Implementierungsrichtlinien und Best Practices für Storage

Enterprise applications

NetApp
May 03, 2024

Inhalt

Implementierungsrichtlinien und Best Practices für Storage . . . 1
- Überblick . . . 1
- NetApp Storage- und Windows Server-Umgebung . . . 2
- Bereitstellung in SAN-Umgebungen . . . 6
- Bereitstellung in SMB-Umgebungen . . . 15
- Hyper-V Storage-Infrastruktur auf NetApp . . . 18
- Storage-Effizienz . . . 29
- Sicherheit . . . 32
- Einsatz von Nano-Server . . . 32
- Implementieren des Hyper-V-Clusters . . . 36
- Bereitstellung von Hyper-V Live Migration in einer Cluster-Umgebung . . . 37
- Implementierung von Hyper-V Live Migration außerhalb einer Cluster-Umgebung . . . 38
- Bereitstellung von Hyper-V Storage Live Migration . . . 39
- Bereitstellung von Hyper-V Replica außerhalb einer Cluster-Umgebung . . . 40
- Bereitstellung von Hyper-V-Replikaten in einer Cluster-Umgebung . . . 42
- Wo Sie weitere Informationen finden . . . 43

Implementierungsrichtlinien und Best Practices für Storage

Überblick

Microsoft Windows Server ist ein Betriebssystem der Enterprise-Klasse, das Netzwerke, Sicherheit, Virtualisierung, Private Cloud, Hybrid Cloud, Virtual Desktop Infrastructure, Zugriffsschutz, Informationsschutz, Webservices, Anwendungsplattform Infrastruktur, und vieles mehr.

Diese Dokumentation ersetzt die zuvor veröffentlichten technischen Berichte *TR-4568: NetApp-Bereitstellungsrichtlinien und bewährte Speichermethoden für Windows Server*

Die NetApp ONTAP® Managementsoftware wird auf NetApp Storage-Controllern ausgeführt. Es ist in mehreren Formaten erhältlich.

- Eine Unified Architecture, die Datei-, Objekt- und Blockprotokolle unterstützt Auf diese Weise können die Storage-Controller sowohl als NAS- und SAN-Geräte als auch als Objektspeicher agieren
- Ein All-SAN-Array (ASA), das sich nur auf Blockprotokolle konzentriert und die I/O-Wiederaufnahme-Zeiten (IORT) optimiert, indem symmetrisches aktiv/aktiv-Multipathing für connect Hosts hinzugefügt wird
- Eine softwaredefinierte Unified Architecture
  - ONTAP Select auf VMware vSphere oder KVM
  - Cloud Volumes ONTAP wird als Cloud-native Instanz ausgeführt
- First-Party-Angebote von Hyperscale-Cloud-Providern
  - Amazon FSX für NetApp ONTAP
  - Azure NetApp Dateien
  - Google Cloud NetApp Volumes

ONTAP bietet NetApp Funktionen zur Steigerung der Storage-Effizienz, beispielsweise die NetApp Snapshot Technologie, Klonen, Deduplizierung, Thin Provisioning, Thin Replication, Komprimierung, Virtual Storage Tiering und vieles mehr mit verbesserter Performance und Effizienz.

Zusammen können Windows Server und ONTAP in großen Umgebungen betrieben werden und Datacenter-Konsolidierung und Private oder Hybrid Cloud-Implementierungen einen enormen Mehrwert bringen. Diese Kombination bietet auch effiziente unterbrechungsfreie Workloads und unterstützt nahtlose Skalierbarkeit.

Zielgruppe

Dieses Dokument richtet sich an System- und Storage-Architekten, die NetApp Storage-Lösungen für Windows Server entwerfen.

