




**Dell EqualLogic PS Series iSCSI-Speicherarrays mit
Microsoft Windows Server Failover-Clustern
Hardwareinstallations- und
Fehlerbehebungshandbuch**



Anmerkungen, Vorsichtshinweise und Warnungen

-  **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie den Computer besser einsetzen können.
-  **VORSICHT:** Ein VORSICHTSHINWEIS macht aufmerksam auf mögliche Beschädigung der Hardware oder Verlust von Daten bei Nichtbefolgung von Anweisungen.
-  **WARNUNG:** Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Irrtümer und technische Änderungen vorbehalten.

© 2012 Dell Inc. Alle Rechte vorbehalten.

Die Vervielfältigung oder Wiedergabe dieser Unterlagen in jeglicher Weise ohne vorherige schriftliche Genehmigung von Dell Inc. ist strengstens untersagt.

In diesem Text verwendete Marken: Dell™, das Dell Logo, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™ und Vostro™ sind Marken von Dell Inc. Intel®, Pentium®, Xeon®, Core® und Celeron® sind eingetragene Marken der Intel Corporation in den USA und anderen Ländern. AMD® ist eine eingetragene Marke und AMD Opteron™, AMD Phenom™ und AMD Sempron™ sind Marken von Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS® und Windows Vista® sind Marken oder eingetragene Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Red Hat® und Red Hat® Enterprise Linux® sind eingetragene Marken von Red Hat, Inc. in den USA und/oder anderen Ländern. Novell® ist eine eingetragene Marke und SUSE® ist eine Marke von Novell Inc. in den USA und anderen Ländern. Oracle® ist eine eingetragene Marke von Oracle Corporation und/oder ihren Tochterunternehmen. Citrix®, Xen®, XenServer® und XenMotion® sind eingetragene Marken oder Marken von Citrix Systems, Inc. in den USA und/oder anderen Ländern. VMware®, Virtual SMP®, vMotion®, vCenter® und vSphere® sind eingetragene Marken oder Marken von VMware, Inc. in den USA oder anderen Ländern. IBM® ist eine eingetragene Marke von International Business Machines Corporation.

Andere in diesem Dokument möglicherweise verwendete Marken und Handelsnamen beziehen sich auf die entsprechenden Eigentümer oder deren Produkte. Dell Inc. erhebt keinen Anspruch auf Marken und Handelsbezeichnungen mit Ausnahme der eigenen.

2012 - 02

Rev. A05

Inhaltsverzeichnis

Anmerkungen, Vorsichtshinweise und Warnungen.....	2
Kapitel 1: Einführung.....	5
Clusterlösung.....	5
Hardwareanforderungen für Cluster.....	6
Clusterknoten.....	6
Clusterspeicher.....	6
Empfohlene Netzwerkkonfigurationen.....	8
Unterstützte Clusterkonfigurationen.....	9
iSCSI-SAN-Attached-Cluster.....	9
Weitere nützliche Dokumente.....	9
Kapitel 2: Hardwareverkabelung für Cluster.....	11
Informationen über Maus-, Tastatur- und Bildschirm-Verkabelung	11
Informationen über die Verkabelung von Netzteilen.....	11
Informationen zum Verkabeln des Clusters für öffentliche und private Netzwerke.....	12
Für öffentliches Netzwerk.....	13
Für privates Netzwerk.....	13
NIC-Teaming.....	14
Informationen zur Verkabelung der Speicherarrays.....	14
Verkabelung des Speichers bei einem iSCSI-SAN-Attached-Cluster.....	14
Kapitel 3: Vorbereiten der Systeme für den Clusterbetrieb.....	27
Konfigurieren eines Clusters.....	27
Installationsübersicht.....	28
Zusätzliche Informationen zur Installation von iSCSI-NICs.....	28
Host-Integrationstools.....	28
Installation des Microsoft iSCSI-Software-Initiators.....	35
Ändern der Einstellungen in der Registry.....	35
Konfigurationsübersicht von gemeinsamen Speicherarrays.....	36
Erweiterte Speichermerkmale.....	39
Snapshots.....	40
Volumes.....	40
Replikation.....	42
Volumesammlungen.....	43
Thin Provisioning (Schlanke Speicherzuweisung).....	43
Installation und Konfiguration eines Failover-Clusters.....	44

Kapitel 4: Fehlerbehebung.....	45
Kapitel 5: Cluster-Datenformular.....	51
Kapitel 6: iSCSI-Konfigurationsarbeitsblatt.....	53

Einführung

Ein Dell Failover Cluster bietet erhöhte Verfügbarkeit für die darin betriebenen Anwendungen und Dienste. Dies wird durch die Kombination spezieller Hardware- und Softwarekomponenten erreicht. Failover Cluster reduzieren das Risiko, dass die im Cluster betriebenen Anwendungen und Dienste durch den Ausfall einer einzigen Systemkomponente nicht mehr verfügbar sind. Komponenten wie Server, Speichernetzteile, Verbindungen zwischen den Knoten und dem/den Speicherarray(s), Verbindungen zu Client-Systemen oder anderen Servern in einer mehrschichtigen Enterprise-Anwendungsarchitektur sollten in einem Cluster möglichst redundant vorhanden sein.

Das vorliegende Dokument enthält Informationen und spezifische Konfigurationaufgaben, die die Konfiguration eines Failover-Clusters mit Dell EqualLogic PS Series Internet Small Computer System Interface (iSCSI)-Speicherarray(s) ermöglichen.

Weitere Informationen zum Bereitstellen eines Clusters mit Microsoft Windows Server 2003- Betriebssystemen finden Sie im *Dell Failover Clusters with Microsoft Windows Server 2003 Installation and Troubleshooting Guide* (Dell Failover Clusters unter Microsoft Windows Server 2003 Installations- und Fehlerbehebungshandbuch) unter support.dell.com/manuals.

Weitere Informationen zum Bereitstellen eines Clusters mit Windows Server 2008 finden Sie im *Dell Failover Clusters with Microsoft Windows Server 2008 Installation and Troubleshooting Guide* (Dell Failover Clusters unter Microsoft Windows Server 2008 Installations- und Fehlerbehebungshandbuch) unter support.dell.com/manuals.

Eine Liste der unterstützten Betriebssysteme, Hardwarekomponenten und Treiber- oder Firmwareversionen für Ihren Failover-Cluster finden Sie in den *Dell Cluster Configuration Support Matrices* (Support-Matrizen zur Dell Clusterkonfiguration) unter dell.com/ha.

Clusterlösung

Ein Cluster unterstützt mindestens zwei Knoten und höchstens acht Knoten (Windows Server 2003) bzw. sechzehn Knoten (Windows Server 2008) und bietet die folgenden Funktionen:

- Gigabit- und 10-Gigabit-Ethernet-iSCSI-Technologien
- Hohe Verfügbarkeit von Ressourcen für Netzwerk-Clients
- Redundante Pfade zum gemeinsamen Speicher
- Ausfallwiederherstellung für Anwendungen und Dienste
- Flexible Wartungsmerkmale, mit denen Knoten oder Speicherarrays repariert, gewartet oder aufgerüstet werden können, ohne den gesamten Cluster vom Netz nehmen zu müssen.

Das iSCSI-Protokoll schließt iSCSI-Frames, die Befehle, Daten und Statusinformationen enthalten, in TCP/IP-Pakete ein, sodass sie über Ethernet-Netzwerke transportiert werden können. Die iSCSI-Frames werden zwischen dem hostresidenten Microsoft iSCSI-Initiator und dem iSCSI-Ziel – in der Regel ein Speichergerät – übermittelt. Die Implementierung von iSCSI in einem Cluster bietet folgende Vorteile:

Geografische Verteilung	Dank der größeren Reichweite der Ethernet-Technologie können sich Clusterknoten und Speicherarrays an unterschiedlichen Standorten befinden.
Hohe Verfügbarkeit bei niedrigen Kosten	Redundante Verbindungen stellen mehrere Datenpfade bereit, die mittels preiswerter TCP/IP-Netzwerkkomponenten hergestellt werden können.

Verbindungen

Eine einheitliche Technologie zum Anschließen von Speicherarrays, Clusterknoten und Clients.




Hardwareanforderungen für Cluster

Im Cluster werden die folgenden Hardwarekomponenten benötigt:

- Clusterknoten
- Clusterspeicher

Clusterknoten

Der folgende Abschnitt enthält die Hardwareanforderungen für die Clusterknoten.

Komponente	Minimale Anforderungen
Clusterknoten	Mindestens zwei identische Dell PowerEdge-Systeme werden benötigt. Wie viele Knoten maximal unterstützt werden, hängt von der im Cluster eingesetzten Variante des Windows Server-Betriebssystems ab.
RAM	Die Mindestgröße des benötigten System-Arbeitsspeichers hängt davon ab, welche Windows Server-Betriebssystemversion auf den Clusterknoten installiert ist.
Microsoft iSCSI-Software-Initiator	Erleichtern die Initialisierung der Arrays und die Konfiguration und Verwaltung des Hostzugriffs auf die Arrays. Microsoft iSCSI-Software-Initiator ist in den Host Integration Tools enthalten.
Netzwerkadapter (NICs) für den iSCSI-Zugriff	Zwei iSCSI-NICs oder zwei iSCSI-NIC-Anschlüsse pro Knoten: Konfigurieren Sie die NICs an separaten PCI-Bussen, um die Verfügbarkeit und Leistung zu optimieren. Für iSCSI-Datenverkehr werden auch TOE-NICs (TOE = TCP/IP Offload Engine) unterstützt.
NICs (öffentliche und private Netzwerke)	Mindestens zwei Netzwerkadapter (NICs): einen Netzwerkadapter für das öffentliche Netzwerk und einen weiteren für das private Netzwerk.  ANMERKUNG: Wenn Ihre Konfiguration mehr als zwei iSCSI-NIC-Ports erfordert, wenden Sie sich an Dell Services.  ANMERKUNG: Es wird empfohlen, an jedem öffentlichen Netzwerk und an jedem privaten Netzwerk jeweils identische NICs zu betreiben.
Interner Laufwerkcontroller	Pro Knoten ein Controller, der an mindestens zwei interne Laufwerke angeschlossen ist. Es kann jeder unterstützte RAID-Controller (Redundant Array of Independent Disk) bzw. Laufwerkcontroller verwendet werden. Es sind mindestens zwei Laufwerke für die Spiegelung (RAID 1) und mindestens drei Laufwerke für das Zusammenfassen von Laufwerken (RAID 5) erforderlich.  ANMERKUNG: Es wird nachdrücklich empfohlen, hardwarebasiertes RAID oder softwarebasierte Fehlertoleranz für die internen Laufwerke zu verwenden.

Clusterspeicher

Clusterknoten können gemeinsam auf externe Speicherarrays zugreifen. Allerdings kann ein Volume im externen Speicherarray zu jedem Zeitpunkt jeweils nur zu einem der Knoten gehören. Microsoft Cluster Services (MSCS) legt fest, welche Knoten auf die einzelnen Speicherlaufwerke zugreifen.

Der folgende Abschnitt enthält die Konfigurationsanforderungen für das Speichersystem, die Clusterknoten und an das Speichersystem angeschlossene Einzelsysteme.

Anforderungen für Clusterspeicher


Hardwarekomponenten	Anforderung
Speichersystem	Eine oder mehrere Gruppen der Dell EqualLogic PS Series. Jede Dell EqualLogic PS5000/PS5500/PS6000/PS6010/PS6100/PS6110/PS6500/PS6510-Gruppe unterstützt bis zu 16 Speicherarrays (Mitglieder) und jede PS4000/PS4100/PS4110 - Gruppe unterstützt bis zu zwei Speicherarrays. Hinweise zu spezifischen Anforderungen für Speicherarrays finden Sie unter „Anforderungen für Dell EqualLogic PS Series Speicherarrays“.
Verbindung der Speichersysteme untereinander	Alle Knoten müssen über ein iSCSI-SAN mit einem oder mehreren Speicherarrays verbunden sein.
Mehrere Cluster und eigenständige Systeme	Freigabe eines oder mehrerer unterstützter Speicherarrays im Netzwerk möglich.

Dell EqualLogic PS Series Speicherarrays sind mit redundanten, hot-swap-fähigen Laufwerken, Lüftern, Netzteilen und Controllern ausgerüstet. Der Ausfall einer dieser Komponenten führt nicht dazu, dass das Array offline gesetzt wird. Die ausgefallene Komponente kann bei laufendem Array-Betrieb ersetzt werden.

Der folgende Abschnitt enthält die Hardwareanforderungen für die Dell EqualLogic PS Series Speicherarrays.

Anforderungen für Dell EqualLogic PS Series Speicherarrays

Dell EqualLogic Array-Modell	Mindestanforderungen
PS4000 — PS4000E/PS4000X/PS4000XV	Redundante Controller
PS4100 — PS4100E/PS4100X/PS4100XV	
PS4110 — PS4110E/PS4110X/PS4110XV	
PS5000 — PS5000E/PS5000X/PS5000XV	
PS5500 — PS5500E	
PS6000 — PS6000E/PS6000X/PS6000XV/PS6000S	
PS6010 — PS6010E/PS6010X/PS6010XV/PS6010S/PS6010XVS	
PS6100 — PS6100E/PS6100X/PS6100XV/PS6100S/PS6100XS	
PS6110 — PS6110E/PS6110X/PS6110XV/PS6110S/PS6110XS	
PS6500 — PS6500E/PS6500X	
PS6510 — PS6510E/PS6510X	

 **ANMERKUNG:** Stellen Sie sicher, dass die Speicherarrays über eine unterstützte Firmwareversion verfügen. Spezifische Firmware-Versionanforderungen finden Sie in den *Dell Cluster Configuration Support Matrices* unter dell.com/ha.

Gesonderte NICs für iSCSI


Der vom iSCSI-Software-Initiator gesteuerte NIC fungiert als E/A-Adapter, über den der Erweiterungsbus und das/die Speicherarray(s) des Systems angeschlossen werden. Die mit den EqualLogic PS Series Speicherarrays konfigurierten Failover Cluster-Lösungen erfordern zwei iSCSI NICs- oder NIC-Ports in jedem PowerEdge-System. Dies liefert redundante Pfade und Lastverteilung der E/A-Datenübertragung zu oder von den Speicherarrays.

Reservierte Netzwerk-Switches für iSCSI

Die Gigabit- oder 10-Gigabit-Switches für den iSCSI-Zugriff fungieren als reguläre Netzwerk-Switches, die dedizierte Verbindungen zwischen den Knoten und den Speicherarrays bereitstellen.

Empfohlene Netzwerkkonfigurationen

Es wird empfohlen, die in aufgeführten Richtlinien zu befolgen. Zusätzlich gelten für Gruppenmitglieder alle üblichen Regeln für eine ordnungsgemäße Netzwerkkonfiguration.

Empfehlung	Beschreibung
Netzwerkverbindungen zwischen Arrays und Hosts	Verbinden Sie die Arrays und die Hosts mit einem Switch-Netzwerk und stellen Sie sicher, dass es sich bei allen Netzwerkverbindungen zwischen den Hosts und den Arrays um Gigabit- oder 10-Gigabit-Ethernet handelt.
Zuverlässige und angemessen ausgelegte Netzwerkverbindung für Replikation	Um eine effektive und berechenbare Replikation zu gewährleisten, stellen Sie sicher, dass die Netzwerkverbindung zwischen den primären und sekundären Gruppen zuverlässig ist und ausreichend Bandbreite zum Kopieren von Daten bietet.
Keine STP-Funktion (Spanning-Tree Protocol) an Switch-Ports, die Endknoten verbinden	Verwenden Sie kein STP an Switch-Ports, die Endknoten verbinden (iSCSI-Initiatoren oder SAN-Schnittstellen). Wenn Sie allerdings STP oder RSTP (Rapid Spanning-Tree Protocol; vorzugsweise statt STP) verwenden wollen, sollten Sie die Porteinstellungen mancher Switches aktivieren, die den Port nach Verbindungsherstellung sofort in den Zustand STP-Forwarding versetzen. Mit dieser Funktion lassen sich Netzwerkunterbrechungen reduzieren, die beim Neustart von Geräten auftreten, und sollten nur an Switch-Ports aktiviert werden, die Endknoten verbinden.  ANMERKUNG: Es wird empfohlen, Spanning-Tree und Trunking für Mehrfach-Kabelverbindungen zwischen Switches zu verwenden.
Verbindungen zwischen Switches	Die iSCSI-Switches müssen miteinander verbunden werden. Erstellen Sie mithilfe von Stack-Ports oder Port Trunking Verbindungen mit hoher Bandbreite zwischen den Switches. Wenn eine einzelne Nicht-Stack-Verbindung eingesetzt wird, kann sie zum Engpass werden und sich negativ auf die Leistung des Speichersystems auswirken.
Aktivieren von Flusskontrolle auf Switches und NICs	Aktivieren Sie die Flusskontrolle auf jedem Switch-Port und NIC, über den iSCSI-Datenverkehr erfolgt. Dell EqualLogic PS-Arrays reagieren korrekt auf Flusskontrolle.
Deaktivieren von Unicast-Sturm-Control auf Switches	Deaktivieren Sie Unicast-Sturm-Control auf jedem Switch, über den iSCSI-Datenverkehr erfolgt, wenn der Switch über diese Funktion verfügt. Der Einsatz von Broadcast und Multicast Storm Control wird jedoch auf Switches empfohlen.
Aktivieren von Jumbo-Frames auf Switches und NICs	Aktivieren Sie Jumbo-Frames auf jedem Switch und NIC, über den iSCSI-Datenverkehr erfolgt, um die Leistung zu steigern und konsistentes Verhalten sicherzustellen.
Deaktivieren von iSCSI-Optimierung auf Switches	Deaktivieren Sie die iSCSI-Optimierung, wenn der Switch dies ermöglicht. So vermeiden Sie, dass die interne Kommunikation zwischen den Array-Mitgliedern blockiert wird.

Unterstützte Clusterkonfigurationen

iSCSI-SAN-Attached-Cluster

Bei einem iSCSI-Switch-Attached-Cluster sind alle Knoten über redundante iSCSI SANs mit einem oder mehreren Speicherarrays verbunden, um hohe Verfügbarkeit zu gewährleisten. iSCSI-SAN-Attached-Cluster bieten maximale Flexibilität bei der Konfiguration, Erweiterbarkeit und hohe Leistung.

