Dell™ PowerVault™
Netzwerk Attached Storage
(NAS) Lösung

iSCSI Bereitstellungshandbuch

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie das System besser einsetzen können.

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

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

Mai 2009 **Rev. A00**

Inhalt

1

Einführung

Diese Dokumentation enthält Informationen zur Konfiguration des Internet Small Computer System Interface (iSCSI) Software Target beim Dell™ PowerVault™-Speichersystem als Blockspeichergerät.

Über iSCSI lässt sich auf praktische und relativ kostengünstige Weise Speicherplatz für neue Anwendungen oder ein Netzwerkspeicherpool für vorhandene Anwendungen schaffen. Dell und seine Partner aus der Speicherbranche bieten hierfür ein breites Spektrum an leicht implementierbaren Speicherlösungen an. Die vorliegende Dokumentation bietet Administratoren und IT-Managern die Möglichkeit, die iSCSI-Technologie anhand von Beispielen aus dem alltäglichen Einsatz kennenzulernen.

Folgende Themen werden in der Dokumentation behandelt:

- Kurzanleitung für die Installation–Liefert eine Anleitung zum Erstellen eines iSCSI-Targets und dem Einrichten einer Verbindung zu einem Microsoft ® iSCSI-Initiator
- Vollständige iSCSI-Konfiguration:
  - Ausführliche Anleitung zur Installation und Konfiguration von Microsoft iSCSI Initiator Software und von Microsoft iSCSI Software Target
  - Konfigurieren der Verbindungen zwischen Initiator und Target
- Einrichten geschützter iSCSI-Verbindungen
- Microsoft iSNS Server und weitere Einzelheiten der Konfiguration

ANMERKUNG: In dieser Dokumentation wird der iSCSI-Initiator als *Initiator* und das iSCSI-Software-Target als *Target* bezeichnet.

Begriffe und Definitionen

In den folgenden Abschnitten werden die in dieser Dokumentation verwendeten Begriffe erläutert.

PowerVault-Speichersystem

Innerhalb dieser Dokumentation bezieht sich der Begriff *PowerVault-Speichersystem* auf die einzelne Speichereinheit. Der Begriff *PowerVault Speicherlösung* bezieht sich auf die Konfiguration des Servers allein oder zusammen mit den Speicherarrays.

iSCSI

iSCSI ist ein Standard zur Übermittlung von SCSI-Befehlen über TCP/IP (Transfer Control Protocol/Internet Protocol)– Ein Protokoll, das Datenblöcke über IP-Netzwerke transportiert, ohne dass eine spezielle Netzwerkinfrastruktur (z. B. Fibre Channel) benötigt wird.

Bei Systemspeicherlösungen ermöglicht iSCSI beliebigen Clientrechnern (Initiatoren) in einem IP-Netzwerk, einen dedizierten Remote-Server (Target) zu kontaktieren und darauf Block-E/A-Operationen wie auf einer lokalen Festplatte durchzuführen.

iSNS

Microsoft iSCSI Internet Storage Name Service (iSNS) ist ein Dienst, der iSNS-Registrierungen, Registrierungsaufhebungen und Abfragen von iSNS-Clients über TCP/IP durchführt und zudem eine Datenbank dieser Registrierungen verwaltet (ähnlich, wie es ein DNS-Server tut). Ein weitverbreitetes Einsatzgebiet von Microsoft iSNS Server ist es, iSNS-Clients (Initiatoren und Targets) die Möglichkeit zu verschaffen, sich selbst zu registrieren und andere registrierte iSNS-Clients abfragen zu können. Die Registrierungen und Abfragen werden per TCP/IP-Remoteverbindung ausgeführt.

iSNS Server kann von der Microsoft-Support-Webseite unter **support.microsoft.com** auf einen separaten Server heruntergeladen und installiert werden, auf dem Microsoft iSCSI Initiator oder Target nicht installiert ist.

ANMERKUNG: Einzelheiten zu Installation und Konfiguration von iSNS Server finden Sie unter„Anhang“ auf Seite 43.

Bevor Sie die PowerVault Speicherlösung als iSCSI-Target einrichten

Bevor Sie Ihre Speicherlösung als iSCSI-Target einrichten, lesen Sie diesen Abschnitt vollständig durch. Sie müssen Punkte wie Ethernet-Einstellungen und Sicherheitseinstellungen für iSCSI-Targets berücksichtigen.

Bewährte Vorgehensweisen zur Einrichtung des iSCSI-Speicherbereichsnetzwerks

Tabelle 1-1 enthält Informationen über das Konfigurieren von Netzwerkkarten (beim Target) in verschiedenen Modellen von iSCSI-Netzwerken.

- Sie können redundante Pfade bei Initiatoren (Hosts) konfigurieren. Microsoft Multipath I/O (MPIO) wird vom Initiator Version 2.06 oder höher unterstützt.
- Sie benötigen für eine effiziente MPIO-Verbindung in der PowerVault Speicherlösung zwei dedizierte iSCSI-Netzwerkkarten beim Target und beim Initiator.
- iSCSI Netzwerkkarten-Teaming wird nicht unterstützt.
- Sie können je nach Ihren Erfordernissen Initiatoren mit einer oder zwei dedizierten Netzwerkkarten für iSCSI konfigurieren.

ANMERKUNG: Tabelle 1-1 enthält Informationen über die Konfiguration der Netzwerkkarte beim iSCSI-Target. Informationen zur optimalen Verbindung werden ebenfalls als Option bereitgestellt. Sie können die iSCSI-Netzwerkkarten Ihren Netzwerkerfordernissen gemäß konfigurieren.

Tabelle 1-1. Verwenden einer einzelnen PowerVault Speicherlösung als Target

Zahl der Netzwerkkarten	Einzelheiten	Siehe Abbildung
4	Netzwerkkarte-1 und Netzwerkkarte-2 - geteamte Netzwerkkarten für öffentliches Netzwerk Netzwerkkarte-3 - iSCSI dedizierter Datenverkehr (Subnetz A) Netzwerkkarte-4 - iSCSI dedizierter Datenverkehr (Subnetz B)	Abbildung 1-1

Tabelle 1-1. Verwenden einer einzelnen PowerVault Speicherlösung als Target

Zahl der Netzwerkkarten	Einzelheiten	Siehe Abbildung
3 **ANMERKUNG:** Verwenden Sie diese Konfiguration, wenn der iSCSI-Datenverkehr eine höhere Priorität besitzt als der Datenverkehr von Dateien.	Netzwerkkarte-1- Netzwerkkarte für öffentliches Netzwerk Netzwerkkarte-2 - iSCSI dedizierter Datenverkehr (Subnetz A) Netzwerkkarte-3 - iSCSI dedizierter Datenverkehr (Subnetz B)	Abbildung 1-2

- Es hat sich bewährt, über zwei für iSCSI dedizierte Ports zu verfügen. Konfigurieren Sie jede Netzwerkkarte (oder Port, wenn Sie eine Multiport-Netzwerkkarte haben) in einem separaten Subnetz.
- Mit dem Challenge-Handshake Authentication Protocol (CHAP) ist ein sicheres iSCSI möglich. Weitere Informationen zu den CHAP-Einstellungen finden Sie unter „Konfigurieren gesicherter iSCSI-Verbindungen über das CHAP (Challenge-Handshake Authentication Protocol)“ auf Seite 39.

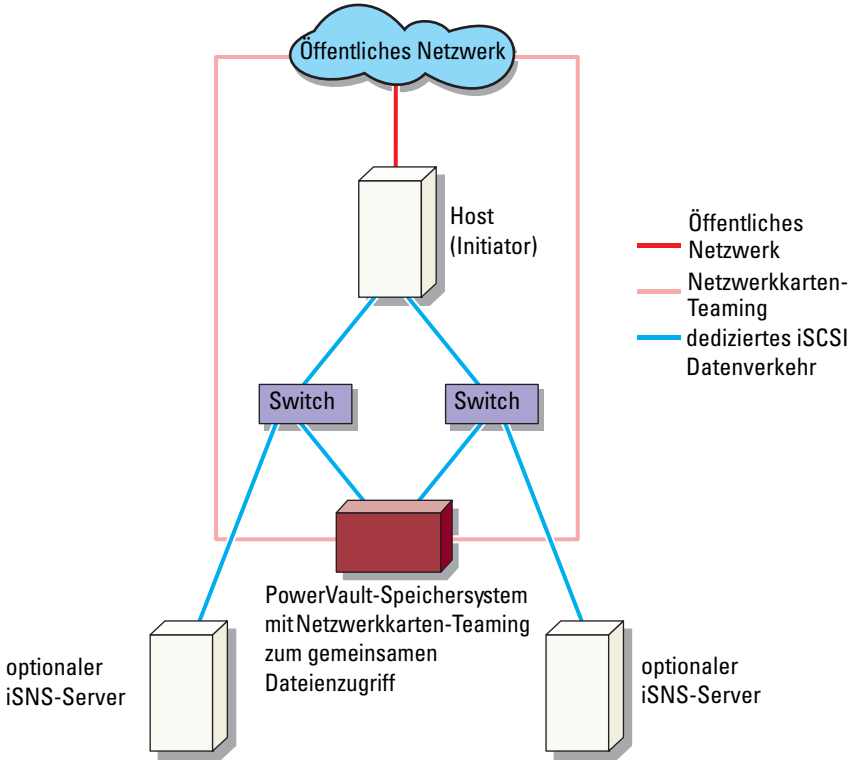
Tabelle 1-2. Arbeitsblatt

	Optionen	Host IP	Target IP
Netzwerkkarte 1	iSCSI Öffentlich Andere		
Netzwerkkarte 2	iSCSI Öffentlich Andere		
Netzwerkkarte 3	iSCSI Öffentlich Andere		
Netzwerkkarte 4	iSCSI Öffentlich Andere		

ANMERKUNG: IQNs sind die Standardnamenskonvention zur Identifizierung von Targets und Initiatoren. Es wird empfohlen, IQN wenn immer möglich als Kennung zu verwenden.

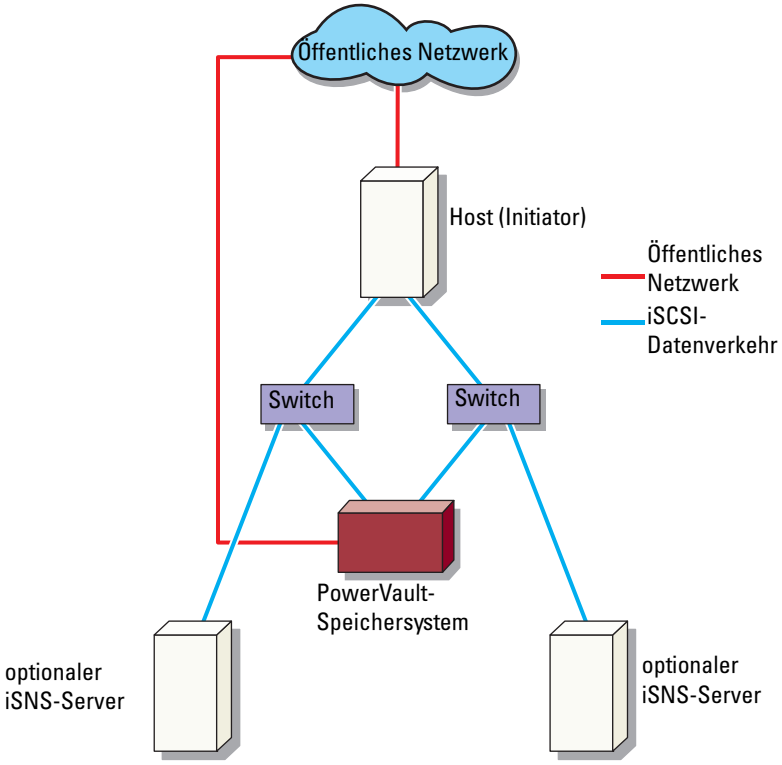
ANMERKUNG: Es wird empfohlen, dedizierte iSCSI-Netzwerkkarten nicht im öffentlichen Netzwerk zu konfigurieren, sondern auf separaten Subnetzen.

Abbildung 1-1. Redundante iSCSI-Pfade und Netzwerkkarten-Teaming zum gemeinsamen Datenzugriff bei vier Netzwerkkarten.



ANMERKUNG: Einzelheiten zur Konfiguration von iSCSI-Targets finden Sie unter„Einzelheiten zum Target“ auf Seite 23.

Abbildung 1-2. Redundante iSCSI-Pfade bei drei Netzwerkkarten



ANMERKUNG: Einzelheiten zur Konfiguration von iSCSI-Targets finden Sie unter „Einzelheiten zum Target“ auf Seite 23.

2

Schritte zur Einrichtung einer Verbindung zwischen Initiator und Target

Dieser Abschnitt enthält eine Schritt-für-Schritt-Anleitung zur Einrichtung eines iSCSI-Targets und zur Herstellung einer Verbindung von einem Initiator aus. Es wird vorausgesetzt, dass der Benutzer mit folgendem vertraut ist:

- Arbeitsweise des iSCSI-Protokolls
- Informationen zur iSCSI-Verbindung zwischen Initiator und Target
- Installation und Setup von Microsoft® iSCSI Initiator, Microsoft Software iSCSI Target und Microsoft iSNS Server

Voraussetzungen

Führen Sie vor dem Einrichten des iSCSI-Targets folgende Schritte durch:

1. Laden Sie die aktuelle Microsoft iSCSI Initiator-Software von der Microsoft-Support-Website unter **support.microsoft.com** herunter und installieren Sie den Initiator (Host).
2. Installieren Sie MS Software iSCSI Target von der mitgelieferten CD auf Ihrem Speichersystem.
3. Konfigurieren Sie das iSCSI-Netzwerk und weisen Sie ihm mit Hilfe des „Arbeitsblatt“ auf Seite 10 die IP-Adressen zu.

Bevor Sie iSCSI-Targets konfigurieren, führen Sie folgende Punkte durch:

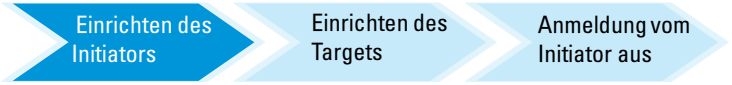
1. Erzeugen Sie einige LUNs und reservieren Sie Speicherplatz, um virtuelle Festplatten für iSCSI-Targets zu erzeugen.
2. Klicken Sie mit der rechten Maustaste auf das **iSCSI-Target** und wählen Sie **Properties** (Eigenschaften), um dedizierte iSCSI-Netzwerkkarten für den iSCSI-Datenverkehr zu konfigurieren (siehe Abbildung 3-1 "Erzeugen von iSCSI-Targets" auf Seite 25).

