

# Hardwareinstallations- und Fehlerbehebungshandbuch

[Einführung](#)

[Verkabelung der Clusterhardware](#)

[Vorbereiten der Systeme für den Clusterbetrieb](#)

[Fehlerbehebung](#)

[Cluster-Datenformular](#)

[iSCSI-Konfigurationsarbeitsblatt](#)

---

## Anmerkungen und Vorsichtshinweise

 **ANMERKUNG:** Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie den Computer besser einsetzen können.

 **VORSICHTSHINWEIS:** Ein **VORSICHTSHINWEIS** macht aufmerksam auf mögliche Beschädigung der Hardware oder Verlust von Daten bei Nichtbefolgung von Anweisungen.

---

**Irrtümer und technische Änderungen vorbehalten.**  
© 2008–2010 Dell Inc. Alle Rechte vorbehalten.

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

In diesem Text verwendete Marken: Dell™, das DELL Logo, PowerEdge™ und PowerVault™ sind Marken von Dell Inc. Microsoft®, Active Directory®, Windows® und Windows Server® sind Marken oder eingetragene Marken von Microsoft Corporation in den USA und/oder anderen Ländern.

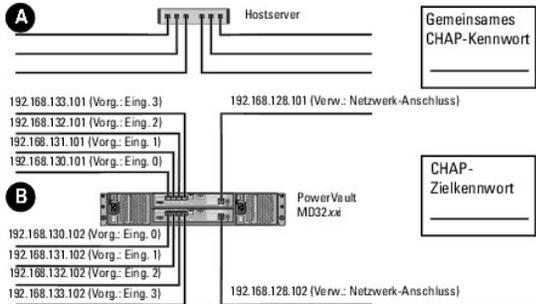
Alle anderen in dieser Dokumentation genannten Marken und Handelsbezeichnungen sind Eigentum der entsprechenden Hersteller und Firmen. Dell Inc. erhebt keinen Anspruch auf Markenzeichen und Handelsbezeichnungen mit Ausnahme der eigenen.

**Juni 2010    Rev. A01**

# iSCSI-Konfigurationsarbeitsblatt

Hardwareinstallations- und Fehlerbehebungshandbuch

## IPv4-Einstellungen

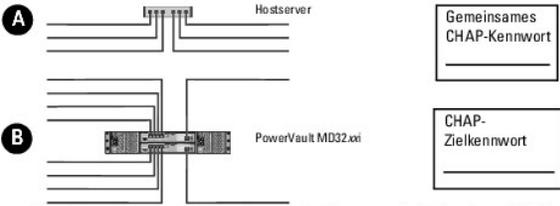


Wenn Sie zusätzlichen Platz für weitere Hostserver benötigen, verwenden Sie ein weiteres Arbeitsblatt.

<b>A</b> Feste IP-Adresse (Hostserver)	Subnetz <i>(jeder NIC benötigt ein eigenes Subnetz)</i>	Standard-Gateway
iSCSI-Port 1	-----	-----
iSCSI-Port 2	-----	-----
iSCSI-Port 3	-----	-----
iSCSI-Port 4	-----	-----
Verwaltungsschnittstelle	-----	-----
Verwaltungsschnittstelle	-----	-----

<b>B</b> Feste IP-Adresse (Hostserver)	Subnetz	Standard-Gateway
iSCSI-Controller 0, Eing. 0	-----	-----
iSCSI-Controller 0, Eing. 1	-----	-----
iSCSI-Controller 0, Eing. 2	-----	-----
iSCSI-Controller 0, Eing. 3	-----	-----
Verwaltungsport-Contrl. 0	-----	-----
iSCSI-Controller 1, Eing. 0	-----	-----
iSCSI-Controller 1, Eing. 1	-----	-----
iSCSI-Controller 1, Eing. 2	-----	-----
iSCSI-Controller 1, Eing. 3	-----	-----
Verwaltungsport-Contrl. 1	-----	-----

## IPv6-Einstellungen:



Wenn Sie zusätzlichen Platz für weitere Hostserver benötigen, verwenden Sie ein weiteres Arbeitsblatt.

**A**

Host-iSCSI-Port 1	Host-iSCSI-Port 2
Lokale IP-Adresse verbinden	Lokale IP-Adresse verbinden
Routingfähige IP-Adresse	Routingfähige IP-Adresse
Subnetz-Präfix	Subnetz-Präfix
Gateway	Gateway

**B**

iSCSI-Controller 0, Eing. 0

IP-Adresse FE80 : 0000 : 0000 : 0000 : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 1 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 2 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Router-IP-Adresse \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

iSCSI-Controller 0, Eing. 1

IP-Adresse FE80 : 0000 : 0000 : 0000 : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 1 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 2 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Router-IP-Adresse \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

iSCSI-Controller 0, Eing. 2

IP-Adresse FE80 : 0000 : 0000 : 0000 : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 1 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 2 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Router-IP-Adresse \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

iSCSI-Controller 0, Eing. 3

IP-Adresse FE80 : 0000 : 0000 : 0000 : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 1 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 2 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Router-IP-Adresse \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

iSCSI-Controller 1, Eing. 0

IP-Adresse FE80 : 0000 : 0000 : 0000 : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 1 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 2 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Router-IP-Adresse \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

iSCSI-Controller 1, Eing. 1

IP-Adresse FE80 : 0000 : 0000 : 0000 : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 1 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 2 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Router-IP-Adresse \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

iSCSI-Controller 1, Eing. 2

IP-Adresse FE80 : 0000 : 0000 : 0000 : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 1 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 2 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Router-IP-Adresse \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

iSCSI-Controller 1, Eing. 3

IP-Adresse FE80 : 0000 : 0000 : 0000 : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 1 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Routingfähige IP-Adresse 2 \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_

Router-IP-Adresse \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_ : \_\_\_\_\_



[Zurück zum Inhaltsverzeichnis](#)

## Verkabelung der Clusterhardware

Hardwareinstallations- und Fehlerbehebungshandbuch

- [Verkabeln von Maus, Tastatur und Bildschirm](#)
- [Verkabeln der Netzteile](#)
- [Verkabeln des öffentlichen und privaten Netzwerks](#)
- [Verkabeln der Speichersysteme](#)

In den folgenden Abschnitten ist beschrieben, wie die verschiedenen Komponenten des Clusters verkabelt werden.

---

### Verkabeln von Maus, Tastatur und Bildschirm

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

---

### Verkabeln der Netzteile

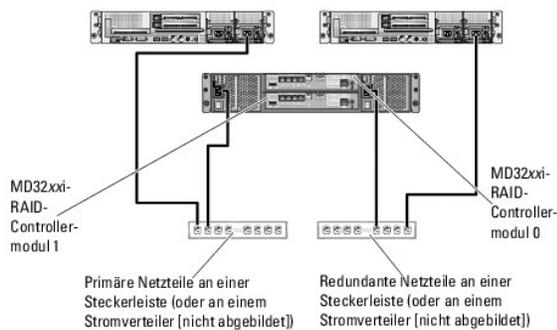
Stellen Sie anhand der Dokumentation zu den einzelnen Komponenten der Clusterlösung sicher, dass die jeweiligen Anforderungen an die Stromversorgung erfüllt sind.

Folgende Richtlinien werden empfohlen, um die Clusterlösung gegen Stromausfälle zu schützen:

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

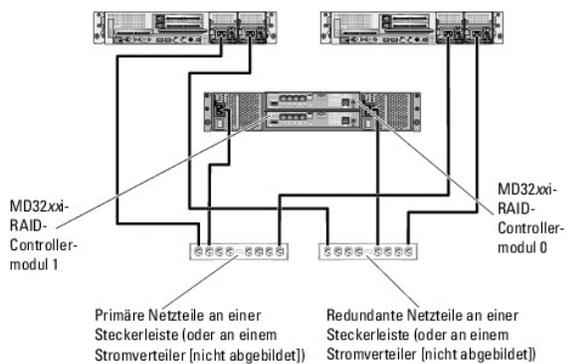
[Abbildung 2-1](#) und [Abbildung 2-2](#) zeigen empfohlene Methoden zur elektrischen Verkabelung einer Clusterlösung mit zwei Dell PowerEdge-Systemen und einem Speichersystem. Um Redundanz zu gewährleisten, werden die primären Netzteile aller Komponenten an einem oder an zwei Stromkreisen angeschlossen und die redundanten Netzteile an einem anderen Stromkreis.

**Abbildung 2-1. Beispiele für die elektrische Verkabelung mit einem Netzteil pro PowerEdge-System**



**ANMERKUNG:** Diese Darstellung der Stromverteilung zu den Komponenten dient lediglich als Beispiel.

**Abbildung 2-2. Beispiel für die Verkabelung mit zwei Netzteilen pro PowerEdge-System**



**ANMERKUNG:** Diese Darstellung der Stromverteilung zu den Komponenten dient lediglich als Beispiel.

## Verkabeln des öffentlichen und privaten Netzwerks

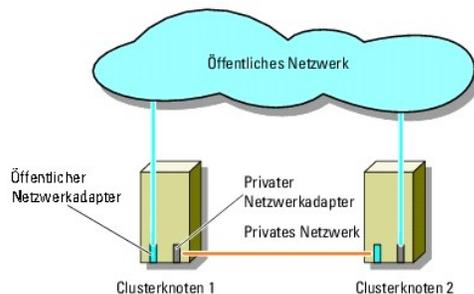
Die Netzwerkkadpter der Clusterknoten stellen für jeden Knoten mindestens zwei Netzwerkverbindungen bereit. Diese Verbindungen sind in [Tabelle 2-1](#) beschrieben.

Tabelle 2-1. Netzwerkverbindungen

Netzwerkverbindung	Beschreibung
Öffentliches Netzwerk	Alle Verbindungen zum Client-LAN.  Mindestens ein öffentliches Netzwerk muss für Mischbetrieb (öffentlich und privat) konfiguriert sein, damit ein Failover des privaten Netzwerks möglich ist.
Privates Netzwerk	Eine gesonderte Verbindung für den Austausch von Clusterdaten und Zustandsmeldungen zwischen den Clusterknoten.  Mit dem LAN verbundene Netzwerkkadpter können außerdem Redundanz auf der Kommunikationsebene zur Verfügung stellen, falls die interne Clusterverbindung ausfällt.  Weitere Informationen über Redundanz im privaten Netzwerk finden Sie in der Dokumentation zur Microsoft Failover-Clusterunterstützung.

[Abbildung 2-3](#) zeigt ein Beispiel für die Verkabelung von Netzwerkkadptern, bei dem reservierte Netzwerkkadpter auf jedem Knoten mit dem öffentlichen Netzwerk und die übrigen Netzwerkkadpter untereinander verbunden sind (für das private Netzwerk).

Abbildung 2-3. Beispiel einer Netzwerkverkabelung



## Öffentliches Netzwerk verkabeln

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

## Verkabeln des privaten Netzwerks

Die private Netzwerkverbindung zu den Clusterknoten erfolgt über einen zweiten oder nachfolgenden Netzwerkadapter, der auf jedem Knoten installiert ist. Dieses Netzwerk wird für die Kommunikation innerhalb des Clusters verwendet.

In [Tabelle 2-2](#) sind die erforderlichen Hardwarekomponenten und die Verbindungsmethode für drei mögliche private Netzwerkkonfigurationen aufgeführt.

**Tabelle 2-2. Hardwarekomponenten und Verbindungen privater Netzwerke**

Methode	Hardwarekomponenten	Verbindung
Netzwerk-Switch	Gigabit- oder 10-Gigabit-Ethernet-Netzwerkadapter und -Switches.	Installieren Sie je nach Hardware, CAT5e- oder CAT6-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- oder 10-Gigabit-Ethernet-Netzwerkadapter mit RJ-45-Anschlüssen.	Verbinden Sie die Netzwerkadapter in beiden Knoten mit einem Standard-Ethernetkabel (CAT5e oder CAT6).
	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.

 **ANMERKUNG:** In diesem Dokument bezieht sich der Ausdruck Gigabit-Ethernet entweder auf Gigabit-Ethernet oder auf 10-Gigabit-Ethernet.

## Verwenden von Netzwerkadaptern mit zwei Ports für das private Netzwerk

Sie können den Cluster so konfigurieren, dass das öffentliche Netzwerk zum Failover für die private Netzverbindung genutzt wird. Verwenden Sie jedoch beim Einsatz von Netzwerkadaptern mit zwei Ports nicht beide Ports zugleich zur Unterstützung von öffentlichem und privatem Netzwerk.

## NIC-Teaming

Beim so genannten NIC-Teaming werden zwei oder mehrere Netzwerkadapter (NICs) kombiniert, um für Lastausgleich bzw. Fehlertoleranz zu sorgen. Der Cluster unterstützt NIC-Teaming, aber nur in einem öffentlichen Netzwerk; NIC-Teaming wird in einem privaten Netzwerk nicht unterstützt.

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

---

## Verkabeln der Speichersysteme

Dieser Abschnitt enthält Informationen zum Verbinden des Clusters mit einem Speichersystem.

 **ANMERKUNG:** Wie Sie Dell Blade-Systemmodule in einem Dell PowerEdge-Cluster konfigurieren, erfahren Sie in der Dokumentation Using Dell Blade Servers in a Dell PowerEdge High Availability Cluster (Verwendung von Dell Blade-Servern in einem Dell PowerEdge High Availability Cluster) unter [support.dell.com/manuals](http://support.dell.com/manuals).

 **ANMERKUNG:** Weitere Details und Beschreibungen zu Einstellungen der Speicherhardware finden Sie im Hardwarebenutzerhandbuch zum Dell PowerVault MD3200i / MD3220i RAID-Speichergehäuse unter [support.dell.com/manuals](http://support.dell.com/manuals).

Die Speicherverwaltung erfolgt entweder bandintern über die Host-zu-Controller-Schnittstelle oder bandextern über eine Ethernet-Verbindung. Zur bandexternen Speicherverwaltung müssen die Ethernet-Anschlüsse des Speicherarrays mit dem öffentlichen Netzwerk verbunden werden.

 **ANMERKUNG:** Es wird empfohlen, das Dell PowerVault MD3200i / MD3220i- Gehäuse für die bandexterne Verwaltung zu konfigurieren.

## Verkabeln des Clusters in einer Direct-Attach-Konfiguration

Bei der Direct-Attach-Konfiguration sind alle Clusterknoten über zwei Netzwerkkabel und einen Zweiport-NIC bzw. zwei Einzelport-NICs direkt mit den PowerVault MD3200i / MD3220i-RAID-Controllermodulen verbunden.

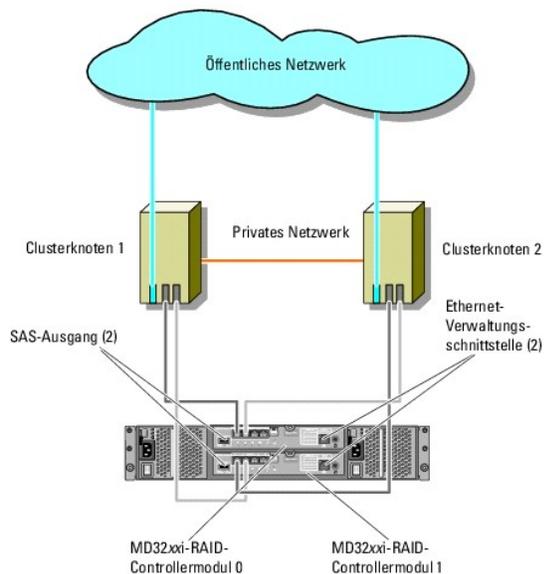
Wenn eine Komponente des Speicherpfads ausfällt - etwa der Port, das Kabel oder der Speichercontroller - leitet der Multipath-Treiber die E/A-Anforderungen automatisch auf den alternativen Pfad um, sodass der Betrieb des Speicherarrays nicht unterbrochen wird. Die Konfiguration mit zwei Einzelport-NICs bietet höhere Verfügbarkeit, da der Failover-Cluster die Clusterressourcen beim Ausfall eines NICs nicht auf den anderen Clusterknoten zu verschieben braucht.

Der Cluster wird wie folgt verkabelt:

1. Verbinden Sie Clusterknoten 1 mit dem Speichersystem:
  - a. Verbinden Sie Clusterknoten 1, iSCSI-NIC 1 (oder NIC-Port 1) über ein Netzwerkkabel mit RAID-Controllermodul 0, Port In-0.
  - b. Verbinden Sie Clusterknoten 1, iSCSI-NIC 2 (oder NIC-Port 2) über ein Netzwerkkabel mit RAID-Controllermodul 1, Port In-1.
2. Verbinden Sie Clusterknoten 2 mit dem Speichersystem:
  - a. Verbinden Sie Clusterknoten 2, iSCSI-NIC 1 (oder NIC-Port 1) über ein Netzwerkkabel mit RAID-Controllermodul 1, Port In-0.

