



Allgemeines zur SAN Host-Bereitstellung

ONTAP 9

NetApp
March 21, 2023

Inhaltsverzeichnis

- Allgemeines zur SAN Host-Bereitstellung 1
 - SAN-Bereitstellung mit iSCSI 1
 - iSCSI-Service-Management 2
 - SAN Provisionierung mit FC 8
 - SAN-Provisionierung mit NVMe 9

Allgemeines zur SAN Host-Bereitstellung

SAN-Bereitstellung mit iSCSI

In SAN-Umgebungen sind Storage-Systeme Ziele mit Storage-Zielgeräten. Bei iSCSI und FC werden die Storage-Zielgeräte als LUNs (logische Einheiten) bezeichnet. Bei Non-Volatile Memory Express (NVMe) über Fibre Channel werden die Storage-Zielgeräte als Namespaces bezeichnet.

Sie konfigurieren Storage, indem Sie LUNs für iSCSI und FC erstellen oder Namespaces für NVMe erstellen. Auf die LUNs oder Namespaces wird von Hosts über iSCSI (Internet Small Computer Systems Interface)- oder FC-Protokollnetzwerke (Fibre Channel) zugegriffen.

Zur Verbindung mit iSCSI-Netzwerken können Hosts standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte iSCSI Host Bus Adapter (HBAs) verwenden.

Für die Verbindung mit FC-Netzwerken benötigen Hosts FC-HBAs oder CNAs.

Unterstützte FC-Protokolle:

- FC
- FCoE
- NVMe

Netzwerkverbindungen und Namen der iSCSI-Zielknoten

iSCSI-Zielknoten können sich auf verschiedene Weise mit dem Netzwerk verbinden:

- Über Ethernet-Schnittstellen mit in ONTAP integrierter Software
- Über mehrere Systemschnittstellen hinweg kann eine für iSCSI verwendete Schnittstelle auch den Datenverkehr für andere Protokolle, wie SMB und NFS, übertragen.
- Mit einem Unified Target Adapter (UTA) oder einem konvergierten Netzwerkadapter (CNA).

Jeder iSCSI-Knoten muss einen Knotennamen haben.

Die beiden Formate bzw. Typenbezeichnungen für iSCSI-Knotennamen sind *iqn* und *eui*. Das iSCSI-Ziel der SVM verwendet immer den iqn-Typ-Designator. Der Initiator kann entweder den iqn-Typ oder den eui-Typ-Designator verwenden.

Name des Storage-System-Nodes

Jede SVM, auf der iSCSI ausgeführt wird, verfügt über einen Standard-Node-Namen, der auf einem umgekehrten Domänennamen und einer eindeutigen Kodierungsnummer basiert.

Der Node-Name wird im folgenden Format angezeigt:

```
iqn.1992-08.com.netapp:sn.unique-encoding-number
```

Im folgenden Beispiel wird der Standardknotenname für ein Speichersystem mit einer eindeutigen

Kodierungsnummer angezeigt:

iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6

TCP-Port für iSCSI

Das iSCSI-Protokoll ist in ONTAP für die Verwendung von TCP-Portnummer 3260 konfiguriert.

ONTAP unterstützt nicht das Ändern der Portnummer für iSCSI. Die Portnummer 3260 ist als Teil der iSCSI-Spezifikation registriert und kann von keiner anderen Anwendung oder einem anderen Dienst verwendet werden.

Verwandte Informationen

["NetApp Dokumentation: ONTAP SAN Host-Konfiguration"](#)

ISCSI-Service-Management

ISCSI-Service-Management

Über das können Sie die Verfügbarkeit des iSCSI-Service auf den logischen iSCSI-Schnittstellen der Storage Virtual Machine (SVM) managen `vserver iscsi interface enable` Oder `vserver iscsi interface disable` **Befehle.**

Standardmäßig ist der iSCSI-Service auf allen logischen iSCSI-Schnittstellen aktiviert.

Wie iSCSI auf dem Host implementiert wird

iSCSI kann auf dem Host mithilfe von Hardware oder Software implementiert werden.

Sie können iSCSI auf eine der folgenden Arten implementieren:

- Mit Initiator-Software, die die Standard-Ethernet-Schnittstellen des Hosts verwendet.
- Über einen iSCSI-Host Bus Adapter (HBA): Ein iSCSI-HBA erscheint dem Host-Betriebssystem als SCSI-Festplattenadapter mit lokalen Festplatten.
- Verwendung eines Adapters für die TCP Offload Engine (TOE), der die TCP/IP-Verarbeitung entlastet.

