SAN-Konzepte

ONTAP 9

NetApp
April 24, 2024

Inhalt

SAN-Konzepte . . . 1
SAN-Bereitstellung mit iSCSI . . . 1
ISCSI-Service-Management . . . 2
SAN Provisionierung mit FC . . . 7
SAN-Provisionierung mit NVMe . . . 9
SAN Volumes . . . 9
SAN-Host-seitiges Speicherplatzmanagement . . . 15
Allgemeines zu Initiatorgruppen . . . 16
Geben Sie Initiator-WWPNs und iSCSI-Node-Namen für eine Initiatorgruppe an . . . 17
Storage-Virtualisierung mit Copy-Offload von VMware und Microsoft . . . 17

SAN-Konzepte

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 hexadezimales 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 unbekannten 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-Schnittstellenzutrittslisten 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.

Internet Storage Name Service (iSNS)

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 die SVM „`VS1`“ die SVM-Management-LIF „`VS1_mgmt_LIF`“, um sich beim iSNS-Server zu registrieren. Während der iSNS-Registrierung sendet eine SVM alle iSCSI-LIFs über die SVM-Management-LIF an den iSNS-Server. Nach Abschluss der iSNS-Registrierung enthält der iSNS-Server eine Liste aller LIFs, die iSCSI in „`VS1`“ bereitstellen. 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 kann Host A, nachdem der iSNS-Server die Registrierung beim Ziel abgeschlossen hat, alle LIFs für „`VS1`“ über den iSNS-Server ermitteln, wie in Schritt 1 angegeben. Nachdem Host A die Erkennung der LIFs für „`VS1`“ abgeschlossen hat, kann Host A wie in Schritt 2 gezeigt eine Verbindung zu jedem der LIFs in „`VS1`“ herstellen. Host A erkennt keine der LIFs in „`VS2`“, bis sich die Management-LIF „`VS2_mgmt_LIF`“ für „`VS2`“ beim iSNS-Server registriert hat.

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 dem Zeitpunkt, an dem ONTAP das Update an den iSNS-Server sendet, kann es zu einer Verzögerung von einigen Minuten kommen. 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	`vserver iscsi isns create`
Starten Sie einen iSNS-Dienst	`vserver iscsi isns start`
Ändern eines iSNS-Dienstes	`vserver iscsi isns modify`
ISNS-Servicekonfiguration anzeigen	`vserver iscsi isns show`

Aktualisierung der registrierten iSNS-Informationen erzwingen	`vserver iscsi isns update`
Stoppen Sie einen iSNS-Dienst	`vserver iscsi isns stop`
Entfernen Sie einen iSNS-Dienst	`vserver iscsi isns delete`
Zeigen Sie die man-Page für einen Befehl an	`man` *`command name`*

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 handelt, 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 Zielports 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.

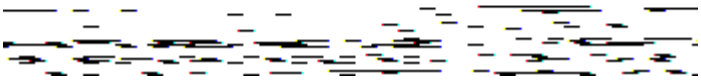
Die weltweiten Namen scheinen aus folgenden Gründen nicht sequenziell zu sein:

- 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. Wenn Sie haben "ONTAP One", Die NVMe-Lizenzen sind enthalten. 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"

SAN Volumes

Über SAN Volumes – Übersicht

ONTAP bietet drei grundlegende Volume-Bereitstellungsoptionen: Thick Provisioning, Thin Provisioning und semi-Thick Provisioning. Jede Option nutzt unterschiedliche Methoden zum Managen des Volume-Speicherplatzes und des Platzbedarfs für die ONTAP Technologien zur gemeinsamen Nutzung von Blöcken. Wenn Sie verstehen, wie diese Optionen funktionieren, können Sie die beste Option für Ihre Umgebung wählen.

> Es wird nicht empfohlen, SAN-LUNs und NAS-Freigaben in ein und demselben FlexVol-Volume einzurichten. Sie sollten separate FlexVol Volumes speziell für Ihre SAN LUNs bereitstellen, und Sie sollten separate FlexVol Volumes speziell für Ihre NAS-Freigaben bereitstellen. Dies vereinfacht die Implementierung von Management und Replizierung und Parallelen zur Unterstützung von FlexVol Volumes durch Active IQ Unified Manager (ehemals OnCommand Unified Manager).

Thin Provisioning für Volumes

Wenn ein Thin Provisioning Volume erstellt wird, reserviert ONTAP bei der Erstellung des Volume keinen zusätzlichen Speicherplatz. Wenn Daten auf das Volume geschrieben werden, fordert das Volume zur Erfüllung der Schreibvorgänge den erforderlichen Storage vom Aggregat an. Bei der Verwendung von Volumes, die Thin Provisioning einsetzen, können Sie Ihr Aggregat bei einer Überprovisionierung einsetzen. Dadurch wird es möglich, dass das Volume den erforderlichen Speicherplatz nicht sichern kann, wenn dem Aggregat der freie Speicherplatz ausgeht.

Sie erstellen ein FlexVol-Volume mit Thin Provisioning, indem Sie dessen festlegen `-space-guarantee` Option auf `none`.

Thick Provisioning für Volumes

Wenn ein Thick Provisioning Volume erstellt wird, legt ONTAP ausreichend Storage vom Aggregat ab, um sicherzustellen, dass jeder Block im Volume jederzeit geschrieben werden kann. Wenn Sie ein Volume für die Nutzung von Thick Provisioning konfigurieren, können Sie jede der ONTAP Storage-Effizienz-Funktionen einsetzen, beispielsweise für Komprimierung und Deduplizierung, um die höheren Storage-Anforderungen im Vorfeld zu erfüllen.

Sie erstellen ein per Thick Provisioning bereitgestelltes FlexVol-Volume durch Festlegen dessen `-space-slo` (Service Level Objective)-Option nach `thick`.

Semi-Thick Provisioning für Volumes

Wenn ein Volume mit semi-Thick Provisioning erstellt wird, legt ONTAP Storage vom Aggregat zu, um die Volume-Größe zu berücksichtigen. Wenn dem Volume der freie Speicherplatz zur Verfügung steht, weil Blöcke durch Block-Sharing-Technologien genutzt werden, ist ONTAP bemüht, geschützte Datenobjekte (Snapshot-Kopien, FlexClone Dateien und LUNs) zu löschen, um den Platz freizugeben. Solange ONTAP die geschützten Datenobjekte schnell genug löschen kann, um mit dem für Überschreibungen erforderlichen Speicherplatz Schritt zu halten, sind die Schreibvorgänge weiterhin erfolgreich. Dies wird als „`Best Effort`“-Garantie bezeichnet.

