-Adapter handeln).

Anwendungen

Dynamisches Trunking funktioniert mit Switches, die IEEE 802.3ad Link Aggregation im dynamischen Modus mit LACP unterstützen. Lastausgleich für eingehenden Verkehr ist Switch-abhängig. Im Allgemeinen erfolgt der Lastausgleich für den Switch-Verkehr auf der Basis von Schicht-2-Adressen. In diesem Fall werden alle Netzwerkprotokolle wie IP, IPX und NetBEUI einem Lastausgleich unterzogen. Daher wird dieser Teaming-Modus empfohlen, wenn der Switch LACP unterstützt, es sei denn, es ist Switch-Fehlertoleranz erforderlich. Der einzige Teaming-Modus, der Switch-Fehlertoleranz unterstützt, ist SLB.

Konfigurationsempfehlungen

Dynamisches Trunking unterstützt die Verbindung von Ports in einem Team mit Switches, vorausgesetzt, sie befinden sich in derselben Broadcast-Domäne und unterstützen IEEE 802.3ad LACP-Trunking. Die Verbindung mit einem Router oder Schicht-3-Switch wird dagegen nicht unterstützt, da die Ports sich im selben Subnetz befinden müssen.

LiveLink

LiveLink ist eine Funktion von QLASP, die für die Teamarten Smart Load Balancing (SLB) und SLB (Auto-Fallback deaktiviert) zur Verfügung steht. LiveLink dient dazu, einen Verbindungsverlust hinter dem Switch zu erkennen und den Datenverkehr nur durch die Teammitglieder zu leiten, die über eine Live-Verbindung verfügen. Diese Funktion steht über die Teaming-Software zur Verfügung. Die Teaming-Software überprüft regelmäßig ein oder mehrere bestimmte Zielnetzwerkgeräte (indem von jedem Teammitglied ein Verbindungspaket gesendet wird). Die zu überprüfenden Zielgeräte antworten nach Empfang des Verbindungspakets. Wenn ein Teammitglied die Antwort nicht innerhalb eines festgelegten Zeitraums erkennt, ist dies das Anzeichen dafür, dass die Verbindung getrennt wurde und dass die Teaming-Software den Datenverkehr nicht mehr durch dieses Teammitglied leitet. Wenn ein Teammitglied zu einem späteren Zeitpunkt von einem zu überprüfenden Zielgerät eine Antwort erkennt, ist dies das Anzeichen dafür, dass die Verbindung wiederhergestellt worden ist und dass die Teaming-Software automatisch wieder den Datenverkehr durch dieses Teammitglied leitet. LiveLink funktioniert nur mit TCP/IP.

Die LiveLink-Funktion wird von den 32-Bit- und 64-Bit-Windows-Betriebssystemen unterstützt. Informationen zu vergleichbaren Funktionen in Linux-Betriebssystemen finden Sie unter den Channel Bonding-Informationen in der Red Hat-Dokumentation.

Attribute der mit jeder Teamart verbundenen Leistungsmerkmale

In [Tabelle 11-5](#) sind die Attribute der mit jeder Teamart verbundenen Leistungsmerkmale zusammengefasst.

Tabelle 11-5. Teaming-Attribute

Leistungsmerkmal	Attribut
Smart Load Balancing	
Benutzeroberfläche	QLogic Control Suite (QCS)
Anzahl der Teams	Maximal 16
Anzahl an Adaptern pro Team	Maximal 16

Tabelle 11-5. Teaming-Attribute (fortgesetzt)

Leistungsmerkmal	Attribut
Hot-Replace	Ja
Hot-Add	Ja
Hot-Remove	Ja
Unterstützte Übertragungsrate	Verschiedene Raten
Rahmen-Protokoll	IP
Verwaltung eingehender Pakete	QLASP
Verwaltung ausgehender Pakete	QLASP
LiveLink-Unterstützung	Ja
Failover-Ereignis	Verbindungsverlust
Failover-Zeit	<500 ms
Fallback-Zeit	1,5 s (Nährwert) ^a
MAC-Adresse	Verschieden
Herstellerunabhängiges Teaming	Ja
Allgemeines Trunking	
Benutzeroberfläche	QLogic Control Suite (QCS)
Anzahl der Teams	Maximal 16
Anzahl an Adaptern pro Team	Maximal 16
Hot-Replace	Ja
Hot-Add	Ja
Hot-Remove	Ja
Unterstützte Übertragungsrate	Verschiedene Raten ^b
Rahmen-Protokoll	Alle
Verwaltung eingehender Pakete	Switch
Verwaltung ausgehender Pakete	QLASP
Failover-Ereignis	Nur Verbindungsverlust
Failover-Zeit	< 500 ms
Fallback-Zeit	1,5 s (Nährwert) ^a

Tabelle 11-5. Teaming-Attribute (fortgesetzt)

Leistungsmerkmal	Attribut
MAC-Adresse	Identisch für alle Adapter
Herstellerunabhängiges Teaming	Ja
Dynamisches Trunking	
Benutzeroberfläche	QLogic Control Suite (QCS)
Anzahl der Teams	Maximal 16
Anzahl an Adaptern pro Team	Maximal 16
Hot-Replace	Ja
Hot-Add	Ja
Hot-Remove	Ja
Unterstützte Übertragungsraten	Verschiedene Raten
Rahmen-Protokoll	Alle
Verwaltung eingehender Pakete	Switch
Verwaltung ausgehender Pakete	QLASP
Failover-Ereignis	Nur Verbindungsverlust
Failover-Zeit	< 500 ms
Fallback-Zeit	1,5 s (Nährwert) ^a
MAC-Adresse	Identisch für alle Adapter
Herstellerunabhängiges Teaming	Ja

^a Stellen Sie sicher, dass Port Fast oder Edge Port aktiviert ist.

^b Einige Switches erfordern übereinstimmende Übertragungsraten für das korrekte Aushandeln zwischen Trunk-Verbindungen.

Für jede Teamart unterstützte Übertragungsraten

In [Tabelle 11-6](#) werden die verschiedenen Übertragungsraten zusammengefasst, die für jede Teamart unterstützt werden. Wenn verschiedene Raten angegeben sind, können die Teaming-Adapter mit unterschiedlichen Übertragungsraten arbeiten.

Tabelle 11-6. Übertragungsraten beim Teaming

Teamart	Übertragungsrate	Richtung des Datenverkehrs	Ratenunterstützung
SLB	10/100/1000/10000	Eingehend und ausgehend	Verschiedene Raten
FEC	100	Eingehend und ausgehend	Identische Raten
GEC	1000	Eingehend und ausgehend	Identische Raten
IEEE 802.3ad	10/100/1000/10000	Eingehend und ausgehend	Verschiedene Raten

Teaming und andere erweiterte Netzwerkeigenschaften

In diesem Abschnitt werden die folgenden Teaming- und erweiterten Netzwerkeigenschaften behandelt:

- [Checksum Offload \(Prüfsummenverschiebung\)](#)
- [IEEE 802.1p QoS-Markierung](#)
- [Large Send Offload \(Large Send-Verschiebung\)](#)
- [Jumbo-Rahmen](#)
- [IEEE 802.1Q VLANs](#)
- [Wake on LAN](#)
- [Preboot Execution Environment](#)

Bevor Sie ein Team erstellen, Teammitglieder hinzufügen oder entfernen oder die erweiterten Einstellungen eines Teammitglieds ändern, sollten Sie sicherstellen, dass alle Teammitglieder in ähnlicher Weise konfiguriert wurden. Die Einstellungen für VLANs, QoS-Paketmarkierung, Jumbo-Rahmen und die verschiedenen Entlastungen müssen überprüft werden. Angaben zu den erweiterten Adaptereigenschaften und zur Teaming-Unterstützung finden Sie in [Tabelle 11-7](#).

Tabelle 11-7. Erweiterte Adaptereigenschaften und Teaming-Unterstützung

Adaptereigenschaften	Unterstützung durch virtuellen Teaming-Adapter
Prüfsummenverschiebung	Ja
IEEE 802.1p QoS-Markierung	Nein
Large Send-Verschiebung	Ja ^a
Jumbo-Rahmen	Ja ^b
IEEE 802.1Q VLANs	Ja ^c
Wake on LAN	Nein ^d
Preboot Execution Environment (PXE)	Ja ^e

^a Diese Funktion muss von allen Adaptern im Team unterstützt werden. Einige Adapter unterstützen diese Funktion u. U. nicht, wenn außerdem ASF/IPMI aktiviert ist.

^b Muss von allen Adaptern im Team unterstützt werden.

^c Nur für QLogic-Adapter.

^d Siehe [Wake on LAN](#).

^e Nur als PXE-Server, nicht als Client.

Ein Team übernimmt nicht notwendigerweise Adaptereigenschaften, sondern verschiedene Eigenschaften hängen vielmehr von spezifischen Funktionen ab. Die Flusskontrolle beispielsweise ist eine Eigenschaft für physische Adapter und steht in keiner Verbindung zu QLASP. Diese Eigenschaft wird an einem bestimmten Adapter aktiviert, wenn die Flusskontrolle des Miniport-Treibers für diesen Adapter aktiviert ist.

ANMERKUNG

Alle Adapter im Team müssen die in [Tabelle 11-7](#) aufgeführte Eigenschaft unterstützen, damit das Team diese Eigenschaft unterstützt.

Checksum Offload (Prüfsummenverschiebung)

Checksum Offload (Prüfsummenverschiebung) ist eine Eigenschaft der QLogic-Netzwerkadapter, die es ermöglicht, dass die TCP/IP/UDP-Prüfsummen zum Senden und Empfangen von Datenverkehr statt von der Host-CPU von der Adapterhardware berechnet werden. Bei hohem Verkehrsaufkommen kann ein System dadurch mehr Verbindungen effizienter handhaben, als dies bei einer Prüfsummen-Berechnung durch die Host-CPU möglich wäre. Dabei handelt es sich naturgemäß um eine Hardwareeigenschaft. Bei einer reinen Softwareimplementierung ließe sich daraus kein Nutzen ziehen. Ein Adapter, der die Prüfsummenverschiebung unterstützt, kündigt dem Betriebssystem diese Fähigkeit an, so dass die Prüfsumme nicht im Protokollstapel berechnet werden muss. Die Prüfsummenverschiebung wird derzeit nur für IPv4 unterstützt.

IEEE 802.1p QoS-Markierung

Der Standard IEEE 802.1p umfasst ein 3-Bit-Feld (mit Unterstützung für maximal acht Prioritätsebenen), das eine Priorisierung des Datenverkehrs ermöglicht. Der QLASP Intermediate-Treiber bietet keine Unterstützung für IEEE 802.1p QoS-Markierung.

Large Send Offload (Large Send-Verschiebung)

Large Send Offload (Large Send-Verschiebung) ist eine von QLogic-Netzwerkadaptern bereitgestellte Funktion, die verhindert, dass ein höheres Kommunikationsprotokoll wie TCP ein großes Datenpaket in eine Reihe kleinerer Pakete mit angehängten Kopfzeilen unterteilt. Der Protokollstapel muss nur eine einzige Kopfzeile für ein Datenpaket mit einer Größe von 64 KB generieren, und die Adapterhardware unterteilt den Datenpuffer in Ethernet-Rahmen von angemessener Größe mit den Kopfzeilen in korrekter Folge (basierend auf der einzelnen, ursprünglich angegebenen Kopfzeile).

Jumbo-Rahmen

Jumbo-Rahmen wurden erstmals 1998 von Alteon Networks, Inc. vorgestellt. Die Maximalgröße eines Ethernet-Rahmens wurde damit auf 9600 Byte erhöht. Obwohl die Unterstützung für Jumbo-Rahmen nie offiziell von der IEEE 802.3-Arbeitsgruppe angenommen wurde, wurde diese Funktion doch in den QLogic BCM57xx und BCM57xxx-Adaptern implementiert. Der QLASP Intermediate-Treiber unterstützt Jumbo-Rahmen, vorausgesetzt, dass alle physischen Adapter im Team ebenfalls Jumbo-Rahmen unterstützen und für alle Adapter im Team dieselbe Größe eingerichtet ist.

IEEE 802.1Q VLANs

1998 wurde der 802.3ac-Standard vom IEEE genehmigt. Dieser Standard definiert Rahmenformaterweiterungen zur Unterstützung von Virtual Bridged Local Area Network-Markierung in Ethernet-Netzwerken, wie in der IEEE 802.1Q-Spezifikation angegeben. Das VLAN-Protokoll ermöglicht das Einfügen eines Tags in einen Ethernet-Frame, um das VLAN zu bestimmen, zu dem ein Frame gehört. Wenn vorhanden, wird der 4 Byte lange VLAN-Tag in den Ethernet-Rahmen zwischen der Quell-MAC-Adresse und dem Feld für Länge/Typ eingefügt. Die ersten 2 Byte des VLAN-Tags bestehen aus dem IEEE 802.1Q-Tagtyp, während die letzten 2 Byte ein Feld für die Benutzerpriorität und die VLAN-ID (VID) enthalten. Virtuelle LANs (VLANs) ermöglichen es dem Benutzer, das physische LAN in logische Unterteile aufzugliedern. Jedes definierte VLAN verhält sich wie ein separates Netzwerk, dessen Datenverkehr und Broadcasts von den anderen Netzwerken getrennt sind, sodass die Bandbreiteneffizienz innerhalb der einzelnen logischen Gruppen erhöht wird. VLANs ermöglichen es dem Administrator außerdem, entsprechende Richtlinien für Sicherheit und Servicequalität (Quality of Service, QoS) festzulegen. Mit QLASP können pro Team oder Adapter bis zu 64 VLANs erstellt werden: 63 markierte und ein unmarkiertes. Die tatsächliche Anzahl möglicher VLANs wird jedoch durch das Betriebssystem und die Systemressourcen eingeschränkt. Der Standard IEEE 802.1q bietet VLAN-Unterstützung. VLANs werden sowohl in einer Teaming-Umgebung als auch an einem einzelnen Adapter unterstützt. Beachten Sie, dass VLANs nur bei homogenem Teaming unterstützt werden, nicht aber bei herstellerunabhängigem Teaming. Der QLASP Intermediate-Treiber unterstützt VLAN-Markierung. Ein oder mehrere VLANs können an eine einzelne Instanz des Intermediate-Treibers gebunden sein.

Wake on LAN

Mit Wake on LAN (WoL) kann der Ruhemodus eines Systems beendet werden, wenn ein bestimmtes Paket über die Ethernet-Schnittstelle eingeht. Da ein virtueller Adapter als reines Softwaregerät implementiert ist, fehlen ihm die Hardwarefunktionen zur Implementierung von Wake on LAN. Über einen virtuellen Adapter kann der Ruhemodus eines Systems deshalb nicht beendet werden. Die physischen Adapter hingegen unterstützen diese Eigenschaft auch dann, wenn sie Teil eines Teams sind.

ANMERKUNG

Wake-on-LAN wird nur an einem physikalischen Anschluss (Anschluss 1) für folgende Adapter unterstützt:

- BCM957810A1006DC (N20KJ)
 - BCM957810A1006DLPC (Y40PH)
-

Preboot Execution Environment

Preboot Execution Environment (PXE) ermöglicht einem System das Booten mithilfe eines Betriebssystems-Image über das Netzwerk. Definitionsgemäß wird PXE aufgerufen, bevor ein Betriebssystem geladen ist, sodass der QLASP Intermediate-Treiber keine Gelegenheit hat, ein Team zu laden und zu aktivieren. Infolge dessen wird Teaming als PXE-Client nicht unterstützt, obwohl ein physischer Adapter in einem Team beim Laden des Betriebssystems als PXE-Client verwendet werden kann. Ein Team-Adapter kann zwar nicht als PXE-Client verwendet werden, er kann jedoch als PXE-Server fungieren, der PXE-Clients Betriebssystem-Images bereitstellt, wobei er eine Kombination aus Dynamic Host Control Protocol (DHCP) und Trivial File Transfer Protocol (TFTP) verwendet. Beide Protokolle können über IP betrieben werden und unterstützen alle Teaming-Modi.

Allgemeine Netzwerkaspekte

Zu den allgemeinen Netzwerkaspekten zählt:

- [Teaming mit Microsoft Virtual Server 2005](#)
- [Switch-übergreifendes Teaming](#)
- [Spanning Tree-Algorithmus](#)
- [Schicht-3-Routing und -Switching](#)
- [Teaming mit Hubs \(nur zur Problembehebung\)](#)
- [Teaming mit Microsoft Network Load Balancing](#)

Teaming mit Microsoft Virtual Server 2005

Als einzige QLASP-Teamkonfiguration bei Verwendung von Microsoft Virtual Server 2005 wird eine Konfiguration mit einer Smart Load Balancing-Teamart unterstützt, der aus einem einzigen primären QLogic-Adapter und einem Standby-QLogic-Adapter besteht. Stellen Sie sicher, dass die „Virtual Machine Network Services“ jedes Teamelements vor der Erstellung der virtuellen Netzwerke mit Microsoft Virtual Server gelöst oder abgewählt werden. Erstellen Sie darüber hinaus ein virtuelles Netzwerk in dieser Software und verbinden Sie es anschließend mit dem von einem Team erstellten virtuellen Adapter. Das direkte Verbinden eines Gast-Betriebssystems mit einem virtuellen Teamadapter führt unter Umständen nicht zu den gewünschten Ergebnissen.

ANMERKUNG

Zum Zeitpunkt der Dokumenterstellung wurde Windows Server 2008 von Microsoft Virtual Server 2005 nicht als Betriebssystem unterstützt. Dementsprechend ist Teaming bei dieser Kombination möglicherweise nicht den Erwartungen entsprechend möglich.

Switch-übergreifendes Teaming

SLB-Teaming kann über mehrere Switches konfiguriert werden. Die Switches müssen jedoch verbunden sein. Allgemeines Trunking und Link Aggregation funktionieren nicht Switch-übergreifend, da jede dieser Implementierungen erfordert, dass alle physischen Adapter in einem Team dieselbe Ethernet MAC-Adresse haben. Beachten Sie, dass SLB nur den Verbindungsverlust zwischen den Ports im Team und ihrem unmittelbaren Verbindungspartner erkennen kann. SLB ist nicht in der Lage, auf andere Hardwarestörungen in den Switches zu reagieren oder Verbindungsverluste an anderen Ports zu erkennen.

Fehlertoleranz bei Switch-Verbindung

Die Abbildungen in diesem Abschnitt demonstrieren den Betrieb eines SLB-Teams in einer Konfiguration mit Switch-Fehlertoleranz. QLogic zeigt die Zuordnung der Ping-Anforderung und der Ping-Antwort in einem SLB-Team mit zwei aktiven Mitgliedern. Alle Server (Blue, Gray und Red) senden sich gegenseitig einen Dauerping. Diese Beispiele veranschaulichen das Prinzip des Switch-übergreifenden Teamings und die Bedeutung des Verbindungskabels.

- [Abbildung 11-3](#) zeigt eine Konfiguration ohne Verbindungskabel zwischen den beiden Switches.
- In [Abbildung 11-4](#) ist das Verbindungskabel vorhanden.
- [Abbildung 11-5](#) zeigt ein Beispiel für ein Failover-Ereignis mit vorhandenem Verbindungskabel.

Die Abbildungen zeigen, wie das sekundäre Teammitglied die ICMP-Echoanfrage sendet (gelbe Pfeile), während das primäre Teammitglied die entsprechende ICMP-Echoantwort empfängt (blaue Pfeile). Dieser Sende- und Empfangsvorgang veranschaulicht eine Haupteigenschaft der Teaming-Software. Durch die Lastausgleichsalgorithmen wird die Art des Lastausgleichs von Rahmen beim Senden oder Empfangen nicht synchronisiert. Rahmen für eine bestimmte Konversation können an verschiedene Schnittstellen im Team gesendet und dort empfangen werden. Dies trifft auf alle Teaming-Arten zu, die von QLogic unterstützt werden. Daher muss eine Verbindung zwischen den Switches bestehen, die mit Ports im selben Team verbunden sind.

In der Konfiguration ohne das Verbindungskabel wird eine ICMP-Anforderung von Blue an Gray von Port 82:83 abgeschickt, die für den Gray-Port 5E:CA bestimmt ist. Der Top Switch hat jedoch keine Möglichkeit zum Senden, da er den Gray-Port 5E:C9 nicht benutzen kann. Eine ähnliche Situation tritt ein, wenn Gray versucht, einen Ping an Blue zu senden. Eine ICMP-Anforderung, bestimmt für Blue 82:82, wird von 5E:C9 gesendet, erreicht ihr Ziel jedoch nicht. Dem Top Switch fehlt der Eintrag für 82:82 in der CAM-Tabelle, da es keine Verbindung zwischen den beiden Switches gibt. Zwischen Red und Blue und zwischen Red und Gray können die Pings jedoch fließen.

Ein Failover-Ereignis würde außerdem zu weiterem Konnektivitätsverlust führen. Angenommen, an Port 4 am Top Switch würde das Kabel entfernt. In diesem Fall würde Gray die ICMP-Anforderung an Red 49:C9 senden. Da allerdings der Bottom Switch keinen Eintrag für 49:C9 in seiner CAM-Tabelle vorfindet, wird der Frame an alle Ports gesendet, dieser kann 49:C9 jedoch nicht erreichen.

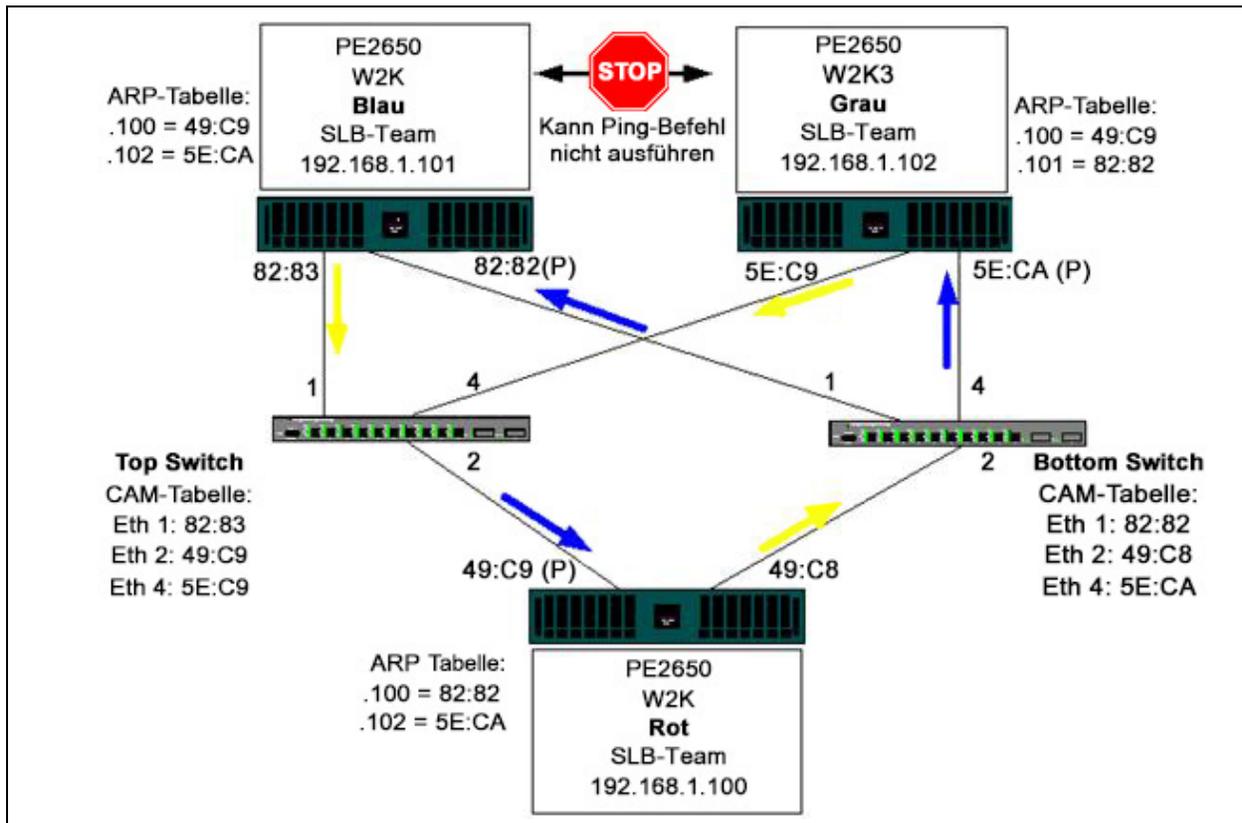


Abbildung 11-3. Switch-übergreifendes Teaming ohne Verbindung zwischen den Switches

Werden die Switches miteinander gekoppelt, kann der Verkehr von Blue nach Gray und umgekehrt problemlos fließen. Beachten Sie die zusätzlichen Einträge in der CAM-Tabelle für beide Switches. Die Verbindung ist entscheidend für den korrekten Betrieb des Teams. Daher empfiehlt QLogic dringend die Einrichtung eines Link Aggregation-Trunks zur Koppelung der beiden Switches, damit eine hohe Verfügbarkeit der Verbindung gewährleistet werden kann.

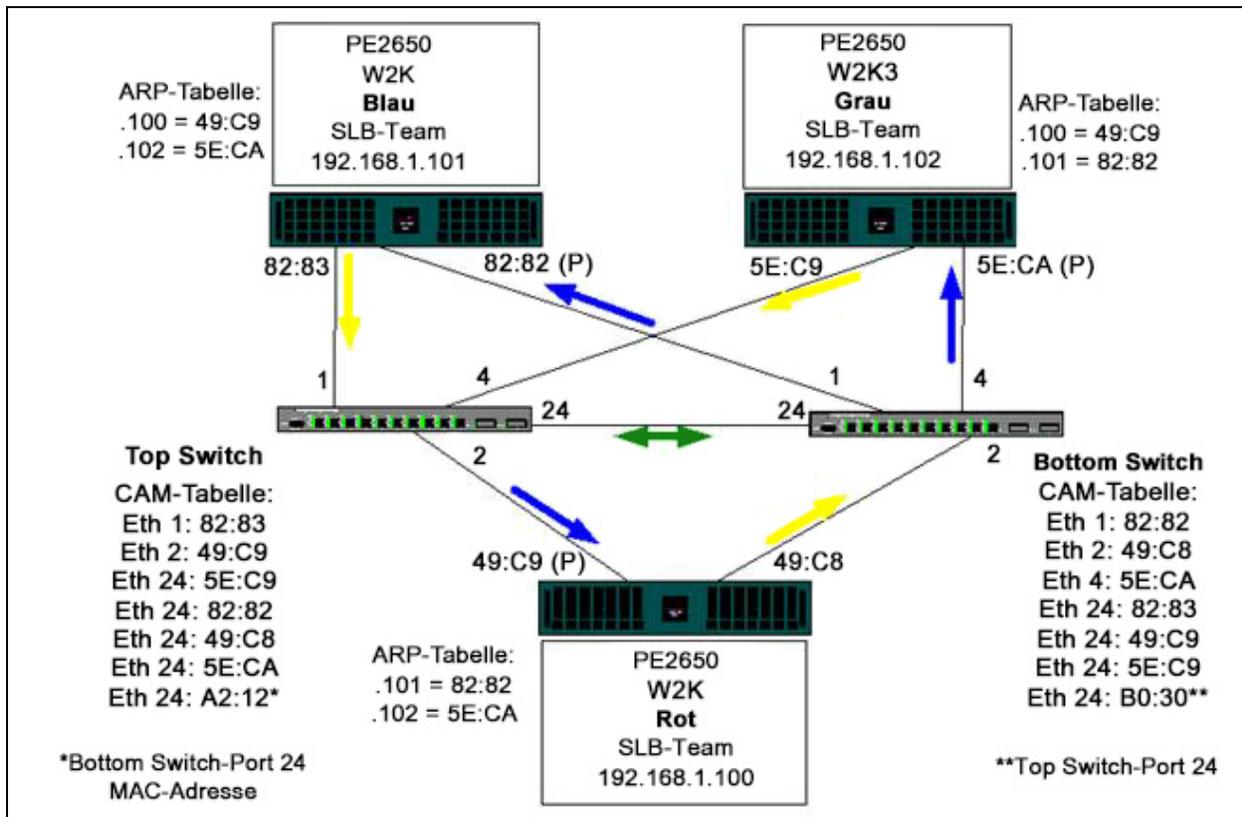


Abbildung 11-4. Switch-übergreifendes Teaming mit Schnittstelle

Abbildung 11-5 zeigt ein Failover-Ereignis, bei dem das Kabel an Port 4 des Top Switches herausgezogen wurde. Dieses Ereignis ist ein erfolgreiches Failover, und alle Stationen senden sich gegenseitig Pings, ohne dass es zu Verbindungsverlusten kommt.

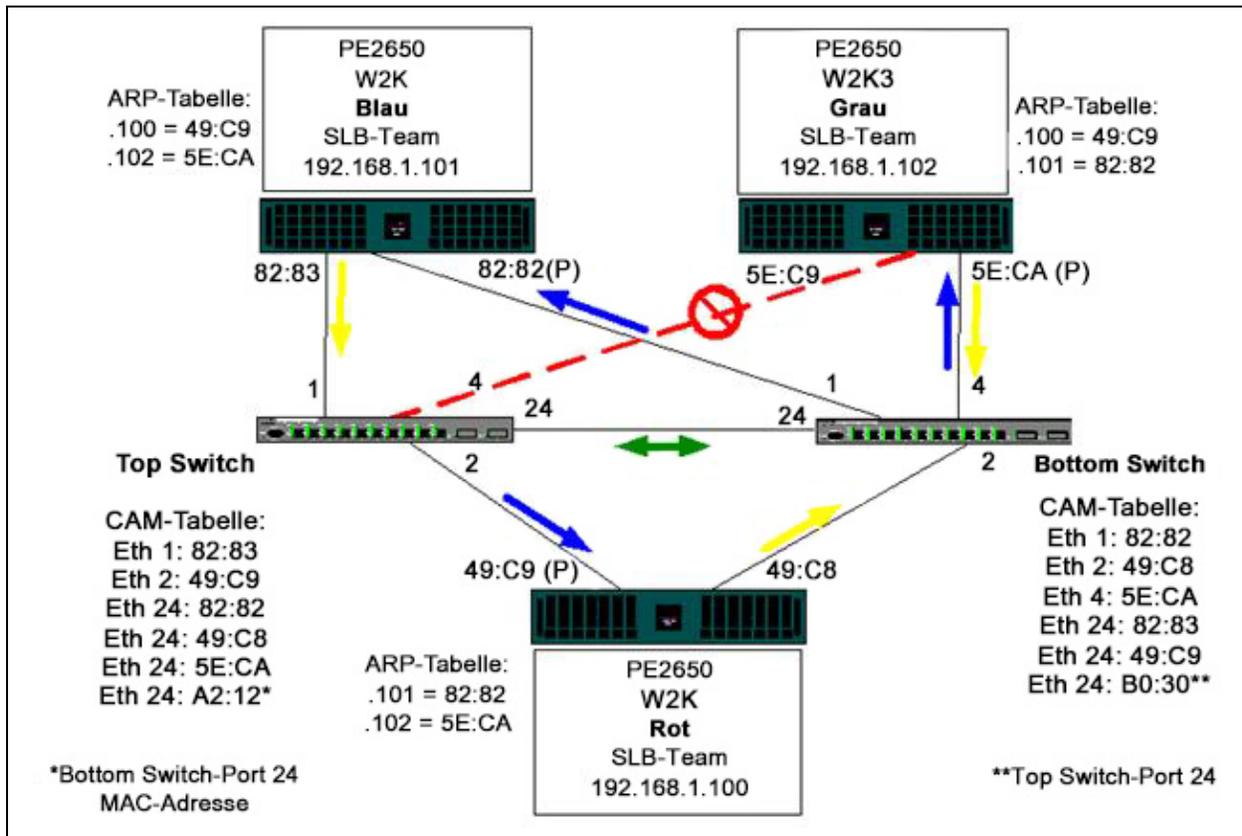


Abbildung 11-5. Failover-Ereignis

Spanning Tree-Algorithmus

In Ethernet-Netzwerken existiert u. U. nur ein aktiver Pfad zwischen zwei Bridges oder Switches. Bei mehreren aktiven Pfaden zwischen Switches kann es zu Schleifen im Netzwerk kommen. Wenn Schleifen auftreten, erkennen einige Switches Stationen auf beiden Seiten des Switches. Dies führt zu einer Störung im Forwarding-Algorithmus, so dass doppelte Rahmen weitergeleitet werden. Spanning Tree-Algorithmen ermöglichen Pfadredundanz, indem sie einen Tree definieren, der alle Switches in einem erweiterten Netzwerk umfasst, und dann bestimmte redundante Datenpfade in einen Standby-Status (blockiert) zwingen. In regelmäßigen Abständen senden und empfangen die Switches im Netzwerk Spanning Tree-Pakete, die sie zur Identifizierung des Pfades verwenden. Falls ein Netzwerksegment nicht mehr erreicht werden kann oder wenn sich der Spanning Tree-Zeitaufwand ändert, konfiguriert der Spanning Tree-Algorithmus die Spanning Tree-Topologie neu und stellt die Verbindung wieder her, indem er den Standby-Pfad aktiviert. Der Spanning Tree-Betrieb ist für Endstationen transparent, die nicht erkennen, ob sie mit einem einzelnen LAN-Segment oder einem Switched-LAN aus mehreren Segmenten verbunden sind.

Spanning Tree Protocol (STP) ist ein Schicht-2-Protokoll, das für Bridges und Switches ausgelegt ist. Die Spezifikation für STP ist im Standard IEEE 802.1d definiert. Die Hauptaufgabe von STP besteht darin, sicherzustellen, dass es nicht zu einer Schleifensituation kommt, wenn redundante Pfade im Netzwerk vorhanden sind. STP erkennt und deaktiviert Netzwerkschleifen und bietet Backup-Verbindungen zwischen Switches oder Bridges. Es ermöglicht dem Gerät, mit anderen STP-kompatiblen Geräten im Netzwerk zu interagieren, und stellt damit sicher, dass nur ein Pfad zwischen jeweils zwei Stationen im Netzwerk existiert.

Nachdem eine stabile Netzwerktopologie eingerichtet wurde, empfangen alle Bridges BPDU-Nachrichten (Bridge Protocol Data Units), die von der Root-Bridge übertragen werden. Empfängt eine Bridge nach einem vordefinierten Intervall (Max Age) keine BPDU-Nachricht, nimmt die Bridge an, dass die Verbindung zur Root-Bridge unterbrochen wurde. Diese Bridge beginnt dann Verhandlungen mit anderen Bridges zur Neukonfiguration des Netzwerks, um wieder eine gültige Netzwerktopologie herzustellen. Der Vorgang zum Erstellen einer neuen Topologie kann bis zu 50 Sekunden in Anspruch nehmen. In dieser Zeit ist die End-to-End-Kommunikation unterbrochen.

Für Ports, die mit Endstationen verbunden sind, empfiehlt QLogic nicht die Verwendung von Spanning Tree, da eine Endstation definitionsgemäß keine Schleife in einem Ethernet-Segment erstellt. Wenn ein Team-Adapter mit einem Port verbunden und der Spanning Tree aktiviert ist, kann es außerdem zu unerwarteten Konnektivitätsproblemen kommen. Angenommen, bei einem Adapter im Team ist ein Verbindungsverlust an einem der physischen Adapter aufgetreten. Würde die Verbindung des physischen Adapters wiederhergestellt (auch als Fallback bezeichnet), würde der Intermediate-Treiber erkennen, dass die Verbindung wieder aufgebaut wurde und beginnen, Datenverkehr durch den Port zu leiten. Der Datenverkehr würde verloren gehen, wenn der Port vorübergehend durch das Spanning Tree Protocol (STP) blockiert würde.

Dieser Abschnitt enthält Details zu:

- [Topology Change Notice \(TCN\)](#)
- [Port Fast und Edge Port](#)

Topology Change Notice (TCN)

Eine Bridge oder ein Switch erstellt eine Forwarding-Tabelle mit MAC-Adressen und Portnummern, indem sie/er die Quell-MAC-Adresse lernt, die an einem bestimmten Port empfangen wurde. Die Tabelle wird verwendet, um Rahmen an einen bestimmten Port weiterzuleiten, anstatt den Rahmen an alle Ports zu senden. Die maximale Verfallszeit der Einträge beträgt normalerweise 5 Minuten. Erst wenn ein Host 5 Minuten lang nicht gesendet hat, wird der Eintrag aus der Tabelle entfernt. In manchen Situationen ist es von Vorteil, die Verfallszeit zu reduzieren. Ein Beispiel: Eine Verbindung wechselt aus dem Weiterleitungszustand in den blockierten Zustand, und eine andere Verbindung wechselt aus dem blockierten Zustand in den Weiterleitungszustand. Dieser Wechsel könnte bis zu 50 Sekunden dauern. Am Ende der STP-Neuberechnung stünde ein neuer Pfad für die Kommunikation zwischen Endstationen zur Verfügung. Da jedoch die Forwarding-Tabelle noch immer Einträge auf Basis der alten Topologie enthalten würde, könnte die Kommunikation möglicherweise erst nach 5 Minuten wiederhergestellt werden, wenn die betroffenen Port-Einträge aus der Tabelle entfernt sind. Der Datenverkehr würde dann an alle Ports gesendet und neu gelernt werden. In diesem Fall wäre eine Reduzierung der Verfallszeit von Vorteil. Diese Reduzierung ist der Zweck einer speziellen BPDU namens TCN (Topology Change Notice). Eine TCN wird von der betroffenen Bridge bzw. vom Switch an die Root-Bridge/den Root-Switch gesendet. Sobald eine Bridge/ein Switch eine Änderung der Topologie erkennt (wenn eine Verbindung verloren geht oder ein Port in den weiterleitenden Zustand wechselt), wird über den Root-Port eine TCN an die Root-Bridge gesendet. Die Root-Bridge kündigt dann dem gesamten Netzwerk eine BPDU mit einer TCN an. Dadurch reduziert jede Bridge die Verfallszeit der MAC-Tabelle für einen bestimmten Zeitraum auf 15 Sekunden. Durch die Zeitreduzierung kann der Switch die MAC-Adressen neu lernen, sobald STP erneut konvergiert.

TCN BPDUs werden gesendet, wenn ein Port aus dem weiterleitenden Zustand in den blockierten Zustand wechselt oder umgekehrt. Eine TCN BPDU initiiert keine STP-Neuberechnung. Sie beeinflusst lediglich die Verfallszeit der Einträge der Forwarding-Tabelle im Switch. Sie führt keine Änderung der Topologie herbei und erstellt keine Schleifen. Endknoten wie Server oder Clients lösen eine Topologieänderung aus, wenn sie aus- und wieder eingeschaltet werden.

Port Fast und Edge Port

Um die Auswirkungen von TCNs auf das Netzwerk (z. B. eine verstärkte Überflutung der Switch-Ports) zu reduzieren, sollten Endknoten, die häufig ein- bzw. ausgeschaltet werden, auf dem Switch-Port, an den sie angeschlossen sind, die Port Fast- oder Edge Port-Einstellung verwenden. Port Fast oder Edge Port ist ein Befehl, der auf bestimmte Ports angewendet wird und die folgenden Auswirkungen hat:

- Ports, deren Verbindung aus dem inaktiven in den aktiven Zustand wechselt, werden in den weiterleitenden STP-Modus versetzt, anstatt aus dem wartenden Zustand in den lernenden und dann in den weiterleitenden Zustand überzugehen. STP wird auf diesen Ports weiterhin ausgeführt.
- Der Switch generiert keine Benachrichtigung über eine Topologieänderung, wenn der Port aktiv oder wieder inaktiv wird.

Schicht-3-Routing und -Switching

Der Switch, mit dem die Ports im Team verbunden sind, darf kein Layer-3-Switch oder -Router sein. Die Ports im Team müssen sich im selben Netzwerk befinden.

Teaming mit Hubs (nur zur Problembhebung)

SLB-Teaming kann bei 10 und 100-Hubs eingesetzt werden, QLogic empfiehlt jedoch nur die Verwendung zu Problembhebungszwecken, wie beim Anschluss eines Netzwerkanalysators für den Fall, dass Switch-Port-Spiegelung nicht in Frage kommt.

Die Hub-Teaming-Informationen umfassen:

- [Verwendung von Hubs in Teaming-Netzwerkkonfigurationen](#)
- [SLB-Teams](#)
- [SLB-Teams mit Anschluss an einen einzelnen Hub](#)
- [Allgemeines und Dynamisches Trunking \(FEC/GEC/IEEE 802.3ad\)](#)

Verwendung von Hubs in Teaming-Netzwerkkonfigurationen

Obwohl die Verwendung von Hubs in Netzwerktopologien in einigen Fällen zweckmäßig sein kann, sollten unbedingt Auswirkungen auf den Durchsatz berücksichtigt werden. Netzwerk-Hubs haben eine maximale Halbduplex-Übertragungsrate von 100 MBit/s, wodurch die Leistung in einer Gigabit- oder 100-MBit/s-Switched-Netzwerkconfiguration erheblich beeinträchtigt wird. Die Hub-Bandbreite wird von allen verbundenen Geräten gemeinsam genutzt. Daher reduziert sich beim Anschluss mehrerer Geräte an den Hub die Bandbreite, die für jedes einzelne an den Hub angeschlossene Gerät verfügbar ist, direkt proportional zur Anzahl der mit dem Hub verbundenen Geräte.

QLogic empfiehlt nicht, Teammitglieder an den Hub anzuschließen; es sollten nur Switches zur Verbindung mit Ports im Team verwendet werden. Ein SLB-Team kann allerdings zum Zweck der Problembehebung direkt an einen Hub angeschlossen werden. Bei anderen Teamarten kann es zu Konnektivitätsverlusten kommen, wenn bestimmte Störungen auftreten. Sie sollten daher nicht gemeinsam mit Hubs verwendet werden.

SLB-Teams

SLB-Teams sind als einzige Teamart nicht von der Switch-Konfiguration abhängig. Der Intermediate-Treiber des Servers bewältigt Lastausgleichs- und Fehlertoleranzverfahren ohne Hilfe vom Switch. Aufgrund dieser Elemente ist SLB die einzige Teamart, bei der Failover- und Fallback-Eigenschaften erhalten bleiben, wenn Team-Ports direkt mit einem Hub verbunden werden.

SLB-Teams mit Anschluss an einen einzelnen Hub

SLB-Teams in der in [Abbildung 11-6](#) dargestellten Konfiguration behalten ihre Fehlertoleranzeigenschaften bei. Bei einem Ausfall einer der Serververbindungen blieben die Netzwerkfunktionen trotzdem erhalten. Auch bei direktem Anschluss von Clients an den Hub wäre die Fehlertoleranz noch immer gewährleistet; die Serverleistung würde allerdings beeinträchtigt werden.