Methode 1 (Erkennung über Targetportale)

Die Targeterkennung kann durch Eingabe der IP-Adresse einer der Netzwerkkarten des PowerVault-Speichersystems durchgeführt werden. Die betreffende Netzwerkkarte muss im Initiator für iSCSI-Datenverkehr konfiguriert sein, damit der Initiator alle Targets dieses Targetservers erkennen kann.

Die folgenden Schritte führen Sie durch die Einrichtung eines iSCSI-Targets und das Herstellen einer Verbindung von einem Initiator aus.

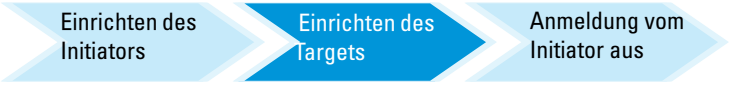
Konfigurieren des Initiators (Host)



Konfigurieren Sie den Microsoft iSCSI-Initiator mit der IP-Adresse des Target-Servers. So konfigurieren Sie den Initiator:

1. Wechseln Sie zu dem System, auf dem Microsoft iSCSI-Initiator installiert ist.
2. Klicken Sie auf **Start**→ **Programs** (Programme)→ **Microsoft iSCSI Initiator**→ **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators)→ Registerkarte **Discovery** (Erkennung).
3. Wählen Sie **Add portal** (Portal hinzufügen).
4. Fügen Sie am PowerVault-Speichersystem die IP-Adresse einer für iSCSI-Datenverkehr konfigurierten Netzwerkkarte hinzu (siehe Abbildung 1-1).
5. Klicken Sie auf **OK**.

Konfigurieren einer iSCSI-Verbindung mit dem PowerVault NAS-Speichersystem



Erzeugen des Targets

1. Wählen Sie in der PowerVault NAS-Anwendung **Start**→ **Server Manager**→ **Storage** (Speicherung)→ **MS Software Target**.
2. Wählen Sie das Symbol **Microsoft iSCSI Software Target**.

Die folgenden Optionen werden angezeigt–**iSCSI Targets**, **Devices** (Geräte) und **Snapshots** (Speicherauszüge).

3 Wählen Sie **iSCSI Targets** und klicken Sie entweder mit der rechten Maustaste darauf oder wählen Sie die Option **More Actions** (Weitere Aktionen) in der Registerkarte **Actions** (Aktionen).

4 Wählen Sie die Option **Create iSCSI Target** (iSCSI-Target erzeugen).

5 Das Fenster **Welcome to the Create iSCSI Target Wizard** (Willkommen beim Assistenten zum Erzeugen von iSCSI-Targets) wird eingeblendet. Wählen Sie **Next** (Weiter).

Der Assistent führt Sie durch die zur Erzeugung eines Targets erforderlichen Schritte.

6 Der **Create iSCSI Target Wizard** (Assistent zum Erzeugen von iSCSI-Targets) zeigt die Option **iSCSI Target Identification** (Identifizieren von iSCSI-Targets) an. Geben Sie im Feld **Name** einen Namen und im Feld **Description** (Beschreibung) eine Beschreibung (optional) für das iSCSI-Target ein und klicken Sie auf **Next** (Weiter). Der Bildschirm **iSCSI initiators identifiers** (iSCSI-Initiatorkennungen) wird angezeigt.

7 Klicken Sie auf **Browse** (Durchsuchen) und wählen Sie den IQN für den Host, der mit dem Target verbunden ist. Der Host wird nur aufgelistet, wenn Schritt Schritt 1 in „Konfigurieren des Initiators (Host)“ auf Seite 14 erfolgreich beendet wurde.

ANMERKUNG: Das Feld für die IQN-Kennung muss ausgefüllt werden. Sie können die IQN-Kennung des Initiators entweder manuell eintippen oder sie im Fenster mithilfe der Optionen **Browse** (Durchsuchen) und **Advanced** (Erweitert) hinzufügen. Weitere Informationen zur Option Browse (Durchsuchen) finden Sie in Schritt 8. Weitere Informationen zur Option Advanced (Erweitert) finden Sie in Schritt 9.

8 Wenn Sie die Option **Browse** (Durchsuchen) wählen, führen Sie folgende Schritte durch, um den **IQN identifier** (die IQN-Kennung) auszuwählen:

a Wählen Sie **Browse** (Durchsuchen) und das Fenster **Add iSCSI Initiator** (iSCSI-Initiator hinzufügen) öffnet sich.

b Einzelheiten der iSCSI-Initiatorliste werden angezeigt. Sie können den iSCSI-Initiator manuell eintippen oder aus der Liste auswählen, den Namen des iSCSI-Initiators eingeben und auf **OK** klicken. Der von Ihnen eingegebene oder ausgewählte Wert wird daraufhin in das Feld **IQN identifier** (IQN-Kennung) im Fenster **iSCSI Initiators Identifiers** (iSCSI-Initiatorkennungen) übernommen. Wählen Sie **Next** (Weiter). Fahren Sie mit Schritt 10 fort.

9 Wenn Sie die Option **Advanced** (Erweitert) wählen, können Sie den **IQN identifier** (die IQN-Kennung) wie folgt auswählen:

a Wenn Sie die Option **Advanced...** (Erweitert...) auswählen, öffnet sich das Fenster **Advanced Identifiers** (Erweiterte Kennungen) und die Option **Add** (Hinzufügen) wird angezeigt. Wählen Sie **Add** (Hinzufügen).

b Das Fenster **Add/Edit Identifier** (Kennung Hinzufügen/Bearbeiten) wird angezeigt und bietet folgende vier Optionen an, um den **IQN identifier** (die IQN-Kennung) hinzuzufügen: **IQN**, **DNS Domain Name** (DNS-Domainname), **IP address** (IP-Adresse) und **MAC Address** (MAC-Adresse). Wählen Sie eine der vier Optionen aus.

c Tippen Sie den Wert ein oder wählen Sie ihn über die Option **Browse** (Durchsuchen) aus und klicken Sie auf **OK**.

Die IQN-Kennung wird im Fenster **Advanced Identifiers** (Erweiterte Kennungen) angezeigt und die Felder **IQN**, **DNS Domain Name** (DNS-Domainname), **IP Address** (IP-Adresse) und **MAC Address** (MAC-Adresse) werden ausgefüllt.

d Wählen Sie den so übernommenen Wert aus und klicken Sie auf **OK**.

e Die passenden Informationen werden im Fenster **iSCSI-Initiator Identifiers** (iSCSI-Initiatorkennungen) in das Feld **IQN identifier** (IQN-Kennung) übernommen. Klicken Sie auf **Advanced** (Erweitert), um alternative Kennungen anzuzeigen.

f Wählen Sie **Next** (Weiter).

ANMERKUNG: IQNs arbeiten unabhängig von der DNS-Konfiguration. Sie können somit auch die IP-Adresse oder die MAC-Adresse des Initiators ungeachtet der DNS-Konfiguration angeben.
Die Option, einen DNS-Domainnamen anzugeben, ist in das Snap-in von iSCSI Software Target integriert. Wenn Sie DNS-Namen verwenden, müssen Sie DNS korrekt konfigurieren (einschließlich Forward und Reverse Lookup-Zonen) und den vollständigen qualifizierten Domainnamen (fully qualified domain name (FQDN)) des Initiators angeben. Wenn Sie das Target auch nach Angabe der Initiator-FQDN nicht mit dem Initiator verbinden können, starten Sie den Befehl **nslookup InitiatorIP** am Targetserver, um festzustellen, ob Reverse Lookup korrekt aktiviert ist. Funktioniert der Befehl *nslookup* nicht, zeigt Ihnen dies an, dass der Reverse Lookup im DNS nicht konfiguriert ist. Konfigurieren Sie in diesem Fall das Target neu, um den Initiator-IQN, die IP-Adresse oder die MAC-Adresse zu verwenden.

10 Das Fenster **Completing the Create iSCSI Target Wizard** (Fertigstellen des Assistenten zum Erzeugen von iSCSI-Targets) wird geöffnet. Klicken Sie auf **Finish** (Fertigstellen).

Erzeugen einer virtuellen Festplatte

1 Klicken Sie mit der rechten Maustaste auf das neu erzeugte Target und klicken Sie dann auf **Create Virtual Disk for iSCSI Target** (Virtuelle Festplatte für iSCSI-Target erzeugen). Der **Create Virtual Disk Wizard** (Assistent zum Erzeugen von virtuellen Festplatten) wird geöffnet. Wählen Sie **Next** (Weiter).

2 Um eine Datei zu erstellen, wählen Sie die Option **Browse** (Durchsuchen), wählen Sie einen Datenträger im Speicherarray aus und geben Sie einen Dateinamen mit der Erweiterung **.vhd** ein.

Erstellen Sie zum Beispiel **Z:\vol1.vhd**, wobei Z der Datenträger des Speicherarrays und *vol1.vhd* der Dateiname ist. Wählen Sie **Next** (Weiter).

3 Wählen Sie im Fenster **Size** (Größe) unter **Currently available free space** (Verfügbarer freier Speicher) die passende Größe aus und klicken Sie auf **Next** (Weiter).

4 Unter Umständen wird das Fenster **Description** (Beschreibung) angezeigt. Falls erforderlich, geben Sie hier eine Beschreibung der virtuellen Festplatte ein und klicken Sie auf **Next** (Weiter).

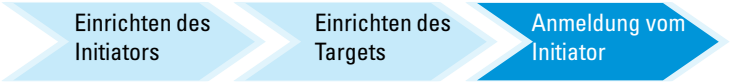
5 Wählen Sie im Fenster **Add** (Hinzufügen) den Targetnamen aus und klicken Sie auf **Next** (Weiter).

6 Das Fenster **Completing the Create Virtual Disk Wizard** (Fertigstellen des Assistenten zum Erzeugen von virtuellen Festplatten) wird geöffnet. Klicken Sie auf **Finish** (Fertigstellen).

VORSICHT: Wenn mehrere Hosts auf dasselbe Target zugreifen, können Daten korrumpiert werden. Weitere Informationen finden Sie unter „Aktivieren von Multi-Path beim Initiator“ auf Seite 50.

ANMERKUNG: Sie können mehrere virtuelle Festplatten auf demselben Datenträger erzeugen.

Anmelden - Konfigurieren der Initiator-Target-Verbindung vom Initiator (Host) aus



1 Klicken Sie am iSCSI-Initiator (Host) auf **Start**→ **Programs** (Programme)→ **Microsoft iSCSI Initiator**→ **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators)→ Registerkarte **Targets**.

2 Aktualisieren Sie die Bildschirmanzeige. Das Targetgerät des PowerVault Speichersystems, das Sie in „Konfigurieren einer iSCSI-Verbindung mit dem PowerVault NAS-Speichersystem“ auf Seite 14 erstellt haben, wird im IQN-Namensformat angezeigt.

3 Wählen Sie im Fenster **Log On to Target** (Anmeldung beim Target) **Logon** (Anmeldung), **Automatically Restore** (Automatisch Wiederherstellen) und **Enable multi-path** (Multi-Path aktivieren).

4 Klicken Sie auf **Advanced** (Erweitert). Wählen Sie im Fenster **Advanced Settings** (Erweiterte Einstellungen) die Registerkarte **General** (Allgemein) und wählen Sie die nachstehenden Optionen aus dem Drop-Down-Menü aus:

- **Local Adapter** (Lokaler Adapter) – Microsoft iSCSI-Initiator
- **Source IP** (Quellen-IP)– Eine der Host-IP-Adressen, die für den iSCSI-Datenverkehr verwendet wird
- **Target Portal**– Die iSCSI-IP-Addresse der PowerVault Speicherlösung

5 Klicken Sie im Fenster **Advanced Settings** (Erweiterte Einstellungen) auf **OK**.

6 Klicken Sie im Fenster **Log On to Target** (Anmeldung beim Target) auf **OK**.

In der Registerkarte **Targets** wird der Status des Targets als **Connected** (Verbunden) angezeigt.

7 Um Multipathing zu ermöglichen, können Sie Microsoft MPIO dazu verwenden, mehrere Sitzungen vom Host zum selben Targetgerät einzurichten. So richten Sie Mehrfachsitzungen ein:

a Öffnen Sie die Registerkarte **Targets** und wählen Sie das Target mit dem Status **Connected** (Verbunden) aus.

b Wiederholen Sie Schritt 1 bis Schritt 5.

c Klicken Sie auf **Advanced Settings** (Erweiterte Einstellungen). Wählen Sie in den **Targetportal**adressen die redundante Host-IP-Adresse und die IP-Adresse der PowerVault Speicherlösung aus.

ANMERKUNG: Während der Installation der iSCSI Initiator-Software wird bereits Microsoft MPIO ausgewählt. MPIO wird vom Initiator Version 2.06 oder höher unterstützt. Für eine effiziente MPIO-Verbindung benötigen Sie zwei dedizierte iSCSI-Netzwerkkarten beim Target und beim Initiator. Mehrfachverbindungen pro Sitzung (Multiple connections per session (MC/S)) wird von der PowerVault Speicherlösung nicht unterstützt.

8 Um die iSCSI-Festplatte als lokale Festplatte zu initialisieren und zu konfigurieren und iSCSI-E/A-Operationen durchzuführen, wählen Sie **Computer Management**→ Option **Disk Management** (Laufwerksverwaltung).

VORSICHT: Wenn mehrere Hosts auf dasselbe Target zugreifen, können Daten korrumpiert werden. Weitere Informationen finden Sie unter „Aktivieren von Multi-Path beim Initiator“ auf Seite 50.

Methode 2 (Erkennung über den iSNS-Server)

In diesem Abschnitt wird die iSCSI-Target-Erkennung mithilfe des iSNS-Servers beschrieben. Weitere Informationen über den iSNS-Server finden Sie unter „Anhang“ auf Seite 43.

Voraussetzungen

Führen Sie vor der iSCSI-Target-Erkennung folgende Schritte durch:

1. Bestimmen Sie ein System, das als iSNS-Server dienen soll.
2. Stellen Sie sicher, dass sich Initiator und Target im selben Netzwerk wie der iSNS-Server befinden (siehe Abbildung 1-1 und Abbildung 1-2).
3. Laden Sie die Software Microsoft iSCSI Initiator von der Microsoft-Support-Website unter **support.microsoft.com** herunter und installieren Sie den Initiator (Host).
4. Laden Sie die Software Microsoft iSNS Server von der Microsoft-Support-Website unter **support.microsoft.com** herunter und installieren Sie die Software auf einem Client/Server, auf dem ein Microsoft® Windows®-Betriebssystem läuft.