Die iSCSI-Protokollverarbeitung wird weiterhin von der Host-Software durchgeführt.

Funktionsweise der iSCSI-Authentifizierung

Während der ersten Phase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanforderung an das Speichersystem, um eine iSCSI-Sitzung zu starten. Das Storage-System erlaubt dann entweder die Login-Anfrage oder lehnt sie ab oder stellt fest, dass keine Anmeldung erforderlich ist.

iSCSI-Authentifizierungsmethoden:

- Challenge Handshake Authentication Protocol (CHAP): Der Initiator meldet sich mit einem CHAP-Benutzernamen und -Passwort an.

Sie können ein CHAP-Kennwort festlegen oder ein hexadezimaler Geheimkennwort generieren. Es gibt zwei Typen von CHAP-Benutzernamen und -Passwörtern:

- Inbound – das Storage-System authentifiziert den Initiator.

Eingehende Einstellungen sind erforderlich, wenn Sie die CHAP-Authentifizierung verwenden.

- Outbound – Dies ist eine optionale Einstellung, die es dem Initiator ermöglicht, das Speichersystem zu authentifizieren.

Sie können Outbound-Einstellungen nur verwenden, wenn Sie einen eingehenden Benutzernamen und ein Kennwort auf dem Speichersystem definieren.

- Deny- der Initiator wird dem Zugriff auf das Speichersystem verweigert.
- Keine – das Storage-System erfordert keine Authentifizierung für den Initiator.

Sie können die Liste der Initiatoren und deren Authentifizierungsmethoden definieren. Sie können auch eine Standardauthentifizierungsmethode definieren, die für Initiatoren gilt, die nicht in dieser Liste enthalten sind.

Verwandte Informationen

["Multipathing-Optionen für Windows mit Data ONTAP: Fibre Channel und iSCSI"](#)

Verwalten der iSCSI-Initiator-Sicherheit

ONTAP bietet eine Reihe von Funktionen zum Verwalten der Sicherheit für iSCSI-Initiatoren. Sie können eine Liste der iSCSI-Initiatoren und die Authentifizierungsmethode für jeden definieren, die Initiatoren und ihre zugehörigen Authentifizierungsmethoden in der Authentifizierungsliste anzeigen, Initiatoren aus der Authentifizierungsliste hinzufügen oder entfernen sowie die Standard-Authentifizierungsmethode für iSCSI-Initiatoren definieren, die nicht in der Liste enthalten sind.

Isolierung von iSCSI-Endpunkten

Ab ONTAP 9.1 wurden bestehende iSCSI-Sicherheitsbefehle auf den IP-Adressbereich oder mehrere IP-Adressen erweitert.

Alle iSCSI-Initiatoren müssen die Ursprung-IP-Adressen bereitstellen, wenn eine Sitzung oder Verbindung zu einem Ziel eingerichtet wird. Durch diese neue Funktion wird verhindert, dass sich ein Initiator beim Cluster anmelden kann, wenn die Ursprung-IP-Adresse nicht unterstützt oder unbekannt ist und somit ein eindeutiges Identifikationsschema bereitgestellt wird. Jeder Initiator, der von einer nicht unterstützten oder unbekanntem IP-Adresse stammt, wird seine Anmeldung auf der iSCSI-Sitzungsebene abgelehnt. Dies verhindert, dass der Initiator auf beliebige LUNs oder Volumes innerhalb des Clusters zugreift.

Implementieren Sie diese neue Funktion mit zwei neuen Befehlen, um bereits vorhandene Einträge zu verwalten.

Fügen Sie den Adressbereich des Initiators hinzu

Verbessern Sie das Sicherheitsmanagement für iSCSI-Initiatoren, indem Sie dem einen IP-Adressbereich oder mehrere IP-Adressen hinzufügen `vserver iscsi security add-initiator-address-range` Befehl.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

Entfernen Sie den Adressbereich des Initiators

Entfernen Sie einen IP-Adressbereich oder mehrere IP-Adressen mit dem `vserver iscsi security remove-initiator-address-range` Befehl.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

Welche CHAP-Authentifizierung ist

Das Challenge Handshake Authentication Protocol (CHAP) ermöglicht die authentifizierte Kommunikation zwischen iSCSI-Initiatoren und Zielen. Wenn Sie CHAP-Authentifizierung verwenden, definieren Sie sowohl auf dem Initiator als auch auf dem Speichersystem CHAP-Benutzernamen und -Kennwörter.