- b. Verbinden Sie Clusterknoten 2, iSCSI-NIC 2 (oder NIC-Port 2) über ein Netzwerkkabel mit RAID-Controllermodul 0, Port In-1.
3. Verbinden Sie ggf. den Knoten 3 mit dem Speichersystem. Knoten 3 kann entweder Clusterknoten 1 des einzigen Clusters in der Konfiguration, Clusterknoten 1 des zweiten Clusters oder ein eigenständiger Server sein.
  - a. Verbinden Sie Clusterknoten 3, iSCSI-NIC 1 (oder NIC-Port 1) über ein Netzwerkkabel mit RAID-Controllermodul 0, Port In-2.
  - b. Verbinden Sie Clusterknoten 3, iSCSI-NIC 2 (oder NIC-Port 2) über ein Netzwerkkabel mit RAID-Controllermodul 1, Port In-3.
4. Verbinden Sie ggf. den Knoten 4 mit dem Speichersystem. Knoten 4 kann entweder Clusterknoten 4 des einzigen Clusters in der Konfiguration, Clusterknoten 2 des zweiten Clusters oder ein eigenständiger Server sein.
  - a. Verbinden Sie Clusterknoten 4, iSCSI-NIC 1 (oder NIC-Port 1) über ein Netzwerkkabel mit RAID-Controllermodul 1, Port In-2.
  - b. Verbinden Sie Clusterknoten 4, iSCSI-NIC 2 (oder NIC-Port 2) über ein Netzwerkkabel mit RAID-Controllermodul 0, Port In-3.

Abbildung 2-4. Direct-Attach-Clusterkonfiguration



**ANMERKUNG:** Der SAS-Ausgangsport stellt die SAS-Verbindung für MD1200 / MD1220-Erweiterungsgehäuse bereit.

## Verkabeln des Clusters in einer Network-Attach-Konfiguration

Bei einer Network-Attach-Konfiguration werden alle Clusterknoten über redundante 1-Gb-Ethernet-Standardswitches für IP-Speichernetzwerk (SAN) sowie über einen Zweiport-iSCSI-NIC bzw. zwei Einzelport-iSCSI-NICs mit dem Speichersystem verbunden. Wenn eine Komponente des Speicherpfads ausfällt - etwa der iSCSI-NIC, das Kabel, der Switch oder der Speichercontroller - leitet der Multipath-Treiber die E/A-Anforderungen automatisch auf den alternativen Pfad um, sodass der Betrieb des Speicherarrays nicht unterbrochen wird. Die Konfiguration mit zwei Einzelport-NICs bietet höhere Verfügbarkeit, da der Microsoft Failover-Cluster die Clusterressourcen beim Ausfall eines NICs nicht auf den anderen Clusterknoten zu verschieben braucht.

Diese Konfiguration unterstützt bis zu 32 Hosts gleichzeitig. Einige Beispiele für diese Konfiguration:

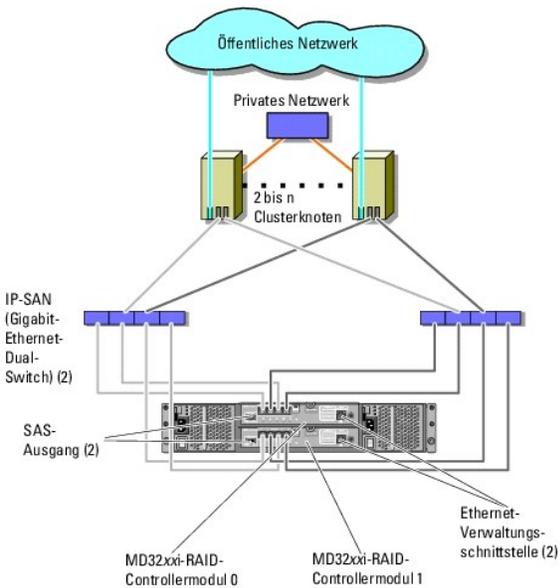
- 1 Ein Cluster.
- 1 Zwei Cluster.
- 1 Ein Cluster mit acht Knoten, zwei Cluster mit zwei Knoten und ein Standalone-System.

Der Cluster wird wie folgt verkabelt:

1. Verbinden Sie das Speichersystem mit dem iSCSI-Netzwerk:
  - a. Verbinden Sie Switch 1 über ein Netzwerkkabel mit Controller 0, Port In-0.
  - b. Verbinden Sie Switch 1 über ein Netzwerkkabel mit Controller 1, Port In-0.
  - c. Verbinden Sie Switch 2 über ein Netzwerkkabel mit Controller 0, Port In-1.
  - d. Verbinden Sie Switch 2 über ein Netzwerkkabel mit Controller 1, Port In-1.
  - e. Verbinden Sie Switch 1 über ein Netzwerkkabel mit Controller 0, Port In-2.

- f. Verbinden Sie Switch 1 über ein Netzwerkkabel mit Controller 1, Port In-2.
  - g. Verbinden Sie Switch 2 über ein Netzwerkkabel mit Controller 0, Port In-3.
  - h. Verbinden Sie Switch 2 über ein Netzwerkkabel mit Controller 1, Port In-3.
2. Verbinden Sie den Cluster mit dem iSCSI-Netzwerk:
- a. Verbinden Sie Clusterknoten 1, iSCSI-NIC 1 (oder NIC-Port 1) über ein Netzwerkkabel mit Netzwerk-Switch 1.
  - b. Verbinden Sie Clusterknoten 1, iSCSI-NIC 2 (oder NIC-Port 2) über ein Netzwerkkabel mit Netzwerk-Switch 2.
  - c. Wiederholen Sie [Schritt a](#) und [Schritt b](#) für jeden weiteren Clusterknoten.
3. Wiederholen Sie [Schritt 2](#), um weitere Cluster oder Standalone-Systeme mit dem iSCSI-Netzwerk zu verbinden.

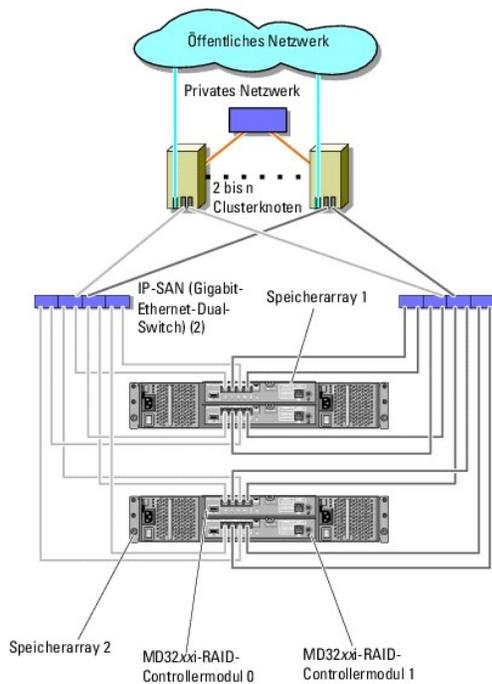
Abbildung 2-5. Network-Attach-Clusterkonfiguration



## Verbinden eines PowerEdge-Clusters mit mehreren PowerVault MD3200i / MD3220i-Speichersystemen

Sie können die Speicherkapazität des Clusters erhöhen, indem Sie mehrere Speichersysteme über redundante Netzwerkeswitches an den Cluster anschließen. PowerEdge-Clustereysteme unterstützen Konfigurationen mit mehreren an PowerVault MD3200i / MD3220i-Clustereysteme angeschlossenen Speichersystemen. In diesem Szenario kann die Failover-Cluster-Software für die Laufwerke jedes freigegebenen und an den Cluster angeschlossenen Speicherarrays einen Failover zwischen den Clusterknoten durchführen.

Abbildung 2-6. Network-Attach-Clusterkonfiguration mit mehreren Speicherarrays



Beim Verbinden mehrerer PowerVault MD3200i / MD3220i-Speichersysteme mit dem Cluster gelten folgende Regeln:

- 1 Maximal vier PowerVault MD3200i / MD3220i-Speichersysteme pro Cluster.
- 1 Die gemeinsamen Speichersysteme und die Firmware müssen identisch sein. Unterschiedliche Speichersysteme und Firmware im gemeinsamen Speicher werden nicht unterstützt.
- 1 Windows begrenzt den Zugriff auf Laufwerke durch die maximale Anzahl der möglichen Laufwerksbuchstaben. Diese beträgt 22. Weil die Laufwerksbuchstaben A bis D für lokale Datenträger reserviert sind, können den Datenträgern des Speichersystems maximal 22 Laufwerksbuchstaben (E bis Z) zugewiesen werden.
- 1 Windows Server2008 Enterprise Edition unterstützt Bereitstellungspunkte, wodurch mehr als 22 Laufwerke pro Cluster möglich sind.

---

[Zurück zum Inhaltsverzeichnis](#)





[Zurück zum Inhaltsverzeichnis](#)

## Einführung

Hardwareinstallations- und Fehlerbehebungshandbuch

- [Übersicht](#)
- [Clusterlösung](#)
- [Anforderungen für den Cluster](#)
- [Unterstützte Clusterkonfigurationen](#)
- [Weitere nützliche Dokumente](#)

Dieses Dokument enthält Informationen über die Installation und Verwaltung der Clusterlösung mit den Speichersystemen Dell PowerVault MD3200i und MD3220i. Es richtet sich an erfahrene IT-Fachleute, die die Clusterlösung konfigurieren und an geschulte Service-Techniker, die Upgrade- und Wartungsmaßnahmen durchführen. Zudem ist es auch für Leser gedacht, die sich mit der Clustertechnologie vertraut machen möchten.

---

## Übersicht

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

Dieses Handbuch erläutert die Konfiguration der iSCSI-Speicherarrays Dell MD3200i und MD3220i für den Betrieb mit einem oder mehreren Windows Server Failover-Clustern. Es enthält Anleitungen und spezifische Konfigurationsschritte, die es Ihnen ermöglichen, den gemeinsamen Speicher für Ihren Cluster zu aktivieren.

Weitere Informationen zur Bereitstellung eines Clusters finden Sie im *Installations- und Fehlerbehebungshandbuch für Dell Failover-Cluster unter Microsoft Windows Server* unter [support.dell.com/manuals](http://support.dell.com/manuals).

 **ANMERKUNG:** In diesem gesamten Dokument ist mit der Bezeichnung Windows Server 2008 sowohl das Betriebssystem Windows Server 2008 x64 Enterprise Edition als auch Windows Server 2008 R2 x64 Enterprise Edition gemeint.

Eine Liste der empfohlenen Betriebssysteme, Hardwarekomponenten und Treiber- oder Firmwareversionen für Dell Windows Server Failover-Cluster finden Sie in den *Support-Matrizen für Dell Clusterkonfiguration* unter [dell.com/ha](http://dell.com/ha).

---

## Clusterlösung

Ein iSCSI-Cluster besteht aus mindestens zwei und höchstens 16 Knoten und bietet die folgenden Funktionen:

- 1 iSCSI-Technologie (iSCSI = Internet Small Computer System Interface)
- 1 Hohe Verfügbarkeit der Systemdienste und Ressourcen für Netzwerk-Clients
- 1 Redundante Pfade zum gemeinsamen Speicher
- 1 Ausfallwiederherstellung für Anwendungen und Dienste
- 1 Flexible Wartungsmerkmale, mit denen einzelne Clusterknoten repariert, gewartet oder aufgerüstet werden können, ohne den gesamten Cluster vom Netz nehmen zu müssen.

Die Implementierung von iSCSI-Technologie in einem Cluster bietet folgende Vorteile:

- 1 **Flexibilität** - iSCSI basiert auf TCP/IP. Daher können sich Clusterknoten und Speichersysteme an unterschiedlichen Standorten befinden.
- 1 **Verfügbarkeit** - iSCSI-Komponenten enthalten redundante Verbindungen und sorgen so für alternative Datenwege und größere Verfügbarkeit für die Clients.
- 1 **Anschlussmöglichkeiten** - iSCSI ermöglicht mehr Geräteverbindungen als SCSI. Da iSCSI-Geräte hot-swap-fähig sind, lassen sich Elemente an den Knoten hinzufügen oder entfernen, ohne den Cluster abschalten zu müssen.

---

## Anforderungen für den Cluster

Im Cluster werden die folgenden Komponenten benötigt:

- 1 Server (Clusterknoten)
- 1 Speicher und Speicherverwaltungssoftware

## Clusterknoten

[Tabelle 1-1](#) enthält die Hardwareanforderungen für die Clusterknoten.

**Tabelle 1-1. Anforderungen für Clusterknoten**

Komponente	Mindestanforderungen
Prozessor	Mindestens ein Prozessor für jeden Clusterknoten.
Clusterknoten	Es werden mindestens zwei identische PowerEdge-Systeme benötigt.
RAM	Mindestens 1 GB RAM auf jedem Clusterknoten.
iSCSI-Initiator	Vollständige Installation - bestehend aus iSCSI-Port-Treiber, InitiatorDienst und Software-Initiator - auf jedem Knoten.  <b>ANMERKUNG:</b> Microsoft Multipath-E/A (MPIO) Multipathing Support für iSCSI ist nicht installiert.
Netzwerkadapter (NICs) für den iSCSI-Zugriff	Zwei iSCSI-NICs oder NIC-Ports pro Knoten. Setzen Sie die NICs in getrennte PCI-Busse ein, um Verfügbarkeit und Leistung zu erhöhen. Für iSCSI-Datenverkehr werden auch TOE-NICs (TOE = TCP/IP Offload Engine) unterstützt. Eine Liste der empfohlenen Betriebssysteme, Hardwarekomponenten und Treiber- oder Firmwareversionen für Dell Windows Server Failover-Cluster finden Sie in den <i>Support-Matrizen für Dell Clusterkonfiguration</i> unter <a href="http://dell.com/ha">dell.com/ha</a> .
NICs (öffentlich und privat)	Mindestens zwei Netzwerkadapter: einen Netzwerkadapter für das öffentliche Netzwerk und einen weiteren für das private Netzwerk.  <b>ANMERKUNG:</b> Es wird empfohlen, dass die Netzwerkadapter auf jedem öffentlichen Netzwerk vom gleichen Typ sind und dass die Netzwerkadapter auf jedem privaten Netzwerk vom gleichen Typ sind.
Interner Datenträgercontroller	Ein mit den internen Datenträgern verbundener Controller pro Knoten. Es kann jeder unterstützte RAID-Controller (Redundant Array of Independent Disk) bzw. Laufwerkcontroller verwendet werden.  Für Spiegelung (RAID 1) sind zwei und für Disk-Striping mit Parität (RAID 5) mindestens drei physische Datenträger erforderlich.  <b>ANMERKUNG:</b> Es wird empfohlen, hardwarebasiertes RAID oder softwarebasierte Fehlertoleranz für die internen Laufwerke zu verwenden.

## Clusterspeicher

In [Tabelle 1-2](#) sind die Konfigurationsanforderungen für das gemeinsame Speichersystem aufgeführt.

Tabelle 1-2. Anforderungen für Clusterspeicher

Hardwarekomponenten	Mindestanforderungen
Unterstützte Speichersysteme	Ein Dell PowerVault MD3200i / MD3220i RAID-Speichergehäuse.  Bis zu sieben Dell PowerVault MD1200 / MD1220-Erweiterungsgehäuse mit jeweils maximal 96 Festplatten.
Stromversorgung und Kühlung	Zwei integrierte, hot-swap-fähige Netzteil-/Lüftermodule.
Physische Laufwerke	Mindestens zwei physische Datenträger im PowerVault MD3200i / MD3220i-RAID-Gehäuse.
Mehrere Cluster und eigenständige Systeme	Bei einer Switch-Attach-Konfiguration können ein oder mehrere PowerVault MD3200i / MD3220i-Systeme von Clustern und Einzelsystemen gemeinsam genutzt werden.

 **ANMERKUNG:** RAID 0 und unabhängige Datenträger sind möglich, werden aber für ein hochverfügbares System nicht empfohlen, da bei Laufwerksausfall keine Datenredundanz besteht.

## Cluster-Speicherverwaltungssoftware

### Dell PowerVault Modular Disk Storage Manager

Die Software läuft auf der Verwaltungsstation oder einem beliebigen mit dem Speicherarray verbundenen Hostsystem, um die zentrale Verwaltung der PowerVault MD3200i / MD3220i-RAID-Gehäuse zu gewährleisten. Mit Dell PowerVault Modular Disk Storage Manager (MDSM) können verschiedene Aufgaben durchgeführt werden, wie etwa das Erstellen und Verwalten von RAID-Arrays, das Binden von virtuellen Laufwerken und das Herunterladen von Firmware.

MDSM ist eine grafische Benutzerschnittstelle (GUI) mit assistentengesteuerten Tools und einer aufgabenbasierten Struktur. Die Anwendung erfüllt folgende Funktionen:

- 1 Sie erleichtert die Installation, Konfiguration und Verwaltung des Speicherarrays und die Durchführung von Diagnosemaßnahmen.
- 1 Sie enthält einen Ereignisüberwachungsdienst, der Alarme sendet, wenn ein kritisches Problem im Speicherarray aufgetreten ist.
- 1 Sie stellt eine Befehlszeilenschnittstelle (Command Line Interface, CLI) bereit, damit Befehle über der Eingabeaufforderung auf Betriebssystemebene ausgeführt werden können.

### Modular Disk Storage Manager Agent

Diese Software ist auf allen Clusterknoten installiert und erfasst systembasierte Topologiedaten, die von MDSM verwaltet werden können.

## Multipath-Software

Der Multipath-E/A-Treiber (auch als Failover-Treiber bezeichnet) ist resident auf allen Clusterknoten aktiv, über die die Verwaltung der redundanten Datenpfade zwischen System und RAID-Gehäuse läuft. Damit der Multipath-Treiber einen redundanten Pfad korrekt verwalten kann, muss die Konfiguration redundante NICs und Verkabelungen bereit stellen.