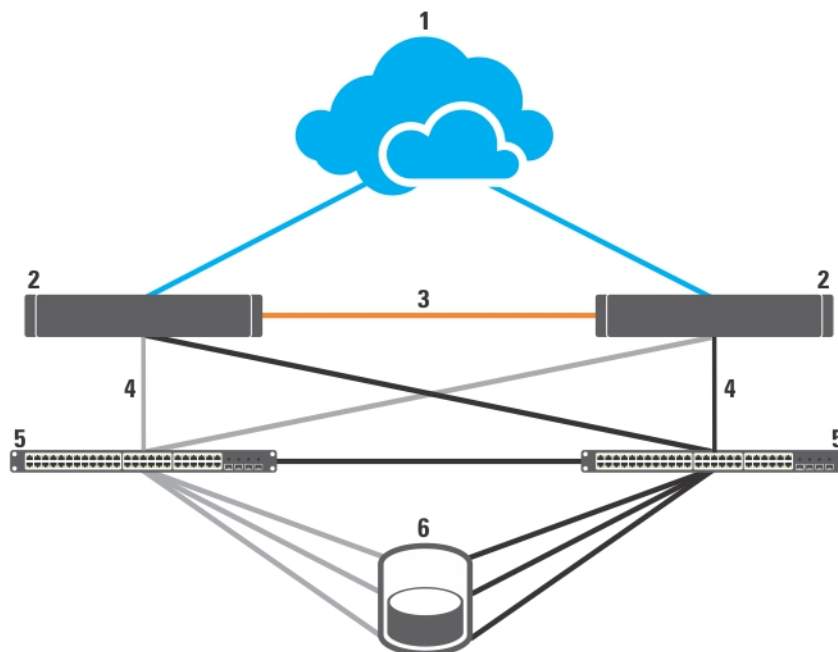


Abbildung 1. iSCSI-SAN-Attached-Cluster

1. Öffentliches Netzwerk
2. Clusterknoten
3. privates Netzwerk
4. iSCSI-Verbindungen
5. Gigabit- oder 10-Gigabit-Ethernet-Switches
6. Speichersystem

Weitere nützliche Dokumente

⚠ VORSICHT: Wichtige Informationen über die Sicherheitsanforderungen und Betriebsvorschriften finden Sie in den Sicherheitshinweisen zum System. Garantiebestimmungen können als separates Dokument beigelegt sein.

Die folgende Dokumentation steht unter support.dell.com/manuals und equallogic.com zur Verfügung:

- Im zusammen mit der Rack-Lösung gelieferten *Rack Installation Guide* (Rack-Installationshandbuch) ist beschrieben, wie das System in einem Rack installiert wird.
- Im *Getting Started Guide* (Handbuch zum Einstieg) finden Sie eine Übersicht über die Ersteinrichtung des Systems.
- Das *Dell Failover Clusters with Microsoft Windows Server 2003 Installation and Troubleshooting Guide* (Installations- und Fehlerbehebungshandbuch für Dell Failover Cluster unter Microsoft Windows Server 2003) enthält weitere Informationen zum Betrieb des Clusters Windows Server 2003.

- Das *Dell Failover Clusters with Microsoft Windows Server 2008 Installation and Troubleshooting Guide* (Installations- und Fehlerbehebungshandbuch für Dell Failover Cluster unter Microsoft Windows Server 2008) enthält weitere Informationen zum Betrieb des Clusters Windows Server 2008.
- Die *Support-Matrizen für Dell Clusterkonfiguration* enthalten eine Liste empfohlener Betriebssysteme, Hardwarekomponenten und Treiber- oder Firmwareversionen für den Failover-Cluster.
- In der Dokumentation zum Betriebssystem ist beschrieben, wie das Betriebssystem installiert (sofern erforderlich), konfiguriert und verwendet wird.
- Die Dokumentation separat erworbener Hardware- und Softwarekomponenten enthält Informationen zur Konfiguration und Installation dieser Zusatzgeräte.
- Die Dokumentation zur Dell PowerVault-Bandbibliothek enthält Informationen zum Installieren, zur Störungsbehebung und Aktualisierung der Bandbibliothek.
- Dell EqualLogic-Dokumentation:
 - Versionshinweise – Enthalten die neuesten Informationen zu Speicherarrays der Dell EqualLogic PS-Reihe und/oder Host Integration Tools.
 - QuickStart – Beschreibt das Einrichten der Arrayhardware und das Erstellen einer Dell EqualLogic PS-Gruppe.
 - Group Administration (Administration von Speicherarraygruppen) – Erläutert die Verwaltung einer Gruppe von Speicherarrays der Dell|EqualLogic PS-Reihe über die Group Manager-GUI.
 - CLI-Referenzhandbuch – Beschreibt, wie Sie mit der CLI (Befehlszeilenschnittstelle) von Group Manager eine Gruppe und einzelne Arrays der Dell|EqualLogic PS-Reihe verwalten können.
 - Hardware-Wartungshandbuch – Enthält Informationen zur Wartung der Arrayhardware.
 - Host Integration Tools Installation and User Guide (Installations- und Benutzerhandbuch zu Host Integration Tools) – Enthält Informationen zum Erstellen und Erweitern von Dell EqualLogic PS-Gruppen, zur Konfiguration von Multipath-E/A, zur Durchführung manueller Transfer-Replizierung und zur Sicherung und Wiederherstellung von Daten.
 - *Host Integration Tools EqualLogic Auto-Snapshot Manager/Microsoft Edition User Guide* (Host Integration Tools EqualLogic Auto-Snapshot Manager/Microsoft Edition Benutzerhandbuch) – Enthält Informationen zum Erstellen und Verwalten von Kopien von Speicherobjekten (zum Beispiel Volumes oder Datenbanken), die sich in Dell EqualLogic PS-Gruppen befinden.
 - SAN HeadQuarters Benutzerhandbuch – Bietet zentrale Überwachung, Leistungstrends und Ereignis-Berichterstellung für mehrere PS-Gruppen.
 - Onlinehilfe – Erweitern Sie in der grafischen Benutzerschnittstelle von Group Manager den Eintrag **Tools** (Extras) im äußeren linken Bereich, und klicken Sie dann auf Online Help (Onlinehilfe), um Hilfe zur GUI- und CLI-Umgebung anzuzeigen.
- Gegebenenfalls sind Versionsinformationen oder Readme-Dateien vorhanden, die den letzten Stand der Änderungen am System oder an der Dokumentation wiedergeben oder fortgeschrittenes technisches Referenzmaterial für erfahrene Benutzer oder IT-Fachleute enthalten.

Hardwareverkabelung für Cluster

In diesem Abschnitt finden Sie Informationen zur Hardware-Verkabelung.

Informationen über Maus-, Tastatur- und Bildschirm-Verkabelung

Bei der Installation einer Clusterkonfiguration im Rack muss ein Umschalter zum Verbinden der Maus, der Tastatur und des Bildschirms mit den Knoten verwendet werden. Wie Sie die Anschlüsse der einzelnen Knoten mit dem Umschalter verbinden, erfahren Sie in der Dokumentation zum Rack.

Informationen über die Verkabelung von Netzteilen

Stellen Sie anhand der Dokumentation für die einzelnen Komponenten der Clusterlösung sicher, dass die jeweiligen Anforderungen an die Stromversorgung erfüllt sind.

Es wird empfohlen, die folgenden grundsätzlichen Vorsichtsmaßnahmen zu beachten, um die Clusterlösung vor einer Beschädigung durch Stromausfälle zu schützen:

- Bei Clusterknoten und Speicherarrays mit mehreren Netzteilen sollten Sie jedes Netzteil an einen eigenen Wechselstromkreis anschließen.
- Verwenden Sie unterbrechungsfreie Stromversorgungen (USV).
- In bestimmten Umgebungen sollten Sie Notstromgeneratoren und eine elektrische Versorgung über getrennte Unterwerke in Betracht ziehen.

Die folgenden Abbildungen zeigen empfohlene Vorgehensweisen zur elektrischen Verkabelung einer Clusterlösung mit zwei Dell PowerEdge-Systemen und einem Speicherarray. Um Redundanz zu gewährleisten, werden die primären Netzteile aller Komponenten an einem oder an zwei Stromkreisen angeschlossen, und die redundanten Netzteile an einem anderen Stromkreis.

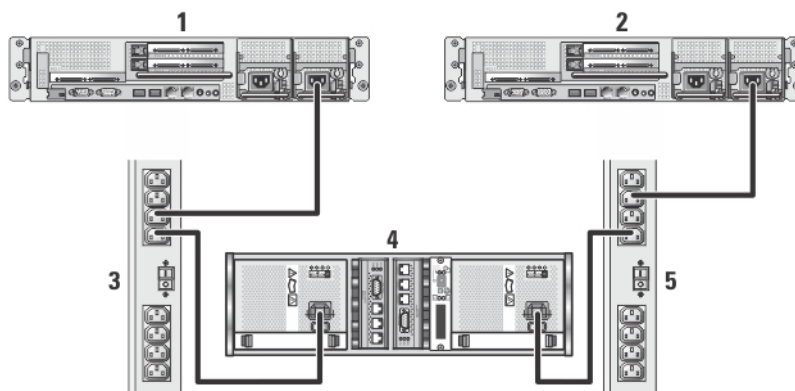


Abbildung 2. Beispiel für die elektrische Verkabelung mit einem Netzteil pro PowerEdge-System

1. Clusterknoten 1
2. Clusterknoten 2

3. Primäre Netzteile an einer Netzstrom-Steckerleiste
4. EqualLogic PS Series-Speicherarray
5. Redundante Netzteile an einer Netzstrom-Steckerleiste

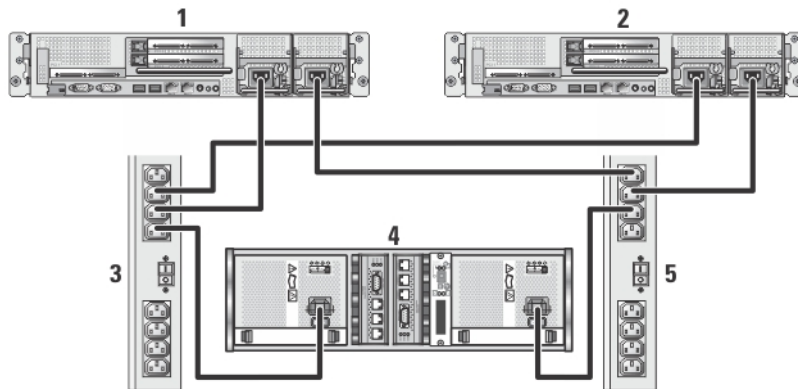


Abbildung 3. Beispiel für die Verkabelung mit zwei Netzteilen in den PowerEdge-Systemen

1. Clusterknoten 1
2. Clusterknoten 2
3. Primäre Netzteile an einer Netzstrom-Steckerleiste
4. EqualLogic PS Series-Speicherarray
5. Redundante Netzteile an einer Netzstrom-Steckerleiste

Informationen zum Verkabeln des Clusters für öffentliche und private Netzwerke

Die Netzwerkadapter der Clusterknoten stellen für jeden Knoten mindestens zwei Netzwerkverbindungen bereit. Im folgenden Abschnitt werden die Netzwerkverbindungen beschrieben.

Netzwerkanschluss Beschreibung

Öffentliches Netzwerk

- Alle Verbindungen zum Client-LAN.
- Es muss mindestens ein öffentliches Netzwerk für die Clientzugriffe und die Clusterkommunikation konfiguriert werden.

Privates Netzwerk

Reservierte Verbindung nur zur gemeinsamen Nutzung von Zustands- und Statusinformationen über den Cluster.

Die folgende Abbildung zeigt ein Beispiel für eine Verkabelung, bei der reservierte Netzwerkadapter in jedem Knoten untereinander verbunden sind (für das private Netzwerk) und die übrigen Adapter mit dem öffentlichen Netzwerk verbunden sind.

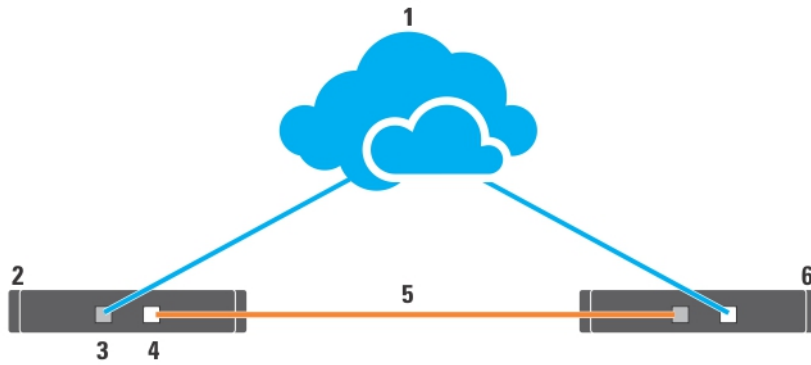


Abbildung 4. Beispiel für eine Netzwerkverkabelung

- | | |
|---------------------------------|----------------------|
| 1. Öffentliches Netzwerk | 5. Privates Netzwerk |
| 2. Clusterknoten 1 | 6. Clusterknoten 2 |
| 3. Öffentlicher Netzwerkadapter | |
| 4. Privater Netzwerkadapter | |

Für öffentliches Netzwerk

Für die Verbindung mit den öffentlichen Netzwerksegmenten lässt sich ein beliebiger Netzwerkadapter verwenden, der von einem System mit TCP/IP unterstützt wird. Sie können weitere Netzwerkadapter installieren, um andere öffentliche Netzwerksegmente zu unterstützen oder für den Fall eines defekten primären Netzwerkadapters bzw. Switch-Ports Redundanz zu gewährleisten.

Für privates Netzwerk

Die private Netzwerkverbindung zu den Knoten erfolgt für jeden Knoten mit einem anderen Netzwerkadapter. Dieses Netzwerk wird für die Kommunikation innerhalb des Clusters verwendet. Die folgende Tabelle beschreibt zwei mögliche private Netzwerkkonfigurationen.

Methode	Hardwarekomponenten	Verbindung
Netzwerk-Switch	Gigabit- oder 10-Gigabit-Ethernet-Netzwerkadapter und -Switches	Installieren Sie je nach Hardware CAT5e- CAT6-, CAT6a- oder CAT7-Kabel, Multimode-Glasfaserkabel mit LC-Steckern (Local Connector) oder Twinaxialkabel zwischen den Netzwerkadaptern in den Knoten mit einem Switch.
Punkt-zu-Punkt (nur Cluster mit zwei Knoten)	Kupfer-Gigabit-Netzwerkadapter mit RJ-45- Anschlüssen	Verbinden Sie die Netzwerkadapter in beiden Knoten mit einem CAT5e- oder besser (CAT6-, CAT6a- oder CAT7-)Ethernet-Kabel.
	Kupfer-10-Gigabit-Ethernet-Netzwerkadapter mit RJ-45 Anschlüssen	Verbinden Sie die Netzwerkadapter in beiden Knoten mit einem CAT6- oder besser (CAT6a- oder CAT7-)Ethernet-Kabel.

Methoden	Hardwarekomponenten	Verbindung
	Kupfer-10-Gigabit-Ethernet-Netzwerkadapter mit SFP+ Anschlüssen	Verbinden Sie die Netzwerkadapter in beiden Knoten mit einem Twinaxialkabel.
	Optische Gigabit- oder 10-Gigabit-Ethernet-Netzwerkadapter mit LC-Anschlüssen	Verbinden Sie die Netzwerkadapter in beiden Knoten mit einem Multimode-Glasfaserkabel.

Verwenden von Netzwerkadaptern mit zwei Ports

Sie können den Cluster so konfigurieren, dass das öffentliche Netzwerk zum Failover für die private Netzwerkverbindung genutzt wird. Wenn Netzwerkadapter mit zwei Ports zum Einsatz kommen, verwenden Sie nicht beide Ports zugleich zur Unterstützung von öffentlichem und privatem Netzwerk.

NIC-Teaming

Beim NIC-Teaming werden zwei oder mehr NICs kombiniert, um für Lastausgleich und Fehlertoleranz zu sorgen. Der Cluster unterstützt NIC-Teaming, aber nur für das öffentliche Netzwerk; NIC-Teaming wird für das private Netzwerk bzw. iSCSI-Netzwerk nicht unterstützt.



ANMERKUNG: Die Netzwerkadapter eines NIC-Teams sollten von der gleichen Marke sein und auch bei den Teaming-Treibern lassen sich die Marken nicht mischen.

Informationen zur Verkabelung der Speicherarrays

Dieser Abschnitt enthält Informationen zur Verbindung des Clusters mit einem oder mehreren Speicherarrays.

Stellen Sie die Kabelverbindungen zwischen den iSCSI-Switches her, und konfigurieren Sie die iSCSI-Switches. Weitere Informationen finden Sie unter „Empfohlene Netzwerkkonfigurationen“.

Verbinden Sie mithilfe von entsprechenden Netzkabeln die iSCSI-Ports von den Servern und Arrays mit den Gigabit-Switches.

Für Gigabit iSCSI-Ports mit RJ-45-Anschlüssen: verwenden Sie CAT5e oder besser (CAT6, CAT6a oder CAT7)

Für 10 Gigabit iSCSI-Ports:

- Mit RJ-45-Anschlüssen: verwenden Sie CAT6 oder besser (CAT6a oder CAT7)
- Mit LC-Anschlüssen: verwenden Sie ein für 10GBASE-SR geeignetes Glasfaserkabel
- Mit SFP+ Anschlüssen: verwenden Sie Twinaxialkabel

Verkabelung des Speichers bei einem iSCSI-SAN-Attached-Cluster

Ein iSCSI-SAN-Attached-Cluster ist eine Clusterkonfiguration, in der alle Clusterknoten über ein Netzwerk und redundante iSCSI-Switches an ein einzelnes Speicherarray oder an mehrere Speicherarrays angeschlossen sind.

Die folgenden Abbildungen zeigen Beispiele eines iSCSI SAN-Attached-Clusters mit zwei Knoten und eines iSCSI SAN-Attached-Clusters mit sechzehn Knoten.

Ähnliche Verkabelungsmuster können bei Clustern mit einer anderen Knotenanzahl verwendet werden.



ANMERKUNG: Bei den in diesem Abschnitt beschriebenen Verfahren zum Herstellen von redundanten Verbindungen zwischen den Clusterknoten und dem Speicherarray handelt es sich jeweils um eine bewährte Vorgehensweise. Möglich sind auch andere Verfahren, mit denen sich eine vergleichbare Verbindungsredundanz erreichen lässt.

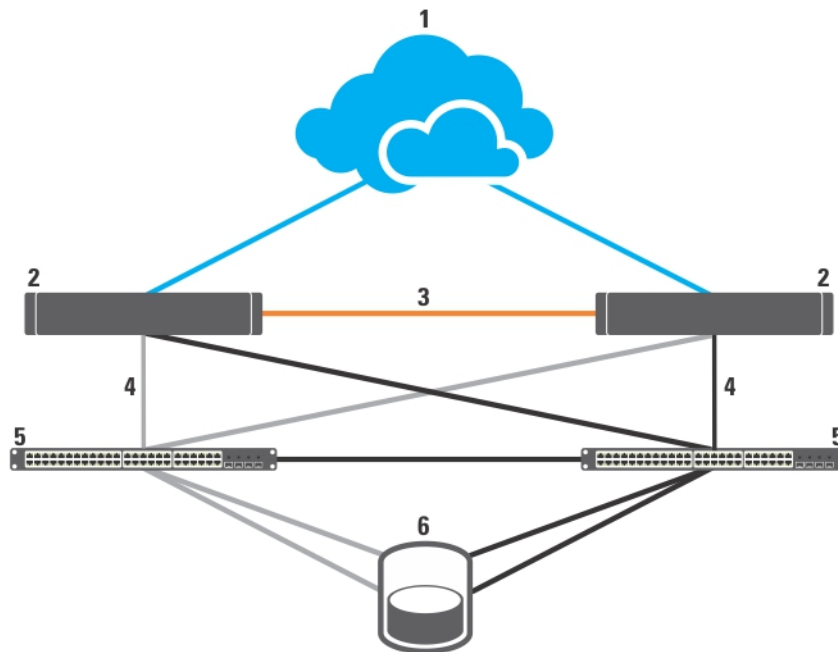


Abbildung 5. iSCSI-SAN-Attached-Cluster mit zwei Knoten

- | | |
|--------------------------|---|
| 1. Öffentliches Netzwerk | 5. Gigabit- oder 10-Gigabit-Ethernet-Switches |
| 2. Clusterknoten | 6. Speichersystem |
| 3. privates Netzwerk | |
| 4. iSCSI-Verbindungen | |

Die Gigabit-NICs können auf die 10-Gigabit-iSCSI-Ports an den EqualLogic PS4110/PS6010/PS6110/PS6510-Speichersystemen zugreifen, wenn eine der folgenden Bedingungen zutrifft:

- Der Switch unterstützt Gigabit- und 10-Gigabit-Ethernet.
- Die Server, die mit einem Gigabit-Ethernet-Switch verbunden sind, sind mit dem 10-Gigabit-Ethernet am Speichersystem kaskadiert.