Während der ersten Phase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanforderung an das Speichersystem, um die Sitzung zu starten. Die Anmeldeanforderung umfasst den CHAP-Benutzernamen und den CHAP-Algorithmus des Initiators. Das Speichersystem reagiert mit einer CHAP-Herausforderung. Der Initiator liefert eine CHAP-Antwort. Das Storage-System überprüft die Antwort und authentifiziert den Initiator. Das CHAP-Passwort wird zur Berechnung der Antwort verwendet.

Richtlinien für die Verwendung der CHAP-Authentifizierung

Bei der Verwendung der CHAP-Authentifizierung sollten Sie bestimmte Richtlinien befolgen.

- Wenn Sie einen eingehenden Benutzernamen und ein Kennwort auf dem Speichersystem definieren, müssen Sie denselben Benutzernamen und dasselbe Kennwort für ausgehende CHAP-Einstellungen auf dem Initiator verwenden. Wenn Sie außerdem einen ausgehenden Benutzernamen und ein Kennwort auf dem Speichersystem definieren, um die bidirektionale Authentifizierung zu aktivieren, müssen Sie denselben Benutzernamen und dasselbe Kennwort für eingehende CHAP-Einstellungen auf dem Initiator verwenden.
- Sie können nicht denselben Benutzernamen und dasselbe Kennwort für ein- und ausgehende Einstellungen auf dem Speichersystem verwenden.
- CHAP-Benutzernamen können 1 bis 128 Bytes betragen.

Ein Null-Benutzername ist nicht zulässig.

- CHAP-Passwörter (Schlüssel) können 1 bis 512 Bytes betragen.

Passwörter können hexadezimale Werte oder Strings sein. Für hexadezimale Werte sollten Sie den Wert mit einem Präfix von „0x“ oder „0X“ eingeben. Ein Null-Kennwort ist nicht zulässig.

ONTAP ermöglicht die Verwendung von Sonderzeichen, nicht englischen Buchstaben, Zahlen und Leerzeichen für CHAP-Passwörter (Secrets). Dies unterliegt jedoch Host-Einschränkungen. Wenn einer dieser Server von Ihrem spezifischen Host nicht erlaubt ist, können diese nicht verwendet werden.



Der Microsoft iSCSI-Software-Initiator beispielsweise erfordert, dass die CHAP-Passwörter für Initiator und Ziel mindestens 12 Bytes betragen, wenn keine IPsec-Verschlüsselung verwendet wird. Die maximale Kennwortlänge beträgt 16 Byte, unabhängig davon, ob IPsec verwendet wird.

Weitere Einschränkungen finden Sie in der Dokumentation des Initiators.

Die Verwendung von Zugriffslisten für iSCSI-Schnittstellen zur Begrenzung von Initiator-Schnittstellen kann Performance und Sicherheit erhöhen

MITHILFE VON ISCSI-Schnittstellenzugriffslisten kann die Anzahl der LIFs in einer SVM begrenzt werden, auf die ein Initiator zugreifen kann. Dies erhöht die Performance und Sicherheit.

Wenn ein Initiator eine Erkennungssitzung unter Verwendung eines iSCSI startet `SendTargets` Befehl erhält er die IP-Adressen, die dem LIF (Netzwerkschnittstelle) in der Zugriffsliste zugeordnet sind. Standardmäßig haben alle Initiatoren Zugriff auf alle iSCSI LIFs in der SVM. Mithilfe der Zugriffsliste können Sie die Anzahl der LIFs in einer SVM, auf die ein Initiator Zugriff hat, einschränken.

Registrierungsanforderungen für den iSNS-Server

Was iSNS ist

Der Internet Storage Name Service (iSNS) ist ein Protokoll, das die automatische Erkennung und Verwaltung von iSCSI-Geräten in einem TCP/IP-Speichernetzwerk ermöglicht. Ein iSNS-Server speichert Informationen über aktive iSCSI-Geräte im Netzwerk, einschließlich ihrer IP-Adressen, iSCSI-Knotennamen IQN's und Portalgruppen.