Hinweis: die folgende Funktionalität wird auf Volumes, die semi-Thick Provisioning verwenden, nicht unterstützt:

- Storage-Effizienztechnologien wie Deduplizierung, Komprimierung und Data-Compaction
- Microsoft Offloaded Data Transfer (ODX)

Sie erstellen ein FlexVol-Volume mit semi-Thick-Provision-Funktion, indem Sie dessen festlegen `-space-slo` (Service Level Objective)-Option nach `semi-thick`.

Nutzung mit platzsparenden Dateien und LUNs

Eine speicherreservierte Datei oder eine LUN ist eine Datei, für die beim Erstellen Speicherplatz zugewiesen wird. Ursprünglich hat NetApp den Begriff „`Thin-Provision-LUN`“ verwendet, um eine LUN zu bedeuten, für die Platzreservierung deaktiviert ist (eine nicht-space-reservierte LUN).

Hinweis: nicht-speicherreservierte Dateien werden allgemein nicht als “Thin Provisioning-Dateien” bezeichnet.

In der folgenden Tabelle sind die wichtigsten Unterschiede zwischen der Verwendung der drei Optionen zur Volume-Bereitstellung für platzreservierte Dateien und LUNs zusammengefasst:

Volume-Provisionierung	LUN-/Dateispeicherreservierung	Überschreibung	Sicherungsdaten[2]	Storage-Effizienz[3]
Dick	Unterstützt	Garantiert[1]	Garantiert	Unterstützt
Dünn	Keine Auswirkung	Keine	Garantiert	Unterstützt

Volume-Provisionierung	LUN-/Dateispeicherreservierung	Überschreibung	Sicherungsdaten[2]	Storage-Effizienz[3]
Semi-dick	Unterstützt	Bester Aufwand[1]	So gut wie möglich	Nicht unterstützt

Hinweise

1. Um Überschreibungen zu garantieren oder ihnen eine optimale Überschreibsicherung zu ermöglichen, ist die Speicherplatzreservierung auf dem LUN oder der Datei aktiviert.
2. Zu den Sicherungsdaten gehören Snapshot-Kopien sowie FlexClone-Dateien und LUNs, die zum automatischen Löschen markiert sind (Backup-Klone).
3. Storage-Effizienz umfasst Deduplizierung, Komprimierung sowie alle FlexClone-Dateien und LUNs, die nicht zum automatischen Löschen markiert sind (aktive Klone) und Unterdateien von FlexClone (für Copy Offload verwendet).

Unterstützung von SCSI Thin Provisioning LUNs

ONTAP unterstützt T10 SCSI Thin Provisioning LUNs sowie NetApp Thin Provisioning LUNs. Mit T10 SCSI Thin Provisioning können Host-Applikationen SCSI-Funktionen unterstützen, einschließlich LUN-Speicherplatzrückgewinnung und LUN-Speicherplatzüberwachung für Umgebungen mit Blöcken. T10 SCSI Thin Provisioning muss von Ihrer SCSI-Host-Software unterstützt werden.

Sie verwenden die ONTAP `space-allocation` Einstellung zum Aktivieren/Deaktivieren der Unterstützung für das T10 Thin Provisioning auf einer LUN Sie verwenden die ONTAP `space-allocation enable` Einstellung zum Aktivieren von T10 SCSI Thin Provisioning auf einem LUN.

Der `[-space-allocation {enabled|disabled}]` Befehl im ONTAP Command Reference Manual enthält weitere Informationen zum Aktivieren/Deaktivieren der Unterstützung für das T10 Thin Provisioning und zur Aktivierung von T10 SCSI Thin Provisioning auf einer LUN.

"ONTAP 9-Befehle"

Konfiguration der Bereitstellungsoptionen für Volumes

Sie können ein Volume für Thin Provisioning, Thick Provisioning oder Semi-Thick Provisioning konfigurieren.

Über diese Aufgabe

Einstellen des `-space-slo` Option auf `thick` Stellt Folgendes sicher:

- Das gesamte Volume wird im Aggregat vorab zugewiesen. Sie können das nicht verwenden `volume create` Oder `volume modify` Befehl zum Konfigurieren des Volume `-space-guarantee` Option.
- 100 % des für Überschreibungen benötigten Speicherplatzes ist reserviert. Sie können das nicht verwenden `volume modify` Befehl zum Konfigurieren des Volume `-fractional-reserve` Option

Einstellen des `-space-slo` Option auf `semi-thick` Stellt Folgendes sicher:

- Das gesamte Volume wird im Aggregat vorab zugewiesen. Sie können das nicht verwenden `volume create` Oder `volume modify` Befehl zum Konfigurieren des Volume `-space-guarantee` Option.

- Kein Speicherplatz für Überschreibungen reserviert. Sie können das verwenden `volume modify` Befehl zum Konfigurieren des Volume `-fractional-reserve` Option.
- Das automatische Löschen von Snapshot-Kopien ist aktiviert.

Schritt

1. Konfiguration der Bereitstellungsoptionen für Volumes:

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

   Der `-space-guarantee` Die Option ist standardmäßig aktiviert `none` Für AFF Systeme und für DP-Volumes ohne All Flash FAS. Andernfalls wird standardmäßig auf verwendet `volume`. Verwenden Sie für vorhandene FlexVol-Volumes das `volume modify` Befehl zum Konfigurieren von Bereitstellungsoptionen.

   Der folgende Befehl konfiguriert vol1 auf SVM vs1 für Thin Provisioning:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   Mit dem folgenden Befehl wird vol1 auf SVM vs1 für Thick Provisioning konfiguriert:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
   ```

   Mit dem folgenden Befehl wird vol1 auf SVM vs1 für semi-Thick Provisioning konfiguriert:

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
   thick
   ```

SAN Volume-Konfigurationsoptionen

Sie müssen verschiedene Optionen auf dem Volume festlegen, das Ihre LUN enthält. Die Art und Weise, wie Sie die Volume-Optionen festlegen, bestimmt die Menge an Speicherplatz, die LUNs im Volume zur Verfügung steht.