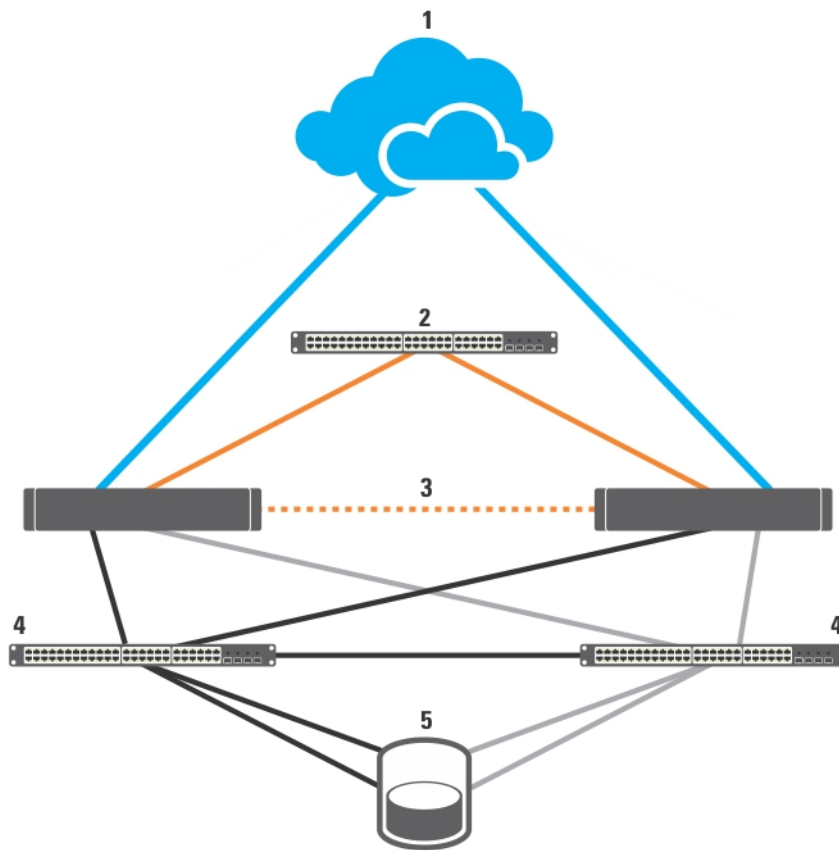


Abbildung 6. iSCSI-SAN-Attached-Cluster mit sechzehn Knoten

1. Öffentliches Netzwerk
2. privates Netzwerk
3. Clusterknoten (2-16)
4. Gigabit- oder 10-Gigabit-Ethernet-Switches
5. Speichersystem

Verkabelung eines iSCSI-SAN-Attached-Clusters mit Speicherarrays der Dell EqualLogic PS Series

1. Verbinden Sie Clusterknoten 1 mit den iSCSI-Switches:
 - a) Verbinden Sie ein Netzkabel zwischen iSCSI-NIC 0 (oder NIC-Port 0) und dem Netzwerk-Switch 0.
 - b) Verbinden Sie ein Netzkabel zwischen iSCSI-NIC 1 (oder NIC-Port 1) und dem Netzwerk-Switch 1.
2. Wiederholen Sie Schritt 1 für jeden Clusterknoten.
3. Verbinden Sie die Dell EqualLogic PS-Speicherarrays mit den iSCSI-Switches.
Weitere Informationen zur Verkabelung der Speicherarrays finden Sie in den folgenden Abschnitten.

Verkabelung der Dell EqualLogic PS4110/PS6110 Speicherarrays

1. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 0.
2. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 1 und Ethernet 0 am Controller 1.
3. Wiederholen Sie Schritte 1 und 2, um die Dell EqualLogic PS4110/PS6110-Speicherarrays mit den iSCSI-Switches zu verbinden.

ANMERKUNG: Sie können jeweils nur einen der zwei 10 Gb Ethernet-Ports auf jedem Controller verwenden. Verwenden Sie bei einem 10GBASE-T-Port (linker Ethernet 0-Port) ein CAT6- oder ein besseres Kabel. Verwenden Sie bei SFP+ Port (rechter Ethernet 0-Port) ein für 10GBASE-SR oder Twinaxialkabel geeignetes Glasfaserkabel.

Weitere Informationen finden Sie in den nachstehenden Abbildungen.

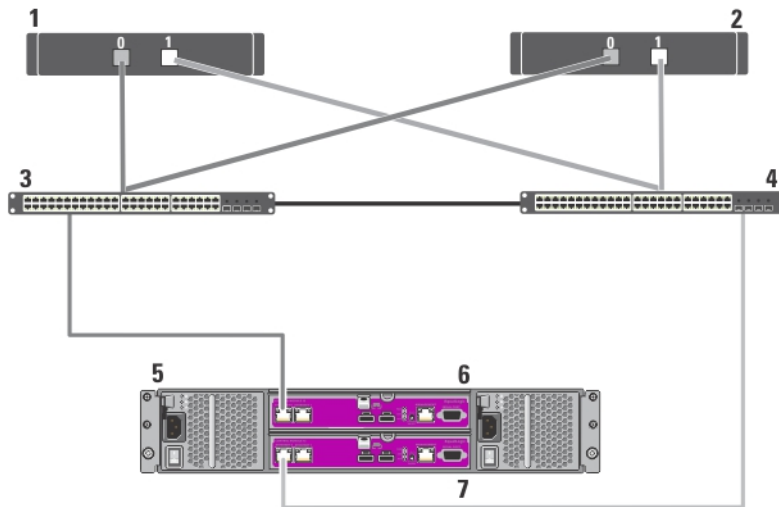


Abbildung 7. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS4110 Speicherarray

- | | |
|--------------------|--|
| 1. Clusterknoten 1 | 5. Speichersystem Dell EqualLogic PS4110 |
| 2. Clusterknoten 2 | 6. Controller 0 |
| 3. Switch 0 | 7. Controller 1 |
| 4. Switch 1 | |

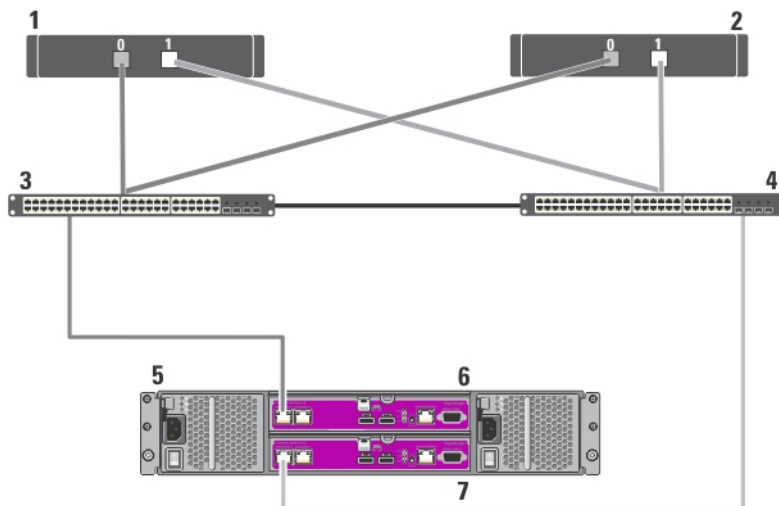


Abbildung 8. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS6110 Speicherarray

1. Clusterknoten 1
2. Clusterknoten 2
3. Switch 0
4. Switch 1

5. Speichersystem Dell EqualLogic PS6110
6. Controller 0
7. Controller 1

Verkabelung der Dell EqualLogic PS4000/PS4100/PS6010/PS6510 Speicherarrays

1. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
2. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 0.
3. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 1 und Ethernet 1 am Controller 1.
4. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 1 am Controller 1.
5. Wiederholen Sie Schritte 1 und 4, um die Dell EqualLogic PS4000/PS4100/PS6010/PS6510-Speicherarrays mit den iSCSI-Switches zu verbinden.

ANMERKUNG: Die Verwendung aller vier Kabel in den Schritten 1 bis 4 bietet für PS4100 Speicherarray den höchsten Grad an Redundanz. Es funktioniert gut mit nur 2 Kabeln. Sie können entweder Schritt 1 oder 2, und entweder Schritt 3 oder 4 überspringen.

Weitere Informationen finden Sie in den nachstehenden Abbildungen.

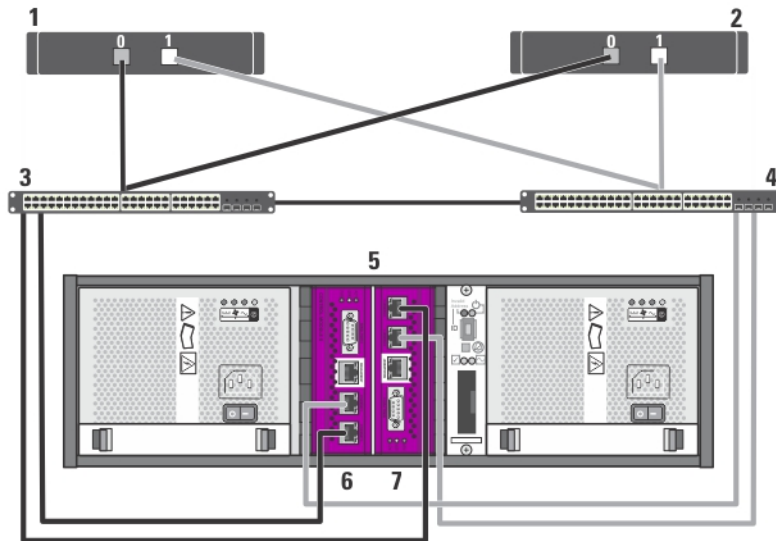


Abbildung 9. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS4000 Speicherarray

1. Clusterknoten 1
2. Clusterknoten 2
3. Switch 0
4. Switch 1

5. Speichersystem Dell EqualLogic PS4000
6. Controller 1
7. Controller 0

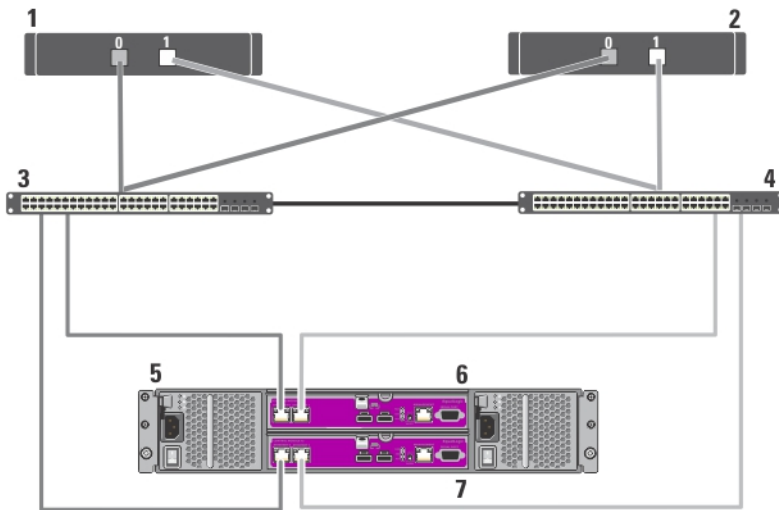


Abbildung 10. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS4100 Speicherarray

- | | |
|--------------------|--|
| 1. Clusterknoten 1 | 5. Speichersystem Dell EqualLogic PS4100 |
| 2. Clusterknoten 2 | 6. Controller 0 |
| 3. Switch 0 | 7. Controller 1 |
| 4. Switch 1 | |

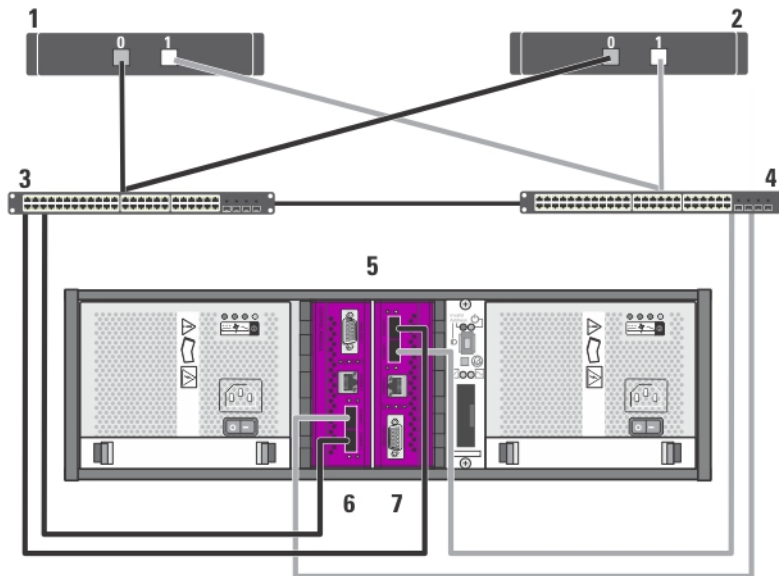


Abbildung 11. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS6010 Speicherarray

- | | |
|--------------------|--|
| 1. Clusterknoten 1 | 4. Switch 1 |
| 2. Clusterknoten 2 | 5. Speichersystem Dell EqualLogic PS6010 |
| 3. Switch 0 | 6. Controller 1 |

7. Controller 0

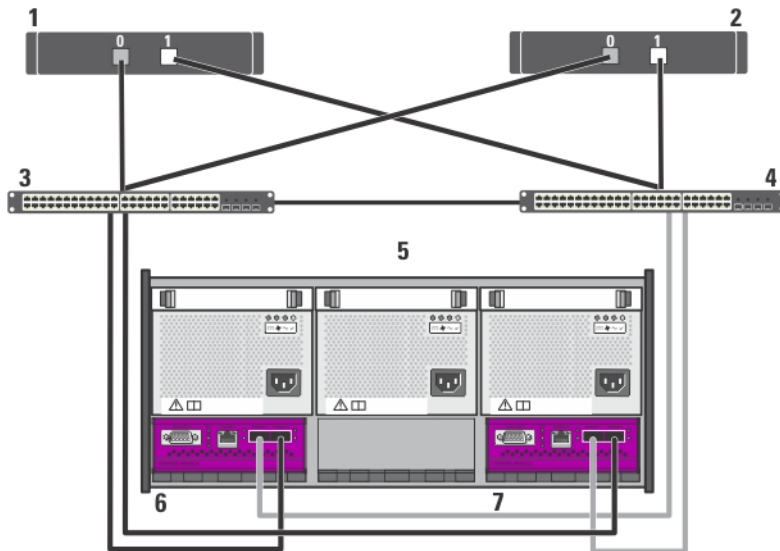


Abbildung 12. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS6510 Speicherarray

- | | |
|--------------------|--|
| 1. Clusterknoten 1 | 5. Speichersystem Dell EqualLogic PS6510 |
| 2. Clusterknoten 2 | 6. Controller 1 |
| 3. Switch 0 | 7. Controller 0 |
| 4. Switch 1 | |

Verkabelung der Dell EqualLogic PS5000/PS5500 Speicherarrays

1. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
2. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 1 und Ethernet 0 am Controller 1.
3. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 1 und Ethernet 2 am Controller 1.
4. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
5. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 1 am Controller 1.
6. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 2.
7. Wiederholen Sie Schritte 1 und 6, um die Dell EqualLogic PS5000/PS5500-Speicherarrays mit den iSCSI-Switches zu verbinden.

Weitere Informationen finden Sie in den nachstehenden Abbildungen.

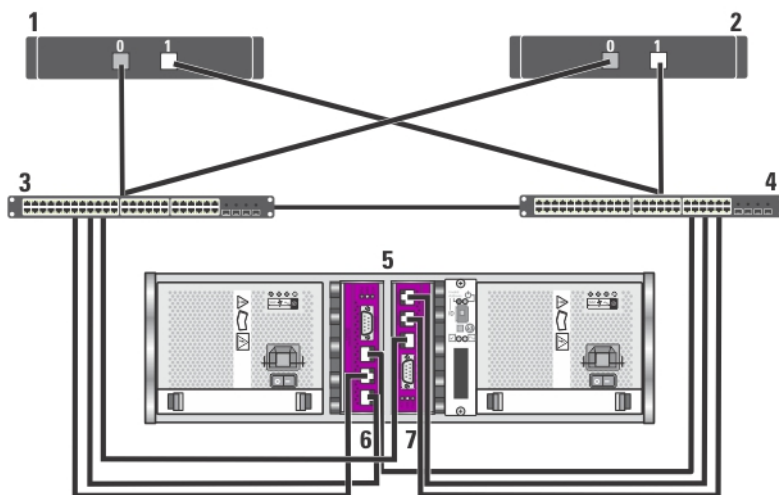


Abbildung 13. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS5000 Speicherarray

- | | |
|--------------------|--|
| 1. Clusterknoten 1 | 5. Speichersystem Dell EqualLogic PS5000 |
| 2. Clusterknoten 2 | 6. Controller 1 |
| 3. Switch 0 | 7. Controller 0 |
| 4. Switch 1 | |

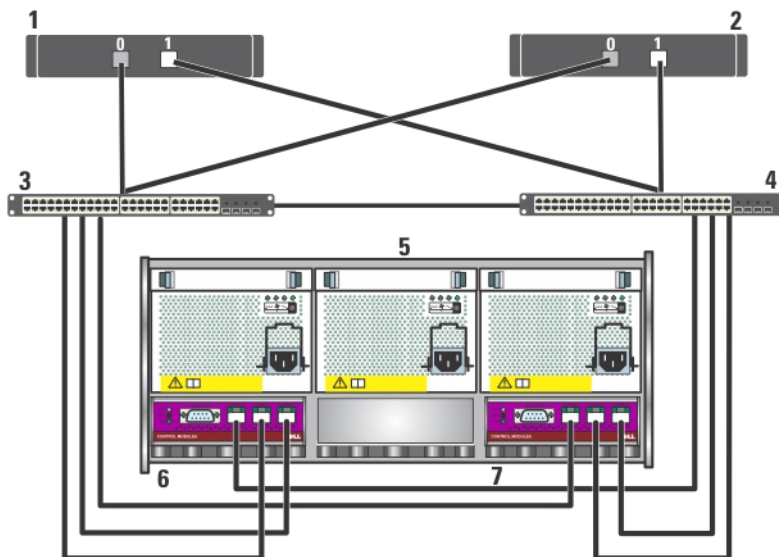


Abbildung 14. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS5500-Speicherarray

- | | |
|--------------------|--|
| 1. Clusterknoten 1 | 5. Speichersystem Dell EqualLogic PS5500 |
| 2. Clusterknoten 2 | 6. Controller 1 |
| 3. Switch 0 | 7. Controller 0 |
| 4. Switch 1 | |

Verkabelung der Dell EqualLogic PS6000/PS6100/PS6500 Speicherarrays

1. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
2. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 1 und Ethernet 0 am Controller 1.
3. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 1 und Ethernet 2 am Controller 1.
4. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 1 und Ethernet 1 am Controller 3.
5. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
6. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 1 am Controller 1.
7. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 2.
8. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 3.
9. Wiederholen Sie Schritte 1 und 8, um die Dell EqualLogic PS6000/PS6100/PS6500-Speicherarrays mit den iSCSI-Switches zu verbinden.