Der Multipath-Treiber identifiziert Mehrfachpfade zu einem virtuellen Laufwerk und richtet einen bevorzugten Pfad zu dem betreffenden Laufwerk ein. Wenn eine Komponente des bevorzugten Pfads ausfällt, leitet der Treiber E/A-Anforderungen automatisch über den alternativen Pfad weiter, sodass das Speicherarray ohne Unterbrechung verfügbar bleibt.

## Erweiterte Funktionen

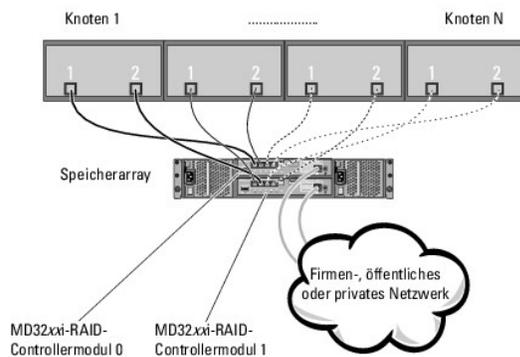
Die Speichersysteme PowerVault MD3200i und MD3220i bieten unter anderem die folgenden erweiterten Funktionen:

- 1 **Snapshot Virtual Disk** - Ermöglicht es, Momentaufnahmen von virtuellen Laufwerken zur Sicherung, zum Testen oder zur Datenverarbeitung zu erstellen, ohne den Inhalt des jeweiligen virtuellen Quelllaufwerks zu verändern.
- 1 **Virtual Disk Copy** - Beim Kopieren eines virtuellen Laufwerks in einem Speicherarray wird auf dem virtuellen Ziellaufwerk eine vollständige Kopie der auf dem virtuellen Quelllaufwerk befindlichen Daten erstellt. Virtual Disk Copy kann genutzt werden, um Daten zu sichern, Daten von Datenträgergruppen mit Datenträgern von geringerer Kapazität in Datenträgergruppen mit größeren Datenträgern zu kopieren oder um Daten vom virtuellen Snapshot-Laufwerk auf das virtuelle Quelllaufwerk zurückzukopieren.

 **ANMERKUNG:** Anweisungen zum Anwenden der korrekten Optionen in der Clusterumgebung finden Sie unter [Verwenden von erweiterten Funktionen \(Premium\) von PowerVault Modular Disk Storage Manager](#).

## Unterstützte Clusterkonfigurationen

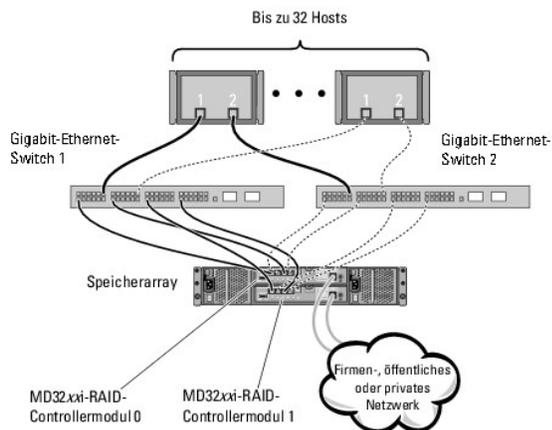
Abbildung 1-1. Direct-Attach-Clusterkonfiguration



 **ANMERKUNG:** Die Konfiguration kann bis zu vier Knoten aufweisen (N = 2, 3 oder 4). Mögliche Knoten sind:

- 1 ein Cluster
- 1 zwei verschiedene Cluster
- 1 ein Cluster und eigenständige(r) Server

Abbildung 1-2. Redundante Network-Attach-Clusterkonfiguration



**ANMERKUNG:** Die Konfiguration kann bis zu 32 Knoten aufweisen. Mögliche Knoten sind:

- 1 ein Cluster (bis zu 16 Knoten)
- 1 mehrere Cluster
- 1 mehrere Cluster und eigenständige(r) Server

## Weitere nützliche Dokumente

**VORSICHTSHINWEIS:** Die mit dem Computer gelieferten Sicherheitshinweise enthalten wichtige Sicherheits- und Betriebsbestimmungen. **Garantiebestimmungen können als separates Dokument beigelegt sein.**

**ANMERKUNG:** Wie Sie Dell Blade-Servermodule in einem Dell PowerEdge-Cluster konfigurieren, erfahren Sie in der Dokumentation Using Dell Blade Servers in a Dell PowerEdge High Availability Cluster (Verwendung von Dell Blade-Servern in einem Dell PowerEdge High Availability Cluster) unter [support.dell.com/manuals](http://support.dell.com/manuals).

- 1 In der zusammen mit der Rack-Lösung gelieferten *Rack-Installationsanleitung* ist beschrieben, wie das System in einem Rack installiert wird.
- 1 Das *Handbuch zum Einstieg* enthält eine Übersicht, um Ihr System anfangs einzurichten.
- 1 Das *Dell Failover-Cluster unter Microsoft Windows Server 2008 Installations- und Fehlerbehebungshandbuch* enthält weitere Informationen zur Bereitstellung des Clusters.
- 1 Die *Support-Matrizen für Dell Clusterkonfiguration* enthalten eine Liste empfohlener Betriebssysteme, Hardwarekomponenten und Treiber- oder Firmwareversionen für den Dell Windows Server Failover-Cluster.
- 1 In der Dokumentation zum Betriebssystem ist beschrieben, wie das Betriebssystem installiert (sofern erforderlich), konfiguriert und verwendet wird.
- 1 Das *Benutzerhandbuch zu den Dell PowerVault RAID-Gehäusen MD3200i und MD3220i* enthält Anweisungen zum Verwenden der Arrayverwaltungssoftware für die Konfiguration von RAID-Systemen.
- 1 Die Dokumentation separat erworbener Komponenten enthält Informationen zur Konfiguration und Installation dieser Zusatzgeräte.
- 1 Die Dokumentation zur Dell PowerVault-Bandbibliothek, enthält Informationen zum Installieren, zur Störungsbehebung und Aktualisierung der Bandbibliothek.
- 1 Möglicherweise sind auch Aktualisierungen beigelegt, in denen Änderungen am System, an der Software und/oder an der Dokumentation beschrieben sind.
- 1 Im Benutzerhandbuch für das PowerEdge-System sind die Systemmerkmale und technische Daten beschrieben, und es enthält Informationen zum System-Setup-Programm (sofern zutreffend), zum Software-Support und zum Systemkonfigurationsprogramm.
- 1 Das Hardware-Benutzerhandbuch zum *Dell PowerVault MD3200i / MD3220i* enthält Informationen über das Hardwaregehäuse.
- 1 Das *CLI-Handbuch zu PowerVault Modular Disk Storage Manager* erklärt die Verwendung der Befehlszeilenschnittstelle (CLI).
- 1 Die *Dell PowerVault MD3200i / MD3220i Resource-DVD* enthält Dokumentationen zu den Konfigurations- und Verwaltungsprogrammen sowie alle in diesem Abschnitt aufgeführten Dokumentationen.
- 1 Das *Handbuch zum Einstieg für Dell PowerVault MD-Systeme* enthält einen Überblick für das Einrichten und Verkabeln des Speicherarrays.
- 1 Das *Bereitstellungshandbuch für Dell PowerVault MD3220i / MD3200i Speicherarrays* enthält Installations- und Konfigurationshinweise für die Einrichtung des Speichersystems zur erstmaligen Inbetriebnahme.
- 1 Die *Support-Matrix für Dell PowerVault MD-Systeme* enthält Informationen zu der von PowerVault MD-Systemen unterstützten Software und Hardware.

**ANMERKUNG:** Lesen Sie diese Aktualisierungen immer zuerst, da sie frühere Informationen gegebenenfalls außer Kraft setzen.

1. Möglicherweise sind Versionshinweise oder Readme-Dateien vorhanden - diese enthalten neueste Updates der Systemdokumentation bzw. fortgeschrittenes technisches Referenzmaterial für erfahrene Benutzer oder Techniker.

---

[Zurück zum Inhaltsverzeichnis](#)

## Vorbereiten der Systeme für den Clusterbetrieb

Hardwareinstallations- und Fehlerbehebungshandbuch

- [Überblick über die Clusterkonfiguration](#)
- [Installationsübersicht](#)

 **VORSICHTSHINWEIS:** Nur geschulte Servicetechniker sind dazu befugt, Komponenten im Innern des Systems zu entfernen und zu warten. Ausführliche Informationen zu den Sicherheitsvorkehrungen, über das Arbeiten im Innern des Computers und zum Schutz vor elektrischer Entladung finden Sie in den mitgelieferten Sicherheitshinweisen.

---

### Überblick über die Clusterkonfiguration

1. Stellen Sie sicher, dass die elektrischen Voraussetzungen für den Cluster am Ort der Installation gegeben sind.

Ihr Verkaufsberater kann Sie über die Anforderungen der örtlichen Stromversorgung informieren.

2. Installieren Sie die Server, das/die gemeinsamen Speicherarray(s) und die Verbindungs-Switches (z. B. in einem Geräte-Rack). Stellen Sie sicher, dass alle Komponenten eingeschaltet sind.

 **ANMERKUNG:** Weitere Informationen zu [Schritt 3](#) bis [Schritt 7](#) und [Schritt 10](#) bis [Schritt 12](#) finden Sie im Abschnitt Vorbereiten der Systeme für den Clusterbetrieb des *Installations- und Fehlerbehebungshandbuch für Dell Failover-Cluster unter Microsoft Windows Server 2008* unter [support.dell.com/manuals](http://support.dell.com/manuals).

3. Stellen Sie das Betriebssystem (einschließlich aller relevanten Service Packs und Hotfixes), Netzwerkadapertreiber und Speicheradapertreiber (einschließlich Multipath-E/A Treibern (MPIO)) auf allen Servern bereit, die als Clusterknoten fungieren sollen. Je nach der verwendeten Bereitstellungsmethode ist möglicherweise eine Netzwerkverbindung erforderlich, um diesen Schritt abzuschließen.

 **ANMERKUNG:** Sie können die Clusterkonfiguration auf dem Cluster-Datenformular notieren und so die Planung und Bereitstellung des Clusters erleichtern. Weitere Informationen finden Sie unter [Cluster-Datenformular](#) und bei den iSCSI-Konfigurationshinweisen im Arbeitsblatt unter [iSCSI-Konfigurationsarbeitsblatt](#).

4. Richten Sie auf allen Serverknoten die physische Netzwerktopologie und die TCP/IP-Einstellungen für Netzwerkadapter ein, um den Zugang zu den öffentlichen und privaten Clusternetzwerken zu ermöglichen.

5. Konfigurieren Sie jeden Serverknoten als Mitgliedserver der gleichen Windows Active Directory-Domäne.

 **ANMERKUNG:** Die Clusterknoten können als Domänencontroller konfiguriert werden. Weitere Informationen finden Sie im Abschnitt Auswahl des Domänenmodells des *Installations- und Fehlerbehebungshandbuch für Dell Failover-Cluster unter Microsoft Windows Server 2008* unter [support.dell.com/manuals](http://support.dell.com/manuals).

6. Richten Sie die physische Speichertopologie ein und nehmen Sie alle weiteren Netzwerkeinstellungen vor, die benötigt werden, um Verbindungen zwischen dem Speicherarray und den als Clusterknoten konfigurierten Servern herzustellen. Konfigurieren Sie die Speichersysteme gemäß der Dokumentation zum Speichersystem.

7. Erstellen Sie mit den Dienstprogrammen zur Speicherarrayverwaltung mindestens eine logische Gerätenummer (LUN = Logical Unit Number). Die LUN wird als Zeugendatenträger für den Microsoft Windows Server 2008 Failover-Cluster verwendet. Stellen Sie sicher, dass die LUN für die Server präsent ist, die als Clusterknoten konfiguriert werden müssen.

 **ANMERKUNG:** Aus Sicherheitsgründen wird empfohlen, die LUN beim Einrichten des Clusters auf einem Einzelknoten zu konfigurieren wie in [Schritt 8](#) beschrieben. Später können Sie die LUN entsprechend der Beschreibung in [Schritt 9](#) konfigurieren, damit weitere Clusterknoten darauf zugreifen können.

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. Weitere Informationen finden Sie unter [Vorbereiten der Systeme für den Clusterbetrieb](#).

 **ANMERKUNG:** Wenn Sie einen Failover-Cluster unter Windows Server 2008 erstellen, führen Sie den **Cluster Validation Wizard** (Assistent zur Clustervalidierung) aus, um sicherzustellen, dass Ihr System für die Clusterbildung bereit ist.

9. Fügen Sie den/die verbliebenen Knoten zum Failover-Cluster hinzu. Weitere Informationen finden Sie unter [Vorbereiten der Systeme für den Clusterbetrieb](#).

10. Konfigurieren Sie die Rollen für Clusternetzwerke. Stellen Sie sicher, dass alle zur iSCSI-Speicherung (oder zu anderen Zwecken außerhalb des Clusters) verwendeten Netzwerkschnittstellen nicht durch den Cluster kontrolliert werden.

11. Testen Sie die Failover-Funktionen des neuen Clusters.

 **ANMERKUNG:** Sie können dazu auch den **Cluster Validation Wizard** (Assistent zur Clustervalidierung) verwenden.

12. Konfigurieren Sie hochverfügbare Anwendungen und Dienste auf dem Failover-Cluster. Je nach Konfiguration kann es erforderlich sein, hierfür weitere LUNs am Cluster bereitzustellen oder neue Cluster- Ressourcengruppen anzulegen. Testen Sie die Failover-Funktionen der neuen Ressourcen.
13. Konfigurieren Sie Client-Systeme für den Zugriff auf die auf dem Failover- Cluster gehosteten hochverfügbaren Anwendungen und Dienste.

---

## Installationsübersicht

Auf allen Knoten in Ihrem Dell Windows Server 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 2008 R2 Enterprise x64 Edition konfiguriert sein. Wenn auf den verschiedenen Knoten unterschiedliche Betriebssystemversionen installiert sind, kann der Failover-Cluster nicht erfolgreich konfiguriert werden. Je nach dem auf dem Cluster konfigurierten Betriebssystem wird empfohlen, vor dem Konfigurieren des Failover-Clusters zunächst Systemrollen einzurichten.

Eine Liste der empfohlenen Betriebssysteme, Hardwarekomponenten und Treiber- oder Firmwareversionen für Dell Windows Server Failover-Cluster finden Sie in den *Support-Matrizen für Dell Clusterkonfiguration* unter [dell.com/ha](http://dell.com/ha).

Weitere Informationen zum Bereitstellen eines Clusters mit Windows Server 2008 finden Sie im *Installations- und Fehlerbehebungshandbuch für Dell Failover-Cluster unter Microsoft Windows Server 2008* unter [support.dell.com/manuals](http://support.dell.com/manuals).

In den folgenden Unterabschnitten werden die Schritte beschrieben, über die Sie die Kommunikation zwischen den Clusterknoten und einem oder mehreren freigegebenen MD3200i / MD3220i Speicherarray(s) einrichten und Laufwerke des/der Speicherarrays für den Cluster präsent machen können.

1. [Installation des iSCSI-NICs.](#)
2. [Installation des Microsoft iSCSI-Software-Initiators.](#)
3. [Installieren und Konfigurieren der Speicherverwaltungssoftware.](#)
4. [Konfiguration des gemeinsamen Speichersystems.](#)
5. [Konfigurieren eines Failover-Clusters.](#)

## Installation des iSCSI-NICs

Es wird empfohlen, die neueste unterstützte Version des Treibers zu installieren. Wenn der NIC-Treiber die Installation von Service-Packs oder Hotfixes für das Betriebssystem erfordert, installieren Sie zunächst diese.

Eine Liste der empfohlenen Betriebssysteme, Hardwarekomponenten und Treiber- oder Firmwareversionen für Dell Windows Server Failover-Cluster finden Sie in den *Support-Matrizen für Dell Clusterkonfiguration* unter [dell.com/ha](http://dell.com/ha).

## Aktivieren von TOE-NICs

Die TOE nimmt die TCP/IP Pakete, die von dem/den Prozessor(en) des Systems verarbeitet werden sollen, und lädt sie beim NIC ab. Sie entlastet den Hauptprozessor und den Arbeitsspeicher und beugt so Engpässen durch intensiven Netzwerk-Datenverkehr vor. TOE-NICs verbessern die Performance bei iSCSI-Datenverkehr.

 **ANMERKUNG:** Bei iSCSI-Datenverkehr müssen in allen Knoten in einer Clusterlösung NICs desselben Typs eingesetzt werden - also entweder TOE-NICs oder Standard-NICs. Die Kombination von TOE-NICs und regulären NICs wird bei einer Clusterlösung nicht unterstützt.

Bevor Sie die Microsoft Failover-Clusterunterstützung installieren, müssen Sie zunächst die öffentlichen, privaten und iSCSI-Netzwerke in jedem Knoten konfigurieren. In den folgenden Abschnitten sind die Prinzipien und Vorgehensweisen bei der Netzwerkkonfiguration beschrieben.

 **ANMERKUNG:** Wenn die iSCSI-Netzwerke nicht für DHCP konfiguriert sind, müssen statische IP-Adressen verwendet werden. Damit die iSCSI-Anschlüsse des Speichersystems vollständig genutzt werden können, sind die IP-Adressen so konfiguriert, dass der Zugriff auf die einzelnen iSCSI-Ports auf die Clusterknoten verteilt wird. Wenn das Speichersystem beispielsweise die vier Subnetze .10, .11, .12 und .13 hat, kann sich folgende Aufteilung ergeben: Die beiden iSCSI-NICs am ersten Clusterknoten befinden sich in den Subnetzen .10 und .11, die beiden NICs am zweiten Clusterknoten in den Subnetzen .12 und .13, die beiden iSCSI-NICs am dritten Clusterknoten in den Subnetzen .10 und .11 und der vierte Clusterknoten in den Subnetzen .12 und .13.