Autogrow

Sie können Autogrow aktivieren oder deaktivieren. Wenn Sie es aktivieren, ermöglicht es Autogrow ONTAP, die Größe des Volumes automatisch auf eine maximale Größe zu erhöhen, die Sie vorab bestimmen. Um das automatische Wachstum des Volumes zu unterstützen, muss im enthaltenden Aggregat Platz vorhanden sein. Wenn Sie Autogrow aktivieren, müssen Sie daher den freien Speicherplatz im Aggregat, der enthält, überwachen und bei Bedarf mehr hinzufügen.

Autogrow kann nicht ausgelöst werden, um Snapshot Erstellung zu unterstützen. Wenn Sie versuchen, eine Snapshot Kopie zu erstellen und es zu wenig Speicherplatz auf dem Volume gibt, schlägt die Snapshot-Erstellung fehl, selbst wenn Autogrow aktiviert ist.

Wenn Autogrow deaktiviert ist, bleibt die Größe Ihres Volumes dieselbe.

Autochrink

Sie können Autochrink aktivieren oder deaktivieren. Wenn Sie ihn aktivieren, ermöglicht Autochrink es ONTAP, die Gesamtgröße eines Volumes automatisch zu verringern, wenn die Menge an Speicherplatz, die im Volume verbraucht wird, einen vorab festgelegten Schwellenwert verringert. Dies erhöht die Storage-Effizienz, indem Volumes automatisch ungenutzten freien Speicherplatz freigeben.

Snapshot wird automatisches Löschen erstellt

Durch das automatische Löschen von Snapshots werden Snapshot Kopien automatisch gelöscht, wenn eine der folgenden tritt:

- Das Volume ist fast voll.
- Der Speicherplatz der Snapshot Reserve ist fast voll.
- Der Speicherplatz der Überschreibungsreserve ist voll.

Sie können die Snapshot automatisches Löschen konfigurieren, um Snapshot Kopien von ältesten bis neuesten oder von neuesten bis ältesten zu löschen. Durch das Löschen von Snapshots werden keine Snapshot Kopien gelöscht, die mit Snapshot-Kopien in geklonten Volumes oder LUNs verknüpft sind.

Wenn Ihr Volume zusätzlichen Speicherplatz benötigt und Sie sowohl Autogrow als auch Snapshot Autodelete aktiviert haben, versucht ONTAP standardmäßig, den erforderlichen Speicherplatz durch Auslösung von Autogrow zu erwerben. Wenn nicht genügend Speicherplatz durch Autogrow erfasst wird, dann wird Snapshot Autodelete ausgelöst.

Snapshot Reserve

Die Snapshot Reserve definiert die Menge an Speicherplatz im Volume, das für Snapshot Kopien reserviert ist. Der zur Snapshot Reserve zugewiesenen Speicherplatz kann nicht für andere Zwecke verwendet werden. Wenn der gesamte für die Snapshot-Reserve zugewiesene Speicherplatz verwendet wird, dann beginnen Snapshot Kopien, zusätzlichen Speicherplatz auf dem Volume zu belegen.

Anforderung für das Verschieben von Volumes in SAN-Umgebungen

Bevor Sie ein Volume mit LUNs oder Namespaces verschieben, müssen Sie bestimmte Anforderungen erfüllen.

- Für Volumes mit einer oder mehreren LUNs sollten mindestens zwei Pfade pro LUN (LIFs) vorhanden sein, die mit jedem Node im Cluster verbunden sind.

  So werden Single Points of Failure eliminiert und das System kann den Ausfall von Komponenten überleben.

- Für Volumes, die Namespaces enthalten, muss auf dem Cluster ONTAP 9.6 oder höher ausgeführt werden.

  Die Volume-Verschiebung wird für NVMe Konfigurationen mit ONTAP 9.5 nicht unterstützt.

Überlegungen bei der Festlegung der fraktionalen Reserve

Die fraktionale Reserve, auch *LUN Overwrite Reserve* genannt, ermöglicht Ihnen die Abschaltung der Überschreibungsreserve für platzsparende LUNs und Dateien in einem FlexVol Volume. So können Sie Ihre Storage-Auslastung maximieren, aber wenn Ihre Umgebung durch mangelnde Schreibzugriffe beeinträchtigt ist, müssen Sie die Anforderungen dieser Konfiguration kennen und verstehen, die diese Konfiguration mit sich bringt.

Die Einstellung der fraktionalen Reserve wird als Prozentsatz angegeben; die einzigen gültigen Werte sind `0` Und `100` Prozent Die Einstellung der fraktionalen Reserve ist ein Attribut des Volume.

Einstellung der fraktionalen Reserve auf `0` Verbessern Sie Ihre Storage-Auslastung. Wenn jedoch für eine Applikation, die auf Daten im Volume zugreift, ein Datenausfall auftritt, könnte es sein, wenn das Volume über keinen freien Speicherplatz verfügt, selbst wenn die Volume-Garantie festgelegt wurde `volume`. Durch ordnungsgemäße Volume-Konfiguration und Nutzung können Sie jedoch die Wahrscheinlichkeit eines Schreibversagens minimieren. ONTAP bietet eine „`Best Effort`“-Garantie für Volumes mit als fraktionaler Reserve `0` Wenn *all* der folgenden Anforderungen erfüllt sind:

- Die Deduplizierung wird nicht verwendet
- Die Komprimierung wird nicht verwendet
- Die Unterdateien von FlexClone werden nicht verwendet
- Alle FlexClone Dateien und FlexClone LUNs sind zum automatischen Löschen aktiviert

  Dies ist nicht die Standardeinstellung. Sie müssen das automatische Löschen entweder während der Erstellung oder durch Ändern der FlexClone Datei oder der FlexClone LUN nach der Erstellung aktivieren.

- ODX und FlexClone Copy Offload werden derzeit nicht genutzt
- Die Volume-Garantie ist auf festgelegt `volume`
- Datei- oder LUN-Speicherplatzreservierung ist `enabled`
- Die Snapshot-Reserve des Volumes ist auf festgelegt `0`
- Das automatische Löschen von Volume Snapshot Kopien ist `enabled` Mit einem Maß an Engagement `destroy`, Eine zerstörte Liste von `lun_clone,vol_clone,cifs_share,file_clone,sfsr`, Und ein Auslöser von `volume`

  Diese Einstellung stellt zudem sicher, dass FlexClone Dateien und FlexClone LUNs im Bedarfsfall gelöscht werden.