ANMERKUNG: Die Verwendung aller acht Kabel in den Schritten 1 bis 4 bietet für PS6100 Speicherarray den höchsten Grad an Redundanz. Es funktioniert gut mit nur 4 Kabeln. Sie können entweder Schritt 1 oder 5, entweder Schritt 2 oder 6, entweder Schritt 3 oder 7 und entweder Schritt 4 oder 8 überspringen.

Weitere Informationen finden Sie in den nachstehenden Abbildungen.

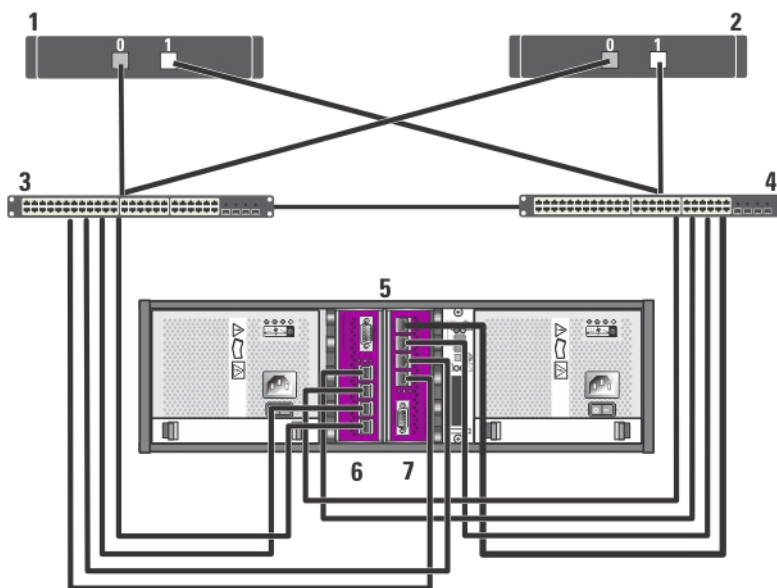


Abbildung 15. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS6000 Speicherarray

- | | |
|--------------------|--|
| 1. Clusterknoten 1 | 5. Speichersystem Dell EqualLogic PS6000 |
| 2. Clusterknoten 2 | 6. Controller 1 |
| 3. Switch 0 | 7. Controller 0 |
| 4. Switch 1 | |

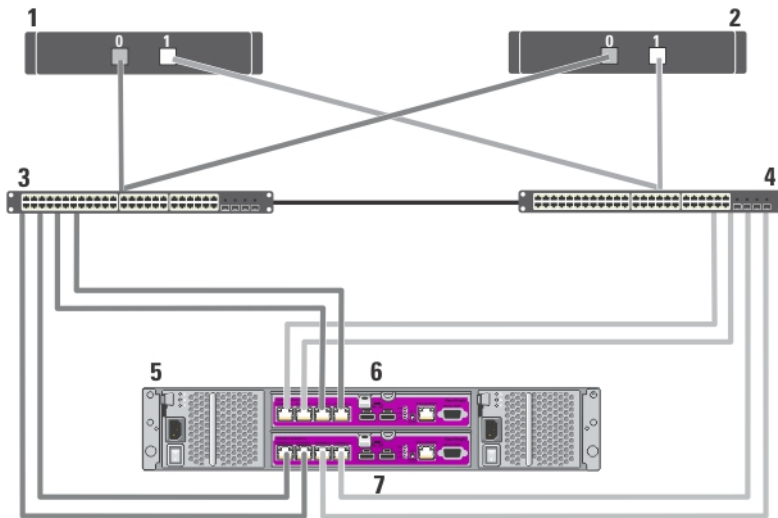


Abbildung 16. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS6100 Speicherarray

- | | |
|--------------------|--|
| 1. Clusterknoten 1 | 5. Speichersystem Dell EqualLogic PS6100 |
| 2. Clusterknoten 2 | 6. Controller 0 |
| 3. Switch 0 | 7. Controller 1 |
| 4. Switch 1 | |

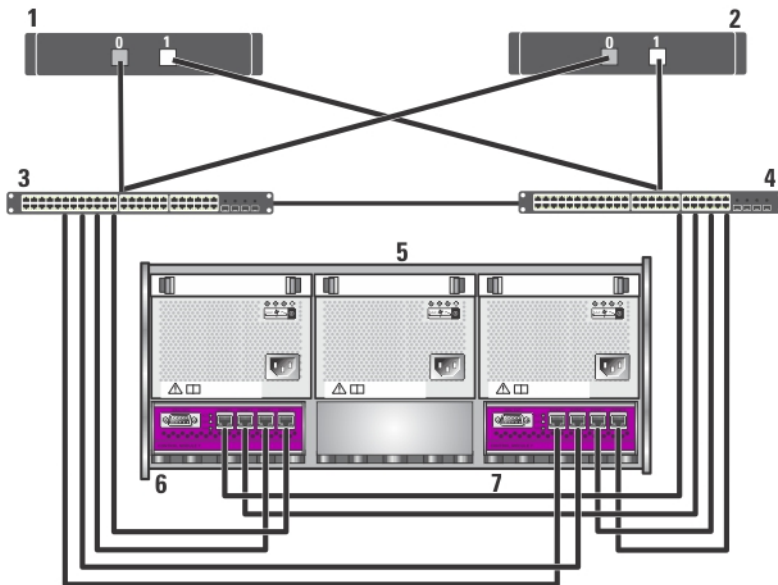


Abbildung 17. Verkabelung eines iSCSI-SAN-Attached-Clusters mit einem Dell EqualLogic PS6500 Speicherarray


- | | |
|--------------------|-------------|
| 1. Clusterknoten 1 | 3. Switch 0 |
| 2. Clusterknoten 2 | 4. Switch 1 |

- 5. Speichersystem Dell EqualLogic PS6500
- 6. Controller 1

7. Controller 0

Verkabelung mehrerer iSCSI-SAN-Attached-Cluster mit Speicherarrays der Dell EqualLogic PS Series

Um mehrere Cluster mit den Speicherarrays zu verkabeln, verbinden Sie die Clusterknoten mit den entsprechenden iSCSI-Switches, und verbinden Sie dann die iSCSI-Switches mit den entsprechenden Controllern der Dell EqualLogic PS-Speicherarrays.


 **ANMERKUNG:** Beim nachfolgend beschriebenen Verfahren wird die Abbildung mit dem Titel „Verkabelung eines iSCSI SAN-Attached-Clusters mit einem Dell EqualLogic PS5000-Speicherarray“ als Beispiel für die Verkabelung weiterer Cluster verwendet.

1. Verbinden Sie im ersten Cluster den Clusterknoten 1 mit den iSCSI-Switches.
 - a) Verbinden Sie ein Netzkabel zwischen iSCSI-NIC 0 (oder NIC-Port 0) und dem Netzwerk-Switch 0.
 - b) Verbinden Sie ein Netzkabel zwischen iSCSI-NIC 1 (oder NIC-Port 1) und dem Netzwerk-Switch 1.
2. Wiederholen Sie Schritt 1 für jeden Knoten.
3. Wiederholen Sie Schritt 1 und Schritt 2 für jeden weiteren Cluster.
4. Verbinden Sie die Dell EqualLogic PS-Speicherarrays mit den iSCSI-Switches.

Weitere Informationen zur Verkabelung der Speicherarrays finden Sie in den folgenden Abschnitten.


Verkabelung mehrerer iSCSI SAN-Attached-Clusters für Dell EqualLogic PS4110/PS6110-Speicherarrays

1. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 0.
2. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 1 und Ethernet 0 am Controller 1.
3. Wiederholen Sie Schritte 1 und 2, um die Dell EqualLogic PS4110/PS6110-Speicherarrays mit den iSCSI-Switches zu verbinden.

 **ANMERKUNG:** Sie können jeweils nur einen der zwei 10 Gb Ethernet-Ports auf jedem Controller verwenden. Verwenden Sie bei einem 10GBASE-T-Port (linker Ethernet 0-Port) ein CAT6- oder ein besseres Kabel. Verwenden Sie bei SFP+ Port (rechter Ethernet 0-Port) ein für 10GBASE-SR oder Twinaxialkabel geeignetes Glasfaserkabel.

Verkabelung mehrerer iSCSI SAN-Attached-Clusters für Dell EqualLogic PS4000/PS4100/PS6010/PS6510-Speicherarrays

1. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
2. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 0.
3. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 1 und Ethernet 1 am Controller 1.
4. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 0 und Ethernet 1 am Controller 1.
5. Wiederholen Sie Schritte 1 und 4, um die Dell EqualLogic PS4000/PS4100/PS6010/PS6510-Speicherarrays mit den iSCSI-Switches zu verbinden.

 **ANMERKUNG:** Die Verwendung aller vier Kabel in den Schritten 1 bis 4 bietet für PS4100 Speicherarray den höchsten Grad an Redundanz. Es funktioniert gut mit nur 2 Kabeln. Sie können entweder Schritt 1 oder 2, und entweder Schritt 3 oder 4 überspringen.


Verkabelung mehrerer iSCSI SAN-Attached-Clusters für Dell EqualLogic PS5000/PS5500-Speicherarrays

1. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
2. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 1 und Ethernet 0 am Controller 1.
3. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 1 und Ethernet 2 am Controller 1.
4. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
5. Installieren Sie ein Netzkabel zwischen dem Netzwerk-Switch 0 und Ethernet 1 am Controller 1.

6. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 2.
7. Wiederholen Sie Schritte 1 und 6, um die Dell EqualLogic PS5000/PS5500-Speicherarrays mit den iSCSI-Switches zu verbinden.

Verkabelung mehrerer iSCSI SAN-Attached-Clusters für Dell EqualLogic PS6000/PS6100/PS6500-Speicherarrays


1. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
2. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 1 und Ethernet 0 am Controller 1.
3. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 1 und Ethernet 2 am Controller 1.
4. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 1 und Ethernet 1 am Controller 3.
5. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 1.
6. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 1 am Controller 1.
7. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 2.
8. Installieren Sie ein Netzwerkkabel zwischen dem Netzwerk-Switch 0 und Ethernet 0 am Controller 3.
9. Wiederholen Sie Schritte 1 und 8, um die Dell EqualLogic PS6000/PS6100/PS6500-Speicherarrays mit den iSCSI-Switches zu verbinden.

 **ANMERKUNG:** Die Verwendung aller acht Kabel in den Schritten 1 bis 4 bietet für PS6100 Speicherarray den höchsten Grad an Redundanz. Es funktioniert gut mit nur 4 Kabeln. Sie können entweder Schritt 1 oder 5, entweder Schritt 2 oder 6, entweder Schritt 3 oder 7 und entweder Schritt 4 oder 8 überspringen.

Weitere Informationen

Weitere Informationen zur Konfiguration der Cluster-Komponenten finden Sie in der Speicher- und Band-Backup-Dokumentation auf der Dell Support-Website unter support.dell.com/manuals.


Vorbereiten der Systeme für den Clusterbetrieb

 **VORSICHT:** Viele Reparaturen am Computer dürfen nur von einem zertifizierten Servicetechniker ausgeführt werden. Sie sollten nur die Behebung von Störungen sowie einfache Reparaturen unter Berücksichtigung der jeweiligen Angaben in den Produktdokumentationen von Dell durchführen bzw. die elektronischen oder telefonischen Anweisungen des Service- und Supportteams von Dell befolgen. Schäden durch nicht von Dell genehmigte Wartungsversuche werden nicht durch die Garantie abgedeckt. Lesen und beachten Sie die Sicherheitshinweise, die Sie zusammen mit Ihrem Produkt erhalten haben.


Konfigurieren eines Clusters

Mithilfe folgender Anweisungen erhalten Sie einen Überblick über die Konfiguration eines Clusters.


1. Stellen Sie sicher, dass am Standort eine ausreichende Stromversorgung für den Cluster gegeben ist. Ihr Verkaufsberater kann Sie über die Anforderungen der örtlichen Stromversorgung informieren.
2. Installieren Sie die Systeme, die gemeinsamen Speicherarrays und die Verbindungs-Switches (zum Beispiel in einem Rack), und achten Sie darauf, dass alle Komponenten eingeschaltet sind.
3. Stellen Sie das Betriebssystem (einschließlich aller relevanten Servicepacks und Hotfixes) und die Netzwerkadapter-Treiber auf allen Clusterknoten bereit. Je nach der verwendeten Bereitstellungsmethode ist möglicherweise eine Netzwerkverbindung erforderlich, um diesen Schritt erfolgreich abzuschließen.


 **ANMERKUNG:** Um sich die Planung und Bereitstellung des Clusters zu erleichtern, erfassen Sie die relevanten Informationen zur Clusterkonfiguration im Cluster-Datenformular und die iSCSI-Konfigurationsdaten im iSCSI-Konfigurationsarbeitsblatt.

4. Richten Sie die physische Netzwerktopologie und die TCP/IP-Einstellungen für Netzwerkadapter auf jedem Clusterknoten ein, um den Zugang zum öffentlichen und privaten Netzwerk des Clusters herzustellen.
5. Konfigurieren Sie alle Clusterknoten als Mitglieder derselben Microsoft Active Directory-Domäne.

 **ANMERKUNG:** Die Clusterknoten können als Domänencontroller konfiguriert werden. Weitere Informationen finden Sie unter Auswahl des Domänen-Modells im *Dell Failover Clusters with Microsoft Windows Server 2003 Installation and Troubleshooting Guide* (Dell Failover Clusters unter Microsoft Windows Server 2003 Installations- und Fehlerbehebungshandbuch) oder *Dell Failover Clusters with Microsoft Windows Server 2008 Installation and Troubleshooting Guide* (Dell Failover Clusters unter Microsoft Windows Server 2008 Installations- und Fehlerbehebungshandbuch) unter support.dell.com/manuals.

6. Richten Sie die physische Speichertopologie ein, und nehmen Sie die erforderlichen Einstellungen an den Speicherarrays vor, um die Verbindung zwischen dem Speicherarray und den Systemen, die als Clusterknoten konfiguriert werden, herzustellen. Konfigurieren Sie die Speicherarrays gemäß der Speicherarray-Dokumentation.
7. Erstellen Sie mit der Speicherarray-Verwaltung mindestens ein Volume, und weisen Sie anschließend die Volumes allen Clusterknoten zu. Das Volume dient bei einem Failover Cluster mit Microsoft Windows Server 2003 als Quorumdatenträger oder bei einem Failover Cluster mit Windows Server 2008 als Witness-Datenträger.
8. Wählen Sie eines der Systeme aus, und bilden Sie einen neuen Failover Cluster, indem Sie den Clusternamen, die Clusterverwaltungs-IP-Adresse und die Quorumressource konfigurieren. Nähere Informationen finden Sie im Abschnitt „Vorbereiten der Systeme für den Clusterbetrieb“.

 **ANMERKUNG:** Führen Sie bei Failover Clusters mit Windows Server 2008 den **Cluster Validation Wizard** (Clustervalidierungsassistenten) aus, um sicherzustellen, dass das System zur Clusterbildung bereit ist.

9. Fügen Sie den/die verbliebenen Knoten zum Failover-Cluster hinzu. Nähere Informationen finden Sie im Abschnitt „Vorbereiten der Systeme für den Clusterbetrieb“.
 10. Konfigurieren Sie die Rollen für Clusternetzwerke. Stellen Sie sicher, dass keine der zur iSCSI-Speicherung (oder zu anderen Zwecken außerhalb des Clusters) verwendeten Netzwerkschnittstellen durch den Cluster kontrolliert wird.
 11. Testen Sie die Failover-Funktionen des neuen Clusters.
-  **ANMERKUNG:** Bei Failover Clustern mit Windows Server 2008 können Sie auch den **Cluster Validation Wizard** (Assistent zur Clustervalidierung) nutzen.
12. Konfigurieren Sie hochverfügbare Anwendungen und Dienste auf dem Failover-Cluster. Je nach Konfiguration kann es erforderlich sein, hierfür weitere Volumes am Cluster bereitzustellen oder neue Cluster-Ressourcengruppen anzulegen. Testen Sie die Failover-Funktionen der neuen Ressourcen.
 13. Konfigurieren Sie Clientsysteme für den Zugriff auf die hochverfügbaren Anwendungen und Dienste, die auf dem Failover Cluster aktiv sind.

Installationsübersicht

Auf allen Cluster-Knoten im Failover-Cluster muss das Betriebssystem Windows in derselben Version, Edition, Service-Pack-Stufe und Prozessorarchitektur installiert sein. So können beispielsweise alle Knoten mit Windows Server 2003 R2 Enterprise x64 Edition konfiguriert sein. Wenn auf den verschiedenen Knoten unterschiedliche Betriebssystemversionen installiert sind, lässt sich der Failover Cluster unter Umständen nicht richtig konfigurieren. Je nach dem auf dem Cluster konfigurierten Betriebssystem wird empfohlen, vor dem Konfigurieren des Failover Clusters zunächst Serverrollen einzurichten.

Eine Liste der Dell PowerEdge-Systeme, iSCSI-NICs, eine Liste der unterstützten Betriebssystemversionen sowie spezifische Treiber- und Firmwareversionen finden Sie in den *Dell Cluster Configuration Support Matrices* (Support-Matrizen zur Dell Clusterkonfiguration) unter dell.com/ha.

In den folgenden Unterabschnitten werden die Schritte beschrieben, über die Sie die Kommunikation zwischen den Clusterknoten und dem/den freigegebenen Dell EqualLogic PS Series-Speicherarray(s) einrichten und Laufwerke des/der Speicherarray(s) für den Cluster präsent machen können.

- Installation der iSCSI-NICs
- Installieren der Host Integration Tools
- Installation des Microsoft iSCSI-Software-Initiators
- Ändern der Einstellungen in der Registry
- Konfiguration der gemeinsamen Speicherarrays
- Installation und Konfiguration eines Failover-Clusters


Zusätzliche Informationen zur Installation von iSCSI-NICs


- Es wird empfohlen, die aktuellen und kompatiblen Service-Packs oder Hotfixes für den NIC-Treiber zu installieren.
- Um die Leistung zu optimieren, sollten Sie die Flusskontrolle und Jumbo-Frames an allen NICs und Switches aktivieren, über die iSCSI-Datenverkehr läuft.
- Informationen über unterstützte NICs und Treiber finden Sie in den *Dell Cluster Configuration Support Matrices* (Support-Matrizen zur Dell Clusterkonfiguration) unter dell.com/ha.