Sie können einen iSNS-Server von einem Drittanbieter beziehen. Wenn Sie in Ihrem Netzwerk einen iSNS-Server konfiguriert und für die Verwendung durch den Initiator und das Ziel aktiviert haben, können Sie die Management-LIF für eine Storage Virtual Machine (SVM) verwenden, um alle iSCSI-LIFs für diese SVM auf dem iSNS-Server zu registrieren. Nach Abschluss der Registrierung kann der iSCSI-Initiator den iSNS-Server abfragen, um alle LIFs für diese bestimmte SVM zu ermitteln.

Wenn Sie sich für die Verwendung eines iSNS-Dienstes entscheiden, müssen Sie sicherstellen, dass Ihre Storage Virtual Machines (SVMs) ordnungsgemäß bei einem Internet Storage Name Service (iSNS)-Server registriert sind.

Wenn Sie keinen iSNS-Server im Netzwerk haben, müssen Sie jedes Ziel manuell so konfigurieren, dass es für den Host sichtbar ist.

Was macht ein iSNS-Server

Ein iSNS-Server verwendet das iSNS-Protokoll (Internet Storage Name Service), um Informationen über aktive iSCSI-Geräte im Netzwerk zu erhalten, einschließlich ihrer IP-Adressen, iSCSI-Node-Namen (IQNs) und Portalgruppen.

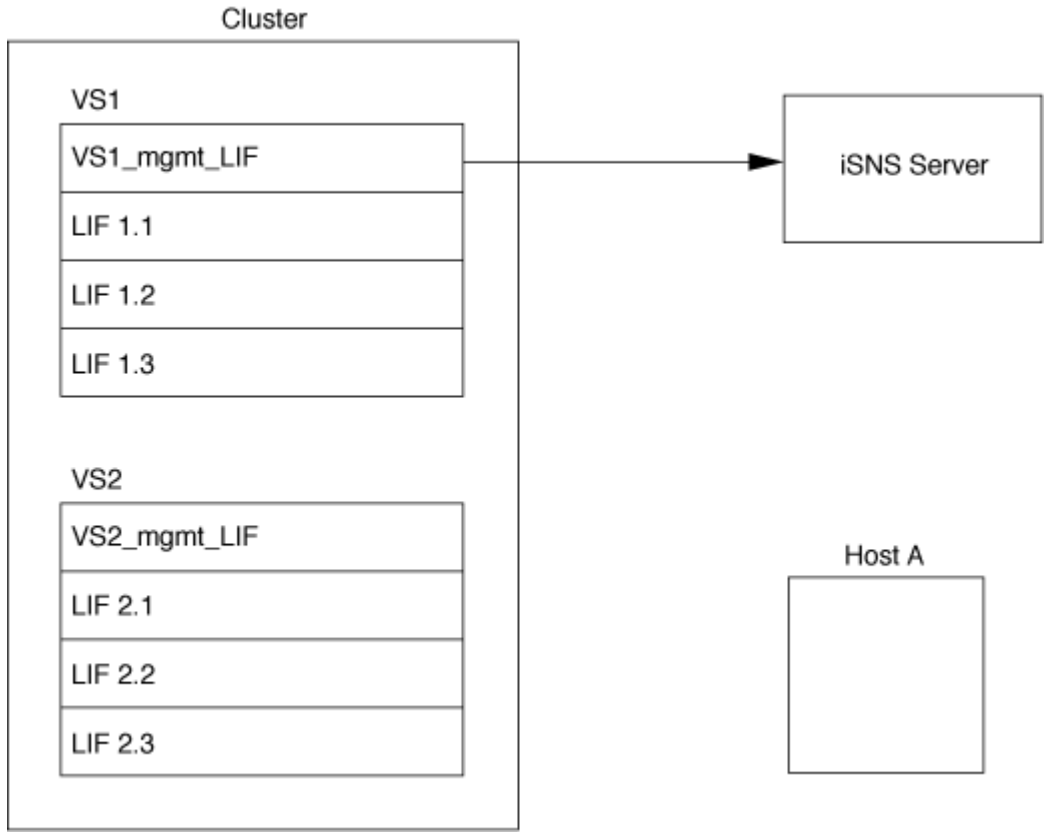
Das iSNS-Protokoll ermöglicht die automatische Erkennung und Verwaltung von iSCSI-Geräten in einem IP-Speichernetzwerk. Ein iSCSI-Initiator kann den iSNS-Server abfragen, um iSCSI-Zielgeräte zu ermitteln.