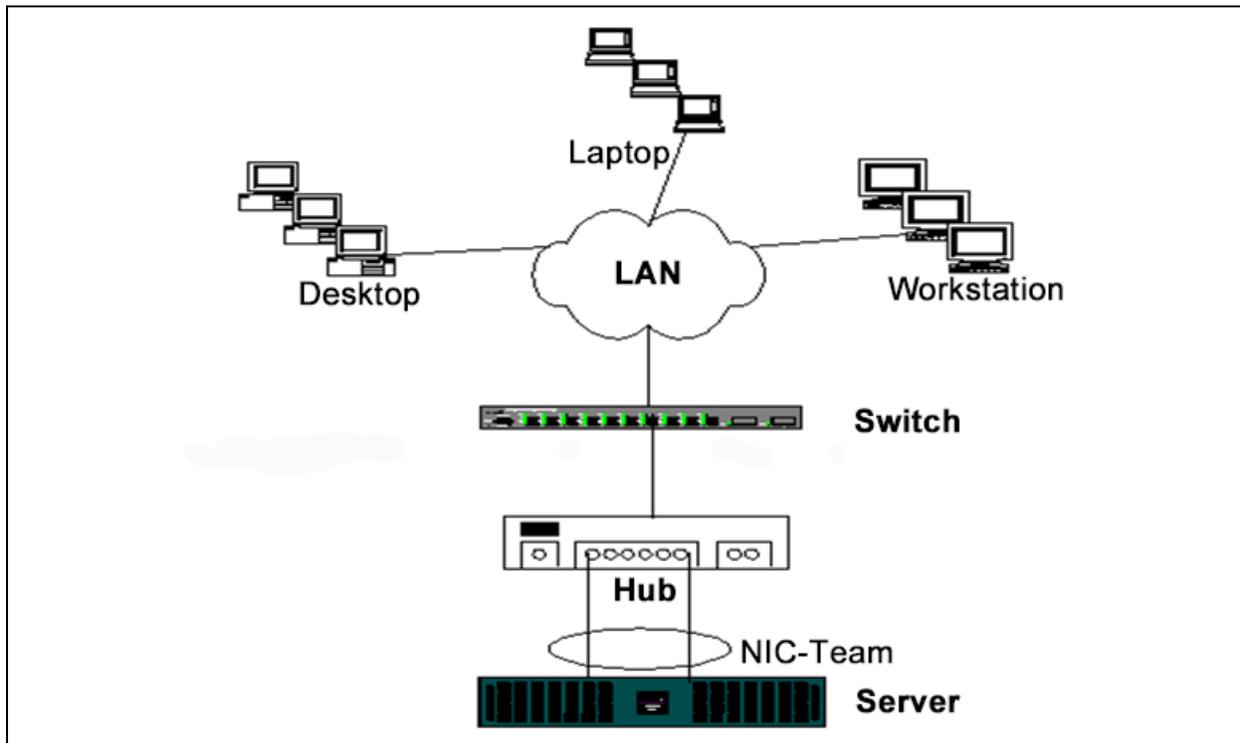


Abbildung 11-6. Team mit Anschluss an einen einzelnen Hub

Allgemeines und Dynamisches Trunking (FEC/GEC/IEEE 802.3ad)

FEC, GEC- und IEEE 802.3ad-Teams können nicht mit Hub-Konfigurationen verbunden werden. Teams dieser Art müssen an einen Switch angeschlossen werden, der ebenfalls für diese Teamart konfiguriert wurde.

Teaming mit Microsoft Network Load Balancing

Teaming funktioniert *nicht* im Microsoft Network Load Balancing-Unicast-Modus, sondern nur im Multicast-Modus. Aufgrund des vom Network Load Balancing-Dienst verwendeten Verfahrens sollte in dieser Umgebung die Teaming-Konfiguration Failover eingesetzt werden (SLB mit einer Standby-Netzwerkkarte), da der Lastausgleich von Network Load Balancing verwaltet wird.

Anwendungsaspekte

Behandelte Anwendungsaspekte:

- [Teaming und Clustering](#)
- [Teaming und Netzwerkbackup](#)

Teaming und Clustering

Die Informationen zu Teaming und Clustering umfassen:

- [Microsoft Cluster-Software](#)
- [High-Performance Computing Cluster](#)
- [Oracle](#)

Microsoft Cluster-Software

Dell Server-Clusterlösungen integrieren Microsoft Cluster Services (MSCS) mit PowerVault™ SCSI-Speicher oder Dell und EMC-Speicher auf Fibre-Channel-Basis, Dell-Servern, Speicheradaptern, Speicher-Switches und Netzwerkadaptern, um HA-Lösungen (High-Availability) für eine hohe Verfügbarkeit bereitzustellen. HA-Clustering bietet Unterstützung für alle Adapter, die für unterstützte Dell-Server geeignet sind.

QLogic empfiehlt dringend, in jedem Clusterknoten mindestens zwei Netzwerkadapter zu installieren (die Verwendung von On-Board-Adaptern ist möglich). Diese Schnittstellen dienen einem doppelten Zweck:

- Ein Adapter wird ausschließlich für die Intracluster-*Heartbeat*-Kommunikation verwendet. Dieser Adapter wird als *private adapter* (privater Adapter) bezeichnet und befindet sich normalerweise in einem separaten privaten Subnetzwerk.
- Der andere Adapter wird zur Client-Kommunikation verwendet und als *public adapter* (öffentlicher Adapter) bezeichnet.

Es können mehrere Adapter für jeden dieser Zwecke eingesetzt werden: private Intracluster-Kommunikation und öffentliche Kommunikation mit externen Clients. Microsoft Cluster-Software unterstützt alle QLogic-Teaming-Modi ausschließlich für den öffentlichen Adapter. Teaming für private Netzwerkadapter wird nicht unterstützt. Nach Angaben von Microsoft wird Teaming an der privaten Schnittstelle eines Serverclusters deshalb nicht unterstützt, weil es beim Senden und Empfangen von Heartbeat-Paketen zwischen den Knoten zu Verzögerungen kommen könnte. Wenn Redundanz für die private Verbindung gewünscht wird, sollten Sie Teaming deaktivieren und mit den verfügbaren Ports eine zweite private Verbindung bilden. Mit dieser Verbindung erzielen Sie dasselbe Ergebnis und erhalten zwei robuste Kommunikationspfade, über die die Knoten kommunizieren können.

QLogic empfiehlt beim Teaming in einer Clusterumgebung, Adapter derselben Marke zu verwenden.

Abbildung 11-7 zeigt einen Fibre-Channel-Cluster mit zwei Knoten und drei Netzwerkschnittstellen pro Clusterknoten: eine private und zwei öffentliche. Die beiden öffentlichen Adapter an jedem Knoten sind Team-Adapter, im Gegensatz zum privaten Adapter. Teaming wird über einen Switch oder auch über zwei Switches hinweg unterstützt. [Abbildung 11-8 auf Seite 185](#) zeigt denselben Fibre-Channel-Cluster mit zwei Knoten in dieser Konfiguration.

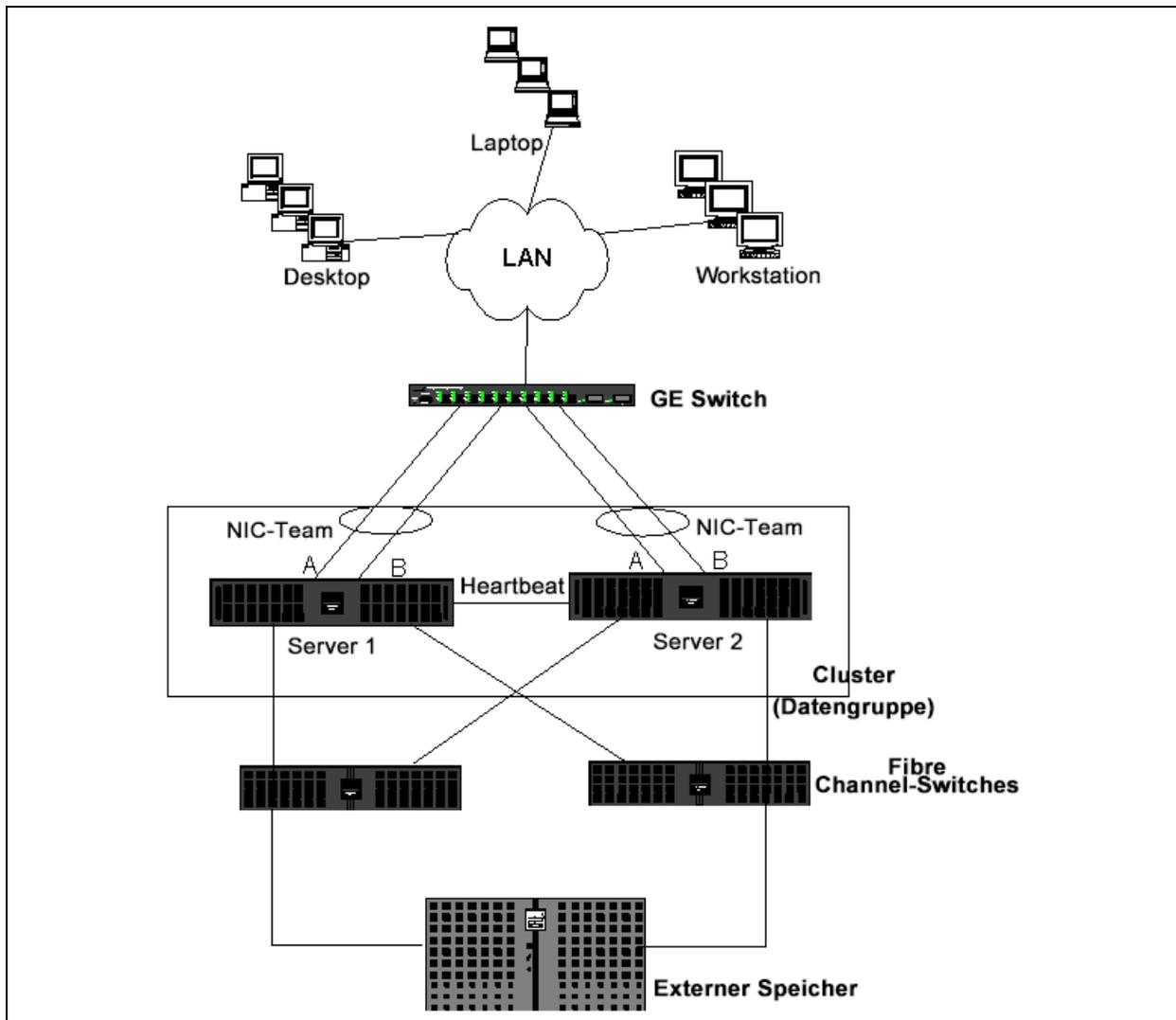


Abbildung 11-7. Clustering mit Teaming über einen Switch

ANMERKUNG

Microsoft Cluster-Software bietet keine Unterstützung für Microsoft Network Load Balancing.

High-Performance Computing Cluster

In HPCC-Anwendungen (High-Performance Computing Cluster) wird Gigabit Ethernet normalerweise zu den folgenden Zwecken eingesetzt:

- **Inter-Process-Communications (Prozessinterne Kommunikation, IPC):**
Bei Anwendungen, die keine Verbindungen mit hoher Bandbreite und niedriger Latenzzeit erfordern (wie Myrinet™, InfiniBand®) kann Gigabit Ethernet für die Kommunikation zwischen den Compute-Knoten verwendet werden.
- **I/A (E/A):** Ethernet kann für die Dateifreigabe und zur Versorgung der Compute-Knoten mit Daten verwendet werden. Dazu werden ein NFS-Server oder parallele Dateisysteme wie PVFS verwendet.
- **Management and Administration (Verwaltung und Administration):**
Ethernet wird für das Out-of-Band-Management (Dell Embedded Remote Access [ERA]) und das In-Band-Management (Dell OpenManage™ Server Administrator [OMSA]) der Knoten im Cluster verwendet. Außerdem kann es zur Jobplanung und -überwachung eingesetzt werden.

In den aktuellen HPCC-Angeboten von Dell wird nur einer der On-Board-Adapter verwendet. Ist Myrinet oder InfiniBand vorhanden, dient dieser Adapter I/O- und Verwaltungszwecken; andernfalls ist er zusätzlich für IPC zuständig. Sollte ein Adapter ausfallen, kann der Administrator mithilfe des Felix¹-Pakets problemlos den zweiten (Standby-)Adapter konfigurieren. In HPCC-Anwendungen wurde Adapter-Teaming auf der Host-Seite weder getestet noch wird es unterstützt.

Erweiterte Funktionen

Bei der Bereitstellung des Clusters (Installation und Wiederherstellung von Compute-Knoten) wird PXE in großem Umfang verwendet. Teaming kommt normalerweise auf der Host-Seite nicht zum Einsatz und ist nicht Teil des Standardangebots von QLogic. Link Aggregation wird häufig zwischen Switches verwendet, insbesondere bei umfangreichen Konfigurationen. Jumbo-Rahmen sind nicht Bestandteil des Standardangebots von QLogic, können jedoch in einigen Anwendungen aufgrund der Reduzierung des CPU-Overheads zu Leistungsverbesserungen führen.

¹ Der Lösungsstapel zur Bereitstellung von Felix 3.1 ist in 32-Bit-HPCC-Konfigurationen von Dell integriert. Felix ist auf einer Zusammenarbeit von MPI Software Technologies Inc. (MSTI) und Dell entstanden.

Oracle

In den Oracle® Solution Stacks von QLogic wird Adapter-Teaming sowohl in privaten Netzwerken (Verbindung zwischen RAC-Knoten) als auch in öffentlichen Netzwerken mit Clients oder der Anwendungsebene über der Datenbankebene unterstützt, wie in [Abbildung 11-8](#) gezeigt.

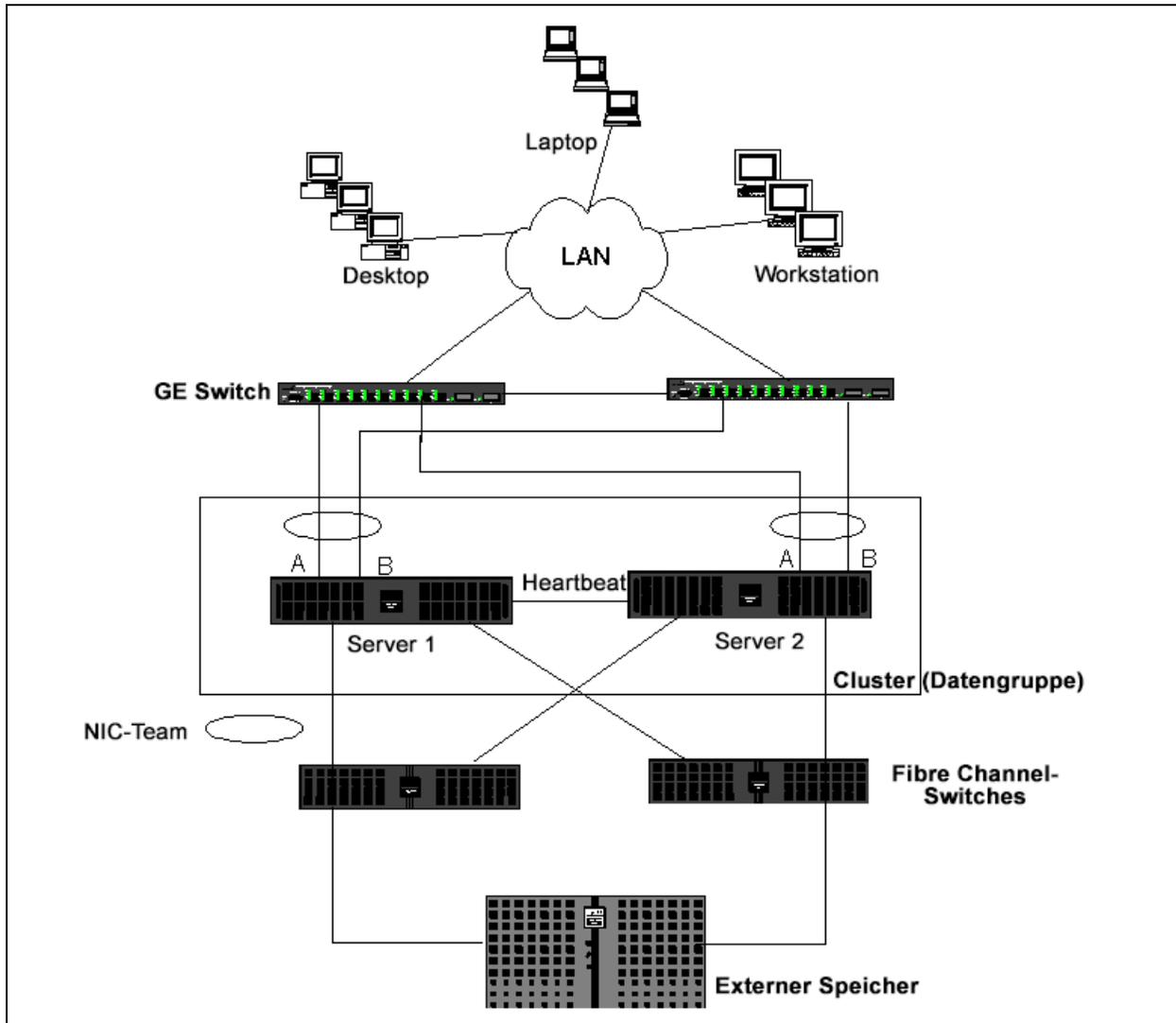


Abbildung 11-8. Clustering mit Teaming über zwei Switches

Teaming und Netzwerkbackup

Bei der Ausführung von Netzwerkbackups in einer Umgebung ohne Teams kann der Gesamtdurchsatz an einem Adapter auf einem Backupserver aufgrund des übermäßigen Datenverkehrs und der Adapterüberlastung leicht beeinträchtigt werden. Je nach Anzahl der Backupserver und Datenströme und in Abhängigkeit von der Bandlaufwerksgeschwindigkeit kann der Backupverkehr unter Umständen einen hohen Prozentsatz der Bandbreite der Netzverbindung beanspruchen und so die Produktionsdaten und die Backupleistung des Bands beeinflussen. Netzwerkbackups umfassen in der Regel einen speziellen Backupserver, der mit Bandbackup-Software wie NetBackup™ oder Backup Exec™ arbeitet. Der Backupserver ist entweder direkt mit einer SCSI-Bandeinheit verbunden, oder es ist eine Bandbibliothek über ein Fibre-Channel-SAN (Storage Area Network) angeschlossen. Über das Netzwerk gesicherte Systeme werden in der Regel als *Client*- oder *Remote*-Server bezeichnet. Normalerweise ist für solche Systeme ein Bandbackup-Softwareagent installiert. [Abbildung 11-9](#) zeigt eine typische 1-GBit/s-Netzwerkumgebung ohne Teams mit Bandbackup-Implementierung.

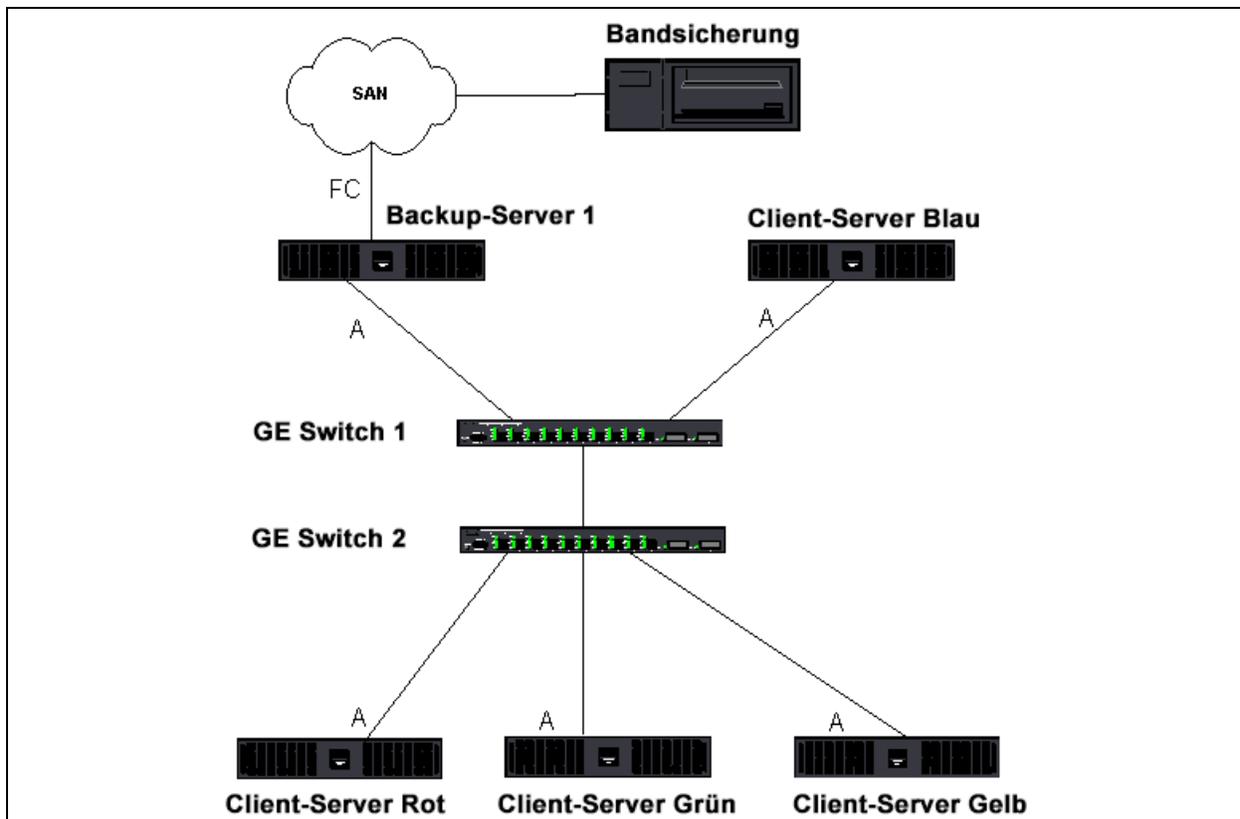


Abbildung 11-9. Netzwerkbackup ohne Teaming

Da es vier Client-Server gibt, kann der Backupserver simultan vier Backupjobs (einen pro Client) an einen Autoloader mit mehreren Laufwerken streamen. Da jedoch nur eine Verbindung zwischen dem Switch und dem Backupserver besteht, können Adapter und Verbindung bei einem Backup mit vier Datenströmen schnell ausgelastet werden. Wenn der Adapter auf dem Backupserver mit 1 GBit/s (125 MB/s) betrieben wird und jeder Client während des Bandbackups Daten mit 20 MB/s streamen kann, beträgt der Durchsatz zwischen Backupserver und Switch 80 MB/s ($20 \text{ MB/s} \times 4$), was 64 % der Netzbandbreite entspricht. Dieser Wert liegt zwar innerhalb des Bandbreitenbereichs des Netzwerks; 64 % stellen jedoch einen hohen Prozentsatz dar, wenn dieselbe Verbindung auch von anderen Anwendungen genutzt wird.

Die Informationen zu Teaming und Netzwerkbackup umfassen:

- [Lastausgleich und Failover](#)
- [Fehlertoleranz](#)

Lastausgleich und Failover

Mit zunehmender Zahl der Backup-Streams erhöht sich der Durchsatz insgesamt. Es ist jedoch möglich, dass nicht jeder Datenstrom in der Lage ist, dieselbe Leistung wie ein einzelner Backup-Stream mit 25 MB/s aufrecht zu erhalten. Mit anderen Worten: Obwohl ein Backupserver Daten von einem einzelnen Client mit 25 MB/s streamen kann, ist nicht damit zu rechnen, dass vier simultan ausgeführte Backupjobs Daten mit 100 MB/s ($25 \text{ MB/s} \times 4 \text{ Streams}$) streamen. Obgleich sich der Gesamtdurchsatz mit der Anzahl der Backup-Streams erhöht, können sich mit der Bandsoftware oder dem Netzwerkstapel verbundene Einschränkungen auf die einzelnen Backup-Streams auswirken.

Damit ein Bandbackup-Server beim Backup von Clients verlässlich von Adapterleistung und Netzwerkbandbreite Gebrauch macht, muss eine Netzwerkinfrastruktur Teaming-Funktionen wie Lastausgleich und Fehlertoleranz implementieren. Datenzentren beinhalten redundante Switches, Link Aggregation und Trunking im Rahmen ihrer fehlertoleranten Lösung. Obwohl Teaming-Gerätetreiber die Art des Datenflusses durch Team-Schnittstellen und Failover-Pfade manipulieren, ist dieser Vorgang für Bandbackup-Anwendungen transparent und führt nicht zur Unterbrechung der Bandbackup-Prozesse, wenn Remote-Systeme über das Netzwerk gesichert werden. [Abbildung 11-10 auf Seite 190](#) zeigt eine Netzwerktopologie, die Bandbackup in einer QLogic-Teamumgebung veranschaulicht und verdeutlicht, wie durch Smart Load Balancing Bandbackup-Daten über Team-Adapter einem *Lastausgleich* unterzogen werden können.

Der Client-Server kann zum Senden von Daten an den Backupserver vier Pfade verwenden; während des Datentransfers wird jedoch nur einer dieser Pfade zugewiesen. Einer der möglichen Pfade, die der Client-Server Red zum Senden von Daten an den Backupserver nutzen kann, wird im folgenden Beispiel gezeigt.

Beispielpfad: Client-Server Red sendet Daten über Adapter A, Switch 1 und Backupserver-Adapter A.

Der zugewiesene Pfad wird von zwei Faktoren bestimmt:

- ARP-Cache des Client-Servers verweist auf die MAC-Adresse des Backupservers. Diese Adresse wird durch den Lastausgleichalgorithmus für eingehenden Verkehr des QLogic Intermediate-Treibers bestimmt.
- Die physische Adapterschnittstelle am Client-Server Red wird zur Übertragung der Daten verwendet. Der Lastausgleichalgorithmus für ausgehenden Verkehr des QLogic Intermediate-Treibers bestimmt die Daten (siehe [„Ausgehender Verkehr“ auf Seite 158](#) und [„Eingehender Verkehr \(nur SLB\)“ auf Seite 159](#)).

Die Team-Schnittstelle auf dem Backupserver sendet ein unangefordertes G-ARP (Gratuitous Address Resolution Protocol) an den Client-Server Red, was wiederum dazu führt, dass der ARP-Cache des Client-Servers mit der MAC-Adresse des Backupservers aktualisiert wird. Das Lastausgleichverfahren in der Team-Schnittstelle bestimmt die MAC-Adresse, die im G-ARP eingebettet ist. Die ausgewählte MAC-Adresse ist im Wesentlichen das Ziel für den Datentransfer vom Client-Server.

Im Client-Server Red bestimmt der SLB-Teaming-Algorithmus, welche der beiden Adapterschnittstellen zur Datenübertragung verwendet wird. In diesem Beispiel werden Daten vom Client-Server Red an der Adapterschnittstelle A des Backupservers empfangen. Zur Veranschaulichung der SLB-Mechanismen bei Einwirkung einer zusätzlichen Datenlast an der Team-Schnittstelle stellen Sie sich ein Szenario vor, in dem der Backupserver einen zweiten Backupvorgang initiiert: einen zum Client-Server Red und einen zum Client-Server Blue. Die Route, die der Client-Server Blue zum Senden von Daten an den Backupserver verwendet, hängt von seinem ARP-Cache ab, der auf die MAC-Adresse des Backupservers verweist. Da der Adapter A des Backupservers bereits durch den Backupvorgang mit dem Client-Server Red belastet ist, ruft der Backupserver seinen SLB-Algorithmus auf, um den Client-Server Blue darüber zu *informieren* (durch ein G-ARP), seinen ARP-Cache mit der MAC-Adresse von Adapter B des Backupservers zu aktualisieren. Wenn der Client-Server Blue Daten übertragen muss, verwendet er eine der Adapterschnittstellen, die durch seinen eigenen SLB-Algorithmus bestimmt wird. Wichtig ist, dass die Daten vom Client-Server Blue von der Adapterschnittstelle B des Backupservers und nicht von der Adapterschnittstelle A empfangen werden. Diese Aktion ist deshalb von Bedeutung, da der Backupserver Datenströme von verschiedenen Clients einem *Lastausgleich* unterziehen muss, wenn beide Backup-Streams simultan laufen. Sind beide Backup-Streams aktiv, verarbeitet jede Adapterschnittstelle auf dem Backupserver die gleiche Last, sodass Daten über beide Adapterschnittstellen ausgeglichen werden.

Derselbe Algorithmus wird angewendet, wenn ein dritter und vierter Backupvorgang vom Backupserver eingeleitet wird. Die Team-Schnittstelle auf dem Backupserver sendet ein Unicast-G-ARP an Backup-Clients, um sie zur Aktualisierung ihres ARP-Cache zu veranlassen. Jeder Client überträgt dann Backupdaten entlang einer Route an die MAC-Adresse auf dem Backupserver.

Fehlertoleranz

Wenn eine Netzverbindung während des Bandbackups ausfällt, wird der gesamte Verkehr zwischen Backupserver und Client gestoppt und die Backupjobs schlagen fehl. Wurde jedoch die Netzwerktopologie sowohl für QLogic-SLB als auch für die Switch-Fehlertoleranz konfiguriert, können die Bandbackup-Vorgänge während des Verbindungsausfalls ohne Unterbrechung fortgesetzt werden. Alle Failover-Vorgänge innerhalb des Netzwerks sind für Bandbackup-Softwareanwendungen transparent.

Informationen dazu, wie Backup-Datenströme beim Netzwerk-Failover gelenkt werden, gibt die Topologie in [Abbildung 11-10](#). Der Client-Server Red überträgt über Pfad 1 Daten an den Backupserver, zwischen dem Backupserver und dem Switch kommt es jedoch zu einem Verbindungsausfall. Da die Daten nicht länger von Switch 1 an die Adapterschnittstelle A auf dem Backupserver gesendet werden können, werden sie von Switch 1 über Switch 2 an die Adapterschnittstelle B auf dem Backupserver umgeleitet. Diese Umleitung geschieht ohne Wissen der Backupanwendung, da alle fehlertoleranten Vorgänge von der Adapterteam-Schnittstelle und den Trunk-Einstellungen der Switches bewältigt werden. Aus der Perspektive des Client-Servers läuft der Betrieb genauso, als würden Daten über den Originalpfad gesendet.

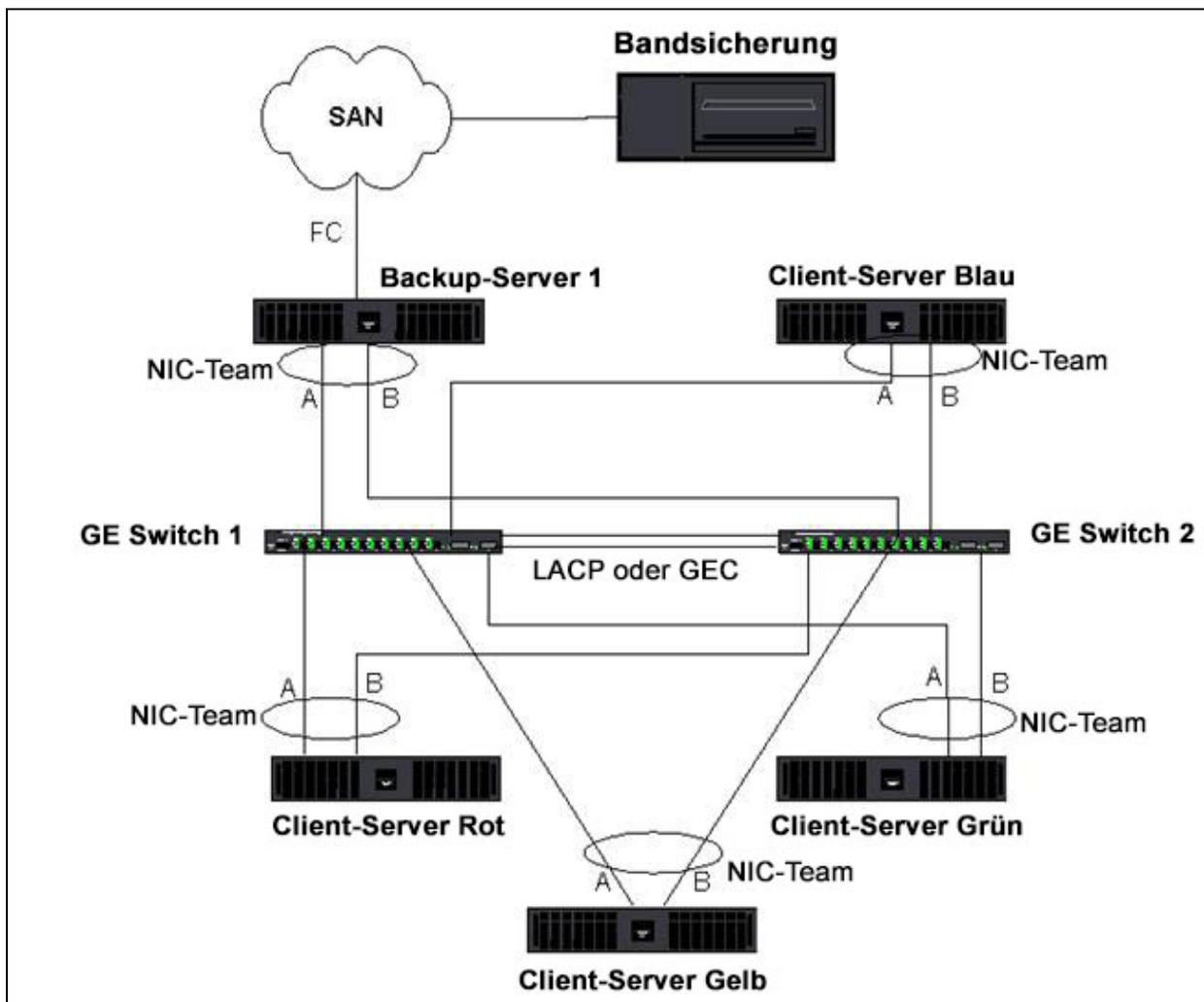


Abbildung 11-10. Netzwerkbakup mit SLB-Teaming über zwei Switches

Behebung von Teaming-Problemen

Bei Ausführung eines Protokollanalysators über einer Team-Schnittstelle eines virtuellen Adapters ist die in den gesendeten Rahmen angezeigte MAC-Adresse möglicherweise falsch. Der Analysator zeigt die Rahmen nicht so an, wie sie von QLASP konstruiert wurden; anstelle der MAC-Adresse der Schnittstelle, die den Rahmen überträgt, wird die MAC-Adresse des Teams angezeigt. QLogic empfiehlt folgendes Verfahren zur Überwachung eines Teams:

- Spiegeln Sie alle Uplink-Ports des Teams am Switch.
- Umfasst das Team zwei Switches, spiegeln Sie auch den Trunk, über den die Switches gekoppelt sind.

- Prüfen Sie alle Spiegel-Ports unabhängig voneinander.
- Verwenden Sie am Analysator einen Adapter und einen Treiber, der QoS- und VLAN-Daten nicht filtert.

Details zur Behebung von Teaming-Problemen werden behandelt in:

- [Tipps zur Teaming-Konfiguration](#)
- [Richtlinien für die Problembeseitigung](#)

Tipps zur Teaming-Konfiguration

Vergewissern Sie sich bei der Behebung von Problemen mit der Netzwerkanbindung oder mit Teaming-Funktionen, dass die folgenden Angaben auf Ihre Konfiguration zutreffen.

- Obwohl Dell SLB-Teaming mit verschiedenen Raten unterstützt, empfiehlt QLogic eine einheitliche Rate für alle Adapter in einem Team (entweder alle Gigabit Ethernet oder Fast Ethernet). Für Übertragungsraten von 10 GBit/s empfiehlt QLogic eine einheitliche Rate für alle Adapter in einem Team.
- Wenn LiveLink nicht aktiviert ist, deaktivieren Sie das Spanning Tree Protocol (STP), oder aktivieren Sie einen STP-Modus, der die Initialphasen für die mit einem Team verbundenen Switch-Ports umgeht (z. B. Port Fast, Edge Port).
- Alle Switches, mit denen das Team direkt verbunden ist, müssen dieselbe Hardware-, Firmware- und Softwareversion haben. Andernfalls ist keine Unterstützung gewährleistet.
- Adapter, die ein Team bilden sollen, müssen demselben VLAN angehören. Falls mehrere Teams konfiguriert werden, sollte sich jedes Team in einem separaten Netzwerk befinden.
- Weisen Sie niemals eine lokal verwaltete Adresse einem physischen Adapter zu, der dem Team angehört.
- Überprüfen Sie, ob die Energieverwaltung für alle physischen Mitglieder aller Teams deaktiviert wurde.
- Löschen Sie alle statischen IP-Adressen in den einzelnen physischen Teammitgliedern, bevor das Team erstellt wird.
- Ein Team, für das maximaler Durchsatz erforderlich ist, sollte LACP oder GEC\FEC verwenden. In diesen Fällen ist der Intermediate-Treiber nur verantwortlich für den Lastausgleich für ausgehenden Datenverkehr, während der Switch für den Lastausgleich für eingehenden Datenverkehr zuständig ist.

- Gebündelte Teams (802.3ad \ LACP und GEC\FEC) müssen an nur einen Switch angeschlossen werden, der IEEE 802.3a, LACP oder GEC/FEC unterstützt.
- Es wird von QLogic nicht empfohlen, ein Team an einen Hub anzuschließen, da Hubs nur den Halbduplex-Modus unterstützen. Hubs sollten nur zum Zweck der Problembehebung mit einem Team verbunden werden. Deaktivieren des Gerätetreibers eines Netzwerkadapters, der an einem LACP- oder GEC/FEC-Team teilnimmt, kann sich ungünstig auf die Netzwerkanbindung auswirken. QLogic empfiehlt, dass der Adapter erst physisch vom Switch getrennt wird, bevor der Gerätetreiber deaktiviert wird, um einen Verlust der Netzwerkverbindung zu vermeiden.
- Überprüfen Sie, ob die Basistreiber (Miniport) und Teamtreiber (Intermediate) demselben Versionspaket entstammen. Das Mischen von Basis- und Teaming-Treibern aus verschiedenen Versionen wird von Dell nicht unterstützt. Auch diesbezügliche Tests wurden von Dell nicht durchgeführt.
- Testen Sie vor dem Einsatz in eine Produktionsumgebung die Konnektivität für jeden physischen Adapter vor dem Teaming.
- Testen Sie das Failover- und Fallback-Verhalten des Teams.
- Beim Übergang von einem Nicht-Produktionsnetzwerk zu einem Produktionsnetzwerk wird dringend empfohlen, erneut Failover- und Fallback-Tests durchzuführen.
- Testen Sie das Leistungsverhalten des Teams, bevor Sie es in einer Produktionsumgebung einsetzen.
- Netzwerk-Teaming wird nicht unterstützt, wenn der iSCSI-Datenverkehr über den Microsoft iSCSI Initiator oder iSCSI-Offload erfolgt. Für diese Ports sollte stattdessen MPIO und nicht QLogic-Netzwerk-Teaming verwendet werden.
- Weitere Informationen zu iSCSI-Boot und iSCSI-Offload-Einschränkungen finden Sie unter [Kapitel 10 iSCSI-Protokoll](#).

Richtlinien für die Problembehebung

Bevor Sie sich an den Support von Dell wenden, stellen Sie sicher, dass Sie die folgenden Schritte zur Behebung von Problemen mit der Netzwerkanbindung ausgeführt haben, wenn auf dem Server Adapter-Teaming verwendet wird.

1. Stellen Sie sicher, dass das Verbindungssignal für alle Adapter leuchtet und dass alle Kabel angeschlossen sind.
2. Überprüfen Sie, ob die passenden Basis- und Intermediate-Treiber derselben Dell-Version angehören und ordnungsgemäß geladen sind.

3. Überprüfen Sie mit dem Windows-Befehl `ipconfig`, ob eine gültige IP-Adresse vorhanden ist.
4. Überprüfen Sie, ob an den Switch-Ports, die mit dem Team verbunden sind, STP deaktiviert oder Edge Port oder Port Fast aktiviert ist oder ob LiveLink verwendet wird.
5. Überprüfen Sie, ob die Konfiguration von Adaptern und Switch für die Übertragungsrates und Duplex übereinstimmt.
6. Wenn möglich, lösen Sie das Team auf, und überprüfen Sie die Konnektivität für alle Adapter unabhängig voneinander, um festzustellen, ob das Problem in direktem Zusammenhang mit dem Teaming steht.
7. Überprüfen Sie, ob alle mit dem Team verbundenen Switch-Ports sich im selben VLAN befinden.
8. Überprüfen Sie, ob die Switch-Ports korrekt für die Teamart Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static konfiguriert sind und ob dies der Teamart des Adapters entspricht. Wenn das System für ein Team der Art SLB konfiguriert ist, stellen Sie sicher, dass die entsprechenden Switch-Ports *nicht* für die Teamart Allgemeines Trunking (FEC/GEC)/802.3ad-Draft Static konfiguriert wurden.

Häufig gestellte Fragen

Frage: Unter welchen Bedingungen wird der Datenverkehr keinem Lastausgleich unterzogen? Warum wird nicht sämtlicher Datenverkehr gleichmäßig über die Teammitglieder verteilt?

Antwort: Der größte Teil des Datenverkehrs verwendet nicht IP, TCP oder UDP, oder der Großteil der Clients befindet sich in einem anderen Netzwerk. Receive Load Balancing (RLB) ist keine Funktion der Datenverkehrslast, sondern eine Funktion der Anzahl der Clients, die mit dem Server verbunden sind.

Frage: Für welche Netzwerkprotokolle erfolgt in einem Team ein Lastausgleich?

Antwort: Die Teaming-Software von QLogic unterstützt nur IP-, TCP- und UDP-Datenverkehr. Der übrige Datenverkehr wird an den Primäradapter weitergeleitet.

Frage: Für welche Protokolle erfolgt ein Lastausgleich mit SLB und für welche nicht?

Antwort: Nur für IP-, TCP- und UDP-Protokolle erfolgt ein Lastausgleich in beide Richtungen, also beim Senden und beim Empfangen. IPX wird nur für den gesendeten Datenverkehr ausgeglichen.

Frage: Kann ich einen Port mit 100 MBit/s und einen Port mit 1000 MBit/s in einem Team zusammenfassen?

Antwort: Das Mischen von Übertragungsraten innerhalb eines Teams wird nur bei der Teamart „Smart Load Balancing“ und bei 802.3ad-Teams unterstützt.

Frage: Kann ich ein Team aus einem Fiber-Adapter und einem kupferkabelbasierten GbE-Adapter bilden?

Antwort: In der Teamart SLB ist dies möglich. Es ist auch möglich, wenn der Switch dies für FEC und GEC und 802.3ad unterstützt.

Frage: Worin besteht der Unterschied zwischen dem Lastausgleich über Adapter und Network Load Balancing von Microsoft?

Antwort: Der Lastausgleich über Adapter findet auf der Ebene der Netzwerksitzung statt, während Network Load Balancing auf der Ebene der Serveranwendung ausgeführt wird.

Frage: Kann ich die Team-Adapter an einen Hub anschließen?

Antwort: Team-Ports können nur zum Zweck der Problembhebung an einen Hub angeschlossen werden. Dieses Vorgehen wird jedoch für den Normalbetrieb nicht empfohlen, da es aufgrund der Hub-Einschränkungen zu Beeinträchtigungen der Leistung kommen würde. Verbinden Sie die Team-Ports stattdessen mit einem Switch.

Frage: Kann ich die Team-Adapter an die Ports eines Routers anschließen?

Antwort: Nein. Alle Ports in einem Team müssen sich im selben Netzwerk befinden, in einem Router bildet jedoch jeder Port per Definition ein separates Netzwerk. In allen Teaming-Modi muss der Verbindungspartner ein Schicht-2-Switch sein.

Frage: Kann ich Teaming mit Microsoft Cluster Services einsetzen?

Antwort: Ja. Teaming wird nur im öffentlichen Netzwerk unterstützt, nicht im privaten Netzwerk, das für die Heartbeat-Verbindung verwendet wird.

Frage: Funktioniert PXE über einen virtuellen Adapter (Team)?

Antwort: Ein PXE-Client wird in einer Umgebung verwendet, in der noch kein Betriebssystem geladen ist, folglich wurden noch keine virtuellen Adapter aktiviert. Wenn der physische Adapter PXE unterstützt, kann er als PXE-Client verwendet werden, unabhängig davon, ob er Teil eines virtuellen Adapters ist, wenn das Betriebssystem geladen wird. PXE-Server können über einen virtuellen Adapter betrieben werden.

Frage: Funktioniert WoL über einen virtuellen Adapter (Team)?

Antwort: Die WoL-Funktion (Wake On LAN) wird in einer Umgebung verwendet, in der noch kein Betriebssystem geladen ist. WoL tritt auf, wenn das System ausgeschaltet ist oder sich im Standby-Modus befindet, es ist also kein Team konfiguriert.

Frage: Wie viele Ports können maximal zu einem Team zusammengefasst werden?

Antwort: Einem Team können bis zu 16 Ports zugewiesen werden, von denen ein Port Mitglied des Standby-Teams sein kann.

Frage: Wie viele Teams können maximal auf demselben Server konfiguriert werden?

Antwort: Auf einem Server können bis zu 16 Teams konfiguriert werden.

Frage: Warum geht bei meinem Team in den ersten 30 bis 50 Sekunden nach der Wiederherstellung des primären Adapters (Fallback) die Verbindung verloren?

Antwort: Dies liegt daran, dass der Port durch das Spanning Tree Protocol vom blockierten Zustand in den weiterleitenden Zustand versetzt wird. Sie müssen auf den Switch-Ports, die mit dem Team verbunden sind, Port Fast oder Edge Port aktivieren oder LiveLink verwenden, um die STP-Verzögerung zu berücksichtigen.