Host-Integrationstools

Die Host Integration Tools (Host-Integrationstools) umfassen folgende Anwendungen:

Remote-Installationsassistent	Zum Initialisieren von Dell EqualLogic PS Series-Speicherarrays und zum Einrichten und Konfigurieren des Zugangs zu einer Dell EqualLogic PS Series-Gruppe. Der Assistent ermöglicht auch die Konfiguration von Multipath-E/A (MPIO) unter Windows Server 2003 und Windows Server 2008.
Multipath-E/A-gerätespezifisches Modul (DSM)	Ermöglicht die Konfiguration mehrerer redundanter Netzwerkpfade zwischen einem System mit Windows-Betriebssystem und Speicherlaufwerken einer Dell EqualLogic PS Series-Gruppe, um Verfügbarkeit und Leistung zu maximieren.
Auto-Snapshot Manager/ Microsoft Edition (ASM/ME)	Ermöglicht das Implementieren von Microsoft Volume Snapshot Service (VSS) zum Erstellen von Snapshots, Klonen und Duplikaten; damit lassen sich kritische Daten unterstützter Anwendungen wie Microsoft SQL Server, Exchange Server, Hyper-V und NTFS-Freigaben zeitpunktgenau sichern. Auto-Snapshot Manager ist ein VSS-Requestor und beinhaltet einen VSS-Anbieter.

 **ANMERKUNG:** Weitere Informationen zur Verwendung von ASM im Cluster finden Sie im *Host Integration Tools EqualLogic Auto-Snapshot Manager/Microsoft Edition User Guide* (Host Integration Tools EqualLogic Auto-Snapshot Manager/Microsoft Edition Benutzerhandbuch) unter support.dell.com/manuals.

-  **ANMERKUNG:** ASM wird in der Clusterumgebung mit Host Integration Tools Version 3.2 oder höher unterstützt.
- VDS Provider – Ermöglicht die Nutzung von Microsoft VDS (Virtual Disk Service) und Microsoft Storage Manager for SANs zum Erstellen und Verwalten von Volumes in einer Dell EqualLogic PS Series-Gruppe.
 - Umfasst den iSCSI-Port-Treiber, Initiatordienst und Software-Initiator. Unterstützt iSCSI-Geräte beim Aufbau von Verbindungen über den Windows TCP/IP-Stack mit NICs. Informationen zum Einsatz des Microsoft iSCSI-Software-Initiators finden Sie in der Dokumentation unter microsoft.com.

Installieren der Host Integration Tools

1. Laden Sie das Host Integration Tools-Kit von der Technischen Support-Website herunter oder verwenden Sie den mit einem EqualLogic PS Series-Array ausgelieferte *Host Integration Tools*-Datenträger.
2. Starten Sie die Installation, indem Sie das Kit von der Website herunterladen oder das Medium *EqualLogic Host Integration Tools for Microsoft Windows* ins System einlegen.
3. Klicken Sie im Installationsbildschirm auf **View Documentation** (Dokumentation anzeigen), um das *Host Integration Tools User Guide* (Host Integration Tools-Benutzerhandbuch) anzuzeigen. Es wird dringend empfohlen, vor dem Fortsetzen des Installationsvorgangs das *Benutzerhandbuch* und die *Host Integration Tools Release Notes* (Versionshinweise zu den Host Integration Tools) zu lesen.
4. Bei der Host Integration Tools-Version 3.1.1 führen Sie die Datei **setup.exe** aus. Bei der Host Integration Tools-Version 3.2 oder höher führen Sie die Datei **setup.exe -cluster** aus.
5. Geben Sie Informationen zur Installation ein, wenn Sie dazu aufgefordert werden. Sie können entweder die Installationsvariante **Typical** (Typisch) mit allen vom Betriebssystem unterstützten Tools wählen, oder die Variante **Custom** (Benutzerdefiniert), bei der Sie selbst entscheiden, welche Tools installiert werden.

Ausführen des Remote-Setup-Assistenten

Der **Remote-Installationsassistent** erleichtert die Einrichtung von Dell EqualLogic PS Series-Gruppen (SAN) und Windows-Computern.

Nach Installation der Host Integration Tools können Sie den Remote-Installationsassistenten automatisch starten. Um ihn stattdessen später manuell auszuführen, verwenden Sie den folgenden Schritt:

1. Klicken Sie auf **Start Programme** → **Equallogic** → **Remote Setup Wizard (Remote-Installationsassistent)**.
2. Wählen Sie die Aufgabe aus, die ausgeführt werden soll:
 - Array initialisieren (und eine Gruppe erstellen oder erweitern).
 - System für den Zugriff auf ein PS-SAN konfigurieren.

- MPIO (Multipath-E/A) zwischen einem System und PS-Gruppen-Volumes konfigurieren.

EqualLogic PS Series-Arrays und Gruppen

Der Remote-Installationsassistent ermöglicht es, ein EqualLogic PS Series-Array zu initialisieren und eine EqualLogic PS Series-Gruppe zu erstellen, der das Array als erstes Mitglied angehört. Darüber hinaus richtet der Assistent den Systemzugriff auf diese Gruppe ein, indem er die Gruppen-IP-Adresse als Erkennungsadresse für das iSCSI-Target konfiguriert und den Zugriff eines Microsoft-Dienstes (VSS oder VDS) auf die Gruppe über CHAP-Authentifizierung (CHAP = Challenge-Handshake Authentication Protocol) aktiviert.

Bevor Sie ein Array initialisieren und eine Gruppe erstellen, informieren Sie sich über die Konfiguration von Arrays und Gruppen. Weitere Informationen finden Sie in den nachstehenden Tabellen. Der **Remote-Installationsassistent** fordert Sie zur Eingabe der Array- und Gruppeninformationen auf.

Arraykonfiguration

Eingabe	Beschreibung
Member name (Name des Mitglieds)	Eindeutiger Name (bis zu 63 Ziffern, Buchstaben oder Bindestriche). Dient zur Identifizierung des Arrays in der Gruppe. Das erste Zeichen muss ein Buchstabe oder eine Ziffer sein.
IP-Adresse	Netzwerkadresse der Ethernet-0-Netzwerkschnittstelle.
Netmask (Netzmaske)	Dient zusammen mit der IP-Adresse zur Identifizierung des Subnetzes, dem die Ethernet-0-Netzwerkschnittstelle angehört.
Default gateway (Standard-Gateway)	Netzwerkadresse für das Gerät zum Verbinden von Subnetzen und Weiterleiten von Netzwerkdatenverkehr über das lokale Netzwerk hinaus. Ein Standard-Gateway ermöglicht der Ethernet-0-Netzwerkschnittstelle, außerhalb des lokalen Netzwerks zu kommunizieren (zum Beispiel, um Computern von außerhalb des lokalen Netzwerks den Zugriff auf Volumes zu ermöglichen).



ANMERKUNG: Das Standard-Gateway muss dem gleichen Subnetz wie die Ethernet-0-Netzwerkschnittstelle angehören.

RAID policy (RAID-Richtlinie)	Die RAID-Richtlinie, die für das erste Mitglied der Gruppe konfiguriert ist: <ul style="list-style-type: none"> – RAID-10 – Striping, aufgesetzt auf mehrere RAID-1 (Spiegelungs-) Sätze, mit einem oder zwei Ersatzlaufwerken. – RAID-10 bietet gute Leistung für wahlfreie Schreibvorgänge und höchste Verfügbarkeit. – RAID-50 – Striping, aufgesetzt auf mehrere RAID-5-Sätze (verteilte Parität), mit einem oder zwei Ersatzlaufwerken. RAID-50 ist ausgewogen in Bezug auf Leistung (besonders für aufeinanderfolgende Schreibvorgänge), Verfügbarkeit und Kapazität. – RAID 5 – Ein RAID-5-Satz mit einem Ersatzlaufwerk. RAID-5 ähnelt RAID-50, mit mehr Kapazität (zwei zusätzliche Laufwerke), aber weniger Verfügbarkeit und Leistung. – RAID 6 – Von der Gesamtanzahl der im Array installierten Laufwerke werden zwei für die Parität verwendet und ein Laufwerk ist ein Ersatzlaufwerk. Die übrigen Laufwerke sind Datenlaufwerke.
--------------------------------------	---

Group Configuration (Gruppenkonfiguration)

Eingabe	Beschreibung
Group name (Gruppenname)	Eindeutiger Name (bis zu 63 Buchstaben, Ziffern oder Bindestriche). Dient zur Identifizierung der Gruppe. Das erste Zeichen muss ein Buchstabe oder eine Ziffer sein.

Eingabe	Beschreibung
Group IP address (IP-Adresse der Gruppe)	Netzwerkadresse für die Gruppe. Die Gruppen-IP-Adresse wird für die Gruppenverwaltung und die Erkennung von Ressourcen (d. h. Volumes) verwendet. Der Zugriff auf die Ressourcen erfolgt über eine physische Port-IP-Adresse.
Password for managing group membership	Kennwort, das zum Hinzufügen neuer Mitglieder zur Gruppe benötigt wird. Das Kennwort muss aus 3 bis 16 alphanumerischen Zeichen bestehen, wobei zwischen Groß- und Kleinschreibung unterschieden wird.
Password for the default group administration account	Kennwort, das das herstellerseitig festgelegte Kennwort (grpadmin) für das Standardkonto grpadmin außer Kraft setzt. Das Kennwort muss aus 3 bis 16 alphanumerischen Zeichen bestehen, wobei zwischen Groß- und Kleinschreibung unterschieden wird.
Microsoft service user name and password	CHAP-Benutzername und -Kennwort zum Aktivieren des Microsoft Servicezugangs (VSS oder VDS) zur Gruppe. Der Benutzername muss aus 3 bis 54 alphanumerischen Zeichen bestehen. Das Kennwort muss aus 12 bis 16 alphanumerischen Zeichen bestehen, wobei zwischen Groß- und Kleinschreibung unterschieden wird. Die auf dem Rechner ausgeführten Microsoft Services müssen Gruppenzugriff haben, damit VSS-Schnappschüsse in der Gruppe gemacht werden können oder damit die Gruppe VDS verwenden kann.


Initialisieren eines Arrays und Erstellen einer Gruppe


1. Starten Sie den **Remote-Installationsassistenten**.
2. Wählen Sie im **Begrüßungsdialog** die Option **Initialize a PS Series array** (Array der PS-Serie initialisieren), und klicken Sie auf **Next** (Weiter).
Im Dialogfeld **Select an Array to Initialize** (Wählen Sie das Array für die Initialisierung) wird eine Liste mit Arrays angezeigt.
3. Wählen Sie ein Array aus und klicken Sie auf **Details**, um ausführliche Informationen einschließlich der Seriennummer und MAC-Adresse anzuzeigen.
4. Wählen Sie das Array, das Sie initialisieren möchten, und klicken Sie auf **Next** (Weiter).
5. Geben Sie die Netzwerkkonfigurationsdaten für das Array in das Dialogfeld **Initialize an Array** (Array initialisieren) ein. Weitere Informationen finden Sie unter „Array-Konfiguration“.
6. Klicken Sie auf die Verknüpfung für einen Feldnamen, um Hilfe zu dem betreffenden Feld anzuzeigen. Wählen Sie außerdem die Option zum Erstellen einer neuen Gruppe. Klicken Sie anschließend auf **Next** (Weiter).
7. Geben Sie die Gruppenkonfiguration in das Dialogfeld **Creating a Group** (Gruppe erstellen) ein, und klicken Sie dann auf **Next** (Weiter). Weitere Informationen finden Sie unter „Gruppenkonfiguration“.
Nachdem das Array initialisiert wurde, erscheint eine Meldung.
8. Klicken Sie auf **OK**.
9. Wenn das Dialogfeld **Finish** (Fertig stellen) angezeigt wird, haben Sie folgende Möglichkeiten:
 - Klicken Sie auf **View Log** (Protokoll anzeigen), um eine Konfigurationsübersicht anzuzeigen.
 - Klicken Sie auf **Next** (Weiter), um ein weiteres Array zu initialisieren und zur Gruppe hinzuzufügen.
 - Klicken Sie auf **Finish** (Fertig stellen), um die Konfiguration abzuschließen und den Assistenten zu beenden.

Wenn Sie auf **Finish** (Fertig stellen) klicken, der Assistent:

- Er konfiguriert die Gruppen-IP-Adresse als iSCSI-Erkennungsadresse auf dem Computer.
- Speichert die CHAP-Zugangsdaten (Benutzername und Kennwort), mit denen Microsoft-Dienste (VDS oder VSS) auf die Gruppe im Computer zugreifen können.

- Erstellt einen entsprechenden VSS/VDS-Zugriffskontrolldatensatz und ein lokales CHAP-Benutzerkonto in der Gruppe.

 **ANMERKUNG:** Um den VSS/VDS Zugriffskontrolldatensatz anzuzeigen, klicken Sie auf **Group Configuration (Gruppenkonfiguration)** → **VSS/VDS**.

 **ANMERKUNG:** Um das lokale CHAP-Benutzerkonto in der Gruppe anzuzeigen, klicken Sie auf die Registerkarte **Group Configuration (Gruppenkonfiguration)** → **iSCSI**.

Nachdem Sie eine Gruppe erstellt haben, können Sie die Volumes über die grafische Benutzeroberfläche (GUI) des Group Manager oder die Befehlszeilenschnittstelle (CLI) verwalten.

Initialisieren eines Arrays und Erweitern einer Gruppe

Mit dem **Remote-Installationsassistenten** können Sie ein Array der Dell EqualLogic PS-Serie initialisieren und einer vorhandenen Gruppe hinzufügen. Zudem konfiguriert der Assistent die Gruppen-IP-Adresse als iSCSI-Erkennungsadresse auf dem Computer.

Bevor Sie ein Array initialisieren und eine Gruppe erweitern, stellen Sie sicher, dass Sie über folgende Informationen verfügen:

- Die in der Array-Konfigurations-Tabelle beschriebenen Array-Konfigurationsdetails.
- Gruppenname, IP-Adresse und Mitgliedschafts-Kennwort, wie in der Gruppenkonfigurations-Tabelle beschrieben.

So initialisieren Sie ein Array und erweitern eine vorhandene Gruppe:


1. Starten Sie den **Remote-Installationsassistenten**.
2. Wählen Sie im **Begrüßungsdialog** die Option **Initialize a PS Series array** (Array der PS-Serie initialisieren), und klicken Sie auf **Next** (Weiter).
3. Wählen Sie das Array, das Sie initialisieren möchten, und klicken Sie auf **Next** (Weiter).
4. Geben Sie die Netzwerkkonfigurationsdaten für das Array in das Dialogfeld **Initialize an Array** (Array initialisieren) ein.
Weitere Informationen finden Sie in der Array-Konfigurations-Tabelle.
5. Wählen Sie das Array aus, das einer bestehenden Gruppe hinzugefügt werden muss und klicken Sie auf **Next** (Weiter).
6. Geben Sie den Gruppennamen, die IP-Adresse und das Mitgliedschafts-Kennwort in das Dialogfeld **Joining a Group** (Einer Gruppe beitreten) ein, und klicken Sie auf **Next** (Weiter).
Wenn das initialisierte Array der Gruppe beigetreten ist, wird die folgende Meldung angezeigt:
Member Successfully Added to Group (Mitglied der Gruppe erfolgreich hinzugefügt) .
7. Klicken Sie auf **Yes** (Ja), um die Benutzeroberfläche des Group Managers zu öffnen und eine RAID-Richtlinie für das neue Mitglied zu konfigurieren, oder klicken Sie auf **No** (Nein), um den RAID-Level später zu konfigurieren.
8. Wenn das Dialogfeld **Finish** (Fertigstellen) angezeigt wird, haben Sie folgende Möglichkeiten:
 - Klicken Sie auf **View Log** (Protokoll anzeigen), um eine Konfigurationsübersicht anzuzeigen.
 - Klicken Sie auf **Next** (Weiter), um ein weiteres Array zu initialisieren und zur Gruppe hinzuzufügen.
 - Klicken Sie auf **Finish** (Fertig stellen), um die Konfiguration abzuschließen und den Assistenten zu beenden.

Wenn Sie den Assistenten beenden, konfiguriert er die Gruppen-IP-Adresse als iSCSI-Erkennungsadresse auf dem Computer, falls dies nicht bereits erfolgt ist.

Nachdem Sie das Array einer Gruppe hinzugefügt haben, können Sie die Volumes über die grafische Benutzeroberfläche (GUI) des Group Managers oder die Befehlszeilenschnittstelle (CLI) verwalten.

Computerzugriff auf eine Gruppe

Mit dem **Remote-Installationsassistenten** kann der Zugriff von Windows-Computern auf eine Dell EqualLogic PS-Gruppe aktiviert werden. Zudem können über den Assistenten vorhandene Gruppenzugriffsinformationen für einen Computer geändert werden (beispielsweise, falls sich die IP-Adresse der Gruppe geändert hat).

-  **ANMERKUNG:** Wenn Sie mit dem **Remote-Installationsassistenten** eine Gruppe erstellen, wird der Computerzugriff auf diese Gruppe automatisch konfiguriert. Dieser Abschnitt ist nur relevant, wenn Sie den **Remote-Installationsassistenten** auf einem anderen Computer gestartet haben, um die Gruppe anzulegen oder wenn die Gruppe über serielles Kabel anstatt über den **Remote-Installationsassistenten** angelegt wurde.


Wenn mit dem **Remote-Installationsassistenten** der Computerzugriff auf eine Gruppe aktiviert wird, führt der Assistent die folgenden Schritte durch:


1. Er konfiguriert die Gruppen-IP-Adresse als iSCSI-Zeil-Erkennungsadresse. Dies ermöglicht dem Computer, Volumes und Snapshots (iSCSI-Targets) in der Gruppe zu erkennen.
2. Speicherung der CHAP-Zugangsdaten (Benutzername und Kennwort), mit denen Microsoft-Dienste (VDS oder VSS) auf die Gruppe zugreifen können.

Aktivieren des Computerzugriffs auf eine Gruppe

So aktivieren Sie den Computerzugriff auf eine Gruppe oder ändern vorhandene Zugriffsinformationen für eine Gruppe:

1. Beschaffen Sie sich die folgenden Informationen:
 - Name und IP-Adresse der Gruppe.
 - Die in der Gruppe bereits konfigurierten CHAP-Zugangsdaten (Benutzername und Kennwort), mit denen Microsoft-Dienste (VSS oder VDS) auf die Gruppe zugreifen.


-  **ANMERKUNG:** Um den VSS/ VDS-Zugriffskontrolldatensatz über die Group Manager-GUI anzuzeigen, klicken Sie auf **Group Configuration** → **VSS/VDS**.

-  **ANMERKUNG:** Um das lokale CHAP-Benutzerkonto in der Gruppe anzuzeigen, klicken Sie auf **Group Configuration (Gruppenkonfiguration)** → **iSCSI**.