Beachten Sie, dass wenn Ihre Änderungsrate hoch ist, in seltenen Fällen kann das automatische Löschen der Snapshot-Kopie den Wert hinterherhinken, sodass das Volume nicht mehr über genügend Speicherplatz verfügt. Dies gilt auch für alle oben genannten Konfigurationseinstellungen.

Darüber hinaus können Sie optional die Funktion Volume Autogrow verwenden, um die Wahrscheinlichkeit zu verringern, dass Volume-Snapshot-Kopien automatisch gelöscht werden müssen. Wenn Sie die Autogrow-Funktion aktivieren, müssen Sie den freien Speicherplatz im zugehörigen Aggregat überwachen. Wenn das Aggregat voll genug ist, um das Volume nicht mehr zu wachsen, werden wahrscheinlich mehr Snapshot-Kopien gelöscht, da der freie Speicherplatz im Volume erschöpft ist.

Wenn Sie nicht alle oben genannten Konfigurationsanforderungen erfüllen können und Sie sicherstellen

müssen, dass das Volume nicht über genügend Speicherplatz verfügt, müssen Sie die Einstellung für die fraktionale Reserve des Volume auf festlegen `100`. Dies erfordert vorab mehr freien Speicherplatz, garantiert jedoch, dass Datenänderungen auch dann erfolgreich ausgeführt werden, wenn die oben aufgeführten Technologien eingesetzt werden.

Der Standardwert und die zulässigen Werte für die Einstellung der fraktionalen Reserve hängen von der Garantie des Volume ab:

Volume-Garantie	Standardmäßige fraktionale Reserve	Zulässige Werte
Datenmenge	100	0, 100
Keine	0	0, 100

SAN-Host-seitiges Speicherplatzmanagement

In einer durch Thin Provisioning bereitgestellten Umgebung rundet das Platzmanagement auf der Host-Seite den Prozess des Speicherplatzmanagements auf dem Storage-System ab, das im Host-Filesystem freigegeben wurde.

Ein Host-Filesystem enthält Metadaten, um zu verfolgen, welche Blöcke zum Speichern neuer Daten verfügbar sind und welche Blöcke gültige Daten enthalten, die nicht überschrieben werden dürfen. Diese Metadaten werden innerhalb der LUN gespeichert. Wenn eine Datei im Host-Filesystem gelöscht wird, werden die Metadaten des Filesystems aktualisiert, um die Blöcke dieser Datei als freien Speicherplatz zu markieren. Der gesamte freie Speicherplatz des Filesystems wird dann neu berechnet, um die neu freigegebenen Blöcke einzubeziehen. Für das Speichersystem werden diese Metadatenaktualisierungen nicht von anderen Schreibvorgängen angezeigt, die vom Host ausgeführt werden. Daher ist im Storage-System keine Löschung aufgetreten.

Dadurch entsteht eine Diskrepanz zwischen der Menge an freiem Speicherplatz, die vom Host gemeldet wird, und der Menge an freiem Speicherplatz, die vom zugrunde liegenden Storage-System gemeldet wird. Nehmen wir beispielsweise an, dass Ihrem Host durch Ihr Storage-System eine neu bereitgestellte 200-GB-LUN zugewiesen ist. Sowohl der Host als auch das Speichersystem berichten von 200 GB freiem Speicherplatz. Ihr Host schreibt dann 100 GB Daten. An diesem Punkt berichten sowohl der Host als auch das Speichersystem von 100 GB belegten Speicherplatz und 100 GB nicht genutztem Speicherplatz.

Dann löschen Sie 50 GB Daten von Ihrem Host. An dieser Stelle meldet Ihr Host 50 GB verbrauchten Speicherplatz und 150 GB nicht genutzten Speicherplatz. Ihr Speichersystem wird jedoch 100 GB verwendeten Speicherplatzes und 100 GB nicht genutzten Speicherplatz melden.

Das Host-seitige Speicherplatzmanagement verwendet verschiedene Methoden, um den Speicherplatzunterschied zwischen dem Host und dem Storage-System abzugleichen.

Vereinfachtes Host-Management mit SnapCenter

Mit SnapCenter können Sie einige Management- und Datensicherungsaufgaben von iSCSI- und FC-Storage vereinfachen. SnapCenter ist ein optionales Management-Paket für Windows- und UNIX-Hosts.

Mit SnapCenter lassen sich mühelos virtuelle Festplatten aus Storage-Pools erstellen, die auf verschiedene Storage-Systeme verteilt werden können. Die Storage-Provisionierung wird automatisiert und die Erstellung von Snapshot Kopien und Klonen von Snapshot Kopien, die mit Host-Daten konsistent sind, wird vereinfacht.

Weitere Informationen finden Sie in der NetApp Produktdokumentation "SnapCenter".

Weiterführende Links

"Aktivieren Sie die Speicherplatzzuweisung für Thin Provisioning LUNs von SCSI"

Allgemeines zu Initiatorgruppen

Initiatorgruppen sind Tabellen mit FC-Protokoll-Host-WWPNs oder iSCSI-Host-Node-Namen. Sie können Initiatorgruppen definieren und sie LUNs zuordnen, um zu steuern, welche Initiatoren Zugriff auf LUNs haben.

Normalerweise möchten Sie, dass alle Initiator-Ports oder Software-Initiatoren des Hosts Zugriff auf eine LUN haben. Wenn Sie Multipathing-Software oder Cluster-Hosts verwenden, benötigt jeder Initiator- oder Software-Initiator jedes Cluster-Hosts redundante Pfade zu derselben LUN.

Sie können Initiatorgruppen erstellen, die angeben, welche Initiatoren entweder vor oder nach dem Erstellen der LUNs Zugriff auf die LUNs haben. Sie müssen jedoch Initiatorgruppen erstellen, bevor Sie eine LUN einer Initiatorgruppe zuordnen können.