## Installation des Microsoft iSCSI-Software-Initiators

Der Microsoft iSCSI-Initiator ist unter Windows Server 2008 direkt installiert.

## Installieren und Konfigurieren der Speicherverwaltungssoftware

Das Installationsprogramm für die PowerVault MD3200i / MD3220i Speichersoftware stellt unter anderem die Kernsoftware, Provider und optionale Hilfsprogramme bereit.

Die Kernsoftware enthält den hostbasierten Speicheragenten, den Multipath-Treiber und die Anwendung MDSM zu Konfiguration, Verwaltung und Überwachung der Speicherarray-Lösung.

Provider sind für die Microsoft VDS (Virtual Disk Service) und Microsoft VSS (Volume Shadow-Copy Service)-Frameworks sowie für den SMI-S-Standard (SNIA

Storage Management Initiative Specification) verfügbar.

MDCU (Modular Disk Configuration Utility) ist ein optionales Hilfsprogramm, das einen konsolidierten Ansatz für die Konfiguration der Verwaltungsports und der iSCSI-Hostports sowie für die Erstellung von Sitzungen für die modularen iSCSI-Festplatten-Speicherarrays bietet. Es wird empfohlen, MDCU für die iSCSI-Konfiguration auf jedem Host zu verwenden, der mit dem PowerVault MD3200i / MD3220i verbunden ist.

 **ANMERKUNG:** Weitere Informationen über die Provider für Microsoft VDS und Microsoft VSS finden Sie im Benutzerhandbuch. Weitere Informationen zur Arbeit mit dem SMI-S-Provider finden Sie im SMI-S Programmer's Guide (Programmierhandbuch für SMI-S).

## Installation der Speicherverwaltungs-Software

1. Schließen Sie alle anderen Programme, bevor Sie neue Software installieren.
2. Legen Sie den Resource-Datenträger ein.
3. Wählen Sie die Option **MD32xxi-Storage-Software installieren** aus.
4. Installieren Sie die MD Storage Software.
5. Wählen Sie eine der folgenden Installationsoptionen:
  - o Vollständig (empfohlen) - Dieses Paket installiert die Hauptsoftware, Anbieter und Programme. Dazu zählen der benötigte hostbasierte Speicheragent, der Multipath-Treiber, MD Storage Manager, Provider und optionale Programme.
  - o Nur Host - Dieses Paket umfasst den hostbasierten Speicheragent, Multipath-Treiber und optionale Programme zum Konfigurieren des Hosts.
  - o Verwaltungsstation - Dieses Paket umfasst MD-Storage-Manager, Provider und optionale Programme.
  - o Benutzerdefiniert - Mithilfe dieser Option können Sie bestimmte Komponenten auswählen.
6. Führen Sie einen Neustart der einzelnen Hostserver durch.

Ein Speicherarray lässt sich auf zwei Weisen verwalten:

- 1 Bandexterne Verwaltung
- 1 Bandinterne Verwaltung

 **ANMERKUNG:** Es wird empfohlen, die bandexterne Verwaltung zu verwenden.

## Konfiguration des gemeinsamen Speichersystems

Bevor Sie mit der Konfiguration von iSCSI beginnen, sollten Sie das [iSCSI-Konfigurationsarbeitsblatt](#) ausfüllen. Das Erfassen der relevanten Informationen über Ihr Netzwerk vor Durchführung der Konfigurationsschritte trägt dazu bei, den Zeitaufwand für den gesamten Prozess zu verkürzen.

### Terminologie

Die nachstehende Tabelle erläutert die Begriffe, die in den iSCSI-Konfigurationsschritten weiter unten in diesem Abschnitt verwendet werden.

**Tabelle 3-1. Wichtige Standardterminologie für die iSCSI-Konfiguration**

Begriff	Definition
CHAP (Challenge Handshake Authentication Protocol)	Ein optionales Sicherheitsprotokoll, das den Zugriff auf ein iSCSI-Speichersystem kontrolliert, indem es <b>Nutzungsbeschränkungen für die iSCSI-Datenports</b> am Hostserver und am Speicherarray einrichtet.
Host oder Hostserver	Ein Server, der über iSCSI-Ports mit dem Speicherarray verbunden ist.
Hostserver-Port	Der iSCSI-Port am Hostserver, über den die Verbindung zum Speicherarray hergestellt wird.
iSCSI-Initiator	Die auf dem Hostserver installierte iSCSI-spezifische Software, die die Kommunikation zwischen Hostserver und Speicherarray steuert.
iSCSI-Speicherport	iSCSI-Port am Speicherarray (vier je Controller).
iSNS (Microsoft Internet Storage Naming Service)	Ein Dienst zur automatisierten Erkennung, Verwaltung und Konfiguration, der von einigen iSCSI-Geräten <b>genutzt</b> wird.
Verwaltungsstation	Das System, von dem aus die Hostserver/Speicherarray-Konfiguration verwaltet wird.
Speicherarray	Das Gehäuse, auf dem sich die Speicherdaten befinden, auf die der Hostserver zugreift.
Target	Ein iSCSI-Port am Speicherarray, der Anfragen von dem auf dem Hostserver installierten iSCSI-Initiator entgegennimmt und darauf reagiert.

### Verwenden von iSNS (Internet Storage Naming Service) Server

Mit iSNS (Internet Storage Naming Service) Server ist es nicht mehr notwendig, jedes einzelne Speicherarray mit einer spezifischen Liste von Initiatoren und

Target-IP-Adressen manuell zu konfigurieren. iSNS erkennt, verwaltet und konfiguriert alle in der Netzwerkumgebung vorhandenen iSCSI-Geräte automatisch.

Weitere Informationen zu iSNS sowie Hinweise zu Installation und Konfiguration finden Sie unter [www.microsoft.com](http://www.microsoft.com).

## Konfiguration von iSCSI auf dem Speicherarray

Die folgenden Abschnitte enthalten Schritt-für-Schritt-Anleitungen zur Konfiguration von iSCSI auf dem Speicherarray. Vor dem Beginn müssen Sie wissen, wo in Ihrer Hostserver/Speicherarray-Umgebung die einzelnen Arbeitsschritte jeweils durchgeführt werden.

[Tabelle 3-2](#) enthält die Reihenfolge der Schritte und die jeweilige Ortsangabe zur Konfiguration der spezifischen iSCSI-Verbindungen. In den nachfolgenden Unterabschnitten werden die einzelnen Schritte näher erläutert.

**Tabelle 3-2. Hostserver vs. Speicherarray**

Dieser Schritt wird am HOSTSERVER über den Microsoft-iSCSI-Initiator durchgeführt:	Dieser Schritt wird am SPEICHERARRAY mit MD Storage Manager durchgeführt:
	1. Erkennung des Speicherarrays 2. Konfiguration der iSCSI-Port-Authentifizierung am Speicherarray
3. Durchführung der Target-Erkennung vom iSCSI-Initiator aus	
	4. Konfiguration des Hostzugriffs 5. (Optional) Konfigurieren von CHAP
6. (Optional) Konfiguration der CHAP-Authentifizierung am Hostserver 7. Verbindungsaufbau vom Hostserver zum Target-Speicherarray	
	8. (Optional) Einrichten der bandinternen Verwaltung

Das Hilfsprogramm MDCU stellt eine assistentengeführte Benutzerschnittstelle zur koordinierten Konfiguration des iSCSI-Hostservernetzwerks und der iSCSI-basierten Modular-Disk-Speicherarrays (PowerVault MD32xxi) bereit. Zudem ermöglicht es die Best-Practice-konforme Konfiguration der iSCSI-Sitzungen des Hostservers und die Einrichtung von Lastausgleichspfaden mit den iSCSI-Hostports des Speicherarrays.

 **ANMERKUNG:** Die von diesem Hilfsprogramm durchgeführten Konfigurationsaufgaben können auch manuell vorgenommen werden. Die Anleitung für die manuelle Konfiguration finden Sie in Anhang A - Manuelle Konfiguration des Bereitstellungshandbuchs für Dell PowerVault MD3220i / MD3200i Speicherarrays.

Das Hilfsprogramm MDCU wird nach der Installation von MDSM automatisch gestartet, sofern bei der Installation der Hostsoftware die Option **Launch the MDCU After Reboot** (MDCU nach Neustart aufrufen) ausgewählt wurde. Das Programm lässt sich auch manuell aufrufen.

MDCU führt die beiden folgenden wichtigen Aufgaben durch:

- 1 Speicherarray-Konfiguration
- 1 Hostkonfiguration

So konfigurieren Sie das/die iSCSI-basierten MD Speicherarray(s) mit MDCU:

1. Falls MDCU nicht bereits automatisch gestartet wurde, starten Sie es von dem Server, über den Sie auf die Verwaltungsschnittstellen des/der zu konfigurierenden Speicherarray(s) zugreifen.
2. Unter Windows: Klicken Sie auf **Start**→ **Alle Programme**→ **Dell**→ **MD Storage Software**→ **Modular Disk Configuration Utility**.
3. Unter Linux: Klicken Sie auf das MDCU-Symbol auf dem Desktop oder navigieren Sie in einem Terminalfenster zum Verzeichnis `/opt/dell/mdstoragesoftware/mdconfigurationutility` und führen Sie MDCU aus.
4. Klicken Sie auf **Next** (Weiter), um fortzufahren.
5. Wählen Sie **Configure Modular Disk Storage Array** (MD-Speicherarray konfigurieren) und klicken Sie auf **Next** (Weiter), um fortzufahren.
6. Wählen Sie Methode, mit der das Hilfsprogramm die zu konfigurierenden Speicherarrays erkennen soll und klicken Sie auf **Next** (Weiter).
  - 1 Automatic Discovery (Automatische Erkennung) - Bei der automatischen Erkennung werden alle iSCSI-basierten MD-Speicherarrays im lokalen Teilnetzwerk abgefragt. Dies kann einige Minuten dauern.
  - 1 Manual Discovery (Manuelle Erkennung) - Über die manuelle Erkennung können Sie iSCSI-basierte MD-Speicherarrays außerhalb des lokalen Teilnetzwerks lokalisieren. Dabei müssen Sie angeben, ob Ihr Speicherarray über einen einzelnen Controller (Simplexkonfiguration) oder zwei Controller (Duplexkonfiguration) verfügt und ob die Kommunikation mit der Verwaltungsschnittstelle des Speicherarrays über das Protokoll IPv4 oder IPv6 erfolgen soll.

Der folgende Bildschirm zeigt eine Liste der iSCSI-basierten MD-Speicherarrays an, die mit dem in [Schritt 3](#) ausgewählten Verfahren erkannt wurden. Wenn die automatische Erkennung (**Automatic Discovery**) ausgewählt wurde, erscheint eine Liste der im Teilnetzwerk erkannten iSCSI-basierten MD-Speicherarrays. Wenn die Manuelle Erkennung (**Manual Discovery**) ausgewählt wurde, enthält die Liste nur das Array, dessen IP-Adresse angegeben wurde. Um weitere Arrays zur Liste hinzuzufügen, klicken Sie auf diesem Bildschirm auf **Add** (Hinzufügen).

7. Klicken Sie auf die Optionsschaltfläche neben dem Speicherarray, das Sie auswählen möchten, und klicken Sie anschließend auf **Next** (Weiter).
8. Geben Sie den Namen des Speicherarrays und das Kennwort ein.
9. Wenn Sie ein neues Kennwort für das Array festlegen möchten, klicken Sie auf das Kontrollkästchen **Set Password** (Kennwort festlegen). Tragen Sie anschließend das neue Kennwort in den Feldern **New Password** (Neues Kennwort) und **Confirm New Password** (Neues Kennwort bestätigen) ein. Klicken Sie auf **Next** (Weiter), um fortzufahren.
10. Wählen Sie das IP-Protokoll für die Kommunikation über die Verwaltungsschnittstellen aus (IPv4/IPv6). Geben Sie zudem für jedes Protokoll an, ob die IP-Adressen der Verwaltungsschnittstellen manuell oder automatisch konfiguriert werden müssen. Weitere Informationen finden Sie in der Online-Hilfe.
11. Klicken Sie auf **Next** (Weiter), um fortzufahren. Wenn Sie für keines der beiden Protokolle die Option **Specify Configuration Manually** (Konfiguration manuell festlegen) ausgewählt haben, fahren Sie mit [Schritt 13](#) fort.
12. Wenn Sie für eines der beiden im letzten Schritt genannten Protokolle die Option **Specify Configuration Manually** ausgewählt haben, werden mehrere aufeinander folgende Bildschirme angezeigt, die Backend-Darstellungen der Speicherarray-Controller zeigen. Jede Darstellung enthält IP-Adressen der Controller-Verwaltungsschnittstellen. Zudem ist auf jeder Darstellung eine Verwaltungsschnittstelle rot hervorgehoben.
  - 1 Um die IPv4-Adresse der hervorgehobenen Verwaltungsschnittstelle zu ändern, geben Sie IP-Adresse, Teilnetzmaske und Gateway-Adresse in die unter dem Bild befindlichen Felder ein.
  - 1 Um die IPv6-Adresse der hervorgehobenen Verwaltungsschnittstelle zu ändern, geben Sie die lokale IP-Adresse, die weiterleitbare IP-Adresse und die Router-IP-Adresse in die unter dem Bild befindlichen Felder ein.

Klicken Sie auf **Next** (Weiter), um die Darstellungen weiter durchzugehen und die Konfiguration aller Verwaltungsschnittstellen für die ausgewählten Protokolle fertig zu stellen.
13. Wählen Sie im Bildschirm **CHAP Configuration** (CHAP-Konfiguration) die CHAP-Methode und klicken Sie auf **Next** (Weiter). Weitere Informationen zu CHAP finden Sie unter [Funktionsweise der CHAP-Authentifizierung](#).
14. Prüfen Sie im Bildschirm **Summary** (Übersicht) die von Ihnen eingegebenen Informationen zum Speicherarray.
15. Klicken Sie auf **Apply** (Anwenden), um die Änderungen am Array zu speichern.

 **ANMERKUNG:** Klicken Sie auf **Cancel Array** (Abbrechen), um die Konfiguration des Speicherarrays abzubrechen und ein anderes Speicherarray für die Konfiguration auszuwählen.

16. Geben Sie im Bildschirm **Configure Additional Arrays** an, ob Sie weitere Arrays konfigurieren möchten. Klicken Sie auf **Next** (Weiter), um fortzufahren.
17. Wenn Sie in [Schritt 16](#) **Yes** (Ja) gewählt haben, wiederholen Sie [Schritt 6](#) bis [Schritt 15](#), um ein weiteres Array zu konfigurieren.

Wenn Sie in [Schritt 16](#) **No** (nein) gewählt haben, führen Sie im Bildschirm **Configure Host Connectivity** (Hostverbindungen konfigurieren) die folgenden Schritte durch:

- a. Legen Sie fest, ob Sie die Verbindungen für den iSCSI-Initiator des aktuellen Hosts konfigurieren möchten.
- b. Klicken Sie auf **Next** (Weiter), um fortzufahren.
- c. Klicken Sie auf **No** (Nein), um die Konfigurationsaufgabe abzuschließen und mit [Schritt f](#) fortzufahren.
- d. Klicken Sie auf **Yes** (Ja), um die Verbindungen für den iSCSI-Initiator des aktuellen Hosts zu konfigurieren. Der Bildschirm **Select Storage Array** (Speicherarray auswählen) wird angezeigt.
- e. Wählen Sie das Speicherarray, das Sie für die Verbindung zum lokalen Host konfigurieren möchten.
- f. Klicken Sie im letzten Bildschirm auf **Finish** (Fertig stellen), um das Hilfsprogramm zu beenden.

 **ANMERKUNG:** Die Namen der gerade über das Hilfsprogramm konfigurierten Speicherarrays werden in der Liste mit dem Hinweis **Configuration Complete** (Konfiguration abgeschlossen) gekennzeichnet. Daran erkennen Sie sofort, welche Arrays bereit sind, um für den Hostzugriff konfiguriert zu werden.

18. Führen Sie im Bildschirm **Storage Array Login** (Anmeldung beim Speicherarray) die folgenden Schritte durch:
  - a. Wählen Sie in der Spalte **Controller#** (Controllernr.) den iSCSI-Hostport des Speicherarrays, das Sie konfigurieren möchten sowie die IP-Adressen aus.
  - b. Wählen Sie in der Spalte **Host Address** (Hostadresse) die Host-IP-Adresse aus, die sich beim iSCSI-Hostport des Speicherarrays anmelden muss.
  - c. Klicken Sie auf **Next** (Weiter), um die Anmeldeinformationen für einen weiteren Controller einzugeben oder auf **Apply** (Übernehmen), um die Anmeldeinformationen zu übermitteln.
19. Wählen Sie im Bildschirm **Connect to Additional Arrays** aus, ob Sie eine Verbindung zu einem weiteren Speicherarray konfigurieren möchten. Um eine Verbindung zu einem weiteren Speicherarray zu konfigurieren, wiederholen Sie die obenstehenden Schritte von [Schritt d](#) an. Wenn Sie keine Verbindungen zu weiteren Speicherarrays konfigurieren möchten, klicken Sie im letzten Bildschirm auf **Finish** (Fertig stellen), um das Hilfsprogramm zu beenden.