Wir gehen in diesem Dokument von folgenden Annahmen aus:

- Der Leser hat allgemeine Kenntnisse über NetApp Hardware- und Softwarelösungen. Siehe "Systemadministrationshandbuch für Clusteradministratoren" Entsprechende Details.
- Der Leser verfügt über allgemeine Kenntnisse zu Block-Zugriffsprotokollen wie iSCSI, FC und dem Dateizugriffsprotokoll SMB/CIFS. Siehe "Clustered Data ONTAP SAN-Management" Für SAN-bezogene

Informationen. Siehe "NAS-Management" Für CIFS/SMB-bezogene Informationen.

- Der Leser hat allgemeine Kenntnisse über das Betriebssystem Windows Server und Hyper-V.

Eine vollständige, regelmäßig aktualisierte Matrix getesteter und unterstützter SAN- und NAS-Konfigurationen finden Sie im "Interoperabilitäts-Matrix-Tool (IMT)" Auf der NetApp Support-Website. Mithilfe des IMT können Sie die genauen Produkt- und Funktionsversionen ermitteln, die für Ihre spezifische Umgebung unterstützt werden. NetApp IMT definiert die Produktkomponenten und -Versionen, die mit von NetApp unterstützten Konfigurationen kompatibel sind. Die dort angezeigten Ergebnisse basieren auf der spezifischen Infrastruktur des jeweiligen Kunden bzw. auf den technischen Daten der in dieser Infrastruktur enthaltenen Komponenten.

NetApp Storage- und Windows Server-Umgebung

Wie im erwähnt "Überblick", NetApp Storage Controller bieten eine echte Unified Architecture, die Datei-, Block- und Objektprotokolle unterstützt. Dazu zählen SMB/CIFS, NFS, NVMe/TCP, NVMe/FC, iSCSI FC (FCP) und S3 zugreifen. Sie erstellen außerdem einen einheitlichen Client- und Host-Zugriff. Derselbe Storage Controller kann gleichzeitig Block-Storage-Service in Form von SAN-LUNs und Fileservices wie NFS und SMB/CIFS bereitstellen. ONTAP ist auch als All-SAN-Array (ASA) verfügbar, das den Hostzugriff über symmetrisches aktiv/aktiv-Multipathing mit iSCSI und FCP optimiert, während die Unified ONTAP-Systeme asymmetrisches aktiv/aktiv-Multipathing verwenden. In beiden Modi verwendet ONTAP ANA für NVMe over Fabrics (NVMe-of) Multipath-Management.

Ein NetApp Storage Controller mit ONTAP Software kann die folgenden Workloads in einer Windows Serverumgebung unterstützen:

- VMs werden auf kontinuierlich verfügbaren SMB 3.0-Freigaben gehostet
- VMs, die auf LUNs für Cluster Shared Volume (CSV) gehostet werden und auf iSCSI oder FC ausgeführt werden
- SQL Server-Datenbanken auf SMB 3.0-Freigaben
- SQL Server-Datenbanken auf NVMe-of, iSCSI oder FC
- Anderen Applikations-Workloads

Darüber hinaus bietet NetApp Storage-Effizienzfunktionen wie Deduplizierung, NetApp FlexClone Kopien, NetApp Snapshot Technologie, Thin Provisioning, Komprimierung, Storage Tiering kommt bei Workloads, die auf Windows Server ausgeführt werden, erheblichen Nutzen aus.