   ANMERKUNG: Installieren Sie die Software iSNS Server nicht auf dem Initiator (Host) oder dem Target (PowerVault Speicherlösung). Installieren Sie die Software auf einem eigenen Client/Server mit Windows-Betriebssystem.
5. Schalten Sie das PowerVault-Speichersystem ein und erstellen Sie einen oder mehrere Datenträger im Storagearray, um virtuelle Festplatten für iSCSI-Targets zu erzeugen.

Konfigurieren von Einstellungen vom Initiator aus

Einrichten des Initiators → Einrichten des Targets → Anmeldung vom Initiator aus

1. Konfigurieren Sie den Microsoft iSCSI-Initiator mit den Daten vom iSNS-Server. Öffnen Sie **Start**→ **Programs** (Programme)→ **Administrative Tools** (Verwaltung)→ **Microsoft iSCSI Initiator**→ Registerkarte **Discovery** (Erkennung)→ **Add iSNS** (iSNS hinzufügen).
2. Fügen Sie die IP-Adresse des iSNS-Servers hinzu und klicken Sie auf **OK** (siehe Abbildung 1-1 und Abbildung 1-2).

Einrichten des Targets (PowerVault Speichersystem)

Einrichten des Initiators → Einrichten des Targets → Anmeldung vom Initiator aus

1. Öffnen Sie im PowerVault-Speichersystem **Start**→ **Server Manager**→ **Storage** (Speicherung)→ **Microsoft iSCSI Software Target**.

Die **PowerVault Server Manager Management Console** öffnet sich.

2 Wählen Sie **Microsoft iSCSI Software Target**, das sich im Speicher-Snap-in befindet, und klicken Sie mit der rechten Maustaste auf **Properties** (Eigenschaften).

3 Öffnen Sie im Fenster **Properties** (Eigenschaften) die Registerkarte **iSNS** und fügen Sie die Daten des iSNS-Servers (DNS-Name oder IP-Adresse) hinzu.

ANMERKUNG: Es wird empfohlen, nur Netzwerkkarten für das iSCSI Netzwerk zu aktivieren.

4 Um ein Target zu erzeugen, folgen Sie den Anweisungen unter „Konfigurieren einer iSCSI-Verbindung mit dem PowerVault NAS-Speichersystem“ auf Seite 14.

ANMERKUNG: Verwenden Sie unter Schritt 7der Targetkonfiguration die Option **Browse** (Durchsuchen), um sicherzustellen, dass im Fenster **iSCSI Initiator Identifier** (iSCSI-Initiatorkennung) alle Initiatoren dargestellt werden, die beim iSNS-Server registriert sind.

5 Um eine virtuelle Festplatte zu erzeugen, folgen Sie den Anweisungen unter „Erzeugen einer virtuellen Festplatte“ auf Seite 17.

Anmeldung - Konfigurieren der Initiator-Target-Verbindung vom Initiator (Host) aus

Informationen über das Konfigurieren der Initiator-Target-Verbindung finden Sie unter „Anmelden - Konfigurieren der Initiator-Target-Verbindung vom Initiator (Host) aus“ auf Seite 18.

3

Einzelheiten zum Target

In diesem Abschnitt wird der vollständige iSCSI-Setup beschrieben, der die Einstellungen für iSCSI-Initiator und Target sowie für das Einrichten von Verbindungen umfasst.

Einrichten von Target-IP-Adressen in der PowerVault™ NAS Speicherlösung

Weisen Sie je nach Ihrer Systemkonfiguration (mit einer oder zwei dedizierten Netzwerkkarten) den iSCSI-Netzwerkkarten IP-Adressen zu. Verwenden Sie die IP-Adresse, die Sie der/den iSCSI-Netzwerkkarte(n) in der Registerkarte **Target Portals** (Targetportale) des Initiators zur Erkennung zugewiesen haben.

Konfigurieren von Microsoft® iSCSI Software Targets

Bevor Sie iSCSI-Targets konfigurieren, müssen Sie einige LUNs erzeugen und Speicherplatz für das Erzeugen von virtuellen Festplatten für iSCSI-Targets reservieren. Im folgenden Abschnitt finden Sie eine Schritt-für-Schritt-Anleitung für das Erzeugen von Speicherplatz.

1. Netzwerkeinstellungen auf dem iSCSI-Targetgerät konfigurieren–Die PowerVAult NAS Speicherlösung ist so konfiguriert, dass sie für die Netzwerkeinstellungen DHCP als Standardeinstellung verwendet. Das PowerVault-Speichersystem ist für Multi-Path-Operationen ausgelegt und mit zwei RJ45-Ethernet-Anschlüssen ausgestattet. Sie können eine optionale zusätzliche Netzwerkkarte hinzufügen. Im Fenster **PowerVault NAS Configuration tasks** (PowerVault Konfigurationsaufgaben) werden die grundlegenden Einstellungen angezeigt.

   ANMERKUNG: Es wird empfohlen, dedizierte iSCSI-Netzwerkkarten nicht im öffentlichen Netzwerk sondern in separaten Subnetzen zu konfigurieren.

ANMERKUNG: An dieser Stelle soll auch darauf hingewiesen werden, dass die Größe der LUN der Speicherlösung nicht mit der Größe des iSCSI-Targets zu verwechseln ist. Das iSCSI-Target wird in einem späteren Schritt konfiguriert und dem Speicher zugeordnet, der für eine bestimmte Anwendung auf dem Host-Server benötigt wird. Es wird empfohlen, die Größe der LUN in der Speicherhardware so groß wie vernünftigerweise möglich zu wählen, damit das Speicher-Untersystem die Benutzung des der erzeugten LUN zugrundeliegenden physikalischen Laufwerks optimieren kann. In diesem Fall entscheiden wir uns wie unten gezeigt dafür, eine LUN mit der maximalen bei dieser Hardware verfügbaren Größe zu erzeugen. Diese iSCSI-LUN kann die iSCSI-Targets, die später aufgrund des Bedarfs der Host-Anwendung erzeugt werden, nicht aufnehmen.

2 LUNs für die Verwendung vorbereiten–Die PowerVault NAS Speicherlösung läuft auf einer Plattform, die auf einem Microsoft Windows® - Betriebssystem basiert. Die Schritte zur Vorbereitung von LUNs, wie beispielsweise einen Laufwerkbuchstaben für den Internen Server zuzuweisen, einen Namen für den Datenträger zu vergeben usw., dienen dem Setup des Windows-Betriebssystems. Der Setup-Assistent fordert Sie zur Eingabe der erforderlichen Informationen auf und fasst diese dann in einem Fenster zusammen, bevor er die notwendigen Schritte zur Bereitstellung des Speicherplatzes unternimmt.

Die LUN wurde nun erzeugt und kann verwendet werden. Schritt 3 erzeugt iSCSI-Targets und ordnet die iSCSI-Targets der neu erzeugten LUN zu.

3 Konfigurieren von Netzwerkkarten für den iSCSI-Datenverkehr bei der PowerVault Speicherlösung–Sie müssen zunächst dedizierte Netzwerkkarten für den iSCSI-Datenverkehr konfigurieren und dann iSCSI-Targets erzeugen.

ANMERKUNG: Erzeugen Sie iSCSI-Targets erst, nachdem Sie die Registerkarte **Discovery** (Erkennung) im iSCSI-Initiator konfiguriert haben.

So konfigurieren Sie dedizierte iSCSI-Netzwerkkarten:

a Öffnen Sie **PowerVault NAS Management Console→ iSCSI Target**.

b Klicken Sie mit der rechten Maustaste auf iSCSI Software Target und wählen Sie **Properties** (Eigenschaften).

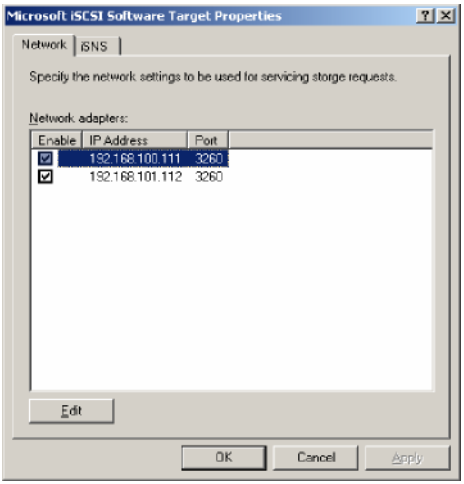
c Öffnen Sie im Fenster **Microsoft iSCSI Software Target Properties** (Eigenschaften von Microsoft iSCSI Software Target) die Registerkarte **Network** (Netzwerk). Alle Netzwerkkarten der PowerVault NAS Speicherlösung werden aufgelistet.

d Klicken Sie auf **Edit** (Bearbeiten) und deaktivieren Sie IP-Adressen für das öffentliche und das interne Netzwerk in der Liste. Durch das Deaktivieren der IP-Adressen für das öffentliche und das interne Netzwerk in der Liste stellen Sie sicher, dass nur die dedizierten iSCSI-Netzwerkkarten für den iSCSI-Datenverkehr konfiguriert werden.

e Wenn Sie in Ihrem Netzwerk einen iSNS-Server konfiguriert haben, öffnen Sie die Registerkarte **iSNS** und fügen Sie die IP-Adresse des iSNS-Servers hinzu. Klicken Sie auf **OK**.

4 Erzeugen von iSCSI-Targets–So erzeugen Sie ein iSCSI-Target:

Abbildung 3-1. Erzeugen von iSCSI-Targets



a Klicken Sie in der **PowerVault NAS Management Console** mit der rechten Maustaste auf **iSCSI Targets** im linken Fensterbereich, um den **Create iSCSI Target Wizard** (Assistenten zum Erzeugen von iSCSI-Targets) zu starten.
Das Fenster **Welcome to the Create iSCSI Target Wizard** (Willkommen beim Assistenten zum Erzeugen von iSCSI-Targets) wird angezeigt.

b Klicken Sie auf **Next** (Weiter).
Das Fenster **iSCSI Target identification** (Identifikation von iSCSI-Targets) wird angezeigt.

c Geben Sie im Feld **Target name** einen Targetnamen und im Feld **Description** eine Beschreibung des Targets ein. Sie können die Option **Browse** (Durchsuchen) verwenden, um die Server/Clients im Netzwerk anzuzeigen und auszuwählen.
Das Fenster **iSCSI initiators identifiers** (iSCSI-Initiatorkennungen) wird angezeigt. Sie müssen jedem iSCSI-Target einen iSCSI-Initiator zuordnen. Der iSCSI-Initiator ist der Host, der Zugriff auf den durch den iSCSI-Targetnamen repräsentierten Speicher anfordert.

d Geben Sie im Fenster **iSCSI Initiators Identifiers** (iSCSI-Initiatorkennungen) den IQN (iSCSI Qualified Name) des iSCSI-Initiators ein. Sie können den IQN entweder manuell eintippen oder die Option **Browse** (Durchsuchen) verwenden und den iSCSI-Initiator aus der Liste auswählen. Sie können den iSCSI-Initiator ebenfalls angeben, indem Sie die Option **Advanced** (Erweitert) verwenden. Wenn Sie auf **Advanced** (Erweitert) klicken, wird das Fenster **Advanced Identifiers** (Erweiterte Kennungen) eingeblendet. Klicken Sie im Fenster **Advanced Identifier** (Erweiterte Kennung) auf **Add** (Hinzufügen) und geben Sie den Kennungstyp sowie die besonderen Kennungsinformationen ein.

Öffnen Sie **Advanced Identifier** (Erweiterte Kennung)→ **Add** (Hinzufügen)→ **Add/Edit Identifier** (Kennung Hinzufügen/Bearbeiten→ **Identifier Type** (Kennungstyp) und wählen Sie entweder den IQN, den DNS-Domainnamen, die IP-Adresse oder die MAC-Adresse aus, um die Initiatorkennung hinzuzufügen. In Abbildung A-5 erfolgt die Erkennung des iSCSI-Initiators über die IP-Adresse. Sie können die Option **Browse** (Durchsuchen) verwenden, um den Wert aus der Liste der verfügbaren Targets auszuwählen.

ANMERKUNG: Es wird empfohlen, den IQN als Kennung zu verwenden.

Die **PowerVault NAS Management Console** zeigt nun das neu erstellte iSCSI-Target an. Die **PowerVault NAS Management Console** zeigt auch die für die iSCSI-Targets verfügbaren Geräte an. Der von den iSCSI-Initiatoren (Anwendungs-Hosts) verwendete Speicher wird in einem späteren Schritt bei der Erstellung der virtuellen Festplatten definiert.

5 Erstellen und Zuordnen von virtuellen Festplatten zu einem Target–Bei Microsoft-basierten iSCSI-Target-Lösungen müssen Sie auf den iSCSI-Targets virtuelle Festplatten anlegen. Die virtuellen Festplatten repräsentieren die von den iSCSI-Initiatoren verwendeten Speicherdatenträger. Die maximale Kapazität aller virtuellen Festplatten auf einem iSCSI-Target bei einer Microsoft-basierten iSCSI-Target-Lösung beträgt 16 Terabyte (16 TB) je Target.

Die folgende Vorgehensweise beschreibt das Erzeugen einer virtuellen Festplatte. In diesem Beispiel werden eine virtuelle Festplatte mit 100 GB und eine virtuelle Festplatte mit 200 GB auf dem iSCSI-Target angelegt. Diese beiden virtuellen Festplatten werden von den iSCSI-Initiatoren über das TCP/IP-Netzwerk als Laufwerke identifiziert.

a Klicken Sie mit der rechten Maustaste auf den Targetnamen und starten Sie den **Create Virtual Disk Wizard** (Assistent zum Erzeugen virtueller Festplatten).

b Klicken Sie auf **Next** (Weiter). Das Fenster **File** (Datei) wird angezeigt.

Erzeugen Sie die virtuelle Festplatte auf dem internen Festplatten-Laufwerk (die auf dem angeschlossenen Speicherarray verfügbaren RAID-Laufwerke), das für das iSCSI-Target verfügbar ist.

ANMERKUNG: Wählen Sie im Fenster File (Datei) mithilfe der Option Browse (Durchsuchen) das interne Festplatten-Laufwerk aus und geben Sie einen Namen für die virtuelle Festplattendatei mit der Erweiterung .vhd ein.

c Klicken Sie auf **Next** (Weiter). Das Fenster **Size** (Größe) wird angezeigt.