## Funktionsweise der CHAP-Authentifizierung

Bevor Sie mit [Konfiguration der CHAP-Authentifizierung am Speicherarray \(optional\)](#) oder [Konfiguration der CHAP-Authentifizierung am Hostserver \(optional\)](#) fortfahren, sollten Sie sich hier einen Überblick über die Funktionsweise der CHAP-Authentifizierung verschaffen.

## Was ist CHAP?

CHAP (Challenge Handshake Authentication Protocol) ist ein optionales iSCSI-Authentifizierungsverfahren, bei dem das Speicherarray (Target) iSCSI-Initiatoren am Hostserver authentifiziert. Es werden zwei Arten von CHAP unterstützt: *Target-CHAP* und *Mutual* (gegenseitiges) CHAP.

## Target-CHAP

Beim Target-CHAP-Verfahren authentifiziert das Speicherarray alle von dem/den iSCSI-Initiatoren ausgesandten Zugriffsanfragen für den Hostserver über ein CHAP-Secret. Um die Target-CHAP-Authentifizierung einzurichten, geben Sie zunächst am Speicherarray ein CHAP-Secret ein. Anschließend konfigurieren Sie die einzelnen iSCSI-Initiatoren am Hostserver so, dass sie das CHAP-Secret bei jedem Versuch, auf das Speicherarray zuzugreifen, übermitteln.

## Mutual (gegenseitiges) CHAP

Als Erweiterung des Target-CHAP-Verfahrens können Sie die gegenseitige CHAP-Authentifizierung einrichten. Bei diesem Verfahren erfolgt die Authentifizierung vonseiten des Speicherarrays *und* vonseiten des iSCSI-Initiators. Um die gegenseitige CHAP-Authentifizierung einzurichten, konfigurieren Sie am iSCSI-Initiator ein CHAP-Secret, das das Speicherarray an den Hostserver übermitteln muss, um eine Verbindung aufbauen zu können. Bei dieser Zwei-Wege-Authentifizierung müssen sowohl der Hostserver als auch das Speicherarray Informationen übermitteln, die von der jeweils anderen Seite validiert werden. Erst danach kann eine Verbindung aufgebaut werden.

Die CHAP-Authentifizierung ist ein optionales Merkmal, das für den Betrieb von iSCSI nicht erforderlich ist. Wenn Sie die CHAP-Authentifizierung nicht einrichten, kann jedoch jeder Hostserver, der an dasselbe IP-Netzwerk angeschlossen ist, Daten vom Speicherarray lesen und darauf schreiben.

 **ANMERKUNG:** Wenn Sie sich für die Nutzung der CHAP-Authentifizierung entscheiden, müssen Sie sie zunächst sowohl am Speicherarray (mit MD Storage Manager) als auch am Hostserver (mit dem iSCSI-Initiator) konfigurieren, bevor Sie die virtuellen Laufwerke für die Aufnahme von Daten vorbereiten. Wenn Sie die Datenträger zur Aufnahme von Daten vorbereiten, bevor Sie die CHAP-Authentifizierung einrichten, sind die Datenträger nach der CHAP-Konfiguration nicht mehr sichtbar.

## CHAP-Definitionen

[Tabelle 3-3](#) enthält eine Übersicht der Unterschiede zwischen Target-CHAP- und gegenseitiger CHAP-Authentifizierung.

**Tabelle 3-3. Definierte CHAP-Typen**

CHAP-Typ	Beschreibung
Target-CHAP	Es werden Zugriffskonten eingerichtet, über die die iSCSI-Initiatoren die Verbindung zum Target-Speicherarray aufbauen. Anschließend authentifiziert das Target-Speicherarray den iSCSI-Initiator.
Mutual (gegenseitiges) CHAP	Wird als Erweiterung des Target-CHAP-Verfahrens eingesetzt. Bei der gegenseitigen CHAP-Authentifizierung wird ein Zugriffskonto eingerichtet, über das ein Target-Speicherarray eine Verbindung zum iSCSI-Initiator aufbaut. Anschließend wird der iSCSI-Initiator vom Target authentifiziert.

## Einrichten der CHAP-Authentifizierung

Die beiden folgenden iSCSI-Konfigurationsschritte, [Konfiguration der CHAP-Authentifizierung am Speicherarray \(optional\)](#) und [Konfiguration der CHAP-Authentifizierung am Hostserver \(optional\)](#), enthalten Schritt-für-Schritt-Anleitungen zur Einrichtung der CHAP-Authentifizierung am Speicherarray und am Hostserver.

### Konfiguration der CHAP-Authentifizierung am Speicherarray (optional)

Wenn Sie ausschließlich die Target-CHAP-Authentifizierung konfigurieren, führen Sie [Konfiguration der CHAP-Authentifizierung am Speicherarray \(optional\)](#) und [Konfiguration der CHAP-Authentifizierung am Hostserver \(optional\)](#) durch.

Wenn Sie die gegenseitige CHAP-Authentifizierung konfigurieren, führen Sie [Konfiguration der gegenseitigen CHAP-Authentifizierung am Speicherarray](#) und [Konfiguration der CHAP-Authentifizierung am Hostserver \(optional\)](#) durch.

Wenn Sie **keine** CHAP-Authentifizierung einrichten, fahren Sie mit [Konfigurieren eines Failover-Clusters](#) fort.

 **ANMERKUNG:** Wenn Sie gegenseitige CHAP-Authentifizierung einrichten möchten, müssen Sie zunächst die Target-CHAP-Authentifizierung konfigurieren.

Denken Sie daran, dass sich der Begriff *Target* bei der iSCSI-Konfiguration immer auf das Speicherarray bezieht.

### Konfiguration der Target-CHAP-Authentifizierung am Speicherarray

1. Klicken Sie in MD Storage Manager auf das Register **iSCSI**, und wählen Sie anschließend **Change Target Authentication** (Target-Authentifizierung ändern).

Wählen Sie eine der folgenden Optionen aus:

Tabelle 3-4. CHAP-Einstellungen

Auswahl	Beschreibung
NONE	Dies ist die Standardeinstellung. Wenn <b>None</b> (Keine) die einzige Auswahl ist, kann sich jeder iSCSI-Initiator am Speicherarray anmelden, ohne CHAP-Authentifizierungsdaten irgendeiner Art zu übermitteln.
None (Keine) und CHAP	Bei dieser Einstellung können sich iSCSI-Initiatoren mit oder ohne CHAP-Authentifizierung am Speicherarray anmelden.
CHAP	Wenn <b>CHAP</b> ausgewählt und <b>None</b> (Keine) deaktiviert wurde, fordert das Speicherarray CHAP-Authentifizierung an, bevor es Zugriff gewährt.

- Um ein CHAP-Secret zu konfigurieren, wählen Sie **CHAP** und anschließend **CHAP Secret** (CHAP-Secret).
- Geben Sie das **Target CHAP Secret** ein (oder wählen Sie **Generate Random Secret**), um das Secret zufallsgesteuert zu generieren), bestätigen Sie es unter **Confirm Target CHAP Secret**, und klicken Sie auf **OK**.

Viele iSCSI-Initiatoren unterstützen für das CHAP-Secret nur bis zu 16 Zeichen (128 Bit), obwohl das Speicherarray 12 bis 57 Zeichen zulässt.

 **ANMERKUNG:** Ein einmal eingegebenes CHAP-Secret ist nicht wieder abrufbar. Notieren Sie sich deshalb das CHAP-Secret, und bewahren Sie es an einem gut zugänglichen Ort auf. Wenn die Option **Generate Random Secret** verwendet wird, kopieren Sie das generierte Secret zur späteren Verwendung in eine Textdatei, da dasselbe CHAP-Secret zur Authentifizierung neuer Hostserver dient, die Sie ggf. später zum Speicherarray hinzufügen möchten. Wenn Sie das CHAP-Secret vergessen, müssen Sie alle mit dem Speicherarray verbundenen Hosts von diesem trennen und die in diesem Kapitel beschriebenen Schritte erneut durchführen, um sie wieder hinzuzufügen.

- Klicken Sie auf **OK**.

#### Konfiguration der gegenseitigen CHAP-Authentifizierung am Speicherarray

Das Initiator-Secret muss für jeden Hostserver, der auf das Speicherarray zugreift, eindeutig sein und darf nicht mit dem Target-CHAP-Secret übereinstimmen.

- Klicken Sie in MD Storage Manager auf das Register **iSCSI** und wählen Sie anschließend **Enter Mutual Authentication Permissions** (Berechtigungen für gegenseitige Authentifizierung eingeben).
- Wählen Sie einen Initiator am Hostserver aus und klicken Sie auf **CHAP Secret** (CHAP-Secret).
- Geben Sie unter **Initiator CHAP Secret** das CHAP-Secret für den Initiator ein, bestätigen Sie es unter **Confirm Initiator CHAP Secret** (Initiator CHAP-Secret bestätigen) und klicken Sie auf **OK**.

 **ANMERKUNG:** Es kann vorkommen, dass bereits ein Initiator-CHAP-Secret in Ihrer Konfiguration definiert ist. In diesem Fall verwenden Sie es hier.

- Klicken Sie auf **Schließen**.

 **ANMERKUNG:** Um ein CHAP-Secret zu entfernen, müssen Sie den Host-Initiator löschen und erneut hinzufügen.

#### Konfiguration der CHAP-Authentifizierung am Hostserver (optional)

Führen Sie die folgenden Schritte nur durch, wenn Sie in [Konfiguration der CHAP-Authentifizierung am Speicherarray \(optional\)](#) die CHAP-Authentifizierung konfiguriert haben. Andernfalls fahren Sie mit [Konfigurieren eines Failover-Clusters](#) fort.

So konfigurieren Sie die optionale CHAP-Authentifizierung am Hostserver:

- Klicken Sie auf **Start** → **Programme** → **Microsoft iSCSI Initiator**.
- Wenn Sie die gegenseitige CHAP-Authentifizierung nicht verwenden, fahren Sie mit [Schritt 4](#) fort.
- Wenn Sie die gegenseitige CHAP-Authentifizierung verwenden:
  - Klicken Sie auf die Registerkarte **General** (Allgemein).
  - Wählen Sie **Secret**.
  - Tragen Sie im Fenster **Enter a secure secret** (Geben Sie eine sichere Secret-Kennung ein) das CHAP-Secret zur gegenseitigen Authentifizierung ein, das Sie für das Speicherarray eingegeben haben.
- Klicken Sie auf die Registerkarte **Discovery** (Suche).
- Wählen Sie unter **Target Portals** (Target-Portale) die IP-Adresse des iSCSI-Ports am Speicherarray und klicken Sie auf **Remove** (Entfernen).

Der iSCSI-Port, der bei der Target-Erkennung am Speicherarray konfiguriert wurde, sollte nun verschwinden. Sie müssen diese IP-Adresse bei aktiver CHAP-Authentifizierung zurücksetzen. Folgen Sie dazu den nachstehenden Schritten.

6. Klicken Sie unter **Target Portals** (Target-Portale) auf **Add** (Hinzufügen) und geben Sie die **IP-Adresse oder den DNS-Namen** des (oben gelöschten) iSCSI-Ports am Speicherarray ein.
7. Klicken Sie auf **Advanced** (Erweitert) und legen Sie auf der Registerkarte **General** (Allgemein) die folgenden Werte fest:
  - 1 **Local Adapter** (Lokaler Adapter): Stellen Sie für diese Option immer den Wert **Microsoft iSCSI Initiator** ein.
  - 1 **Source IP**: (Quell-IP-Adresse) Die Quell-IP-Adresse des Hosts, zu dem eine Verbindung hergestellt werden soll.
  - 1 **Data Digest and Header Digest** (Daten- und Headerdigest): Auf Wunsch können Sie festlegen, dass bei der Übertragung ein Digest mit Daten- oder Headerinformationen kompiliert wird, der die Fehlerbehebung erleichtert.
  - 1 **CHAP logon information** (CHAP-Anmeldeinformationen): Tragen Sie Benutzername und Secret für die Target-CHAP-Authentifizierung ein, die Sie (für den Hostserver) am Speicherarray eingegeben haben.
  - 1 **Perform mutual authentication** (Gegenseitige Authentifizierung durchführen): Aktivieren Sie diese Option, wenn die gegenseitige CHAP-Authentifizierung konfiguriert wurde.

 **ANMERKUNG:** IPSec wird nicht unterstützt.

8. Klicken Sie auf **OK**.

Wenn Failover für Erkennungssitzungen erwünscht ist, wiederholen Sie [Schritt 5](#) und [Schritt 6](#) für alle iSCSI-Ports des Speicherarrays. Andernfalls ist die Konfiguration an einem einzelnen Hostport ausreichend.

 **ANMERKUNG:** Wenn die Verbindung nicht funktioniert, überprüfen Sie, ob alle IP-Adressen korrekt eingegeben wurden. Verbindungsprobleme sind häufig auf fehlerhaft eingegebene IP-Adressen zurückzuführen.

## Verbindungsaufbau vom Hostserver zum Target-Speicherarray

1. Klicken Sie auf **Start** → **Programme** → **Microsoft iSCSI Initiator**.
  2. Klicken Sie auf die Registerkarte **Targets**.  
Wenn die vorige Target-Erkennung erfolgreich verlaufen ist, sollte die *iqn* des Speicherarrays unter **Targets** angezeigt werden.
  3. Klicken Sie auf **Log On** (Anmelden).
  4. Wählen Sie **Automatically restore this connection when the system boots** (Verbindung bei Systemneustart automatisch wiederherstellen).
  5. Wählen Sie **Enable multipath** (Multipath aktivieren).
  6. Klicken Sie auf **Advanced** (Erweitert) und nehmen Sie auf der Registerkarte **General** (Allgemein) die folgenden Einstellungen vor:
    - 1 **Local Adapter** (Lokaler Adapter): Stellen Sie für diese Option den Wert **Microsoft iSCSI-Initiator** ein.
    - 1 **Source IP**: Die Quell-IP-Adresse des Hostservers, von dem aus eine Verbindung hergestellt werden soll.
    - 1 **Target Portal** (Target-Portal): Wählen Sie den iSCSI-Port des Speicherarray-Controllers aus, zu dem eine Verbindung hergestellt werden soll.
    - 1 **Data Digest and Header Digest** (Daten- und Headerdigest): Auf Wunsch können Sie festlegen, dass bei der Übertragung ein Digest mit Daten- oder Headerinformationen kompiliert wird, der die Fehlerbehebung erleichtert.
    - 1 **CHAP logon information** (CHAP-Anmeldeinformationen): Wenn CHAP-Authentifizierung erforderlich ist, aktivieren Sie diese Option und geben Sie das **Target Secret** ein.
    - 1 **Perform mutual authentication** (Gegenseitige Authentifizierung durchführen): Aktivieren Sie diese Option, wenn die gegenseitige CHAP-Authentifizierung konfiguriert wurde.
-  **ANMERKUNG:** IPSec wird nicht unterstützt.
7. Klicken Sie auf **OK**.  
Um Failover der Speicherarray-Controller zu unterstützen, muss der Hostserver an jedem Controller mit mindestens einem iSCSI-Port verbunden sein. Wiederholen Sie [Schritt 3](#) bis [Schritt 8](#) für jeden iSCSI-Port am Speicherarray, der als Failover-Target eingerichtet werden soll (jeder Port, zu dem Sie eine Verbindung aufbauen, erhält eine eigene **Target Portal**-Adresse).  
Das **Status**-Feld auf der Registerkarte **Targets** wird als **Connected** (Verbunden) angezeigt.
  8. Klicken Sie auf **OK**, um den Microsoft iSCSI-Initiator zu schließen.

## Statusanzeige für iSCSI-Verbindungen

Wenn Sie in MD Storage Manager auf die Registerkarte **iSCSI** und anschließend auf **Configure iSCSI Host Ports** (iSCSI-Hostports konfigurieren) klicken, werden der Status jedes iSCSI-Ports, auf den ein Zugriffsversuch erfolgte, sowie der Konfigurationsstatus aller IP-Adressen angezeigt. Wenn der Status **Disconnected** (Nicht verbunden) bzw. **Unconfigured** (Nicht konfiguriert) angezeigt wird, überprüfen Sie die nachstehend aufgeführten Punkte, und wiederholen Sie die iSCSI-Konfigurationsschritte:

- 1 Sind alle Kabel fest mit den Ports am Hostserver und am Speicherarray verbunden?
- 1 Ist TCP/IP an allen Target-Hostports korrekt konfiguriert?
- 1 Wurde CHAP am Hostserver und am Speicherarray korrekt eingerichtet?

## Einrichten der bandinternen Verwaltung (optional)

Es wird empfohlen, das Speicherarray bandextern zu verwalten. Optional kann jedoch die bandinterne Verwaltung eingerichtet werden. Nehmen Sie dazu die folgende Konfiguration vor:

Controller 0: IP: 192.168.128.101 Subnetzmaske: 255.255.255.0

Controller 1: IP: 192.168.128.102 Subnetzmaske: 255.255.255.0

 **ANMERKUNG:** Die verwendete Verwaltungsstation muss für Netzwerkkommunikation für das gleiche IP-Subnetz wie die iSCSI-Hostports des PowerVault MD3200i / MD3220i-Speicherarrays konfiguriert sein.

1. Bauen Sie eine iSCSI-Sitzung zum MD3200i / MD3220i RAID- Speicherarray auf.
2. Starten Sie den Dienst SMagent neu.
3. Rufen Sie MD Storage Manager auf, und klicken Sie auf **New** (Neu).