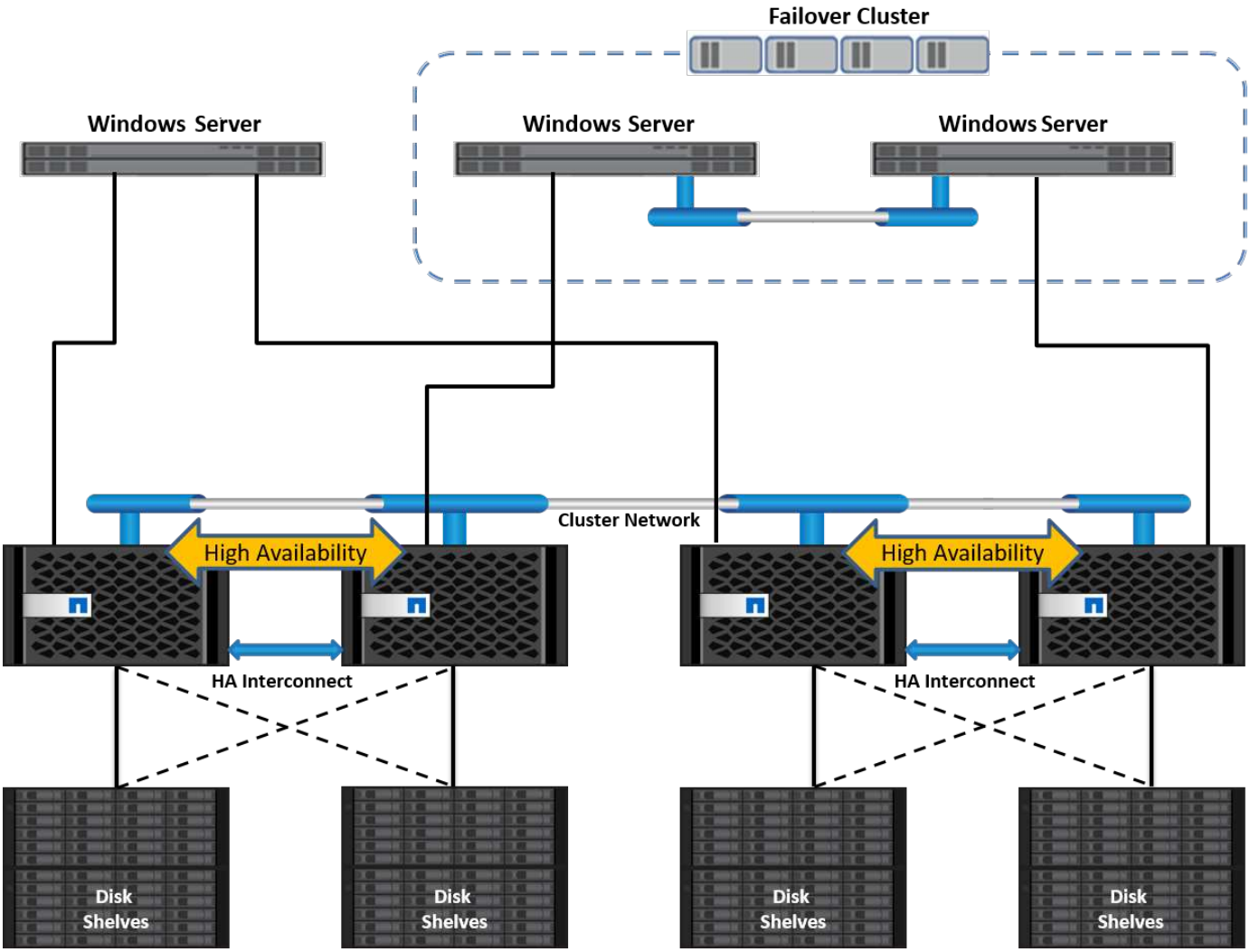
ONTAP Datenmanagement

ONTAP ist eine Management-Software, die auf einem NetApp Storage Controller ausgeführt wird. Ein als Node bezeichnet NetApp Storage Controller ist ein Hardwaregerät mit Prozessor, RAM und NVRAM. Der Node kann mit SATA-, SAS- oder SSD-Festplattenlaufwerken oder einer Kombination dieser Laufwerke verbunden werden.