Die Größe der virtuellen Festplatte hängt von den Anforderungen des Hostservers ab.

d Wählen Sie die Größe der virtuellen Festplatte aus und klicken Sie auf **Next** (Weiter). Im vorliegenden Beispiel wird eine Größe von 100 GB bei einer Gesamtkapazität von 501 GB auf dem Laufwerk gewählt. Das Fenster **Description** (Beschreibung) wird angezeigt.

e Das Feld **Description** (Beschreibung) ist optional. Sie sollten jedoch eine Beschreibung eingeben, um die Verwaltung zu erleichtern.

f Klicken Sie auf **Next** (Weiter). Das Fenster **Access** (Zugriff) wird angezeigt.

g Klicken Sie auf **Add** (Hinzufügen) und geben Sie die Informationen zum iSCSI-Target ein.

Damit der Anwendungs-Host die virtuelle Festplatte als iSCSI-Speicherlaufwerk nutzen kann, müssen Sie die virtuelle Festplatte einem iSCSI-Target zuordnen.

h Klicken Sie auf Next (Weiter). Das Fenster **Completing the Create Virtual Disk Wizard** (Fertigstellen des Assistenten zum Erzeugen einer virtuellen Festplatte) wird angezeigt und informiert Sie darüber, dass die virtuelle Festplatte erfolgreich erzeugt wurde.

i Wiederholen Sie Schritt a bis Schritt h, um eine weitere virtuelle Festplatte zu erzeugen.

Nach ihrer Konfiguration werden die dem iSCSI-Target zugeordneten virtuellen Festplatten in der **PowerVault NAS Management Console** angezeigt.

In der Ansicht **iSCSI-Targetgerät** werden die Gesamtkapazität des Laufwerks und der freie Speicherplatz auf der für iSCSI-Targets verfügbaren Festplatte (RAID-Laufwerk) angezeigt.

Die Konfiguration des iSCSI-Targets ist jetzt abgeschlossen.

Konfigurieren von Geräten

Sie können alle Operationen in Verbindung mit virtuellen Festplatten (Geräten) mit den folgenden Optionen der **PowerVault NAS Management Console** durchführen:

- Create/Delete Virtual Disk (virtuelle Festplatte Erzeugen/Entfernen)–Virtuelle Festplatten werden durch die Erweiterung **.vhd** dargestellt. Mit dieser Option können Sie virtuelle Festplatten erzeugen oder entfernen.
- Extend Virtual Disk (Virtuelle Festplatte Erweitern)–Sie können die Größe einer virtuellen iSCSI-Festplatte ohne Datenverlust oder Neustart des iSCSI-Targets dynamisch vergrößern.
- Import (Importieren)–Sie können alte virtuelle Festplatten oder zuvor auf demselben oder einem anderen Server erstellte bestehende virtuelle Festplatten importieren. Diese Option ist während eines Software-Upgrades hilfreich.
- Disable (Deaktivieren)–Sie können die virtuelle Festplatte offline setzen und sie mit der Option **Enable** (Aktivieren) wieder online stellen.

- Assign/Remove Target (Target Zuweisen/Entfernen)–Ordnen Sie virtuelle Festplatten einem oder mehreren Targets zu, entfernen Sie eine bestehende Zuordnung.
- Create Snapshot (Speicherauszug anfertigen)–Sie können bei jeder Gelegenheit einen Speicherauszug des Inhalts der virtuellen Festplatte anfertigen.
- Disk Access (Festplattenzugriff)–Einbinden ("mount") mit Lese-/Schreibzugriff (Lese-/Schreibzugriff für die virtuelle Festplatte, indem sie als Laufwerk des PowerVault NAS Speichersystems eingebunden wird. Die eingebundene virtuelle Festplatte erscheint als lokale Festplatte).

VORSICHT: Bevor Sie die virtuelle Festplatte einbinden, trennen Sie alle iSCSI-Targets, die diese virtuelle Festplatte benutzen. Unterlassen Sie dies, kann eine Korrumpierung von Daten die Folge sein.

ANMERKUNG: Lastverteilung und Ausfallsicherung sind durch Nutzung von Microsoft MPIO oder durch mehrere Verbindungen pro Sitzung (Multiple Connections per Session (MC/S)) möglich. Momentan wird nur die Option MPIO von PowerVault NAS Speicherlösungs unterstützt, die mit einer 3.2 iSCSI Target und Microsoft iSCSI Initiator Version 2.06 oder höher ausgestattet sind. Die MC/S-Option wird vom PowerVault NAS-Speichersystem nicht unterstützt.

Konfigurieren von iSCSI-LUNs

1 Konfigurieren Sie das iSCSI-Targetgerät über das Disk Management (Datenträgerverwaltung). Gehen Sie zum iSCSI-Initiator-Host und klicken Sie auf **Start**→ **Control Panel** (Bedienfeld)→ **Administrative tools** (Verwaltung)→ **Computer Management**→ **Disk Management** (Datenträgerverwaltung).

Im rechten Fensterbereich wird die iSCSI-Festplatte mit dem Status **Unknown Not Initialized** (Unbekannt und nicht initialisiert) und **Unallocated** (Nicht zugeordnet) angezeigt.

2 Das Fenster **Welcome to the Initialize and Convert Disk Wizard** (Willkommen beim Assistenten zum Initialisieren und Konvertieren von Datenträgern) wird angezeigt. Starten Sie den **Initialize and Convert Disk Wizard** (Assistenten zum Initialisieren und Konvertieren von Datenträgern).

a Behalten Sie die Standardeinstellungen bei und klicken Sie in allen Fenstern auf **Next** (Weiter).

b Das Fenster **Completing the Initialize and Convert Disk Wizard** (Fertigstellen des Assistenten zum Initialisieren und Konvertieren von Datenträgern) wird angezeigt. Klicken Sie auf **Finish** (Fertigstellen).

ANMERKUNG: Dynamische Datenträger werden bei der iSCSI-Konfiguration nicht unterstützt.

3 Kehren Sie zum **Disk Management** (Datenträgerverwaltung) zurück. Die iSCSI-Festplatte mit dem Status **Unallocated** (Nicht zugeordnet) wird nun als **Basic** (Minimal) und **Unallocated** (Nicht zugeordnet) angezeigt. Klicken Sie mit der rechten Maustaste auf die iSCSI-Festplatte und wählen Sie die Option **New Partition...** (Neue Partition...)

a Der **New Partition Wizard** (Assistent zum Erstellen neuer Partitionen) wird gestartet. Klicken Sie auf **Next** (Weiter).

b Wählen Sie im Fenster **Select Partition Type** (Partitionstyp festlegen) den Partitionstyp **Primary Partition** (Primäre Partition) aus. Klicken Sie auf **Next** (Weiter).

c Geben Sie im Fenster **Specify Partition Size** (Partitionsgröße festlegen) die Partitionsgröße an. Klicken Sie auf **Next** (Weiter).

d Weisen Sie im Fenster **Assign Drive Letter or Path** (Laufwerkbuchstaben oder -pfad zuordnen) über das Drop-Down-Menü einen Laufwerkbuchstaben zu. Klicken Sie auf **Next** (Weiter).

e Formatieren Sie die Partition mit den im Fenster **Format Partition** (Partition formatieren) vorgegebenen Standardeinstellungen. Geben Sie eine Laufwerkbezeichnung ein und klicken Sie auf **Next** (Weiter).

ANMERKUNG: Markieren Sie das Kontrollkästchen **Perform quick format** (Schnellformatierung durchführen), um den Formatierungsvorgang zu beschleunigen.

f Klicken Sie im Fenster **Completing the New Partition Wizard** (Fertigstellen des Assistenten zum Erstellen neuer Partitionen) auf **Finish** (Fertigstellen). Die neue Partition wurde erfolgreich erstellt.

4 Kehren Sie zum **Disk Management** (Datenträgerverwaltung) zurück. Die iSCSI-Festplatte wird mit der von Ihnen eingegebenen Laufwerkbezeichnung dargestellt.

ANMERKUNG: Dynamische Datenträger werden bei iSCSI nicht unterstützt.

Mehrfachsitzungen

Sie können Mehrfachsitzungen mit verschiedenen Initiator-Target-Kombinationen auf verschiedenen Geräten durchführen.

- Sie können einen Initiator so konfigurieren, dass er Zugriff auf verschiedene iSCSI-Targets mehrerer PowerVault NAS-Speichersysteme hat.
- Sie können mehrere Initiatoren so konfigurieren, dass sie Zugriff auf verschiedene iSCSI-Targets desselben oder verschiedener PowerVault NAS-Speichersysteme haben.
- Sie können jedoch mehrere Initiatoren nicht so konfigurieren, dass sie Zugriff auf dasselbe iSCSI-Target einer PowerVault NAS Speicherlösung haben.

VORSICHT: Ein Zugriff auf dasselbe Targetgerät mit mehreren iSCSI-Initiatoren mit 3.2 iSCSI-Targets wird nicht unterstützt, da dies nicht unterstütztes Host-Clustering erfordern würde. Ein Versuch, mit mehreren iSCSI-Initiatoren mit 3.2 iSCSI-Target auf dasselbe Targetgerät zuzugreifen, kann Daten korrumpieren.

iSCSI-Speicherauszüge

Sie können mit Microsoft iSCSI Software Target Speicherauszüge als Teil eines umfassenden Backup- und Wiederherstellungssystems erstellen und verwalten. Speicherauszüge sind Schattenkopien, die mithilfe der Volume Shadow Copy Service (VSS)-Technologie erstellt werden.

Um die Erstellung von Speicherauszügen und die Einbindung von virtuellen iSCSI-Festplatten für regelmäßige Backups zu automatisieren, können Sie den **Schedule Snapshot Wizard** (Assistent für planmäßige Speicherauszüge) verwenden. Speicherauszüge von virtuellen Festplatten, die sich auf einem Datenträger mit NTFS-Dateisystem befinden, sind persistent, d. h. sie bleiben nach einem Systemneustart erhalten.

Speicherauszüge, die auf dem iSCSI-Targetserver erstellt werden, sind absturzsicher. iSCSI-Speicherauszüge werden mithilfe von VSS und einem Speicherarray mit einem auf Verwendung mit VSS abgestimmten Hardwareprovider erstellt. Um unter Microsoft iSCSI Software Target absturzsichere Speicherauszüge erstellen zu können, benötigen Sie den Microsoft iSCSI Software Target VSS Hardware Provider. Der Microsoft iSCSI Software Target VSS Hardware Provider ist als Installationsoption in iSCSI Software Target verfügbar. Der

Hardwareprovider erstellt zusammen mit der lokalen VSS ein absturzsicheres Bild des Datenträgers, das auf einen zentralen Backup-Server übertragen werden kann.

Bei einem PowerVault-Speichersystem können Sie einen iSCSI-Speicherauszug auf zwei Arten erstellen:

- Erzeugen Sie manuell einen Speicherauszug einer einzelnen virtuellen Festplatte in der Microsoft iSCSI Software Target Console.
- Verwenden Sie den **Schedule Snapshot Wizard** (Assistent für planmäßige Speicherauszüge), um einen Plan zur Erstellung eines einzelnen Speicherauszugs oder zur automatischen Erstellung von wiederholten Speicherauszügen aufzustellen.

Vor dem Erstellen von Speicherauszügen

Vor dem Erstellen von Speicherauszügen virtueller Festplatten führen Sie folgende Schritte durch:

ANMERKUNG: Verwenden Sie den Windows Explorer, um den Datenträger zu öffnen, der die virtuelle Festplatte enthält, für die sie Speicherauszüge erstellen möchten.

1. Öffnen Sie **Volume** (Datenträger)→ **Properties** (Eigenschaften)→ **Shadow Copies** (Schattenkopien)→ **Settings** (Einstellungen). Stellen Sie sicher, dass bei der Option **Located on this volume** (Auf diesem Datenträger) in der Registerkarte **Storage Area** (Speicherbereich) der Laufwerkbuchstabe angezeigt wird, der dem Datenträger entspricht.
2. Klicken Sie auf **Details** (Einzelheiten), um die Verwendung des Datenträgers zu überprüfen. Die Standardeinstellungen lauten wie folgt:
   - **Maximale Größe**
   - **Use limit** (Benutzungsgrenze)–Größe in MB oder **No Limit** (Keine Begrenzung)

   Ändern Sie die Größe entsprechend der virtuellen Festplatte/dem Speicherauszug oder ändern Sie die Einstellung in **No Limit** (Keine Begrenzung).

VORSICHT: Stellen Sie sicher, dass Sie über genug Speicherplatz zur Aufnahme der Speicherauszüge der virtuellen Festplatte verfügen. Ist nicht genug Speicherplatz vorhanden, gehen die Speicherauszüge verloren.

3 Nachdem Sie die notwendigen Änderungen vorgenommen haben, klicken Sie auf **OK**.

VORSICHT: Auch wenn Sie die Standardeinstellungen nicht ändern, öffnen Sie Volume (Datenträger)→ Properties (Eigenschaften)→ Shadow Copies (Schattenkopien)→ Settings (Einstellungen) und klicken Sie auf OK. Hierdurch wird sichergestellt, dass Speicherauszüge im Falle des Versagens eines Knotens korrekt wiederhergestellt werden. Überschreitet die Größe der Speicherauszüge den maximalen Speicherplatz, wird der älteste Speicherauszug gelöscht.

ANMERKUNG: Von jedem Datenträger können ungeachtet der Anzahl der darin erzeugten virtuellen Festplatten bis zu 512 Speicherauszüge von virtuellen iSCSI-Festplatten erstellt werden. Speicherauszüge erleichtern die effiziente Speicherplatznutzung, da nur die Änderungen seit der letzten Datensicherung gespeichert werden.

Einen Plan für Speicherauszüge erstellen

So erstellen Sie planmäßig Speicherauszüge von virtuellen iSCSI-Festplatten:

1 Öffnen Sie **PowerVault NAS Management Console→ Microsoft iSCSI Software Target**.

2 Gehen Sie auf die Registerkarte **Snapshots** (Speicherauszüge), klicken Sie mit der rechten Maustaste auf **Schedules** (Pläne) und wählen Sie **Create Schedule** (Plan erstellen).

Das Fenster **Welcome to the Schedule Snapshot Wizard** (Willkommen beim Assistenten zum Planen von Speicherauszügen) wird angezeigt.

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

4 Das Fenster **Schedule Actions** (Aktionen planen) öffnet sich und bietet folgende Optionen:

`Take snapshots of the Virtual Disks (default)(Speicherauszüge von virtuellen Festplatten anfertigen (Standardeinstellung))`

`Take snapshots of the Virtual Disks and mount the snapshots locally (Speicherauszüge von virtuellen Festplatten anfertigen und lokal einbinden)`

Wählen Sie eine Option und klicken Sie auf **Next** (Weiter).