 **ANMERKUNG:** Wenn Sie die erste Speicherarrayverwaltung einrichten, wird das Fenster **Add New Storage Array** (Neues Speicherarray hinzufügen) angezeigt.

4. Wählen Sie **Manual** (Manuell) und klicken Sie auf **OK**.
5. Wählen Sie **In-band management** (Bandinterne Verwaltung), und geben Sie den/die Hostservernamen oder IP-Adresse(n) des angeschlossenen Hosts an, auf dem MD Storage Manager ausgeführt wird.
6. Klicken Sie auf **Add** (Hinzufügen).

Die bandinterne Verwaltung ist nun fertig konfiguriert.

## Konfiguration des Hostzugriffs

Wenn der Host-Context-Agent auf den mit dem Speicherarray verbundenen Hosts läuft, werden Hosts und Hostports von MDSM automatisch erkannt und auf der Registerkarte **Mappings** (Zuweisungen) des Fensters **Array Management** (Arrayverwaltung) aufgelistet.

Falls der Host nicht erkannt wird:

1. Starten Sie MDSM.
2. Wechseln Sie zum Fenster **Array Management** und klicken Sie auf **Manually Define Hosts** (Hosts manuell definieren).
3. Geben Sie im Fenster **Enter Host Name** (Hostnamen eingeben) den Namen des Hostservers für die Zuweisung der virtuellen Laufwerke ein. Sie können diesen Namen frei wählen; es muss nicht unbedingt ein Name sein, der zur Identifikation des Hostservers im Netzwerk gebraucht wird.
4. Wählen Sie im Feld **Do you plan to use the storage partitions in this storage array?** (Sollen die Speicherpartitionen in diesem Speicherarray genutzt werden?) die zutreffende Antwort aus und klicken Sie auf **Next** (Weiter).

Das Fenster **Specify Host Port Identifiers** (Hostport-Kennungen festlegen) wird angezeigt.

 **ANMERKUNG:** Wenn der Cluster das Speicherarray gemeinsam mit weiteren Clustern nutzt, wählen Sie Yes (Ja). Anderenfalls wählen Sie No (Nein).

5. Wählen Sie eine Methode zum Hinzufügen der Hostport-Kennung.
6. Wählen Sie den Hosttyp aus.
7. Legen Sie fest, ob der Hostserver Teil einer Hostservergruppe sein soll, die gemeinsam auf dieselben virtuellen Laufwerke zugreift. Wählen Sie nur dann **Yes** (Ja), wenn der Host Teil eines Microsoft-Clusters ist.
8. Klicken Sie auf **Next** (Weiter).
9. Legen Sie fest, ob dieser Host Teil einer Hostgruppe sein muss.
10. Klicken Sie auf **Finish** (Fertig stellen).

## Erstellen einer Hostgruppe

Eine Hostgruppe ist ein logischer Verbund von zwei oder mehreren Hosts, die den Zugriff auf spezifische virtuelle Laufwerke im Speicherarray gemeinsam nutzen.

So erstellen Sie Hostgruppen:

1. Wählen Sie im Fenster **Array Management** (Arrayverwaltung) das Register **Mappings** (Zuweisungen).
2. Wählen Sie im Feld **Topology** (Topologie) das Speicherarray oder die Standardgruppe aus.
3. Führen Sie eine der folgenden Aktionen aus:
  - o Wählen Sie **Mappings** → **Define** → **Host Group**.
  - o Klicken Sie mit der rechten Maustaste auf das Speicherarray oder **Default Group** (Standardgruppe) und wählen Sie im Popupmenü **Define** → **Host Group**.
4. Geben Sie im Feld **Enter new host group name** (Neuen Hostgruppennamen eingeben) einen Namen für die neue Hostgruppe ein.
5. Wählen Sie im Feld **Select Hosts to Add Area** (Hinzuzufügenden Host auswählen) die gewünschten Hosts aus und klicken Sie auf **Add** (Hinzufügen).
6. Klicken Sie auf **OK**. Die Hostgruppe wird zum Speicherarray hinzugefügt.

## Erstellen von Datenträgergruppen und virtuellen Laufwerken

In manchen Fällen sind die virtuellen Laufwerke bereits bei der Lieferung verbunden. Gleichwohl ist es wichtig, dass Sie die Verwaltungssoftware installieren und überprüfen, ob die gewünschte Konfiguration virtueller Laufwerke vorhanden ist.

Die Remote-Verwaltung der virtuellen Laufwerke ist über PowerVault Modular Disk Storage Manager möglich. Für eine Aktiv-Passiv-Clusterkonfiguration benötigen Sie mindestens ein virtuelles Laufwerk und für eine Aktiv-Aktiv-Clusterkonfiguration mindestens zwei virtuelle Laufwerke.

Datenträgergruppen werden im nicht konfigurierten Speicher des Speicherarrays erstellt, und virtuelle Laufwerke werden im verfügbaren Speicher einer Datenträgergruppe erstellt. Die mit dem Speicherarray verbundenen Hosts lesen und schreiben Daten auf das virtuelle Laufwerk.

 **ANMERKUNG:** Bevor Sie virtuelle Laufwerke erstellen können, müssen Sie zunächst die physischen Datenträger in Datenträgergruppen organisieren und den Hostzugriff konfigurieren. Danach lassen sich virtuelle Laufwerke in einer Datenträgergruppe erstellen.

Um ein virtuelles Laufwerk zu erstellen, gehen Sie nach einem der folgenden Verfahren vor:

- 1 Automatische Konfiguration
- 1 Manuelle Konfiguration

Um Datenträgergruppen mit der automatischen Konfiguration zu erstellen, folgen Sie der nachstehenden Anleitung:

1. Um den **Assistenten zum Erstellen von Datenträgergruppen** zu starten, führen Sie eine der nachstehenden Aktionen durch:
  - o Um eine Datenträgergruppe aus nicht konfigurierten Kapazitäten im Speicherarray zu erstellen: Wählen Sie auf der Registerkarte **Logical** (Logische Laufwerke) den Knoten **Unconfigured Capacity** (Unkonfigurierte Kapazität) aus und wählen Sie **Disk Group** → **Create**. Sie können auch mit der rechten Maustaste auf den Knoten **Unconfigured Capacity** (Unkonfigurierte Kapazität) klicken und im Popupmenü die Option **Create Disk Group** (Datenträgergruppe erstellen) auswählen.
  - o Um eine Datenträgergruppe aus nicht zugewiesenen physischen Datenträgern im Speicherarray zu erstellen: Wählen Sie auf der Registerkarte **Physical** (Physische Datenträger) einen oder mehrere nicht zugewiesene physische Datenträger aus und wählen Sie **Disk Group** → **Create**. Sie können auch mit der rechten Maustaste auf die nicht zugewiesenen physischen Datenträger klicken und im Popupmenü die Option **Create Disk Group** (Datenträgergruppe erstellen) auswählen.
  - o Um eine geschützte Datenträgergruppe zu erstellen: Wählen Sie auf der Registerkarte **Physical** (Physische Datenträger) einen oder mehrere nicht zugewiesene physische Datenträger mit Sicherheitsmerkmalen aus und wählen Sie **Disk Group** → **Create**. Sie können auch mit der rechten Maustaste auf die nicht zugewiesenen physischen Datenträger mit Sicherheitsmerkmalen klicken und im Popupmenü die Option **Create Disk Group** (Datenträgergruppe erstellen) auswählen. Das Fenster **Create Disk Group** wird angezeigt.
2. Klicken Sie auf **Next** (Weiter). Das Fenster **Disk Group Name and Physical Disk Selection** (Name der Datenträgergruppe und Auswahl physischer Datenträger) wird angezeigt.
3. Geben Sie im Feld **Disk Group Name** (Name der Datenträgergruppe) einen Namen für die Datenträgergruppe ein (bis zu 30 Zeichen).
4. Wählen Sie aus den folgenden Optionen die gewünschte Konfigurationsmethode zur Auswahl der physischen Datenträger:
  - o Automatisch (siehe [Schritt 6](#))
  - o Manuell (siehe [Schritt 7](#))
5. Klicken Sie auf **Next** (Weiter).
6. Bei Auswahl der automatischen Konfiguration wird das Fenster **RAID Level and Capacity** (RAID-Level und Kapazität) angezeigt.

- a. Wählen Sie im Feld **Select RAID Level** (RAID-Level auswählen) den gewünschten RAID-Level aus. Die verfügbaren RAID-Level sind 0, 1/10, 6 und 5. Die für den gewählten RAID-Level verfügbaren physischen Datenträger werden in der Tabelle **Select Capacity** (Kapazität auswählen) angezeigt.
  - b. Wählen Sie in der Tabelle **Select Capacity** die gewünschte Kapazität der Datenträgergruppe aus und klicken Sie auf **Finish** (Fertig stellen).
7. Bei Auswahl der manuellen Konfiguration wird das Fenster **Manual Physical Disk Selection** (Manuelle Auswahl physischer Datenträger) angezeigt.
- a. Wählen Sie im Feld **Select RAID Level** (RAID-Level auswählen) den gewünschten RAID-Level aus. Die verfügbaren RAID-Level sind 0, 1/10, 6 und 5. Die für den gewählten RAID-Level verfügbaren physischen Datenträger werden in der Tabelle **Unselected Physical Disks** (Nicht ausgewählte physische Datenträger) angezeigt.
  - b. Wählen Sie im Feld **Unselected Physical Disks** die gewünschten physischen Datenträger aus und klicken Sie auf **Add** (Hinzufügen).

 **ANMERKUNG:** Um mehrere physische Datenträger in einem Vorgang auszuwählen, halten Sie die Taste <Strg> oder <Umschalt> gedrückt und wählen Sie weitere physische Datenträger aus.

- 8. Klicken Sie auf **Calculate Capacity** (Kapazität berechnen), um die Kapazität der neuen Datenträgergruppe anzuzeigen.
- 9. Klicken Sie auf **Finish** (Fertig stellen). Es erscheint eine Bestätigungsmeldung, die darüber informiert, dass die Datenträgergruppe erfolgreich hinzugefügt wurde und dass mindestens ein virtuelles Laufwerk ausgewählt werden muss, damit die Kapazität der neuen Datenträgergruppe genutzt werden kann.

So erstellen Sie virtuelle Laufwerke:

1. Rufen Sie den **Assistenten zum Erstellen virtueller Laufwerke** mit einem der nachstehend beschriebenen Verfahren auf:
  - o Um ein virtuelles Laufwerk aus nicht konfigurierten Kapazitäten im Speicherarray zu erstellen: Wählen Sie auf der Registerkarte **Logical** (Logische Laufwerke) den Knoten **Unconfigured Capacity** (Unkonfigurierte Kapazität) aus und wählen Sie **Virtual Disk** → **Create**. Sie können auch mit der rechten Maustaste auf den Knoten **Unconfigured Capacity** (Unkonfigurierte Kapazität) klicken und im Popupmenü die Option **Create Virtual Disk** (Virtuelles Laufwerk erstellen) auswählen.
  - o Um ein virtuelles Laufwerk aus freien Kapazitäten auf einer Datenträgergruppe zu erstellen: Wählen Sie auf der Registerkarte **Logical** (Logische Laufwerke) den Knoten **Free Capacity** (Freie Kapazität) aus und wählen Sie **Virtual Disk** → **Create**. Sie können auch mit der rechten Maustaste auf den Knoten **Free Capacity** (Freie Kapazität) klicken und im Popupmenü die Option **Create Virtual Disk** (Virtuelles Laufwerk erstellen) auswählen.
  - o Um ein virtuelles Laufwerk aus nicht zugewiesenen physischen Datenträgern im Speicherarray zu erstellen: Wählen Sie auf der Registerkarte **Physical** (Physische Datenträger) einen oder mehrere nicht zugewiesene physische Datenträger aus und wählen Sie **Virtual Disk** → **Create**. Sie können auch mit der rechten Maustaste auf die nicht zugewiesenen physischen Datenträger klicken und im Popupmenü die Option **Create Virtual Disk** (Virtuelles Laufwerk erstellen) auswählen.
  - o Um ein geschütztes virtuelles Laufwerk zu erstellen: Wählen Sie auf der Registerkarte **Physical** (Physische Datenträger) einen oder mehrere nicht zugewiesene physische Datenträger mit Sicherheitsmerkmalen aus und wählen Sie **Virtual Disk** → **Create**. Sie können auch mit der rechten Maustaste auf die nicht zugewiesenen physischen Datenträger mit Sicherheitsmerkmalen klicken und im Popupmenü die Option **Create Virtual Disk** (Virtuelles Laufwerk erstellen) auswählen. Wenn Sie zum Erstellen eines virtuellen Laufwerks einen Knoten mit nicht konfigurierter Kapazität (**Unconfigured Capacity**) oder nicht zugewiesenen physischen Datenträgern auswählen, wird das Fenster **Disk Group Required** (Datenträgergruppe erforderlich) angezeigt. Klicken Sie auf **Yes** (Ja) und legen Sie mithilfe des **Create Disk Group Wizard** (Assistent zum Erstellen von Datenträgergruppen) eine Datenträgergruppe an. Nach dem Anlegen der Datenträgergruppe wird der **Create Virtual Disk Wizard** (Assistent zum Erstellen virtueller Laufwerke) angezeigt. Wenn Sie einen Knoten mit freier Kapazität (**Free Capacity**) anzeigen, wird das Fenster **Create Virtual Disk** (Virtuelles Laufwerk erstellen) angezeigt.
2. Klicken Sie auf **Next** (Weiter). Das Fenster **Specify Capacity/Name** (Kapazität/Name festlegen) wird angezeigt.
3. Wählen Sie die gewünschte Speichereinheit aus dem Listenmenü **Units** (Einheiten) aus, und geben Sie im Feld **New Virtual Disk Capacity** (Kapazität des neuen virtuellen Laufwerks) die Kapazität des virtuellen Laufwerks ein.
4. Geben Sie im Feld **Virtual Disk Name** (Name des virtuellen Laufwerks) einen beschreibenden Namen für das virtuelle Laufwerk ein (bis zu 30 Zeichen).
5. Im Feld **Advanced Virtual Disk Parameters** (Erweiterte Parameter für virtuelle Laufwerke) können Sie zwischen folgenden Optionen wählen:
  - o Use recommended settings. (Empfohlene Einstellungen verwenden.)
  - o Customize settings. (Einstellungen anpassen.)
6. Klicken Sie auf **Next** (Weiter).
7. Wählen Sie im Fenster **Customize Advanced Virtual Disk Parameters** (Erweiterte Parameter für virtuelle Laufwerke) die passenden E/A-Merkmale des virtuellen Laufwerks. Folgende Optionen stehen zur Auswahl:
  - o Dateisystem (typisch)
  - o Datenbank
  - o Multimedia
  - o Benutzerdefiniert

 **ANMERKUNG:** Wenn Sie die Option Custom (Benutzerdefiniert) wählen, müssen Sie eine geeignete Segmentgröße angeben.

- 8. Wählen Sie das bevorzugte RAID-Controllermodul aus.

Weitere Informationen zum Erstellen von Datenträgergruppen und virtuellen Laufwerken finden Sie im *Benutzerhandbuch zu Dell PowerVault Modular Disk Storage Manager* unter [support.dell.com/manuals](http://support.dell.com/manuals).

Es wird empfohlen, für jede Anwendung mindestens ein virtuelles Laufwerk zu erstellen. Wenn mehrere NTFS-Volumes mit der **Windows-Datenträgerverwaltung** auf einem einzigen virtuellen Laufwerk erstellt werden, erfolgt das Failover für diese Volumes gemeinsam anstatt individuell von Knoten zu Knoten.

 **ANMERKUNG:** Es wird empfohlen, einen anderen RAID-Level als RAID 0 (auch als Striping bezeichnet) zu verwenden. RAID 0-Konfigurationen bieten zwar eine sehr hohe Leistungsfähigkeit, können aber nicht die für Quorumressourcen benötigte Verfügbarkeit garantieren. Nähere Informationen zur Einrichtung der RAID-Levels für das System finden Sie in der Dokumentation des Speichersystems.

### Erstellen von Zuweisungen zwischen Hosts und virtuellen Laufwerken

So erstellen Sie Zuweisungen zwischen virtuellen Laufwerken und Hostgruppen, die Clusterknoten enthalten:

1. Wählen Sie im Fenster **Array Management** (Arrayverwaltung) das Register **Mappings** (Zuweisungen).
2. Wählen Sie im Feld **Topology** eine der folgenden Optionen aus:
  - o Default Group (Standardgruppe)
  - o Undefined Mappings Node (Knoten für nicht definierte Zuweisungen)
  - o Individual Defined Mapping (Einzeln definierte Zuweisung)
  - o Host Group (Hostgruppe)
  - o Host
3. Wählen Sie in der Symbolleiste **Mappings**→**Define**→**Additional Mapping**. Das Fenster **Define Additional Mapping** (Weitere Zuweisung definieren) wird angezeigt.
4. Wählen Sie im Feld **Host Group** (Hostgruppe) oder **Host** die gewünschte Hostgruppe aus.
5. Wählen Sie im Feld **Logical Unit Number** (Logische Gerätenummer) eine LUN aus. Unterstützt werden die LUNs 0 bis 255.
6. Wählen Sie im Bereich **Virtual Disk** (Virtuelles Laufwerk) das virtuelle Laufwerk aus. Im Bereich **Virtual Disk** werden Namen und Kapazitäten der virtuellen Laufwerke aufgelistet, die für die gewählte Hostgruppe / den gewählten Host für eine Zuweisung zur Verfügung stehen.
7. Klicken Sie auf **Add** (Hinzufügen).