Initiatorgruppen können mehrere Initiatoren haben, und mehrere Initiatorgruppen können denselben Initiator haben. Sie können eine LUN jedoch nicht mehreren Initiatorgruppen zuordnen, die denselben Initiator haben. Ein Initiator kann nicht Mitglied von iGroups verschiedener ostypes sein.

Beispiel dafür, wie Initiatorgruppen LUN-Zugriff geben

Sie können mehrere Initiatorgruppen erstellen, um zu definieren, welche LUNs Ihren Hosts zur Verfügung stehen. Wenn Sie beispielsweise ein Host-Cluster haben, können Sie Initiatorgruppen verwenden, um sicherzustellen, dass bestimmte LUNs nur für einen Host im Cluster oder für alle Hosts im Cluster sichtbar sind.

In der folgenden Tabelle wird erläutert, wie vier Initiatorgruppen für vier verschiedene Hosts, die auf das Storage-System zugreifen, auf die LUNs zugreifen. Die Cluster-Hosts (host3 und Host4) sind beide Mitglieder derselben Initiatorgruppe (Gruppe 3) und können auf die LUNs zugreifen, die dieser Initiatorgruppe zugeordnet sind. Die igroup namens group4 enthält die WWPNs von Host4 zum Speichern von lokalen Informationen, die vom Partner nicht erkannt werden sollen.

Hosts mit HBA-WWPNs, IQNs oder EUIs	igroups	WWPNs, IQNs, EUIs, die Initiatorgruppen hinzugefügt wurden	LUNs zugeordnet zu Initiatorgruppen
Host1, Single Path (iSCSI Software Initiator) iqn.1991-05.com.microsoft:host1	gruppe1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host 2, Multipath (zwei HBAs) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	gruppe2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	`/vol/vol2/lun2`

Hosts mit HBA-WWPNs, IQNs oder EUIs	igroups	WWPNs, IQNs, EUIs, die Initiatorgruppen hinzugefügt wurden	LUNs zugeordnet zu Initiatorgruppen
Host3, Multipath, Cluster mit Host 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	gruppe3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree1/lun3`
HOST4, Multipath, Clustered (nicht als Host sichtbar) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	Gruppe 4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

Geben Sie Initiator-WWPNs und iSCSI-Node-Namen für eine Initiatorgruppe an

Sie können die iSCSI-Node-Namen und WWPNs der Initiatoren angeben, wenn Sie eine Initiatorgruppe erstellen oder sie später hinzufügen können. Wenn Sie beim Erstellen der LUN die iSCSI-Node-Namen und WWPNs des Initiators angeben, können diese später, falls erforderlich, entfernt werden.

Befolgen Sie die Anweisungen in der Dokumentation zu Host Utilities, um WWPNs abzurufen und die iSCSI-Node-Namen zu finden, die einem bestimmten Host zugeordnet sind. Verwenden Sie für Hosts, auf denen ESX-Software ausgeführt wird, Virtual Storage Console.

Storage-Virtualisierung mit Copy-Offload von VMware und Microsoft

Überblick: Storage-Virtualisierung mit VMware und Microsoft Copy-Offload

Kopierauslagerungsoperationen von VMware und Microsoft zur Steigerung der Performance und des Netzwerkdurchsatzes Sie müssen Ihr System so konfigurieren, dass es die Anforderungen der Betriebssystemumgebungen von VMware und Windows erfüllt, damit die jeweiligen Funktionen zur Offload von Kopien genutzt werden können.

Bei der Nutzung von VMware und Microsoft Copy-Offload in virtualisierten Umgebungen müssen Ihre LUNs aufeinander abgestimmt werden. Nicht ausgerichtete LUNs können die Performance beeinträchtigen.

Vorteile der Nutzung einer virtualisierten SAN-Umgebung

Wenn Sie eine virtualisierte Umgebung mithilfe von Storage Virtual Machines (SVMs) und LIFs erstellen, können Sie Ihre SAN-Umgebung auf alle Nodes im Cluster erweitern.

- Dezentrales Management

  Sie können sich bei jedem Node in der SVM anmelden, um alle Nodes in einem Cluster zu verwalten.

- Verbesserter Datenzugriff

  Mit MPIO und ALUA haben Sie Zugriff auf Ihre Daten über alle aktiven iSCSI oder FC LIFs für die SVM.

- Kontrollierter LUN-Zugriff

  Wenn Sie SLM und Portsätze verwenden, können Sie die Anzahl der LIFs begrenzen, die ein Initiator zum Zugriff auf LUNs verwenden kann.

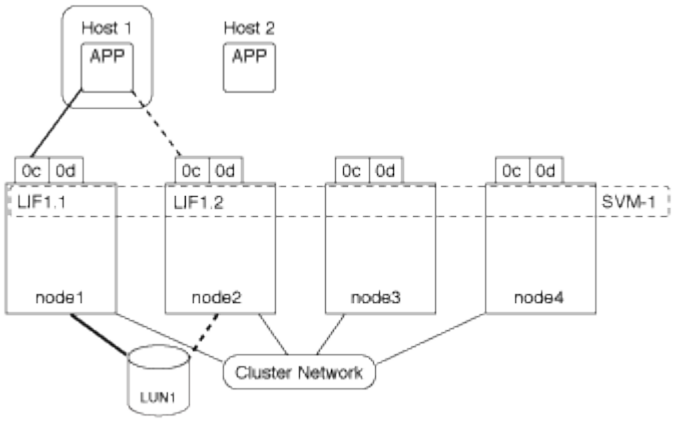
Der Zugriff auf LUNs erfolgt in einer virtualisierten Umgebung

In einer virtualisierten Umgebung können Hosts (Clients) mithilfe von optimierten und nicht optimierten Pfaden auf LUNs zugreifen.

Eine LIF ist eine logische Schnittstelle, die die SVM mit einem physischen Port verbindet. Obwohl mehrere SVMs mehrere LIFs am selben Port aufweisen können, gehört eine LIF zu einer SVM. Die LUNs können über die LIFs der SVMs aufgerufen werden.