2. Starten Sie den **Remote-Installationsassistenten**.
3. Wählen Sie in Begrüßungsfenster des **Remote-Installationsassistenten** die Option **Configure this computer to access a PS Series SAN** (Zugriff auf ein SAN der PS-Serie für diesen Computer konfigurieren), und klicken Sie auf **Next** (Weiter).
4. Im Fenster **Configuring Group Access** (Gruppenzugriff konfigurieren) haben Sie folgende Möglichkeiten:
 - Klicken Sie auf **Add Group** (Gruppe hinzufügen), um eine Gruppe hinzuzufügen, auf die der Computer zugreifen kann.
 - Wählen Sie eine Gruppe aus, und klicken Sie auf **Modify Group** (Gruppe ändern), um einen vorhandenen Gruppenzugriff zu ändern.
5. Im Dialogfeld **Add or Modify Group Information** (Gruppeninformationen hinzufügen oder ändern):
 - a) Legen Sie den Gruppennamen und die IP-Adresse nach Bedarf fest, oder ändern Sie sie.
 - b) Wenn die Gruppe so konfiguriert ist, dass Microsoft-Dienste (VDS oder VSS) über CHAP auf sie zugreifen können, legen Sie die passenden CHAP-Zugangsdaten (Benutzername und Kennwort) für den VSS/VDS-Zugriffskontrolldatensatz und das in der Gruppe bereits konfigurierte lokale CHAP-Konto fest.
 - c) Wenn die Konfiguration der PS Series-Gruppe die Erkennung aufgrund der CHAP-Zugangsdaten einschränkt, klicken Sie auf das Kontrollkästchen neben der Option **Use CHAP credentials for iSCSI discovery** (CHAP-Anmeldeinformationen zur iSCSI-Erkennung verwenden).
 - d) Klicken Sie auf **Save** (Speichern).
6. Klicken Sie im Dialogfeld **Configuring Group Access** (Gruppenzugriff konfigurieren) auf **Finish** (Fertigstellen):

Konfiguration von MPIO (Multipath-E/A) zwischen einem Computer und einer Gruppe

So konfigurieren Sie MPIO (Multipath-E/A) zwischen einem Computer und einer Gruppe:


1. Starten Sie den **Remote-Installationsassistenten**.
 2. Wählen Sie im Begrüßungsdialogfeld die Option **Configure MPIO settings for this computer** (MPIO-Einstellungen für diesen Computer konfigurieren), und klicken Sie auf **Next** (Weiter).
Das Dialogfeld **Configure MPIO Settings** (MPIO-Einstellungen konfigurieren) wird angezeigt.
 3. In der Vorgabeeinstellung sind alle Hostadapter in allen Subnetzen, auf die die PS-Gruppe zugreifen kann, für Multipath-E/A (MPIO) konfiguriert. Um ein Subnetz auszuschließen, verschieben Sie es vom linken in das rechte Teilfenster. Geben Sie auch an, ob Sie den E/A-Lastausgleich über die Adapter hinweg aktivieren möchten.
-  **ANMERKUNG:** Um eine bestimmte IP-Adresse in einem Subnetz auszuschließen, bearbeiten Sie die Variablen in der Registry manuell. Weitere Informationen finden Sie in den *Versionshinweisen zu den Host Integration Tools*.
4. Klicken Sie auf **Finish** (Fertig stellen), um die Multipath-E/A-Konfiguration abzuschließen. Klicken Sie gegebenenfalls auf **Back** (Zurück), um Änderungen vorzunehmen.

Änderungen an der Liste der eingeschlossenen oder ausgeschlossenen Subnetze werden bei neuen Verbindungen sofort wirksam. Änderungen bei vorhandenen Verbindungen können einige Minuten dauern.

Konfiguration der Firewall für die Annahme von ICMP ECHO-Anfragen

Wenn Ihr System durch eine Windows-Firewall geschützt wird, müssen Sie die Firewall so konfigurieren, dass ICMP (Internet Control Message Protocol) ECHO-Anfragen für ICMPv4 zulässig sind.

So konfigurieren Sie die Firewall:

 **ANMERKUNG:** Bei anderen Windows-Betriebssystemversionen finden Sie die erforderlichen Informationen in der Dokumentation Ihres Betriebssystems. Dieses Verfahren kann nur bei Windows Server 2008 eingesetzt werden.

1. Klicken Sie auf **Start Verwaltung Windows Firewall with Advanced Security** (Windows-Firewall mit erweiterten Sicherheitsfunktionen).
2. Klicken Sie im **Hauptfensterbereich** auf **Inbound Rules** (Regel für Eingangsverkehr) und im **Aktionen-Fensterbereich** auf **New Rule** (Neue Regel).
3. Markieren Sie die Option **Custom** (Benutzerdefiniert), und klicken Sie auf **Next** (Weiter).
4. Markieren Sie **All programs** (Alle Programme) und klicken Sie auf **Next** (Weiter).
5. Wählen Sie im Drop-Down-Menü **Protocol Type** (Protokolltyp) die Option **ICMPv4** (ICMPv4).
6. Klicken Sie auf **Customize Internet Control Message Protocol (ICMP)** (ICMP-Einstellungen anpassen).
7. Markieren Sie die Option **Specific ICMP types** (Bestimmte ICMP-Typen) und anschließend die Option **Echo request** (Echo-Anforderung).
8. Klicken Sie auf **OK** und anschließend auf **Next** (Weiter).
9. Geben Sie die lokale und die Remote-IP-Adresse an. Markieren Sie für jeden Adresstyp (lokal oder Remote) eine der Optionen **Any IP Address** (Beliebige IP-Adresse) oder **These IP addresses** (Diese IP-Adressen). Wenn Sie die letzte Option markieren, müssen Sie zusätzlich eine oder mehrere IP-Adressen eingeben. Wenn Sie mit dem Festlegen der IP Adressen fertig sind, klicken Sie auf **Next** (Weiter).
10. Markieren Sie **Allow the connection** (Verbindung zulassen) und klicken Sie anschließend auf **Next** (Weiter). Suchen Sie die Optionen unter der Überschrift: **When does this rule apply?** (Wann wird diese Regel angewendet?)
11. Markieren Sie eine der folgenden Optionen:
 - Domain (Domäne)
 - Private (Privat)
 - Public (Öffentlich)
12. Klicken Sie auf **Next** (Weiter).
13. Geben Sie einen Namen und optional eine Beschreibung für diese Regel ein.
14. Klicken Sie auf **Finish** (Fertig stellen).

Installation des Microsoft iSCSI-Software-Initiators

Dieser Abschnitt gilt für solche Windows Server 2003-Betriebssysteme, bei denen nicht die Host Integration Tools zur Installation des Initiators verwendet werden. Im Lieferumfang der Host Integration Tools ist eine Version des Microsoft iSCSI-Software-Initiators enthalten. Informationen über die unterstützte iSCSI-Software-Initiator-Version finden Sie in den *Dell Cluster Configuration Support Matrices* (Dell Clusterkonfigurationssupport-Matrizen) unter dell.com/ha. Wenn die Initiatorversion der Host Integration Tools nicht in der Support-Matrix aufgeführt ist, laden Sie den Microsoft iSCSI-Software-Initiator herunter und installieren Sie ihn wie folgt:

1. Öffnen Sie einen Webbrowser und rufen Sie die Microsoft Download Center-Website unter microsoft.com/downloads auf.
2. Suchen Sie nach *iscsi initiator*.
3. Laden Sie die neueste unterstützte Version der Initiator-Software für das Betriebssystem und die zugehörige Dokumentation herunter.
4. Doppelklicken Sie die ausführbare Datei. Der Installationsassistent wird gestartet.
5. Im **Willkommensbildschirm** klicken Sie auf **Next** (Weiter).
6. Wählen Sie in den folgenden Bildschirmen die Optionen **Initiator Service**, **Software Initiator** und **Microsoft MPIO Multipathing Support for iSCSI**.
7. Klicken Sie auf **Next** (Weiter), um mit der Installation fortzufahren.
8. Lesen Sie den Lizenzvertrag, stimmen Sie den Vertragsbedingungen zu, und klicken Sie auf **Next** (Weiter), um die Software zu installieren.
9. Klicken Sie im letzten Bildschirm auf **b**, um die Installation abzuschließen.
10. Wählen Sie die Option **Do not restart now** (Jetzt nicht neu starten). Das System wird erst nach dem Ändern der Einstellungen in der Registry im Abschnitt „Ändern der Einstellungen in der Registry“ neu gestartet.

Ändern der Einstellungen in der Registry

Im Anschluss an die Installation des **Host Integration Tools**-Kits Version 3.1.1 oder höher wird das Dienstprogramm **EqISetupUtil.exe** im Verzeichnis **\EqualLogic\bin** installiert.

Um die oben angeführten Registry-Werte zu konfigurieren, führen Sie die folgenden Schritte für jeden Cluster-Host durch:


1. Um die oben angeführten Registry-Werte zu konfigurieren, führen Sie die folgenden Schritte für jeden Cluster-Host durch:
2. Wechseln Sie zum Verzeichnis **EqualLogic\bin**. Der Standard-Speicherort ist **c:\Programme\EqualLogic\bin**.
3. Für einen Host unter Windows Server 2003, führen Sie das Programm mit folgendem Parameter aus:
EqISetupUtil.exe -PRKey <PR-Schlüssel>
Falls der Host unter Windows Server 2008 läuft, führen Sie das Programm *EqISetupUtil.exe* ohne Parameter aus.
4. Starten Sie das System neu.

Sie können **EqISetupUtil.exe** ausführen, um die folgenden Registry-Werte zu konfigurieren:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk]
"TimeoutValue"=dword:0000003c [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\<Instance Number>
\Parameters
```

Zudem muss jeder Windows Server 2003 Cluster-Host die folgenden Registry-Werte aufweisen:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\msiscdsm
\PersistentReservation] "UsePersistentReservation"=dword:00000001
"PersistentReservationKey"=hex:<PR key>
```

 **ANMERKUNG:** Der <PR-Schlüssel> ist ein eindeutiger binärer 8-Byte-Wert. Er besteht aus einer 6-Byte-Komponente für den Cluster und einer 2-Byte-Komponente für den Knoten. Ein Beispiel: Bei einem Drei-Knoten-Cluster können Sie *Oxaabbccccbaa* als die clusterspezifische Komponente zuweisen.

- Knoten 1: *Oxaabbccccbaa0001*
- Knoten 2: *Oxaabbccccbaa0002*
- Knoten 3: *Oxaabbccccbaa0003*

Konfigurationsübersicht von gemeinsamen Speicherarrays

Dieser Abschnitt behandelt die folgenden Themen:

- Ausführen der grafischen Schnittstelle des Group Manager.
- Erstellen von Volumes.
- Erstellen von Zugriffskontrolldatensätzen.
- Verbinden von Host mit Volumes.
- Erweiterte Speichermerkmale.

Ausführen der grafischen Schnittstelle des Group Managers

Über die grafische Benutzeroberfläche (GUI) des Group Managers können Sie die Speicherarrays konfigurieren und weitere Aufgaben rund um die Gruppenadministration unter Verwendung einer der folgenden Methoden durchführen:

- Bedienung per Webbrowser über eine Standard-Internetverbindung mit HTTP (Port 80).
- Installieren der GUI auf einem lokalen System und Nutzung als eigenständige Anwendung.

So führen Sie die Group Manager-GUI über einen Webbrowser aus:

1. Geben Sie die Gruppen-IP-Adresse wie nachstehend in ein Webbrowserfenster ein: **http://gruppen_ip_adresse**
Wobei *gruppen_ip_adresse* die IP-Adresse ist, die Sie für die Gruppe konfiguriert haben.
Sobald die Verbindung zur Gruppe hergestellt ist, wird das Anmeldedialogfeld angezeigt.
2. Geben Sie einen Anmeldenamen für das Gruppenadministrationskonto ein.
Wenn keine anderen Konten eingerichtet wurden, können Sie die Zugangsdaten für das **grpadmin**-Standardkonto verwenden, das beim Anlegen der Gruppe eingerichtet wurde.

Group Manager-GUI-Komponenten

Die Group Manager-GUI ermöglicht die Verwaltung einer Reihe von Gruppenkomponenten, auf die Sie zugreifen können, indem Sie auf Objekte in der Baumverzeichnisstruktur im Teilfenster ganz links klicken und diese erweitern:

- **Group Configuration** (Gruppenkonfiguration) – Ändern der Gruppenkonfiguration und Einrichten von Konten, Ereignisbenachrichtigungen, Netzwerkdiensten, Authentifizierung und SNMP.
- **Group Monitoring** (Gruppenüberwachung) – Überwachen von iSCSI-Verbindungen zur Gruppe, Snapshot- und Duplikatplänen, Duplikatkonfigurationen und Aktivitäten für Volumes, Administrationsitzungen und Anmeldeverläufe sowie aktiven Operationen in Bezug auf Mitglieder und Volumes.
- **Events** (Ereignisse) – Anzeigen von Ereignissen in der Gruppe.
- **Storage Pools** (Speicherpools) – Erstellen und Verwalten von Pools in der Gruppe.
- **Members** (Gruppenmitglieder) – Überwachen und Verwalten von Gruppenmitgliedern einschließlich der Konfiguration von Netzwerkschnittstellen.
- **Volumes** – Überwachen und Verwalten von Volumes, Snapshots, Duplikaten und Zeitplänen.
- **Volume Collections** (Volume-Sammlungen) – Erstellen und Verwalten von Volume-Sammlungen. Mehrere zusammengehörige Speicherlaufwerke können in einer Kollektion zusammengefasst werden. So können

Snapshots oder Replikate aller Laufwerke in einem einzigen Arbeitsgang bzw. über einen einzigen zeitgesteuerten Befehl erstellt werden.

- **Replication Partners** (Replizierungspartner) – Überwachen und Verwalten von Replizierungspartnern.

Erstellen von Volumes

Um auf Speicher in einer PS-Gruppe zuzugreifen, müssen Sie einen oder mehrere Speicherpools erstellen und anschließend den Volumes Teile des/der Speicherpool(s) zuweisen. Jedem Volume sind eine Größe, ein Speicherpool und Zugriffssteuerungen zugeordnet. Volumes werden im Netzwerk als iSCSI-Targets wahrgenommen. Nur Hosts mit einem iSCSI-Initiator und den richtigen Anmeldedaten können auf ein Volume zugreifen. Die Gruppe generiert automatisch einen iSCSI-Targetnamen für jedes Volume. Dieser Name wird von den iSCSI-Initiatoren beim Zugriff auf das Volume verwendet.

So erstellen Sie ein Volume:

1. Klicken Sie auf **Volumes** und **Create volume** (Volume erstellen).

Das Dialogfeld **Create Volume – General Settings** (Volume erstellen – Allgemeine Einstellungen) wird angezeigt. Sie können Informationen in die folgenden Felder eingeben:

- **Volume name** (Name des Volumes) – Eindeutiger Name mit einer Länge von bis zu 64 alphanumerischen Zeichen (einschließlich Punkten, Bindestrichen und Doppelpunkten). Dient zur Identifizierung des Volumes bei Administrationsmaßnahmen. Der Name des Volumes erscheint am Ende des iSCSI-Targetnamens, der für das Volume erzeugt wird. Der Host greift nicht über den Namen des Volumes, sondern immer über den iSCSI-Target-Namen auf das Volume zu.
- **Description** (Beschreibung) – Die Beschreibung des Volumes ist optional.
- **Storage pool** (Speicherpool) – Alle Volume-Daten werden auf die Mitglieder des Pools beschränkt. Standardmäßig wird das Volume dem Standardpool zugewiesen. Wenn mehrere Pools vorhanden sind, können Sie das Volume einem anderen Pool zuweisen.

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

Das Dialogfeld **Create Volume – Space Reserve** (Volume erstellen – Speicherplatzreserve) wird angezeigt. Geben Sie Informationen in die folgenden Felder ein:

- **Volume size** (Größe des Volumes) – Dies ist die von den iSCSI-Initiatoren gemeldete Größe des Volumes. Die minimale Größe beträgt 15 MB. Außerdem werden Größenangaben für Volumes auf das nächste Vielfache von 15 aufgerundet.
- **Thin provisioned volume** (Volume mit schlanker Speicherzuweisung) – Markieren Sie dieses Kontrollkästchen, um die schlanke Speicherzuweisung für das Volume zu aktivieren. Wenn diese Option aktiv ist, werden im Teilfenster **Reported volume size** (Gemeldete Volumegröße) Schieberegler angezeigt. Mit diesen Reglern können Sie die folgenden Standardwerte für die schlanke Speicherzuweisung ändern:
 - * **Minimum volume reserve** (Mindest-Speicherkapazität) – Die minimale Speicherkapazität, die dem Volume zugewiesen wird. Im Verlauf der Nutzung wird dem Volume weitere Speicherkapazität zugewiesen, so dass sich dieser Wert erhöht. Der vorgegebene Wert beträgt 10 % der Größe des Volumes.
 - * **In-use space warning value** (Kapazitätsnutzungs-Warnung) – Wenn die genutzte Speicherkapazität diesen Wert (angegeben als Prozentsatz der Volumekapazität) erreicht, wird eine Warnmeldung ausgegeben. Sie weist auf die Nutzung der Volumekapazität hin, so dass Sie bei Bedarf die erforderlichen Anpassungen vornehmen können. Der Standardwert entspricht der Einstellung für alle Volumes der Gruppe.
 - * **Maximum in-use space value** – Wenn die genutzte Speicherkapazität diesen Wert (angegeben als Prozentsatz der Volumekapazität) erreicht, wird das Volume in den Offline-Status versetzt. Der Standardwert entspricht der Einstellung für alle Volumes der Gruppe.
- **Snapshot reserve** (Snapshot-Reserve) – Wenn Sie Snapshots des Volumes erstellen wollen, geben Sie den zu reservierenden Poolspeicherplatz für Snapshots an, und zwar als Prozentsatz der Volumereserve.

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


Das Dialogfeld **Create Volume – iSCSI Access Policy** (Volume erstellen – iSCSI-Zugriffsrichtlinie) wird angezeigt, in dem Sie einen Zugriffskontrolldatensatz für das Volume erstellen können.

Erstellen von Zugriffskontrolldatensätzen

Zugriffskontrolldatensätze schränken den Zugriff auf Volumes ein. Hosts müssen für den Zugriff entweder bekannte CHAP-Zugangsdaten (Benutzername und Kennwort) übermitteln oder eine bekannte IP-Adresse beziehungsweise einen bekannten iSCSI-Initiator-Namen aufweisen (alle drei Erkennungsmerkmale sind beliebig kombinierbar).

So erstellen Sie einen Zugriffskontrolldatensatz für ein Volume und seine Snapshots:

1. Klicken Sie im Dialogfeld **Create Volume – iSCSI Access Policy** (Volume erstellen – iSCSI-Zugriffsrichtlinie) auf **Restricted access** (Zugriffsbeschränkung) und auf eine oder mehrere der folgenden Optionen:
 - **Authenticate using CHAP user name** (Authentifizierung über CHAP-Benutzername) – Schränkt den Zugriff auf Hosts ein, die den angegebenen CHAP-Benutzernamen und das entsprechende Kennwort übermitteln. Der Benutzername muss einem lokalen CHAP-Konto oder einem Konto auf einem externen RADIUS-Server entsprechen.
 - **Limit access by IP address** (Zugriff auf bestimmte IP-Adresse einschränken) – Schränkt den Zugriff auf Hosts mit der angegebenen Initiator-IP-Adresse ein (zum Beispiel 12.16.22.123). Gegebenenfalls lassen sich Sternsymbole als Platzhalter verwenden (zum Beispiel 12.16.*.*). Ein Sternsymbol kann für ein gesamtes Oktett stehen, aber nicht für eine Stelle innerhalb eines Oktetts.
 - **Limit access to iSCSI initiator name** (Zugriff auf bestimmten iSCSI-Initiatornamen einschränken) – Schränkt den Zugriff auf Hosts mit dem angegebenen iSCSI-Initiatornamen ein.