NetApp bietet keine iSNS Server an oder verkauft diese weiter. Sie können diese Server von einem von NetApp unterstützten Anbieter beziehen.

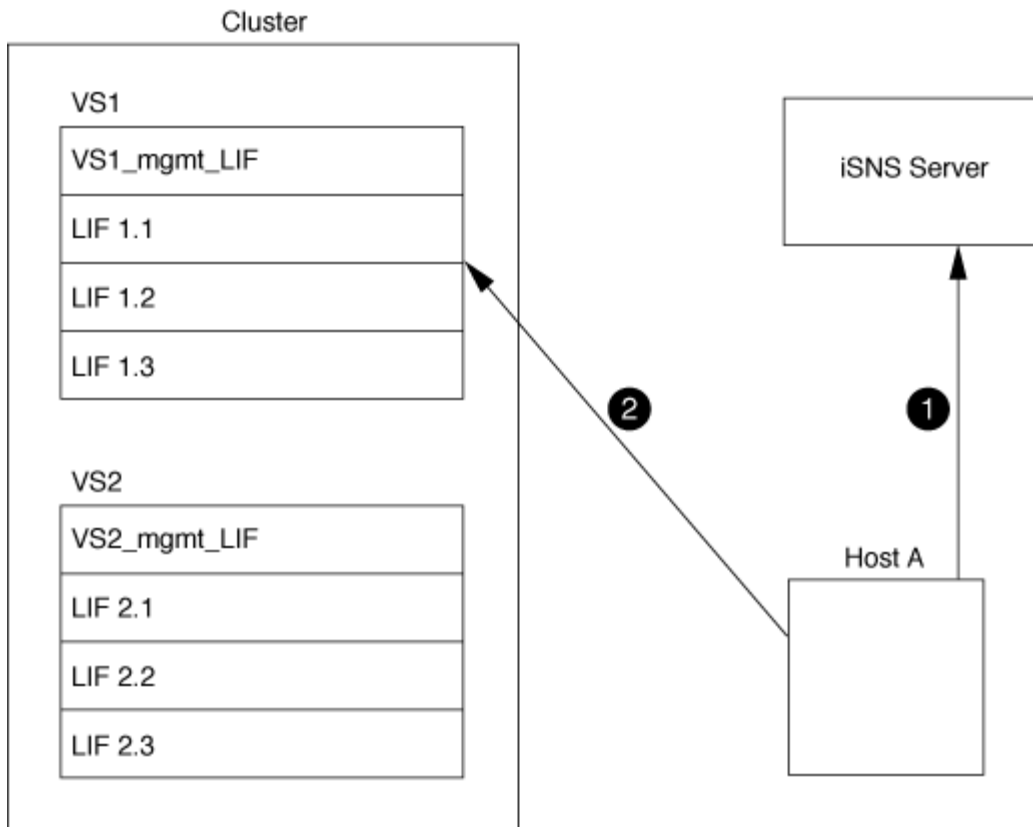
Interaktion von SVMs mit einem iSNS-Server

Der iSNS-Server kommuniziert über die SVM-Management-LIF mit jeder Storage Virtual Machine (SVM). Die Management-LIF registriert alle iSCSI-Zielknotennamen, -Alias und -Portalinformationen beim iSNS-Service für eine bestimmte SVM.

Im folgenden Beispiel verwendet SVM VS1 die SVM-Management-LIF vs1_mgmt_lif zur Registrierung beim iSNS-Server. Während der iSNS-Registrierung sendet eine SVM alle iSCSI-LIFs über die SVM-Management-LIF an den iSNS-Server. Nach Abschluss der iSNS-Registrierung verfügt der iSNS-Server über eine Liste aller LIFs, die iSCSI in VS1 bedienen. Wenn ein Cluster mehrere SVMs enthält, muss sich jede SVM einzeln beim iSNS-Server registrieren, um den iSNS-Service nutzen zu können.



Im nächsten Beispiel, nachdem der iSNS-Server die Registrierung mit dem Ziel abgeschlossen hat, kann Host A alle LIFs für VS1 über den iSNS-Server erkennen, wie in Schritt 1 angegeben. Nachdem Host A die Erkennung der LIFs für VS1 abgeschlossen hat, kann Host A, wie in Schritt 2 dargestellt, eine Verbindung mit einer der LIFs in VS1 herstellen. Host A kennt keine der LIFs in VS2, bis sich das Management-LIF VS2_mgmt_LIF für VS2 beim iSNS-Server registriert.