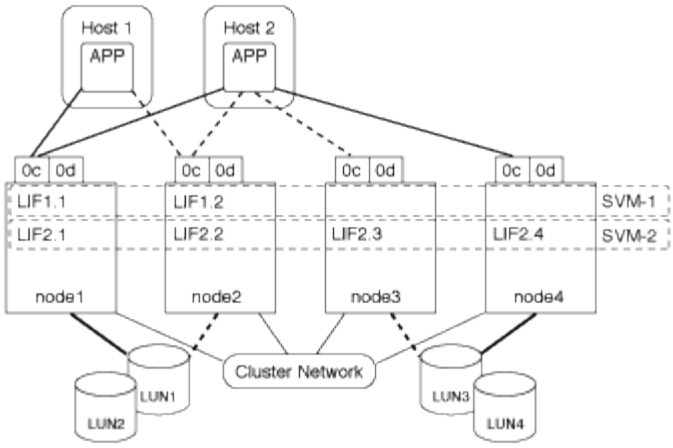
Beispiel für einen LUN-Zugriff über eine einzelne SVM in einem Cluster

Im folgenden Beispiel stellt Host 1 eine Verbindung zu LIF1.1 und LIF1.2 in SVM-1 her, um auf LUN1 zuzugreifen. LIF1.1 verwendet den physischen Port Nr. 1:0c und LIF1.2 mit dem Node2:0c. LIF1.1 und LIF1,2 gehören nur zu SVM-1. Wenn eine neue LUN auf Node 1 oder Node 2 für SVM-1 erstellt wird, können sie dieselben LIFs verwenden. Wenn eine neue SVM erstellt wird, können neue LIFs mit physischen Ports 0c oder 0d der beiden Nodes erstellt werden.



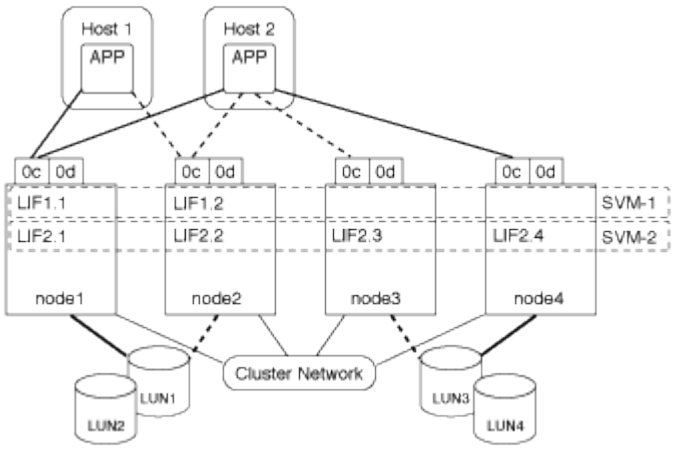
Beispiel eines LUN-Zugriffs mit mehreren SVMs in einem Cluster

Ein physischer Port kann mehrere LIFs unterstützen, die unterschiedliche SVMs unterstützen. Da LIFs einer bestimmten SVM zugeordnet sind, können die Cluster-Nodes den eingehenden Datenverkehr an die richtige SVM senden. Im folgenden Beispiel verfügt jeder Node von 1 bis 4 über eine LIF für SVM-2 mit dem physischen Port 0c auf jedem Node. Host 1 stellt eine Verbindung zu LIF1.1 und LIF1.2 in SVM-1 her, um auf LUN1 zuzugreifen. Host 2 stellt eine Verbindung zu LIF2-1 und LIF2-2 in SVM-2 her, um auf LUN2 zuzugreifen. Beide SVMs teilen sich den physischen Port 0c auf den Nodes 1 und 2. SVM-2 verfügt über zusätzliche LIFs, über die Host 2 auf LUNs 3 und 4 zugreift. Diese LIFs verwenden den physischen Port 0c an den Nodes 3 und 4. Mehrere SVMs können die physischen Ports auf den Nodes gemeinsam nutzen.



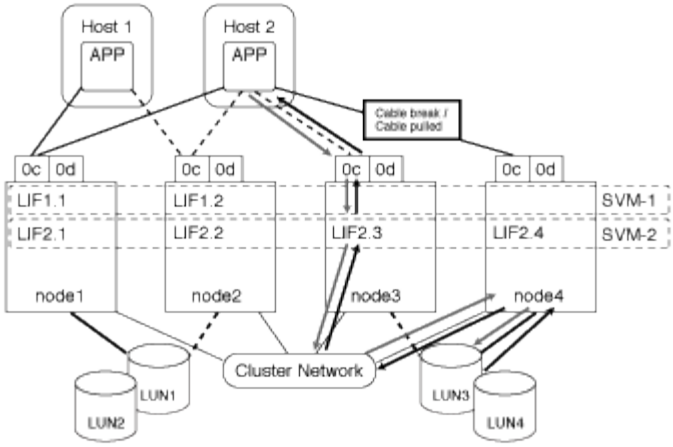
Beispiel eines aktiven oder optimierten Pfads zu einer LUN von einem Host-System aus

In einem aktiven oder optimierten Pfad bewegt sich der Datenverkehr nicht über das Cluster-Netzwerk. Er reist die direkteste Route zur LUN. Der aktive oder optimierte Pfad zu LUN1 erfolgt über LIF1.1 in node1, wobei der physische Port 0c verwendet wird. Host 2 verfügt über zwei aktive oder optimierte Pfade, einen Pfad zu node1, LIF2.1, der den physischen Port 0c und den anderen Pfad zu node4, LIF2.4 nutzt, der physischen Port 0c verwendet.



Beispiel eines aktiven oder nicht optimierten Pfads (indirekter) zu einer LUN von einem Host-System aus

In einem aktiven oder nicht optimierten Pfad (indirekter) wird der Datenverkehr über das Cluster-Netzwerk übertragen. Dieses Problem tritt nur auf, wenn alle aktiven oder optimierten Pfade eines Hosts nicht zur Verarbeitung des Datenverkehrs zur Verfügung stehen. Wenn der Pfad von Host 2 zu SVM-2 LIF2.4 verloren geht, durchläuft der Zugriff auf LUN3 und LUN4 das Cluster-Netzwerk. Zugriff von Host 2 verwendet LIF2.3 auf node3. Dann gelangt der Traffic zum Cluster-Netzwerk-Switch und sichert bis zu node4 für den Zugriff auf LUN3 und LUN4. Diese erfolgt dann wieder über den Cluster-Netzwerk-Switch und dann über LIF2.3 auf Host 2. Dieser aktive oder nicht optimierte Pfad wird verwendet, bis der Pfad zu LIF2.4 wiederhergestellt ist oder eine neue LIF auf einem anderen physischen Port auf Node 4 für SVM-2 eingerichtet wurde.