 **ANMERKUNG:** Die Schaltfläche Add wird erst aktiviert, nachdem eine Hostgruppe / ein Host, eine LUN und ein virtuelles Laufwerk ausgewählt worden sind.

8. Um weitere Zuweisungen zu definieren, wiederholen Sie [Schritt 4](#) bis [Schritt 7](#).

 **ANMERKUNG:** Nachdem ein virtuelles Laufwerk einmal zugewiesen wurde, ist es nicht mehr im Bereich Virtual Disk (Virtuelles Laufwerk) verfügbar.

9. Klicken Sie auf **Schließen**. Die Zuweisungen werden gespeichert. Die Teilfenster **Topology** (Topologie) und **Defined Mappings** (Definierte Zuweisungen) im Register **Mappings** (Zuweisungen) werden aktualisiert, und die Zuweisungen werden angezeigt.

## Hilfsmittel zur Fehlerbehebung

Dell PowerVault MDSM fragt jedes verwaltete Array ab und bestimmt seinen derzeitigen Status. Bei Problemen mit einem Speicherarray bietet MDSM verschiedene Möglichkeiten zur Behebung:

### Event Log (Ereignisprotokoll)

Über die Ereignisprotokollanzeige (Event Log Viewer) können Sie eine detaillierte Liste der in einem Speicherarray auftretenden Ereignisse anzeigen. Das Ereignisprotokoll wird auf den Laufwerken des Speicherarrays in reservierten Bereichen gespeichert. Es zeichnet Konfigurationsereignisse und Ausfälle von Komponenten des Speicherarrays auf.

 **VORSICHTSHINWEIS:** Verwenden Sie diese Option nur unter Anleitung eines Mitarbeiters des technischen Supports.

Im Ereignisprotokoll werden ca. 8.000 Ereignisse gespeichert, bevor die ältesten Ereignisse durch neue überschrieben werden. Sie können die aufgezeichneten Ereignisse anderweitig speichern, wenn Sie sie aufbewahren möchten oder sie auch aus dem Ereignisprotokoll löschen.

Im Ereignisprotokollfenster sind die folgenden Anzeigetypen für Ereignisse verfügbar:

- Übersicht - Zeigt die Ereignisse übersichtsartig in einer Tabelle an.
- Detailansicht - Zeigt ausführliche Informationen zum ausgewählten Ereignis an.

So zeigen Sie das Ereignisprotokoll an:

1. Wählen Sie im Fenster **Array Management** (Arrayverwaltung) **Advanced**→**Troubleshooting**→**View Event Log**. Das Ereignisprotokoll (**Event Log**) wird

angezeigt. Standardmäßig wird die Übersicht dargestellt.

2. Um ausführliche Informationen zu einem gewählten Protokolleintrag anzuzeigen, wählen Sie **View Details** (Details anzeigen). Daraufhin wird das Teilfenster **Detail** mit Informationen zu dem betreffenden Eintrag angezeigt. Ausführliche Informationen können jeweils nur für einen ausgewählten Protokolleintrag angezeigt werden.
3. So speichern Sie das Ereignisprotokoll:
  - a. Klicken Sie auf **Save As** (Speichern unter). Das Dialogfeld **Save Events** (Ereignisse speichern) wird angezeigt.
  - b. Navigieren Sie zum gewünschten Ordner und geben Sie den gewünschten Dateinamen ein.
  - c. Klicken Sie auf **Save** (Speichern).
4. Klicken Sie auf **Clear All** (Alle löschen), um alle Protokolleinträge aus dem Ereignisprotokoll zu löschen.
5. Klicken Sie auf **Close** (Schließen), um das Ereignisprotokoll zu schließen.

Weitere Informationen finden Sie in den Online-Hilfethemen zu PowerVault Modular Disk Storage Manager.

## Recovery Guru

Recovery Guru ist eine Komponente von MDSM, mit der sich kritische Ereignisse im Speicherarray diagnostizieren und schrittweise beheben lassen.

Um das **Recovery Guru**-Fenster im Fenster **Array Management** (Arrayverwaltung) anzuzeigen, führen Sie eine der folgenden Aktionen durch:

1. Klicken Sie auf **Recovery Guru**.
1. Klicken Sie im Register **Support** auf **Recover from Failure** (Wiederherstellung nach Ausfall).
1. Klicken Sie im Teilfenster **Status** der Registerkarte **Summary** (Übersicht) auf **Storage Array Needs Attention** (Speicherarray benötigt Eingriff).

Auf Probleme werden Sie mit folgenden Hinweisen aufmerksam gemacht:

1. Statussymbole anders als Optimal
1. Alarmmeldungen, die an entsprechende Ziele gesendet werden
1. Hardware-Leuchtanzeigen

Die Statussymbole kehren zum Status **Optimal** zurück, sobald das Problem behoben ist.

## Speicherprofil

Das Speicherarray-Profil enthält eine Beschreibung aller Komponenten und Anzeigen des Speicherarrays. Die im Speicherarray-Profil enthaltenen Informationen lassen sich auch als Textdatei speichern. Das Speicherarray-Profil kann als Hilfsmittel bei der Wiederherstellung oder als Übersicht der aktuellen Konfiguration des Speicherarrays verwendet werden. Wenn sich die Konfiguration ändert, erstellen Sie eine neue Version des Speicherarray-Profiles.

1. Um das Speicherarray-Profil im Fenster **Array Management** (Arrayverwaltung) anzuzeigen, führen Sie eine der folgenden Aktionen durch:
  - o Wählen Sie **Storage Array** → **View** → **Profile**.
  - o Wählen Sie die Registerkarte **Summary** (Übersicht) und klicken Sie im Bereich **Status** auf **Storage Array Profile** (Speicherarray-Profil).
  - o Wählen Sie die Registerkarte **Support** (Übersicht) und klicken Sie auf **View Storage Array Profile** (Speicherarray-Profil anzeigen).

Das Fenster **Storage Array Profile** (Speicherarray-Profil) wird angezeigt. Der Bildschirm **Storage Array Profile** enthält mehrere Registerkarten. Die Bezeichnung jeder Registerkarte beschreibt die darin enthaltenen Informationen.

2. Führen Sie im Bildschirm **Storage Array Profile** eine der folgenden Aktionen durch:
  - o Ausführliche Informationen anzeigen - Fahren Sie mit [Schritt 3](#) fort.
  - o Speicherarray-Profil durchsuchen - Fahren Sie mit [Schritt 4](#) fort.
  - o Speicherarray-Profil speichern - Fahren Sie mit [Schritt 5](#) fort.
  - o Speicherarray-Profil schließen - Fahren Sie mit [Schritt 6](#) fort.
3. Um die Informationen im Speicherarray-Profil anzuzeigen, wählen Sie eine der Registerkarten aus und verwenden Sie die horizontale und vertikale Bildlaufleiste. Um das Speicherarray-Profil zu durchsuchen, zu speichern oder zu schließen, folgen Sie den anderen Schritten in dieser Anleitung.
4. Um das Speicherarray-Profil zu durchsuchen, führen Sie die nachstehenden Schritte durch:
  - a. Klicken Sie auf **Find** (Finden).
  - b. Geben Sie im Feld **Find** den Begriff ein, nach dem Sie suchen möchten. Wenn der Begriff auf der aktuellen Registerkarte enthalten ist, wird er in den Informationen des Speicherarray-Profiles hervorgehoben.

 **ANMERKUNG:** Die Suche ist auf die aktuelle Registerkarte beschränkt. Um auf anderen Registerkarten nach dem Begriff zu suchen, wählen Sie die gewünschte Registerkarte aus und klicken Sie erneut auf die Schaltfläche Find.

- c. Um nach weiteren Vorkommen des Begriffs auf derselben Registerkarte zu suchen, klicken Sie erneut auf die Schaltfläche **Find**.
5. Um das Speicherarray-Profil zu speichern, führen Sie die nachstehenden Schritte durch:
- a. Klicken Sie auf **Save As** (Speichern unter).
  - b. Um alle Bereiche des Speicherarray-Profiles zu speichern, wählen Sie **All Sections** (Alle Bereiche).
  - c. Um Informationen aus bestimmten Bereichen des Speicherarray- Profils zu speichern, wählen Sie die Option **Select Sections** (Bereiche auswählen) und klicken Sie auf die Kontrollkästchen neben den Bereichen, die Sie speichern möchten.
  - d. Wählen Sie das gewünschte Verzeichnis.
  - e. Geben Sie im Feld **Dateiname** den gewünschten Dateinamen ein. Um die Datei mit einer bestimmten Softwareanwendung zu verknüpfen, in der sie geöffnet werden soll, geben Sie eine Dateierweiterung an, z. B. **.txt**.
-  **ANMERKUNG:** Die Datei wird als ASCII-Textdatei gespeichert.
- f. Klicken Sie auf **Save** (Speichern).
6. Um das Speicherarray-Profil zu schließen, klicken Sie auf **Close** (Schließen).

## Statussymbole

Statussymbole zeigen einen von sechs Zuständen des Speicherarrays an. Verwenden Sie für alle nicht optimalen Statussymbole Recovery Guru, um das Problem zu erkennen und zu beheben. Nachstehend werden die sechs möglichen Statusbedingungen beschrieben:

- 1 Optimal - Alle Komponenten in dem verwalteten Array funktionieren wie vorgesehen.
- 1 **Benötigt Eingriff** - Es besteht ein Problem mit dem verwalteten Array, das einen Eingriff erfordert.
- 1 Wird repariert - Ein Zustand, bei dem ein *Eingriff erforderlich* ist, wurde korrigiert und der Status des verwalteten Arrays wird derzeit zu *Optimal* geändert.
- 1 Keine Antwort - Die Speicherverwaltungsstation kann nicht mit dem Array bzw. mit einem oder beiden Controllern im Speicherarray kommunizieren. Warten Sie nach einem Wiederherstellungsvorgang mindestens fünf Minuten darauf, dass das Speicherarray in den Status *Optimal* zurückkehrt.
- 1 Nicht unterstützt - Der Knoten wird von dieser MDSM-Version nicht unterstützt.
- 1 Software nicht unterstützt - Der Speicherarray wird mit einer Softwareversion betrieben, die von MDSM nicht mehr unterstützt wird.

## Konfiguration des RAID-Level für gemeinsame Speicher-Untersysteme

Die virtuellen Laufwerke im gemeinsamen Speichersubsystem müssen mit Dell PowerVault MDSM als Datenträgergruppen oder virtuelle Laufwerke konfiguriert werden. Alle virtuellen Laufwerke sollten gebunden werden und den angemessenen RAID-Level enthalten, um eine hohe Verfügbarkeit sicherzustellen. Dies gilt vor allem, wenn sie als Quorumressource genutzt werden.

 **ANMERKUNG:** Es wird empfohlen, einen anderen RAID-Level als RAID 0 (auch als Striping bezeichnet) zu verwenden. RAID 0-Konfigurationen bieten zwar eine sehr hohe Leistungsfähigkeit, können aber nicht die für Quorumressourcen benötigte Verfügbarkeit garantieren. Nähere Informationen zur Einrichtung der RAID-Levels für das System finden Sie in der Dokumentation des Speichersystems.

## Windows-Betriebssysteme und dynamische Speicher-Volumes

Das Betriebssystem Windows unterstützt keine dynamischen Datenträger (Upgrade-Datenträger) oder Volumes für den gemeinsamen Clusterspeicher. Wenn der gemeinsame Clusterspeicher als dynamischer Datenträger konfiguriert ist, kann der Assistent für die Clusterkonfiguration die Datenträger nicht erkennen, und Cluster und Netzwerk können nicht darauf zugreifen.

## Zuweisen von Laufwerkbuchstaben und Bereitstellungspunkten

Ein Bereitstellungspunkt ist ein Datenträger, das mit einem leeren Ordner auf einem NTFS-Laufwerk verbunden ist. Ein Bereitstellungspunkt funktioniert auf die gleiche Weise wie ein normales Laufwerk, allerdings wird ihm statt eines Laufwerkbuchstabens eine Bezeichnung oder ein Name zugewiesen. Durch die Verwendung von Bereitstellungspunkten kann ein Cluster mehr gemeinsame Datenträger unterstützen, als Laufwerkbuchstaben zur Verfügung stehen.

Bei der Clusterinstallation wird der Bereitstellungspunkt den Laufwerken nicht automatisch hinzugefügt, die vom Cluster verwaltet werden. Um den Bereitstellungspunkt zum Cluster hinzuzufügen, müssen Sie in der Clusterressourcengruppe für jeden Bereitstellungspunkt eine physische Festplattenressource erstellen. Die neue physische Datenträgerressource muss sich in derselben Clusterressourcengruppe befinden und abhängig vom Laufwerk mit dem Stammverzeichnis sein (d. h. dem Laufwerk, von dem aus der Bereitstellungspunkt hinzugefügt wird).

 **ANMERKUNG:** Beim Bereitstellen eines Datenträgers auf einem NTFS- Datenträger dürfen die Bereitstellungspunkte nicht von der Quorumressource aus oder zwischen den im Cluster zusammengefassten Laufwerken und den lokalen Laufwerken erstellt werden. Bereitstellungspunkte müssen sich in der gleichen Clusterressourcengruppe befinden, und sie müssen abhängig vom Laufwerk mit dem Stammverzeichnis sein.

## Benennen und Formatieren von Laufwerken im gemeinsamen Speichersystem

Im PowerVault Modular Disk Storage Manager erstellte Datenträger erscheinen in der Windows-Datenträgerverwaltung als physische Datenträger. Führen Sie für jeden physischen Datenträger die folgenden Schritte durch:

- 1 Legen Sie die Laufwerksignatur fest.

- 1 Erstellen Sie die Partition.
- 1 Weisen Sie den Laufwerkbuchstaben zu.
- 1 Formatieren Sie die Partition mit NTFS.

**⚠ VORSICHTSHINWEIS:** Die Laufwerkbuchstaben werden vom zweiten Knoten aus manuell zugewiesen. So sind die gemeinsamen Datenträger gleichzeitig für beide Knoten zugänglich. Um vor der Installation der Microsoft Failover-Clusterunterstützung die Integrität des Dateisystems sicherzustellen und möglichem Datenverlust vorzubeugen, muss jede E/A-Aktivität zu den gemeinsamen Laufwerken unterbunden werden. Führen Sie dazu auf jeweils einem der Knoten den folgenden Vorgang durch, während der andere Knoten heruntergefahren sein muss.

Die einzelnen Servern des Clusters benötigen möglicherweise unterschiedlich viele Laufwerkbuchstaben. Es wird empfohlen, dass die Benennung der freigegebenen Laufwerke in umgekehrter alphabetischer Reihenfolge beginnend mit dem Buchstaben z erfolgt. So weisen Sie Laufwerkbuchstaben im gemeinsamen Speichersystem zu und formatieren Laufwerke:

1. Öffnen Sie bei heruntergefahrenem Knoten 2 die **Datenträgerverwaltung** auf Knoten 1.
2. Lassen Sie Windows für alle neuen physikalischen oder logischen Laufwerke eine Signatur zuweisen.

 **ANMERKUNG:** Erweitern bzw. konvertieren Sie Ihre Datenträger nicht zu dynamischen Datenträgern.

3. Suchen Sie das Symbol des ersten unformatierten Datenträgers des gemeinsamen Speichersystems, das keine Bezeichnung hat.
4. Klicken Sie mit der rechten Maustaste auf das Symbol, und wählen Sie danach im Untermenü **Erstellen**. Wenn die unformatierten Datenträger nicht sichtbar sind, überprüfen Sie folgende Punkte:
  - 1 Die Zielverbindungen des iSCSI-Initiators sind aktiv.
  - 1 Die LUNs wurden den Hosts zugeordnet.
  - 1 Das Speichersystem ist ordnungsgemäß an die Server angeschlossen.
5. Erstellen Sie im Dialogfeld eine Partition mit der Größe des gesamten Datenträgers (Standardeinstellung), und klicken Sie auf **OK**.

 **ANMERKUNG:** Ein virtuelles Laufwerk, das vom Speichersystem einem bzw. mehreren Clusterknoten zugewiesen wurde erscheint im Windows-Betriebssystem auf jedem Knoten als physischer Datenträger. Microsoft Cluster ermöglicht zu einem gegebenen Zeitpunkt jeweils nur einem Knoten den Zugriff auf eine physische Datenträgerressource. Bei einem partitionierten Datenträger, der mehrere NTFS-Speicherlaufwerke enthält, ist der gleichzeitige Zugriff auf verschiedene Speicherlaufwerke deshalb nur über den Clusterknoten möglich, der die physische Datenträgerressource kontrolliert. Wenn zwei NTFS-Speicherlaufwerke von verschiedenen Knoten aus kontrolliert werden sollen, müssen sie sich auf verschiedenen Datenträgern befinden.

6. Klicken Sie auf **Ja**, um die Partition zu bestätigen.
7. Klicken Sie noch einmal mit der rechten Maustaste auf das gleiche Symbol, und wählen Sie im Untermenü **Laufwerkbuchstaben und -pfad ändern**.
8. Weisen Sie dem NTFS-Datenträger einen Laufwerkbuchstaben zu, oder erstellen Sie einen Bereitstellungspunkt.