Frage: Kann ich ein Team über mehrere Switches hinweg verbinden?

Antwort: Smart Load Balancing eignet sich für den Einsatz mit mehreren Switches, da jeder physische Adapter im System eine eindeutige Ethernet-MAC-Adresse verwendet. Link Aggregation und Allgemeines Trunking können nicht über mehrere Switches eingerichtet werden, da hier alle physischen Adapter dieselbe Ethernet MAC-Adresse haben müssen.

Frage: Wie kann ich den Intermediate-Treiber (QLASP) aktualisieren?

Antwort: Der Intermediate-Treiber kann nicht über „Local Area Connection Properties“ (LAN-Verbindungseigenschaften) aktualisiert werden. Die Aktualisierung muss über das Setup-Installationsprogramm erfolgen.

Frage: Wie kann ich eine Leistungsstatistik für einen virtuellen Adapter (Team) erstellen lassen?

Antwort: Klicken Sie in QLogic Control Suite auf die Registerkarte **Statistics** (Statistik) für den virtuellen Adapter.

Frage: Kann ich Network Load Balancing und Teaming gleichzeitig konfigurieren?

Antwort: Ja, allerdings nur, wenn Network Load Balancing in einem Multicast-Modus ausgeführt wird (Network Load Balancing wird von MS Cluster Services nicht unterstützt).

Frage: Sollte sowohl für den Backupserver als auch für die Client-Server, die gesichert werden, Adapter-Teaming verwendet werden?

Antwort: Da die Datenlast für den Backupserver am höchsten ist, sollte bei diesem für Link Aggregation und Failover stets Adapter-Teaming verwendet werden. Ein vollständig redundantes Netzwerk erfordert jedoch Teaming sowohl für Switches als auch Backup-Clients für Fehlertoleranz und Link Aggregation.

Frage: Führt der Adapter-Teaming-Algorithmus bei Backupvorgängen den Lastausgleich für Daten auf Byte-Ebene oder auf Sitzungsebene durch?

Antwort: Bei Verwendung von Adapter-Teaming wird die Datenlast nur auf Sitzungsebene und nicht auf Byte-Ebene ausgeglichen, damit Frames in ungeordneter Reihenfolge vermieden werden. Lastausgleich bei Adapter-Teaming funktioniert nicht in derselben Weise wie andere Lastausgleichsverfahren (z. B. EMC PowerPath).

Frage: Ist für die Bandbackup-Software oder -Hardware eine besondere Konfiguration erforderlich, damit sie mit Adapter-Teaming funktioniert?

Antwort: Es ist keine besondere Konfiguration der Bandbackup-Software erforderlich, damit sie mit Teaming funktioniert. Teaming ist für Bandbackup-Anwendungen transparent.

Frage: Woher weiß ich, welchen Treiber ich derzeit verwende?

Antwort: Die exakte Methode zum Überprüfen der Treiberversion ist in allen Betriebssystemen identisch: Suchen Sie die eigentliche Treiberdatei und überprüfen Sie die Eigenschaften.

Frage: Kann SLB einen Switch-Ausfall in einer Konfiguration mit Switch-Fehlertoleranz erkennen?

Antwort: Nein. SLB kann nur den Verbindungsverlust zwischen dem Team-Port und seinem unmittelbaren Verbindungspartner erkennen. Verbindungsausfälle an anderen Ports kann SLB nicht erkennen.

Frage: Wo erhalte ich die neuesten unterstützten Treiber?

Antwort: Aktualisierungen für Treiberpakete und Support-Dokumente finden Sie auf der Support-Website von Dell unter <http://support.dell.com>.

Frage: Warum geht bei meinem Team in den ersten 30 bis 50 Sekunden nach der Wiederherstellung des primären Adapters (Fallback nach Failover) die Verbindung verloren?

Antwort: Während eines Fallbacks wird die Verbindung wiederhergestellt und Spanning Tree Protocol konfiguriert den Port für den blockierten Zustand, bis in den weiterleitenden Zustand gewechselt werden kann. Sie müssen auf den Switch-Ports, die mit dem Team verbunden sind, Port Fast oder Edge Port aktivieren, um durch STP verursachte Kommunikationsverluste zu verhindern.

Frage: Wo kann ich Echtzeitstatistiken für ein Adapter-Team auf einem Windows-Server überwachen?

Antwort: Verwenden Sie QLogic Control Suite (QCS) zur Überwachung allgemeiner, IEEE 802.3- und benutzerdefinierter Leistungsindikatoren.

Frage: Welche Leistungsmerkmale werden bei einem herstellerunabhängigen Team nicht unterstützt?

Antwort: VLAN-Markierung und RSS werden bei einem herstellerunabhängigen Team nicht unterstützt.

Ereignisprotokollmeldungen

Zu den Ereignisprotokollmeldungen zählen Folgende:

- [Ereignisprotokollmeldungen unter Windows](#)
- [Basistreiber \(Physischer Adapter oder Miniport\)](#)
- [Intermediate-Treiber \(Virtueller Adapter oder Team\)](#)
- [Virtual Bus Driver \(VBD\)](#)

Ereignisprotokollmeldungen unter Windows

Die bekannten Ereignisprotokoll-Statusmeldungen für Basis- und Intermediate-Treiber in Windows-Systemen für QLogic BCM57xx und BCM57xxx-Adapter sind in [Tabelle 11-8 auf Seite 198](#) und [Tabelle 11-9 auf Seite 203](#) aufgeführt. Beim Laden eines QLogic-Adaptertreibers zeigt Windows einen Statuscode in der Ereignisanzeige des Systems an. Für diese Ereigniscodes kann es bis zu zwei Klassen von Einträgen geben, je nachdem, ob beide Treiber geladen werden (ein Satz für den Basis- oder Miniport-Treiber und ein Satz für den Intermediate- oder Teaming-Treiber).

Basistreiber (Physischer Adapter oder Miniport)

Der Basistreiber wird durch die Quelle **L2ND** gekennzeichnet. [Tabelle 11-8](#) listet die Ereignisprotokollmeldungen auf, die vom Basistreiber unterstützt werden, erläutert die Ursache der jeweiligen Meldung und informiert über die empfohlenen Maßnahmen.

ANMERKUNG

In [Tabelle 11-8](#) gelten Meldungen mit Nummer 1 bis 17 für die Treiber NDIS 5.x und NDIS 6.x, Meldungen mit Nr. 18 bis 23 gelten nur für den Treiber NDIS 6.x.

Tabelle 11-8. Ereignisprotokollmeldungen für Basistreiber

Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
1	Fehler	Failed to allocate memory for the device block. (Speicher für Geräteblock konnte nicht zugewiesen werden.) Überprüfen Sie die Auslastung der Systemspeicherressourcen.	Der Treiber kann keinen Betriebssystemspeicher zuweisen.	Schließen Sie laufende Anwendungen, um Speicher freizugeben.
2	Fehler	Failed to allocate map registers. (Es konnten keine Map-Register zugewiesen werden.)	Der Treiber kann aus dem Betriebssystem keine Map-Register zuordnen.	Entfernen Sie andere Treiber, die möglicherweise Map-Register zuordnen.
3	Fehler	Failed to access configuration information. (Auf die Konfigurationsdaten konnte nicht zugegriffen werden.) Installieren Sie den Netzwerktreiber neu.	Der Treiber kann nicht auf die PCI-Konfigurationsregister auf dem Adapter zugreifen.	Bei zusätzlichen Adaptern: Setzen Sie den Adapter erneut in den Steckplatz ein, wählen Sie einen anderen PCI-Steckplatz für den Adapter aus, oder tauschen Sie den Adapter aus.
4	Warnung	The network link is down. (Die Netzwerkverbindung ist nicht aktiv.) Überprüfen Sie, ob das Netzkabel richtig angeschlossen ist.	Der Adapter hat die Verbindung zum Verbindungspartner verloren.	Überprüfen Sie, ob das Netzkabel angeschlossen und vom richtigen Typ ist und ob der Verbindungspartner (z. B. Switch oder Hub) korrekt funktioniert.
5	Zur Information	The network link is up. (Die Netzwerkverbindung ist aktiv.)	Der Adapter hat eine Verbindung hergestellt.	Keine Maßnahme erforderlich.

Tabelle 11-8. Ereignisprotokollmeldungen für Basistreiber (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
6	Zur Information	Network controller configured for 10Mb half-duplex link. (Netzwerkcontroller ist für 10-Mb-Halbduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
7	Zur Information	Network controller configured for 10Mb full-duplex link. (Netzwerkcontroller ist für 10-Mb-Vollduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
8	Zur Information	Network controller configured for 100Mb half-duplex link. (Netzwerkcontroller ist für 100-Mb-Halbduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
9	Zur Information	Network controller configured for 100Mb full-duplex link. (Netzwerkcontroller ist für 100-Mb-Vollduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.

Tabelle 11-8. Ereignisprotokollmeldungen für Basistreiber (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
10	Zur Information	Network controller configured for 1Gb half-duplex link. (Netzwerkcontroller ist für 1-Gb-Halbduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
11	Zur Information	Network controller configured for 1Gb full-duplex link. (Netzwerkcontroller ist für 1-Gb-Vollduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
12	Zur Information	Network controller configured for 2.5 Gb full-duplex link. (Netzwerkcontroller ist für 2.5 Gb full-duplex link konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
13	Fehler	Medium not supported. (Medium wird nicht unterstützt.)	Das IEEE 802.3-Medium wird vom Betriebssystem nicht unterstützt.	Starten Sie das Betriebssystem neu, führen Sie eine Virenüberprüfung durch, führen Sie eine Festplattenüberprüfung durch (chkdsk), und installieren Sie das Betriebssystem neu.
14	Fehler	Unable to register the interrupt service routine. (Interrupt Service Routine konnte nicht registriert werden.)	Der Gerätetreiber kann den Interrupt-Handler nicht installieren.	Starten Sie das Betriebssystem neu. Entfernen Sie andere Gerätetreiber, die u. U. dieselbe IRQ verwenden.

Tabelle 11-8. Ereignisprotokollmeldungen für Basistreiber (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
15	Fehler	Unable to map IO space. (IO-Space kann nicht zugewiesen werden.)	Der Gerätetreiber kann keine im Speicher abgebildete Ein-/Ausgabe (I/O) für den Zugriff auf Treiberregister zuweisen.	Entfernen Sie andere Adapter aus dem System, verringern Sie die Menge des installierten physischen Speichers, und tauschen Sie den Adapter aus.
16	Zur Information	Driver initialized successfully. (Treiber wurde erfolgreich initialisiert.)	Der Treiber wurde erfolgreich geladen.	Keine Maßnahme erforderlich.
17	Zur Information	NDIS is resetting the miniport driver. (NDIS setzt den Miniport-Treiber zurück.)	Die NDIS-Schicht hat ein Problem beim Senden/Empfangen von Paketen entdeckt und setzt den Treiber zurück, um das Problem zu lösen.	Führen Sie das QLogic Control Suite-Diagnoseprogramm aus; überprüfen Sie das Netzkabel auf Beschädigungen.
18	Fehler	Unknown PHY detected. (Unbekannte PHY entdeckt.) Es wird eine Standard-Routine zur PHY-Initialisierung verwendet.	Der Treiber konnte die PHY-ID nicht lesen.	Tauschen Sie den Adapter aus.
19	Fehler	This driver does not support this device. (Der Treiber bietet keine Unterstützung für dieses Gerät.) Aktualisieren Sie auf den neuesten Treiber.	Der Treiber erkennt den installierten Adapter nicht.	Aktualisieren Sie auf eine Treiberversion, die diesen Adapter unterstützt.

Tabelle 11-8. Ereignisprotokollmeldungen für Basistreiber (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
20	Fehler	Driver initialization failed. (Treiberinitialisierung fehlgeschlagen.)	Unspezifizierter Fehler bei der Treiberinitialisierung.	Installieren Sie den Treiber neu, aktualisieren Sie auf eine aktuellere Treiberversion, führen Sie das QLogic Control Suite-Diagnoseprogramm aus oder tauschen Sie den Adapter aus.
21	Zur Information	Network controller configured for 10 Gb full-duplex link. (Netzwerkcontroller ist für 10 Gb full-duplex link konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
22	Fehler	Network controller failed initialization because it cannot allocate system memory. (Der Netzwerkcontroller konnte nicht initialisiert werden, da er keinem Systemspeicher zugeordnet werden konnte.)	Der Treiber konnte aufgrund von zu wenig Systemspeicher nicht initialisiert werden.	Systemspeicher erhöhen.
23	Fehler	Network controller failed to exchange the interface with the bus driver. (Der Netzwerkcontroller konnte die Schnittstelle nicht mit dem Bus-Treiber austauschen.)	Treiber und Bus-Treiber sind nicht kompatibel.	Installieren Sie den neuesten Treibersatz und achten Sie darauf, dass die Haupt- und Unterversionen für NDIS und Bus-Treiber übereinstimmen.

Intermediate-Treiber (Virtueller Adapter oder Team)

Der Zwischentreiber ist durch die Quelle **BLFM** gekennzeichnet, unabhängig von der Revision des Basistreibers. [Tabelle 11-9](#) listet die Ereignisprotokollmeldungen auf, die vom Intermediate-Treiber unterstützt werden, erläutert die Ursache der jeweiligen Meldung und informiert über die empfohlenen Maßnahmen.

Tabelle 11-9. Ereignisprotokollmeldungen für Intermediate-Treiber

Systemereignis-Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
1	Zur Information	Event logging enabled for QLASP driver. (Ereignisprotokollierung für QLASP-Treiber aktiviert.)	–	Keine Maßnahme erforderlich.
2	Fehler	Unable to register with NDIS. (Registrierung an NDIS nicht möglich.)	Der Treiber kann sich nicht an der NDIS-Schnittstelle registrieren.	Entfernen Sie andere NDIS-Treiber.
3	Fehler	Unable to instantiate the management interface. (Managementschnittstelle konnte nicht instanziiert werden.)	Der Treiber kann keine Geräteinstanz erstellen.	Starten Sie das Betriebssystem neu.
4	Fehler	Unable to create symbolic link for the management interface. (Es konnte keine symbolische Verknüpfung für die Managementschnittstelle erstellt werden.)	Ein anderer Treiber hat einen Gerätenamen erstellt, der potentiell Konflikte verursacht.	Entfernen Sie den Gerätetreiber, der den Namen <i>Bif</i> verwendet und potentiell Konflikte verursacht.
5	Zur Information	QLASP Driver has started. (QLASP-Treiber wurde gestartet.)	Der Treiber wurde gestartet.	Keine Maßnahme erforderlich.
6	Zur Information	QLASP Driver has stopped. (QLASP-Treiber wurde angehalten.)	Der Treiber wurde angehalten.	Keine Maßnahme erforderlich.

Tabelle 11-9. Ereignisprotokollmeldungen für Intermediate-Treiber (fortgesetzt)

Systemereignismeldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
7	Fehler	Could not allocate memory for internal data structures. (Es konnte kein Speicher für interne Datenstrukturen zugewiesen werden.)	Der Treiber kann keinen Betriebssystemspeicher zuweisen.	Schließen Sie laufende Anwendungen, um Speicher freizugeben.
8	Warnung	Could not bind to adapter. (Bindung an Adapter nicht möglich.)	Der Treiber konnte keinen der physischen Adapter im Team öffnen.	Entfernen Sie und laden Sie den Treiber des physischen Adapters neu, installieren Sie einen aktualisierten Treiber für den physischen Adapter, oder tauschen Sie den physischen Adapter aus.
9	Zur Information	Successfully bind to adapter. (Bindung an Adapter erfolgreich.)	Der Treiber hat den physischen Adapter geöffnet.	Keine Maßnahme erforderlich.
10	Warnung	Network adapter is disconnected. (Netzwerkadapter ist getrennt.)	Der physische Adapter ist nicht mit dem Netzwerk verbunden (es wurde keine Verbindung hergestellt).	Überprüfen Sie, ob das Netzkabel angeschlossen und vom richtigen Typ ist und ob der Verbindungspartner (Switch oder Hub) korrekt funktioniert.
11	Zur Information	Network adapter is connected. (Netzwerkadapter ist verbunden.)	Der physische Adapter ist mit dem Netzwerk verbunden (es wurde eine Verbindung hergestellt).	Keine Maßnahme erforderlich.

Tabelle 11-9. Ereignisprotokollmeldungen für Intermediate-Treiber (fortgesetzt)

Systemereignis-Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
12	Fehler	QLASP Features Driver is not designed to run on this version of operating system. (Funktionstreiber wurde nicht dazu konzipiert, auf dieser Betriebssystemversion ausgeführt zu werden.)	Der Treiber bietet keine Unterstützung für das Betriebssystem, auf dem er installiert wurde.	Lesen Sie in den Versionshinweisen zum Treiber nach, und installieren Sie den Treiber unter einem unterstützten Betriebssystem, oder aktualisieren Sie den Treiber.
13	Zur Information	Hot-standby adapter is selected as the primary adapter for a team without a load balancing adapter. (Hot-Standby-Adapter ist als primärer Adapter für ein Team ohne einen Adapter für Lastausgleich ausgewählt.)	Es wurde ein Standby-Adapter aktiviert.	Ersetzen Sie den ausgefallenen physischen Adapter.
14	Zur Information	Network adapter does not support Advanced Failover. (Netzwerkadapter bietet keine Unterstützung für erweitertes Failover.)	Der physikalische Adapter unterstützt die QLogic NIC-Erweiterung (NICE) nicht.	Ersetzen Sie den Adapter durch einen anderen, der NICE unterstützt.
15	Zur Information	Network adapter is enabled through management interface. (Der Netzwerkadapter ist durch die Managementschnittstelle aktiviert.)	Der Treiber hat erfolgreich einen physischen Adapter über die Managementschnittstelle aktiviert.	Keine Maßnahme erforderlich.

Tabelle 11-9. Ereignisprotokollmeldungen für Intermediate-Treiber (fortgesetzt)

Systemereignis-Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
16	Warnung	Network adapter is disabled through management interface. (Der Netzwerkadapter ist durch die Managementschnittstelle deaktiviert.)	Der Treiber hat erfolgreich einen physischen Adapter über die Managementschnittstelle deaktiviert.	Keine Maßnahme erforderlich.
17	Zur Information	Network adapter is activated and is participating in network traffic. (Netzwerkadapter wurde aktiviert und nimmt am Netzwerkverkehr teil.)	Ein physischer Adapter wurde dem Team hinzugefügt oder in einem Team aktiviert.	Keine Maßnahme erforderlich.
18	Zur Information	Network adapter is deactivated and is no longer participating in network traffic. (Der Netzwerkadapter ist deaktiviert und nimmt nicht mehr am Netzwerkverkehr teil.)	Der Treiber erkennt den installierten Adapter nicht.	Keine Maßnahme erforderlich.
19	Zur Information	The LiveLink feature in QLASP connected the link for the network adapter. (Die LiveLink-Funktion in QLASP hat die Verbindung für den Netzwerkadapter hergestellt.)	Die Verbindung zu den Remote-Zielen für das für LiveLink aktivierte Teammitglied wurde aufgebaut oder wiederhergestellt.	Keine Maßnahme erforderlich.

Tabelle 11-9. Ereignisprotokollmeldungen für Intermediate-Treiber (fortgesetzt)

Systemereignismeldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
20	Zur Information	The LiveLink feature in QLASP disconnected the link for the network adapter. (Die LiveLink-Funktion in QLASP hat die Verbindung für den Netzwerkadapter unterbrochen.)	Das für LiveLink aktivierte Teammitglied kann keine Verbindung zu den Remote-Zielen herstellen.	Keine Maßnahme erforderlich.

Virtual Bus Driver (VBD)

In [Tabelle 11-10](#) sind VBD-Ereignisprotokollmeldungen aufgeführt.

Tabelle 11-10. Virtual Bus Driver (VBD)-Ereignisprotokollmeldungen

Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
1	Fehler	Failed to allocate memory for the device block. (Speicher für Geräteblock konnte nicht zugewiesen werden.) Überprüfen Sie die Auslastung der Systemspeicherressourcen.	Der Treiber kann keinen Betriebssystemspeicher zuweisen.	Schließen Sie laufende Anwendungen, um Speicher freizugeben.
2	Zur Information	The network link is down. (Die Netzwerkverbindung ist nicht aktiv.) Überprüfen Sie, ob das Netzkabel richtig angeschlossen ist.	Der Adapter hat die Verbindung zum Verbindungspartner verloren.	Überprüfen Sie, ob das Netzkabel angeschlossen und vom richtigen Typ ist und ob der Verbindungspartner (z. B. Switch oder Hub) korrekt funktioniert.

Tabelle 11-10. Virtual Bus Driver (VBD)-Ereignisprotokollmeldungen (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
3	Zur Information	The network link is up. (Die Netzwerkverbindung ist aktiv.)	Der Adapter hat eine Verbindung hergestellt.	Keine Maßnahme erforderlich.
4	Zur Information	Network controller configured for 10Mb half-duplex link. (Netzwerkcontroller ist für 10-Mb-Halbduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
5	Zur Information	Network controller configured for 10Mb full-duplex link. (Netzwerkcontroller ist für 10-Mb-Vollduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
6	Zur Information	Network controller configured for 100Mb half-duplex link. (Netzwerkcontroller ist für 100-Mb-Halbduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
7	Zur Information	Network controller configured for 100Mb full-duplex link. (Netzwerkcontroller ist für 100-Mb-Vollduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.

Tabelle 11-10. Virtual Bus Driver (VBD)-Ereignisprotokollmeldungen (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
8	Zur Information	Network controller configured for 1Gb half-duplex link. (Netzwerkcontroller ist für 1-Gb-Halbduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
9	Zur Information	Network controller configured for 1Gb full-duplex link. (Netzwerkcontroller ist für 1-Gb-Vollduplex-Verbindung konfiguriert.)	Der Adapter wurde manuell für die ausgewählte Übertragungsrate und die ausgewählten Duplexeinstellungen konfiguriert.	Keine Maßnahme erforderlich.
10	Fehler	Unable to register the interrupt service routine. (Interrupt Service Routine konnte nicht registriert werden.)	Der Gerätetreiber kann den Interrupt-Handler nicht installieren.	Starten Sie das Betriebssystem neu. Entfernen Sie andere Gerätetreiber, die u. U. dieselbe IRQ verwenden.
11	Fehler	Unable to map IO space. (IO-Space kann nicht zugewiesen werden.)	Der Gerätetreiber kann keine im Speicher abgebildete Ein-/Ausgabe (I/O) für den Zugriff auf Treiberregister zuweisen.	Entfernen Sie andere Adapter aus dem System, verringern Sie die Menge des installierten physischen Speichers, und tauschen Sie den Adapter aus.
12	Zur Information	Driver initialized successfully. (Treiber wurde erfolgreich initialisiert.)	Der Treiber wurde erfolgreich geladen.	Keine Maßnahme erforderlich.

Tabelle 11-10. Virtual Bus Driver (VBD)-Ereignisprotokollmeldungen (fortgesetzt)

Meldungsnummer	Schweregrad	Meldung	Ursache	Korrekturmaßnahme
13	Fehler	Driver initialization failed. (Treiberinitialisierung fehlgeschlagen.)	Unspezifizierter Fehler bei der Treiberinitialisierung.	Installieren Sie den Treiber neu, aktualisieren Sie auf eine aktuellere Treiberversion, führen Sie das QLogic Control Suite-Diagnoseprogramm aus oder tauschen Sie den Adapter aus.
14	Fehler	This driver does not support this device. (Der Treiber bietet keine Unterstützung für dieses Gerät.) Aktualisieren Sie auf den neuesten Treiber.	Der Treiber erkennt den installierten Adapter nicht.	Aktualisieren Sie auf eine Treiberversion, die diesen Adapter unterstützt.
15	Fehler	This driver fails initialization because the system is running out of memory. (Dieser Treiber kann nicht initialisiert werden, weil das System nicht genug Arbeitsspeicher hat.)	Der Treiber konnte aufgrund von zu wenig Systempeicher nicht initialisiert werden.	Systemspeicher erhöhen.

12 NIC-Partitionierung und Bandbreitenverwaltung

Die in diesem Kapitel behandelte NIC-Partitionierung und Bandbreitenverwaltung umfasst folgende Angaben:

- [Übersicht](#)
- [„Konfigurieren der NIC-Partitionierung“ auf Seite 212](#)

Übersicht

Durch die NIC-Partitionierung (NPAR) wird ein QLogic BCM57xx und BCM57xxx 10 Gigabit Ethernet-NIC in mehrere virtuelle NICs aufgeteilt, indem mehrere physische PCI-Funktionen pro Port zur Verfügung stehen. Jede PCI-Funktion ist einem anderen virtuellen NIC zugeordnet. Für das Betriebssystem und das Netzwerk erscheinen die einzelnen physischen Funktionen als separate NIC-Ports.

Die Anzahl der Partitionen für die einzelnen Ports kann im Bereich zwischen 1 und 4 liegen. Ein Dual-Port-NIC kann damit maximal acht Partitionen haben. Jede Partition verhält sich wie ein unabhängiger NIC-Port.

Vorteile des partitionierten 10 G-NIC:

- Weniger Kabel und Ports, wenn er eingesetzt wird, um eine Vielzahl von 1 G-NICs zu ersetzen.
- Serversegmentierung mit separaten Subnetzen und VLANs.
- Hohe Serververfügbarkeit mit NIC-Failover und NIC-Verbindungsbandbreitenaggregation.
- Server-I/O-Virtualisierung mit virtuellem Betriebssystem und Unterstützung für monolithisches Betriebssystem.
- Es sind keine Änderungen am Betriebssystem erforderlich.
- Switch-unabhängiger Teaming-Typ wird unterstützt.

Unterstützte Betriebssysteme für die NIC-Partitionierung

NIC-Partitionierung wird von den QLogicBCM57xx und BCM57xxx 10 Gigabit Ethernet-Adaptoren für die folgenden Betriebssysteme unterstützt:

- Windows
 - Serverfamilie 2008 und höher
 - Serverfamilie ab Version 2012
 - 2016 Server
 - Nano Server

- Linux
 - RHEL 6.x Familie und höher
 - RHEL 7.x-Familie oder höher
 - SLES 11.x Familie und höher
 - SLES 12.x-Familie oder höher

- VMware
 - ESX 5.x Familie und höher
 - ESX 6.x-Familie oder höher

ANMERKUNG

32-Bit Linux-Betriebssysteme besitzen nur einen geringen Speicherplatz für Kernel-Datenstrukturen. Deshalb empfiehlt QLogic, dass Sie ausschließlich 64-Bit-Linux verwenden, um NPAR zu konfigurieren.

Für einige ältere BS-Versionen benötigen Sie möglicherweise eine ältere Treiberversion.

Konfigurieren der NIC-Partitionierung

Wenn die NIC-Partitionierung auf einem Adapter aktiviert ist, werden standardmäßig gar keine Offloads auf physischen Funktionen (PF) oder virtuelle NIC (vNIC) aktiviert. Um die FCoE- und/oder iSCSI-Offload-Funktion zu nutzen, muss der Anwender Speicherentlastungen auf einer PF konfigurieren.

Die NIC-Partitionierung kann mit dem **UEFI HII**-Menü konfiguriert werden. Sie können auf das **UEFI HII**-Menü zugreifen, indem Sie die Dell Taste F2 während des Systemstarts drücken (UEFI wird von den meisten Dell Server-BIOS unterstützt). Weitere Informationen zur Verwendung des **UEFI HII**-Menüs finden Sie in der Dell Server-Dokumentation.

Die Partitionierung der Netzwerkschnittstellenkarte kann außerdem über die QCC-Benutzeroberfläche, QCS CLI und das QCC vSphere-Benutzeroberflächen-Plug-in konfiguriert werden. Weitere Informationen finden Sie in den jeweiligen Benutzerhandbüchern.

ANMERKUNG

Im NPAR-Modus kann SR-IOV nicht auf einer PF (VNIC) aktiviert werden, auf der ein Speicher-Offload (FCoE oder iSCSI) konfiguriert ist. Dies gilt nicht für Adapter, die sich im Einzelfunktions-(SF-)Modus befinden.

So konfigurieren Sie mit dem CCM-Dienstprogramm eine Netzwerkschnittstellenkarte für die Partitionierung:

1. Wählen Sie eine Netzwerkschnittstellenkarte aus der **Device List** (Geräteliste) aus.
2. Wählen Sie im **Main Menu** (Hauptmenü) die Option **Device Hardware Configuration** (Gerätehardwarekonfiguration) aus.
3. Ändern Sie den **Multi-Function Mode** (Multifunktionsmodus) in **NPAR**.
4. Konfigurieren Sie die Netzwerkschnittstellenkarten-Parameter für Ihre Konfiguration auf Basis der in [Tabelle 12-1](#) dargestellten Optionen, die eine Auflistung der Konfigurationsparameter im Fenster „NIC Partitioning Configuration“ (Konfiguration für die Netzwerkschnittstellenkarten-Partitionierung) enthält.

Tabelle 12-1. Konfigurationsoptionen

Parameter	Beschreibung	Optionen
Flow Control (Flusskontrolle):	Konfiguriert den Flow Control-Modus für diesen Port.	<ul style="list-style-type: none">■ Automatisch■ TX Flow Control (Flusskontrolle)■ RX Flow Control (Flusskontrolle)■ TX/RX Flow Control■ Keine
PF#0, PF#2, PF#4, PF#6	Zeigt die Informationen zur physischen Funktion (PF) in Bezug auf die Partition(en) an Port 0. Wählen Sie für die Konfiguration die gewünschte Funktion aus.	Konfigurationsoptionen finden Sie in Tabelle 12-2 .
PF#1, PF#3, PF#5, PF#7	Zeigt die Informationen zur physischen Funktion (PF) in Bezug auf die Partition(en) auf Port 1 an. Wählen Sie für die Konfiguration die gewünschte Funktion aus.	Konfigurationsoptionen finden Sie in Tabelle 12-2 .

Tabelle 12-1. Konfigurationsoptionen (fortgesetzt)

Parameter	Beschreibung	Optionen
Reset Configuration to Default (Standardeinstellungen für Konfiguration wiederherstellen)	Setzt die Konfiguration der NIC-Partition auf die standardmäßigen Werkseinstellungen zurück.	–

Tabelle 12-2 beschreibt die Funktionen im PF# X-Fenster.

Tabelle 12-2. Funktionsbeschreibung

Funktion	Beschreibung	Option
Ethernet Protocol (Ethernet Protokoll)	Aktiviert und deaktiviert das Ethernet-Protokoll.	<input type="checkbox"/> Aktivieren <input type="checkbox"/> Deaktivieren
iSCSI Offload Protocol (iSCSI-Offload-Protokoll)	Aktiviert und deaktiviert das iSCSI-Protokoll.	<input type="checkbox"/> Aktivieren <input type="checkbox"/> Deaktivieren
FCoE Offload protocol (FCoE-Offload-Protokoll)	Aktiviert und deaktiviert das FCOE-Protokoll.	<input type="checkbox"/> Aktivieren <input type="checkbox"/> Deaktivieren
Bandwidth Weight (Bandbreite)	Konfiguriert die Gewichtung bzw. die Wichtigkeit einer bestimmten Funktion. Für die vier Funktionen pro Port wird die Gewichtung zur Vermittlung zwischen den Funktionen im Falle einer Überlastung verwendet.	Die Summe aller Gewichtungen für die vier Funktionen beträgt entweder 0 oder 100.
Maximum Bandwidth (Maximale Bandbreite)	Konfiguriert den Prozentsatz für die maximale Bandbreite des Physical Port-Links.	–
Network MAC Address (Netzwerk MAC-Adresse ^{a)})	Zeigt die Netzwerk MAC-Adresse an.	–
iSCSI MAC Address (iSCSI-MAC-Adresse ^{a)})	Zeigt die iSCSI MAC-Adresse an.	–
FCoE FIP MAC Address (FCoE FIP MAC-Adresse)	Zeigt die FCoE MAC-Adresse an.	–
FCoE WWPN	Zeigt den weltweiten FCoE-Portnamen an	–
FCoE WWNN	Zeigt den weltweiten FCoE-Knotennamen an.	–

^a Stellen Sie sicher, dass die **Netzwerk MAC-Adresse** und die **iSCSI MAC-Adresse** nicht identisch sind.

ANMERKUNG

Bei Linux-, Citrix XenServer- und VMware ESXi-Betriebssystemen ist das Ethernet-Protokoll für alle Partitionen immer aktiviert, und zwar selbst dann, wenn Sie die Ethernet-Personalität über das QLogic Comprehensive Configuration Management (CCM)-Werkzeug deaktivieren.

Die Konfiguration von gleichen Werten für **Bandwidth Weight** (Bandbreite) für alle Funktionen hat unterschiedliche Auswirkungen, je nachdem, welche Werte für die Konfiguration verwendet werden. Werden beispielsweise alle Funktionen als „0“ oder „25“ konfiguriert, weisen diese Funktionen unterschiedliche Bandbreiteneinstellungen auf, obwohl sie logischerweise den gleichen Effekt haben sollten.

Beachten Sie die folgende Beispielkonfiguration: Vier Funktionen (oder Partitionen) sind mit insgesamt sechs Protokollen konfiguriert, wie im Folgenden beschrieben:

Funktion 0

- Ethernet
- FCoE

Funktion 1

- Ethernet

Funktion 2

- Ethernet

Funktion 3

- Ethernet
- iSCSI

1. Wenn der Wert für **Relative Bandwidth Weight** (Relative Bandbreitengewichtung) für alle vier physischen Funktionen (pF) als „0“ konfiguriert wird, wird die Bandbreite von allen sechs Offloads gemeinsam

genutzt. In diesem Fall wird jedem Offload etwa 16,67 Prozent der gesamten Bandbreite zugewiesen.

2. Wenn der Wert für **Relative Bandwidth Weight** (Relative Bandbreitengewichtung) für alle vier PFs als „25“ konfiguriert wird, werden den Ethernet- und FCoE-Offloads auf Funktion 0 und den Ethernet- und iSCSI-Offloads auf Funktion 3 etwa 12,5 Prozent der gesamten Bandbreite zugewiesen, während den Ethernet- und FcoE auf Funktion 1 und Funktion 2 etwa 25 Prozent der gesamten Bandbreite zugewiesen wird.

13 Linux QCS Installation

Die Installationsinformationen für QLogic Control Suite auf einer Linux-Plattform beinhalten:

- [Übersicht](#)
- [„Installieren von WS-MAN oder CIM-XML auf einem Linux-Server“ auf Seite 219](#)
- [„Installieren von WS-MAN oder CIM-XML auf einem Linux-Client“ auf Seite 227](#)
- [„Installieren von QLogic Control Suite“ auf Seite 228](#)

Übersicht

QLogic Control Suite (QCS) ist eine Management-Anwendung zur Konfiguration der BCM57xx und BCM57xxx-Adapterfamilie, auch bekannt als konvergierte Netzwerkadapter. Die QCS-Software funktioniert unter Server- und Clientbetriebssystemen von Windows und Linux. Dieses Kapitel beschreibt, wie Sie die QCS-Management-Anwendung installieren. Für Windows sind ein GUI und ein CLI verfügbar; für Linux ist ein CLI verfügbar. Um einen Linux-Host unter Verwendung einer QCS-GUI zu verwalten, stellen Sie die QCS-GUI in Windows bereit, und stellen Sie dann eine Verbindung zum Arbeitsplatz unter den in diesem Kapitel beschriebenen Anweisungen her.

Dieses Kapitel beschreibt, wie Sie die QCS-Management-Anwendung auf Linux-Systemen installieren. Für Windows-Systeme wird ein Installationsprogramm mitgeliefert, das die Windows-Treiber und die Management-Anwendungen installiert, einschließlich QCS.

Es gibt zwei Hauptkomponenten des QCS-Dienstprogramms: die Provider-Komponente und die Clientsoftware. Der Provider wird auf einem Server oder Managed Host installiert, der ein oder mehrere Converged Network Adapters (CNA) enthält. Der Provider sammelt Informationen über die CNAs und stellt sie für den Abruf von einem Management-PC bereit, auf dem die Clientsoftware installiert ist. Die Clientsoftware ermöglicht die Anzeige von Informationen der Provider und Konfiguration der CNAs. Die QCS-Clientsoftware umfasst ein CLI.

Kommunikationsprotokolle

Ein Kommunikationsprotokoll ermöglicht den Informationsaustausch zwischen dem Provider und der Clientsoftware. Dies sind eigene Implementierungen oder Open-Source-Implementierungen der Standards Web-Based Enterprise Management (WBEM) und Common Information Model (CIM) von der Distributed Management Task Force (DMTF). Netzwerkadministratoren können abhängig von dem vorherrschenden Standard bei ihrem Netzwerk die beste Möglichkeit wählen.

[Tabelle 13-1](#) zeigt die verfügbaren Optionen basierend auf den Betriebssystemen an, die auf dem Managed Host und dem Client installiert sind.

Tabelle 13-1. Kommunikationsprotokolloptionen

Wenn der Client dieses Betriebssystem verwendet:	Und der Managed Host dieses Betriebssystem verwendet:	dann kann QCS diese Kommunikationsprotokolle verwenden:
Windows	Windows	WMI WS-MAN (WinRM)
Windows	Linux	CIM-XML (OpenPegasus) WS-MAN (OpenPegasus)
Linux	Windows	WS-MAN (WinRM)
Linux	Linux	CIM-XML (OpenPegasus) WS-MAN (OpenPegasus)

WMI = Windows Management Instrumentation.

WS-MAN = Web Service-Management. WinRM ist eine auf Windows basierende Implementierung, und OpenPegasus ist eine Open-Source-Implementierung, die unter Linux funktioniert.

CIM-XML = Eine auf XML basierende Version von OpenPegasus.

Wenn zu Ihrem Netzwerk eine Mischung aus Windows- und Linux-Clients gehört, die auf Windows- und Linux-Server zugreifen, ist WS-MAN eine geeignete Wahl. Wenn Linux das einzige auf den Servern installierte Betriebssystem ist, ist CIM-XML eine Möglichkeit. Wenn zu Ihrem Netzwerk nur Windows-Server und -Clients gehören, ist WMI eine Möglichkeit. WMI ist sehr einfach zu konfigurieren, wird aber nur unter Windows unterstützt.

Bei der QCS-Installation werden auch die Provider-Komponente auf dem Managed Host und die Clientsoftware auf der Verwaltungsstation installiert. Der Installationsvorgang unterscheidet sich je nach den Betriebssystemen, die auf dem Client und dem Managed Host installiert sind, und den ausgewählten Kommunikationsprotokollen.

Installieren von WS-MAN oder CIM-XML auf einem Linux-Server

Befolgen Sie diese Schritte, um WS-MAN oder CIM-XML auf einem Linux-Server zu installieren:

Schritt 1: Installieren von OpenPegasus

Schritt 2: Starten von CIM Server auf dem Server

Schritt 3: Konfigurieren von OpenPegasus auf dem Server

Schritt 4: Installieren des QLogic-CMPI-Providers

Schritt 5: Durchführen der Linux-Firewall-Konfiguration, falls erforderlich

Schritt 6: QCS und zugehörige Management-Anwendungen installieren

Schritt 1: Installieren von OpenPegasus

Unter Red Hat Linux stehen zwei Installationsoptionen zur Verfügung:

- Vom internen RPM (Nur Red Hat)
- Von der Source (Red Hat und SUSE)

Unter SUSE Linux Enterprise Server 11 (SLES 11) müssen Sie das Quell-RPM verwenden.

ANMERKUNG

Das interne RPM unterstützt nicht das WS-MAN-Kommunikationsprotokoll. Um WS-MAN zu verwenden, müssen Sie OpenPegasus von der Source installieren.

Vom internen RPM (Nur Red Hat)

Bei Red Hat Linux steht ein internes OpenPegasus RPM als `tog-pegasus-<version>.<arch>.rpm` zur Verfügung.

1. Geben Sie den folgenden Befehl aus, um `tog-pegasus` zu installieren:

```
rpm -ivh tog-openpegasus-<version>.<arch>.rpm
```

2. Geben Sie den folgenden Befehl aus, um Pegasus zu starten:

```
/etc/init.d/tog-pegasus start
```

ANMERKUNG

Wenn bei Ihrem System „Red Hat-Sicherungsverbesserung für tog-pegasus“ aktiviert ist, deaktivieren Sie es, bevor Sie eine Verbindung zu QCS herstellen. Weitere Details finden Sie in der Datei:

```
/usr/share/doc/tog-pegasus-2.5.2/README.RedHat.Security
```

Um die Funktion zu deaktivieren, entfernen Sie die Zeile aus
`/etc/pam.d/wbem`.

ANMERKUNG

Bei SUSE Linux ist das interne OpenPegasus RPM nicht verfügbar. OpenPegasus muss wie folgt beschrieben von der Source installiert werden.

Beachten Sie, dass im internen Pegasus HTTP nicht standardmäßig aktiviert ist. Nachdem das interne OpenPegasus erfolgreich installiert wurde und keine weitere Konfiguration erforderlich ist, befolgen Sie die Anweisungen in „[Schritt 4: Installieren des QLogic-CMPI-Providers](#)“ auf Seite 225. Um HTTP zu aktivieren, siehe „[Aktivieren von HTTP](#)“ auf Seite 224.

ANMERKUNG

Nachdem der Server neu gebootet wurde, muss der CIM-Server manuell neu gestartet werden, sodass der Client die Verbindung zum Server wiederherstellen kann. Der manuelle Neustart ist eine bekannte Einschränkung des internen RPM von Red Hat v6.2.

Von der Source (Red Hat und SUSE)

Die OpenPegasus-Source kann von der folgenden Website heruntergeladen werden:

www.openpegasus.org

ANMERKUNG

- Falls nicht bereits installiert, laden Sie die Dateien OpenSSL- und libopenssl-devel-RPM herunter, und installieren Sie diese. Dieser Schritt ist optional und nur nötig, wenn Sie HTTPS zur Verbindung zwischen dem Client und dem Managed Host verwenden möchten.
- In manchen Fällen, wenn die OpenPegasus-Installation fehlschlägt, muss OpenSSL mit der `-fPIC`-Option installiert sein:
`./config no-threads --fPIC`. Verwenden Sie diese Option, um OpenSSL und die im Verzeichnis `/usr/local/ssl` enthaltenen Dateien zu installieren. Legen Sie `/usr/local/ssl` für den `OPENSSL_HOME`-Pfad fest, und setzen Sie die Installation von OpenPegasus fort.

Einrichten der Umgebungsvariablen

[Tabelle 13-2](#) beschreibt die Umgebungsvariablen zur Erstellung von OpenPegasus.

Tabelle 13-2. Umgebungsvariablen

Umgebungsvariable	Beschreibung
PEGASUS_ROOT	Speicherort des Pegasus-Verzeichnisbaums
PEGASUS_HOME	Der Speicherort des Programms, das Repository; z. B. die folgenden Unterordner: <code>\$PEGASUS_HOME/bin</code> <code>\$PEGASUS_HOME/lib</code> <code>\$PEGASUS_HOME/repository</code> <code>\$PEGASUS_HOME/mof</code>
PATH	<code>\$PATH:\$PEGASUS_HOME/bin</code>
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	True
PEGASUS_CIM_SCHEMA	"CIM222"
PEGASUS_PLATFORM	Für 32-Bit-Linux-Systeme: "LINUX_I86_GNU" Für 64-Bit-Linux-Systeme: "LINUX_X86_64_GNU"
PEGASUS_HAS_SSL	Optional. Für HTTPS-Support auf "true" setzen.
PEGASUS_ENABLE_PROTOCOL_WSMAN	Optional. Für die Unterstützung des WSMAN-Protokolls auf "true" setzen.

Zusätzliche Einstellungen

Die Variable `$PEGASUS_HOME` muss in der Shell-Umgebung eingerichtet werden, und `$PEGASUS_HOME/bin` muss an die `$PATH`-Umgebung angehängt sein.

Beispiele:

```
export PEGASUS_PLATFORM="LINUX_X86_64_GNU"
export PEGASUS_CIM_SCHEMA="CIM222"
export PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER=true
export PEGASUS_ROOT="/share/pegasus-2.10-src"
export PEGASUS_HOME="/pegasus"
export PATH=$PATH:$PEGASUS_HOME/bin
```

Fügen Sie für SSL-Support die folgende Umgebungsvariable hinzu:

```
export PEGASUS_HAS_SSL=true
```

Fügen Sie für WS-MAN-Support die folgende Umgebungsvariable hinzu:

```
export PEGASUS_ENABLE_PROTOCOL_WSMAN=true
```

CIM-XML und WSMAN verwenden in OpenPegasus dieselben Ports für HTTP oder HTTPS. Die Standardportnummern für HTTP und HTTPS sind jeweils 5989 und 5989.