= :allow-uri-read:

Verbesserung der VMware VAAI-Leistung für ESX-Hosts

ONTAP unterstützt bestimmte VMware vStorage APIs for Array Integration (VAAI)-Funktionen, wenn der ESX Host ESX 4.1 oder höher ausführt. Diese Funktionen helfen, die Vorgänge vom ESX Host auf das Storage-System zu verlagern und den Netzwerkdurchsatz zu erhöhen. Der ESX-Host aktiviert die Funktionen automatisch in der richtigen Umgebung.

Die VAAI-Funktion unterstützt die folgenden SCSI-Befehle:

- `EXTENDED_COPY`

  Diese Funktion ermöglicht es dem Host, den Datentransfer zwischen den LUNs oder innerhalb einer LUN zu initiieren, ohne den Host beim Datentransfer zu involvieren. Dies führt zu Einsparungen von ESX CPU-Zyklen und einer Erhöhung des Netzwerkdurchsatzes. Die Funktion für erweiterte Kopien, auch bekannt als „Copy Offload“, wird in Szenarien wie dem Klonen einer Virtual Machine verwendet. Wenn der ESX Host aufgerufen wird, kopiert die Funktion zum Offload die Daten im Storage-System, anstatt über das Host-Netzwerk zu gehen. Beim Copy-Offload werden Daten auf folgende Weise übertragen:

  - Innerhalb einer LUN
  - Zwischen LUNs in einem Volume erstellt
  - Zwischen LUNs auf verschiedenen Volumes innerhalb einer Storage Virtual Machine (SVM)
  - Zwischen LUNs auf verschiedenen SVMs innerhalb eines Clusters Wenn diese Funktion nicht aufgerufen werden kann, verwendet der ESX Host für den Kopiervorgang automatisch die standardmäßigen LESE- und SCHREIBBEFEHLE.

- `WRITE_SAME`

  Mit dieser Funktion wird ein Storage-Array entlastet, bei dem ein wiederholtes Muster – beispielsweise alle Nullen – geschrieben wird. Der ESX Host verwendet diese Funktion bei Vorgängen wie dem Füllen einer Datei ohne Füllen.

- `COMPARE_AND_WRITE`

  Diese Funktion umgeht bestimmte Grenzwerte für die Parallelität des Dateizugriffs, wodurch Vorgänge wie das Booten von Virtual Machines beschleunigt werden.

Anforderungen für die Nutzung der VAAI Umgebung

Die VAAI-Funktionen sind Teil des ESX-Betriebssystems und werden automatisch vom ESX-Host aufgerufen, wenn Sie die richtige Umgebung eingerichtet haben.

Die Umgebungsanforderungen lauten wie folgt:

- Der ESX Host muss ESX 4.1 oder höher ausführen.
- Das NetApp Storage-System, das den VMware-Datenspeicher hostet, muss ONTAP ausführen.
- (Nur beim Copy Offload) die Quelle und das Ziel des Kopiervorgangs von VMware müssen auf demselben Storage-System innerhalb desselben Clusters gehostet werden.

> Die Copy-Offload-Funktion unterstützt derzeit das Kopieren von Daten zwischen VMware Datenspeichern, die auf verschiedenen Storage-Systemen gehostet werden.

Ermitteln, ob VAAI Funktionen von ESX unterstützt werden

Um zu überprüfen, ob das ESX-Betriebssystem die VAAI-Funktionen unterstützt, können Sie den vSphere-Client prüfen oder andere Mittel zum Zugriff auf den Host verwenden. ONTAP unterstützt standardmäßig die SCSI-Befehle.

Sie können die erweiterten Einstellungen Ihres ESX Hosts überprüfen, um festzustellen, ob die VAAI-Funktionen aktiviert sind. Die Tabelle gibt an, welche SCSI-Befehle den ESX-Steuernamen entsprechen.

SCSI-Befehl	ESX Steuername (VAAI-Funktion)
EXTENDED_COPY	`HardwareAcceleratedMove`
SCHREIBSCHUTZ	`HardwareAcceleratedInit`
COMPARE_AND_WRITE	`HardwareAcceleratedLocking`

Microsoft Offloaded Data Transfer (ODX)

Microsoft Offloaded Data Transfer (ODX), auch bekannt als *Copy Offload*, ermöglicht direkte Datentransfers innerhalb eines Storage-Geräts oder zwischen kompatiblen Storage-Geräten, ohne die Daten über den Host-Computer zu übertragen.

ONTAP unterstützt ODX sowohl für die SMB- als auch für SAN-Protokolle.

Bei Dateiübertragungen ohne ODX werden die Daten von der Quelle gelesen und über das Netzwerk an den Host übertragen. Der Host überträgt die Daten zurück über das Netzwerk an das Ziel. Bei ODX-Dateiübertragung werden die Daten ohne Durchschreiten des Hosts direkt vom Quell- zum Ziel-Volume kopiert.

Da ausgelagerte ODX Kopien direkt zwischen Quelle und Ziel erstellt werden, ergeben sich deutliche Performance-Vorteile, wenn Kopien innerhalb desselben Volumes erstellt werden. Dies umfasst auch schnellere Kopierzeiten für gleiche Volume-Kopien, eine geringere CPU- und Arbeitsspeicherauslastung auf dem Client und eine geringere Netzwerk-I/O-Bandbreitenauslastung. Wenn die Kopien über Volumes verteilt sind, ergeben sich möglicherweise keine nennenswerten Performance-Steigerungen im Vergleich zu

hostbasierten Kopien.

Bei SAN-Umgebungen ist ODX nur verfügbar, wenn er sowohl vom Host als auch vom Storage-System unterstützt wird. Client-Computer, die ODX unterstützen und ODX-fähig sind, nutzen die verlagerte Dateiübertragung automatisch und transparent, wenn Dateien verschoben oder kopiert werden. ODX wird unabhängig davon verwendet, ob Sie Dateien per Drag-and-Drop über den Windows Explorer ziehen oder Befehle zur Befehlszeilendatei kopieren verwenden oder ob eine Client-Applikation Dateikopieanforderungen initiiert.