5 Geben Sie im Fenster **Name** einen Namen für den Plan ein und klicken Sie auf **Next** (Weiter).

6 Das Fenster **Virtual Disks** (Virtuelle Festplatten) öffnet sich und bietet folgende Optionen:

`Include all Virtual Disks (default)(alle virtuellen Festplatten (Standardeinstellung))`

`Include only the selected Virtual Disks (nur ausgewählte virtuelle Festplatten)`

Sie können alle oder nur ausgewählte virtuelle Festplatten für die Anfertigung von Speicherauszügen auswählen.

ANMERKUNG: Bei einer PowerVault NAS Speicherlösung werden alle virtuellen Festplatten im Fenster **Virtual Disks** (Virtuelle Festplatten) aufgelistet.

7 Das Fenster **Frequency** (Häufigkeit) öffnet sich und listet die folgenden Optionen auf–**Daily** (Täglich), **Weekly** (Wöchentlich), **Monthly** (Monatlich) und **One-time only** (nur zu bestimmtem Zeitpunkt). Wählen Sie eine Option und klicken Sie auf **Next** (Weiter).

8 Nun müssen Sie **Start Time (Zeitpunkt)**, **Days** (Tage), **Months** (Monate), **Start Date** (Startdatum) und weitere Zeitparameter wählen, abhängig davon, was Sie unter Schritt 7 als Häufigkeit angegeben haben. Stellen Sie diese Parameter auf die gewünschte Zeit ein. Klicken Sie auf **Next** (Weiter).

ANMERKUNG: Sie können den Plan zur Anfertigung planmäßiger Speicherauszüge auch später noch abändern.

9 Das Fenster **Completing the Schedule Snapshot Wizard** (Fertigstellen des Assistenten zum Planen von Speicherauszügen) wird angezeigt. Klicken Sie auf **Finish** (Fertigstellen).

Überprüfen des Plans für Speicherauszüge (Optional)

Nachdem Sie den Plan für die Speicherauszüge erstellt haben, öffnen Sie **PowerVault NAS Management Console→ Microsoft iSCSI Software Target→ Snapshots** (Speicherauszüge)→ **Schedules** (Pläne) und überprüfen Sie, ob im mittleren Fensterbereich der Name des Plans, die aktuelle Durchführung und die nächste Durchführung mit Zeitstempel angezeigt werden.

Aktive Speicherauszüge

Nachdem Sie den Plan für die Anfertigung von Speicherauszügen eingegeben haben, öffnen Sie die Registerkarte **Active Snapshots** (Aktive Speicherauszüge). Alle Einzelheiten zu Speicherauszügen einschließlich virtueller Quellenfestplatte, Zeitstempel und Exportstatus werden im mittleren Feld aufgelistet.

Sie können aktive Speicherauszüge mithilfe der Registerkarte **Active Snapshots** (Aktive Speicherauszüge) wie eine lokale Festplatte exportieren, löschen, zurücksetzen und einbinden.

- Export Snapshot (Speicherauszug exportieren)–Verwenden Sie diese Option, um einem Remotesystem einen Speicherauszug zur Verfügung zu stellen oder eine redundante Kopie eines Speicherauszugs anzufertigen. Verwenden Sie den **Export Snapshot wizard** (Assistenten zum Exportieren von Speicherauszügen), um den Speicherauszug auf ein iSCSI-Target zu exportieren. Initiatoren haben dann Zugriff auf den Speicherauszug (nur Lesezugriff). So exportieren Sie einen Speicherauszug:
  - **a** Öffnen sie die Registerkarte **Active Snapshots** (Aktive Speicherauszüge), wählen Sie im mittleren Fensterbereich den Speicherauszug, den Sie exportieren möchten, klicken Sie ihn mit der rechten Maustaste an und wählen Sie **Export Snapshot** (Speicherauszug Exportieren)
  - **b** Das Fenster **Welcome to the Export Snapshot Wizard** (Willkommen beim Assistenten zum Exportieren von Speicherauszügen) öffnet sich. Klicken Sie auf **Next** (Weiter).
  - **c** Fügen Sie im Fenster **Snapshot Access** (Zugriff auf Speicherauszüge) die Targets hinzu, denen Sie Lesezugriff auf diesen Speicherauszug gewähren möchten. Klicken Sie auf **Next** (Weiter).
  - **d** Klicken Sie auf **Finish** (Fertig stellen).
  - **e** Gehen Sie zum Target und überprüfen Sie, ob dieser Speicherauszug als virtuelle Festplatte hinzugefügt wurde.
- Delete snapshot (Speicherauszug löschen)–Wählen Sie den Speicherauszug aus, den Sie löschen möchten, klicken Sie ihn mit der rechten Maustaste an und klicken Sie auf **Delete** (Löschen).

  ANMERKUNG: Sie können keine eingebundenen Speicherauszüge löschen. Vor dem Löschen müssen Sie sie freigeben.

- Disk Access (Festplattenzugriff)–Sie können den Speicherauszug einer virtuellen iSCSI-Festplatte, die nur Lesezugriff besitzt, aus dem PowerVault NAS-Speichersystem einbinden, so dass er als lokale Festplatte erscheint.

VORSICHT: Wenn Sie einen Speicherauszug/eine virtuelle Festplatte freigeben, stellen Sie sicher, dass die Festplatte nicht verwendet wird. Eine Unterlassung kann eine Korrumpierung von Daten zur Folge haben.

ANMERKUNG: Sie können entweder eine virtuelle iSCSI-Festplatte (Lese-/Schreibzugriff oder nur Lesezugriff) einbinden oder ihren Speicherauszug (nur Lesezugriff), jedoch nicht beides. Falls Sie eine virtuelle Festplatte eingebunden haben und dann eine Einbindung des Speicherauszugs vornehmen, wird der vorherige Vorgang entfernt, ehe Sie fortfahren können.

- Rollback (Zurücksetzen)–Verwenden Sie diese Option, um eine virtuelle iSCSI-Festplatte auf einen früheren Speicherauszug zurückzusetzen. Für diesen Vorgang wird das Verzeichnis **temp** unter **C:\Windows\Temp** verwendet. Stellen Sie sicher, dass das Verzeichnis **temp** ausreichend Speicherplatz zur Aufnahme der Änderungsdatei aufweist. Das Zurücksetzen misslingt, wenn nicht genug Speicherplatz vorhanden ist.

  a Klicken Sie mit der rechten Maustaste auf den Speicherauszug und wählen Sie **Rollback to snapshot** (Auf Speicherauszug zurücksetzen). Wählen Sie **Yes** (Ja) in der Pop-up-Mitteilung

  b Um den Status des Zurücksetzens zu überprüfen, öffnen Sie die Registerkarte **Devices** (Geräte). Der Fortschritt des Zurücksetzens in % (Prozentsatz) wird im Abschnitt der virtuellen Festplatte des mittleren Fensterbereichs dargestellt.

  c Sie können das Zurücksetzen auch abbrechen. Brechen Sie ein Zurücksetzen jedoch nur ab, wenn Sie zu einem anderen Speicherauszug zurückkehren können. Andernfalls wird dringend empfohlen, das Zurücksetzen zu beenden.

ANMERKUNG: Bei einem Zurücksetzen gehen alle Daten auf der aktuellen virtuellen Festplatte verloren. Trennen Sie alle iSCSI-Targets, die diese virtuelle Festplatte verwenden, vom Initiator. Wenn die virtuelle Festplatte als Festplatte mit Lese-/Schreibzugriff eingebunden ist, geben Sie sie vor dem Zurücksetzen frei.

Trennen/Säubern von iSCSI-Geräten

Dieser Abschnitt beschreibt das Vorgehen zum Säubern von iSCSI-Geräten. Sie müssen das Säuberungsverfahren sowohl beim iSCSI-Target als auch beim iSCSI-Initiator durchführen.

Vom Initiator aus

Trennen Sie eine aktive Verbindung mit dem Target, indem Sie iSCSI-E/A-Vorgänge durch das Ausführen folgender Schritte anhalten:

1. Klicken Sie auf die Registerkarte **Start**→ **All Programs** (Alle Programme)→ **Microsoft iSCSI Initiator**→ **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators)→ Registerkarte **Targets**.
2. Wählen Sie das Target mit dem Status **Connected** (Verbunden) aus und klicken Sie auf **Details** (Einzelheiten).
3. Das Fenster **Target Properties** (Targeteigenschaften) öffnet sich. Wählen Sie in der Registerkarte **Sessions** (Sitzungen) das Kontrollkästchen neben der Kennung und klicken Sie auf **Logoff** (Abmelden). Die Verbindung wird getrennt.
4. Klicken Sie im Fenster **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators) auf die Registerkarte **Persistent Targets** (Dauerhafte Targets) und entfernen Sie die Einträge dauerhafter Targets.
5. Wenn Sie Namenseinträge von Target-IQNs löschen möchten, gehen Sie zur Registerkarte **Discovery** (Erkennung) und entfernen Sie die IP-Adresse /den DNS-Namen des PowerVault NAS-Speichersystems im Abschnitt **Target Portals** (Targetportale) oder entfernen Sie den Eintrag der IP-Adresse/des DNS-Namens des iSNS-Servers.
6. Öffnen Sie die Registerkarte **Targets** und klicken Sie auf **Refresh** (Aktualisieren). Der IQN-Name des Targets ist nicht aufgelistet.

Vom Target aus

Um virtuelle Festplatten vom iSCSI-Target zu entfernen, löschen Sie die virtuelle Festplatte, indem Sie folgende Schritte durchführen:

1. Öffnen Sie **PowerVault NAS Management Console→ Microsoft iSCSI Software Target→ iSCSI Targets**. Wählen Sie das Target und die zugeordneten virtuellen Festplatten, die gelöscht werden sollen.
   a. Im mittleren Fensterbereich werden alle virtuellen Festplatten aufgelistet. Klicken Sie mit der rechten Maustaste auf die zu löschende Festplatte und wählen Sie die Option **Remove Virtual Disk From iSCSI Target** (Virtuelle Festplatte vom iSCSI-Target entfernen).
   b. Wiederholen Sie Schritt a für alle diesem Target zugeordneten virtuellen Festplatten.
2. Um ein Target zu löschen, klicken Sie mit der rechten Maustaste auf das Target und wählen Sie die Option **Delete iSCSI Target** (iSCSI-Target löschen). Durchsuchen Sie Verzeichnisse manuell, um die dem Target zugeordnete **.vhd**-Datei zu lokalisieren und löschen Sie sie.
3. Um eine virtuelle Festplatte zu löschen, wählen Sie die Option **Devices** (Geräte), klicken Sie mit der rechten Maustaste im mittleren Fensterbereich auf die virtuelle Festplatte und wählen Sie **Delete Virtual Disk** (Virtuelle Festplatte löschen).

   ANMERKUNG: Schritt 3 löscht nur die Zuordnung in der iSCSI Target-Software, räumt jedoch nicht den Festplattenspeicherplatz im Datenträger. Sie müssen den Datenträger manuell durchsuchen und die **.vhd**-Datei löschen, um den Speicherplatz zu räumen.
4. Um einen iSNS-Servereintrag zu entfernen, klicken Sie mit der rechten Maustaste auf **Microsoft iSCSI Software Target→** wählen Sie **Properties** (Eigenschaften)→ Registerkarte **iSNS→ Remove the DNS name or IP address entry** (Eintrag des DNS-Namens oder der IP-Adresse entfernen).

4

Konfigurieren gesicherter iSCSI-Verbindungen über das CHAP (Challenge-Handshake Authentication Protocol)

Bis auf Sicherheitsschichten, die in den unteren TCP/IP- und Ethernet-Schichten vorhanden sein können, sind nur wenige Sicherheitsmerkmale des iSCSI-Protokolls in der iSCSI-Schicht selbst lokalisiert. Sie können die iSCSI-Sicherheitsmerkmale nach Bedarf aktivieren und deaktivieren.

Der Microsoft® iSCSI-Initiator überprüft mithilfe des CHAP-Protokolls (CHAP = Challenge-Handshake Authentication Protocol) die Identität von iSCSI-Hostsystemen, die versuchen, auf iSCSI-Targets zuzugreifen. Sowohl der iSCSI-Initiator als auch das iSCSI-Target verwenden CHAP und nutzen gemeinsam ein vordefiniertes Secret. Der Initiator fasst das Secret mit anderen Informationen zu einem Wert zusammen und berechnet mithilfe der Fun- ktion MD5 (Message Digest 5) eine eindirektionale Kontrollsumme. Der Kontrollwert wird an das Target übermittelt. Das Target berechnet aus dem gemeinsam genutzten Secret und weiteren Informationen seinerseits eine eindirektionale Kontrollsumme. Wenn beide Kontrollwerte übereinstimmen, ist die Authentifizierung des Initiators erfolgreich. Zu den weiteren Sicherheitsinformationen gehört ein Kennwert, der mit jedem CHAP-Dialog erhöht wird, um Wiederholungsangriffen vorzubeugen. Die Dell™ PowerVault™ NAS Speicherlösung unterstützt auch Mutual (gegenseitiges) CHAP.

CHAP gilt allgemein als sicherer als das PAP-Protokoll (Password Authentication Protocol).

CHAP und IPSec

Das CHAP-Protokoll dient zur Authentifizierung eines Verbindungspartners und basiert darauf, dass die Verbindungspartner ein Secret (ein Sicherheitsschlüssel, der ähnlich wie ein Passwort funktioniert) gemeinsam nutzen. Beim IP Security (IPSec)-Protokoll werden Authentifizierung und Datenverschlüsselung in der IP-Paketschicht durchgeführt und eine zusätzliche Sicherheitsstufe bereitgestellt.

Eindirektionale CHAP-Authentifizierung

Bei der eindirektionalen CHAP-Authentifizierung wird lediglich der Initiator vom iSCSI-Target authentifiziert. Das Secret wird nur für das Target definiert. Alle Initiatoren, die auf das Target zugreifen, müssen dasselbe Secret verwenden, um sich beim Target anmelden zu können. Um die eindirektionale CHAP-Authentifizierung festzulegen, nehmen Sie die in den nachstehenden Abschnitten beschriebenen Einstellungen für Target und Initiator vor.

Einstellungen für das iSCSI-Target

Bevor Sie die in diesem Abschnitt beschriebenen Einstellungen konfigurieren, stellen Sie sicher, dass bereits einige iSCSI-Targets und virtuelle Festplatten erstellt wurden und dass die virtuellen Festplatten den Targets zugeordnet sind.