Wenn Sie jedoch die Schnittstellenzugriffslisten definieren, kann der Host nur die definierten LIFs in der Schnittstellenzugangsliste verwenden, um das Ziel zu erreichen.

Nach der anfänglichen Konfiguration von iSNS aktualisiert ONTAP den iSNS-Server automatisch, wenn sich die SVM-Konfigurationseinstellungen ändern.

Zwischen dem Zeitpunkt, zu dem Sie die Konfigurationsänderungen vornehmen und wenn ONTAP das Update an den iSNS-Server sendet, kann eine Verzögerung von wenigen Minuten auftreten. Sofortige Aktualisierung der iSNS-Informationen auf dem iSNS-Server erzwingen: `vserver iscsi isns update`

Befehle zum Verwalten von iSNS

ONTAP bietet Befehle zur Verwaltung Ihres iSNS-Service.

Ihr Ziel ist	Befehl
Konfigurieren Sie einen iSNS-Dienst	<code>vserver iscsi isns create</code>
Starten Sie einen iSNS-Dienst	<code>vserver iscsi isns start</code>
Ändern eines iSNS-Dienstes	<code>vserver iscsi isns modify</code>
iSNS-Servicekonfiguration anzeigen	<code>vserver iscsi isns show</code>
Aktualisierung der registrierten iSNS-Informationen erzwingen	<code>vserver iscsi isns update</code>

Ihr Ziel ist	Befehl
Stoppen Sie einen iSNS-Dienst	<code>vserver iscsi isns stop</code>
Entfernen Sie einen iSNS-Dienst	<code>vserver iscsi isns delete</code>
Zeigen Sie die man-Page für einen Befehl an	<code>man <i>command name</i></code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

SAN Provisionierung mit FC

Wichtige Konzepte sollten Sie kennen, um zu verstehen, wie ONTAP FC SAN implementiert.

Wie FC-Ziel-Nodes mit dem Netzwerk verbunden werden

Storage-Systeme und Hosts verfügen über Adapter, sodass sie mit Kabeln FC-Switches verbunden werden können.

Wenn ein Node mit dem FC SAN verbunden ist, registriert jede SVM zusammen mit dem Fabric Name Service den World Wide Port Name (WWPN) ihrer logischen Schnittstelle. Der WWNN der SVM und der WWPN jeder logischen Schnittstelle werden automatisch durch ONTAP zugewiesen.



Die direkte Verbindung zu Nodes von Hosts mit FC wird nicht unterstützt, NPIV ist erforderlich und dies erfordert einen Switch, der verwendet werden muss. Bei iSCSI-Sessions funktioniert die Kommunikation mit Verbindungen, die entweder über Netzwerk oder direkt verbunden sind. Beide Methoden werden jedoch von ONTAP unterstützt.

So werden FC-Knoten identifiziert

Jede mit FC konfigurierte SVM wird durch einen Worldwide Node Name (WWNN) identifiziert.

Verwendung von WWPNs

WWPNs identifizieren jede LIF in einer SVM, die zur Unterstützung von FC konfiguriert ist. Diese LIFs nutzen die physischen FC-Ports in jedem Node im Cluster. Dabei können es sich um FC-Target-Karten, UTA oder UTA2 handeln, die in den Nodes als FC oder FCoE konfiguriert wurden.

- Erstellen einer Initiatorgruppe

Die WWPNs der HBAs des Hosts werden zum Erstellen einer Initiatorgruppe verwendet. Eine Initiatorgruppe wird verwendet, um den Host-Zugriff auf bestimmte LUNs zu steuern. Sie können eine Initiatorgruppe erstellen, indem Sie eine Sammlung von WWPNs von Initiatoren in einem FC-Netzwerk angeben. Wenn Sie eine LUN auf einem Storage-System einer Initiatorgruppe zuordnen, können Sie allen Initiatoren in dieser Gruppe Zugriff auf diese LUN gewähren. Wenn der WWPN eines Hosts nicht zu einer Initiatorgruppe gehört, die einer LUN zugeordnet ist, hat der Host keinen Zugriff auf die LUN. Das bedeutet, dass die LUNs nicht als Datenträger auf diesem Host angezeigt werden.