ANMERKUNG

Sie können diese Exporte am Ende der Datei `.bash_profile` hinzufügen. Diese Datei befindet sich im `/root`-Verzeichnis.

- Die Umgebungsvariablen werden eingerichtet, wenn sich ein Benutzer über PuTTY anmeldet.
- Geben Sie beim Linux-System bei jedem Terminal, für das die Umgebungsvariablen nicht eingerichtet werden, den folgenden Befehl aus:

```
source /root/.bash_profile
```

- Wenn Sie sich ab- und wieder anmelden, werden die Umgebungsvariablen eingerichtet.

Erstellen und Installieren von OpenPegasus

Geben Sie unter `$PEGASUS_ROOT` (dem Speicherort des Pegasus-Quellstammverzeichnisses) die folgenden Befehle aus:

```
make clean
make
make repository
```

ANMERKUNG

Immer wenn OpenPegasus von der Source installiert wird, werden alle Konfigurationen auf die Standardwerte zurückgesetzt. Wenn Sie OpenPegasus erneut installieren, müssen Sie die Konfigurationen neu einrichten, wie in „[Schritt 3: Konfigurieren von OpenPegasus auf dem Server](#)“ auf Seite 223 beschrieben.

Schritt 2: Starten von CIM Server auf dem Server

Geben Sie den Befehl `cimserver` aus, um CIM Server zu starten. Um CIM-Server zu beenden, geben Sie den Befehl `cimserver -s` aus.

Um zu überprüfen, ob OpenPegasus ordnungsgemäß installiert wurde, geben Sie den folgenden Befehl aus:

```
cimcli ei -n root/PG_Interop PG_ProviderModule
```

ANMERKUNG

Damit OpenPegasus von der Quelle kompiliert wird, muss `PEGASUS_HOME` beim Start von CIM-Server definiert werden. Sonst kann CIM-Server das Repository nicht richtig laden. Sie können `PEGASUS_HOME` in der Datei `.bash_profile` einrichten.

Schritt 3: Konfigurieren von OpenPegasus auf dem Server

Verwenden Sie den Befehl `cimconfig`, um OpenPegasus zu konfigurieren, wie in [Tabelle 13-3](#) angegeben.

Tabelle 13-3. cimconfig-Befehlsoptionen

Befehl	Beschreibung
<code>cimconfig -l</code>	Auflisten aller gültigen Eigenschaftsnamen.
<code>cimconfig -l -c</code>	Auflisten aller gültigen Eigenschaftsnamen und deren Werten.
<code>cimconfig -g <property name></code>	Fordern Sie eine bestimmte Eigenschaft an.
<code>cimconfig -s <property name>= <value> -p</code>	Richten Sie eine bestimmte Eigenschaft ein.
<code>cimconfig --help</code>	Weitere Informationen über den Befehl.

CIM-Server muss vor dem Ausführen von `cimconfig` gestartet und zum Übernehmen der Konfigurationsänderungen neu gestartet werden.

Aktivieren der Authentifizierung

Sie müssen die OpenPegasus-Eigenschaften wie in diesem Abschnitt beschrieben einrichten. Andernfalls funktioniert der Broadcom CIM-Provider nicht ordnungsgemäß. Stellen Sie sicher, dass folgende Werte eingerichtet sind, bevor Sie QCS starten und eine Verbindung zum Provider herstellen.

Starten Sie CIM-Server, falls nicht bereits geschehen. Richten Sie anschließend folgende Werte ein:

```
cimconfig -s enableAuthentication=true -p
cimconfig -s enableNamespaceAuthorization=false -p
cimconfig -s httpAuthType=Basic -p
cimconfig -s passwordFilePath=cimserver.passwd -p
cimconfig -s forceProviderProcesses=false -p
```

Wenn Sie möchten, dass für Root-Benutzer eine Remote-Verbindung möglich ist, geben Sie folgenden Befehl aus:

```
cimconfig -s enableRemotePrivilegedUserAccess=true -p
```

Benutzerkonfiguration mit Berechtigung: Für die OpenPegasus-Authentifizierung werden Linux-Systembenutzer verwendet. Fügen Sie wie folgt die Systemanwender zu OpenPegasus unter Verwendung des `cimuser` -Befehls hinzu, um mit QCS zu verbinden:

```
cimuser -a -u <username> -w <password>
```

Beispiel: `cimuser -a -u root -w linux1`

Aktivieren von HTTP

Befolgen Sie diese Schritte, um HTTP zu aktivieren:

1. Wenn CIM-Server noch nicht gestartet wurde, führen Sie den Start jetzt durch.
2. Geben Sie den folgenden Befehl aus, um einen HTTP-Port einzurichten (optional):

```
cimconfig -s httpPort=5988 -p
```

Diese Eigenschaft ist nicht für das interne OpenPegasus verfügbar.

3. Geben Sie den folgenden Befehl aus, um eine HTTP-Verbindung zu aktivieren:

```
cimconfig -s enableHttpConnection=true -p
```

4. Führen Sie die Befehle `cimserver -s` und `cimserver` aus, um den CIM-Server zu beenden und neu zu starten, damit die neue Konfiguration übernommen wird.

Aktivieren von HTTPS

Befolgen Sie diese Schritte, um HTTPS zu aktivieren:

1. Wenn CIM-Server noch nicht gestartet wurde, führen Sie den Start jetzt durch.
2. Geben Sie den folgenden Befehl aus, um einen HTTPS-Port einzurichten (optional):

```
cimconfig -s httpsPort=5989 -p
```

Diese Eigenschaft ist nicht für das interne OpenPegasus verfügbar.

3. Verwenden Sie den folgenden Befehl, um eine HTTPS-Verbindung zu aktivieren:

```
cimconfig -s enableHttpsConnection=true -p
```

4. Führen Sie die Befehle `cimserver -s` und `cimserver` aus, um den CIM-Server zu beenden und neu zu starten, damit die neue Konfiguration übernommen wird.

Schritt 4: Installieren des QLogic-CMPI-Providers

Stellen Sie vor der Installation von CMPI Provider sicher, dass OpenPegasus ordnungsgemäß installiert ist.

Installieren

Geben Sie den folgenden Befehl aus, um QLogic CMPI-Provider zu installieren:

```
% rpm -i QLGC_CMPIProvider-{version}.{arch}.rpm
```

Deinstallieren

Geben Sie den folgenden Befehl aus, um QLogic CMPI-Provider zu deinstallieren:

```
% rpm -e QLGC_CMPIProvider
```

Schritt 5: Durchführen der Linux-Firewall-Konfiguration, falls erforderlich

Befolgen Sie die erforderlichen Schritte, um die passenden Ports in der Firewall zu öffnen.

Red Hat

So konfigurieren Sie die Linux-Firewall auf Red Hat:

1. Klicken Sie auf **System**, wählen Sie **Administration** aus, und wählen Sie dann **Firewall** aus.
2. Wählen Sie **Other Ports** (Andere Ports) aus.
3. Wählen Sie im Dialogfeld „Port and Protocol“ (Port und Protokoll) **User Defined** (Benutzerdefiniert) aus.
4. Geben Sie im Dialogfeld **Port/Port Range** (Port/Portbereich) die Portnummer ein.
5. Fügen Sie im Dialogfeld **Protocol** (Protokoll) das Protokoll als TCP oder UDP ein usw.
6. Klicken Sie auf **Apply** (Übernehmen), damit die Firewallregeln übernommen werden.

Beispiel:

- Für CIM-XML über HTTP werden Portnummer 5988 und das Protokoll TCP verwendet.
- Für CIM-XML über HTTPS werden Portnummer 5989 und das Protokoll TCP verwendet.

SUSE

So konfigurieren Sie die Linux-Firewall auf SUSE:

1. Klicken Sie auf **Compute** (Berechnen) und dann auf **YaST**.
2. Wählen Sie **Security & User** (Sicherheit & Benutzer) im linken Bereich aus.
3. Doppelklicken Sie im rechten Bereich auf **Firewall**.
4. Wählen Sie im linken Bereich **Custom Rules** (Benutzerdefinierte Regeln) aus.
5. Klicken Sie im rechten Bereich auf **Add** (Hinzufügen).
6. Geben Sie die folgenden Werte ein:
 - Source Network** (Quellnetzwerk): 0/0 (bedeutet alle)
 - Protocol** (Protokoll): TCP (oder das passende Protokoll)
 - Destination Port** (Ziel-Port): *<Port Number>* (Portnummer) oder *<Range of Port Numbers>* (Portnummernbereich)

- Source Port** (Quell-Port): Leer lassen

Verwenden Sie zum Beispiel für CIM-XML die folgenden Werte:

- Source Network** (Quellnetzwerk): 0/0 (bedeutet alle)
- Protocol** (Protokoll): TCP
- Destination Port** (Ziel-Port): 5988:5989
- Source Port** (Quell-Port): Leer lassen

7. Klicken Sie auf **Next** (Weiter) und dann auf **Finish** (Fertig stellen), damit die Firewallregeln übernommen werden.

Schritt 6: QCS und zugehörige Management-Anwendungen installieren

Siehe „[Installieren von QLogic Control Suite](#)“ auf Seite 228 für Vorgänge.

Installieren von WS-MAN oder CIM-XML auf einem Linux-Client

Es sind auf dem Linux-Client keine speziellen Softwarekomponenten erforderlich, um HTTP zu verwenden. Es muss lediglich die QCS-Management-Anwendung installiert werden. Allerdings können sie bei WS-MAN-Installationen optional das HTTPS-Protokoll für die Verwendung mit QCS konfigurieren.

Konfigurieren von HTTPS auf einem Linux-Client

Die Konfiguration von HTTPS auf einem Linux-Client erfordert den Import des Zertifikats, einen HTTPS-Test und die SSL-Verbindung.

Importieren eines selbstsignierten Zertifikats auf einem Linux-Client

Beachten Sie bei Linux-Distributionen das folgende Zertifikatsverzeichnis:

- Bei allen SUSE-Versionen lautet das Zertifikatsverzeichnis `/etc/ssl/certs`.
- Bei Red Hat kann sich das Zertifikatsverzeichnis je nach Version unterscheiden. Bei einigen Versionen lautet es `/etc/ssl/certs` oder `/etc/pki/tls/certs`. Suchen Sie bei anderen Versionen das Zertifikatsverzeichnis.

Kopieren Sie die Datei `hostname.pem` des selbstsignierten Zertifikats in das Zertifikatsverzeichnis auf dem Linux-Client. Wenn das Zertifikatsverzeichnis z. B. `/etc/ssl/certs` lautet, kopieren Sie `hostname.pem` in `/etc/ssl/certs`.

1. Ändern Sie das Verzeichnis in:

```
/etc/ssl/certs
```

2. Erstellen Sie einen Hashwert, indem Sie den folgenden Befehl ausgeben:

```
openssl x509 -noout -hash -in hostname.pem
```

Es wird ein Wert ausgegeben, der z. B. wie folgt aussehen kann:

```
100940db
```

3. Erstellen Sie eine symbolische Verknüpfung zum Hash-Wert, indem Sie den folgenden Befehl ausgeben:

```
ln -s hostname.pem 100940db.0
```

Testen der HTTPS/SSL-Verbindung von einem Linux-Client

Geben Sie den folgenden Befehl aus, um zu testen, ob das Zertifikat korrekt unter Linux installiert wurde:

```
# curl -v --capath /etc/ssl/certs https://Hostname or  
IPAddress:5986/wsman
```

Wenn dies fehlschlägt, wurde das Zertifikat nicht korrekt installiert, und es wird eine Fehlermeldung mit der Aufforderung angezeigt, dass Sie eine Korrekturmaßnahme durchführen müssen.

Installieren von QLogic Control Suite

Die QLogic Control Suite (QCS)-Software kann auf einem Linux-System mit dem Linux-RPM-Paket installiert werden. Diese Installation beinhaltet einen QCS CLI-Client.

Vor dem Start:

- Vergewissern Sie sich, dass der/die QLogicNetzwerkadapter in das System eingesetzt wurde(n) und dass der passende Gerätetreiber für die NIC auf dem System installiert wurde, das von diesem Dienstprogramm verwaltet werden soll.
- Vergewissern Sie sich, dass der CIM-Provider ordnungsgemäß auf dem System installiert wurde, das von diesem Dienstprogramm verwaltet werden soll.
- Vergewissern Sie sich für die Verwaltung von iSCSI auf Linux-Hosts, dass die open-iSCSI- und sg-Dienstprogramme auf dem Linux-Host installiert sind.

Um QCS zu installieren:

1. Laden Sie das neueste RPM-Paket für die QCS-Management-Anwendung herunter.
2. Installieren Sie das RPM-Paket mit dem folgenden Befehl:

```
% rpm -i QCS-{version}.{arch}.rpm
```

So verwenden Sie QCS:

Um QCS CLI zu verwenden, lesen Sie die Datei `QCSCLI_Readme.txt`, die mit den Dateien mitgeliefert wird.

So deinstallieren Sie QCS:

Geben Sie den folgenden Befehl aus, um das RPM-Paket zu deinstallieren:

```
% rpm -e QCS
```

14 Fibre Channel Over Ethernet

FCoE (Fibre Channel over Ethernet)-Informationen umfassen Folgendes:

- [Übersicht](#)
- [„FCoE-Boot aus SAN“ auf Seite 231](#)
- [„Konfigurieren von FCoE“ auf Seite 270](#)
- [„N_Port-ID-Virtualisierung \(NPIV\)“ auf Seite 272](#)

Übersicht

In modernen Rechenzentren werden mehrere Netzwerke, darunter NAS (Network Attached Storage)-, Verwaltungs-, IPC- und Speichersysteme, zur Erzielung der gewünschten Leistung und Flexibilität eingesetzt. Neben iSCSI für Speicherlösungen steht nun auch Fibre Channel over Ethernet (FCoE) mit geeigneten QLogic C-NICs zur Verfügung. FCoE ist ein Protokoll, mit dem Fibre Channel-Daten über Ethernet übertragen werden können, wobei bereits vorhandene Fibre Channel-Infrastrukturen sowie Kapitalanlagen erhalten bleiben, und eingehende FCoE- und FIP (FCoE Initialization Protocol)-Frames klassifiziert werden.

Die folgenden FCoE-Funktionen werden unterstützt:

- Receiver-Klassifizierung von FCoE- und FIP-Frames. FIP steht für FCoE Initialization Protocol und wird zur Herstellung und Aufrechterhaltung von Verbindungen verwendet.
- Receiver-CRC-Verschiebung
- Transmitter-CRC-Verschiebung
- Spezielle Warteschlange für Fibre Channel-Datenverkehr
- N_Port ID-Virtualisierung (NPIV) funktioniert unter Windows- und Linux-Betriebssystemen.
- Virtuelle Fibre Channel Host-Bus-Adapter auf einer virtuellen Maschine in Windows Server ab Version 2012 und R2 Hyper-V

- Data Center Bridging (DCB) sorgt für verlustfreie Übertragungen mit Priority Flow Control (PFC).
- DCB weist dem FCoE-Datenverkehr per Enhanced Transmission Selection (ETS) eine bestimmte Verbindungsbandbreite zu.

DCB unterstützt Speicher-, Verwaltungs-, Rechen- und Kommunikations-Fabrics auf einer einzigen physikalischen Fabric, die einfacher bereitzustellen, zu aktualisieren und instandzuhalten ist als in Standard-Ethernet-Netzwerken. Mithilfe der DCB-Technologie können geeignete QLogic C-NICs für verlustfreie Datenübertragung, geringe Latenzzeit und standardbasierte gemeinsame Bandbreitennutzung von physikalischen Verbindungen im Rechenzentrum sorgen. DCB unterstützt FCoE-, iSCSI-, NAS-(Network-Attached Storage-), Verwaltungs- und IPC-Datenverkehrsflüsse. Weitere Informationen zu DCB finden Sie unter [Kapitel 15 Data Center Bridging](#).

Konfigurieren Sie NPIV in Windows QCS GUI, indem Sie auf eine FCoE-Adapter-Instanz klicken und **Create a Virtual Port** (Virtuellen Port erstellen) oder **Create Multiple Virtual Ports** (Mehrere virtuelle Ports erstellen) klicken. Sie können auch die Befehle QCS CLI `createnpivport` und `createmultinpivport` ausführen. Konfigurieren Sie NPIV in Linux, indem Sie den Befehl `vport_create` ausführen.

Fügen Sie Windows Server 2012 R2 vFCs unter Verwendung von Hyper-V Virtual SAN Manager oder durch das Ausführen des PowerShell-Befehls für Windows Server ab Version 2012 R2 `Add-VMFibreChannelHBA` hinzu.

FCoE-Boot aus SAN

In diesem Abschnitt werden die Installations- und Bootverfahren für die Betriebssysteme Windows, Linux und ESXi beschrieben.

Im folgenden Abschnitt wird die BIOS-Einrichtung und Konfiguration der Boot-Umgebung vor der Betriebssysteminstallation ausführlich beschrieben.

Vorbereiten des System-BIOS auf FCoE-Build und -Boot

Um das System-BIOS auf FCoE-Build und -Boot vorzubereiten, passen Sie die System-Boot-Reihenfolge an, und geben Sie falls erforderlich das BIOS-Boot-Protokoll an.

Anpassen der System-Startreihenfolge

Der QLogic-Initiator muss in der Boot-Reihenfolge an erster Stelle stehen. An zweiter Stelle müssen die Installationsdatenträger des Betriebssystems stehen. Die richtige Boot-Reihenfolge ist sehr wichtig, da die Installation anderenfalls nicht ordnungsgemäß durchgeführt werden kann. Entweder die gewünschte Boot-LUN wird nicht erkannt, oder sie wird als offline gekennzeichnet.

Angeben des BIOS-Boot-Protokolls (falls erforderlich)

Auf einigen Plattformen muss das Boot-Protokoll über eine Konfiguration des System-BIOS konfiguriert werden. Auf allen anderen Systemen wird das Boot-Protokoll über das Dienstprogramm Comprehensive Configuration Management (CCM) von QLogic angegeben, und für diese Systeme ist dieser Schritt nicht erforderlich.

Vorbereiten des QLogic Multi-Boot-Agenten auf FCoE-Boot (CCM-Dienstprogramm)

Das CCM-Dienstprogramm ist nur verfügbar, wenn das System auf den Legacy-Boot-Modus gesetzt ist. Es ist nicht verfügbar, wenn die Systeme auf den UEFI-Boot-Modus gesetzt sind. Die Seiten für die UEFI-Gerätekonfiguration sind in beiden Modi verfügbar.

1. Öffnen Sie das CCM-Dienstprogramm während des Selbsttests. Drücken Sie auf dem Broadcom NetXtreme Ethernet Boot Agent-Banner ([Abbildung 14-1](#)) die Tasten CTRL+S.

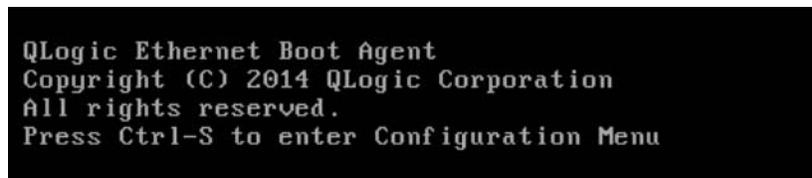


Abbildung 14-1. Öffnen des CCM-Dienstprogramms

2. Wählen Sie in der Geräteliste ([Abbildung 14-2](#)) das Gerät aus, über das das Booten konfiguriert werden soll.

ANMERKUNG

Bei der Ausführung im NIC-Partitionierungs-(NPAR-) Modus wird FCoE-Boot nur unterstützt, wenn der ersten Funktion an jedem Booting-Port die FCoE-Identität zugewiesen wurde. FCoE-Boot wird nicht unterstützt, wenn die FCoE-Identität einer anderen Funktion zugewiesen ist.

```
Comprehensive Configuration Management v7.12.1
Copyright (C) 2014 QLogic Corporation
All rights reserved.

----- Device List -----
<02:00:00> BCM57810 - 00:10:18:A2:FA:F0 MBA:v7.12.6 CCM:v7.12.1
<02:00:01> BCM57810 - 00:10:18:A2:FA:F2 MBA:v7.12.6 CCM:v7.12.1

-----
Select Device to Configure
[Enter]:Enter; [↑|↓]:Next Entry; [ESC]:Quit Menu
```

Abbildung 14-2. CCM-Geräteliste

3. Stellen Sie sicher, dass DCB und DCBX auf dem Gerät ([Abbildung 14-3](#)) aktiviert sind. FCoE-Boot wird nur auf DCBX-fähigen Konfigurationen unterstützt. DCB/DCBX muss aktiviert sein, und der direkt angeschlossene Verbindungs-Peer muss ebenfalls DCBX-fähig sein und Parameter aufweisen, die eine vollständige DCBX-Synchronisierung ermöglichen.

```
Comprehensive Configuration Management v7.12.1
Copyright (C) 2014 QLogic Corporation
All rights reserved.

----- Device Hardware Configuration -----
Multi-Function Mode      : SF
DCB Protocol             : Enabled
SR-IOV                   : Disabled
Number of VFs per PF    : 16 (0)
Max Number of PF MSIX Vectors : 0

-----
Enable/Disable DCB Protocol
[←|→][Enter][Space]:Toggle Value; [↑|↓]:Next Entry; [ESC]:Quit
Current Adapter:Primary, Bus=02 Device=00 Func=00, MAC=00:10:18:A2:FA:F0
```

Abbildung 14-3. CCM-Gerätehardwarekonfiguration

4. Auf einigen Plattformen müssen Sie das Boot-Protokoll ggf. über die System-BIOS-Konfiguration im Fenster für integrierte Geräte wie oben beschrieben einrichten.

Verwenden Sie für alle anderen Geräte über CCM das **MBA Configuration Menu** (MBA-Konfigurationsmenü) die Option **Boot Protocol** (Bootprotokoll), um **FCoE** (Abbildung 14-4) festzulegen.

```
Comprehensive Configuration Management v7.12.1
Copyright (C) 2014 QLogic Corporation
All rights reserved.

----- MBA Configuration Menu -----
Option ROM           : Enabled
Boot Protocol        : FCoE
Boot Strap Type      : Auto
Hide Setup Prompt    : Disabled
Setup Key Stroke     : Ctrl-S
Banner Message Timeout : 10 Seconds
Link Speed           : 10Gbps
Pre-boot Wake On LAN : Disabled
ULAN Mode            : Disabled
ULAN ID              : 1
Boot Retry Count     : 2

Select Boot Protocol
[←|→][Enter][Space]:Scroll Value; [↑|↓]:Next Entry; [ESC]:Quit
Current Adapter:Primary, Bus=02 Device=00 Func=00, MAC=00:10:18:A2:FA:F0
```

Abbildung 14-4. CCM MBA Configuration Menu (MBA-Konfigurationsmenü)

5. Konfigurieren Sie das Boot-Ziel und die LUN. Wählen Sie im Menü **Target Information** (Zielinformationen) den ersten verfügbaren Pfad aus (Abbildung 14-5).

```
Comprehensive Configuration Management v7.12.1
Copyright (C) 2014 QLogic Corporation
All rights reserved.

----- Target Information -----
No.1 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.2 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.3 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.4 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.5 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.6 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.7 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.8 Target: Disabled | WWPN - 0000000000000000 LUN - 0

----- Target Information Summary -----
[Enter]:Enter; [↑↓]:Next Entry; [ESC]:Quit Menu
Bus=02 Device=00 Func=00 WWPN:2001001018A2FAF1 WWNN:2000001018A2FAF1
```

Abbildung 14-5. CCM-Zielinformationen

6. Aktivieren Sie die Option **Connect** (Verbinden) und dann den WWPN und die Boot-LUN-Daten für das Ziel, die für den Boot-Vorgang verwendet werden sollen (Abbildung 14-6).

```
Comprehensive Configuration Management v7.12.1
Copyright (C) 2014 QLogic Corporation
All rights reserved.

-----
                No.1 Target Parameters
-----
Connect   : Enabled
WWPN     : 1234512345123451
Boot LUN : 0

-----
                Enable/Disable Target Establishment
[←|→][Enter][Space]:Toggle Value; [↑|↓]:Next Entry; [ESC]:Quit-
Bus=02 Device=00 Func=00 WWPN:2001001018A2FAF1 WWNN:2000001018A2FAF1
```

Abbildung 14-6. CCM-Zielparameter

Die Zielinformationen zeigen die Änderungen an (Abbildung 14-7).

```
Comprehensive Configuration Management v7.12.1
Copyright (C) 2014 QLogic Corporation
All rights reserved.

-----
                Target Information
-----
No.1 Target: Enabled | WWPN - 1234512345123451 LUN - 0
No.2 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.3 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.4 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.5 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.6 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.7 Target: Disabled | WWPN - 0000000000000000 LUN - 0
No.8 Target: Disabled | WWPN - 0000000000000000 LUN - 0

-----
                Target Information Summary
[Enter]:Enter; [↑|↓]:Next Entry; [ESC]:Quit Menu
Bus=02 Device=00 Func=00 WWPN:2001001018A2FAF1 WWNN:2000001018A2FAF1
```

Abbildung 14-7. CCM-Zielinformationen (nach der Konfiguration)

7. Drücken Sie die Taste ESC, bis Sie dazu aufgefordert werden, die Änderungen zu speichern und das Fenster zu schließen. Um CCM zu beenden, führen Sie einen Neustart des Systems durch und übernehmen Sie die Änderungen, drücken Sie die Tasten STRG+ALT+ENTF.
8. Fahren Sie mit der Betriebssysteminstallation fort, nachdem der Speicherzugriff im SAN eingerichtet wurde.

Vorbereiten des QLogic Multi-Boot-Agenten auf FCoE-Boot (UEFI-Dienstprogramm)

Vorbereiten des QLogic Multi-Boot-Agenten auf FCoE-Boot (UEFI-Dienstprogramm)

1. Rufen Sie die Seite für die System-BIOS-UEFI-Gerätekonfiguration auf, indem Sie während des Einschalt-Selbsttests (POST) auf die Taste F2 drücken. Wählen Sie dann **Device Settings** (Geräteeinstellungen) aus (siehe [Abbildung 6-2](#)).
2. Wählen Sie im Menü „Device Settings“ (Geräteeinstellungen) (siehe [Abbildung 6-3](#)) den gewünschten Geräte-Port aus.
3. Wählen Sie im Menü „Main Configuration Page“ (Hauptkonfigurationsseite) die Option **FCoE Configuration** (FCoE-Konfiguration) aus (siehe [Abbildung 6-4](#)).
Das Menü „FCoE Boot Configuration“ (FCoE-Boot-Konfiguration) wird angezeigt (siehe [Abbildung 14-8](#)).

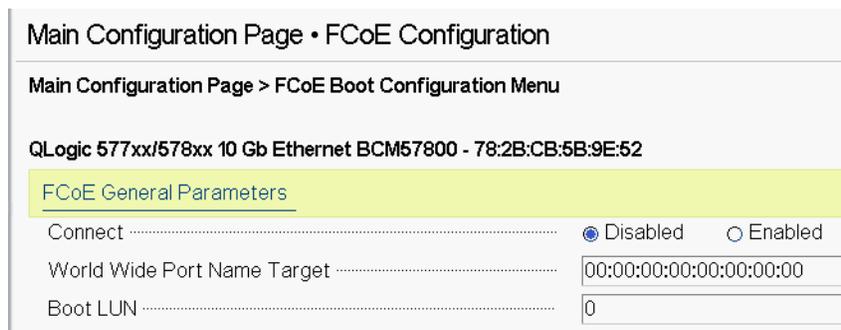
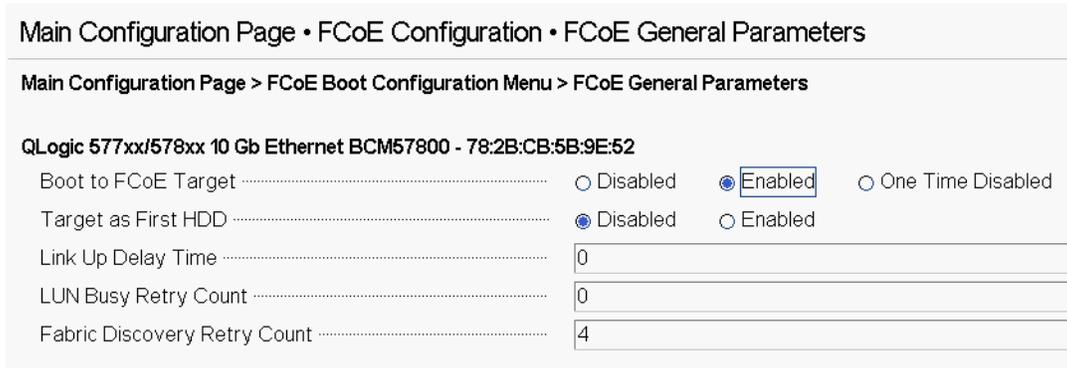


Abbildung 14-8. Menü „FCoE-Boot-Konfiguration“

4. Führen Sie im Menü „FCoE Boot Configuration“ (FCoE-Boot-Konfiguration) die folgenden Schritte aus:
 - a. Wählen Sie die Option **Enabled** (Aktiviert) für das Feld „Connect“ (Verbinden) aus.
 - b. Geben Sie das World Wide Port Name-Ziel ein.
 - c. Geben Sie die Boot-LUN ein.

5. Wählen Sie im Menü „FCoE Configuration“ (FCoE-Konfiguration) die Option **FCoE General Parameters** (Allgemeine FCoE-Parameter) aus.

Das Menü „FCoE General Parameters“ (Allgemeine FCoE-Parameter) wird angezeigt (siehe [Abbildung 14-9](#)).



Main Configuration Page • FCoE Configuration • FCoE General Parameters		
Main Configuration Page > FCoE Boot Configuration Menu > FCoE General Parameters		
QLogic 577xx/578xx 10 Gb Ethernet BCM57800 - 78:2B:CB:5B:9E:52		
Boot to FCoE Target	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled <input type="radio"/> One Time Disabled
Target as First HDD	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Link Up Delay Time	<input type="text" value="0"/>	
LUN Busy Retry Count	<input type="text" value="0"/>	
Fabric Discovery Retry Count	<input type="text" value="4"/>	

Abbildung 14-9. Menü „FCoE-Boot-Konfiguration“, Allgemeine FCoE-Parameter

6. Führen Sie im Menü „FCoE General Parameter“ (Allgemeine FCoE-Parameter) die folgenden Schritte aus:
 - a. Wählen Sie den gewünschten Modus „Boot to FCoE Target“ (Booten auf FCoE-Ziel) (siehe [Einmalige Deaktivierung](#)). Für die Erstinstallation des Betriebssystems auf einer freien FCoE Ziel-LUN von einer CD/DVD-ROM oder einem gemounteten, startfähigen Betriebssysteminstallationsabbild setzen Sie **Boot from Target** (Booten vom Zielsystem) auf **One Time Disabled** (Einmalige Deaktivierung).

Diese Einstellung verhindert, dass das System nach erfolgreicher Anmeldung und Verbindungsaufbau vom konfigurierten FCoE-Ziel bootet. Diese Einstellung wird nach dem nächsten Systemneustart automatisch auf „Enabled“ (Aktiviert) gesetzt.

Die Einstellung „Enabled“ (Aktiviert) ermöglicht, dass das System eine Verbindung mit einem FCoE-Ziel herstellt und versucht, von diesem zu booten.

Die Einstellung „Disabled“ (Deaktiviert) ermöglicht, dass das System eine Verbindung mit einem FCoE-Ziel herstellt, sie verhindert jedoch das Booten von diesem Gerät. Stattdessen wird der Boot-Vektor an das nächste bootfähige Gerät der Startfolge abgegeben.

- b. Wählen Sie den gewünschten Modus „Target as First HDD“ (Ziel als erstes HDD) aus.

Dies Einstellung legt fest, dass das ausgewählte FCoE-Ziellaufwerk als erste Festplatte im System angezeigt wird.

- c. Wählen Sie den gewünschten Wert „LUN Busy Retry Count“ (Anzahl an Wiederholungen bei „LUN besetzt“) aus.

Dieser Wert steuert die Anzahl erneuter Verbindungsversuche, die der FCoE-Boot-Initiator unternimmt, wenn das FCoE-Ziel-LUN beschäftigt ist.

- d. Wählen Sie den gewünschten Wert „Fabric Discovery Retry Count“ (Anzahl an Wiederholungen für Fabric-Ermittlung) aus.

Dieser Wert steuert die Anzahl erneuter Verbindungsversuche, die der FCoE-Boot-Initiator unternimmt, wenn das FCoE-Fabric beschäftigt ist.

Einrichten von Speicherzugriff im SAN

Zum Speicherzugriff gehören die Zoneneinrichtung und die speichergezielte LUN-Darstellung, wobei diese in der Regel pro Initiator-WWPN eingerichtet werden. Für den Speicherzugriff stehen hauptsächlich zwei Pfade zur Verfügung:

- [Vorab-Einrichtung](#)
- [STRG+R-Methode](#)

Vorab-Einrichtung

Beachten Sie bei der Vorab-Einrichtung den Initiator-WWPN, und passen Sie die Zoneneinteilung der Fabric und die speichergezielte LUN-Darstellung manuell an, um den geeigneten Zugriff für den Initiator zu ermöglichen.

Der Initiator-WWPN wird unten im Konfigurationsfenster für das FCoE-Boot-Ziel angezeigt.

Der Initiator-WWPN lässt sich auch direkt von der FIP-MAC-Adresse der vorgesehenen Schnittstelle(n) ableiten. Zwei MAC-Adressen sind auf Aufklebern aufgedruckt, die sich auf dem SFP+-Gehäuse Ihres Adapters befinden. Die FIP-MAC endet mit einer ungeraden Zahl. Der WWPN ist 20:00: + <FIP MAC>. Wenn die FIP-MAC beispielsweise 00:10:18:11:22:33 lautet, ergibt sich der WWPN 20:00:00:10:18:11:22:33.

ANMERKUNG

Der Standard-WWPN ist 20:00: + <FIP MAC>. Der Standard-WWPN ist 10:00: + <FIP MAC>.

ANMERKUNG

Bei Dell FlexAddress™ Konfigurationen wird die SAN- oder FIP-MAC möglicherweise vom Blade-Chassis-Verwaltungssystem überschrieben.

STRG+R-Methode

Mit der STRG+R-Methode können Sie den Boot-Initiator dazu verwenden, die Verbindung zu öffnen und sich bei allen verfügbaren Fabrics und Zielen anzumelden. Mit dieser Methode können Sie sicherstellen, dass der Initiator bei der Fabric bzw. dem Ziel angemeldet ist, bevor Sie Einrichtungsänderungen vornehmen, und Sie dadurch die Einrichtung ohne manuelles Eingeben der WWPNs durchführen können.

1. Konfigurieren Sie mindestens ein Boot-Ziel über CCM wie unter [Vorab-Einrichtung](#) beschrieben.
2. Stellen Sie das System so ein, dass es über den ausgewählten Initiator booten kann.

Sobald der Initiator-Boot gestartet wurde, folgen DCBX-Synchronisierung, FIP Discovery, Fabric-Anmeldung, Ziel-Anmeldung und LUN-Bereitschaftstests. Wenn der Initiator bei Abschluss der einzelnen Phasen nicht zur nächsten Phase übergehen kann, bietet der MBA die Option, die Tasten STRG+R zu drücken.
3. Drücken Sie die Tasten STRG+R.
4. Wenn STRG+R gedrückt wird, hält der Boot-Initiator eine Verbindung in der zuletzt erfolgreichen Phase aufrecht und verschafft Ihnen Zeit, die notwendigen Einrichtungskorrekturen vorzunehmen, um zur nächsten Phase überzugehen.
5. Wenn sich der Initiator bei der Fabric anmeldet, die Anmeldung beim Ziel jedoch nicht gelingt, wird der Boot-Vorgang mit STRG+R unterbrochen, und Sie können die Zoneneinteilung der Fabric konfigurieren.

Nach Abschluss der Zoneneinteilung meldet sich der Initiator automatisch bei allen sichtbaren Zielen an.
6. Wenn der Initiator die zugewiesene LUN auf dem in [Schritt 1](#) eingerichteten Ziel nicht erkennt, wird der Boot-Vorgang mit STRG+R unterbrochen, und Sie können die gezielte LUN-Darstellung konfigurieren.
7. Der Boot-Initiator sendet in regelmäßigen Abständen Bereitschaftsabfragen an die LUN, und sobald Sie den Zugriff auf die LUN eingerichtet haben, wird der Boot-Vorgang automatisch ausgeführt.

ANMERKUNG

Stellen Sie sicher, dass der Boot-Initiator in den Modus der einmaligen Deaktivierung gesetzt wird, wie in [Einmalige Deaktivierung](#) beschrieben.

Einmalige Deaktivierung

Das FCoE ROM von QLogic wird als Starteingangsvektor (Boot Entry Vector, BEV) implementiert. Bei dieser Implementierung stellt das optionale ROM nur dann eine Verbindung zum Ziel her, wenn es von BIOS als gewünschtes Boot-Gerät ausgewählt wurde. Diese Vorgehensweise unterscheidet sich von anderen Implementierungen, bei denen selbst dann eine Verbindung zum Boot-Gerät hergestellt wird, wenn ein anderes Gerät vom System-BIOS ausgewählt wurde.

Bei einer Betriebssysteminstallation über den FCoE-Pfad müssen Sie das optionale ROM anweisen, FCoE zu umgehen und zu den CD-/DVD-Installationsdatenträgern überzugehen. Wie in [„Vorbereiten des QLogic Multi-Boot-Agenten auf FCoE-Boot \(CCM-Dienstprogramm\)“ auf Seite 232](#) angewiesen, muss die Boot-Reihenfolge so konfiguriert werden, dass QLogic-Boot an erster Stelle und die Installationsdatenträger an zweiter Stelle stehen. Des Weiteren ist es während der Betriebssysteminstallation notwendig, FCoE-Boot zu umgehen und zum Booten direkt zu den Installationsdatenträgern zu springen. Dazu muss der Boot-Vorgang des FCoE-Boot-ROM einmalig deaktiviert werden. Es reicht nicht aus, zu warten, bis FCoE ROM einen Boot-Versuch startet und BIOS zu den Installationsdatenträgern wechselt. Außerdem muss das FCoE ROM erfolgreich die Boot-LUN erkennen und deren Bereitschaft ermitteln, damit die Installation ordnungsgemäß ausgeführt werden kann. Wenn es dem Boot-ROM nicht möglich ist, die LUN zu erkennen und einen koordinierten Bypass auszuführen, kann das Betriebssystem nicht ordnungsgemäß auf der LUN installiert werden.

Für den koordinierten Bypass stehen zwei Möglichkeiten zur Verfügung:

- Sobald das FCoE-Boot-ROM eine bereite Ziel-LUN erkennt, werden Sie dazu aufgefordert, innerhalb von 4 Sekunden die Tasten STRG+D zu drücken, um **Stop booting from the target** (das Booten vom Ziel zu stoppen). Drücken Sie STRG+D, und gehen Sie zum Booten von den Installationsdatenträgern über.
- Wählen Sie in CCM unter den MBA-Einstellungen für die Einstellung **Option ROM** (Optionales ROM) die Option **One Time Disabled** (Einmalige Deaktivierung) aus. Mit dieser Einstellung lädt das FCoE ROM einmal und führt einen automatischen Bypass aus, sobald die bereite LUN erkannt wird. Beim anschließenden Neustart nach der Installation wird das optionale ROM automatisch **Enabled** (aktiviert).

Warten Sie, bis alle Banner des optionalen ROM angezeigt werden. Sobald FCoE-Boot aktiviert wird, wird eine Verbindung zum Ziel hergestellt und vier Sekunden lang ein Fenster geöffnet, in dem Sie zur Bypass-Initiierung die Tasten STRG+D drücken können, wie in [Abbildung 14-10](#) dargestellt. Drücken Sie STRG+D, um die Installation durchzuführen.

```
Copyright (C) 2014 QLogic Corporation
FCoE Boot v7.12.2

Starting DCBX process with interface (00:10:18:E3:A7:A1) ... Succeeded
Discovering FC Fabric with interface (00:10:18:E3:A7:A1) ... Succeeded

World Wide Node Name : 20:00:00:10:18:E3:A7:A1
World Wide Port Name : 20:01:00:10:18:E3:A7:A1
Fabric Name          : 10:00:00:05:1E:E0:77:80
FCF MAC Address     : 00:05:1E:E0:77:87
FP MAC Address      : 0E:FC:00:02:0F:01
ULAN ID             : 1002

Fabric Login via interface (00:10:18:E3:A7:A1) ... Succeeded
Login to target [5006016346E032A2:021101:LUN=000] ... Succeeded

FC Target Drive: DGC          RAID 0          (Rev: 0430)

Press <Ctrl-D> within 4s to stop booting from the target ... _
```

Abbildung 14-10. FCoE-Boot

FCoE-Boot-Installation mit Windows 2008 R2 und Windows Server 2008 SP2

Boot-Installation unter Windows Server 2008:

1. Stellen Sie sicher, dass kein USB-Flashlaufwerk angeschlossen ist, bevor Sie das Installationsprogramm des Betriebssystems starten.
Die EVBD- und BXFCOE-Treiber müssen während der Installation geladen werden.
2. Führen Sie die regulären Schritte zur Betriebssysteminstallation aus.
3. Wenn keine Laufwerke gefunden werden, werden Sie von Windows aufgefordert, zusätzliche Treiber zu laden.
4. Schließen Sie dann ein USB-Flash-Laufwerk an, auf dem der gesamte Inhalt der bereitgestellten EVBD- und OFC-Boot-Treiberordner gespeichert ist.
Nachdem alle entsprechenden Treiber geladen sind, zeigt das Setup den/die Zieldatenträger an.
5. Trennen Sie das USB-Flashlaufwerk vor der Auswahl des Datenträgers für die Installation.