1. Öffnen Sie bei einem iSCSI-Target **PowerVault NAS Management Console**→ **Microsoft iSCSI Software Target**→ **iSCSI Targets**→ <Targetname> und klicken Sie entweder mit der rechten Maustaste darauf und wählen **Properties** (Eigenschaften) oder öffnen Sie im Fensterbereich **Actions** (Aktionen)→ **More Actions** (Weitere Aktionen)→ **Properties** (Eigenschaften).

   Das Fenster **<Target Name> Properties** (Eigenschaften von <Targetname>) wird angezeigt. *Targetname* ist der Name des iSCSI-Targets, für das Sie die iSCSI-Einstellungen konfigurieren.

2. Markieren Sie in der Registerkarte **Authentication** (Authentifizierung) das Kontrollkästchen **Enable CHAP** (CHAP aktivieren) und tippen Sie den Benutzernamen (den IQN-Namen des Initiators) ein. Sie können den IQN entweder manuell eingeben oder ihn über die Option **Browse** (Durchsuchen) aus einer Liste auswählen.

3. Geben Sie das **Secret** ein, geben Sie denselben Wert noch einmal in **Confirm Secret** (Secret bestätigen) ein und klicken Sie auf **OK**. Das Secret muss aus 12 bis 16 Zeichen bestehen.

   ANMERKUNG: Wenn IPSec nicht verwendet wird, sollten die CHAP-Secrets von sowohl Initiator als auch Target größer oder gleich 12 Bytes und kleiner oder gleich 16 Bytes sein. Wird IPsec verwendet, müssen die Secrets für Initiator und Target größer als 1 Byte und kleiner oder gleich 16 Bytes sein.

Einstellungen für den iSCSI-Initiator

1. Öffnen Sie die Registerkarte **Discovery** (Erkennung).
2. Melden Sie sich bei dem Target an, für dass Sie CHAP aktiviert haben. Klicken Sie dazu auf **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators)→ Registerkarte **Targets**→ **Log On...** (Anmeldung...). (Siehe auch „Einstellungen für das iSCSI-Target“ auf Seite 40).
3. Klicken Sie im Fenster **Log On to Target** (Anmeldung beim Target) auf **Advanced** (Erweitert).
4. Markieren Sie im Fenster **Advanced Settings** (Erweiterte Einstellungen) das Kontrollkästchen **CHAP logon information** (CHAP-Anmeldeinformationen).

   Im Feld **User name** (Benutzername) wird automatisch der IQN des Initiators angezeigt.
5. Geben Sie im Feld **Target secret** (Target-Secret) das Target-Secret ein, das Sie für das iSCSI-Target festgelegt haben, und klicken Sie auf OK.

   Wenn das Target-Secret korrekt eingegeben wurde, sind Sie nun beim Target angemeldet. Andernfalls schlägt die Anmeldung fehl und es wird ein Authentifizierungsfehler gemeldet.

Gegenseitige CHAP-Authentifizierung

Bei der gegenseitigen CHAP-Authentifizierung authentifizieren sich Target und Initiator wechselseitig. Für jedes Target und jeden Initiator im Speichernetzwerk (SAN = Storage Area Network) wird ein eigenes Secret definiert.

Einstellungen für den Initiator

1. Gehen Sie im iSCSI-Initiator auf **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators)→ Registerkarte **General** (Allgemein)→ Schaltfläche **Secret**.
2. Das Fenster **CHAP Secret Setup** (Einrichtung des CHAP-Secrets) wird angezeigt. Geben Sie im Feld **Enter a secure secret** (Geben Sie ein sicheres Secret ein) einen 12 bis 16 Zeichen langen geheimen Code ein und klicken Sie auf **OK**.

   ANMERKUNG: Das CHAP-Secret des Initiators darf nicht identisch mit dem CHAP-Secret des Targets sein.

3 Die Anmeldung am Target ist erst möglich, nachdem das CHAP-Secret des Initiators am Target definiert wurde. Deshalb müssen Sie die Target-Einstellungen abschließen und anschließend die Anmeldung am iSCSI-Initiator durchführen.

Einstellungen für das Target

Konfigurieren Sie die Target-Einstellungen für die CHAP-Authentifizierung entsprechend der Anleitung in „Einstellungen für das iSCSI-Target“ auf Seite 40 und führen Sie folgende Schritte durch:

1 Öffnen Sie im Fenster **<Target Name> Properties** (Eigenschaften von <Targetname>) die Registerkarte **Authentication** (Authentifizierung).

2 Markieren Sie das Kontrollkästchen **Enable reverse CHAP authentication** (Gegenseitige CHAP-Authentifizierung aktivieren). Geben Sie im Feld **User name** (Benutzername) den IQN des Initiators ein.

3 Geben Sie im Fenster **Reverse Secret** (Komplementäres Secret) den Wert ein, den Sie im Initiator unter **Secret** festgelegt haben.

ANMERKUNG: Achten Sie darauf, dass das komplementäre Secret nicht mit dem CHAP-Secret identisch ist. Das komplementäre Secret muss 12 bis 16 Zeichen lang sein.

Einstellungen für den Initiator – Fortsetzung

1 Konfigurieren Sie die CHAP-Einstellungen für den Initiator entsprechend der Anleitung in „Einstellungen für den iSCSI-Initiator“ auf Seite 41.

2 Wählen Sie im Fenster **Advanced Settings** (Erweiterte Einstellungen)→ die Option **CHAP logon information** (CHAP-Anmeldeinformationen)→ und geben Sie unter **User name** den Benutzernamen und unter **Target secret** das Target-Secret ein. Markieren Sie das Kontrollkästchen **Perform mutual authentication** (Gegenseitige Authentifizierung durchführen) und klicken Sie auf **OK**.

Für die Anmeldung werden alle Anmeldeinformationen benötigt, die am Target und am Initiator definiert wurden.

A

Anhang

Die vorangehenden Kapitel dieser Dokumentation beschreiben grundlegende Vorgehensweisen für iSCSI-Sitzungen/Verbindungsinformationen. Dieses Kapitel beschreibt kurz die Vorgehensweisen für einige erweiterte Konfigurationseinstellungen.

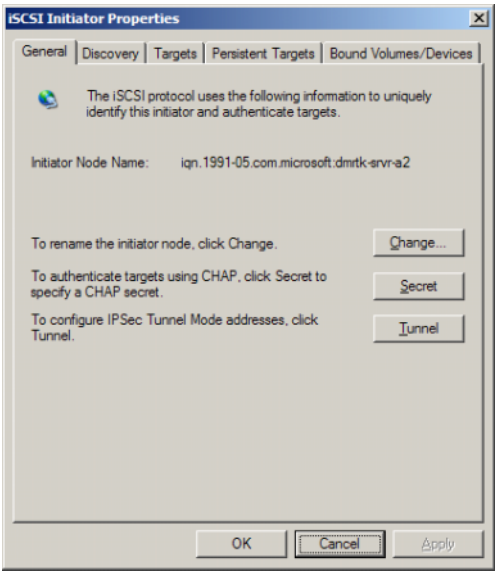
Einzelheiten zum Initiator

Dieser Abschnitt beschreibt die verschiedenen Möglichkeiten des Fensters **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators).

Registerkarte General (Allgemein)

Auf der Registerkarte **General** (Allgemein) wird der Initiator-Knotenname angezeigt. Dabei handelt es sich um den IQN (iSCSI Qualified Name) des Initiators.

Abbildung A-1. Registerkarte General (Allgemein) im Fenster iSCSI Initiator Properties (Eigenschaften des iSCSI-Initiators)



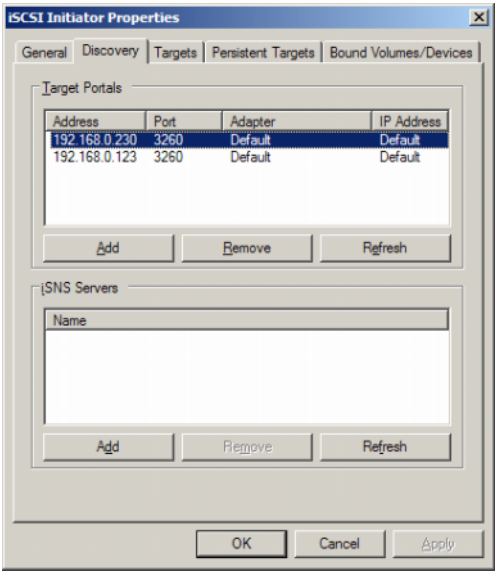
Die Registerkarte **General** (Allgemein) enthält drei Optionen–**Change** (Ändern), **Secret** und **Tunnel**.

- Change (Ändern)–Ermöglicht das Ändern des angezeigten Initiator-Knotennamens.
- Secret–das zur iSCSI-Sicherheit bereitgestellte CHAP-Secret. Weitere Informationen finden Sie unter „Konfigurieren gesicherter iSCSI-Verbindungen über das CHAP (Challenge-Handshake Authentication Protocol)“ auf Seite 39.
- Tunnel–Sie können diese Option für erweiterte Konfigurationen unter IPSec verwenden.

Registerkarte Discovery (Erkennung)

Target Portals (Targetportale)–Die Registerkarte **Discovery** (Erkennung) enthält die Liste der erkannten und für den Initiator verfügbaren iSCSI-Targetportale. Das Targetportal ist die primäre IP-Adresse der iSCSI Target Solution und liefert eine IP-Adresse einer dedizierten iSCSI-Netzwerkkarte für die PowerVault NAS Storage Solution. Wenn keine Targetportale aufgeführt sind, können Sie sie hinzufügen, indem Sie die IP-Adresse oder den DNS-Namen des Targetservers angeben. Im folgenden Beispiel wurden bereits zwei iSCSI-Targetportale hinzugefügt.

Abbildung A-2. Registerkarte Discovery (Erkennung) im Fenster iSCSI Initiator Properties (Eigenschaften des iSCSI-Initiators).



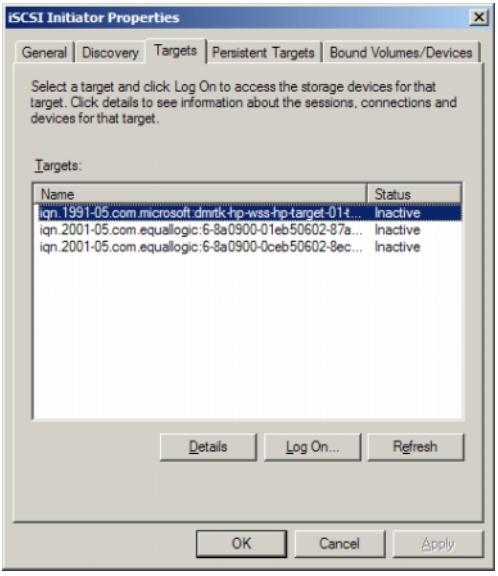
iSNS-Server–Die Targeterkennung kann auch mithilfe von iSNS-Servern durchgeführt werden.

Geben Sie die IP-Adresse oder den DNS-Namen des iSNS-Servers an. Wenn der iSNS-Dienst auf einem Server aktiv ist, werden alle an diesem Server registrierten Clients (Initiatoren und Targets) im Fenster **Registered Clients** (Registrierte Clients) aufgeführt. Im Fenster **Microsoft iSNS Properties** (Eigenschaften von Microsoft iSNS)→ **Registered Clients** (Registrierte Clients) können Sie diese Information auf dem iSNS-Server abrufen.

Registerkarte Targets

Auf der Registerkarte **Targets** sind die einzelnen Targets aufgeführt, die für den iSCSI-Initiator verfügbar sind. Im nachstehenden Beispiel kann der iSCSI-Initiator auf drei Targets zugreifen.

Abbildung A-3. Registerkarte Targets im Fenster iSCSI Initiator Properties (Eigenschaften des iSCSI-Initiators)



ANMERKUNG: Die Abbildung oben zeigt ein Beispiel für die Erkennung in der Registerkarte **Targets**. In der Praxis werden die Targets erst erkannt, nachdem Sie das PowerVault NAS Speichersystem als Target konfiguriert haben.

Log On (Anmeldung)–Um auf das Target zugreifen zu können, muss sich der Initiator beim Target anmelden. Wenn nur ein Pfad zum Target vorhanden ist, genügt ein Schritt für die Anmeldung. Klicken Sie auf **Log On...** (Anmeldung...), legen Sie den **Target name** (Targetnamen) fest und klicken Sie dann auf **OK**.

Sind mehrere Pfade zum Target vorhanden, so benötigt der iSCSI?Initiator für jeden der Pfade eine eigene Beschreibung. So übermitteln Sie mehrere Pfadbeschreibungen an den Initiator:

1. Wählen Sie im Fenster **Log On to Target** (Anmeldung beim Target) die Option **Enable multi-path** (Multi-Path Aktivieren) und klicken Sie auf) **Advanced** (Erweitert).

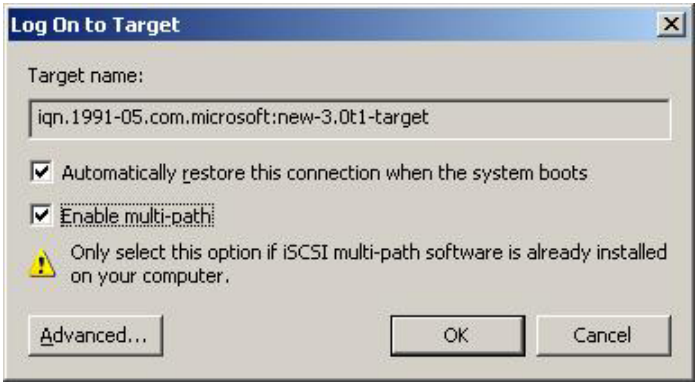
   Die Option **Advanced** (Erweitert) liefert ein Drop-Down-Menü mit allen möglichen Quell (Initiator)-IP-Adressen und ein weiteres Drop-Down-Menü mit allen möglichen Targetportaladressen. In diesem Szenario werden die tatsächlichen Pfade und IP-Adressen intern von der Target Solution verwaltet. Andere Target Solutions zeigen alle verfügbaren IP-Adressen an, die für Multi-Path-Operationen verwendet werden können.

2. Um mehrere Sitzungen für dasselbe Targetgerät auszuführen, wählen Sie alle gewünschten Kombinationen von Quellen-IP-Adresse und Target-IP-Adresse und melden Sie sie separat an.

3. Um eine kontinuierliche Verbindung zu gewährleisten und zu verhindern, dass während eines Spannungsanstiegs oder eines Systemneustarts eine Target-/Initiator-Zuordnung erfolgt, wählen Sie **Automatically restore this connection when the system boots** (Verbindung bei Systemneustart automatisch wiederherstellen).