 **ANMERKUNG:** Wenn Sie den Zugriff auf bestimmte IP-Adressen oder iSCSI-Initiatornamen einschränken, müssen Sie für jede von einem autorisierten Host übermittelte IP-Adresse bzw. für jeden von einem autorisierten Host übermittelten iSCSI-Initiatornamen einen Zugriffskontrolldatensatz anlegen. Weitere Datensätze können hinzugefügt werden. Wenn Sie zu diesem Zeitpunkt keinen Zugriffskontrolldatensatz anlegen möchten, wählen Sie **No access** (Kein Zugriff). Bevor Sie einen Zugriffskontrolldatensatz angelegt haben, kann kein Host auf das Volume zugreifen.

2. Markieren Sie das Kontrollkästchen **Enable shared access to the iSCSI target from multiple initiators** (Gemeinsamen Zugriff auf das iSCSI-Ziel durch mehrere Initiatoren freigegeben).
3. Nachdem Sie die Zugriffsinformationen angegeben haben, klicken Sie auf **Next** (Weiter), um das Dialogfeld **Create Volume - Summary** (Volume erstellen – Übersicht) anzuzeigen.
4. Klicken Sie auf **Finish** (Fertig stellen), um das Volume zu erstellen.
5. Vergewissern Sie sich, dass das Volume für den gemeinsamen Zugriff durch mehrere Initiatoren freigegeben ist:
 - Klicken Sie mit der rechten Maustaste auf das zuvor erstellte Volume, und wählen Sie die Option **Modify Volume Settings** (Volume-Einstellungen ändern).
 - Wählen Sie die Registerkarte **Advanced** (Erweitert).
 - Stellen Sie sicher, dass das Kontrollkästchen **Enable shared access to the iSCSI target from multiple initiators** (Gemeinsamen Zugriff auf das iSCSI-Ziel durch mehrere Initiatoren freigegeben) markiert ist.

Verbinden von Host mit Volumes

Dieser Abschnitt erläutert den Aufbau von Verbindungen zu SANs der PS-Series. Er erklärt das Hinzufügen des Ziel-Portals und das Einrichten der Verbindungen von den Volumes zum Host. Fügen Sie über den Microsoft iSCSI-Initiatordienst ein Ziel-Portal hinzu. Falls nicht vorhanden, verwenden Sie die IP-Adresse der PS-Gruppe. Dies ermöglicht dem Host, die verfügbaren Ziels zu erkennen. Dieser Vorgang wird im Bereich **Discovery** (Erkennung) des Initiator-Eigenschaftenfensters durchgeführt.

Ein Volume wird im Netzwerk als iSCSI-Ziel wahrgenommen, auf das nur ein auf einem Host installierter iSCSI-Initiator zugreifen kann.

So melden Sie sich bei einem Volume oder Ziel an:


1. Wählen Sie unter **Targets** (Ziele) das Volume, zu dem eine Verbindung hergestellt werden soll.
2. Klicken Sie auf **Log On** (Anmelden).
3. Markieren Sie das Kontrollkästchen **Enable multi-path** (Multipath aktivieren), wenn Sie sich beim Ziel anmelden.
4. Markieren Sie das Kontrollkästchen **Automatically restore this connection when the system boots** (Diese Verbindung beim Systemstart automatisch wiederherstellen), um die Verbindung dauerhaft einzurichten.
5. Klicken Sie auf **Advanced** (Erweitert).
 - a) Wählen Sie im Dropdownfeld **Local Adapter** (Lokaler Adapter) die Option **Microsoft iSCSI Initiator**.
 - b) Wählen Sie im Dropdownfeld **Source IP** (Quell-IP) die IP-Adresse des zugehörigen iSCSI-NICs.
 - c) Wählen Sie im Dropdownfeld **Target Portal** (Ziel-Portal) die IP-Adresse der PS-Gruppe.
 - d) Wenn CHAP als Erkennungsmethode verwendet wird, fügen Sie den Ziel-Geheimschlüssel hinzu, um die Verbindung fertigzustellen.
6. Wiederholen Sie Schritt 2 bis Schritt 5 und verwenden Sie dabei die IP-Adresse der anderen von Ihnen ausgewählten Schnittstelle in Schritt 5b.

Nachdem einmal eine Verbindung hergestellt wurde, baut der MPIO-DSM-Verbindungsmanager alle benötigten Verbindungen auf und ersetzt vorhandene Verbindungen bei Bedarf. So würden beispielsweise bei zwei NICs und drei Arrays sechs Verbindungen pro Volume aufgebaut werden. Nachdem die Verbindung erstmals hergestellt wurde, warten Sie ein oder zwei Minuten, damit der DSM mit der Arraygruppe kommunizieren und die erforderlichen Informationen zum Aufbau mehrerer Verbindungen abrufen kann.


Wenn der Initiator am iSCSI-Ziel angemeldet ist, erkennt der Host das Volume als normalen Datenträger, der sich mit üblichen Betriebssystemfunktionen formatieren lässt.


Erweiterte Speichermerkmale

Zu Datensicherungs- oder Fehlerbehebungs Zwecken können Sie Volume-Snapshots erstellen, Volumes klonen oder sie in einer anderen Gruppe replizieren. Snapshots oder Duplikate aller Volumes (Snapshot- oder Duplikatsammlungen) können in einem einzigen Arbeitsgang erstellt werden. Mit schlanker Speicherzuweisung (Thin Provisioning) können Sie die Speicherressourcen effizient nutzen.

 **ANMERKUNG:** Weitere Informationen zur Nutzung von Snapshots, Replikation, Klonen, Volume-Sammlungen, und schlanker Speicherzuweisung finden Sie im *Gruppenverwaltungshandbuch* unter equallogic.com.

In diesem Abschnitt werden die Funktionen der Group Manager-GUI beschrieben. Sie können mit ASM auch Daten in der Windows-Clusterumgebung sichern und wiederherstellen. ASM verwendet Microsoft VSS, um ein Framework zum Erstellen schneller, koordinierter Kopien von Anwendungsdatenbank-Volumes in der PS-Gruppe bereitzustellen. So wird sichergestellt, dass die gesicherten Daten einfach wiederherzustellen und für eine Recovery zu verwenden sind.

 **VORSICHT:** Wenn Sie einen Snapshot, Klon oder ein Duplikat eines Volumes unter Verwendung der Group Manager-GUI mounten möchten, mounten Sie es an einem eigenständigen Knoten oder einem Clusterknoten, der einem anderen Cluster angehört. Ein Snapshot, Klon oder Duplikat hat die gleiche Laufwerkssignatur wie der Originallaufwerk und darf deshalb nicht an einem Knoten gemountet werden, der dem gleichen Cluster wie dieser angehört. Wenn Windows zwei Laufwerke mit der gleichen Laufwerkssignatur entdeckt, ändert es die Signatur eines der Laufwerke. In den meisten Fällen versucht Windows, die Laufwerkssignatur des Snapshots, Klons oder Duplikats zu ändern. Wenn kein Schreibzugriff für das Laufwerk besteht, kann Windows die Signatur nicht ändern, und das Volume wird nicht gemountet. Besteht hingegen Schreibzugriff, so ändert Windows die Laufwerkssignatur. Das hat zur Folge, dass eine spätere Wiederherstellung des Laufwerks scheitert, da die Signaturen nicht identisch sind. In seltenen Fällen kann es zudem vorkommen, dass Windows die Laufwerkssignatur des ursprünglichen Laufwerks ändert, weil es den Snapshot, Klon bzw. das Duplikat irrtümlich als Clusterlaufwerk identifiziert. Dies kann dazu führen, dass Daten verloren gehen oder kein Zugriff auf den Snapshot, Klon bzw. das Duplikat möglich ist.

 **ANMERKUNG:** Weitere Informationen zur Verwendung von ASM im Cluster finden Sie im *Host Integration Tools EqualLogic Auto-Snapshot Manager/Microsoft Edition Benutzerhandbuch* unter equallogic.com.



ANMERKUNG: Sie können ASM zum Mounten eines Snapshots, Klons oder Duplikats an dem gleichen Knoten oder an einem anderen Knoten im gleichen Cluster verwenden. VSS ändert die Laufwerkssignatur des Snapshots, Klons oder Duplikats vor dem Mounten.

Snapshots

Ein Snapshot ist eine Kopie der Daten auf einem Volume zu einem bestimmten Zeitpunkt und dient zum Schutz vor Fehlern, Viren oder Datenbankschäden. Der Zugriff auf das Volume wird durch das Erstellen eines Snapshots nicht unterbrochen. Snapshots werden im Netzwerk als iSCSI-Ziele wahrgenommen. Sie können in den Online-Status versetzt werden, sodass Hosts mit iSCSI-Initiatoren darauf zugreifen können. Um Daten auf einem Volume wiederzugewinnen, kann das Volume entweder von einem Snapshot wiederhergestellt werden, oder es wird durch Klonen eines Snapshots ein neues Volume erstellt.

Erstellen von Snapshots

So erstellen Sie einen Snapshot zum aktuellen Zeitpunkt:

1. Klicken Sie auf **Volumes** → **volume_name** → **Create snapshot (Snapshot erstellen)**.
Das Dialogfeld **Create Snapshot (Snapshot erstellen)** wird angezeigt.
2. In diesem Dialogfeld können folgende Informationen angegeben werden:
 - Optionale Beschreibung des Snapshots.
 - Gewünschter Status des Snapshots (offline [Standard] oder online)
 - Gewünschte Zugriffsrechte für den Snapshot (Lese- und Schreibzugriff [Standard] oder nur Lesezugriff).
3. Klicken Sie auf **OK**, um den Snapshot zu erstellen. Der Snapshot wird im Teilfenster ganz links unter dem Namen des Volumes angezeigt und ist an Datum und Uhrzeit seiner Erstellung zu erkennen.

Wiederherstellen von Snapshots

So stellen Sie ein Volume mit einem Snapshot wieder her:

1. Versetzen Sie die Clusterressourcengruppe, der das Volume angehört, mit der Cluster-Verwaltung oder dem Failover Cluster-Management in den Offline-Status.
2. Führen Sie über die Gruppenadministration folgende Aufgaben durch:
 - Versetzen Sie das Volume und den Snapshot in den Offline-Status.
 - Wählen Sie das Volume aus, führen Sie eine Wiederherstellung durch, und wählen Sie den Snapshot aus, von dem das Volume wiederhergestellt werden soll.
 - Versetzen Sie das Volume in den Online-Status.
3. Melden Sie mit dem Microsoft iSCSI-Initiatordienst alle Clusterknoten wieder beim Volume an.
4. Versetzen Sie die Clusterressourcengruppe mit der Cluster-Verwaltung oder dem Failover Cluster-Management in den Online-Status.



ANMERKUNG: Verwenden Sie nicht die Group Manager-GUI zum Mounten des Snapshots eines Clusterlaufwerks an einem Knoten im gleichen Cluster.

Volumes

Beim Klonen eines Volumes wird ein neues Volume mit einem neuen Namen erstellt, das die gleiche Größe, den gleichen Inhalt und die gleichen Einstellungen für schlanke Speicherzuweisung aufweist wie das ursprüngliche Volume. Das neue Volume befindet sich im gleichen Speicherpool wie das ursprüngliche Volume und ist sofort verfügbar. Das ursprüngliche Volume wird durch das Klonen nicht verändert und besteht nach Abschluss des Vorgangs fort. Ein geklontes Volume belegt in dem Speicherpool, in dem sich das ursprüngliche Volume befindet, 100 % von dessen

Laufwerkskapazität. Wenn Sie Snapshots und Duplikate des neuen Volumes erstellen möchten, benötigen Sie zusätzlichen Speicherplatz im Pool.

Klonen von Volumes

So klonen Sie ein Volume:

1. Klicken Sie auf **Volumes** → **volume_name** → **Clone volume (Volume klonen)**.
Das Dialogfeld **Clone Volume** – General Settings (Volume klonen – Allgemeine Einstellungen) wird angezeigt.
2. Geben Sie in den nachstehenden Feldern Informationen zum neuen Volume an:
 - **Volume name** (Name des Volumes) – Eindeutiger Name mit einer Länge von bis zu 64 alphanumerischen Zeichen (einschließlich Punkten, Bindestrichen und Doppelpunkten). Dient zur Identifizierung des Volumes bei Administrationsmaßnahmen. Der Name des Volumes erscheint am Ende des iSCSI-Zielnamens, der für das Volume erzeugt wird. Der Host greift nicht über den Namen des Volumes, sondern immer über den iSCSI-Ziel-Namen auf das Volume zu.
 - **Description** (Beschreibung) – Optionale Beschreibung des Volumes.
3. Klicken Sie auf **Next** (Weiter).
Das Dialogfeld **Clone Volume** – **Space Reserve** (Volume klonen – Speicherplatzreserve) wird angezeigt.
4. Im **Snapshot-Reserve**-Feld können Sie die Kapazität (als Prozentsatz der Volume-Reserve) angeben, die für Snapshots des neuen Volumes reserviert werden soll. Der Standardwert entspricht der Einstellung für alle Volumes der Gruppe.
5. Klicken Sie auf **Next** (Weiter).
Das Dialogfeld **Clone Volume** – **iSCSI Access Policy** (Volume klonen – iSCSI-Zugriffsrichtlinie) wird angezeigt. Hier können Sie einen Zugriffskontrolldatensatz erstellen, der den Hostzugriff auf das neue Volume und seine Snapshots eingeschränkt.
6. Wählen Sie die Methode der Zugriffsbeschränkung, und geben Sie die erforderlichen Informationen ein.
7. Klicken Sie auf **Next** (Weiter).
Das Dialogfeld **Clone Volume** – **Summary** (Volume klonen – Übersicht), das die Konfiguration des Volumes zusammenfasst, wird angezeigt.
8. Wenn die Einstellungen korrekt sind, klicken Sie auf **Finish** (Fertig stellen), um das Volume zu klonen. Klicken Sie gegebenenfalls auf **Back** (Zurück), um Änderungen vorzunehmen.

Wiederherstellen von Volumes

So stellen Sie ein Volume über einen Klon wieder her:

1. Versetzen Sie die Clusterressourcengruppe, der das Volume angehört, mit der Cluster-Verwaltung oder dem Failover Cluster-Management in den Offline-Status.
2. Führen Sie über die grafische Benutzeroberfläche des Microsoft iSCSI-Initiatordiensts an jedem Clusterknoten folgenden Aufgaben durch:
 - Melden Sie das Volume ab.
 - Löschen Sie das Volume aus der Liste der dauerhaften Targets.
3. Führen Sie über die Gruppenadministration folgende Aufgaben durch:
 - Versetzen Sie das Volume in den Offline-Status.
 - Stellen Sie sicher, dass der Klon Lese- und Schreibzugriff hat und in seiner Zugriffssteuerungsliste alle Clusterknoten verzeichnet sind.
 - Versetzen Sie den Klon in den Online-Status.
4. Melden Sie mit dem Microsoft iSCSI-Initiatordienst alle Clusterknoten wieder beim Klon an.
5. Versetzen Sie die Clusterressourcengruppe mit der Cluster-Verwaltung oder dem Failover Cluster-Management in den Online-Status.



ANMERKUNG: Verwenden Sie nicht die Group Manager GUI zum Mounten des Klons eines Clusterlaufwerks an einem Knoten im gleichen Cluster.

Replikation

Die Replizierungstechnologie ermöglicht es, die Daten eines Volumes zwischen Gruppen hin- und herzukopieren, die im gleichen Gebäude oder einer gewissen Entfernung voneinander untergebracht sind. Replikation schützt die Daten vor Ausfällen – vom Defekt eines Volumes bis zur Lahmlegung eines kompletten Standorts, und Verfügbarkeit und Leistung bleiben uneingeschränkt erhalten. Ein Duplikat bildet ähnlich wie ein Snapshot die Daten eines Volumes zu einem bestimmten Zeitpunkt ab. There must be adequate network bandwidth and full IP routing between the groups.

Das Volume befindet sich in der Primärgruppe. Die Duplikate des Volumes befinden sich in dem Kapazitätsbereich der Sekundärgruppe, der an die Primärgruppe abgestellt wurde. Gegenseitige Authentifizierung gewährleistet die Sicherheit beim Datenaustausch zwischen den Gruppen. Wenn erstmals ein Duplikat eines Volumes erstellt wird, werden die Daten des Volumes aus der Primärgruppe über das Netzwerk vollständig in die Sekundärgruppe übertragen. Bei späteren Duplikaten werden nur die Daten zur Sekundärgruppe übertragen, die seit dem letzten Duplikat geändert wurden. Wenn bei der ersten Replikation eine große Menge an Volumedaten übertragen werden muss, kann dies manuell geschehen.

Dabei werden die Daten vom Volume auf ein externes Medium kopiert und von diesem auf den Duplikatsatz in der Sekundärgruppe übertragen. Nach Abschluss der ersten Datenübertragung wird die Replikation wie gewohnt über das Netzwerk fortgeführt.



ANMERKUNG: Verwenden Sie das Dienstprogramm für manuellen Transfer, um die Daten remote zu kopieren, wenn Sie eine Replikation einrichten.

Replikation von Volumes

So replizieren Sie ein Volume von einer Gruppe zu einer anderen:

1. Konfigurieren Sie zwei Gruppen als Replikationspartner:
 - a) Melden Sie sich bei jeder Gruppe an.
 - b) Konfigurieren Sie die jeweils andere Gruppe als Replikationspartner, und stellen Sie Speicherkapazität für den Partner ab.
 - c) Zur gegenseitigen Authentifizierung geben Sie in jeder Gruppe den Namen, die Gruppen-IP-Adresse und das Kennwort der jeweiligen Partnergruppe.
2. Konfigurieren Sie die Replikation für das Volume:
 - a) Melden Sie sich bei der Primärgruppe an, und konfigurieren Sie die Replikation für das Volume.
 - b) Geben Sie für jedes Volume die folgenden Informationen an:
 - * Die Partnergruppe (Sekundärgruppe), in der die Duplikate gespeichert werden.
 - * Die Reservekapazität für Duplikate in der Sekundärgruppe.
 - * Die Reservekapazität für lokale Replikation in der Primärgruppe, und ob die Option „borrow free space“ (Freie Kapazität ausleihen) aktiviert werden soll.
 - * Ob die erste Replikation über das Netzwerk oder manuell durchgeführt wird.
 - * Ob der Failback-Snapshot beibehalten werden soll. Wenn dies der Fall ist, muss mehr Kapazität für die lokale Replikation reserviert werden.
3. Beginnen Sie mit dem Replikationsvorgang:

Erstellen Sie entweder ein Replikat, oder richten Sie einen Zeitplan zur regelmäßigen Erstellung von Replikaten ein.
4. Vergewissern Sie sich, dass die Replikation vollständig durchgeführt wird:

Überprüfen Sie regelmäßig die Speicherplatzbelegung durch die Replikation, und nehmen Sie bei Bedarf Änderungen vor.

Sie können Volumedaten von Duplikaten in der Sekundärgruppe wiederherstellen, indem Sie durch Klonen eines einzelnen Duplikats ein neues Volume erstellen. Weiterhin ist es möglich, mit der Failback-Funktion vorübergehend ein Volume in der Sekundärgruppe zu hosten – beispielsweise zu Datensicherungszwecken, oder wenn die Primärgruppe wegen eines Ausfalls oder aufgrund von Wartungsmaßnahmen nicht verfügbar ist. Später kann in bestimmten Fällen ein Failback zur Primärgruppe durchgeführt und die ursprüngliche Replikationskonfiguration wiederhergestellt werden. Dabei werden nur die Änderungen an den Volumedaten repliziert, die vorgenommen wurden, während das Volume in der Sekundärgruppe gehostet wurde. Die Failback-Funktion kann auch genutzt werden, um die Rollen der Partner permanent zu vertauschen.