FCoE-Boot-Installation unter Windows Server 2008 SP2:

1. Laden Sie zuerst den EVBD-Treiber ([Abbildung 14-11](#)).

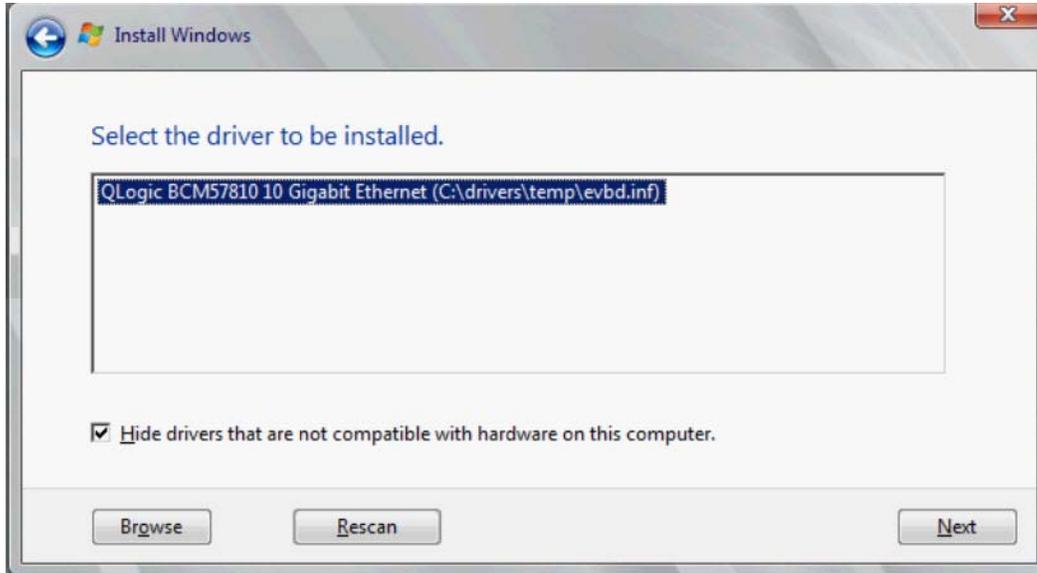


Abbildung 14-11. Installieren des EVBD-Treibers

2. Laden Sie dann den bxfcoe (OFC)-Treiber ([Abbildung 14-12](#)).

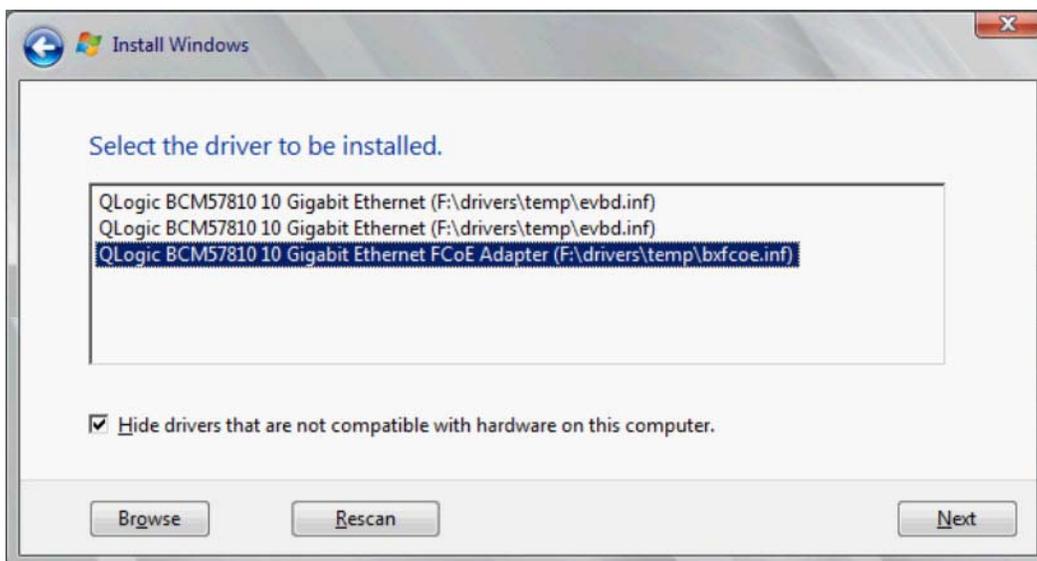


Abbildung 14-12. Installieren des bxfcoe-Treibers

3. Wählen Sie die zu installierende Boot-LUN aus ([Abbildung 14-13](#)):

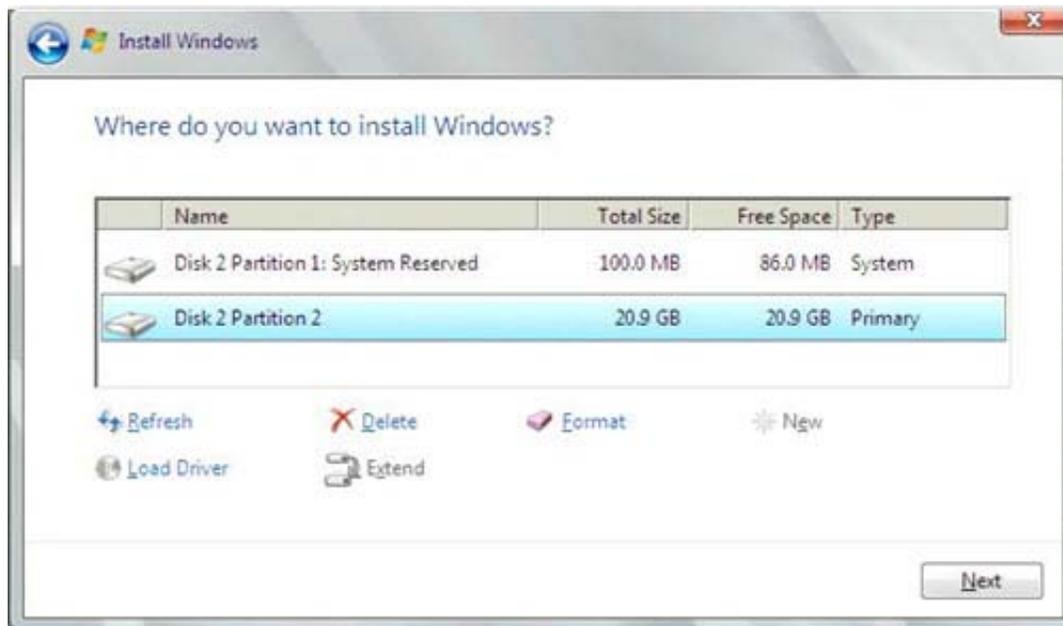


Abbildung 14-13. Auswählen der Installations-CD-Partition

4. Führen Sie die restliche Installation durch.
5. Nachdem die Installation abgeschlossen und in SAN gebootet ist, führen Sie das bereitgestellte Windows Treiberinstallationsprogramm und einen Neustart aus. Der Installationsvorgang ist nun abgeschlossen.

ANMERKUNG

Der Boot-Initiator muss so konfiguriert werden, dass er auf die gewünschte Installations-LUN zeigt, und der Boot-Initiator muss die Bereitschaft der LUN erfolgreich ermitteln und protokollieren, bevor die Installation gestartet wird. Wenn diese Anforderungen nicht erfüllt werden, werden die Geräte zwar in der obigen Laufwerkliste [Abbildung 14-13](#) angezeigt, während der Installation treten jedoch Fehler beim Lesen/Schreiben auf.

FCoE-Start-Installation für Windows Server 2012, 2012 R2 und 2016

Für Startvorgänge unter Windows Server 2012, 2012 R2 und 2016 aus einer SAN-Installation erfordert QLogic die Verwendung einer „Slipstream“-DVD oder eines ISO-Images mit den neuesten QLogic-Treibern (siehe [„Einfügen \(Slipstreaming\) der QLogic-Treiber in die Windows-Imagedateien“ auf Seite 113](#)). Weitere Informationen finden Sie auch im Microsoft Knowledge Base-Artikel KB974072 unter support.microsoft.com, der auch für FCoE-Startvorgänge von SAN unter für Windows Server 2012 und 2016 hilfreich ist. Das Verfahren von Microsoft fügt nur die OIS-, VBD- und NDIS-Treiber hinzu. QLogic empfiehlt dringend das Einfügen aller Treiber, insbesondere derer, die unten in **Fettdruck** angeführt sind:

- **EVBD**
- VBD
- BXND
- OIS
- **FCoE**
- NDIS

Sobald Sie eine korrekte Slipstream-ISO-Datei haben, können Sie diese für die normale Windows Server 2012- oder 2016-Installation verwenden, ohne dafür mitgelieferte USB-Treiber zu benötigen.

FCoE-Boot-Installation unter Linux

Konfigurieren Sie die Adapter-Boot-Parameter und die Zielinformationen (drücken Sie STRG+S, und geben Sie das CCM-Dienstprogramm ein, wie in [„Vorbereiten des System-BIOS auf FCoE-Build und -Boot“ auf Seite 231](#) beschrieben). Verwenden Sie dann die Richtlinien in den folgenden Abschnitten für die FCoE-Boot-Installation mit der passenden Linux-Version.

- [Installation von SLES 11 SP3 und SLES 12](#)
- [RHEL 6-Installation](#)
- [RHEL 7-Installation](#)

Installation von SLES 11 SP3 und SLES 12

1. So starten Sie die Installation:
 - a. Booten Sie vom SLES-Installationsmedium.
 - b. Drücken Sie auf dem Begrüßungsbildschirm F6, um den Treiberaktualisierungs-Datenträger zu laden.
 - c. Wählen Sie **Yes** (Ja) aus.
 - d. Geben Sie in den **Boot Options** (Boot-Optionen) `withfcoe=1` ein.

- e. Klicken Sie auf **Installation**, um den Vorgang fortzusetzen (Abbildung 14-14).

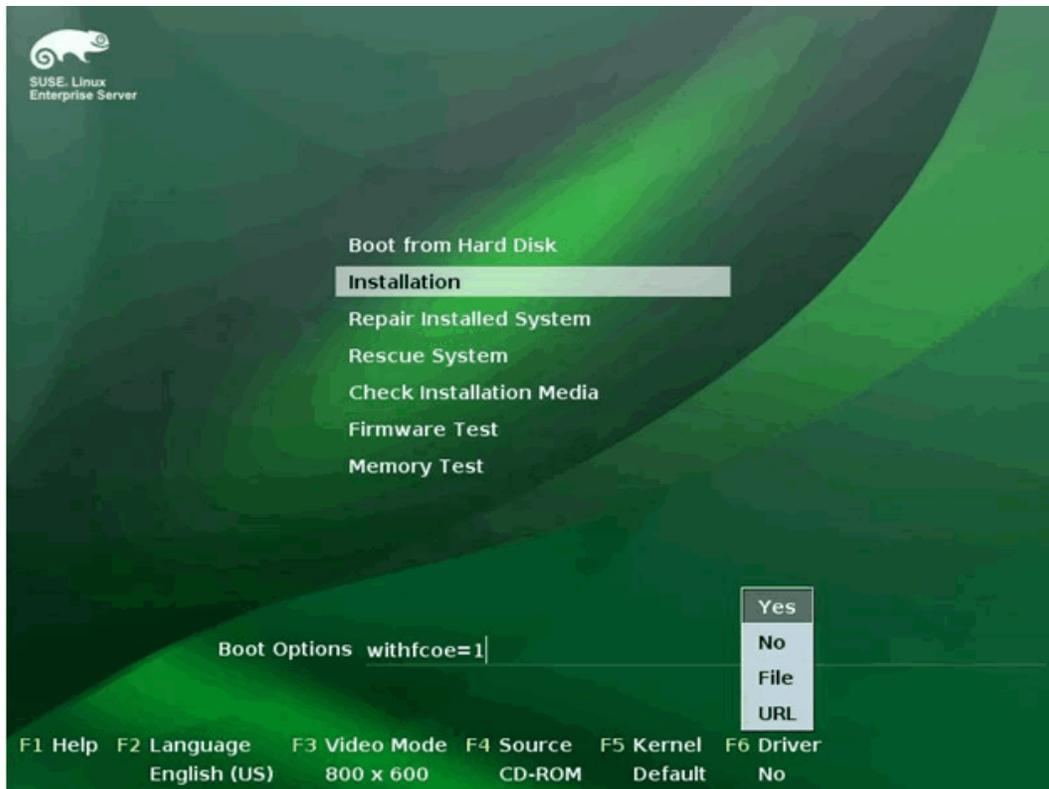


Abbildung 14-14. Starten der SLES-Installation

2. Befolgen Sie die Anweisungen, um den Datenträger zur Treiberaktualisierung ([Abbildung 14-15](#)) auszuwählen und die Treiber ([Abbildung 14-16](#)) zu laden.

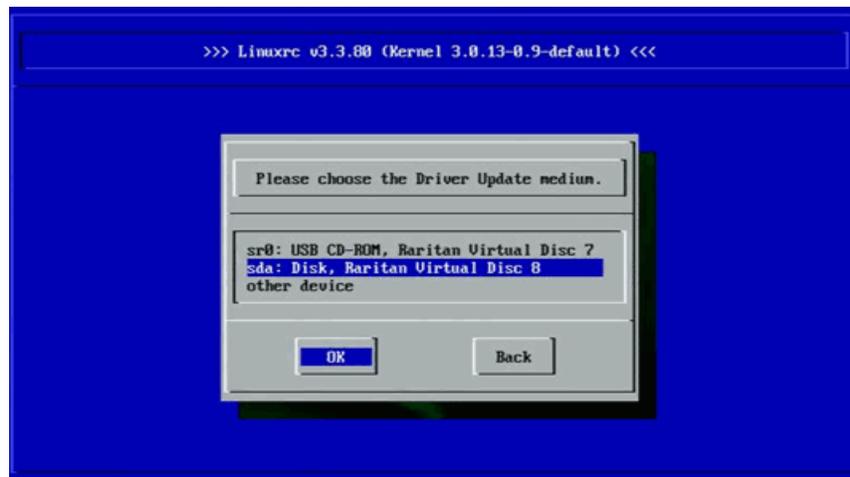


Abbildung 14-15. Auswählen des Datenträgers zur Treiberaktualisierung

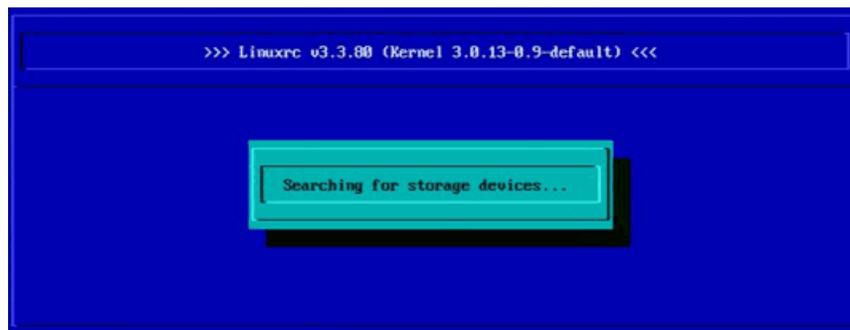


Abbildung 14-16. Laden des Treibers

3. Wählen Sie nach Abschluss der Treiberaktualisierung **Next** (Weiter) aus, um die Betriebssysteminstallation fortzusetzen.

4. Klicken Sie nach entsprechender Aufforderung auf **Configure FCoE Interfaces** (FCoE-Schnittstellen konfigurieren) (Abbildung 14-17).



Abbildung 14-17. Aktivieren des Datenträgers

5. Achten Sie darauf, dass auf den 10 GbE QLogic Initiator-Ports, die Sie als SAN-Boot-Pfad(e) ([Abbildung 14-18](#)) verwenden möchten, **FCoE Enable** (FCoE aktivieren) auf **yes** (ja) eingestellt ist.

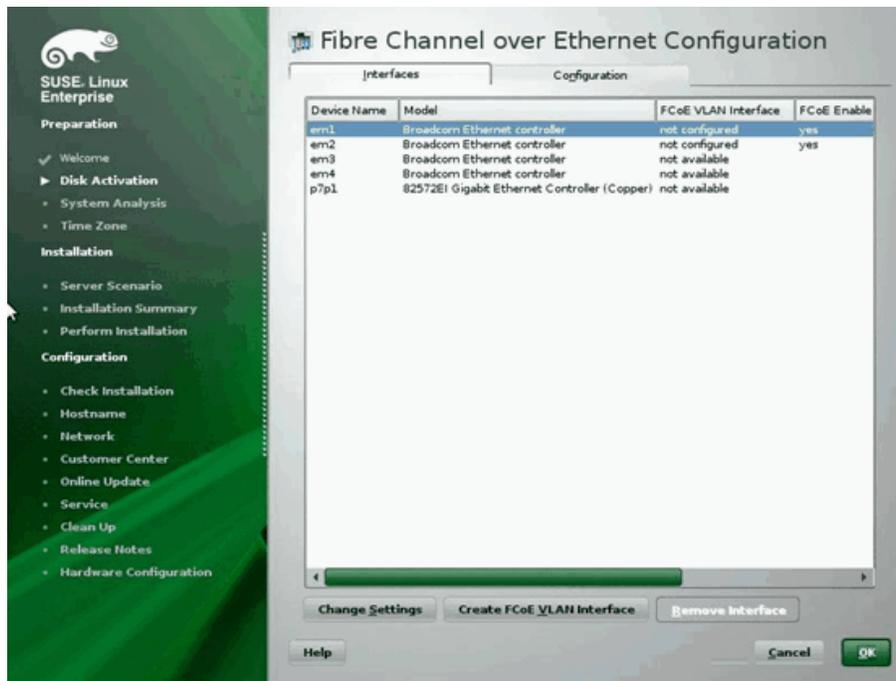


Abbildung 14-18. Aktivieren von FCoE

6. Klicken Sie für jede Schnittstelle, die für den FCoE-Boot aktiviert werden soll, auf:
 - a. **Change Settings** (Einstellungen ändern)
 - b. Stellen Sie im Fenster „Change FCoE Settings“ (FCoE-Einstellungen ändern) ([Abbildung 14-19](#)) sicher, dass **FCoE Enable** (FCoE aktivieren) und **Auto_VLAN** auf **yes** (ja) eingestellt sind.
 - c. Stellen Sie sicher, dass **DCB Required** (DCB erforderlich) auf **no** (nein) eingestellt ist.
 - d. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu speichern.



Abbildung 14-19. Ändern der FCoE-Einstellungen

7. Klicken Sie für jede Schnittstelle, die für den FCoE-Boot aktiviert werden soll, auf:
 - a. **Create FCoE VLAN Interface** (FCoE VLAN-Schnittstelle erstellen).
 - b. Klicken Sie im Dialogfeld zur Erstellung der VLAN-Schnittstelle auf **Yes** (Ja), um die automatische FIP VLAN-Erkennung zu starten.

Wenn dies gelingt, wird das VLAN unter **FCoE VLAN Interface** (FCoE VLAN-Schnittstelle) angezeigt. Wenn kein VLAN angezeigt wird, prüfen Sie die Verbindung, und wechseln Sie die Konfiguration.

8. Sobald die Konfiguration aller Schnittstellen abgeschlossen ist, klicken Sie auf **OK**, um den Vorgang fortzusetzen ([Abbildung 14-20](#)).

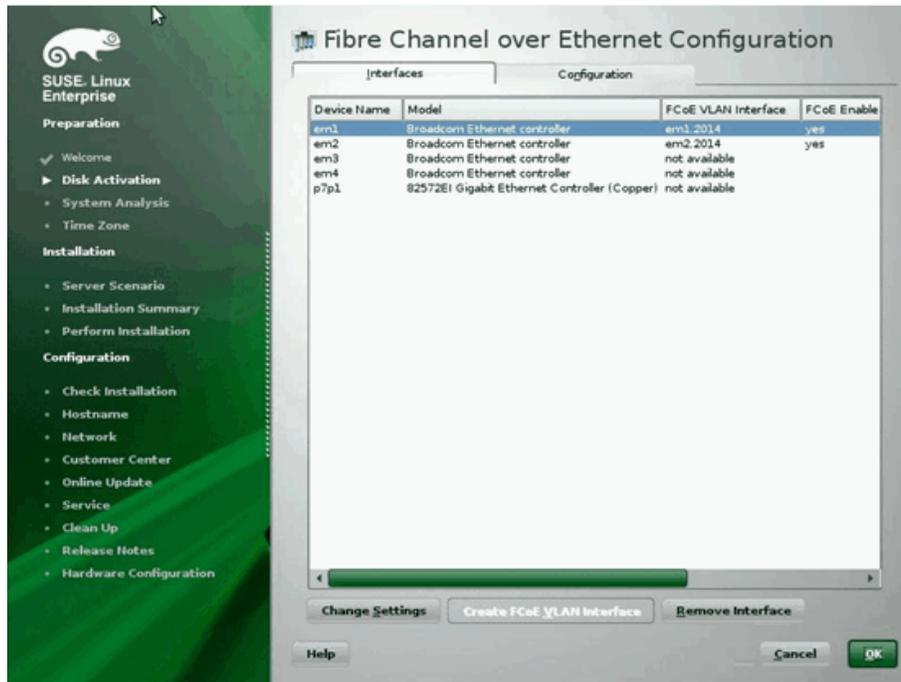


Abbildung 14-20. Konfiguration der FCoE-Schnittstelle

9. Klicken Sie auf **Next** (Weiter), um die Installation fortzusetzen.

10. Sie werden von YaST2 aufgefordert, Multipath zu aktivieren. Antworten Sie entsprechend ([Abbildung 14-21](#)).



Abbildung 14-21. Aktivieren des Datenträgers

11. Setzen Sie die Installation wie gewohnt fort.

12. Klicken Sie auf der Seite „Expert“ (Experte) im Fenster „Installation Settings“ (Installationseinstellungen) auf **Booting** (Booten) (Abbildung 14-22).

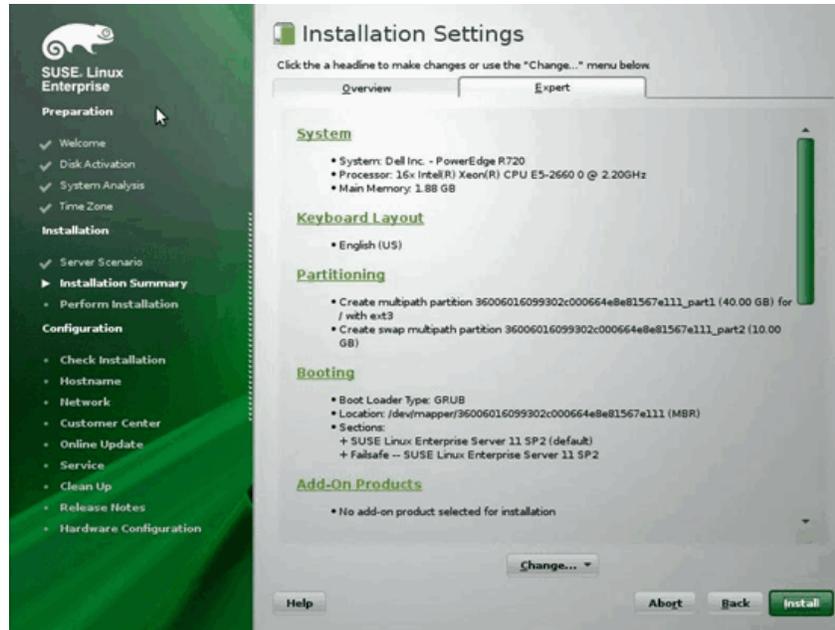


Abbildung 14-22. Installationseinstellungen

13. Klicken Sie auf die Registerkarte **Boot Loader Installation** (Installation des Bootloaders), und wählen Sie anschließend **Boot Loader Installation Details** (Einzelheiten zur Installation des Bootloaders) aus. Stellen Sie sicher, dass nur eine Eingabe für den Bootloader vorhanden ist. Löschen Sie alle übrigen Eingaben (*Abbildung 14-23*).



Abbildung 14-23. Bootlader-Gerätezuweisungstabelle

14. Klicken Sie auf **OK**, und stellen Sie die Installation fertig.

RHEL 6-Installation

FCoE-Boot-Installation unter Linux bei RHEL 6:

1. Booten Sie vom Installationsmedium. Anweisungen für RHEL 6.3 und 6.4 variieren.

Für RHEL 6.3:

- a. Für FCoE BFS wird ein aktualisiertes Anaconda-Image benötigt. Dieses aktualisierte Image wird von Red Hat unter der folgenden URL bereitgestellt:

<http://rvykydal.fedorapeople.org/updates.823086-fcoe.img>

- b. Auf dem Begrüßungsbildschirm:

- (1) Drücken Sie die TAB (Tabulator) taste.

- (2) Fügen Sie die Option

dd updates=<URL_TO_ANACONDA_UPDATE_IMAGE> zu der Boot-Befehlszeile hinzu.

(3) Drücken Sie zum Fortfahren die ENTER (Eingabe) taste.
Lesen Sie das *Red Hat-Installationshandbuch*, Abschnitt 28.1.3, um Einzelheiten zur Installation des aktualisierten Anaconda-Images zu erfahren.

http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Installation_Guide/ap-admin-options.html#sn-boot-options-update

Für RHEL ab Version 6.4:

Es wird kein aktualisiertes Anaconda-Image benötigt.

- a. Drücken Sie im Installationsbegrüßungsfenster auf die TABULATOR-TASTE.
- b. Fügen Sie die Option `dd` zu der Boot-Befehlszeile hinzu, wie in [Abbildung 14-24](#) beschrieben.
- c. Drücken Sie zum Fortfahren die ENTER (Eingabe) taste.

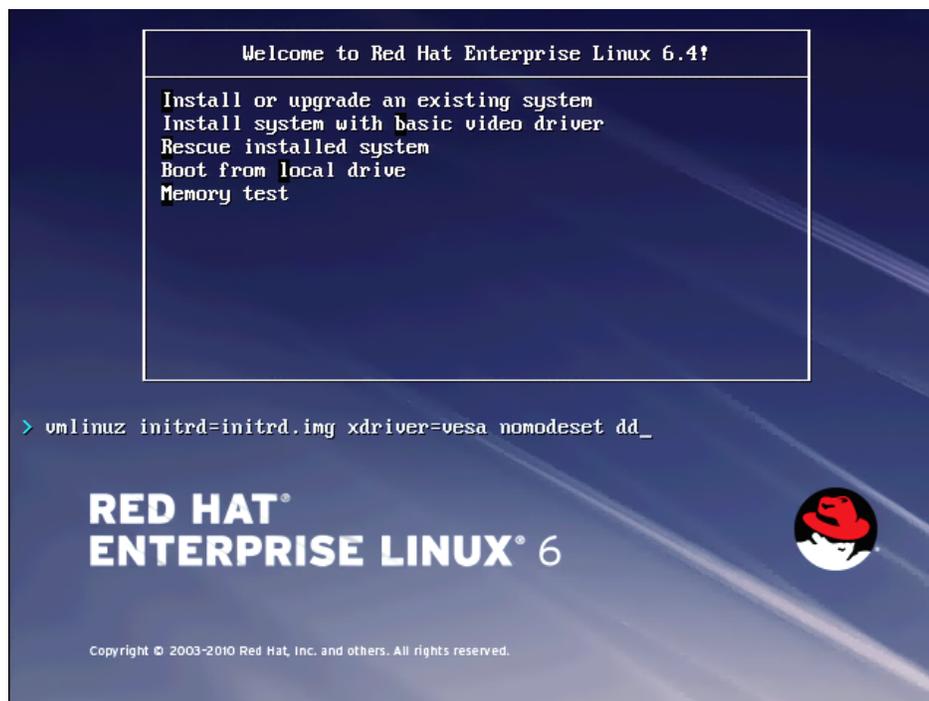


Abbildung 14-24. Hinzufügen der dd-Option

2. Antworten Sie auf die angezeigte Frage **Do you have a driver disk** (Haben Sie einen Treiberdatenträger) mit **Yes** (Ja) (Abbildung 14-25).

ANMERKUNG

RHEL erlaubt nicht, dass Datenträger für die Treiberaktualisierung über das Netzwerk geladen werden, wenn Treiberaktualisierungen für Netzwerkgeräte installiert werden. Verwenden Sie lokale Datenträger.

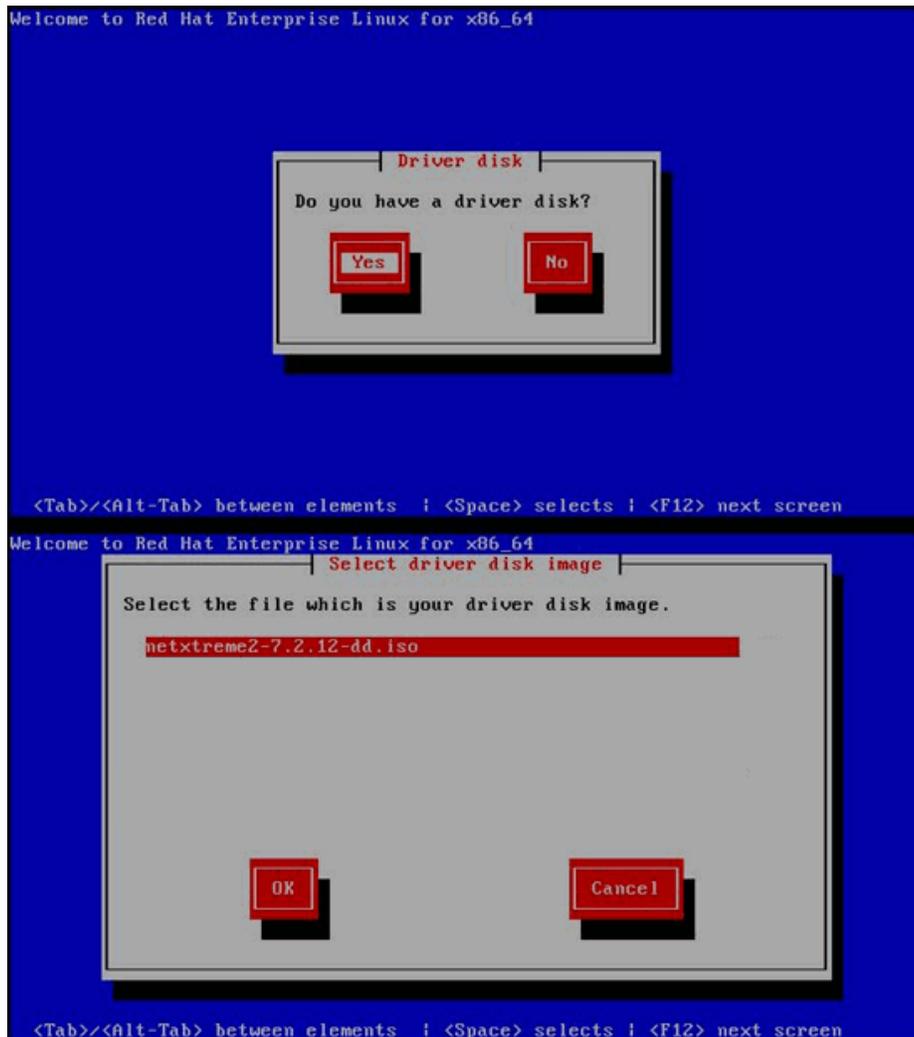


Abbildung 14-25. Auswählen eines Treiberdatenträgers

3. Fahren Sie mit der Installation fort, sobald die Treiber geladen sind.
4. Wählen Sie **Specialized Storage Devices** (Spezielle Speichergeräte) aus, wenn Sie dazu aufgefordert werden.

5. Klicken Sie auf **Add Advanced Target** (Erweitertes Ziel hinzufügen).
6. Wählen Sie **Add FCoE SAN** (FCoE SAN hinzufügen) aus und klicken Sie anschließend auf **Add drive** (Laufwerk hinzufügen) ([Abbildung 14-26](#)).

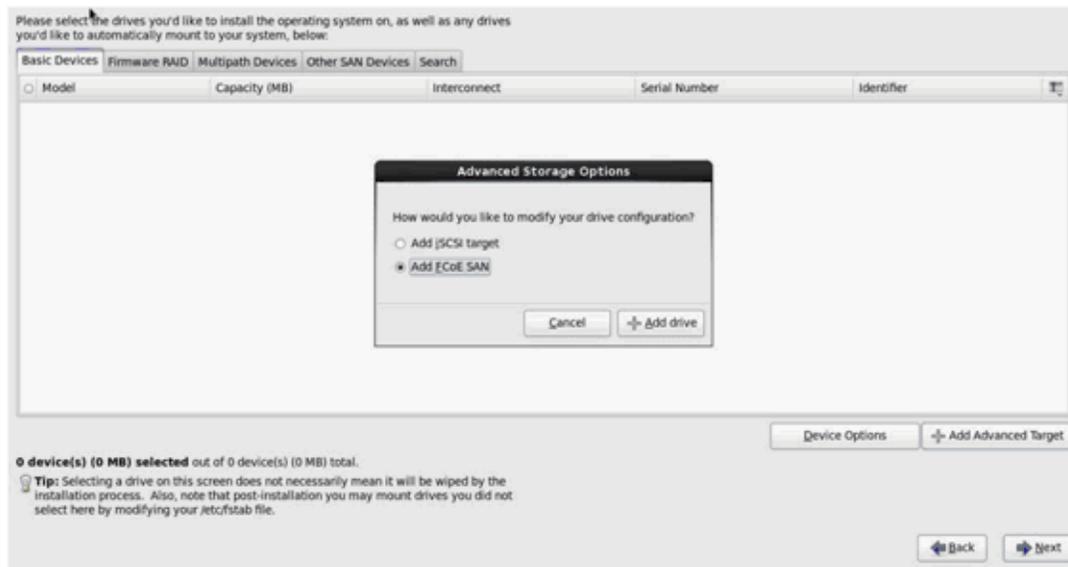


Abbildung 14-26. Hinzufügen eines FCoE SAN-Treibers

- Wählen Sie für jede Schnittstelle, die für den FCoE-Boot aktiviert werden soll, die Schnittstelle aus, heben Sie die Auswahl des Kontrollkästchens **Use DCB** (DCB verwenden) auf, wählen Sie **Use auto vlan** (Auto VLAN verwenden) aus, und klicken Sie anschließend auf **Add FCoE Disk(s)** (FCoE-Datenträger hinzufügen) (Abbildung 14-27).

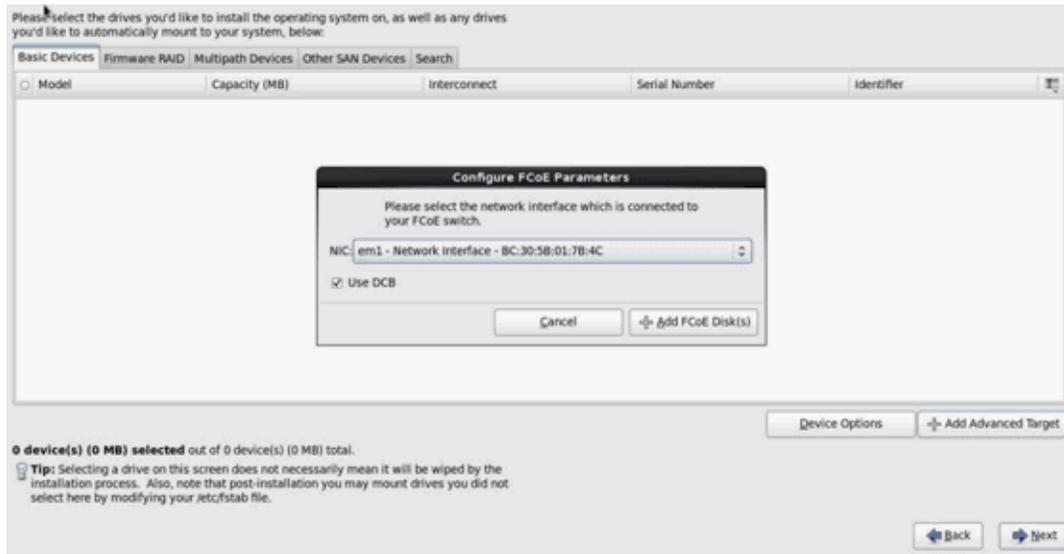


Abbildung 14-27. Konfigurieren von FCoE-Parametern

- Wiederholen Sie die Schritte 8 bis 10 für alle Initiator-Ports.
- Prüfen Sie, ob alle sichtbaren FCoE-Datenträger unter „Multipath Devices“ (Multipath-Geräte) und/oder „Other SAN Devices“ (Andere SAN-Geräte) (Abbildung 14-28) angezeigt werden.

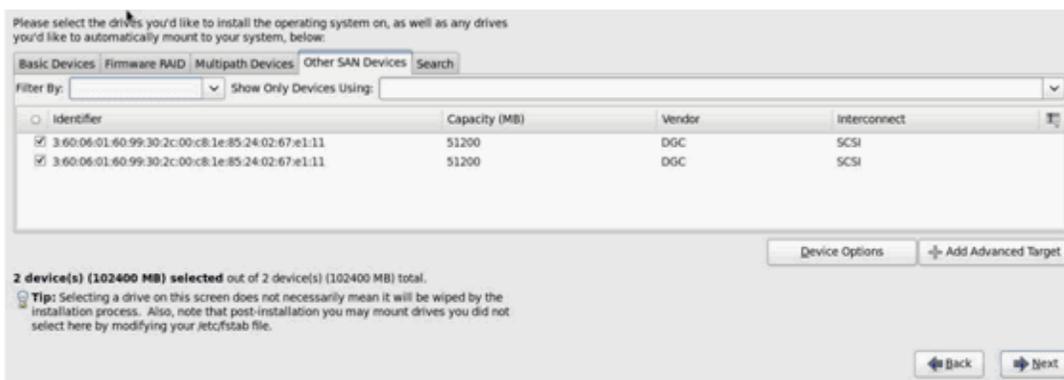


Abbildung 14-28. Bestätigen von FCoE-Treibern

- Klicken Sie auf **Next** (Weiter), um den Vorgang fortzusetzen.

11. Klicken Sie auf **Next** (Weiter), und stellen Sie die Installation wie gewohnt fertig.
Nach dem Abschluss der Installation wird das System neu gestartet.
12. Stellen Sie nach dem Neustart sicher, dass alle Boot-Pfad-Geräte so eingestellt sind, dass sie beim Booten gestartet werden. Legen Sie den Wert **onboot=yes** unter jeder `config`-Datei für die Netzwerkschnittstelle in `/etc/sysconfig/network-scripts` fest.
13. **Nur bei RHEL 6.4:** Bearbeiten Sie `/boot/grub/menu.lst` wie folgt:
 - a. Löschen Sie alle Parameter der Art `fcoe=<INTERFACE>:nodcb` aus der Zeile `kernel /vmlinuz ...`. Dort sollten sich so viele `fcoe=-`Parameter befinden, wie FCoE-Schnittstellen bei der Installation konfiguriert wurden.
 - b. Fügen Sie `fcoe=edd:nodcb` in die Zeile `kernel /vmlinuz ...` ein.

RHEL 7-Installation

So führen Sie die FCoE-Boot-Installation unter Linux bei RHEL 7 durch:

1. Booten Sie vom Installationsmedium.
2. Drücken Sie auf dem Begrüßungsbildschirm die TAB (Tabulator) taste.
3. Fügen Sie die Option `dd` zu der Boot-Befehlszeile hinzu, wie in [Abbildung 14-29](#) beschrieben.

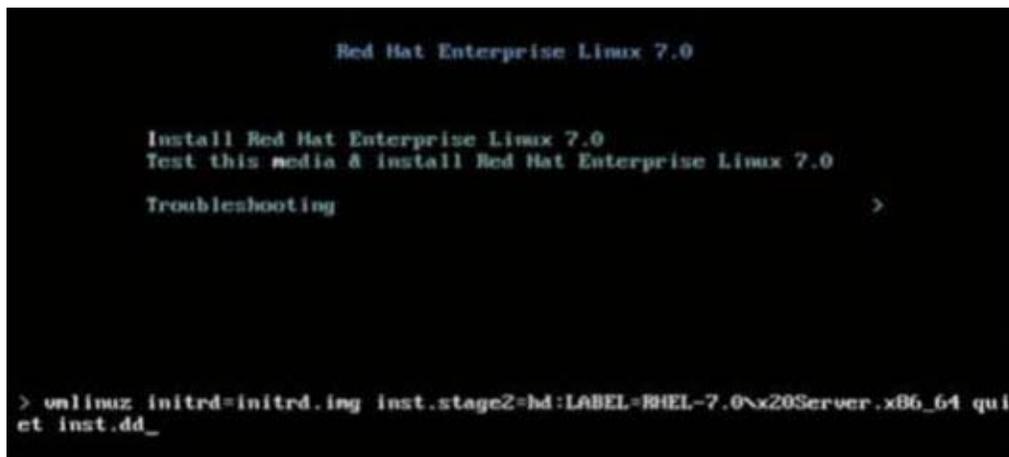


Abbildung 14-29. Hinzufügen der dd-Option

4. Drücken Sie zum Fortfahren die ENTER (EINGABE)-Taste.

5. Bei Aufforderung zur **Driver disk device selection** (Auswahl des Treiberdatenträger-Geräts):
 - a. Aktualisieren Sie die Geräteliste, indem Sie die Taste R drücken.
 - b. Geben Sie die entsprechende Zahl für Ihre Datenträger ein.
 - c. Drücken Sie die Taste C, um fortzufahren.

ANMERKUNG

RHEL erlaubt nicht, dass Datenträger für die Treiberaktualisierung über das Netzwerk geladen werden, wenn Treiberaktualisierungen für Netzwerkgeräte installiert werden. Verwenden Sie lokale Datenträger.

6. Fahren Sie durch Drücken von „C“ mit der Installation fort, sobald die Treiber geladen sind.
7. Klicken Sie im Fenster „Installation Summary“ (Installationszusammenfassung) auf **Installation Destination** (Installationsziel).
8. Klicken Sie im Fenster „Installation Destination“ (Installationsziel) unter **Specialized & Network Disks** (Spezial- und Netzwerkdatenträger) auf **Add a disk** (Datenträger hinzufügen).
9. Klicken Sie auf der Seite „Search“ (Suche) auf **Add FCoE SAN** (FCoE SAN hinzufügen).
10. Füllen Sie das Dialogfeld „Please Select the Network Interface“ (Bitte wählen Sie die Netzwerkschnittstelle aus...) wie folgt aus:
 - a. Wählen Sie die entsprechende **NIC** aus.
 - b. Deaktivieren Sie das Kontrollkästchen **Use DCB** (DCB verwenden).
 - c. Klicken Sie auf **Add FCoE Disk(s)** (FCoE-Datenträger hinzufügen).
11. Wählen Sie auf der Seite „Search“ (Suche) den neu hinzugefügten Datenträger, und klicken Sie anschließend auf **Done** (Fertig).

12. Wählen Sie im Fenster „Installation Destination“ (Installationsziel) ([Abbildung 14-30](#)) unter **Other Storage Options** (Andere Speicheroptionen) Ihre **Partitioning** (Partitionierungs) optionen, und klicken Sie dann auf **Done** (Fertig).

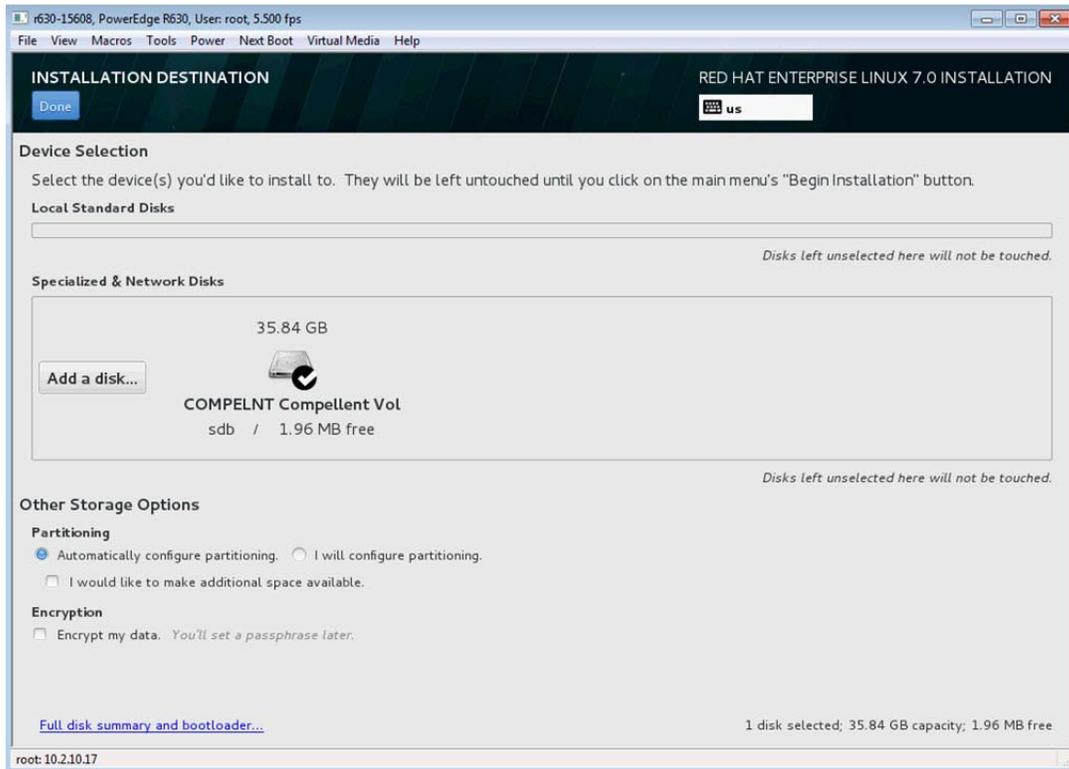


Abbildung 14-30. Auswählen von Partitionierungsoptionen

13. Klicken Sie im Fenster „Installation Summary“ (Installationszusammenfassung) auf **Begin Installation** (Installation starten).

Linux: Hinzufügen von Boot-Pfaden

RHEL erfordert eine Aktualisierung der Netzwerkkonfiguration, wenn neue Boots über einen FCoE-Initiator hinzugefügt werden, der nicht während der Installation konfiguriert wurde.

RHEL ab Version 6.2

Wenn das System unter RHEL ab Version 6.2 so konfiguriert ist, dass der Boot über einen Initiator-Port erfolgt, der zuvor nicht im Betriebssystem konfiguriert wurde, startet das System automatisch erfolgreich, erzeugt jedoch Probleme beim Herunterfahren. Alle neuen Initiator-Ports für den Boot-Pfad müssen im Betriebssystem konfiguriert werden, bevor die FCoE-Boot-Parameter für den Pre-Boot aktualisiert werden.