Mehrere Nodes werden in einem Cluster-System zusammengefasst. Die Nodes im Cluster kommunizieren kontinuierlich mit einander, um Cluster-Aktivitäten zu koordinieren. Außerdem können die Nodes Daten transparent von Nodes zu Nodes verschieben. Hierzu werden redundante Pfade zu einem dedizierten Cluster-Netzwerk mit zwei 10-Gbit-Ethernet-Switches verwendet. Die Nodes im Cluster können sich gegenseitig übernehmen, um in jedem Failover-Fall für Hochverfügbarkeit zu sorgen. Cluster werden über einen vollständigen Cluster statt pro Node verwaltet. Die Daten werden von einer oder mehreren Storage Virtual Machines (SVMs) bereitgestellt. Ein Cluster muss über mindestens eine SVM verfügen, um Daten

bereitzustellen.

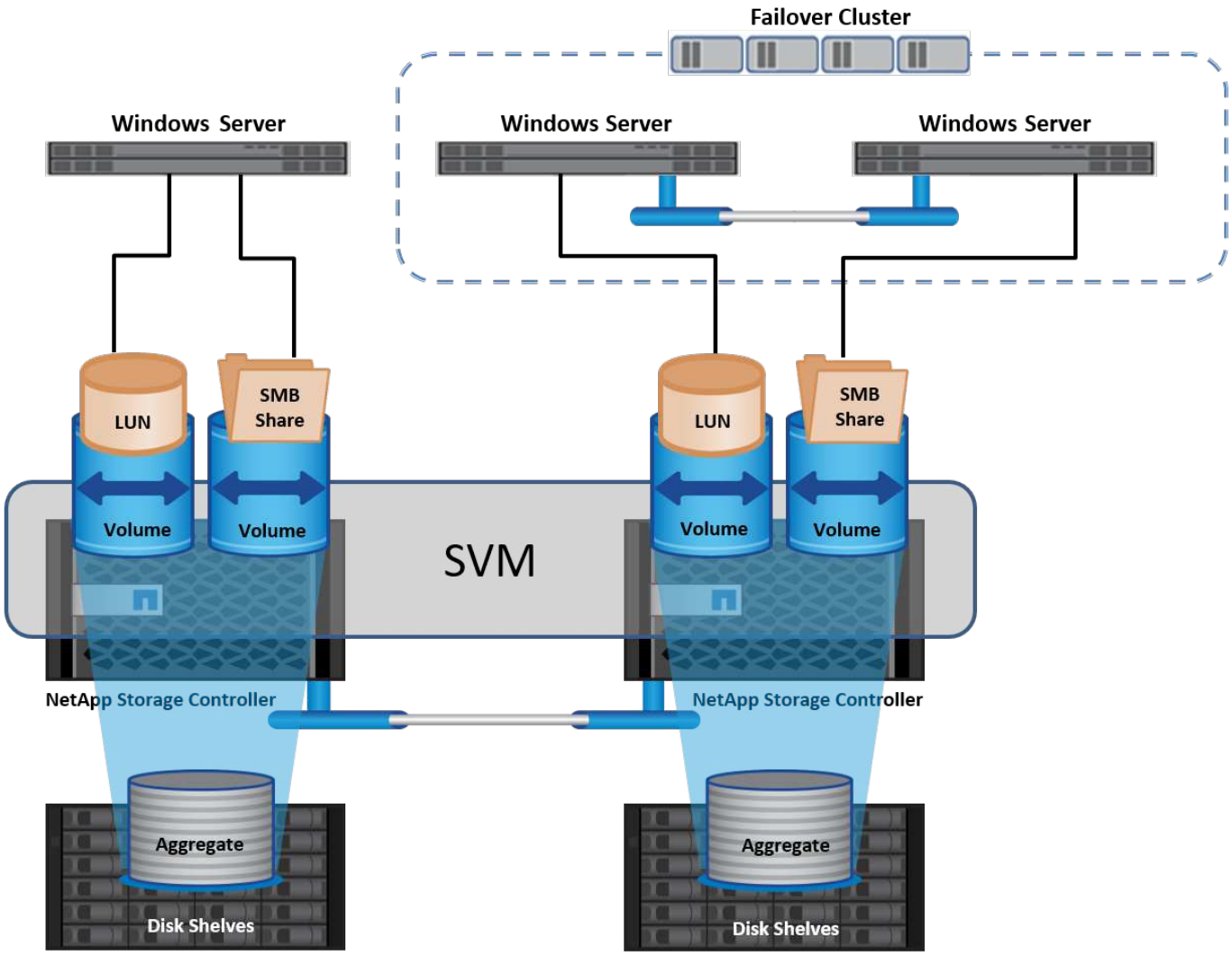
Die Basiseinheit eines Clusters ist der Node, und die Nodes werden dem Cluster als Teil eines Hochverfügbarkeitspaars (HA) hinzugefügt. HA-Paare ermöglichen Hochverfügbarkeit durch Kommunikation untereinander über einen HA Interconnect (getrennt vom dedizierten Cluster-Netzwerk) und durch Beibehalten redundanter Verbindungen zu den Festplatten des HA-Paars. Festplatten werden nicht von HA-Paaren gemeinsam genutzt, obwohl Shelfs Festplatten enthalten können, die zu einem der beiden Mitglieder eines HA-Paars gehören. Die folgende Abbildung zeigt die Bereitstellung von NetApp Storage in einer Windows Server-Umgebung.