4. Wiederholen Sie unter **Log on** die Anmeldung für jede iSCSI-Netzwerkkarte.

Abbildung A-4. Fenster Log On to Target (Anmeldung beim Target)

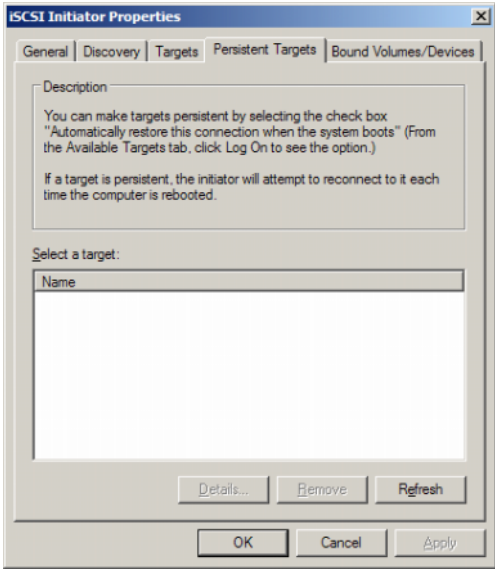


Bei einer MPIO-Verbindung müssen Sie das Target auswählen, für das der Status **Connected** (Verbunden) angezeigt wird und dort **Log On** (Anmeldung) auswählen. Wählen Sie im Fenster **Log On to Target** (Anmeldung beim Target) **Advanced** (Erweitert) aus und konfigurieren Sie redundante IP-Adressen für das iSCSI-Target.

Registerkarte Persistent Targets (Dauerhafte Targets)

Sie können die Option Persistent Targets (Dauerhafte Targets) so konfigurieren, dass die Verbindung zum Target automatisch wiederhergestellt wird, wenn das System neu gestartet wird. Targets, die als dauerhaft konfiguriert wurden, werden auf der Registerkarte **Persistent Targets** (Dauerhafte Targets) angezeigt.

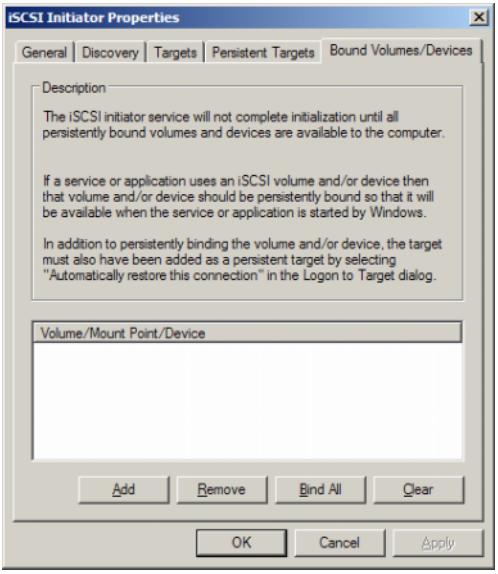
Abbildung A-5. Registerkarte Persistent Targets (Dauerhafte Targets) im Fenster iSCSI Initiator Properties (Eigenschaften des iSCSI-Initiators)



Registerkarte Bound Volumes/Devices (Gebundene Datenträger/Geräte)

Wenn ein Dienst oder eine Anwendung auf dem Host von der Verfügbarkeit eines iSCSI-Datenträgers abhängt, müssen Sie diesen als **bound** (gebunden) konfigurieren. Der iSCSI-Dienst bezieht alle **gebundenen** Datenträger in die Initialisierung ein.

Abbildung A-6. Registerkarte Bound Volumes/Devices (Gebundene Datenträger/Geräte) im Fenster iSCSI Initiator Properties (Eigenschaften des iSCSI-Initiators)



Einzelheiten der erweiterten Konfiguration

Aktivieren von Multi-Path beim Initiator

Nachdem Sie die iSCSI Initiator-Target-Verbindung hergestellt haben, führen Sie zur Aktivierung von Multi-Path folgende Schritte durch:

1. Gehen Sie beim Initiator auf **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators)→ Registerkarte **Targets**→ **Log On...** (Anmeldung...)→ Fenster **Log On to Target** (Anmeldung beim Target) und wählen Sie das Kontrollkästchen der Option **Enable multi-path** (Multi-Path Aktivieren).
2. Sie müssen für einen effizienten Block (iSCSI)-E/A-Betrieb und zur Ausfallsicherung mehrere Netzwerkkarten-Ports für den iSCSI-Betrieb konfigurieren. Die Option Multi-Path ermöglicht zudem mehrere Verbindungen derselben iSCSI-Targets mit verschiedenen IP-Adressen.

Die Option Advanced (Erweitert)

Sie können die Option Advanced (Erweitert) zur Durchführung folgender Funktionen verwenden:

- Öffnen Sie **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators)→ Registerkarte **Targets**→ **LogOn...** (Anmeldung...)→ und wählen Sie im Fenster **Log On to Target** (Anmeldung beim Target) die Option→ **Advanced** (Erweitert). Das Fenster **Advanced Settings** (Erweiterte Einstellungen) öffnet sich und enthält zwei Registerkarten–**Advanced** (Erweitert) und **IPSec**. In der Registerkarte **General** (Allgemein) können Sie die CRC/Prüfsumme, CHAP und die Quell-IP-Adresse einstellen und das Targetportal wählen–IP-Adresse des iSCSI-Target. Sie können die Option Multi-Path verwenden, um die Lastverteilung und Ausfallsicherheitseinstellungen zu konfigurieren.
- Die Registerkarte **Advanced** (Erweitert) Im Fenster **Advanced Settings** (Erweiterte Einstellungen) enthält ein Drop-Down-Menü für alle Quell (Initiator)-IP-Adressen und ein Drop-Down-Menü für alle Targetportaladressen. Bei einer iSCSI Initiator-Target-Verbindung werden die aktellen Pfade und IP-Adressen von der Target Solution intern verwaltet. Wenn Sie verschiedene Target Solutions verwenden, können Sie die IP-Adresse für Multi-Path-Betrieb aus der Liste auswählen.

a Melden Sie sich an und wählen Sie die Kombination aus Quell-IP-Adresse und Target-IP-Adresse.

b Melden Sie sich jeweils separat an, um mehrere Verbindungen für dasselbe Targetgerät zu konfigurieren.

- Im Fenster **Advanced Settings** (Erweiterte Einstellungen) können Sie in der Registerkarte **IPSec** die IPSec -Einstellungen konfigurieren. Wenn Sie IPSec aktivieren, werden alle während der Datenübertragung gesendeten IP-Pakete verschlüsselt und authentifiziert. Bei allen IP-Portalen wird ein gemeinsamer Schlüssel eingerichtet, mit dem sich alle Verbindungspartner authentifizieren und die Paketverschlüsselung vereinbaren können.

Überprüfen der Eigenschaften der verbundenen Targets

Öffnen Sie **iSCSI Initiator Properties** (Eigenschaften des iSCSI-Initiators)→ **Targets**→ , markieren Sie das als **Connected** (Verbunden) angegebene Target und klicken Sie auf **Details**. Das Fenster **Target properties** (Targeteigenschaften) wird angezeigt und enthält drei Registerkarten–**Sessions** (Sitzungen), **Devices** (Geräte) und **Properties** (Eigenschaften). In den folgenden Abschnitten finden Sie weitere Einzelheiten zu diesen Registerkarten.

Registerkarte Sessions (Sitzungen)

Die Registerkarte **Sessions** (Sitzungen) liefert Informationen über **Session Identifier** (Kennung der Sitzung), **Session properties** (Eigenschaften der Sitzung) und **Sessions Connections** (Verbindungen der Sitzung). Mit dieser Registerkarte können Sie Sitzungen abmelden.

Registerkarte Devices (Geräte)

Die Registerkarte **Devices** (Geräte) des Fensters **Target Properties** (Targeteigenschaften) liefert weitere generische Geräteinformationen wie beispielsweise die virtuellen Laufwerke, die dem Target zugeordnet sind.

Klicken Sie auf **Advanced** (Erweitert), um Informationen über MPIO zu erhalten und das Fenster **Device Details** (Einzelheiten zu Geräten) zu starten.

Mit der Registerkarte **MPIO** können Sie die MPIO-Einstellungen ändern. In dieser Registerkarte können Sie Einstellungen der Strategie zur Lastverteilung festlegen. Sie können die Lastverteilung für jede einzelne Verbindung aus den verschiedenen verfügbaren Optionen zur Lastverteilungsstrategie wählen. Wenn Sie die einzelnen Strategien im Feld **Load Balance Policy** (Lastverteilungsstrategie) der Registerkarte **MPIO** anwählen, werden die folgenden Beschreibungen auf dem Bildschirm angezeigt:

- **Fail Over Policy (Strategie "Ausfall")**– The fail over policy employs one active path and designates all other paths as standby. The standby paths will be tried on a round-robin approach upon failure of the active path until an available path is found (Die Strategie "Ausfall" verwendet einen einzigen aktiven Pfad und kenn- zeichnet alle anderen als Stand-by-Pfade. Die Stand-by-Pfade werden bei einem Ausfall des akti- ven Pfads reihum ausprobiert bis ein verfügbarer Pfad gefunden ist).
- **Round Robin (Reihum)**– The round robin policy attempts to evenly distribute incoming requests to all possible paths (The Strategie "Reihum" versucht eingehende Anfragen gleichmäßig auf alle möglichen Pfade zu verteilen).
- **Round Robin With Subset (Reihum mit Auswahl)**– The round robin subset policy executes the round robin policy only on paths designated as active. The stand-by paths will be tried on a round-robin approach upon failure of all active paths (Die Strategie "Reihum mit Auswahl" führt die Strategie "Reihum" nur bei als aktiv gekennzeichneten Pfaden durch. Die Stand-by-Pfade werden bei Ausfall aller akti- ven Pfade reihum ausprobiert).
- **Least Queue Depth (Kleinste Warteschlange)**– The least queue depth policy compensates for uneven loads by distributing propeortiaonately more I/O requests to lightly loaded processing paths (Die Strategie der kleinsten Warteschlange kompensiert

ungleichmäßige Belastung dadurch, dass proportional mehr E/A-An- fragen auf gering belastete Prozesspfade verteilt werden).

- **Weighted Paths (Gewichtete Pfade)**–The weighted paths policy allows the user to specify the relative processing load of each path. A large number means that the path priority is low (Die Strategie der ge- wichteten Pfade ermöglicht es dem Benutzer, die relative Prozessbelastung jedes Pfades festzulegen. Ein hoher Wert bedeutet eine geringe Priorität des Pfades).

Die Standardeinstellung ist **Round Robin** (Reihum). Wählen Sie zur Konfiguration der Lastverteilungsstrategie die benötigte Option aus dem Drop-Down-Menü **Load Balance Policy** (Lastverteilungsstrategie) und klicken Sie auf **Apply** (Anwenden), um Ihre Einstellung zu bestätigen.

Registerkarte Properties (Eigenschaften)

Die Registerkarte **Properties** (Eigenschaften) des Fensters **Target Properties** (Targeteigenschaften) liefert Informationen über Target-Alias, Authentifikation, zugeordnete Netzwerkportale und andere Einzelheiten des Targets.

Installieren und Konfigurieren von iSNS Server

Microsoft iSNS Server kann von der Microsoft-Webseite **www.microsoft.com** gratis heruntergeladen werden und ist in zwei Versionen verfügbar–x86 und IA64. Sie können den iSNS-Server zur Targeterkennung in einem iSCSI-Netzwerk verwenden.

iSNS Server wird von den Betriebssystemen Microsoft Windows 2000 Server Service Pack 4 und Microsoft Windows Server 2003 unterstützt. Führen Sie die folgenden Schritte durch, um iSNS Server zu installieren:

ANMERKUNG: Installieren Sie iSNS Server nicht auf demselben Server, auf dem Microsoft iSCSI Initiator läuft.

1. Installieren Sie iSNS Server Version 3.0 oder höher. Der Installationsprozess ist einfach und wird von einem Assistenten geführt. Klicken Sie im Fenster **Welcome to the Microsoft iSNS Server Setup Wizard** (Willkommen beim Microsoft iSNS Server Setup-Assistenten)auf **Next** (Weiter).

2 Das Fenster **License Agreement** (Lizenzvereinbarung) wird angezeigt. Lesen Sie die Informationen und klicken Sie auf **Next** (Weiter).

3 Der Ordner **Select Installation** (Installation Auswählen) öffnet sich. Geben Sie den Ordnerpfad ein oder wählen Sie einen Ort auf Ihrem lokalen Laufwerk, indem Sie die Option **Browse** (Durchsuchen) verwenden, und klicken Sie auf **Next** (Weiter).

4 Klicken Sie im Fenster **Confirm Installation** (Installation bestätigen) auf **Next** (Weiter).

5 Das Fenster **Installing Microsoft iSNS Server** (Microsoft iSNS Server Installieren) zeigt den Installationsfortgang an. Das **Microsoft iSNS Installation Program** (Microsoft iSNS-Installationsprogramm) fordert Sie auf, unter den **iSNS Installation Options** (iSNS-Installationsoptionen) auszuwählen. Wählen Sie **Install iSNS Service** (iSNS Service installieren) und klicken Sie auf **OK**.

6 Das Fenster **End User License Agreement** (Endbenutzer-Lizenzvereinbarung) öffnet sich. Lesen Sie die Vereinbarung und klicken Sie auf **Agree** (Zustimmen), um das Programm zu installieren.

7 Das Fenster **Microsoft iSNS Service Setup Program** zeigt an, dass das Programm erfolgreich installiert wurde.

8 Das Fenster **Microsoft iSNS Server Information** öffnet sich. Lesen Sie die Informationen und klicken Sie auf **Next** (Weiter).

9 Das Fenster **Installation Complete** (Installation abgeschlossen) öffnet sich und zeigt an, dass die Programminstallation beendet ist. Klicken Sie auf **Close** (Schließen).

iSNS Server konfigurieren

iSNS Server erkennt iSCSI-Initiatoren und -Targets automatisch, nachdem Sie sie beim iSNS-Server registriert haben.

- Die bei iSNS-Servern registrierten Initiatoren erkennen alle Targetgeräte, die unter iSNS in der Registerkarte **Targets** registriert sind und sich bei den Targets anmelden. Sie müssen Initiatoren nicht mit der IP-Adresse oder dem DNS-Namen einzelner Targetserver in **Target Portals** (Targetportale) konfigurieren. iSNS Server führt die Targeterkennung durch.
- Auf gleiche Weise kann das PowerVault NAS Speichersystem (Target) die verfügbaren Server beim iSNS-Server zwecks Zuordnung abfragen.