1. Ermitteln Sie die Netzwerkschnittstellennamen für die neu hinzugefügten Schnittstellen über `ifconfig -a`.
2. Bearbeiten Sie `/boot/grub/menu.lst`, indem Sie für jede neue Schnittstelle `ifname=<INTERFACE>:<MAC_ADDRESS>` der Zeile `kernel /vmlinuz ...` hinzufügen. Die MAC-Adresse muss in Kleinbuchstaben geschrieben und durch einen Doppelpunkt getrennt werden. (z.B.: `ifname=em1:00:00:00:00:00:00`)
3. Erstellen Sie eine Datei der Art `/etc/fcoe/cfg-<INTERFACE>` für jeden neuen FCoE-Initiator, indem Sie die bereits während der Erstinstallation konfigurierte Datei `/etc/fcoe/cfg-<INTERFACE>` duplizieren.
4. Geben Sie den folgenden Befehl aus:
`nm-connection-editor`
 - a. Öffnen Sie **Network Connection** (Netzwerkverbindung), und wählen Sie jede neue Schnittstelle aus.
 - b. Konfigurieren Sie jede Schnittstelle wie gewünscht, einschließlich der DHCP-Einstellungen.
 - c. Klicken Sie auf **Apply** (Anwenden), um die Änderung zu speichern.
5. Bearbeiten Sie für jede neue Schnittstelle `/etc/sysconfig/network-scripts/ifcfg-<INTERFACE>`, um die Zeile `NM_CONTROLLED="no"` hinzuzufügen. Die Änderung dieser Dateien führt automatisch zu einem Neustart des Netzwerkdienstes, was dazu führen kann, dass das System kurzzeitig nicht mehr zu reagieren scheint. QLogic empfiehlt Ihnen sicherzustellen, dass redundante Multipath-Pfade verfügbar sind.

FCoE-Boot-Installation unter VMware ESXi

Der FCoE-Boot von SAN erfordert, dass die neuesten QLogic BCM57xx und BCM57xxx-Async-Treiber im ESXi 6.0 U2- und 6.5-Image enthalten sind. Informationen zum Slipstreaming von Treibern finden Sie im Dokument [Image_builder_doc.pdf](#) von VMware. [Tabelle 14-1](#) zeigt die unterstützte Legacy BFS und uEFI BFS.

Table 14-1. Unterstützte Legacy BFS und uEFI BFS

Version	Legacy-BFS	uEFI-BFS
ESXi 6.0 U2	Unterstützt	Unterstützt
ESXi 6.5	Unterstützt	Unterstützt

So führen Sie eine ESXi FCoE-Boot-Installation aus:

1. Booten Sie über das aktualisierte ESXi 6.0 U2-Installations-Image und wählen Sie bei Aufforderung das **ESXi 6.0 U2 installer** (ESXi 6.0 U2-Installationsprogramm).
2. Drücken Sie im Fenster „Welcome to the VMware ESXi installation“ (Willkommen zur VMware ESXi-Installation) die EINGABETaste, um fortzufahren.
3. Drücken Sie im EULA-Fenster die Taste F11, um die Bedingungen zu akzeptieren und fortzufahren.
4. Scrollen Sie im Fenster „Select a Disk“ (einen Datenträger auswählen) ([Abbildung 14-31](#)) zu der Boot-LUN für die Installation aus, und drücken Sie die EINGABETASTE, um fortzufahren.

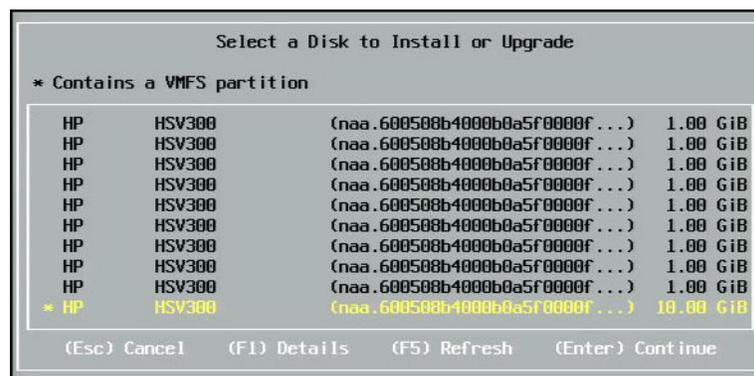


Abbildung 14-31. Auswählen eines ESXi-Datenträgers

5. Wählen Sie im Fenster „ESXi and VMFS Found“ (ESXi und VMFS gefunden) ([Abbildung 14-32](#)) die Installationsmethode.

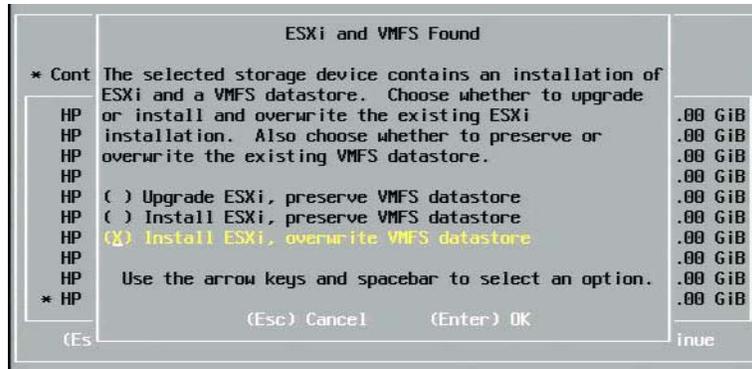


Abbildung 14-32. ESXi und VMFS gefunden

6. Folgen Sie den Eingabeaufforderungen:
- Wählen Sie das Tastaturlayout.
 - Geben Sie das Stammkennwort ein und bestätigen Sie es.
7. Drücken Sie im Fenster „Confirm Install“ (Installation bestätigen) ([Abbildung 14-33](#)) die Taste F11, um die Installation und neue Partitionierung zu bestätigen.



Abbildung 14-33. ESXi Installation bestätigen

8. Drücken Sie zum Neustart nach erfolgreicher Installation ([Abbildung 14-34](#)) die EINGABETASTE.



Abbildung 14-34. ESXi Installation abgeschlossen

- Bei 57800- und 57810-Boards ist das Managementnetzwerk nicht vmnic0. Öffnen Sie nach dem Starten die GUI-Konsole und rufen Sie den Bildschirm „Configure Management Network“ (Managementnetzwerk konfigurieren) und dann das Fenster „Network Adapters“ (Netzwerkadapter) (Abbildung 14-35) auf, um die NIC auszuwählen, die als Management-Netzwerkgerät verwendet werden soll.

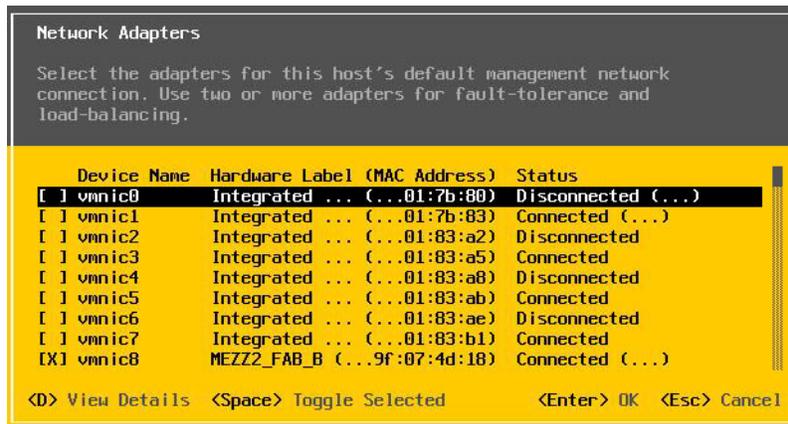


Abbildung 14-35. Auswahl des ESXi-Managementnetzwerks

- Bei BCM57800- und BCM57810-Boards müssen die FCoE-Boot-Geräte über einen separaten vSwitch außer vSwitch0 verfügen. Mit diesem Switch kann DHCP die IP-Adresse dem Managementnetzwerk anstatt dem FCoE-Boot-Gerät zuweisen. Um einen vSwitch für die FCoE-Boot-Geräte zu erstellen, fügen Sie das Boot-Gerät vmnics im vSphere-Client auf der Konfigurationsseite unter **Networking** (Netzwerkbetrieb) hinzu.

Abbildung 14-36 zeigt ein Beispiel.

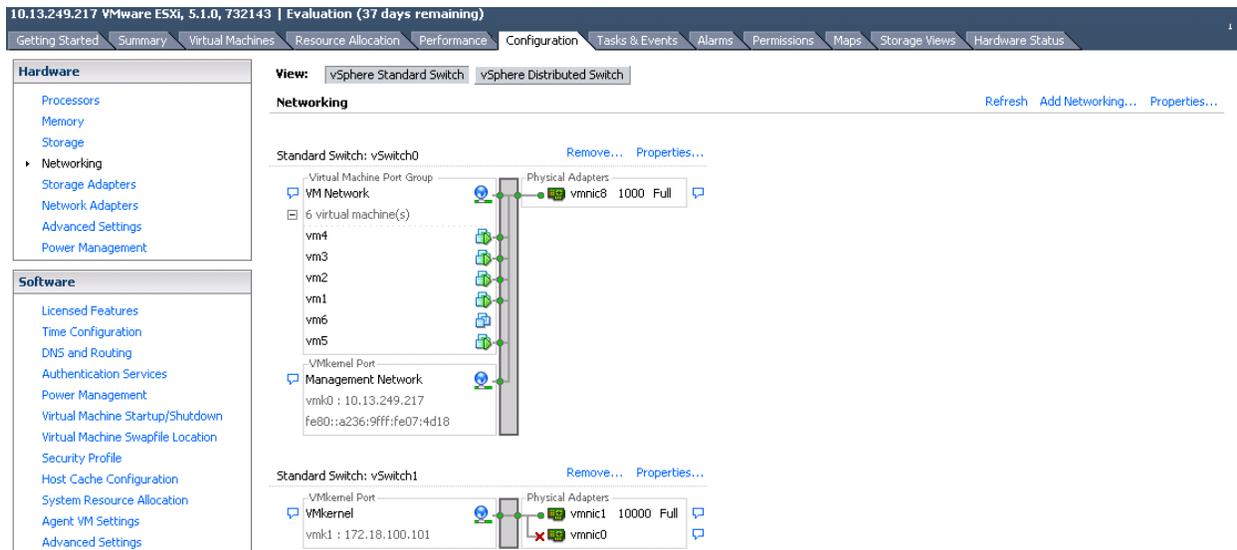


Abbildung 14-36. Netzwerk-Konfiguration des VMware vSphere Client

Konfigurieren des FCoE-Boot von SAN unter VMware

Beachten Sie, dass jeder Host nur Zugriff auf seine eigene Boot-LUN haben darf, nicht auf die Boot-LUNs der anderen Hosts. Verwenden Sie Speichersystem-Software, um sicherzustellen, dass der Host nur auf die zugewiesenen LUNs zugreift.

Booten von SAN nach der Installation

Nachdem die Boot-Konfiguration und die Betriebssysteminstallation abgeschlossen sind, können Sie einen Neustart durchführen und die Installation testen. Bei diesem und allen zukünftigen Neustarts ist keine Interaktion des Benutzers erforderlich. Ignorieren Sie die STRG+D-Aufforderung, und erlauben Sie dem System das Booten zur FCoE SAN LUN, wie in [Abbildung 14-37](#) dargestellt.

```
Copyright (C) 2014 QLogic Corporation
FCoE Boot v7.12.2

Starting DCBX process with interface (00:10:18:E3:A7:A1) ... Succeeded
Discovering FC Fabric with interface (00:10:18:E3:A7:A1) ... Succeeded

World Wide Node Name : 20:00:00:10:18:E3:A7:A1
World Wide Port Name : 20:01:00:10:18:E3:A7:A1
Fabric Name          : 10:00:00:05:1E:E0:77:80
FCF MAC Address      : 00:05:1E:E0:77:87
FP MAC Address       : 0E:FC:00:02:0F:01
ULAN ID              : 1002

Fabric Login via interface (00:10:18:E3:A7:A1) ... Succeeded
Login to target [5006016346E032A2:021101:LUN=000] ... Succeeded

FC Target Drive: DGC          RAID 0          (Rev: 0430)

Press <Ctrl-D> within 4s to stop booting from the target ... _
```

Abbildung 14-37. Booten von SAN nach der Installation

Wenn zusätzliche redundante Failover-Pfade benötigt werden, können Sie diese Pfade über CCM konfigurieren, und der MBA führt ein automatisches Failover zu sekundären Pfaden durch, wenn der erste Pfad nicht verfügbar ist. Des Weiteren ergeben die redundanten Boot-Pfade redundante Pfade, die über Host-MPIO-Software sichtbar werden, sodass eine fehlertolerante Konfiguration ermöglicht wird.

Treiberaktualisierung unter Linux-Boot von SAN-Systemen

1. Entfernen Sie das vorhandene installierte BCM57xx und BCM57xxx-Paket folgendermaßen:

- a. Melden Sie sich als root-Benutzer an.
- b. Abfrage für das vorhandene BCM57xx und BCM57xxx-Paket.
- c. Entfernen Sie es, indem Sie die folgenden Befehle ausführen:

```
# rpm -e <BCM57xx and BCM57xxx-package name>
```

Zum Beispiel:

```
rpm -e netxtreme2
```

oder:

```
rpm -e netxtreme2-x.y.z-1.x86_64
```

2. Installieren Sie die binäre RPM-Datei mit der neuen Treiberversion. Lesen Sie für Anweisungen zur Vorbereitung eines binären Treiber-RPM die Info (README)-Datei zum linux-nx2-Paket.
3. Geben Sie den folgenden Befehl zur Aktualisierung der Ramdisk aus:
 - Führen Sie auf RHEL 6.x-Systemen den folgenden Befehl aus:
dracut -force
 - Führen Sie auf SLES 11 SPX-Systemen den folgenden Befehl aus:
mkinitrd
4. Wenn Sie einen anderen Namen für die initrd unter `/boot` verwenden:
 - a. Überschreiben Sie ihn mit den standardmäßigen Namen, da `dracut/mkinitrd` die Ramdisk mit dem standardmäßigen ursprünglichen Namen aktualisiert.
 - b. Stellen Sie sicher, dass der entsprechende Eintrag für den Boot über das SAN-Setup den richtigen oder aktualisierten `initrd`-Namen in `/boot/grub/menu.lst` verwendet.
5. Um die Treiberaktualisierung abzuschließen, starten Sie das System neu, und wählen Sie den geänderten Eintrag „grub boot“ aus, der die aktualisierte `initrd` enthält.

Fehler während des FCoE-Boots der SAN-Installation unter Windows

Wenn ein USB-Stick angeschlossen ist, während das Windows-Setup Dateien für die Installation lädt, wird eine Fehlermeldung angezeigt, wenn Sie die Treiber bereitstellen und anschließend die SAN-Disk für die Installation auswählen. Die häufigste Fehlermeldung im Windows-Installationsprogramm lautet *„We couldn't create a new partition or locate an existing one* (Es konnte keine neue Partition erstellt oder keine vorhandene Partition gefunden werden). *For more information, see the setup log files* (Weitere Informationen finden Sie in den Setup-Protokolldateien)“ (siehe [Abbildung 14-38](#)).

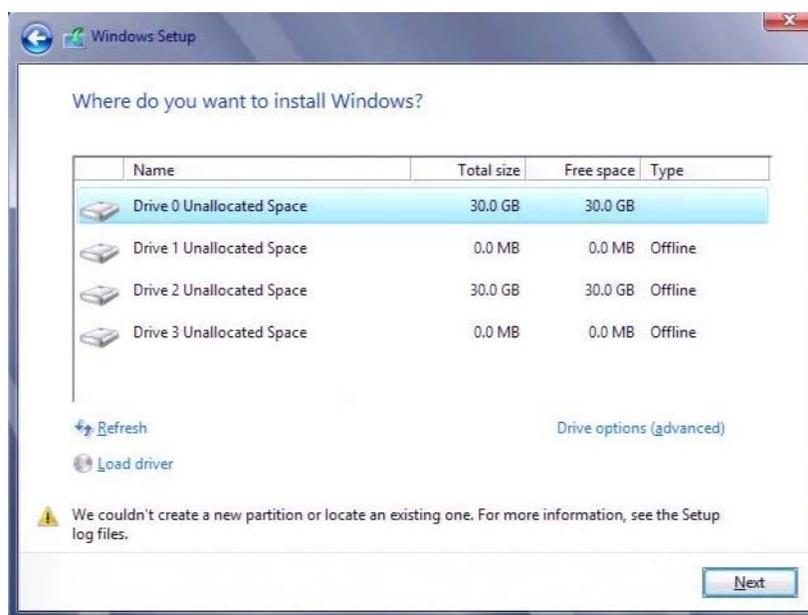


Abbildung 14-38. Windows-Fehlermeldung zu Partition

In anderen Fällen kann die Fehlermeldung Sie auffordern sicherzustellen, dass der Festplattencontroller des Datenträgers im BIOS-Menü des Computers aktiviert ist.

Zur Vermeidung einer der oben genannten Fehlermeldungen müssen Sie sicherstellen, dass kein USB-Stick angeschlossen ist, bis das Setup nach den Treibern fragt. Nachdem Sie die Treiber geladen haben und Ihre SAN-Disk(s) sehen, trennen Sie das USB-Flashlaufwerk sofort, bevor Sie die Festplatte für die weitere Installation auswählen.

Konfigurieren von FCoE

DCB ist standardmäßig auf QLogicBCM57xx und BCM57xxx FCoE-, DCB-kompatiblen C-NICs aktiviert. QLogic BCM57xx und BCM57xxx FCOE erfordert eine DCB-fähige Schnittstelle. Verwenden Sie auf Windows-Betriebssystemen eine der folgenden Komponenten für die Konfiguration der DCB-Parameter.

- QCC-Benutzeroberfläche
- QCC-PowerKit
- QLogic Control Suite (QCS)-Befehlszeilenschnittstelle
- Seite für die Server-BIOS-UEFI-HII-Gerätekonfiguration
- QLogic Comprehensive Configuration Management (CCM)-Dienstprogramm

Weitere Informationen zu QCS finden Sie im Benutzerhandbuch *User's Guide, QLogic Control Suite CLI* mit der Teilenummer BC0054511-00, das Sie von Cavium Inc. beziehen können.

Bei FCoE-Offload müssen bei den BCM57xx und BCM57xxx-Adaptern die Funktionen für den FCoE-Offload und DCB aktiviert werden.

- Verwenden Sie bei allen Betriebssystemen das Pre-Boot-CCM-Dienstprogramm von QLogic oder die Seite für die Pre-Boot-BIOS-UEFI-HII-Gerätekonfiguration des Servers für die Konfiguration der DCB-Parameter.
 - Weitere Informationen zu FCoE auf dem VMware-BS finden Sie im Abschnitt „Unterstützung von FCoE“ im Handbuch *User's Guide, Converged Network Adapters and Intelligent Ethernet Adapters, QLogic FastLinQ 3400 and 8400 Series* (Teilenummer 83840-546-00). Hinweise zum Speicherort dieses Dokuments finden Sie unter [„Herunterladen von Dokumenten“](#) auf Seite xxiii.
 - Informationen zu FCoE auf dem Linux-BS finden Sie im Abschnitt „Installieren der Linux-Treibersoftware“ im Handbuch *User's Guide, Converged Network Adapters and Intelligent Ethernet Adapters, QLogic FastLinQ 3400 and 8400 Series*. Hinweise zum Speicherort dieses Dokuments finden Sie unter [„Herunterladen von Dokumenten“](#) auf Seite xxiii.
 - Verwenden für FCoE auf dem Windows-BS die QCC-Benutzeroberfläche, die QCS-Befehlszeilenschnittstelle oder QCC PowerKit, um die FCoE-Offload-Instanz pro Port unter Windows im Einzelfunktionsmodus zu aktivieren oder zu deaktivieren.

Um den iSCSI-Offload im NPAR-Modus zu konfigurieren, verwenden Sie die NPAR-Konfigurationsseite in einer der folgenden Anwendungen:

- QCC-Benutzeroberfläche
- QCS-Befehlszeilenschnittstelle
- QCC PowerKit
- Pre-Boot-Server UEFI HII
- Pre-Boot-CCM

Gehen Sie wie folgt vor, um die FCoE-Offload-Instanz auf Windows über die QCC-Benutzeroberfläche zu aktivieren oder zu deaktivieren:

1. Öffnen Sie die QCC-Benutzeroberfläche.
2. Wählen Sie im Fensterbereich für die Baumstruktur auf der linken Seite unter dem Port-Knoten die virtuelle Bus-Geräteinstanz des Ports aus.
3. Klicken Sie im Konfigurationsfensterbereich auf der rechten Seite auf die Registerkarte **Port Info** (Port-Info).

Daraufhin wird die Seite „**Resource Config**“ (Ressourcenkonfiguration) angezeigt (siehe [Abbildung 14-39](#)).

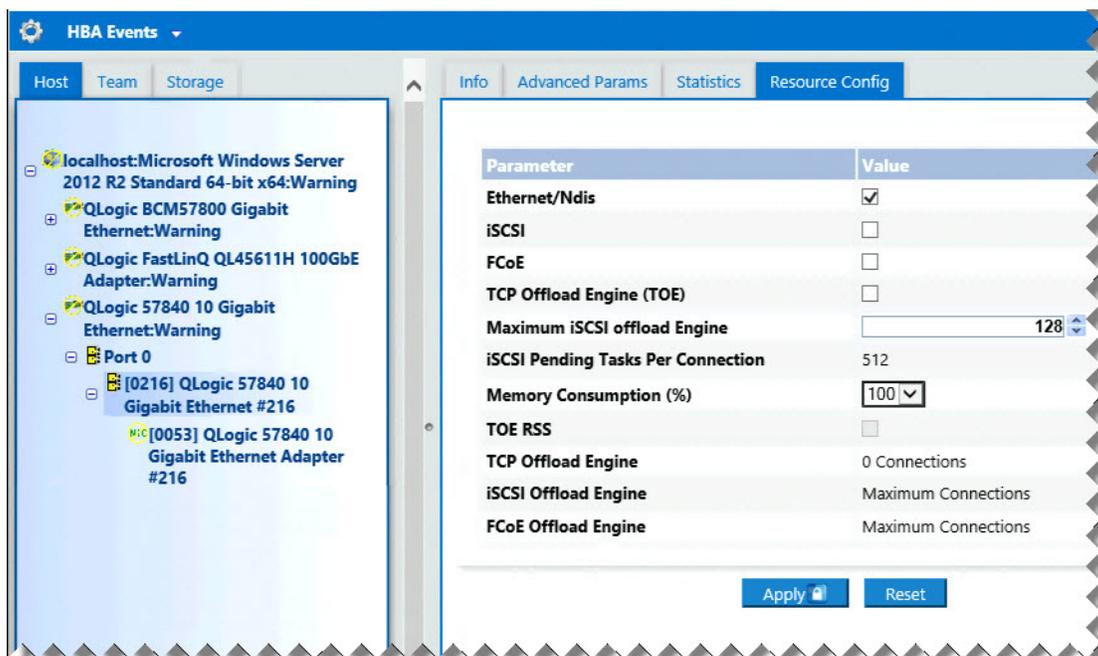


Abbildung 14-39. Ressourcenkonfiguration – Seite

4. Geben Sie gemäß dem folgenden Beispiel Werte für jeden ausgewählten Port auf der Seite „Resource Config“ (Ressourcenkonfiguration) ein:
 - a. Um den FCoE-Offload für den Port zu aktivieren, aktivieren Sie für den FCoE-Parameter das Kontrollkästchen **Value** (Wert).
 - b. Um den FCoE-Offload für den Port zu deaktivieren, löschen Sie für den FCoE-Parameter das Kontrollkästchen **Value** (Wert).
 - c. Klicken Sie auf die Schaltfläche **Apply** (Anwenden).
5. (optional) Wenn Sie den FCoE-Offload im Einzelfunktions- oder NPAR-Modus auf Windows oder Linux über die QCS-Befehlszeilenschnitt aktivieren oder deaktivieren möchten, finden Sie weitere Informationen im Handbuch *User's Guide, QLogic Control Suite CLI* (Teilenummer BC0054511-00). Wenn Sie den FCoE-Offload im Einzelfunktions- oder NPAR-Modus auf Windows oder Linux über QCC PowerKit aktivieren oder deaktivieren möchten, finden Sie weitere Informationen im Handbuch *User's Guide, PowerShell* (Teilenummer BC0054518-00). Hinweise zum Speicherort dieser Dokumente finden Sie unter „[Herunterladen von Dokumenten](#)“ auf Seite xxiii.

N_Port-ID-Virtualisierung (NPIV)

NPIV ist ein Fibre Channel-Protokoll, das die Realisierung mehrerer virtueller N_Ports auf einem physischen N_Port ermöglicht.

- Jeder NPIV-Port verfügt im Fabric über eine eindeutige ID und wird auf der Betriebssystemebene als eindeutiger Initiator-Port angezeigt.
- Die NetXtreme II BCM57xx und BCM57xxx FCoE-Treiber von QLogic unterstützen standardmäßig NPIV, ohne dass dafür eine Benutzeraktivität erforderlich ist.
- Die Anzahl der erstellbaren NPIV-Ports richtet sich nach den jeweiligen Betriebssystemtreibern und den Möglichkeiten/Beschränkungen des Fabric (FCoE/FC-Switch). Es gelten die folgenden Betriebssystem-Treiberbeschränkungen für NetXtreme II BCM57xx und BCM57xxx FCoE-Adapter von QLogic:
 - Microsoft Windows 256
 - Linux: 64
 - ESXi 6.0: Nicht unterstützt
 - ESXi 6.5: 64

15 Data Center Bridging

Dieses Kapitel enthält folgende Informationen zur Funktion Data Center Bridging:

- [Übersicht](#)
- [„DCB-Eigenschaften“ auf Seite 274](#)
- [„Konfigurieren von DCB“ auf Seite 275](#)
- [„Bedingungen für DCB“ auf Seite 275](#)
- [„Data Center Bridging unter Windows Server ab Version 2012“ auf Seite 276](#)

Übersicht

Unter Data Center Bridging (DCB) versteht man verschiedene IEEE-konforme Standarderweiterungen für Ethernet zur Bereitstellung von verlustfreier Datenübertragung, geringer Latenzzeit und standardbasierter gemeinsamer Bandbreitennutzung von physikalischen Verbindungen in Rechenzentren. DCB unterstützt Speicher-, Verwaltungs-, Rechen- und Kommunikations-Fabrics auf einer einzigen physikalischen Fabric, die einfacher bereitzustellen, zu aktualisieren und instandzuhalten ist als in Standard-Ethernet-Netzwerken. DCB verfügt im Kern über eine standardbasierte Bandbreitennutzung, so dass mehrere Fabrics gleichzeitig auf derselben physikalischen Fabric vorhanden sein können. Durch die verschiedenen Eigenschaften von DCB können LAN-Datenverkehr (zahlreiche Datenflüsse und ohne hohe Latenzempfindlichkeit), SAN-Datenverkehr (große Pakete und erfordert verlustfreie Übertragung) sowie IPC (Mitteilungen mit hoher Latenzempfindlichkeit) die Bandbreite derselben physikalischen konvergierten Verbindung nutzen und den nötigen individuellen Durchsatz erzielen.

DCB stellt folgende Funktionen bereit:

- Enhanced Transmission Selection (Erweiterte Übertragungsauswahl, ETS)
- Priority-based Flow Control (Prioritätsbasierte Flusskontrolle, PFC)
- Data Center Bridging eXchange (DCBX)-Protokoll

DCB-Eigenschaften

DCB-Eigenschaften umfassen ETS, PFC und DCBX, wie in diesem Abschnitt beschrieben.

Enhanced Transmission Selection (Erweiterte Übertragungsauswahl, ETS)

Enhanced Transmission Selection (ETS) liefert einen gemeinsamen Verwaltungsrahmen für die Zuordnung von Bandbreite zu Datenverkehrsklassen. Jede Datenverkehrsklasse oder Priorität kann in eine Prioritätsgruppe (PG) sortiert werden und als virtuelle Verbindung oder virtuelle Schnittstellenwarteschlange betrachtet werden. Das Programm zur Übertragungsplanung im Peer ist für die Einhaltung der zugeordneten Bandbreite für jede PG zuständig. Ein Benutzer kann beispielsweise FCoE-Verkehr in PG 0 und iSCSI-Verkehr in PG 1 konfigurieren. Der Benutzer kann dann jeder Gruppe eine bestimmte Bandbreite zuordnen. Beispielsweise 60 % für FCoE und 40 % für iSCSI. Das Programm zur Übertragungsplanung im Peer stellt dann sicher, dass der FCoE-Datenverkehr im Überlastungsfall mindestens 60 % der Verbindungsbandbreite und der iSCSI-Verkehr 40 % nutzen kann. Weitere Referenzen erhalten Sie unter:

<http://www.ieee802.org/1/pages/802.1az.html>

Priority Flow Control (PFC)

Priority Flow Control (PFC) bietet einen Flusskontrollmechanismus auf Verbindungsebene, der sich für jeden Datenverkehrstyp einzeln steuern lässt. Das Ziel dieses Mechanismus ist die Sicherstellung, dass im Überlastungsfall kein Datenverlust in DCB-Netzwerken auftritt. Im herkömmlichen IEEE 802.3 Ethernet wird nicht garantiert, dass ein über das Netzwerk übertragenes Paket seinen vorgesehenen Bestimmungsort erreicht. Upper Level Protocols sind dafür zuständig, die Zuverlässigkeit durch Bestätigung und erneute Übertragung zu gewährleisten. In einem Netzwerk mit mehreren Datenverkehrsklassen ist es sehr schwierig, die Zuverlässigkeit des Datenverkehrs ohne Feedback aufrecht zu erhalten. Abhilfe verschafft für gewöhnlich die Flusskontrolle auf Verbindungsebene.

Wenn PFC in einem Netzwerk mit mehreren Datenverkehrstypen verwendet wird, kann jeder Datenverkehrstyp mit einem unterschiedlichen Prioritätswert verschlüsselt werden, und ein PAUSE Frame kann einen Bezug zu diesem Prioritätswert herstellen und gleichzeitig den Transmitter anweisen, den Datenverkehr zu stoppen und erneut zu starten. Der Wertebereich für das Prioritätsfeld liegt zwischen 0 und 7, so dass acht unterschiedliche Datenverkehrstypen einzeln gestoppt und gestartet werden können. Weitere Referenzen erhalten Sie unter:

<http://www.ieee802.org/1/pages/802.1bb.html>

Data Center Bridging eXchange (DCBX)

Data Center Bridging eXchange (DCBX) ist ein Erkennungs- und Funktions austauschprotokoll, das zur Übermittlung von Funktionen und Konfigurationen von ETS und PFC zwischen Verbindungspartnern verwendet wird, um eine einheitliche Konfiguration in der gesamten Netzwerk-Fabric sicherzustellen. Damit zwei Geräte Informationen austauschen können, muss ein Gerät bereit sein, die Netzwerkkonfiguration des anderen Geräts zu übernehmen. Wenn beispielsweise ein C-NIC so konfiguriert ist, dass er zur Übernahme der ETS- und PFC-Konfigurationseinstellungen von einem angeschlossenen Switch bereit ist, und der Switch die Bereitschaft des C-NIC bestätigt, sendet der Switch dem C-NIC die empfohlenen ETS- und PFC-Parametereinstellungen. Das DCBX-Protokoll verwendet das Link Level Discovery Protocol (LLDP) zum Austauschen von PFC- und ETS-Konfigurationen zwischen Verbindungspartnern.

Konfigurieren von DCB

DCB ist standardmäßig auf QLogic BCM57xx und BCM57xxx DCB-kompatiblen C-NICs aktiviert. Die DCB-Konfiguration ist nur selten erforderlich, da die Standardkonfiguration für die meisten Situationen ausreichend sein sollte. DCB-Parameter können über QCS konfiguriert werden. Weitere Informationen zu QCS CLI finden Sie im Handbuch *User's Guide, QLogic Control Suite CLI*.

ANMERKUNG

Der FCoE-Betrieb ist abhängig von einer erfolgreichen VLAN-Erkennung. Alle Switches, die FCoE unterstützen, unterstützen auch die VLAN-Erkennung, allerdings benötigen einige Switches eine bestimmte Konfiguration. Informationen zur Konfiguration eines Anschlusses für eine erfolgreiche VLAN-Erkennung finden Sie in den Anleitungen zur Switch-Konfiguration.

Bedingungen für DCB

Im Folgenden werden die Bedingungen aufgelistet, die für die Funktion der DCB-Technologie auf dem Netzwerk gelten:

- Wenn DCB auf der Schnittstelle aktiviert ist, wird DCBX automatisch aktiviert und ausgeführt, sobald eine Verbindung hergestellt wurde.
- Wenn ein Fehler bei der Synchronisierung von DCBX mit einem kompatiblen Peer auftritt, greift der Adapter automatisch auf das standardmäßige NIC-Verhalten zurück (keine Prioritätsmarkierung, keine PFC, keine ETS).
- Standardmäßig kündigt der Port selbst seine Bereitschaft an und übernimmt so alle DCB-Einstellungen wie vom Switch angekündigt.

- Wenn PFC wirksam ist, ersetzen die PFC-Einstellungen die Flusskontrolleinstellungen auf Verbindungsebene. Wenn PFC nicht wirksam ist, gelten die Flusskontrolleinstellungen auf Verbindungsebene.
- Bei Konfigurationen mit aktivierter NIC-Partition überschreibt ETS (falls wirksam) die Bandbreitengewichtungen, die den einzelnen Funktionen zugewiesen wurden. Die Gewichtungen für die Übertragungsauswahl gelten stattdessen pro Protokoll und ETS-Einstellungen. Die maximalen Bandbreiten pro Funktion werden bei aktivierter ETS jedoch eingehalten.
- Falls kein Application TLV für iSCSI oder FCoE vorhanden ist, das durch den DCBX-Peer angekündigt wird, verwendet der Adapter die Einstellungen der lokalen Admin MIB.

Data Center Bridging unter Windows Server ab Version 2012

Mit Windows Server 2012 führte Microsoft eine neue Art der Verwaltung von QoS (Quality of Service) auf Betriebssystemebene ein. Die zwei Hauptaspekte von Windows-QoS sind:

- Eine herstellerunabhängige Methode für die Verwaltung von DCB-Einstellungen auf den NICs, sowohl einzeln als auch über eine ganze Domain. Die Managementschnittstelle wird von Windows PowerShell-Cmdlets bereitgestellt.
- Die Fähigkeit, bestimmte Arten von Layer 2-Netzwerkverkehr (wie z. B. SMB-Verkehr) zu kennzeichnen, sodass die Hardwarebandbreite mit ETS verwaltet werden kann.

Alle QLogic Converged Network Adapter, die DCB unterstützen, können mit Windows-QoS betrieben werden.

Um die QoS-Funktion unter Windows zu aktivieren, stellen Sie sicher, dass das QLogic-Gerät DCB-fähig ist:

1. Aktivieren Sie Data Center Bridging mittels CCM oder QCS.
2. Wählen Sie mit dem Windows Geräte-Manager oder QCS den NDIS-Treiber, öffnen Sie die **Advanced** (Erweiterten) Eigenschaften, und aktivieren Sie die **Quality of Service** (Dienstqualitäts)-Eigenschaft.

Wenn QoS aktiviert ist, wird die administrative Steuerung über die DCB-bezogenen Einstellungen an das Betriebssystem übergeben (das bedeutet, dass QCS nicht mehr zur administrativen Steuerung von DCB verwendet werden kann). Sie können PowerShell zum Konfigurieren und Verwalten der QoS-Funktion verwenden. Über PowerShell-Cmdlets können Sie die verschiedenen QoS-Parameter konfigurieren, wie z. B. Datenverkehrsklassifizierung, Priorität für Flusskontrolle und Durchsatzplanung für Datenverkehrsklassen.

Weitere Informationen zur Verwendung von PowerShell-Cmdlets finden Sie im „[DCB Windows PowerShell Benutzer Scripting Guide](#)“ in der Microsoft TechNet Library.

Um wieder zur normalen QCS-Steuerung für die QLogic-DCB-Funktionen zurückzukehren, deinstallieren Sie die Microsoft-QoS-Funktion, oder deaktivieren Sie Quality of Service in QCS oder den Geräte-Manager in den erweiterten Einstellungen von NDIS.

ANMERKUNG

QLogic empfiehlt, die DCB-Funktion nicht zu installieren, wenn SR-IOV-Geräte verwendet werden. Achten Sie bei der Installation der DCB-Funktion darauf, dass die Auswahl von **Enable single-root I/O virtualization (SR-IOV)** (Single Root I/O-Virtualisierung aktivieren (SR-IOV)) im Virtual Switch Manager den zugrunde liegenden Adapter in einen DCB-Zustand versetzt, in dem die betriebssystemeigene DCB-Konfiguration ignoriert wird und die DCB-Konfiguration von QCS gilt. Der benutzerkonfigurierte Wert (nicht Null) **Networking Priority** (Netzwerkpriorität) gilt nicht, obwohl es in QCS den Anschein erweckt.

16 SR-IOV

Dieses Kapitel enthält Informationen zur Single Root I/O-Virtualisierung (SR-IOV):

- [Übersicht](#)
- [Aktivieren von SR-IOV](#)
- [„Überprüfen der SR-IOV-Funktionsfähigkeit“ auf Seite 282](#)
- [„SR-IOV und Speicherfunktion“ auf Seite 283](#)
- [„SRSR-IOV und Jumbo-Pakete“ auf Seite 283](#)

Übersicht

Die Virtualisierung von Netzwerkcontrollern ermöglicht Benutzern, ihre Netzwerkhardware zusammenzuführen und mehrere virtuelle Maschinen gleichzeitig auf zusammengeführter Hardware auszuführen. Die Virtualisierung bietet dem Benutzer auch eine große Auswahl an Funktionen, wie z. B. I/O-Freigabe, Konsolidierung, Isolation und Migration sowie einfachere Verwaltung mit Anforderungen für Teaming und Failover.

Die Virtualisierung kann aufgrund einer Überhitzung des Hypervisors für eine geringere Leistung sorgen. PCI-SIG hat die Spezifikation SR-IOV eingeführt, um diese Leistungsprobleme zu beheben, indem eine virtuelle Funktion (VF) erstellt wird, eine Lightweight PCIe-Funktion, die direkt einer virtuellen Maschine (VM) zugeordnet werden kann, mit der die Hypervisor-Schicht für die Übertragung der Hauptdaten umgangen wird.

Nicht alle QLogic-Adapter unterstützen SR-IOV. Lesen Sie dazu die Systemdokumentation.

Aktivieren von SR-IOV

Bevor Sie versuchen, SR-IOV zu aktivieren, stellen Sie Folgendes sicher:

- Die Adapterhardware unterstützt SR-IOV.
- SR-IOV wird unterstützt und ist im System-BIOS aktiviert.

So aktivieren Sie SR-IOV:

1. Aktivieren Sie die Funktion über QCC GUI, QCS CLI, Dell Pre-Boot UEFI oder Pre-Boot CCM auf dem Adapter.

Wenn Sie Windows QCC GUI verwenden:

- a. Wählen Sie den Netzwerkadapter im Fenster „Explorer View“ (Explorer-Ansicht) aus. Klicken Sie auf die Registerkarte **Configuration** (Konfiguration) und dann auf **SR-IOV Global Enable** (SR-IOV Global aktivieren).
- b. Konfigurieren Sie im Feld **SR-IOV VFs per PF** (SR-IOV VFs pro PF) die Anzahl an virtuellen SR-IOV-Funktionen (VFs), die der Adapter pro physikalische Funktion unterstützen kann, von 0 bis 64, mit einer Schrittweite von 8 (Standard = 16).
- c. Konfigurieren Sie im Feld **SR-IOV Max Chains per VF** (Maximale SR-IOV-Ketten pro VF) die maximale Anzahl an Sender- und Empfängerwarteschlangen (z. B. Receive Side Scaling (Empfangsskalierung, RSS)-Warteschlangen), die für jede virtuelle Funktion verwendet werden können. Die maximale Anzahl ist 16.

Wenn Sie Pre-Boot UEFI verwenden:

- a. Drücken Sie während des Startvorgangs bei der Eingabeaufforderung auf F2, um das System für die Systemeinrichtung „Dell System Setup“ aufzurufen.
- b. Wählen Sie das Menü **Device Settings** (Geräteeinstellungen) aus.
- c. Wählen Sie den SR-IOV-fähigen Adapter-Port aus den Menü „Device Settings“ (Geräteeinstellungen) aus.
- d. Wählen Sie das Menü **Device Level Configuration** (Konfiguration auf Geräteebene) auf der Seite „Main Configuration“ (Hauptkonfiguration) aus.
- e. Wählen Sie in der Liste „Virtualization Mode“ (Virtualisierungsmodus) die Funktion **SR-IOV** oder **NPar+SR-IOV** aus (wenn Sie den SR-IOV-over-NPAR-Modus wünschen).
- f. Wenn Sie sich im SR-IOV-Modus (ohne NPAR-Modus) befinden, wählen Sie die gewünschte Anzahl der VFs für diesen Port im Dialogfenster **Number of VFs Per PF** (Anzahl der VFs pro PF) aus.

Bei 2x1G+2x10G BCM57800 werden bis zu 64 VFs auf jedem 10G-Port unterstützt (bei den beiden 1G-Ports von BCM57800 wird nicht unterstützt). 2x10G BCM57810 unterstützt bis zu 64 VFs pro Port. 4x10G BCM57840 unterstützt bis zu 32 VFs pro Port.

- g. Wenn Sie sich im SR-IOV-Modus (mit NPAR-Modus) befinden, hat jede Partition ihr eigenes Steuerfenster mit der Bezeichnung „Number of VFs Per PF“ (Anzahl an VFs pro PF). Drücken Sie auf ESC, um zur Seite „Main Configuration“ (Hauptkonfiguration) zurückzukehren, und wählen Sie dann das Menü **NIC Partitioning Configuration** (Partitionskonfiguration der Netzwerkschnittstellenkarte) aus (das nur angezeigt wird, wenn der NPAR-Modus im Dialogfeld „Virtualization Mode“ (Virtualisierungsmodus) ausgewählt ist). Wählen Sie auf der Seite „NIC Partitioning Configuration“ (Partitionskonfiguration für die Netzwerkschnittstelle) jedes Menü mit der Bezeichnung **Partition „N“ Configuration** (Partition-N-Konfiguration) aus und setzen Sie das Dialogfeld auf **Number of VFs per PF** (Anzahl der VFs pro PF). Die Gesamtzahl der pro PF auf einem einzigen physischen Ort zugewiesenen VFs darf die Anzahl nicht überschreiben, die in [Schritt f](#) zugewiesen wurden.

Wenn Sie Pre-Boot CCM verwenden:

- a. Drücken Sie während des Startvorgangs an der Eingabeaufforderung auf STRG+S, um das CCM aufzurufen.
- b. Wählen Sie den SR-IOV-fähigen Adapter aus der Geräteliste aus. Wählen Sie im Hauptmenü **Device Hardware Configuration** (Gerätehardwarekonfiguration) und anschließend **SR-IOV Enabled** (SR-IOV aktiviert) aus.
- c. So konfigurieren Sie die Anzahl an VFs, die der Adapter unterstützen kann:
 - Wenn der **Multi-Function Mode** (Multifunktionsmodus) auf **SF** (Einzelfunktion) eingestellt ist, wird das Feld **Number of VFs per PF** (Anzahl der VFs pro PF) angezeigt, wo Sie die Anzahl von 0 bis 64 mit einer Schrittweite von 8 einrichten können (der Standardwert liegt bei 16).
 - Wenn der **Multi-Function Mode** (Multifunktionsmodus) auf **NPAR** eingestellt ist, rufen Sie das Hauptmenü auf, und wählen Sie **NIC Partition Configuration** (NIC-Partition konfigurieren) aus. Wählen Sie dann die zu konfigurierende NPAR-Funktion aus, und geben Sie den passenden Wert in das Feld **Number of VFs per PF** (Anzahl der VFs pro PF) ein.
2. Aktivieren Sie entweder über den Windows-Gerätmanager oder QLogic Control Suite SR-IOV in den erweiterten Eigenschaften des Windows-Treibers.
3. Erstellen Sie im Virtual Switch Manager eine virtuelle Netzwerkschnittstellenkarte über das entsprechende Verfahren für Windows oder ESX.