Storage Virtual Machines

Eine ONTAP SVM ist ein logischer Storage-Server, der den Datenzugriff auf LUNs und/oder einen NAS-Namespace über eine oder mehrere logische Schnittstellen (LIFs) ermöglicht. Damit ist die SVM die grundlegende Einheit der Storage-Segmentierung, die eine sichere Mandantenfähigkeit in ONTAP ermöglicht. Jede SVM ist so konfiguriert, eigene Storage Volumes zu besitzen, die über ein physisches Aggregat bereitgestellt werden, und logische Schnittstellen (LIFs), die einem physischen Ethernet-Netzwerk oder FC-Zielports zugewiesen sind.

Logische Festplatten (LUNs) oder CIFS Shares werden innerhalb der Volumes einer SVM erstellt und Windows Hosts und Clustern zugeordnet, um ihnen Speicherplatz zur Verfügung zu stellen, wie in der folgenden Abbildung dargestellt. SVMs sind Node-unabhängig und Cluster-basiert. Sie können physische Ressourcen wie Volumes oder Netzwerk-Ports im gesamten Cluster verwenden.



Bereitstellung von NetApp Storage für Windows Server

In SAN- und NAS-Umgebungen kann Windows Server Storage bereitstellen. In einer SAN-Umgebung wird der Storage als Disks von LUNs auf einem NetApp-Volume als Block-Storage zur Verfügung gestellt. In einer NAS-Umgebung wird der Storage als CIFS/SMB-Freigaben auf NetApp Volumes als File-Storage bereitgestellt. Diese Laufwerke und Freigaben können in Windows Server wie folgt angewendet werden:

- Storage für Windows Server-Hosts für Applikations-Workloads
- Speicher für Nano Server und Container
- Storage für einzelne Hyper-V Hosts zum Speichern von VMs
- Shared Storage für Hyper-V Cluster in Form von CSVs zum Speichern von VMs
- Storage für SQL Server-Datenbanken

Managen von NetApp Storage

Verwenden Sie eine der folgenden Methoden, um NetApp-Speicher von Windows Server 2016 aus zu verbinden, zu konfigurieren und zu verwalten:

- **Secure Shell (SSH).** Verwenden Sie einen beliebigen SSH-Client auf dem Windows-Server, um NetApp-CLI-Befehle auszuführen.

- **System Manager.** Dies ist das GUI-basierte Manageability-Produkt von NetApp.
- **NetApp PowerShell Toolkit.** Dies ist das NetApp PowerShell Toolkit zur Automatisierung und Implementierung von benutzerdefinierten Skripts und Workflows.