Sie können auch Portsätze erstellen, um eine LUN nur auf bestimmten Zielpoints sichtbar zu machen. Ein

Port-Satz besteht aus einer Gruppe von FC-Ziel-Ports. Sie können eine Initiatorgruppe an einen Portsatz binden. Jeder Host in der Initiatorgruppe kann nur durch Verbindung mit den Ziel-Ports im festgelegten Port auf die LUNs zugreifen.

- Identifizierung von FC-LIFs auf einzigartige Weise

WWPNs identifizieren jede logische FC-Schnittstelle individuell. Das Host-Betriebssystem verwendet die Kombination des WWNN und WWPN, um SVMs und FC LIFs zu identifizieren. Einige Betriebssysteme erfordern eine dauerhafte Bindung, um sicherzustellen, dass die LUN mit derselben Ziel-ID auf dem Host angezeigt wird.

Funktionsweise von weltweiten Namenszuweisungen

Weltweite Namen werden sequenziell in ONTAP erstellt. Aufgrund der Art und Weise, wie ONTAP sie zuweist, werden sie möglicherweise in nicht-sequenzieller Reihenfolge zugewiesen.

Jeder Adapter verfügt über einen vorkonfigurierten WWPN und den WWNN, ONTAP verwendet jedoch diese vorkonfigurierten Werte nicht. Stattdessen weist ONTAP basierend auf den MAC-Adressen der integrierten Ethernet-Ports seine eigenen WWPNs oder WWNNs zu.

Die weltweiten Namen scheinen aus folgenden Gründen nicht sequenziell zu sein:

- Alle Nodes und Storage Virtual Machines (SVMs) im Cluster werden weltweit Namen zugewiesen.
- Freigegebene weltweite Namen werden wiederverwertet und wieder dem Pool verfügbarer Namen hinzugefügt.

So werden FC Switches identifiziert

Fibre Channel-Switches verfügen über einen Worldwide Node Name (WWNN) für das Gerät selbst und einen weltweiten Port-Namen (WWPN) für jeden seiner Ports.

Das folgende Diagramm zeigt beispielsweise, wie den jeweiligen Ports auf einem Brocade Switch mit 16 Ports die WWPNs zugewiesen werden. Weitere Informationen zur Nummer der Ports für einen bestimmten Switch finden Sie in der Dokumentation des Anbieters für diesen Switch.

Port **0**, WWPN 20:**00**:00:60:69:51:06:b4

Port **1**, WWPN 20:**01**:00:60:69:51:06:b4

Port **14**, WWPN 20:**0e**:00:60:69:51:06:b4

Port **15**, WWPN 20:**0f**:00:60:69:51:06:b4

SAN-Provisionierung mit NVMe

Ab ONTAP 9.4 wird NVMe/FC in der SAN-Umgebung unterstützt. Mit NVMe/FC können Storage-Administratoren Namespaces und Subsysteme bereitstellen und anschließend den Namespaces Subsystemen zuordnen, ähnlich der Art und Weise, wie LUNs bereitgestellt und Initiatorgruppen für FC und iSCSI zugeordnet werden.

Ein NVMe Namespace ist eine Menge nicht-flüchtiger Speicher, der in logische Blöcke formatiert werden kann.

Namespaces sind das Äquivalent von LUNs für FC- und iSCSI-Protokolle, und ein NVMe-Subsystem entspricht einer igroup. Ein NVMe-Subsystem kann Initiatoren zugeordnet werden, sodass die zugehörigen Initiatoren auf Namespaces innerhalb des Subsystems zugreifen können.



Obwohl die Funktion analog ist, unterstützen NVMe-Namespaces nicht alle von LUNs unterstützten Funktionen.

Ab ONTAP 9.5 ist eine Lizenz erforderlich, um den Host-bezogenen Datenzugriff mit NVMe zu unterstützen. Wenn NVMe in ONTAP 9.4 aktiviert ist, erhält der Erwerb der Lizenz nach dem Upgrade auf ONTAP 9.5 eine 90-tägige Gnadenfrist. Sie können die Lizenz mit dem folgenden Befehl aktivieren:

```
system license add -license-code NVMe_license_key
```

Verwandte Informationen

["Technischer Bericht von NetApp 4684: Implementieren und Konfigurieren moderner SANs mit NVMe/FC"](#)

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.