In Windows:

- a. Wählen Sie **Allow Management operating system to share the network adapter** (Verwaltungsbetriebssystem erlauben, den Netzwerkadapter freizugeben), wenn dieser vSwitch vom Host zur Verbindung mit den zugeordneten VMs verwendet wird.
- b. Erstellen Sie einen virtuellen Switch und wählen Sie die Option **Enable Single root I/O Virtualization** (Single-Root-E/A-Virtualisierung aktivieren) aus.
- c. Wählen Sie im Virtual Switch Manager den virtuellen Adapter und dann im Navigationsfenster **Hardware Acceleration** (Hardwarebeschleunigung) aus. Wählen Sie im Abschnitt **Single-root I/O virtualization** (Single-Root-E/A-Virtualisierung) die Option **Enable SR-IOV** (SR-IOV aktivieren) aus. SR-IOV muss jetzt abgeschlossen sein und kann, nachdem der vSwitch erstellt wurde, nicht aktiviert werden.

In ESX:

- a. Installieren Sie den bnx2x-Treiber.
- b. Stellen Sie sicher, dass der Ausgabebefehl `lspci` in ESXi die Broadcom 10GNetXtreme-Netzwerkschnittstellenkarte aufweist.
- c. Wählen Sie in `lspci` die 10G-Netzwerkschnittstellen-Sequenznummer aus, für die SR-IOV erforderlich ist. Zum Beispiel:

```
~ # lspci | grep -i Broadcom 0000:03:00.0 Network  
Controllers: Broadcom Corporation NetXtreme II BCM57810  
10 Gigabit Ethernet [vmnic0]
```

Im Folgenden finden Sie eine beispielhafte Ausgabe.

```
0000:03:00.1 Network Controllers: Broadcom Corporation  
NetXtreme II BCM57810 10 Gigabit Ethernet [vmnic1]  
~ #
```

- d. Aktivieren Sie im Treiber SR-IOV, indem Sie den Parameter `max_vfs` verwenden und eine Liste mit der Menge der VFs für jeden Port weitergeben. Stellen Sie im BIOS sicher, dass die Menge der VFs pro PF-Parameter mit einem Minimum der erforderlichen Menge der VFs konfiguriert ist. Jeder PF-Port unterstützt maximal 64 VFs; die Mindestmenge beträgt 1. Zum Beispiel:

```
~ # esxcli system module parameters set -m bnx2x -p  
"max_vfs=64, 64"
```

- e. Starten Sie das System neu.

4. Installieren Sie die QLogic-Treiber für die in der VM erkannten Adapter. Verwenden Sie die neuesten Treiber Ihres Host-Betriebssystemherstellers (verwenden Sie nicht die enthaltenen Treiber). Es muss die gleiche Treiberversion auf dem Host und der VM installiert sein.

Überprüfen der SR-IOV-Funktionsfähigkeit

Folgen Sie den entsprechenden Schritten für die Hyper-V-, VMware vSphere- oder ESXi-Befehlszeilenschnittstelle.

So überprüfen Sie SR-IOV in Hyper-V Manager:

1. Starten Sie die VM.
2. Wählen Sie im Hyper-V Manager den Adapter und dann in der Liste **Virtual Machines** (Virtuelle Maschinen) die VM aus.
3. Klicken Sie auf die Registerkarte **Networking** (Netzwerk) unten im Fenster, und rufen Sie den Adapterstatus auf.

So überprüfen Sie SR-IOV im VMware vSphere 6.0 U2 Web-Client:

1. Bestätigen Sie, dass die VFs als normale VMDirectPath-Geräte angezeigt werden, indem Sie **Host** (Host), **Manage, Settings** (Einstellungen verwalten), **Hardware** (Hardware) und dann **PCI Devices** (PCI-Geräte) auswählen.
2. Klicken Sie mit der rechten Maustaste auf **VM** (VM), **Edit settings** (Einstellungen bearbeiten), **New Device** (Neues Gerät), **Select Network** (Netzwerk auswählen) und dann auf **Add** (Hinzufügen). Klicken Sie auf **New Network** (Neues Netzwerk) und wählen Sie dann **SR-IOV** als Adaptertyp aus. Klicken Sie auf **OK**.

So überprüfen Sie SR-IOV in der ESXi-Befehlszeilenschnittstelle:

1. Führen Sie den Befehl `lspci` aus

```
~ # lspci | grep -i ether
```

Im Folgenden finden Sie eine beispielhafte Ausgabe.

```
0000:03:01.0 Network controller: Broadcom Corporation
NetXtreme II BCM57810 10 Gigabit Ethernet Virtual Function
[PF_0.3.0_VF_0]
```

2. Um die SR-IOV-aktivierte Netzwerkschnittstellenkarte aufzulisten, führen Sie den Befehl `esxcli` aus:

```
~ # esxcli network sriovnic list
```

Im Folgenden finden Sie eine beispielhafte Ausgabe.

Name	PCI Device	Driver	Link	Speed	Duplex	MAC Address	MTU	Description
vmnic0	0000:003:00.0	bnx2x	Up	10000	Full	3c:d9:2b:f6:71:50	1500	Broadcom Corpo
vmnic1	0000:003:00.1	bnx2x	Down	0	Full	3c:d9:2b:f6:71:54	1500	Broadcom Corpo

SR-IOV und Speicherfunktion

Sie können die Speicherfunktion (FCoE oder iSCSI) auf einem SR-IOV-aktivierten Adapter aktivieren. Wenn die Speicherung allerdings bei einer NPAR-aktivierten physikalischen Funktion (PF) verwendet wird, wird die Anzahl der virtuellen Funktionen für diese PF auf 0 gesetzt. Deshalb ist SR-IOV bei dieser PF deaktiviert.

Diese Einschränkung gilt nur, wenn der Adapter im NPAR-Modus konfiguriert ist. Sie gilt nicht, wenn der Adapter im Einzelfunktionsmodus (SF) konfiguriert ist.

In ESX wird der Speicheradapter nach dem Aktivieren von SR-IOV im Betriebssystem für den SF-Modus nicht ermittelt.

SRSR-IOV und Jumbo-Pakete

Wenn SR-IOV für eine virtuelle Funktion (VF) auf dem Adapter aktiviert ist, stellen Sie sicher, dass in der VF und auf dem synthetischen Microsoft-Adapter die gleichen Jumbo-Paketeinstellungen konfiguriert sind. Diese Werte können Sie über „Windows Device Manager“ (Windows Geräte-Manager), „Advanced properties“ (Erweiterte Eigenschaften), konfigurieren.

Wenn die Werte nicht übereinstimmen, wird die SR-IOV-Funktion unter „Hyper-V“, „Networking Status“ (Netzwerkstatus) mit dem Zustand „degraded“ (Heruntergestuft) angezeigt.

17 Spezifikationen

Zu den Spezifikationen, Kenndaten und Anforderungen gehören:

- 10/100/1000BASE-T- und 10GBASE-T-Kabelspezifikationen
- „Schnittstellenspezifikationen“ auf Seite 287
- „Abmessungen der Netzwerkkarte“ auf Seite 288
- „Anforderungen der Netzwerkkarte an die Stromversorgung“ auf Seite 288
- „Anforderungen von Wake on LAN an die Stromversorgung“ auf Seite 290
- „Umgebungsbedingungen“ auf Seite 291

10/100/1000BASE-T- und 10GBASE-T-Kabelspezifikationen

Tabelle 17-1. 10/100/1000BASE-T-Kabelspezifikationen

Porttyp	Anschluss	Speichermedien	Maximale Länge
10BASE-T	RJ45	UTP-Kabel der KATEGORIE 3, 4 oder 5	328ft (100m)
100/1000BASE-T ^a	RJ45	UTP-KABEL DER KATEGORIE 5 ^b	328ft (100m)

^a Bei 1000BASE-T-Signalisierung sind vier TP-Kabel der Kategorie 5 für symmetrische Verkabelung gemäß ISO/IEC 11801:2002 und ANSI/EIA/TIA-568-B erforderlich.

^b Mindestens Kategorie 5. KATEGORIE 5e und KATEGORIE 6 werden vollständig unterstützt.

Tabelle 17-2. 10GBASE-T – Kabelspezifikationen

Porttyp	Anschluss	Speichermedien	Maximale Länge
10GBASE-T	RJ45	UTP-KABEL DER KATEGORIE 6 ^a UTP-KABEL DER KATEGORIE 6A ^a	131 ft (40 m) 328ft (100m)

^a Bei 10GBASE-T-Signalisierung sind vier TP-Kabel der Kategorie 6 oder der Kategorie 6A (erweiterte Kategorie 6) für symmetrische Verkabelung gemäß ISO/IEC 11801:2002 und ANSI/TIA/EIA-568-B erforderlich.

Unterstützte SFP+-Module pro NIC

Tabelle 17-3. BCM57710 – unterstützte Module

Modultyp	Modulhersteller	Modul-Teilenummer
OPTIc-Module (SR)	Finisar Corp.	FTLX8571D3BCL
	Avago	AFBR-707SDZ-D1
	Avago	AFBR-703SDZ-D1
	Intel Corp.	FTLX8571D3BCV-IT
Direktverbindungskabel	Cisco-Molex Inc.	74752-9093
	Cisco-Molex Inc.	74752-9094
	Cisco-Molex Inc.	74752-9096
	Cisco-Molex Inc.	74752-9098

Tabelle 17-4. BCM57810 – unterstützte Module

Modultyp	Dell-Teilenummer	Modulhersteller	Modul-Teilenummer
OPTic-Module (SR)	W365M	Avago	AFBR-703SDZ-D1
	N743D	Finisar Corp.	FTLX8571D3BCL
	R8H2F	Intel Corp.	AFBR-703SDZ-IN2
	R8H2F	Intel Corp.	FTLX8571D3BCV-IT
Direktverbindungskabel	K585N	Cisco-Molex Inc.	74752-9093
	J564N	Cisco-Molex Inc.	74752-9094
	H603N:	Cisco-Molex Inc.	74752-9096
	G840N	Cisco-Molex Inc.	74752-9098
	1539W	Brocade	58-1000026-01
	V239T	Brocade	58-1000027-01
	48V40	Brocade	58-1000023-01
	C4D08 – Force10 1 m Direktverbindungskabel	Amphenol	599700002
	C4D08 – Force10 1 m Direktverbindungskabel	Amphenol	616740001
	53HVN – Force10 3 m Direktverbindungskabel	Amphenol	599700006
	53HVN – Force10 3 m DA	Amphenol	616740003
	5CN56 – Force10 5 m Direktverbindungskabel	Amphenol	599700004
	5CN56 – Force10 5 m Direktverbindungskabel	Amphenol	616740005

Tabelle 17-5. BCM57840 – unterstützte Module

Modultyp	Dell-Teilenummer	Modulhersteller	Modul-Teilenummer
OPTic-Module (SR)	R8H2F	Intel Corp.	AFBR-703SDZ-IN2
		Intel Corp.	FTLX8571D3BCV-IT
Direktverbindungskabel	K585N	Cisco-Molex Inc.	74752-9093
	J564N	Cisco-Molex Inc.	74752-9094
	H603N:	Cisco-Molex Inc.	74752-9096
	G840N	Cisco-Molex Inc.	74752-9098
	1539W	Brocade	58-1000026-01
	V239T	Brocade	58-1000027-01
	48V40	Brocade	58-1000023-01
	C4D08 – Force10 1 m Direktverbindungskabel	Amphenol	599700002
	C4D08 – Force10 1 m Direktverbindungskabel	Amphenol	616740001
	53HVN – Force10 3 m Direktverbindungskabel	Amphenol	599700006
	53HVN – Force10 3 m Direktverbindungskabel	Amphenol	616740003
	5CN56 – Force10 5 m Direktverbindungskabel	Amphenol	599700004
	5CN56 – Force10 5 m Direktverbindungskabel	Amphenol	616740005

Schnittstellenspezifikationen

Tabelle 17-6. 10, 100, und 1000BASE-T – Leistungsspezifikationen

Leistungsmerkmal	Spezifikationen
PCI-Express-Schnittstelle	x4-Verbindungsbreite
10/100/1000BASE-T	10/100/1000Mbit/s

Tabelle 17-7. 10GBASE-T – Leistungsspezifikationen

Leistungsmerkmal	Spezifikationen
PCI-Express-Schnittstelle	x8-Verbindungsbreite
10GBASE-T	10 GBit/s

Abmessungen der Netzwerkkarte

Tabelle 17-8. Abmessungen der Netzwerkkarte

NIC-Typ	NIC-Länge	NIC-Breite
BCM57810S PCI Express x8 Low-Profile	6,6 Zoll (16,8 cm)	2,54 Zoll (6,5 cm)

Anforderungen der Netzwerkkarte an die Stromversorgung

Tabelle 17-9. Anforderungen der Netzwerkkarte BCM957810A1006G an die Stromversorgung

Verbindung	NIC 12 V Spannung (A)	NIC 3,3 V Spannung (A)	NIC Leistung (W) ^a
10G SFP-Modul	1,00	0,004	12,0

^a In Watt (W) gemessene Leistung, ergibt sich aus der Multiplikation von Stromstärke in Ampere (A) mit Spannung in Volt (V). Die maximale Stromaufnahme für den Adapter übersteigt 25 Watt nicht.

Tabelle 17-10. Anforderungen der Netzwerkkarte BCM957810A1008G an die Stromversorgung

Verbindung	NIC 12 V Spannung (A)	NIC 3,3 V Spannung (A)	NIC Leistung (W) ^a
Inaktiv (Keine Verbindung)	0,9	0,004	11,0
100 BASE-T-Verbindung	1,0	0,004	12,0
1000 BASE-T-Verbindung	1,3	0,004	15,5
10 GBASE-T-Verbindung	1,8	0,004	20,0

^a In Watt (W) gemessene Leistung, ergibt sich aus der Multiplikation von Stromstärke in Ampere (A) mit Spannung in Volt (V). Die maximale Stromaufnahme für den Adapter übersteigt 25 Watt nicht.

Tabelle 17-11. Anforderungen der BCM957840A4006G Mezzanine-Karte an die Stromversorgung

Verbindung	Gesamter Stromverbrauch (12 V und 3,3 VAUX) (W) ^a
10G SFP+	12,0
Standby WoL aktiviert	5,0
Standby WoL deaktiviert	0,5

^a In Watt (W) gemessene Leistung, ergibt sich aus der Multiplikation von Stromstärke in Ampere (A) mit Spannung in Volt (V). Die maximale Stromaufnahme für den Adapter übersteigt 25 Watt nicht.

Tabelle 17-12. Anforderungen der BCM957840A4007G Mezzanine-Karte an die Stromversorgung

Verbindung	Gesamter Stromverbrauch (3,3 V) (W) ^a
10G KR-Schnittstelle	10,0
WoL aktiviert	3,5

^a In Watt (W) gemessene Leistung, ergibt sich aus der Multiplikation von Stromstärke in Ampere (A) mit Spannung in Volt (V). Die maximale Stromaufnahme für den Adapter übersteigt 25 Watt nicht.

Anforderungen von Wake on LAN an die Stromversorgung

Nennleistung für WoL:

- BCM957810A1006G: 9,0 W
- BCM957810A1008G: 16,0 W

Umgebungsbedingungen

Tabelle 17-13. BCM5709 und BCM5716 Umgebungsbedingungen

Parameter	Bedingung
Betriebstemperatur	0°C bis 55°C
Belüftungsanforderungen (LFM)	0
Lagertemperatur	-40°C bis 65°C
Lagerluftfeuchtigkeit	5 % bis 95 % (bei Kondensation)
Erschütterungen	IEC 68, FCC Part 68,302, NSTA, 1A
Elektrostatische/Elektromagnetische Empfindlichkeit	EN 61000-4-2, EN 55024

Tabelle 17-14. BCM957810A1006G Umgebungsbedingungen

Parameter	Bedingung
Betriebstemperatur	0°C bis 55°C
Belüftungsanforderungen (LFM)	100
Lagertemperatur	-40°C bis 65°C
Lagerluftfeuchtigkeit	5 % bis 95 % (bei Kondensation)
Erschütterungen	IEC 68, FCC Part 68,302, NSTA, 1A
Elektrostatische/Elektromagnetische Empfindlichkeit	IEC 801-2, 3, 4, 5

Table 17-15. BCM957810A1008G Umgebungsbedingungen

Parameter	Bedingung
Betriebstemperatur	0°C bis 55°C
Belüftungsanforderungen (LFM)	50
Lagertemperatur	-40°C bis 65°C
Lagerluftfeuchtigkeit	5 % bis 95 % (bei Kondensation)
Erschütterungen	IEC 68, FCC Part 68,302, NSTA, 1A
Elektrostatische/Elektromagnetische Empfindlichkeit	IEC 801-2, 3, 4, 5

Table 17-16. BCM957840A4007G Umgebungsbedingungen

Parameter	Bedingung
Betriebstemperatur	0°C bis 65°C
Belüftungsanforderungen (LFM)	200
Lagertemperatur	-40°C bis 65°C
Lagerluftfeuchtigkeit	5 % bis 95 % (bei Kondensation)
Erschütterungen	IEC 68, FCC Part 68,302, NSTA, 1A
Elektrostatische/Elektromagnetische Empfindlichkeit	IEC 801-2, 3, 4, 5

18 Zulassungsbestimmungen

In diesem Kapitel werden unter anderem folgende Zulassungsbestimmungen behandelt:

- Produktsicherheit
- AS/NZS (C-Tick)
- „FCC-Hinweis“ auf Seite 294
- „VCCI-Hinweis“ auf Seite 296
- „CE-Hinweis“ auf Seite 302
- „Konformitätserklärung für Kanada“ auf Seite 303
- „Korea Communications Commission (KCC)-Hinweis (nur für die Republik Korea)“ auf Seite 305
- „BSMI“ auf Seite 308
- „Zulassungen für BCM95709SA0908G, BCM957710A1023G, (E02D001) und BCM957711A1123G (E03D001)“ auf Seite 308

Produktsicherheit

WARNUNG

Schalten Sie vor der Installation der Adapter-Hardware den Computer und alle angeschlossenen Geräte aus, darunter Bildschirme, Drucker und externe Komponenten.

Verwenden Sie BCM57xx und BCM57xxx-Adapter nur mit den aufgelisteten Informationstechnologiegeräten (ITE) oder äquivalenten Geräten. UL- bzw. TÜV-Standardnummer und CB-Zulassungen

- UL 60950-1 (2. Ausgabe) 2007
- CSA C22.2 Nr.60950-1-07 (2. Ausgabe) 2007
- TUV EN60950-1:2006+A11+A1+A12 2. Edition
- TUV IEC 60950-1:2005 2. Edition Am 1:2009 CB

AS/NZS (C-Tick)

AS/NZS; CISPR 22:2009+A1:2010 Klasse A

FCC-Hinweis

FCC, Klasse B

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95708A0804F
- BCM95709A0907G
- BCM95709A0906G
- BCM957810A1008G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA

Dieses Gerät entspricht Abschnitt 15 der FCC-Richtlinien. Der Betrieb unterliegt den beiden folgenden Bedingungen: (1) Das Gerät darf keine Störungen verursachen. (2) Das Gerät muss unempfindlich gegenüber störenden Beeinflussungen, einschließlich Beeinflussungen, die Betriebsstörungen verursachen können, sein.

Dieses Gerät wurde getestet und erfüllt die Anforderungen für digitale Geräte der Klasse B gemäß Teil 15 der Richtlinien der Federal Communications Commission (FCC). Diese Anforderungen gewährleisten angemessenen Schutz gegen Empfangsstörungen im Wohnbereich. Das Gerät erzeugt und verwendet Signale im Frequenzbereich von Rundfunk und Fernsehen und kann diese abstrahlen. Wenn das Gerät nicht gemäß den Anweisungen installiert und betrieben wird, kann es Störungen beim Empfang verursachen. Es kann jedoch nicht in jedem Fall garantiert werden, dass bei einer spezifischen Installation keine Empfangsstörungen auftreten. Wenn das Gerät Störungen im Rundfunk- oder Fernsehempfang verursacht, was durch vorübergehendes Ausschalten des Gerätes überprüft werden kann, versuchen Sie, die Störung durch eine der folgenden Maßnahmen zu beheben:

- Verändern Sie die Ausrichtung oder den Standort der Empfangsantenne.
- Erhöhen Sie den Abstand zwischen dem Gerät und Ihrem Rundfunk- oder Fernsehempfänger.
- Schließen Sie das Gerät an einen anderen Hausstromkreis an als den Rundfunk- oder Fernsehempfänger.
- Wenden Sie sich an Ihren Händler oder an einen ausgebildeten Rundfunk- und Fernstechniker.

Änderungen mechanischer oder elektrischer Art an dem Gerät sind untersagt.

ANMERKUNG

Veränderungen oder Modifikationen des Geräts ohne Genehmigung von QLogic können zum Erlöschen der Betriebserlaubnis führen.

FCC, Klasse A

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller:

- BCM95709A0916G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller:

- BCM957800
- BCM957710A1022G
- BCM957710A1021G
- BCM957711A1113G
- BCM957711A1102G
- BCM957810A1006G
- BCM957840A4006G
- BCM957840A4007G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA

Dieses Gerät entspricht Abschnitt 15 der FCC-Richtlinien. Der Betrieb unterliegt den beiden folgenden Bedingungen: (1) Das Gerät darf keine Störungen verursachen. (2) Das Gerät muss unempfindlich gegenüber störenden Beeinflussungen, einschließlich Beeinflussungen, die Betriebsstörungen verursachen können, sein.

Dieses Produkt wurde getestet und gemäß Abschnitt 15 der FCC-Bestimmungen als den Grenzwerten für ein digitales Gerät der Klasse A entsprechend befunden. Diese Anforderungen gewährleisten einen angemessenen Schutz vor schädlichen Funkstörungen, wenn das Produkt in einer gewerblichen Umgebung eingesetzt wird. Das Produkt erzeugt und verwendet Signale im Frequenzbereich von Rundfunk und Fernsehen und kann diese abstrahlen. Wenn das Gerät nicht gemäß den Anweisungen des Herstellers installiert und betrieben wird, kann es Störungen beim Empfang verursachen. Der Betrieb des Geräts in einem Wohngebiet führt höchstwahrscheinlich zu schädlichen Funkstörungen, was es erforderlich machen würde, die Störungen auf eigene Rechnung zu vermeiden.

Diese Grenzwerte dienen in Bereichen außerhalb von Wohngebieten dem Schutz gegen schädliche Funkstörungen. Es kann jedoch nicht in jedem Fall garantiert werden, dass bei einer spezifischen Installation keine Empfangsstörungen auftreten. Wenn dieses Gerät Störungen im Rundfunk- oder Fernsehempfang verursacht, was durch vorübergehendes Ausschalten des Geräts überprüft werden kann, versuchen Sie, die Störung durch eine der folgenden Maßnahmen zu beheben:

- Verändern Sie die Ausrichtung der Empfangsantenne.
- Verändern Sie den Standort des Systems hinsichtlich des Empfängers.
- Erhöhen Sie die Entfernung zwischen Gerät und Empfänger.
- Verbinden Sie das System mit einem anderen Anschluss, sodass System und Empfänger mit unterschiedlichen Kreisläufen verbunden sind.

Änderungen mechanischer oder elektrischer Art an dem Gerät sind untersagt.

ANMERKUNG

Veränderungen oder Modifikationen des Geräts ohne Genehmigung von QLogic können zum Erlöschen der Betriebserlaubnis führen.

VCCI-Hinweis

Die folgenden Tabellen enthalten die VCCI-Hinweise der physischen Spezifikationen für die QLogicBCM57xx und BCM57xxx-Adapter von Dell.

Tabelle 18-1. Physische Kenndaten der Netzwerktochterkarte QLogic 57800S 1GB und 10GBASE-T Rack

Das Objekt	Beschreibung
Ports	Dual-1-Gbps-Ethernet und Dual-10-Gbps-Ethernet
Formfaktor	Netzwerktochterkarte 92,9 mm × 74,4 mm (3,66 in × 2,93 in)
Unterstützte Server:	13. Generation: R630, R730, R730xd und T630 12. Generation: R620, R720, R720xd, R820 und R920
Anschluss	10G BASE-T und RJ45
Kabel	CAT6a und 7 bis zu 100 Metern CAT6 bis zu 40 Metern

Tabelle 18-1. Physische Kenndaten der Netzwerktochterkarte QLogic 57800S 1GB und 10GBASE-T Rack (fortgesetzt)

Das Objekt	Beschreibung
Zulassungen	RoHS, FCC A, UL, CE, VCCI, BSMI, C-Tick, KCC, TÜV und ICES-003

Tabelle 18-2. Physische Kenndaten der Netzwerktochterkarte QLogic 57800S Quad RJ-45, SFP+ oder Direct Attach Rack

Das Objekt	Beschreibung
Ports	Dual-1-Gbps-Ethernet und Dual-10-Gbps-Ethernet
Formfaktor	Netzwerktochterkarte 92,9 mm × 74,4 mm (3,66 in × 2,93 in)
Unterstützte Server:	13. Generation: R630, R730, R730xd und T630 12. Generation: R620, R720, R720xd, R820 und R920
Anschlüsse	Zwei Ports SFP+ (10 GbE) Zwei Ports RJ45 (1 GbE)
Zulassungen	RoHS, FCC A, UL, CE, VCCI, BSMI, C-Tick, KCC, TÜV und ICES-003

Tabelle 18-3. Physische Kenndaten der PCI-e-Karte QLogic 57810S Dual 10GBASE-T

Das Objekt	Beschreibung
Ports	Dual-10-Gbps-BASE-T-Ethernet-Ports
Formfaktor	PCI-Express Karte mit kurzer, niedriger Bauform 167,64 mm×68,91 mm (6.60 in×2.71 in)
Unterstützte Server:	13. Generation: R630, R730, R730xd und T630 12. Generation: R320, R420, R520, R620, R720, R720xd, R820, T420 und T620
Anschluss	RJ45
Kabel	CAT6a und 7 bis zu 100 Metern CAT6 bis zu 40 Metern
Zulassungen	RoHS, FCC A, UL, CE, VCCI, BSMI, C-Tick, KCC, TÜV und ICES-003

Tabelle 18-4. Physische Kenndaten der PCI-e-Karte QLogic 57810S Dual SFP+ oder Direct Attach

Das Objekt	Beschreibung
Ports	Dual-10-Gbps-Ethernet
Formfaktor	PCI-Express Karte mit kurzer, niedriger Bauform 67,64 mm×68,91 mm
Unterstützte Server:	13. Generation: R630, R730, R730xd und T630 12. Generation: R220, R320, R420, R520, R620, R720, R720xd, R820, R920, T420 und T620
Zulassungen	RoHS, FCC A, UL, CE, VCCI, BSMI, C-Tick, KCC, TÜV und ICES-003

Tabelle 18-5. Physische Kenndaten des Mezzanine-Adapters QLogic 57810S-K Dual KR Blade

Das Objekt	Beschreibung
Ports	Dual-10-Gbps-Ethernet
Formfaktor	Mezzanine Adapter 79,5 mm × 72,4 mm (3,13 in × 2,85 in)
Unterstützte Server:	13. Generation: M630 12. Generation: M420, M520, M620 und M820
Zulassungen	RoHS, FCC A, UL, CE, VCCI, C-Tick, KCC, TÜV und ICES-003

Tabelle 18-6. Physische Kenndaten der Netzwerktochterkarte QLogic 57810S-K Dual KR Blade

Das Objekt	Beschreibung
Ports	Dual-10-Gbps-Ethernet
Formfaktor	Netzwerktochterkarte 62,2 mm × 76,2 mm
Unterstützte Server:	13. Generation: M630 12. Generation: M620 und M820
Zulassungen	RoHS, FCC A, UL, CE, VCCI, C-Tick, KCC, TÜV und ICES-003

Tabelle 18-7. Physische Kenndaten der Netzwerktochterkarte QLogic 57840S Quad 10GbE SFP+ oder Direct Attach Rack

Das Objekt	Beschreibung
Ports	Dual-10-Gbps-Ethernet
Formfaktor	PCI-Express Karte mit kurzer, niedriger Bauform 67,64 mm×68,91 mm
Unterstützte Server:	13. Generation: R630, R730, R730xd und T630 12. Generation: R320, R420, R520, R620, R720, R720xd, R820, T420 und T620
Zulassungen	RoHS, FCC A, UL, CE, VCCI, BSMI, C-Tick, KCC, TÜV und ICES-003

Tabelle 18-8. Physische Kenndaten der Netzwerktochterkarte QLogic 57840S-K Quad KR Blade

Das Objekt	Beschreibung
Ports	Quad 10 Gbps Ethernet
Formfaktor	Netzwerktochterkarte 62,2 mm×76,2 mm (2,45 in×3,00 in)
Unterstützte Server:	13. Generation: M630 12. Generation: M420, M520, M620 und M820
Zulassungen	RoHS, FCC A, UL, CE, VCCI, BSMI, C-Tick, KCC, TÜV und ICES-003

VCCI, Klasse B

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95708A0804F
- BCM95709A0907G
- BCM95709A0906G
- BCM957810A1008G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA

Dies ist ein Produkt der Klasse B nach der vom Voluntary Control Council for Interference (VCCI) für Datenverarbeitungsgeräte festgelegten Norm. Wird dieses Gerät in der Nähe eines Radio- oder Fernsehempfangsgerätes in einem Wohnbereich eingesetzt, kann es zu Funkstörungen kommen. Beachten Sie bei der Aufstellung und dem Einsatz des Geräts die Anweisungen der Bedienungsanleitung.

VORSICHT!

Bei Vorhandensein einer leitungsgeführten Hochfrequenzstrahlung im Frequenzbereich zwischen 59 und 66 MHz kann der Betrieb des Geräts gestört werden. Der Normalbetrieb stellt sich nach Entfernen der Hochfrequenzstrahlung wieder ein.

VCCI Class B Statement (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、電波障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

VCCI, Klasse A

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709A0916G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1022G
- BCM957710A1021G
- BCM957711A1113G
- BCM957711A1102G
- BCM957840A4006G
- BCM957840A4007G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA

Dies ist ein Produkt der Klasse A nach der vom Voluntary Control Council for Interference (VCCI) für Datenverarbeitungsgeräte festgelegten Norm. Wenn das Produkt in Wohnbereichen eingesetzt wird, kann dies Funkstörungen verursachen. Beachten Sie bei der Aufstellung und dem Einsatz des Geräts die Anweisungen der Bedienungsanleitung.

VCCI Class A Statement (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波障害を引き起こす可能性があります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

CE-Hinweis

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95708A0804F
- BCM95709A0907G
- BCM95709A0906G
- BCM95709A0916G
- BCM957810A1008G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1022G
- BCM957710A1021G
- BCM957711A1113G
- BCM957711A1102G
- BCM957840A4006G
- BCM957840A4007G

Dieses Produkt erfüllt die Richtlinien 2006/95/EC (Niederspannungsrichtlinie), 2004/108/EC (EMV-Richtlinie) sowie die Zusatzrichtlinien der Europäischen Union.

Eine „Konformitätserklärung“ in Übereinstimmung mit den vorherigen Richtlinien und Standards wurde abgegeben und ist hinterlegt bei QLogic Corporation, 26650 Aliso Viejo Parkway, Aliso Viejo, California 92656, USA.

Europäische Union, Klasse B

Dieses QLogic-Gerät ist für den Einsatz in einem typischen Wohnbereich der Klasse B ausgelegt.

Europäische Union, Klasse A

WARNUNG: Dies ist ein Produkt der Klasse A. In Wohnbereichen kann dieses Produkt Radiofrequenzinterferenzen verursachen. In diesem Fall muss der Benutzer möglicherweise geeignete Maßnahmen ergreifen.

Konformitätserklärung für Kanada

Industry Canada, Class B

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95708A0804F
- BCM95709A0907G
- BCM95709A0906G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA

This Class B digital apparatus complies with Canadian ICES-003.

Notice: The Industry Canada regulations provide that changes or modifications not expressly approved by QLogic could void your authority to operate this equipment.

Industry Canada, Class A

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709A0916G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1022G
- BCM957710A1021G
- BCM957711A1113G
- BCM957711A1102G
- BCM957810A1008G
- BCM957840A4006G
- BCM957840A4007G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA

Dieses digitale Gerät der Klasse A entspricht der Kanadischen Norm ICES-003.

Notice: The Industry Canada regulations provide that changes or modifications not expressly approved by QLogic could void your authority to operate this equipment.

Industry Canada, classe B

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95708A0804F
- BCM95709A0907G
- BCM95709A0906G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA

Cet appareil numérique de la classe B est conforme à la norme canadienne ICES-003.

Avis: Dans le cadre des réglementations d'Industry Canada, vos droits d'utilisation de cet équipement peuvent être annulés si des changements ou modifications non expressément approuvés par QLogic y sont apportés.

Industry Canada, classe A

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709A0916G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1022G
- BCM957710A1021G
- BCM957711A1113G
- BCM957711A1102G
- BCM957810A1008G
- BCM957840A4006G
- BCM957840A4007G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA

Cet appareil numérique de classe A est conforme à la norme canadienne ICES-003.

Avis : Dans le cadre des réglementations d'Industry Canada, vos droits d'utilisation de cet équipement peuvent être annulés si des changements ou modifications non expressément approuvés par QLogic y sont apportés.

Korea Communications Commission (KCC)-Hinweis (nur für die Republik Korea)

Gerät der Klasse B

B급 기기 (가정용 방송통신기기)	이 기기는 가정용(B급)으로 전자파적합등록을 한 기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.
-----------------------	--

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95708A0804F
- BCM95709A0907G
- BCM95709A0906G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA



1. 기기의 명칭(모델명) : BCM95708A0804F
2. 인적사항번호 : E-G021-05-2568(B)
3. 인적사항번호 자의 상호 : BROADCOM
4. 제조년월일 : 05/31/2005
5. 제조자/제조국가 : Foxconn/China



1. 기기의 명칭(모델명) : BCM95709A0907G
2. 인적사항번호 : BCM-BCM95709A0907G(B)
3. 인적사항번호 자의 상호 : BROADCOM
4. 제조년월일 : 2008/01/15
5. 제조자/제조국가 : LiteOn/CHINA



방송통신위원회

BCM-BCM95709A0906G (B)

Dieses Gerät wurde für die Verwendung zu privaten Zwecken geprüft und zugelassen und kann in jeder Umgebung, einschließlich Wohngebieten, verwendet werden.

Gerät der Klasse A



A급 기기 (업무용 방송통신기기)	이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.
-----------------------	---

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709A0916G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1022G
- BCM957710A1021G
- BCM957711A1113G
- BCM957711A1102G
- BCM957810A1008G
- BCM957840A4006G
- BCM957840A4007G

QLogic Corporation
26650 Aliso Viejo Parkway
Aliso Viejo, CA 92656 USA



1. 기기의 명칭(모델명) : BCM95709A0916G
2. 인증번호 : BCM-BCM95709A0916G(A)
3. 인증받은 자의 상호 : BROADCOM
4. 제조년월일: 2008/08/25
5. 제조자/제조국가 : LiteOn/CHINA



1. 기기의 명칭(모델명) : BCM957710A1022G
2. 인증번호 : BCM-957710A1022G (A)
3. 인증받은 자의 상호 : BROADCOM
4. 제조년월일: 2008/03/14
5. 제조자/제조국가 : LiteOn/CHINA



1. 기기의 명칭(모델명) : BCM957710A1021G
2. 인증번호 : BCM-957710A1021G (A)
3. 인증받은 자의 상호 : BROADCOM
4. 제조년월일: 2008/09/02
5. 제조자/제조국가 : LiteOn/CHINA



방송통신위원회

BCM957711A1113G (A)



방송통신위원회

BCM-957711A1102G (A)

BSMI

BSMI 通告 (僅限於台灣)

大多數的 Dell 電腦系統被 BSMI (經濟部標準檢驗局) 劃分為乙類數位裝置。但是, 使用某些選件會使有些組態的等級變成甲類。若要確定您的電腦系統適用等級, 請檢查所有位於電腦底部或背面板、擴充卡安裝托架, 以及擴充卡上的 BSMI 註冊標籤。如果其中有一甲類標籤, 即表示您的系統為甲類數位裝置。如果只有 BSMI 的檢磁號碼標籤, 則表示您的系統為乙類數位裝置。

一旦確定了系統的 BSMI 等級, 請閱讀相關的 BSMI 通告。請注意, BSMI 通告規定凡是未經 Dell Inc. 明確批准的擅自變更或修改, 將導致您失去此設備的使用權。

此裝置符合 BSMI (經濟部標準檢驗局) 的規定, 使用時須符合以下兩項條件:

- 此裝置不會產生有害干擾。
- 此裝置必須能接受所接收到的干擾, 包括可能導致無法正常作業的干擾。

乙類

此設備經測試證明符合 BSMI (經濟部標準檢驗局) 之乙類數位裝置的限制規定。這些限制的目的是為了在住宅內安裝時, 能防止有害的干擾, 提供合理的保護。此設備會產生、使用並散發射頻能量; 如果未遵照製造廠商的指導手冊來安裝和使用, 可能會干擾無線電通訊。但是, 這並不保證在個別的安裝中不會產生干擾。您可以透過關閉和開啓此設備來判斷它是否會對廣播和電視收訊造成干擾; 如果確實如此, 我們建議您嘗試以下列一種或多種方法來排除干擾:

- 重新調整天線的接收方向或重新放置接收天線。
- 增加設備與接收器的距離。
- 將設備連接至不同的插座, 使設備與接收器連接在不同的電路上。
- 請向經銷商或有經驗的無線電 / 電視技術人員查詢, 以獲得幫助。

Zulassungen für BCM95709SA0908G, BCM957710A1023G, (E02D001) und BCM957711A1123G (E03D001)

Dieser Abschnitt wurde im Auftrag von Dell beigefügt. QLogic übernimmt keine Haftung für die Richtigkeit oder Genauigkeit dieser Informationen.

Der BCM95709SA0908G QLogic BCM57xx und BCM57xxx Gigabit Ethernet Controller, die Ethernet Controller BCM957710A1023G und E02D001 sowie der BCM957711A1123G (E03D001) QLogic BCM57xx und BCM57xxx10 Gigabit Ethernet Controller haben folgende gesetzliche Zulassungen erhalten:

- FCC, Klasse A (USA)
- VCCI Class A Statement (Japan)

- Konformitätserklärung für Kanada, Klasse A (Kanada)
- Korea Communications Commission (KCC)-Hinweis (Republik Korea)

FCC-Hinweis

FCC, Klasse A

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709SA0908G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1023G
- BCM957711A1123G (E03D001)
- E02D001

Dell Inc.

Einhaltung weltweiter gesetzlicher Bestimmungen sowie technischer und umweltbezogener Vorgaben

One Dell Way PS4-30

Round Rock, Texas 78682, USA

512-338-4400

Dieses Gerät entspricht Abschnitt 15 der FCC-Richtlinien. Der Betrieb unterliegt den beiden folgenden Bedingungen: (1) Das Gerät darf keine Störungen verursachen. (2) Das Gerät muss unempfindlich gegenüber störenden Beeinflussungen, die Betriebsstörungen verursachen können, sein.

Dieses Produkt wurde getestet und gemäß Abschnitt 15 der FCC-Bestimmungen als den Grenzwerten für ein digitales Gerät der Klasse A entsprechend befunden. Diese Anforderungen gewährleisten einen angemessenen Schutz vor schädlichen Funkstörungen, wenn das Produkt in einer gewerblichen Umgebung eingesetzt wird. Das Produkt erzeugt und verwendet Signale im Frequenzbereich von Rundfunk und Fernsehen und kann diese abstrahlen. Wenn das Gerät nicht gemäß den Anweisungen des Herstellers installiert und betrieben wird, kann es Störungen beim Empfang verursachen. Der Betrieb des Geräts in einem Wohngebiet führt höchstwahrscheinlich zu schädlichen Funkstörungen, was es erforderlich machen würde, die Störungen auf eigene Rechnung zu vermeiden.

Diese Grenzwerte dienen in Bereichen außerhalb von Wohngebieten dem Schutz gegen schädliche Funkstörungen. Es kann jedoch nicht in jedem Fall garantiert werden, dass bei einer spezifischen Installation keine Empfangsstörungen auftreten. Wenn dieses Gerät Störungen im Rundfunk- oder Fernsehempfang verursacht, was durch vorübergehendes Ausschalten des Geräts überprüft werden kann, versuchen Sie, die Störung durch eine der folgenden Maßnahmen zu beheben:

- Verändern Sie die Ausrichtung der Empfangsantenne.

- Verändern Sie den Standort des Systems hinsichtlich des Empfängers.
- Erhöhen Sie die Entfernung zwischen Gerät und Empfänger.
- Verbinden Sie das System mit einem anderen Anschluss, sodass System und Empfänger mit unterschiedlichen Kreisläufen verbunden sind.

Änderungen mechanischer oder elektrischer Art an dem Gerät sind untersagt.

ANMERKUNG

Veränderungen oder Modifikationen des Geräts ohne Genehmigung von Dell können zum Erlöschen der Betriebserlaubnis führen.

VCCI-Hinweis

Klasse A

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709SA0908G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1023G
- BCM957711A1123G (E03D001)
- E02D001

Dell Inc.

Worldwide Regulatory Compliance, Engineering and Environmental Affairs

One Dell Way PS4-30

Round Rock, Texas 78682, USA

512-338-4400

Dies ist ein Produkt der Klasse A nach der vom Voluntary Control Council for Interference (VCCI) für Datenverarbeitungsgeräte festgelegten Norm. Wenn das Produkt in Wohnbereichen eingesetzt wird, kann dies Funkstörungen verursachen. Beachten Sie bei der Aufstellung und dem Einsatz des Geräts die Anweisungen der Bedienungsanleitung.

VCCI Class A Statement (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると電波障害を引き起こす可能性があります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

CE-Hinweis

Klasse A

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709SA0908G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1023G
- BCM957711A1123G (E03D001)
- E02D001

Dell Inc.

Worldwide Regulatory Compliance, Engineering and Environmental Affairs
One Dell Way PS4-30
Round Rock, Texas 78682, USA
512-338-4400

Dieses Produkt erfüllt die Richtlinien 2006/95/EC (Niederspannungsrichtlinie), 2004/108/EC (EMV-Richtlinie) sowie die Zusatzrichtlinien der Europäischen Union.

Eine „Konformitätserklärung“ in Übereinstimmung mit den vorherigen Richtlinien und Standards wurde abgegeben und ist hinterlegt bei Dell Inc., Worldwide Regulatory Compliance, Engineering and Environmental Affairs, One Dell Way PS4-30 Round Rock, Texas 78682, USA

Europäische Union, Klasse A

WARNING: Dies ist ein Produkt der Klasse A. In Wohnbereichen kann dieses Produkt Radiofrequenzinterferenzen verursachen. In diesem Fall muss der Benutzer möglicherweise geeignete Maßnahmen ergreifen.

Konformitätserklärung für Kanada

Industry Canada, Class A

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709SA0908G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1023G
- BCM957711A1123G (E03D001)
- E02D001

Dell Inc.

Einhaltung weltweiter gesetzlicher Bestimmungen sowie technischer und umweltbezogener Vorgaben

One Dell Way PS4-30

Round Rock, Texas 78682, USA

512-338-4400

Dieses digitale Gerät der Klasse A entspricht der Kanadischen Norm ICES-003.

Notice: The Industry Canada regulations provide that changes or modifications not expressly approved by Dell Inc. could void your authority to operate this equipment.

Industry Canada, classe A

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709SA0908G

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1023G
- BCM957711A1123G (E03D001)
- E02D001

Dell Inc.

Worldwide Regulatory Compliance, Engineering and Environmental Affairs

One Dell Way PS4-30

Round Rock, Texas 78682, USA

512-338-4400

Cet appareil numérique de classe A est conforme à la norme canadienne ICES-003.

Avis : Dans le cadre des réglementations d'Industry Canada, vos droits d'utilisation de cet équipement peuvent être annulés si des changements ou modifications non expressément approuvés par Dell Inc. y sont apportés.