NetApp PowerShell Toolkit

Das NetApp PowerShell Toolkit (PSTK) ist ein PowerShell Modul, das eine End-to-End-Automatisierung bietet und die Storage-Administration von NetApp ONTAP ermöglicht. Das ONTAP Modul enthält über 2,000 Cmdlets und unterstützt Sie bei der Administration von FAS, NetApp All Flash FAS (AFF), Standard-Hardware und Cloud-Ressourcen.

Dinge, die Sie sich merken sollten

- NetApp unterstützt keine Storage Spaces im Windows Server. Storage Spaces werden nur für JBOD verwendet (nur ein paar Disks) und funktionieren nicht mit irgendeiner Art von RAID (Direct-Attached Storage [das] oder SAN).
- Cluster-Speicherpools in Windows Server werden von ONTAP nicht unterstützt.
- NetApp unterstützt das gemeinsam genutzte Virtual Hard Disk Format (VHDX) für Gastclustering in Windows SAN-Umgebungen.
- Windows Server unterstützt nicht das Erstellen von Speicherpools mit iSCSI- oder FC-LUNs.

Weitere Informationen

- Weitere Informationen zum NetApp PowerShell Toolkit finden Sie im "NetApp Support Website".
- Informationen zu Best Practices für das NetApp PowerShell Toolkit finden Sie unter "TR-4475: Best Practices-Leitfaden für das NetApp PowerShell Toolkit".

Best Practices für die Netzwerkumgebung

Ethernet-Netzwerke können in die folgenden Gruppen unterteilt werden:

- Ein Client-Netzwerk für die VMs
- Noch ein Storage-Netzwerk (iSCSI oder SMB, das mit den Storage-Systemen verbunden ist)
- Ein Cluster-Kommunikationsnetzwerk (Heartbeat und andere Kommunikation zwischen den Nodes des Clusters)
- Ein Managementnetzwerk (zur Überwachung und Fehlerbehebung des Systems)
- Ein Migrationsnetzwerk (für Host-Live-Migration)
- VM-Replizierung (ein Hyper-V Replikat)

Best Practices in sich vereint

- NetApp empfiehlt für jede der oben genannten Funktionen dedizierte physische Ports zur Netzwerkisolierung und zur Performance.
- Für jede der oben genannten Netzwerkanforderungen (mit Ausnahme der Speicheranforderungen) können mehrere physische Netzwerkports aggregiert werden, um die Last zu verteilen oder eine Fehlertoleranz bereitzustellen.
- NetApp empfiehlt die Erstellung eines dedizierten virtuellen Switches auf dem Hyper-V Host für die Verbindung zum Gast-Storage innerhalb der VM.

- Stellen Sie sicher, dass die Hyper-V-Host- und iSCSI-Datenpfade verschiedene physische Ports und virtuelle Switches zur sicheren Isolation zwischen dem Gast und dem Host verwenden.
- NetApp empfiehlt, NIC-Teaming für iSCSI-NICs zu vermeiden.
- NetApp empfiehlt die Verwendung von ONTAP Multipath Input/Output (MPIO), der auf dem Host für Storage-Zwecke konfiguriert ist.
- NetApp empfiehlt die Verwendung von MPIO innerhalb einer Gast-VM, wenn Sie iSCSI-Gastinitiatoren verwenden. Die MPIO-Verwendung im Gastsystem muss vermieden werden, wenn Sie Pass-Through-Festplatten verwenden. In diesem Fall sollte die Installation von MPIO auf dem Host ausreichen.
- NetApp empfiehlt, keine QoS-Richtlinien auf den virtuellen Switch anzuwenden, der dem Storage-Netzwerk zugewiesen ist.
- NetApp empfiehlt, keine automatische private IP-Adressierung (APIPA) auf physischen NICs zu verwenden, da APIPA nicht routingfähig ist und nicht im DNS registriert ist.
- NetApp empfiehlt die Aktivierung von Jumbo Frames für CSV-, iSCSI- und Live-Migrationsnetzwerke, um den Durchsatz zu erhöhen und CPU-Zyklen zu reduzieren.
- NetApp empfiehlt, die Option Management Operating System zur Freigabe dieses Netzwerkadapters für den virtuellen Hyper-V-Switch deaktivieren, um ein dediziertes Netzwerk für die VMs zu erstellen.
- NetApp empfiehlt die Erstellung redundanter Netzwerkpfade (mehrere Switches) für die Live-Migration und das iSCSI-Netzwerk, um Ausfallsicherheit und QoS zu gewährleisten.