Volumesammlungen



ANMERKUNG: Verwenden Sie nicht die Group Manager-GUI zum Mounten des Klons eines Clusterlaufwerks an einem Knoten im gleichen Cluster.

Eine Volume-Sammlung besteht aus einem oder mehreren Volumes aus beliebigen Pools. Sie vereinfacht das Erstellen von Snapshots und Duplikaten. Volume-Sammlungen sind praktisch, wenn mehrere zusammengehörige Volumes eingesetzt werden. Sie ermöglichen es, in einem einzigen Arbeitsgang Snapshots oder Duplikate aller Volumes zu erstellen (Snapshot- bzw. Duplikatsammlung).

Erstellen von Volume-Sammlungen

So erstellen Sie eine Volume-Sammlung:

1. Click **Volume Collections** → **Create volume collection (Volume-Sammlungen > Volume-Sammlung erstellen)**. Das Fenster **Create Volume Collection - General** (Volume-Sammlung erstellen – Allgemein) wird angezeigt.
2. Geben Sie einen Namen und optional eine Beschreibung für die Sammlung ein.
3. Klicken Sie auf **Next** (Weiter). Das Fenster **Create Volume Collection - Components** (Volume-Sammlung erstellen – Komponenten) wird angezeigt.
4. Wählen Sie bis zu acht Volumes für die Sammlung aus. Eine Volume-Sammlung kann Volumes aus verschiedenen Pools enthalten.
5. Klicken Sie auf **Next** (Weiter). Das Fenster **Create Volume Collection - Summary** (Volume-Sammlung erstellen – Übersicht) wird angezeigt.
6. Wenn die Einstellungen korrekt sind, klicken Sie auf **Finish** (Fertig stellen), um die Volume-Sammlung zu erstellen.
7. Um Änderungen vorzunehmen, klicken Sie auf **Back** (Zurück).
Nach der Erstellung einer Volume-Sammlung können Sie Snapshots oder Replikate erstellen.

Thin Provisioning (Schlanke Speicherzuweisung)

Mit der Thin-Provisioning-Technologie (schlanke Speicherzuweisung) kann Speicher effizienter bereit gestellt werden. Dabei werden die Anforderungen von Anwendungen und Benutzern weiter erfüllt. Einem Volume mit schlanker Speicherzuweisung wird anfangs nur ein Teil der Volumekapazität zugewiesen. Wenn Daten auf das Volume geschrieben werden, wird ihm automatisch weitere Volumekapazität aus dem freien Pool zugewiesen (sofern verfügbar), und die Reservekapazität des Volumes wird bis zu einem benutzerdefinierten Limit erhöht. Wenn keine Speicherkapazität verfügbar ist, schlägt die automatische Erweiterung fehl. Wenn der genutzte Speicherplatz, typischerweise die Volumegröße, die gesamte Reservekapazität des Volumes belegt, wird das Volume in den Offline-Status versetzt. Der Einsatz von Thin Provisioning ist in einer IT-Umgebung nicht in jedem Fall geeignet oder sinnvoll. Die Methode ist am effizientesten, wenn bekannt und vorhersagbar ist, wie schnell ein Volume mit der Zeit wachsen wird, und wenn die Benutzer nicht darauf angewiesen sind, jederzeit sofort und garantiert auf die gesamte Volumekapazität zugreifen zu können. Bei zunehmender Beanspruchung von Speicherplatz werden regelmäßige Ereignismeldungen ausgegeben. So kann der Administrator bei Bedarf Anpassungen vornehmen. Volumes mit schlanker

Speicherzuweisung ermöglichen es, Speicherressourcen effizient zu nutzen, ohne schwierige Kapazitätsanpassungen am Host vornehmen zu müssen.

Installation und Konfiguration eines Failover-Clusters

Nachdem Sie das private und öffentliche Netzwerk eingerichtet und die freigegebenen Laufwerke in den Speicherarrays den Clusterknoten zugewiesen haben, können Sie die Betriebssystem-Dienste auf Ihrem Failover Cluster konfigurieren. Die Vorgehensweise bei der Konfiguration der Failover Cluster hängt von der verwendeten Windows Server-Betriebssystemversion ab.

Weitere Informationen zum Bereitstellen eines Clusters mit Windows Server 2003 finden Sie im *Dell Failover Clusters with Microsoft Windows Server 2003 Installation and Troubleshooting Guide* (Dell Failover Clusters unter Microsoft Windows Server 2003 Installations- und Fehlerbehebungshandbuch) unter support.dell.com/manuals.

Weitere Informationen zum Bereitstellen eines Clusters mit Windows Server 2008 finden Sie im *Dell Failover Clusters with Microsoft Windows Server 2008 Installation and Troubleshooting Guide* (Dell Failover Clusters unter Microsoft Windows Server 2008 Installations- und Fehlerbehebungshandbuch) unter support.dell.com/manuals.

Fehlerbehebung

Im folgenden Abschnitt werden allgemeine Clusterprobleme sowie mögliche Ursachen und Lösungen für diese Probleme beschrieben.

Problem	Mögliche Ursache	Maßnahme
Die Knoten können nicht auf das Speichersystem zugreifen oder die Clustersoftware funktioniert nicht mit dem Speichersystem.	Das Speichersystem ist nicht korrekt mit den Knoten verkabelt oder die Verkabelung zwischen den Speichersystemen ist fehlerhaft.	Überprüfen Sie, ob die Kabel zwischen dem Knoten und dem Speichersystem korrekt angeschlossen sind. Weitere Informationen finden Sie unter „Verkabeln des Clusters für öffentliches und privates Netzwerk“.
	Eines der Kabel ist fehlerhaft.	Ersetzen Sie das fehlerhafte Kabel.
Einer der Knoten benötigt längere Zeit, um dem Cluster beizutreten. oder Einer der Knoten kann dem Cluster nicht beitreten.	Die Volumes sind den Hosts nicht zugeordnet.	Überprüfen Sie, ob alle Volumes den Hosts zugeordnet sind.
	Das Knoten-zu-Knoten-Netzwerk ist aufgrund eines Kabel- oder Hardwarefehlers ausgefallen.	<ul style="list-style-type: none"> Überprüfen Sie die Netzwerkverkabelung und stellen Sie sicher, dass das Kontrollkästchen für den Multi-Initiator ausgewählt ist. Stellen Sie sicher, dass die Verbindung zwischen den Knoten und das öffentliche Netzwerk an den richtigen NICs angeschlossen sind.
	Längere Verzögerungen bei der Kommunikation zwischen den Knoten sind unter Umständen normal.	<ul style="list-style-type: none"> Stellen Sie sicher, dass die Knoten miteinander kommunizieren können. Führen Sie hierzu den Befehl ping von einem zum anderen Knoten aus. Versuchen Sie das Ausführen des Befehls ping sowohl mit dem Hostnamen als auch mit der IP-Adresse.
	Möglicherweise wurde für einen oder mehrere Knoten die Internetverbindungs-Firewall aktiviert, die nun die RPC (Remote Procedure Call)-Kommunikation zwischen den Knoten blockiert.	<ul style="list-style-type: none"> Konfigurieren Sie die Internetverbindungs-Firewall so, dass die vom Microsoft Cluster Service (MSCS) und den Clusteranwendungen/-diensten benötigte Datenkommunikation zugelassen wird. Weitere Informationen finden Sie unter

Problem	Mögliche Ursache	Maßnahme
Zu einem Cluster lässt sich mit der Clusterverwaltung keine Verbindung aufnehmen.	<ul style="list-style-type: none"> • Der Clusterdienst wurde nicht gestartet. • Im System wurde kein Cluster gebildet. • Das System wurde gerade gebootet und die Dienste sind noch nicht vollständig gestartet. 	<p>support.microsoft.com im Artikel KB883398.</p> <ul style="list-style-type: none"> • Überprüfen Sie, ob der Clusterdienst aktiv ist und ob ein Cluster gebildet wurde. • Suchen Sie in der Ereignisanzeige nach den folgenden Ereignisprotokollen des Clusterdienstes: <pre>Microsoft Cluster Service successfully formed a cluster on this node.</pre> <p>oder</p> <pre>Microsoft Cluster Service successfully joined the cluster.</pre> • Wenn diese Ereignisse nicht in der Ereignisanzeige angezeigt werden, schlagen Sie im <i>Microsoft Cluster Service Administrator's Guide</i> (Administratorhandbuch für den Microsoft-Clusterdienst) nach. Dort erfahren Sie, wie Sie einen Cluster im System einrichten und den Clusterdienst starten.
Sie werden während der MSCS-Installation zur Konfiguration eines Netzwerks anstatt zweier Netzwerke aufgefordert.	<p>Der Netzwerkname des Clusters kann im Netzwerk nicht angesprochen werden, weil die Internetverbindungs-Firewall für einen oder mehrere Knoten aktiviert wurde.</p>	<p>Konfigurieren Sie die Internetverbindungs-Firewall so, dass die von MSCS und den Clusteranwendungen/-diensten benötigte Datenkommunikation zugelassen wird. Weitere Informationen finden Sie unter support.microsoft.com im Artikel KB883398.</p>
	<p>Die TCP/IP-Konfiguration ist nicht korrekt.</p> <p>Das private (Punkt-zu-Punkt-) Netzwerk wurde unterbrochen.</p>	<p>Dem Knoten-zu-Knoten-Netzwerk und dem öffentlichen Netzwerk müssen feste IP-Adressen in unterschiedlichen Subnetzen zugewiesen werden.</p> <p>Überprüfen Sie, ob beide Systeme eingeschaltet sind, damit die Netzwerkadapter im privaten Netzwerk verfügbar sind.</p>

Problem	Mögliche Ursache	Maßnahme
Wenn Sie Microsoft Windows NT 4.0 für die Verwaltung eines Windows Server 2003-Clusters per Remote-Zugriff verwenden, erhalten Sie Fehlermeldungen.	Dies ist ein bekanntes Problem. Bestimmte Ressourcen von Windows Server 2003 stehen unter Windows NT 4.0 nicht zur Verfügung.	Dell empfiehlt nachdrücklich, für die Remote-Verwaltung eines Clusters unter Windows Server 2003 entweder Windows XP Professional oder Windows Server 2003 zu verwenden.
Ein Knoten kann dem Cluster nicht hinzugefügt werden.	Der neue Knoten kann nicht auf die gemeinsamen Laufwerke zugreifen. Die gemeinsamen Laufwerke werden an den Knoten des Clusters vom Betriebssystem anders benannt.	Überprüfen Sie mithilfe der Windows Disk Administration (Laufwerksverwaltung von Windows), ob der neue Knoten die Cluster-Laufwerke auflisten kann. Überprüfen Sie folgende Punkte, falls die Laufwerke in der Laufwerkesverwaltung nicht angezeigt werden: <ol style="list-style-type: none"> 1. Überprüfen Sie alle Kabelverbindungen. 2. Überprüfen Sie die Zuweisungen für die Volumes. 3. Wählen Sie Advanced → Minimum (Erweitert, Minimal).
	Möglicherweise wurde für einen oder mehrere Knoten die Internetverbindungs-Firewall aktiviert, die nun die RPC-Kommunikation zwischen den Knoten blockiert.	Konfigurieren Sie die Internetverbindungs-Firewall so, dass die von MSCS und den Clusteranwendungen/-diensten benötigte Datenkommunikation zugelassen wird. Weitere Informationen finden Sie unter support.microsoft.com im Artikel KB883398.
Microsoft iSCSI-Initiator kann nicht verwendet werden, um die Verbindung mit PS Series Array(s) vom zweiten Knoten aus herzustellen und die folgende Fehlermeldung wird angezeigt: Authorization Failure (Genehmigungsfehler).	Das Kontrollkästchen Enable shared access to the iSCSI target from multiple initiators (Gemeinsamen Zugriff auf das iSCSI-Target von mehreren Initiatoren aktivieren) ist nicht aktiviert.	<ol style="list-style-type: none"> 1. Klicken Sie mit der rechten Maustaste unter „Group Manager GUI“ (Group Manager-Benutzeroberfläche) auf das Volume, bei dem Verbindungsprobleme auftreten. 2. Wählen Sie Modify Volume Settings (Volume-Einstellungen ändern) aus. 3. Klicken Sie anschließend auf die Registerkarte Advanced (Erweitert) und stellen Sie sicher, dass das Volume für den gemeinsamen Zugriff von mehreren Initiatoren aus freigegeben ist.
Die Laufwerke des gemeinsamen Clusterspeichers können nicht gelesen werden oder wurden in der	<ul style="list-style-type: none"> • Dieses Problem tritt auf, wenn Sie den Clusterdienst anhalten. • Unter den Betriebssystemen Windows Server 2003 tritt 	Keine Maßnahme erforderlich.

Problem	Mögliche Ursache	Maßnahme
Laufwerksverwaltung von Windows nicht initialisiert.	dieses Problem auf, falls der Clusterknoten keinen Clusterdatenträger besitzt.	
Der Clusterdienst funktioniert nicht korrekt bei einem Cluster mit Windows Server 2003 und aktivierter Internet-Firewall.	Wenn die Internetverbindungs-Firewall von Windows aktiviert ist, können Konflikte mit dem Clusterdienst auftreten.	<p>Führen Sie folgende Schritte durch:</p> <ol style="list-style-type: none"> 1. Klicken Sie auf dem Windows-Desktop mit der rechten Maustaste auf Arbeitsplatz und anschließend auf Verwalten. 2. Doppelklicken Sie im Fenster Computerverwaltung auf Dienste. 3. Doppelklicken Sie im Fenster Dienste auf Clusterdienste. 4. Doppelklicken Sie im Fenster Clusterdienste auf die Registerkarte Wiederherstellung 5. Klicken Sie auf den nach unten zeigenden Pfeil für den ersten Fehler und wählen Sie die Option zum Neustart des Dienstes. 6. Klicken Sie auf den nach unten zeigenden Pfeil für den zweiten Fehler und wählen Sie die Option zum Neustart des Dienstes. 7. Klicken Sie auf OK. <p>Wie Sie den Cluster mit aktivierter Windows-Internet-Firewall konfigurieren, erfahren Sie in den Artikeln 258469 und 883398 unter support.microsoft.com und microsoft.com/technet.</p>
Clients aus öffentlichen Netzwerken haben keinen Zugriff auf die vom Cluster bereitgestellten Anwendungen oder Dienste.	Möglicherweise wurde für einen oder mehrere Knoten die Internetverbindungs-Firewall aktiviert, die nun die RPC-Kommunikation zwischen den Knoten blockiert.	<p>Konfigurieren Sie die Internetverbindungs-Firewall so, dass die von MSCS und den Clusteranwendungen/-diensten benötigte Datenkommunikation zugelassen wird.</p> <p>Weitere Informationen finden Sie unter support.microsoft.com im Artikel KB883398.</p>
Der Speicherarray-Firmware-Upgrade-Vorgang unter Verwendung von Telnet wird beendet, ohne Ihnen die Eingabe von "y" (Ja) zu der folgenden Nachricht zu ermöglichen: "Do you want to proceed (y/n) [n]:" (Möchten Sie fortfahren (j/n) [n]:)	Das Telnet-Programm sendet eine zusätzliche Zeile, nachdem Sie auf <Eingabetaste> drücken.	<p>Benutzen Sie zur Aktualisierung der Speicherarray-Firmware eine serielle Verbindung.</p> <p>Um den zusätzlichen Zeilenvorschub unter Windows Telnet zu löschen:</p> <ol style="list-style-type: none"> 1. Geben Sie die Kombination ^] (Strg-rechte eckige Klammer) ein. 2. Geben Sie an der Eingabeaufforderung von

Problem	Mögliche Ursache	Maßnahme
Bei der Ausführung des Cluster Validation Wizard (Assistent zur Clustervalidierung) ergibt der Test zur Validierung der IP-Konfiguration, dass zwei iSCSI-NICs dem gleichen Subnetz angehören, und es wird ein Warnhinweis angezeigt.	Es ist vorgesehen, dass die beiden iSCSI-NICs zum gleichen Subnetz gehören.	<p>Microsoft Telnet den Befehl <code>unset crlf</code> ein.</p> <p>3. Drücken Sie die <Eingabetaste>, um zu Telnet zurückzukehren.</p> <p>Keine Maßnahme erforderlich.</p>

Cluster-Datenformular

Sie können Exemplare dieses Vordrucks bei den einzelnen Clusterknoten oder Racks anbringen, um Informationen über Cluster festzuhalten. Verwenden Sie diese Aufzeichnungen, wenn Sie technische Unterstützung anfordern.

Tabelle 1. Informationen zur Clusterkonfiguration

Clusterinformationen	Clusterlösung
Clustername und IP-Adresse	
Servertyp	
Installation durchgeführt von	
Installationsdatum	
Anwendungen	
Standort	
Anmerkungen	

Tabelle 2. Informationen zur Clusterknotenkonfiguration

Knotenname	Service-Tag-Nummer	Öffentliche IP-Adresse	Private IP-Adresse

Tabelle 3. Weitere Informationen zum Netzwerk

Weitere Netzwerke

Tabelle 4. Informationen zur Speicherarraykonfiguration

Array	Service-Tag-Nummer des Arrays	Gruppen-IP-Adresse	Gruppenname	Mitgliedsname	Volume-Namen
1					
2					
3					

Mutual CHAP
Secret

B

Static IP address
(storage array)

Subnet

Default
Gateway

Array 1, Group IP Address	____.____.____.____	____.____.____.____	____.____.____.____
Array 1, Ethernet 0	____.____.____.____	____.____.____.____	____.____.____.____
Array 1, Ethernet 1	____.____.____.____	____.____.____.____	____.____.____.____
Array 1, Ethernet 2	____.____.____.____	____.____.____.____	____.____.____.____
Array 1, Ethernet 3	____.____.____.____	____.____.____.____	____.____.____.____
Array 2, Group IP Address	____.____.____.____	____.____.____.____	____.____.____.____
Array 2, Ethernet 0	____.____.____.____	____.____.____.____	____.____.____.____
Array 2, Ethernet 1	____.____.____.____	____.____.____.____	____.____.____.____
Array 2, Ethernet 2	____.____.____.____	____.____.____.____	____.____.____.____
Array 2, Ethernet 3	____.____.____.____	____.____.____.____	____.____.____.____
Array 3, Group IP Address	____.____.____.____	____.____.____.____	____.____.____.____
Array 3, Ethernet 0	____.____.____.____	____.____.____.____	____.____.____.____
Array 3, Ethernet 1	____.____.____.____	____.____.____.____	____.____.____.____
Array 3, Ethernet 2	____.____.____.____	____.____.____.____	____.____.____.____
Array 3, Ethernet 3	____.____.____.____	____.____.____.____	____.____.____.____
Array 4, Group IP Address	____.____.____.____	____.____.____.____	____.____.____.____
Array 4, Ethernet 0	____.____.____.____	____.____.____.____	____.____.____.____
Array 4, Ethernet 1	____.____.____.____	____.____.____.____	____.____.____.____
Array 4, Ethernet 2	____.____.____.____	____.____.____.____	____.____.____.____
Array 4, Ethernet 3	____.____.____.____	____.____.____.____	____.____.____.____

Target CHAP
Secret