Korea Communications Commission (KCC)-Hinweis (nur für die Republik Korea)

Gerät der Klasse A

A급 기기 (업무용 방송통신기기)	이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.
-----------------------	---

QLogic BCM57xx und BCM57xxx Gigabit-Ethernet-Controller

- BCM95709SA0908G (5709s-mezz)

QLogic BCM57xx und BCM57xxx 10-Gigabit-Ethernet-Controller

- BCM957710A1023G
- BCM957711A1123G (E03D001)
- E02D001

Dell Inc.

Worldwide Regulatory Compliance, Engineering and Environmental Affairs

One Dell Way PS4-30

Round Rock, Texas 78682, USA

512-338-4400



1. 기기의 명칭(모델명) : 5709s-mezz
2. 인증번호 : E2K-5709s-mezz(A)
3. 인증받은 자의 상호 : DELL INC.
4. 제조년월일: 2008/08/12
5. 제조자/제조국가 : LiteOn/CHINA



1. 기기의 명칭(모델명) : BCM957710A1023G
2. 인증번호 : E2K-957710A1023G (A)
3. 인증받은 자의 상호 : DELL INC.
4. 제조년월일: 2008/10/15
5. 제조자/제조국가 : LiteOn/CHINA



방송통신위원회

E2K-E03D001 (A)



방송통신위원회

E2K-E02D001 (A)

19 Fehlerbehebung

Zu den Themen der Problembehebung gehört Folgendes:

- [Hardware-Diagnose](#)
- [„Überprüfen der Port-LEDs“ auf Seite 317](#)
- [„Fehlerbehebung – Checkliste“ auf Seite 317](#)
- [„Überprüfen der geladenen Treiber“ auf Seite 318](#)
- [„Durchführen eines Kabellängentests“ auf Seite 319](#)
- [„Testen der Netzwerkanbindung“ auf Seite 319](#)
- [„Microsoft Virtualization mit Hyper-V“ auf Seite 321](#)
- [„Entfernen der QLogic BCM57xx und BCM57xxx Gerätetreiber“ auf Seite 327](#)
- [„Aktualisieren von Windows-Betriebssystemen“ auf Seite 327](#)
- [„QLogic Boot Agent“ auf Seite 328](#)
- [„QLASP“ auf Seite 328](#)
- [„Linux“ auf Seite 330](#)
- [„NPAR“ auf Seite 331](#)
- [„Kernel-Debugging über Ethernet“ auf Seite 332](#)
- [„Sonstiges“ auf Seite 332](#)

Hardware-Diagnose

Zur Überprüfung der Adapterhardware stehen Prüfschleifen-Diagnosetests zur Verfügung. Diese Tests ermöglichen den Zugriff auf die interne bzw. externe Diagnose des Adapters, wobei Paketinformationen über die physische Verbindung übertragen werden (Anweisungen und Informationen zum Durchführen eines Tests in einer Windows-Umgebung finden Sie in der QCC GUI-Onlinehilfe).

QCS Fehler bei Diagnosetests

Wenn einer der folgenden Tests fehlschlägt, während die Diagnosetests in QCS ausgeführt werden, liegt möglicherweise bei der im System installierten Netzwerkkarte bzw. beim LOM ein Hardwareproblem vor.

- Kontrollregister
- MII-Register
- EEPROM
- Interner Speicher
- Chip-CPU
- Interrupt
- Prüfschleife: MAC
- Prüfschleife: PHY
- LED-Test

Schritte zur Problembeseitigung:

1. Entfernen Sie das fehlerhafte Gerät, und setzen Sie es wieder in den Steckplatz ein. Achten Sie darauf, dass die Karte fest im Steckplatz installiert ist.
2. Führen Sie den Test erneut aus.
3. Wenn die Karte weiterhin fehlerhaft ist, ersetzen Sie sie durch eine andere Karte desselben Modells und führen Sie den Test erneut aus. Wenn der Test mit der neuen Karte fehlerfrei ausgeführt werden kann, wenden Sie sich an den Hardwarehersteller, um Hilfe zum fehlerhaften Gerät zu erhalten.
4. Fahren Sie den Computer herunter, schalten Sie ihn aus, und starten Sie das System neu.
5. Deinstallieren Sie die Diagnosesoftware, und installieren Sie sie neu.
6. Wenden Sie sich an den Hardwarehersteller.

QCSFehler bei Netzwerktests

Normalerweise sind Fehler bei QCS-Netzwerktests auf ein Konfigurationsproblem im Netzwerk oder der IP-Adressen zurückzuführen. Zur Beseitigung von Netzwerkproblemen sollten Sie allgemein folgende Schritte ausführen.

1. Stellen Sie sicher, dass das Kabel angeschlossen ist und die Verbindung hergestellt wurde.
2. Überprüfen Sie, ob die Treiber geladen und aktiviert wurden.
3. Ziehen Sie das Kabel ab, das an die Netzwerkkarte oder am LOM angeschlossen ist, und schließen Sie es wieder an.

4. Überprüfen Sie, ob die IP-Adresse korrekt zugewiesen wurde. Führen Sie hierzu den Befehl `ipconfig` aus, oder verwenden Sie das Betriebssystemtool zum Zuweisen von IP-Adressen.
5. Stellen Sie sicher, dass die IP-Adresse für das Netzwerk, mit dem der oder die Adapter verbunden sind, korrekt eingegeben wurde.

Überprüfen der Port-LEDs

Informationen zum Überprüfen des Netzwerkverbindungsstatus und des Betriebsstatus finden Sie unter „[Netzwerkverbindung und Betriebsanzeige](#)“ auf [Seite 7](#).

Fehlerbehebung – Checkliste

VORSICHT!

Lesen Sie den Abschnitt „[Sicherheitsvorkehrungen](#)“ auf [Seite 20](#), bevor Sie das Gehäuse des Servers zum Hinzufügen oder Entfernen des Adapters öffnen.

In der folgenden Checkliste werden Maßnahmen zur Behebung von Problemen empfohlen, die bei der Installation des QLogic BCM57xx und BCM57xxx-Adapters beziehungsweise bei dessen Betrieb im System auftreten können.

- Überprüfen Sie alle Kabel und Anschlüsse. Überprüfen Sie, ob alle Kabel ordnungsgemäß am Netzwerkadapter und am Switch angeschlossen sind. Überprüfen Sie, ob die Kabellänge und die Kabelauslegung den unter „[Anschließen der Netzkabel](#)“ auf [Seite 22](#) aufgeführten Anforderungen entsprechen.
- Überprüfen Sie die Adapterinstallation anhand der Angaben unter „[Installation der zusätzlichen Netzwerkkarte](#)“ auf [Seite 21](#). Überprüfen Sie, ob der Adapter fest im Steckplatz sitzt. Suchen Sie nach spezifischen Hardwareproblemen, beispielsweise nach einer offensichtlichen Beschädigung einer Platinenkomponente oder des PCI-Stiftsockels.
- Überprüfen Sie die Eigenschaftseinstellungen und ändern Sie diese, falls sie den Einstellungen anderer Komponenten widersprechen.
- Überprüfen Sie, ob der Server das neueste BIOS verwendet.
- Versuchen Sie, den Adapter in einem anderen Steckplatz zu installieren. Wenn die neue Installationsposition funktioniert, ist unter Umständen der ursprüngliche Systemsteckplatz defekt.

- Tauschen Sie den nicht funktionierenden Adapter gegen einen Adapter aus, von dem Sie wissen, dass er korrekt funktioniert. Wenn der zweite Adapter in dem Steckplatz funktioniert, in dem der erste Adapter nicht betrieben werden konnte, ist der erste Adapter vermutlich defekt.
- Installieren Sie den Adapter in einem anderen funktionierenden System, und führen Sie die Tests erneut durch. Wenn der Adaptertest im neuen System erfolgreich ausgeführt werden kann, ist möglicherweise das ursprüngliche System defekt.
- Entfernen Sie alle anderen Adapter aus dem System, und führen Sie die Tests erneut durch. Wenn der Adaptertest erfolgreich verläuft, liegt unter Umständen ein Konflikt mit den anderen Adaptern vor.

Überprüfen der geladenen Treiber

Befolgen Sie die erforderlichen Schritte für Ihr Betriebssystem, um festzustellen, ob die aktuellen Treiber geladen sind.

Windows

In der Onlinehilfe zu QCC GUI finden Sie Informationen zum Betrachten wichtiger Informationen zum Adapter, zum Verbindungsstatus und zur Netzwerkkonnektivität.

Linux

Überprüfen Sie, ob der Treiber `bnx2.o` korrekt geladen ist. Führen Sie dazu folgenden Befehl aus:

```
lsmod | grep -i <module name>
```

Wenn der Treiber geladen wurde, zeigt die Ausgabe dieses Befehls die Treibergröße in Byte und die Anzahl der konfigurierten Adapter sowie deren Namen an. Das folgende Beispiel zeigt die geladenen Treiber für das `bnx2`-Modul:

```
[root@test1]# lsmod | grep -i bnx2
bnx2                199238  0
bnx2fc              133775  0
libfcoe              39764   2 bnx2fc, fcoe
libfc                108727  3 bnx2fc, fcoe, libfcoe
scsi_transport_fc   55235   3 bnx2fc, fcoe, libfc
bnx2i                53488   11
cnic                 86401   6 bnx2fc, bnx2i
libiscsi             47617   8
be2iscsi, bnx2i, cxgb4i, cxgb3i, libcxgbi, ib_iser, iscsi_tcp, libiscsi_tcp
scsi_transport_iscsi 53047   8
be2iscsi, bnx2i, libcxgbi, ib_iser, iscsi_tcp, libiscsi
```

```
bnx2x                1417947  0
libcrc32c            1246    1 bnx2x
mdio                  4732    2 cxgb3, bnx2x
```

Wenn Sie nach dem Laden eines neuen Treibers einen Neustart durchführen, können Sie den folgenden Befehl ausgeben, um zu überprüfen, ob der derzeit geladene Treiber die korrekte Version besitzt.

modinfo bnx2

Im Folgenden finden Sie eine beispielhafte Ausgabe.

```
[root@test1]# lsmod | grep -i bnx2
bnx2                199238  0
```

Sie können auch den folgenden Befehl ausgeben:

```
[root@test1]# ethtool -i eth2
```

Im Folgenden finden Sie eine beispielhafte Ausgabe.

```
Treiber: bnx2x
version: 1.78.07
Firmware-Version: bc 7.8.6
bus-info: 0000:04:00.2
```

Wenn Sie einen neuen Treiber geladen, aber noch nicht gebootet haben, zeigt Ihnen der Befehl `modinfo` nicht die aktualisierten Treiberinformationen an. Stattdessen können Sie durch Ausgeben des folgenden Befehls die Protokolle anzeigen, um zu überprüfen, ob der richtige Treiber geladen wurde, und ob dieser nach dem Neustart aktiv sein wird:

```
dmesg | grep -i "QLogic" | grep -i "bnx2"
```

Durchführen eines Kabellängentests

Informationen zum Durchführen eines Kabellängentests bei Windows-Betriebssystemen finden Sie in der Onlinehilfe zu QCC GUI. Die Kabelanalyse ist für BCM57xx und BCM57xxx Netzwerkadapter mit 10 GbE nicht verfügbar.

Testen der Netzwerkanbindung

ANMERKUNG

Stellen Sie bei der Verwendung erzwungener Übertragungsraten sicher, dass sowohl für den Adapter als auch für den Switch dieselbe Übertragungsrate erzwungen wird.

Windows

Sie können die Netzwerkanbindung auch mit der Funktion in QLogic Control Suite testen.

Alternativ können Sie mit dem `Ping`-Befehl prüfen, ob die Netzwerkverbindung funktioniert.

Testen der Netzwerkanbindung in Windows:

1. Klicken Sie auf **Start** und anschließend **Run** (Ausführen).
2. Geben Sie in das Feld **Open** (Öffnen) `cmd` ein, und klicken Sie dann auf **OK**.
3. Geben Sie den folgenden Befehl aus, um die zu testende Netzwerkverbindung anzuzeigen:

```
ipconfig /all
```

4. Geben Sie den folgenden Befehl aus, und drücken Sie dann die ENTER (EINGABE).

```
ping <IP address>
```

Die angezeigte Ping-Statistik gibt an, ob eine Netzwerkverbindung besteht.

Linux

Vergewissern Sie sich, dass die Ethernet-Schnittstelle aktiviert ist und korrekt funktioniert. Führen Sie dazu den Befehl `ifconfig` aus, und überprüfen Sie den Status der Ethernet-Schnittstelle. Sie können den Befehl `netstat -i` verwenden, um die Statistikdaten zur Ethernet-Schnittstelle zu überprüfen. Weitere Informationen zu `ifconfig` und `netstat` finden Sie unter [Kapitel 7 Linux-Treibersoftware](#).

Senden Sie einen Ping-Befehl an einen IP-Host im Netzwerk, um zu überprüfen, ob die Verbindung hergestellt wurde.

Geben Sie über die Befehlszeile den Befehl `ping <IP-Adresse>` ein, und drücken Sie dann auf die EINGABETASTE.

Die angezeigte Ping-Statistik gibt an, ob eine Netzwerkverbindung besteht.

Microsoft Virtualization mit Hyper-V

Microsoft Virtualization ist ein Hypervisor-basiertes Virtualisierungssystem für Windows Server 2012 R2. Dieser Abschnitt richtet sich an Benutzer, die mit Hyper-V vertraut sind. Es werden Probleme behandelt, die die Konfiguration von Netzwerkadaptern vom Typ BCM57xx und BCM57xxx und von Team-Netzwerkadaptern bei Verwendung von Hyper-V betreffen. Weitere Informationen zu Hyper-V finden Sie unter:

<http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx>

In **Tabelle 19-1** sind die von Hyper-V unterstützten Funktionen aufgeführt, die bei Netzwerkadaptern vom Typ BCM57xx und BCM57xxx konfiguriert werden können. Diese Tabelle enthält keine vollständige Liste aller Funktionen von Hyper-V.

Tabelle 19-1. Bei Netzwerkadaptern konfigurierbare Hyper-V-Funktionen

Leistungsmerkmal	Unterstützt in Windows Server			Kommentare und Einschränkungen
	2008	2008 R2	Ab Version 2012	
IPv4	Ja	Ja	Ja	—
IPv6	Ja	Ja	Ja	—
IPv4 large send offload (LSO, Large Send-Verschiebung) (für Parent- und Child-Partition)	Ja	Ja	Ja	—
IPv4 checksum offload (CO, Prüfsummenverschiebung) (für Parent- und Child-Partition)	Ja	Ja	Ja	—
IPv6 LSO (für Parent- und Child-Partition)	Nein*	Ja	Ja	* bei Bindung an ein virtuelles Netzwerk, Einschränkung hinsichtlich des Betriebssystems.
IPv6 CO (für Parent- und Child-Partition)	Nein*	Ja	Ja	* bei Bindung an ein virtuelles Netzwerk, Einschränkung hinsichtlich des Betriebssystems.
Jumbo-Frames	Nein*	Ja	Ja	* Einschränkung hinsichtlich des Betriebssystems.

Tabelle 19-1. Bei Netzwerkadaptern konfigurierbare Hyper-V-Funktionen (fortgesetzt)

Leistungsmerkmal	Unterstützt in Windows Server			Kommentare und Einschränkungen
	2008	2008 R2	Ab Version 2012	
RSS	Nein*	Nein*	Ja	* Einschränkung hinsichtlich des Betriebssystems.
RSC	Nein*	Nein*	Ja	* Einschränkung hinsichtlich des Betriebssystems.
SR-IOV	Nein*	Nein*	Ja	* Einschränkung hinsichtlich des Betriebssystems.

ANMERKUNG

Um eine vollständige Funktionalität zu gewährleisten, stellen Sie bitte sicher, dass Integrated Services, eine Komponente von Hyper-V, im Gast-Betriebssystem (Child-Partition) installiert ist.

Einzelner Netzwerkadapter

Die Konfiguration von Microsoft Virtualization mit Hyper-V für einen einzelnen Netzwerkadapter unterscheidet sich je nach verwendeter Windows Server-Version.

Windows Server 2008

Bei der Konfiguration eines BCM57xx und BCM57xxx-Netzwerkadapters für ein Hyper-V-System ist Folgendes zu beachten:

- Ein Adapter, der an ein virtuelles Netzwerk gebunden ist, darf für VLAN-Markierungen nicht über die erweiterten Eigenschaften des Treibers konfiguriert werden. Stattdessen sollte ausschließlich Hyper-V die VLAN-Markierung verwalten.
- Da Hyper-V keine Jumbo-Frames unterstützt, empfiehlt QLogic, diese Funktion nicht zu verwenden. Bei der Konnektivität mit der Child-Partition kann es zu Problemen kommen.
- Die von Hyper-V festgelegte lokal verwaltete Adresse (LAA) hat Vorrang vor der Adresse, die in den erweiterten Adaptereigenschaften festgelegt ist.

- In einem IPv6-Netzwerk zeigt ein Team, das CO oder LSO unterstützt und an ein virtuelles Hyper-V-Netzwerk gebunden ist, CO und LSO als Offload-Funktion in QCS an. CO und LSO funktionieren jedoch nicht. Diese Einschränkung des Hyper-V stellt ein Problem dar. Hyper-V bietet keine CO- und LSO-Unterstützung in einem IPv6-Netzwerk.

Windows Server 2008 R2 und 2012

Bei der Konfiguration eines BCM57xx und BCM57xxx-Netzwerkadapters für ein Hyper-V-System ist Folgendes zu beachten:

- Ein Adapter, der an ein virtuelles Netzwerk gebunden ist, darf für VLAN-Markierungen nicht über die erweiterten Eigenschaften des Treibers konfiguriert werden. Stattdessen sollte ausschließlich Hyper-V die VLAN-Markierung verwalten.
- Die von Hyper-V festgelegte lokal verwaltete Adresse (LAA) hat Vorrang vor der Adresse, die in den erweiterten Adaptoreigenschaften festgelegt ist.
- Die LSO- und die CO-Funktion im Gastbetriebssystem sind unabhängig von den Eigenschaften des Netzwerkadapters.
- Um eine Jumbo-Frame-Funktion vom Gastbetriebssystem zu ermöglichen, müssen sowohl auf dem Netzwerkadapter als auch auf dem virtuellen Adapter Jumbo-Frames aktiviert sein. Legen Sie die Eigenschaft „Jumbo MTU“ für den Netzwerkadapter so fest, dass Datenverkehr von großen MTU aus dem Gastbetriebssystem möglich ist. Legen Sie das Jumbo-Paket des virtuellen Adapters fest, um die Sende- und Empfangspakete entsprechend zu segmentieren.

Teaming-Netzwerkadapter

In [Tabelle 19-2](#) sind die von Hyper-V unterstützten Funktionen aufgeführt, die bei Team-Netzwerkadaptern vom Typ BCM57xx und BCM57xxx konfiguriert werden können. Diese Tabelle enthält keine vollständige Liste aller Funktionen von Hyper-V.

Tabelle 19-2. Bei Team-Netzwerkadaptern konfigurierbare Hyper-V-Funktionen

Leistungsmerkmal	Unterstützt in Windows Server Version			Kommentare und Einschränkungen
	2008	2008 R2	Ab Version 2012	
Teamart Smart Load Balancing und Failover (SLB)	Ja	Ja	Ja	SLB-Teams mit mehreren Mitgliedern sind bei der aktuellen QLASP6-Version erlaubt. ANMERKUNG: VM MAC wird externen Switches nicht bereitgestellt.
Teamart Link Aggregation (IEEE 802.3ad LACP)	Ja	Ja	Ja	—
Teamart Allgemeines Trunking (FEC/GEC) 802.3ad Draft Static	Ja	Ja	Ja	—
Failover	Ja	Ja	Ja	—
LiveLink	Ja	Ja	Ja	—
Large send offload (LSO) (Large Send-Verschiebung)	Beschränkt*	Ja	Ja	* Entspricht den Miniport-Einschränkungen in Tabelle 19-1 .
Checksum offload (CO, Prüfsummenverschiebung)	Beschränkt*	Ja	Ja	* Entspricht den Miniport-Einschränkungen in Tabelle 19-1 .
Hyper-V-VLAN über einen Adapter	Ja	Ja	Ja	—
Hyper-V-VLAN über einen Team-Adapter	Ja	Ja	Ja	—

Tabelle 19-2. Bei Team-Netzwerkadaptern konfigurierbare Hyper-V-Funktionen (fortgesetzt)

Leistungsmerkmal	Unterstützt in Windows Server Version			Kommentare und Einschränkungen
	2008	2008 R2	Ab Version 2012	
Hyper-V-VLAN über ein VLAN	Beschränkt*	Beschränkt*	Beschränkt*	Nur ein unmarkiertes VLAN.
Virtueller Hyper-V-Switch über einen Adapter	Ja	Ja	Ja	—
Virtueller Hyper-V-Switch über einen Team-Adapter	Ja	Ja	Ja	—
Virtueller Hyper-V-Switch über ein VLAN	Ja	Ja	Ja	—
iSCSI Boot	Nein	Nein*	Nein*	* Remote-Boot von SAN wird unterstützt.
Virtual Machine Queue (VMQ, Warteschlange einer virtuellen Maschine)	Nein	Ja	Ja	Siehe „ Konfigurieren von VMQ mit SLB-Teaming “ auf Seite 326.
RSC	Nein	Nein	Ja	—

Windows Server 2008

Folgendes ist zu beachten, wenn ein Team von BCM57xx und BCM57xxx-Netzwerkadaptern in einem Hyper-V-System konfiguriert wird:

- Erstellen Sie das Team, bevor Sie es an das virtuelle Hyper-V-Netzwerk anbinden.
- Ein Team sollte nur mit einem Adapter erstellt werden, der noch keinem virtuellen Hyper-V-Netzwerk zugeteilt ist.
- In einem IPv6-Netzwerk zeigt ein Team, das CO oder LSO unterstützt und an ein virtuelles Hyper-V-Netzwerk gebunden ist, CO und LSO als Offload-Funktion in QCS an. CO und LSO funktionieren jedoch nicht. Diese Einschränkung des Hyper-V stellt ein Problem dar. Hyper-V bietet keine CO- und LSO-Unterstützung in einem IPv6-Netzwerk.

- Um eine erfolgreiche VLAN-Markierung mit der QLASP-Teaming-Software für den Host (Parent-Partition) und den Gast (Child-Partition) auszuführen, müssen Sie das Team für Markierungen konfigurieren. Im Gegensatz zur VLAN-Markierung mit einem einzelnen Adapter, kann eine Markierung von Hyper-V nicht verwaltet werden, wenn QLASP-Software verwendet wird.
- Um ein Team zu ändern oder zu entfernen, verwenden Sie den Hyper-V Manager wie folgt:
 1. Löschen Sie die Bindungen des Teams aus allen Gastbetriebssystemen, die die Team-VNICs nutzen
 2. Ändern Sie die Einstellungen.
 3. Binden Sie die Team-VNICs erneut an das Gastbetriebssystem an.

Windows Server 2008 R2

Folgendes ist zu beachten, wenn ein Team von BCM57xx und BCM57xxx-Netzwerkadaptern in einem Hyper-V-System konfiguriert wird:

- Erstellen Sie das Team, bevor Sie es an das virtuelle Hyper-V-Netzwerk anbinden.
- Ein Team sollte nur mit einem Adapter erstellt werden, der noch keinem virtuellen Hyper-V-Netzwerk zugeteilt ist.
- Ein für VLAN-Markierung konfigurierter, virtueller QLASP-Adapter kann an ein virtuelles Hyper-V-Netzwerk gebunden werden und ist eine unterstützte Konfiguration. Die VLAN-Markierungsfunktion in QLASP kann jedoch nicht mit der VLAN-Funktion von Hyper-V kombiniert werden. Um die VLAN-Funktion von Hyper-V zu verwenden, muss die Markierung des QLASP-Teams aufgehoben werden.
- Um ein Team zu ändern oder zu entfernen, verwenden Sie den Hyper-V Manager wie folgt:
 1. Löschen Sie die Bindungen des Teams aus allen Gastbetriebssystemen, die die Team-VNICs nutzen
 2. Ändern Sie die Einstellungen.
 3. Binden Sie die Team-VNICs erneut an das Gastbetriebssystem an.

Konfigurieren von VMQ mit SLB-Teaming

Wenn ein Hyper-V Server in einem System installiert ist, das für die Verwendung der Teamart Smart Load Balance und Failover (SLB) konfiguriert ist, können Sie Virtual Machine Queue (VMQ) aktivieren, um die Leistung des gesamten Netzwerks zu verbessern. VMQ ermöglicht die Übertragung von Paketen von einem externen virtuellen Netzwerk direkt an im SLB-Team definierte virtuelle Maschinen, sodass diese Pakete nicht mehr weitergeleitet werden müssen, wodurch eine Reduzierung des Verwaltungsaufwands entsteht.

So erstellen Sie ein VMQ-fähiges SLB-Team:

1. Erstellen Sie ein SLB-Team. Wenn Sie den Teaming-Assistenten verwenden, wählen Sie neben der SLB-Teamart auch **Enable HyperV Mode** (HyperV-Modus aktivieren) aus. Aktivieren Sie im Expertenmodus die Eigenschaft auf den Seiten **Create Team** (Team erstellen) oder **Edit Team** (Team bearbeiten).
2. Befolgen Sie diese Anweisungen zum Hinzufügen der erforderlichen Registrierungseinträge in Windows:

<http://technet.microsoft.com/en-us/library/gg162696%28v=ws.10%29.aspx>

3. Ändern Sie für jedes Teammitglied, bei dem Sie VMQ aktivieren möchten, die folgenden Registrierungseinträge, und konfigurieren Sie eine eindeutige Instanznummer (im folgenden Beispiel 0026):

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\
  {4D36E972-E325-11CE-BFC1-08002BE10318}\0026]
"*RssOrVmqPreference"="1"
```

Entfernen der QLogic BCM57xx und BCM57xxx Gerätetreiber

Nehmen Sie die Deinstallation der QLogic BCM57xx und BCM57xxx-Gerätetreiber nur über den InstallShield-Assistenten vor. Beim Deinstallieren der Gerätetreiber mit dem Geräte-Manager oder auf andere Weise wird möglicherweise keine volle Deinstallation ausgeführt. Das System kann dadurch instabil werden. Informationen zum Deinstallieren von QLogic BCM57xx und BCM57xxx-Gerätetreibern finden Sie unter „[Entfernen der Gerätetreiber](#)“ auf [Seite 83](#). Beim Entfernen der Gerätetreiber werden auch die QLogic Control Suite und alle anderen Management-Anwendungen entfernt.

Wenn Sie die Gerätetreiber mit dem Geräte-Manager manuell deinstalliert und dann erfolglos versucht haben, die Gerätetreiber wieder zu installieren, führen Sie die Option **Repair** (Reparatur) des InstallShield-Assistenten aus. Informationen zum Reparieren von QLogic-BCM57xx und BCM57xxxGerätetreibern finden Sie unter „[Reparieren oder Neuinstallieren der Treibersoftware](#)“ auf [Seite 83](#).

Aktualisieren von Windows-Betriebssystemen

In diesem Abschnitt werden die folgenden Windows-Aktualisierungen behandelt:

- Von Windows Server 2003 auf Windows Server 2008
- Von Windows Server 2008 auf Windows Server 2008 R2
- Von Windows Server 2008 R2 auf Windows Server 2012

Wenn Sie das Betriebssystem aktualisieren möchten und ein QLogic BCM57xx und BCM57xxx-Adapter im System installiert ist, empfiehlt QLogic die folgende Vorgehensweise:

1. Speichern Sie alle IP-Informationen für das Team und den Adapter.
2. Deinstallieren Sie alle QLogic-Treiber mithilfe des Installationsprogramms.
3. Führen Sie die Windows-Aktualisierung durch.
4. Installieren Sie die aktuellen QLogic-Adapter-Treiber und die QLogic Control Suite-Anwendung neu.

QLogic Boot Agent

Problem: Es können mit PXE keine Netzwerkeinstellungen über DHCP abgefragt werden.

Lösung: Vergewissern Sie sich für einen ordnungsgemäßen Betrieb, dass an dem Port, mit dem der PXE-Client verbunden ist, Spanning Tree Protocol (STP) deaktiviert oder der Portfast-Modus (für Cisco) aktiviert ist. Stellen Sie beispielsweise `spantree portfast 4/12 enable` ein.

QLASP

Problem: Nachdem eine NIC, die Teil eines Teams war, physisch getrennt und ein Neustart durchgeführt wurde, zeigte das Team nicht die erwarteten Leistungen.

Lösung: Um eine Team-NIC von einem System zu trennen, müssen Sie die NIC zunächst im Team löschen. Wird dies vor dem Abschalten nicht durchgeführt, könnte das Team beim anschließenden Neustart beschädigt werden, sodass sich das Team in der Folge möglicherweise nicht wie erwartet verhält.

Problem: Wenn ein Team, das IPv6-Adressen verwendet, gelöscht und anschließend neu erstellt wird, werden die IPv6-Adressen vom alten Team für das neu erstellte Team verwendet.

Lösung: Dies ist ein Problem, das durch ein Drittanbieterprodukt verursacht wird. Um die IPv6-Adressen des alten Teams zu löschen, öffnen Sie unter „Network Connections“ (Netzwerkverbindungen) die TCP/IP-Eigenschaften des Teams, und wählen Sie die Seite „General“ (Allgemein) aus. Sie können jetzt entweder die alten Adressen löschen und neue IPv6-Adressen eingeben oder die IP-Adressen automatisch beziehen.

Problem: Das Hinzufügen eines Network Load Balancing-fähigen Adapters vom Typ BCM57xx und BCM57xxx zu einem Team kann zu nicht vorhersehbaren Ergebnissen führen.

Lösung: Bevor Sie das Team erstellen, heben Sie die Bindung von Network Load Balancing mit dem Adapter vom Typ BCM57xx und BCM57xxx auf, erstellen dann das Team und binden anschließend Network Load Balancing an das Team an.

Problem: Ein System mit einem 802.3ad-Team verursacht einen Fehler des Netlogon Service im Systemereignisprotokoll und verhindert hierdurch während des Starts die Kommunikation mit dem Domänencontroller.

Lösung: Im Microsoft Knowledge Base-Artikel 326152

(<http://support.microsoft.com/kb/326152/en-us>) wird erläutert, dass bei Gigabit-Ethernet (GbE)-Adaptoren aufgrund instabiler Verbindungen möglicherweise Probleme bei der Verbindung mit einem Domänencontroller auftreten, während der Treiber die Verbindung mit der Netzwerkinfrastruktur initialisiert und aushandelt. Die Verbindungsaushandlung wird darüber hinaus beeinträchtigt, wenn die GbE-Adapter aufgrund zusätzlicher Aushandlungen mit einem Switch, der für diese Teamart erforderlich ist, in einem 802.3ad-Team integriert sind. Wie im zuvor erwähnten Artikel der Knowledge Base vorgeschlagen, kann dieses Problem durch die Deaktivierung der Medienabfrage, wie in der Knowledge Base im Artikel 938449

(<http://support.microsoft.com/kb/938449>) beschrieben umgangen werden.

Problem: Zum 802.3ad-Team gehörende Verbindungen werden ständig beendet und erneut wiederhergestellt (gilt für alle Betriebssysteme).

Lösung: Dies ist ein Problem, das durch ein Drittanbieterprodukt verursacht wird. Es tritt nur dann auf, wenn ein 802.3ad-Team mit mehr als zwei zugehörigen Verbindungen auf dem Server konfiguriert und ein HP2524-Switch mit einem aktivierten, auf passiv oder aktiv gesetzten LACP verbunden wird. Bei nur zwei zugehörigen Verbindungen zeigt der HP-Switch erfolgreich einen LACP-Kanal an. Alle anderen zugehörigen Teamverbindungen werden beendet und wiederhergestellt. Dieses Problem tritt bei Cisco Catalyst 6500 nicht auf.

Problem: Ein Team der Teamart „Allgemeines Trunking (GEC/FEC)/802.3ad-Draft Static“ verliert möglicherweise einen Teil der Netzwerkanbindung, wenn der Treiber für ein Teammitglied deaktiviert wird.

Lösung: Wenn ein Teammitglied die zugrunde liegende Verwaltungssoftware (ASF oder UMP) oder Wake-On-LAN unterstützt, bleibt die Verbindung auf dem Switch für den Adapter möglicherweise erhalten, obwohl der dazugehörige Treiber deaktiviert wurde. Diese Verbindung kann dazu führen, dass der Switch den Datenverkehr weiterhin zu dem verbundenen Anschluss und nicht zum Anschluss eines aktiven Teammitglieds weiterleitet. Trennen Sie die Verbindung zwischen dem deaktivierten Adapter und dem Switch, um den Datenverkehr wieder an die anderen aktiven Teammitglieder weiterzuleiten.

Problem: LSO (Large-Send-Verschiebung) und CO (Prüfsummenverschiebung) funktionieren nicht in einem Team.

Lösung: Wenn einer der Adapter eines Teams LSO nicht unterstützt, funktioniert LSO für dieses Team nicht. Entfernen Sie den Adapter aus dem Team, der LSO nicht unterstützt, und ersetzen Sie ihn durch einen Adapter, der LSO unterstützt. Dasselbe gilt für die Prüfsummenverschiebung (Checksum Offload).

Problem: Die erweiterten Eigenschaften eines Teams ändern sich nicht, wenn die erweiterten Eigenschaften eines Adapters geändert werden, der Mitglied des Teams ist.

Lösung: Wenn ein Adapter Mitglied eines Teams ist und Sie eine erweiterte Eigenschaft ändern, müssen Sie das Team neu erstellen, um dafür zu sorgen, dass die erweiterten Eigenschaften des Teams korrekt eingestellt sind.

Linux

Problem: BCM57xx und BCM57xxx -Geräte mit SFP+-Datenflusssteuerung werden standardmäßig auf **Off** (Aus) und nicht auf **Rx/Tx Enable** (Rx/Tx-Aktivierung) eingestellt.

Lösung: Die Standardeinstellung für die Datenflusssteuerung für Version 1.6.x und höher wurde in **Rx Off and Tx Off** (Rx aus und Tx aus) geändert, da SFP+-Geräte die automatische Verhandlung der Datenflusssteuerung nicht unterstützen.

Problem: Wenn bei Kernen, die älter sind als 2.6.16, auf einem Server mit zwei BCM57711-Netzwerkadaptern 16 Partitionen erstellt werden, werden nicht alle Partitionen aktiviert, und es wird der Fehler angezeigt, dass nicht mehr genügend Speicherplatz verfügbar ist.

Lösung: Verwenden Sie auf Architekturen, bei denen die Standardgröße für `vmalloc` relativ klein und für das Laden vieler Schnittstellen nicht ausreichend ist, während des Startvorgangs `vmalloc=<size>`, um den Speicher zu vergrößern.

Problem: Routing funktioniert nicht für 10-GbE-Netzwerkadapter vom Typ BCM57xx und BCM57xxx, die in einem Linux-System installiert sind.

Lösung: Bei 10-GbE-Netzwerkadaptern vom Typ BCM57xx und BCM57xxx, die in Systemen mit Linux-Kernen älter als 2.6.26 installiert sind, können Sie die TPA-Funktion mit „`ethtool`“ (falls verfügbar) oder mit dem Treiberparameter deaktivieren (siehe [„disable_tpa“ auf Seite 47](#)). Verwenden Sie `ethtool`, um TPA (LRO) für einen bestimmten BCM57xx und BCM57xxx 10 GbE-Netzwerkadapter zu deaktivieren.

Problem: Wenn ein 1-GbE-Netzwerkadapter des Typs BCM57xx und BCM57xxx in einer C-Netzwerkschnittstellenumgebung verwendet wird, funktioniert die Flusststeuerung nicht.

Lösung: Obwohl die Flusststeuerung funktioniert, entsteht in einer C-Netzwerkschnittstellenumgebung der Eindruck, als ob dies nicht der Fall wäre. Der Netzwerkadapter kann PAUSE Frames versenden, wenn die Puffer auf dem Chip erschöpft sind, verhindert jedoch, die Head-of-Line-Blockierung anderer empfangener Warteschlangen. Da die Head-of-Line-Blockierung dazu führt, dass die Firmware auf dem Chip Pakete im Empfangspuffer auf dem Chip löscht, falls eine bestimmte Host-Warteschlange leer ist, ist der Empfangspuffer auf dem Chip selten leer. Dies erweckt den Anschein, als würde die Flow Control nicht funktionieren.

Problem: Beim Kompilieren von Treiberquellcode werden Fehlermeldungen ausgegeben.

Lösung: Bei einigen Installationen von Linux-Distributionen werden die Entwicklungs-Tools nicht standardmäßig mit installiert. Sorgen Sie dafür, dass die Entwicklungs-Tools für die von Ihnen verwendete Linux-Distribution installiert werden, bevor Sie mit dem Kompilieren des Treiberquellcodes beginnen.

NPAR

Problem: Die folgende Fehlermeldung wird angezeigt, wenn die Speicherkonfigurationen nicht für alle vier Ports des Geräts im NPAR-Modus einheitlich sind:

```
PXE-M1234: NPAR block contains invalid configuration during boot.
```

Ein Softwarefehler kann verursachen, dass das System keinen BFS-Boot in ein iSCSI- oder FCoE-Ziel durchführen kann, wenn eine iSCSI-Personality in der ersten Partition eines Ports aktiviert ist, während eine FCoE-Personality in der ersten Partition eines anderen Ports aktiviert wurde. Der MBA-Treiber führt eine Überprüfung auf diese Konfiguration durch und fordert den Benutzer zu einer Eingabe auf, wenn sie gefunden wurde.

Lösung: Konfigurieren Sie bei Verwendung der 7.6.x-Firmware und -Treiber zur Umgehung dieses Fehlers den NPAR-Block so, dass, wenn iSCSI oder FCoE in der ersten Partition aktiviert ist, dieses Verfahren bzw. dieses Protokoll auch auf allen Partitionen der vier Ports aktiviert sein muss.

Kernel-Debugging über Ethernet

Problem: Beim Kernel-Debugging über ein Ethernet-Netzwerk unter Windows 8.0 oder Windows Server 2012 kann das System nicht neu gestartet werden. Dieses Problem kann mit einigen Adaptionen auftreten, wenn Windows 8.0 oder Windows Server 2012 für den „unified extensible firmware interface“ (UEFI)-Modus konfiguriert ist. Möglicherweise wird eine Firmware-Fehlermeldung angezeigt, die Sie darauf hinweist, dass im UEFI-Preboot-Environment eine „Non Maskable Interrupt“-Ausnahme auftrat.

Lösung: Weitere Informationen finden Sie auch im Microsoft Knowledge Base-Artikel 2920163, „[Non Maskable Interrupt-Fehler beim Start eines Systems, das für Kernel-Debugging über Ethernet konfiguriert wurde](#)“.

Sonstiges

Problem: Die WOL-Link-Übertragungsrate von 10 GBit/s oder 1 GBit/s wird von der BCM57810-Netzwerkschnittstellenkarte mit 10 GbE nicht unterstützt.

Lösung: Die BCM57810-Netzwerkschnittstellenkarte mit 10 GbE kann aufgrund von Beschränkungen des Stromverbrauchs nur eine WOL-Link-Übertragungsrate von 100 MBit/s unterstützen.

Problem: Das iSCSI-Absturzspeicherabbild funktioniert unter Windows nicht.

Lösung: Nachdem die Gerätetreiber mithilfe des Installationsprogramms aktualisiert wurden, wird auch der iSCSI-Absturzspeicherabbild-Treiber aktualisiert. Anschließend muss auf der QCS-Seite „Configurations“ (Konfigurationen) im Abschnitt **Advanced** (Erweitert) die Option **iSCSI Crash Dump** (iSCSI-Absturzspeicherabbild) wieder aktiviert werden.

Problem: Wenn das Betriebssystem Windows Server 2008 R2 auf einem iSCSI Boot-Betriebssystem läuft, erscheint der VolMgr-Fehler „Das System konnte das Absturzspeicherabbild nicht laden“ im Ereignisprotokoll.

Lösung: Aktivieren Sie **iSCSI Crash Dump** (iSCSI-Absturzspeicherabbild) unter **Advanced** (Erweitert) auf der QCC-Seite „Configurations“ (Konfigurationen).

Problem: Der Adapter vom Typ QLogic BCM57xx und BCM57xxx funktioniert auf einigen Systemen nicht optimal, wenn er nach dem Systemstart hinzugefügt wurde.

Lösung: Bei manchen Systemen legt das System-BIOS nach dem Hinzufügen des Adapters nach dem Systemstart nicht die Cache-Größe und den Latenz-Timer fest. Starten Sie das System erneut, nachdem der Adapter hinzugefügt wurde.

Problem: Nach der Deinstallation von SNP können die Ressourcenzuweisungen in QCC nicht konfiguriert werden.

Lösung: Installieren Sie SNP neu. Stellen Sie vor der Deinstallation von SNP aus dem System sicher, dass NDIS aktiviert ist, indem Sie das Kontrollkästchen im Fenster „Resource Configuration“ (Ressourcenkonfiguration) markieren, das Sie über die Seite „Configurations“ (Konfigurationen) unter **Resource Reservations** (Ressourcenzuweisungen) aufrufen können. Wenn NDIS deaktiviert ist und SNP entfernt wurde, ist kein Zugriff für die erneute Aktivierung des Geräts vorhanden.

Problem: Eine DCOM-Fehlermeldung (Ereignis-ID 10016) wird während der Installation der QLogic-Treiberdateien im Ereignisprotokoll angezeigt.

Lösung: Dies ist ein Microsoft-Problem. Weitere Informationen finden Sie in der Microsoft Knowledge Base KB913119 unter <http://support.microsoft.com/kb/913119>.

Problem: Die Leistung verschlechtert sich, wenn im System mehrere BCM57710-Netzwerkadapter zum Einsatz kommen.

Lösung: Stellen Sie sicher, dass das System mindestens über 2 GB Arbeitsspeicher verfügt, wenn Sie bis zu vier Netzwerkadapter verwenden und 4 GB Arbeitsspeicher, wenn Sie vier oder mehr Netzwerkadapter verwenden.

Problem: Die Remote-Installation von Windows Server 2008 auf einem iSCSI-Ziel über iSCSI-Offload kann nicht abgeschlossen werden und der Computer startet wiederholt neu.

Lösung: Dies ist ein Microsoft-Problem. Weitere Informationen zur Anwendung des Microsoft-Hotfixes finden Sie im Microsoft Knowledge Base-Artikel KB952942 unter <http://support.microsoft.com/kb/952942>.

Problem: Der Netzwerkadapter wurde heruntergefahren, und eine Fehlermeldung wird angezeigt, die angibt, dass der Lüfter des Netzwerkadapters ausgefallen ist.

Lösung: Der Netzwerkadapter wurde heruntergefahren, um dauerhafte Schäden zu vermeiden. Wenden Sie sich an den Dell-Support.

Problem: Bei der Verwendung eines BCM57840 mit vier Port-Adaptoren in einem Blade-Server zeigen die Ports 3 und 4 keine Verbindung an.

Lösung: Das I/O (Switch)-Modul muss 32 interne Ports unterstützen. Wenn dies nicht der Fall ist, können die Ports 3 und 4 keine Verbindung herstellen.



Firmenzentrale Cavium, Inc. 2315 N. First Street San Jose, CA 95131 408-943-7100

Internationale Niederlassungen Großbritannien | Irland | Deutschland | Frankreich | Indien | Japan | China | Hongkong | Singapur | Taiwan | Israel

Copyright © 2015-2018 Cavium, Inc. Weltweit alle Rechte vorbehalten. Die QLogic Corporation ist eine hundertprozentige Tochtergesellschaft im Eigentum von Cavium, Inc. QLogic, FastLinQ und QConvergeConsole sind eingetragene Markenzeichen von Cavium, Inc. Alle anderen Marken- und Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Inhaber.

Dieses Dokument dient lediglich zu Informationszwecken und kann unter Umständen Fehler enthalten. Cavium behält sich das Recht vor, ohne vorherige Ankündigung Änderungen an diesem Dokument, am Produktdesign oder an den technischen Daten vorzunehmen. Cavium gewährt keinerlei ausdrückliche oder stillschweigende Garantien und garantiert nicht, dass die in diesem Dokument beschriebenen Ergebnisse oder Leistungen tatsächlich von Ihnen erzielt werden. Alle Erklärungen zur künftigen Ausrichtung und zu Absichten von Cavium können ohne Vorankündigung geändert werden und beschreiben lediglich Zielsetzungen und Vorhaben.