So weisen Sie dem NTFS-Speicherlaufwerk einen Laufwerkbuchstaben zu:

- a. Klicken Sie auf **Bearbeiten**, und wählen Sie den Buchstaben aus, der für das Laufwerk vergeben werden soll (zum Beispiel z).
- b. Klicken Sie auf **OK**.
- c. Fahren Sie mit [Schritt 9](#) fort.

So erstellen Sie einen Bereitstellungspunkt:

- a. Klicken Sie auf **Hinzufügen**.
- b. Klicken Sie auf **In folgendem leeren NTFS-Ordner bereitstellen**.
- c. Geben Sie den Pfad zu dem leeren Ordner auf dem NTFS- Datenträger ein, oder klicken Sie auf **Durchsuchen**, um den Ordner zu suchen.
- d. Klicken Sie auf **OK**.
- e. Fahren Sie mit [Schritt 9](#) fort.

9. Klicken Sie auf **Ja**, um die Änderungen zu bestätigen.
10. Klicken Sie erneut mit der rechten Maustaste auf das Laufwerksymbol, und wählen Sie dann im Untermenü die Option **Formatieren**.
11. Geben Sie unter **Volumebezeichnung** einen beschreibenden Namen für den neuen Datenträger ein; zum Beispiel Festplatte\_Z oder E-Mail\_Daten.
12. Ändern Sie im Dialogfeld das Dateisystem auf **NTFS**, wählen Sie **Quick Format** (Formatierung mit QuickFormat ausführen), und klicken Sie auf **Start**.

 **ANMERKUNG:** Gemeinsame Datenträgerressourcen unter Microsoft Cluster erfordern das Dateisystemformat NTFS.

13. Wenn die Warnmeldung eingeblendet wird, klicken Sie auf **OK**.
14. Klicken Sie auf **OK**, um zu bestätigen, dass die Formatierung abgeschlossen ist.
15. Klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.
16. Wiederholen Sie [Schritt 3](#) bis [Schritt 15](#) für jedes übrige Laufwerk.
17. Schließen Sie die **Datenträgerverwaltung**.
18. Schalten Sie Knoten 1 aus.
19. Schalten Sie Knoten 2 ein.
20. Öffnen Sie auf Knoten 2 die **Datenträgerverwaltung**.
21. Prüfen Sie, ob die Laufwerksbuchstaben für Knoten 2 korrekt zugewiesen sind. Falls erforderlich, weisen Sie sie erneut zu. Um die Laufwerksbuchstaben erneut zuzuweisen, wiederholen Sie [Schritt 7](#) bis [Schritt 9](#).

## Verwenden von erweiterten Funktionen (Premium) von PowerVault Modular Disk Storage Manager

PowerVault Modular Disk Storage Manager enthält die folgenden erweiterten Funktionen:

- 1 [Snapshot Virtual Disk](#)
- 1 [Virtual Disk Copy](#)

Um diese Premiumfunktionen zu installieren und zu aktivieren, müssen Sie für jede Funktion eine Schlüsseldatei erwerben und dann das entsprechende Host-Speicherarray festlegen. Eine Anleitung für diesen Vorgang finden Sie auf der Karte *Premium Feature Activation* (Aktivierung von Premiumfunktionen), die mit dem Dell PowerVault MD3200i/MD3220i-Speichersystem geliefert wurde.

Diese Premiumfunktionen unterstützen die bestmögliche Verfügbarkeit der Clusterlösung. Sie müssen die nachfolgenden Anweisungen befolgen, um einen ordnungsgemäßen Clusterbetrieb zu gewährleisten.

### Snapshot Virtual Disk

Snapshot Virtual Disk - Ermöglicht es, Momentaufnahmen von virtuellen Laufwerken zur Sicherung, zum Testen oder zur Datenverarbeitung zu erstellen, ohne den Inhalt des jeweiligen virtuellen Quelllaufwerks zu verändern. Sie können entweder Simple Path (Einfacher Pfad) oder Advanced Path (Erweiterter Pfad) verwenden, um einen Snapshot für das Clusterlaufwerk zu erstellen. Das virtuelle Snapshot-Laufwerk kann dem primären Knoten (welcher das Quelllaufwerk besitzt) oder dem sekundären Knoten zugewiesen werden (welcher das Quelllaufwerk nicht besitzt), und zwar zur Datensicherung, zu Testzwecken oder zur Datenverarbeitung.

**⚠ VORSICHTSHINWEIS:** Das virtuelle Snapshot-Laufwerk sollte zu keinem Zeitpunkt mehr als einem Knoten im Cluster zugewiesen sein. Das virtuelle Snapshot-Laufwerk wird nicht vom Failover-Cluster-Manager verwaltet, also besteht, wenn Sie das virtuelle Snapshot-Laufwerk der Hostgruppe oder beiden Knoten im Cluster zuweisen, die Gefahr, dass beide Knoten gleichzeitig auf Daten zugreifen und infolgedessen Daten **beschädigt werden könnten**.

Sie können eine Microsoft VSS (Volume Shadow-Copy Service)-Anwendung zum Erstellen und Zuweisen von Snapshots verwenden. Wenn Sie statt dessen MDSM verwenden, müssen Sie den nachstehend beschriebenen Verfahren folgen.

So weisen Sie das virtuelle Snapshot-Laufwerk dem primären Knoten zu:

1. Verwenden Sie die Host-Zuweisung an virtuelle Laufwerke in Modular Disk Storage Manager. Damit wird sichergestellt, dass dem virtuellen Snapshot-Laufwerk eine andere Laufwerksignatur korrekt zugewiesen wird.
2. Verwenden Sie die Windows-Datenträgerverwaltung, um das virtuelle Snapshot-Laufwerk neu zu erkennen, weisen Sie den Laufwerksbuchstaben zu, und beginnen Sie mit der Nutzung des Laufwerks.

**🔍 ANMERKUNG:** Die Laufwerke müssen eventuell mehrere Male neu erkannt werden, bevor die Windows-Datenträgerverwaltung das virtuelle Snapshot-Laufwerk erkennt. Wenn das virtuelle Snapshot-Laufwerk nicht erkannt wird, warten Sie einige Minuten und führen Sie eine erneute Erkennung durch. Wiederholen Sie den Vorgang, bis das virtuelle Snapshot-Laufwerk erkannt wird; starten Sie nicht den Server neu.

Um das virtuelle Snapshot-Laufwerk dem sekundären Knoten zuzuweisen (welchem das Quelllaufwerk nicht zugeordnet ist), müssen Sie es zunächst dem primären Knoten zuweisen, um sicherzustellen, dass der Snapshot eine neue Laufwerksignatur erhält. Verwenden Sie anschließend Modular Disk Storage Manager, um die Zuweisung des virtuellen Snapshot-Laufwerks vom primären Knoten zu entfernen, weisen Sie es dem sekundären Knoten zu und beginnen Sie mit der Nutzung.

**⚠ VORSICHTSHINWEIS:** Wenn Sie versuchen, das virtuelle Snapshot-Laufwerk dem sekundären Knoten zuzuweisen, bevor die Signatur vom primären Knoten bereitgestellt wurde, besteht die Möglichkeit, dass das Betriebssystem das virtuelle Snapshot-Laufwerk fälschlicherweise als Systemvolumen identifiziert. Dadurch kann es zu Datenverlust kommen und das virtuelle Snapshot-Laufwerk ist eventuell nicht mehr zugänglich.

**🔍 ANMERKUNG:** Bei einer Clusterkonfiguration mit mehreren virtuellen Snapshot-Laufwerken muss jedes virtuelle Laufwerk zuerst dem Knoten zugewiesen werden, dem das verbundene Quelllaufwerk zugeordnet ist. Der primäre Knoten für ein virtuelles Snapshot-Laufwerk ist möglicherweise nicht der primäre Knoten für ein anderes virtuelles Snapshot-Laufwerk.

### Virtual Disk Copy

Virtual Disk Copy - Beim Kopieren eines virtuellen Laufwerks innerhalb eines Speicherarrays wird auf dem virtuellen Ziellaufwerk eine vollständige Kopie der auf dem virtuellen Quelllaufwerk befindlichen Daten erstellt. Virtual Disk Copy kann genutzt werden, um Daten zu sichern, Daten von Datenträgergruppen mit Laufwerken von geringerer Kapazität in Datenträgergruppen mit größeren Laufwerken zu kopieren oder um Daten vom virtuellen Snapshot-Laufwerk auf das virtuelle Quelllaufwerk zurückzukopieren.

So erstellen Sie eine virtuelle Laufwerkkopie eines freigegebenen Microsoft Cluster-Laufwerks:

1. Verwenden Sie ein virtuelles Snapshot-Laufwerk mit dem freigegebenen Clusterlaufwerk als Quelllaufwerk.
2. Führen Sie keine Zuweisung dieses virtuellen Snapshot-Laufwerks auf einen Clusterknoten durch. Verwenden Sie dann das neu erstellte virtuelle Snapshot-Laufwerk als Quelllaufwerk für die virtuelle Laufwerkkopie.

 **ANMERKUNG:** Wenn Sie versuchen, von einem freigegebenen Microsoft-Cluster-Laufwerk direkt eine virtuelle Laufwerkkopie zu erstellen, schlägt der Vorgang fehl und die folgende Fehlermeldung wird angezeigt:  
The operation cannot complete because the selected virtual disk is not a source virtual disk candidate.

Wenn das freigegebene Clusterlaufwerk ausfällt und Sie es vom virtuellen Ziellaufwerk wiederherstellen müssen, ändern Sie in Failover Cluster Manager den Status der Clustergruppe mit dem ausgefallenen Laufwerk auf Offline, und verwenden Sie dann eines der folgenden Verfahren:

1. Verwenden Sie Virtual Disk Copy, um die Daten vom virtuellen Ziellaufwerk auf das freigegebene Clusterlaufwerk zurück zu übertragen.
2. Machen Sie die Zuweisung des freigegebenen Clusterlaufwerks an die Hostgruppe rückgängig, und ordnen Sie das virtuelle Ziellaufwerk der Hostgruppe zu.

## Konfigurieren eines Failover-Clusters

Nachdem Sie das private und öffentliche Netzwerk eingerichtet und die freigegebenen Datenträger im Speicherarray den Clusterknoten zugewiesen haben, können Sie die Betriebssystem-Dienste auf Ihrem Windows Server 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 finden Sie im *Installations- und Fehlerbehebungshandbuch für Dell Failover-Cluster unter Microsoft Windows Server 2008* unter [support.dell.com/manuals](http://support.dell.com/manuals).

---

[Zurück zum Inhaltsverzeichnis](#)

## Fehlerbehebung

### Hardwareinstallations- und Fehlerbehebungshandbuch

In diesem Anhang finden Sie Informationen zur Fehlerbehebung bei Clusterkonfigurationen.

[Tabelle A-1](#) beschreibt allgemeine Clusterprobleme sowie mögliche Ursachen und Lösungen für diese Probleme.

**Tabelle A-1. Allgemeine Fehlerbehebung im Cluster**

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 <a href="#">Verkabelung der Clusterhardware</a> .
	Eines der Kabel ist fehlerhaft.	Ersetzen Sie das fehlerhafte Kabel.
	Hostgruppe oder Zuweisungen zwischen Hostsystemen und virtuellen Laufwerken werden nicht korrekt erstellt.	Überprüfen Sie folgende Punkte: <ul style="list-style-type: none"> <li>1 Die Hostgruppe wurde erstellt, und die Clusterknoten wurden der Hostgruppe hinzugefügt.</li> <li>1 Die Zuweisungen zwischen Hostsystemen und virtuellen Laufwerken wurden erstellt, und die virtuellen Laufwerke wurden der Hostgruppe zugeordnet, die die Clusterknoten enthält.</li> </ul>
Einer der Knoten benötigt längere Zeit, um dem Cluster beizutreten.  ODER  Einer der Knoten kann dem Cluster nicht beitreten.	Das Knoten-zu-Knoten-Netzwerk ist aufgrund eines Kabel- oder Hardwarefehlers ausgefallen.	Überprüfen Sie die Netzwerkverkabelung. Stellen Sie sicher, dass die Verbindung zwischen den Knoten und das öffentliche Netzwerk an den richtigen NIC angeschlossen sind.
	Längere Verzögerungen bei der Kommunikation zwischen den Knoten sind unter Umständen normal.	Überprüfen Sie, ob die Knoten miteinander kommunizieren können, indem Sie von jedem Knoten zum nächsten den Ping-Befehl ausführen. 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 und blockiert die RPC (Remote Procedure Call)-Kommunikation zwischen den Knoten.	Konfigurieren Sie die Internetverbindungs-Firewall so, dass die von der Microsoft Failover-Clusterunterstützung und den Clusteranwendungen/-diensten benötigte Datenkommunikation zugelassen wird. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel KB883398 unter <a href="#">support.microsoft.com</a> .
Zu einem Cluster lässt sich mit dem Failover Cluster Manager keine Verbindung aufnehmen.	Der Clusterdienst wurde nicht gestartet. Im System wurde kein Cluster gebildet. Das System wurde gerade gebootet und die Dienste sind noch nicht vollständig gestartet.	Überprüfen Sie, ob der Clusterdienst aktiv ist und ob ein Cluster gebildet wurde.
	Der Netzwerkname des Clusters kann im Netzwerk nicht angesprochen werden, weil die Internetverbindungs-Firewall für einen oder mehrere Knoten aktiviert wurde.	Konfigurieren Sie die Internetverbindungs-Firewall so, dass die von Microsoft Cluster und den Clusteranwendungen/-diensten benötigte Datenkommunikation zugelassen wird. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel KB883398 unter <a href="#">support.microsoft.com</a> .
Sie werden während der Installation von Microsoft Failover Cluster zur Konfiguration eines Netzwerks anstatt zweier Netzwerke aufgefordert.	Die TCP/IP-Konfiguration ist nicht korrekt.	Dem Knoten-zu-Knoten-Netzwerk und dem öffentlichen Netzwerk müssen feste IP-Adressen auf unterschiedlichen Subnetzen zugewiesen werden. Weitere Informationen über das Zuweisen der Netzwerk-IP-Adressen finden Sie unter Zuweisen von festen IP-Adressen an Clusterressourcen und -komponenten im <i>Installations- und Fehlerbehebungshandbuch für Dell Failover-Cluster unter Microsoft Windows Server 2008</i> .
	Das private (Punkt-zu-Punkt-) Netzwerk wurde unterbrochen.	Überprüfen Sie, ob beide Systeme eingeschaltet sind, damit die Netzwerkadapter im privaten Netzwerk verfügbar sind.
Ein Knoten kann dem Cluster nicht hinzugefügt werden.	Der neue Knoten kann nicht auf die gemeinsamen Datenträger zugreifen.	Stellen Sie mit der Datenträgerverwaltung von Windows sicher, dass der neue Clusterknoten die Datenträger des Clusters benennen kann. Überprüfen Sie folgende Punkte, falls die Datenträger in der Datenträgerverwaltung nicht angezeigt werden: <ul style="list-style-type: none"> <li>1 Überprüfen Sie alle Kabelverbindungen.</li> <li>1 Überprüfen Sie die Access Control-Einstellungen für die angeschlossenen Speichersysteme.</li> </ul>
	Möglicherweise wurde für einen oder mehrere Knoten die Internetverbindungs-Firewall aktiviert, die die RPC-Kommunikation zwischen den Knoten blockiert.	Konfigurieren Sie die Internetverbindungs-Firewall so, dass die vom Microsoft Cluster und den Clusteranwendungen/-diensten benötigte Datenkommunikation zugelassen wird. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel KB883398 unter <a href="#">support.microsoft.com</a> .
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 die RPC-Kommunikation zwischen	Konfigurieren Sie die Internetverbindungs-Firewall so, dass die vom Microsoft Cluster und den Clusteranwendungen/-diensten benötigte Datenkommunikation zugelassen wird.

	den Knoten blockiert.	Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel KB883398 unter <a href="https://support.microsoft.com">support.microsoft.com</a> .
Die Ausführung von Virtual Disk Copy schlägt fehl.	Bei der Ausführung von Virtual Disk Copy dient das Clusterlaufwerk als Quelllaufwerk.	Um einen Virtual Disk Copy-Vorgang für das freigegebenen Clusterlaufwerk durchzuführen, erstellen Sie einen Snapshot des Laufwerks, und führen Sie anschließend Virtual Disk Copy für das virtuelle Snapshot-Laufwerk durch.
Dem virtuellen Snapshot-Laufwerk kann kein Laufwerksbuchstabe zugewiesen werden.  Auf das virtuelle Snapshot-Laufwerk kann nicht zugegriffen werden.  Systemfehlerprotokoll enthält eine Warnung mit Ereignis 59 von <b>partmgr</b> mit dem Inhalt, dass das virtuelle Snapshot-Laufwerk ein redundanter Pfad eines Clusterlaufwerks ist.	Das virtuelle Snapshot-Laufwerk wurde <b>fälschlicherweise dem Knoten</b> zugewiesen, dem das Quelllaufwerk nicht zugeordnet ist.	Heben Sie die Zuweisung des virtuellen Snapshot-Laufwerks an das Quelllaufwerk auf, und weisen Sie ihn dem Knoten zu, dem das Quelllaufwerk zugeordnet ist. Weitere Informationen finden Sie unter <a href="#">Verwenden von erweiterten Funktionen (Premium) von PowerVault Modular Disk Storage Manager</a> .

[Zurück zum Inhaltsverzeichnis](#)