Um den iSNS-Server zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Melden Sie sich beim Server an, auf dem Sie iSNS Server 3.0 oder höher installiert haben, und öffnen Sie **Start**→ **Programs** (Programme)→ **Microsoft iSNS Server**→ **Configure iSNS** Server (iSNS Server konfigurieren).

   Der Bildschirm von iSNS Server besteht aus drei Registerkarten–**General** (Allgemein), **Discovery Domains** (Erkennungsdomains) und **Discovery Domain Sets** (Erkennungsdomainsets). Die Registerkarte **General** (Allgemein) listet alle Geräte (iSCSI-Initiatoren und -Targets) auf, die beim iSNS-Server registriert sind. Gehen Sie folgendermaßen vor, um Targets und Initiatoren zum iSNS -Server hinzuzufügen:

   a. Öffnen Sie **iSCSI Initiator properties** (Eigenschaften des ISCSI-Initiators)→ **Discovery** (Erkennung)→ **iSNS Servers**→ **Add** (Hinzufügen) und fügen Sie die IP-Adresse oder den DNS-Namen des Initiators hinzu und registrieren Sie diesen Initiator am iSNS-Server.

   b. Melden Sie sich beim iSNS-Server an und öffnen Sie **Start**→ **Programs** (Programme)→ **Microsoft iSNS Server**→ **Configure iSNS Server** (iSNS-Server konfigurieren)→ Registerkarte **General** (Allgemein). Der Initiator, den Sie unterSchritt a in iSNS Server registriert haben, wird aufgelistet. In gleicher Weise werden alle iSCSI-Initiatoren, die Sie in iSNS Server registrieren, in der Registerkarte **General** (Allgemein) aufgelistet.

   c. Melden Sie sich bei der PowerVault NAS Storage Solution an, die Sie als Target konfiguriert haben und öffnen Sie **PowerVault NAS Management Console**→ **Microsoft iSCSI Software Target**→ klicken Sie es mit der rechten Maustaste an und wählen Sie **Properties** (Eigenschaften)→ Registerkarte **iSNS** und fügen Sie die IP-Adresse oder den DNS-Namen des iSNS-Servers hinzu.

   d. Um den Erfolg zu überprüfen, melden Sie sich beim iSNS-Server an und sehen Sie in der Registerkarte **General** (Allgemein) nach, ob alle Targets der PowerVault Storage Solution aufgelistet sind.

   Sind mehrere PowerVault NAS Storagesysteme in iSNS Server registriert, werden alle in den PowerVault Speichersystemen erstellten Targetgeräte in iSNS Server aufgelistet.

2. Sie können die Option **Discovery Domains** (Erkennungsdomains) dazu verwenden, um bestimmte Initiatoren und Targets mit besonderem Zugriff zu gruppieren:

a Öffnen Sie **iSNS Server Properties** (Eigenschaften von iSNS Server)→ Registerkarte **Discovery Domains** (Erkennungsdomains)→ klicken Sie auf **Create** (Erzeugen)→ geben Sie einen Namen für die Erkennungsdomain ein→ wählen Sie **Add** (Hinzufügen).

b Das Fenster **Add registered Initiator or Target to Discovery Domain** (Registrierten Initiator oder Target zur Erkennungsdomain hinzufügen) öffnet sich. Wählen Sie die Initiatoren und Targets, die Sie konfigurieren möchten, und klicken Sie auf **OK**.

3 Sie können im iSCSI-Netzwerk mehrere Erkennungsdomains konfigurieren. Die Domains werden in der Registerkarte **Discovery Domain Sets** (Erkennungsdomainsets) aufgelistet. Die Registerkarte **Discovery Domain Sets** (Erkennungsdomainsets) zeigt Standardoptionen für Erkennungsdomains (DD) und Erkennungsdomainsets (DDS) an. Sie können so viele Gruppen erstellen wie nötig.

Bewährte Vorgehensweisen zum effektiven Speichermanagement

Storage Manager for SANs

Storage Manager for SANs ist ein Snap-in der Microsoft Management Console, mit dem Systemadministratoren die Logical Unit Numbers (LUNs) zum Zuordnen von Speicher in Speicherarrays sowohl in Fibre Channel- als auch iSCSI-Umgebungen erzeugen können. Storage Manager for SANs wird mittels eines herkömmlichen Snap-in eingerichtet und kann in Speicherarrays verwendet werden, die auf einem Storage Area Network (SAN) basieren und den Virtual Disk Server (VDS) unterstützen, der einen VDS-Hardwareprovider verwendet. Die beiden Arten unterstützter Umgebungen (iSCSI und Fibre Channel) unterscheiden sich aufgrund von Hardware, Protokoll, Transportschicht und Sicherheitsunterschieden hinsichtlich Konfiguration und LUN-Management. Diese Einrichtung funktioniert mit jeder Art von Host Bus Adapter (HBA) oder Switches im SAN. Eine Liste von VDS-Providern, die den Hardwarekompatibilitätstest (Hardware Compatibility Tests (HCT)) bestanden haben, finden Sie auf der Microsoft-Storage-Webseite unter **www.microsoft.com/storage**.

LUN-Management für iSCSI-Untersysteme

Für iSCSI ist eine LUN einem Target zugewiesen–einer logischen Einheit, die eine oder mehrere LUNs enthält. Ein Server greift auf die LUN zu, indem er sich mithilfe des iSCSI-Initiators des Servers am Target anmeldet. Um sich an einem Target anzumelden, stellt der Initiator eine Verbindung mit Portalen am Target her; ein Untersystem besitzt ein oder mehrere Portale, die dem Target zugeordnet sind. Wenn der Initiator eines Servers am Target angemeldet ist und dem Target eine neue LUN zugewiesen wurde, hat der Server sofort Zugriff auf die LUN.

Sicherung von Daten bei einem iSCSI-SAN–Um eine sichere Datenübertragung zwischen Server und Untersystem zu ermöglichen, konfigurieren Sie die Sicherheit für Anmeldungssitzungen zwischen Initiatoren und Targets. Mit dem Storage Manager for SANs können Sie eindirektionale oder gegenseitige Authentifizierung zwischen Initiatoren und Targets unter dem Challenge Handshake Authentication Protocol (CHAP) sowie die Datenverschlüsselung unter Internet Protocol Security (IPsec) konfigurieren.

ANMERKUNG: Es wird empfohlen, CHAP zu verwenden, wenn der iSCSI-Datenverkehr über das öffentliche Netzwerk erfolgt.

Bekannte Probleme

- Ereignis während der Freigabe eines virtuellen Laufwerks– Wenn Sie eine lokal eingebundene virtuelle Festplatte freigeben, kann das folgende Ereignis im Systemprotokoll auftauchen:

  ```
  Plugplaymanager 12 event:
  The device 'MSFT 00000000F852A09D SCSI Disk
  Device'
  (SCSI\Disk&Ven_MSFT&Prod_00000000F852A09D\1&2afd7
  d61&3&000003) disappeared from the system without
  first being prepared for removal. (Das Gerät 'MSFT
  00000000F852A09D SCSI Disk Device'
  (SCSI\Disk&Ven_MSFT&Prod_00000000F852A09D\1&2afd7
  d61&3&000003) ist vom System verschwunden, ohne
  für die Entfernung freigegeben zu sein.)
  It is safe to ignore these events for normal
  Microsoft iSCSI Software Target dismount
  operations (Es beeinträchtigt die Sicherheit
  nicht, dieses Ereignis bei normalen Freigaben
  ```

unter Microsoft iSCSI Software Target zu ignorieren).

- Zurücksetzen auf eine lokal eingebundene virtuelle Festplatte–Wenn Sie eine virtuelle Festplatte lokal im Lese-/Schreibmodus einbinden, dauert ein Zurücksetzen auf dieser virtuellen Festplatte sehr lange.
- Beendigung der Zurücksetzung–Deaktivieren einer virtuellen Festplatte während einer Zurücksetzung beendet die Zurücksetzung ohne Fehlermeldung. Es wird ein Ereignis eingetragen, das festhält, dass die Zurücksetzung beendet wurde.
- Lokal eingebundene virtuelle Festplatten werden unter den verfügbaren Laufwerken aufgelistet–Wenn Sie eine neue virtuelle Festplatte erzeugen, werden die lokal eingebundenen Festplatten in der Liste verfügbarer Datenträger aufgelistet, die die neue virtuelle Festplatte aufnehmen können. Eine lokal eingebundene virtuelle Festplatte unterstützt die Speicherung einer virtuellen Festplatte nicht. Versuchen Sie dennoch, die lokal eingebundene virtuelle Festplatte als Speicherort für die neue virtuelle Festplatte auszuwählen, so wird die folgende Fehlermeldung angezeigt: `The wizard was unable to import one or more virtual disks. (Der Assistent konnte eine oder mehrere virtuelle Festplatten nicht importieren). Make sure that the files are not in use, and then run the wizard again (Stellen Sie sicher, dass die Dateien nicht verwendet werden und starten Sie den Assistenten nochmals).`
- Ein Initiator kann ein Target nicht anhand des DNS-Namens erkennen–Wenn Sie den Zugriff eines Initiators auf ein iSCSI-Target konfigurieren, sind IQNs vorzuziehen, da sie ungeachtet der DNS-Konfiguration funktionieren. Die Option, einen DNS-Domainnamen anzugeben, ist Bestandteil des Microsoft iSCSI Software Target Snap-in. Wenn Sie die Verwendung von DNS-Namen vorziehen, stellen Sie sicher, dass DNS korrekt konfiguriert ist (einschließlich Forward und Reverse Lookup-Zonen) und legen Sie den vollen qualifizierten Domainnamen (fully qualified domain name (FQDN)) des Initiators fest. Wenn Sie nach der Festlegung eines FQDN Schwierigkeiten haben, das Target mit dem Initiator zu verbinden, geben Sie folgenden Befehl am Targetserver ein, um zu überprüfen, ob DNS Reverse Lookup korrekt aktiviert ist:
  nslookup <InitiatorIP> wobei **<InitiatorIP>** die IP-Adresse des iSCSI-Initiators ist.
  Funktioniert der Befehl *nslookup* nicht, ist Reverse Lookup nicht konfigu-

riert. Konfigurieren Sie das Target neu, damit es den Initiator-IQN, die IP-Adresse oder die MAC-Adresse verwendet. Alternativ können Sie zum Verbinden des Initiators einen NetBIOS-Namen verwenden, der folgende Bedingungen erfüllt:

  – Es sind keine DNS Reverse Lookup-Zonen für das vom Target verwendete Subnetz konfiguriert.

  – Netzwerkerkennung und File Sharing sind auf den Initiator- und Target-Servern aktiviert.

- Schattenkopien lokal eingebundener Datenträger–Es wird empfohlen, keine Schattenkopien lokal eingebundener Datenträger zu erstellen. Wenn Sie eine virtuelle Festplatte lokal einbinden und dann versuchen, mit dem Windows Explorer eine Schattenkopie dieses Datenträgers zu erstellen, scheint die Speicheranwendung hängenzubleiben. Die Ursache hierfür ist die Art und Weise wie Schattenkopien erstellt werden. Wenn Sie eine Schattenkopie einer lokal eingebundenen virtuellen Festplatte erstellen, schreibt die lokal eingebundene Festplatte auf den zugrunde liegenden Datenträger, der die virtuelle Festplatte beherbergt. Dadurch wird erneut auf den Bereich des Datenträgers geschrieben. Das Ergebnis ist dann eine sich wiederholende Reihe von Schreibversuchen, so dass die Speicheranwendung nicht mehr antwortet. Sollte dieses Szenario eintreten, starten Sie die Speicheranwendung erneut.

- Der Initiator kann eine abgebrochene Verbindung nicht wieder herstellen–Der Initiator kann eventuell aufgrund schlechter IP-Adressen eine abgebrochene Verbindung nicht mehr wiederherstellen. In einigen Fällen, in denen die Kommunikation zwischen dem iSCSI-Initiator und Microsoft iSCSI Software Target unterbrochen ist, scheint der Initiator hängenzubleiben, während er die Verbindung wieder aufzunehmen versucht. Dies tritt ein, wenn der Server, auf dem Microsoft iSCSI Software Target läuft, IP-Adressen besitzt, die nicht zur Kommunikation mit dem Initiator verwendet werden. Der Initiator versucht dann, mit jeder der IP-Adressen Verbindung aufzunehmen und wartet bis zu 100 Sekunden auf Antwort. Dies kann ebenso aufgrund einer automatischen Zuweisung interner IP-Adressen auftreten (169.x.x.x). Um einen solchen Vorfall zu verhindern, verwenden Sie statische IP-Adressen, bei denen DHCP nicht verfügbar ist.

  Durch folgende Maßnahmen lässt sich der Fehler umgehen:

  – Geben Sie Quell- und Targetportal anhand ihrer IP-Adressen an.

- Verwenden Sie nur IPv4-Adressen oder nur IPv6-Adressen: vermischen Sie beide Adresstypen nicht.
- Deaktivieren Sie Netzwerkkarten, die nicht mit einem Netzwerk verbunden sind.

- Fehler im Event Viewer (Ereignisbetrachter)–Fehler im Event Viewer können auftreten, wenn Sie versuchen, Microsoft iSCSI Software Target 3.2 zu deinstallieren und erneut zu installieren. Um dies zu umgehen, beenden Sie Microsoft iSCSI Software Target, bevor Sie die Software deinstallieren. Wurde die Software bereits deinstalliert, starten Sie den Computer vor der Neuinstallation von Microsoft iSCSI Software Target neu.
- Zusätzliche Firewallregeln für iSCSI-Initiatoren–Es kann vorkommen, dass Sie zusätzliche Regeln aktivieren müssen, um einen iSCSI-Initiator mit Microsoft iSCSI Software Target unter Windows Storage Server 2008 einzubinden. Hierzu benötigen Sie folgende Firewallregeln:
  - Windows Management Instrumentation (WMI-In) [TCP/All ports]
  - Windows Management Instrumentation (DCOM-In) [TCP/Port 135]
  - Windows Management Instrumentation (ASync-In) [TCP/All ports]
  - Windows Management Instrumentation (WMI-Out) [TCP/All ports]
  - Remote Volume Management (RPC-EPMAP) [TCP/RPC Endpoint Mapper]
  - Remote Volume Management - Virtual Disk Service Loader (RPC) [TCP/Dynamic RPC]
  - Remote Volume Management - Virtual Disk Service (RPC) [TCP/Dynamic RPC]

Stichwortverzeichnis