Anforderungen für die Nutzung von ODX

Wenn Sie Vorhaben, ODX für Copy-Offloaded zu verwenden, müssen Sie sich mit den Anforderungen an Volume-Support, Systemanforderungen und Softwarefunktionen vertraut machen.

Zur Nutzung von ODX ist bei Ihrem System Folgendes erforderlich:

- ONTAP

  ODX ist bei unterstützten Versionen von ONTAP automatisch aktiviert.

- Mindestquellenvolumen: 2 GB

  Für eine optimale Leistung sollte das Quellvolumen größer als 260 GB sein.

- ODX-Unterstützung auf dem Windows-Client

  ODX wird unter Windows Server 2012 oder höher und in Windows 8 oder höher unterstützt. Die Interoperabilitäts-Matrix enthält die neuesten Informationen zu unterstützten Windows-Clients.

  "NetApp Interoperabilitäts-Matrix-Tool"

- Applikationssupport für ODX

  Die Applikation, die den Datentransfer durchführt, muss ODX unterstützen. Zu den Applikationsprozessen, die ODX unterstützen, gehören unter anderem:

  - Management von Hyper-V, z. B. Erstellen und Konvertieren von virtuellen Festplatten (VHDs), Verwalten von Snapshot Kopien und Kopieren von Dateien zwischen Virtual Machines
  - Betrieb in Windows Explorer
  - Windows PowerShell Kopierbefehle
  - Befehle zum Kopieren von Windows-Befehlen die Microsoft TechNet-Bibliothek enthält weitere Informationen zu unterstützten ODX-Anwendungen auf Windows-Servern und -Clients.

- Bei Verwendung komprimierter Volumes muss die Größe der Komprimierungsgruppen 8 KB sein.

  Die Größe der Komprimierungsgruppen 32.000 wird nicht unterstützt.

ODX funktioniert nicht bei den folgenden Volume-Typen:

- Quellvolumen mit einer Kapazität von weniger als 2 GB
- Schreibgeschützte Volumes
- "FlexCache Volumes"

ODX wird auf FlexCache-Ursprungs-Volumes unterstützt.

- "Semi-Thick Provisioning Volumes"

Besondere Anforderungen an Systemdateien

Sie können ODX-Dateien, die in qtrees gefunden wurden, löschen. Andere ODX-Systemdateien dürfen nur entfernt oder geändert werden, wenn Ihnen der technische Support dazu aufgefordert wird.

Bei Nutzung der ODX Funktion liegen in jedem Volume des Systems ODX Systemdateien vor. Diese Dateien ermöglichen die zeitpunktgenaue Darstellung der bei der ODX-Übertragung verwendeten Daten. Die folgenden Systemdateien befinden sich auf der Root-Ebene jedes Volumes, das LUNs oder Dateien enthält, auf die Daten ausgelagert wurden:

- `.copy-offload` (Ein ausgeblendtes Verzeichnis)
- `.tokens` (Datei unter dem verborgenen `.copy-offload` Verzeichnis)

Sie können das verwenden `copy-offload delete-tokens -path dir_path -node` *`node_name`* Befehl zum Löschen eines qtree mit einer ODX-Datei

Anwendungsfälle für ODX

Bei der Verwendung von ODX auf SVMs sollten Sie sich die Anwendungsfälle bewusst sein, damit Sie unter den Umständen, unter denen ODX Ihnen Performance-Vorteile bietet, die Ergebnisse erkennen können.

Windows-Server und -Clients, die ODX unterstützen, nutzen den Copy-Offload als Standardfunktion zum Kopieren von Daten zwischen Remote-Servern. Wenn der Windows-Server oder -Client keine ODX oder eine ODX-Copy-Offload unterstützt, können der Kopier- oder Verladevorgang wieder auf herkömmliche Lese- und Schreibvorgänge für den Kopier- oder Verschiebevorgang zurückgreift.

In den folgenden Anwendungsfällen werden ODX Kopien und Verschiebungen unterstützt:

- Intra-Volume

  Die Quell- und Zieldateien oder LUNs befinden sich innerhalb desselben Volumes.

- Zwischen Volumes, demselben Node, gleiche SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen Volumes, verschiedenen Nodes, dieselbe SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen SVM, demselben Node

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Zwischen SVMs, unterschiedliche Nodes

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf

unterschiedlichen Nodes befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Cluster zwischen Clustern

  Die Quell- und Ziel-LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Nodes über die Cluster befinden. Dies wird nur für SAN unterstützt und funktioniert nicht für SMB.

Es gibt einige weitere spezielle Anwendungsfälle:

- Bei der ONTAP ODX Implementierung können mit ODX Dateien zwischen SMB-Freigaben und virtuellen FC- oder iSCSI-Attached-Laufwerken kopiert werden.

  Mit Windows Explorer, Windows CLI, PowerShell, Hyper-V oder anderen Applikationen, die ODX unterstützen, können Dateien durch eine nahtlose Verschiebung von ODX Kopien zwischen SMB-Freigaben und verbundenen LUNs kopiert oder verschoben werden, sofern sich SMB-Freigaben und LUNs im selben Cluster befinden.

- Hyper-V stellt weitere Anwendungsfälle für den ODX Copy-Offload zur Verfügung:

  - Mithilfe des ODX Copy-Offload-Pass-Through mit Hyper-V können Daten innerhalb oder zwischen VHD-Dateien (Virtual Hard Disk) kopiert oder Daten zwischen zugewiesenen SMB-Shares und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

    Damit können Kopien von Gastbetriebssystemen an den zugrunde liegenden Storage weitergegeben werden.

  - Bei der Erstellung von VHDs mit fester Größe wird ODX zur Initialisierung der Festplatte mit Nullen verwendet, wobei ein bekannter Token mit dem Namen „Zeroed“ verwendet wird.
  - Wenn sich der Quell- und Ziel-Storage auf demselben Cluster befindet, wird eine ODX Copy Offload für die Storage-Migration bei Virtual Machines eingesetzt.

> Um von den Anwendungsfällen für einen ODX Copy-Offload-Pass-Through mit Hyper-V zu profitieren, muss das Gastbetriebssystem ODX unterstützen. Und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die durch Storage (SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten auf dem Gastbetriebssystem unterstützen keine ODX-Pass-Through-Unterstützung.