Bereitstellung in SAN-Umgebungen

ONTAP SVMs unterstützen die Blockprotokolle iSCSI und FC. Wenn eine SVM mit dem Blockprotokoll iSCSI oder FC erstellt wird, erhält die SVM entweder einen iSCSI Qualified Name (IQN) oder einen FC Worldwide Name (WWN). Diese Kennung stellt Hosts, die auf den NetApp-Block-Storage zugreifen, ein SCSI-Ziel dar.

Bereitstellung von NetApp-LUNs auf Windows Server

Voraussetzungen

Der Einsatz von NetApp Storage in SAN-Umgebungen in Windows Server hat folgende Anforderungen:

- Ein NetApp Cluster ist mit einem oder mehreren NetApp Storage Controllern konfiguriert.
- Der NetApp-Cluster oder die Storage-Controller verfügen über eine gültige iSCSI-Lizenz.
- Es sind iSCSI- und/oder FC-konfigurierte Ports verfügbar.
- FC-Zoning wird auf einem FC-Switch für FC durchgeführt.
- Mindestens ein Aggregat wird erstellt.
- Eine SVM sollte über eine LIF pro Ethernet-Netzwerk oder Fibre Channel Fabric auf jedem Storage Controller verfügen, der Daten über iSCSI oder Fibre Channel bereitstellen soll.

Einsatz

1. Erstellen einer neuen SVM mit aktivierter Blockprotokoll-iSCSI und/oder FC Eine neue SVM kann mit einer der folgenden Methoden erstellt werden:
    - CLI-Befehle auf NetApp Storage

    - ONTAP System Manager
    - NetApp PowerShell Toolkit
2. Konfigurieren Sie das iSCSI- und/oder FC-Protokoll.
3. Zuweisung der SVM mit LIFs auf jedem Cluster-Node
4. Starten Sie den iSCSI- und/oder FC-Service auf der SVM.

    .

5. Erstellen Sie iSCSI- und/oder FC-Port-Sets mit den SVM LIFs.
6. Erstellen Sie eine iSCSI- und/oder FC-Initiatorgruppe für Windows mithilfe des erstellten Portgruppe.
7. Fügen Sie der Initiatorgruppe einen Initiator hinzu. Der Initiator ist der IQN für iSCSI und der WWPN für FC. Sie können von Windows Server abgefragt werden, indem das PowerShell Cmdlet Get-InitiatorPort ausgeführt wird.

```
# Get the IQN for iSCSI
Get-InitiatorPort | Where \{$_.ConnectionType -eq 'iSCSI'} | Select-
Object -Property NodeAddress
```

```
# Get the WWPN for FC
Get-InitiatorPort | Where \{$_.ConnectionType -eq 'Fibre Channel'} |
Select-Object -Property PortAddress
```

```
# While adding initiator to the initiator group in case of FC, make sure
to provide the initiator(PortAddress) in the standard WWPN format
```

Der IQN für iSCSI auf Windows Server kann auch in der Konfiguration der iSCSI-Initiator-Eigenschaften geprüft werden.

- Erstellen Sie eine LUN mit dem Assistenten zum Erstellen einer LUN und verknüpfen Sie sie mit der erstellten Initiatorgruppe.

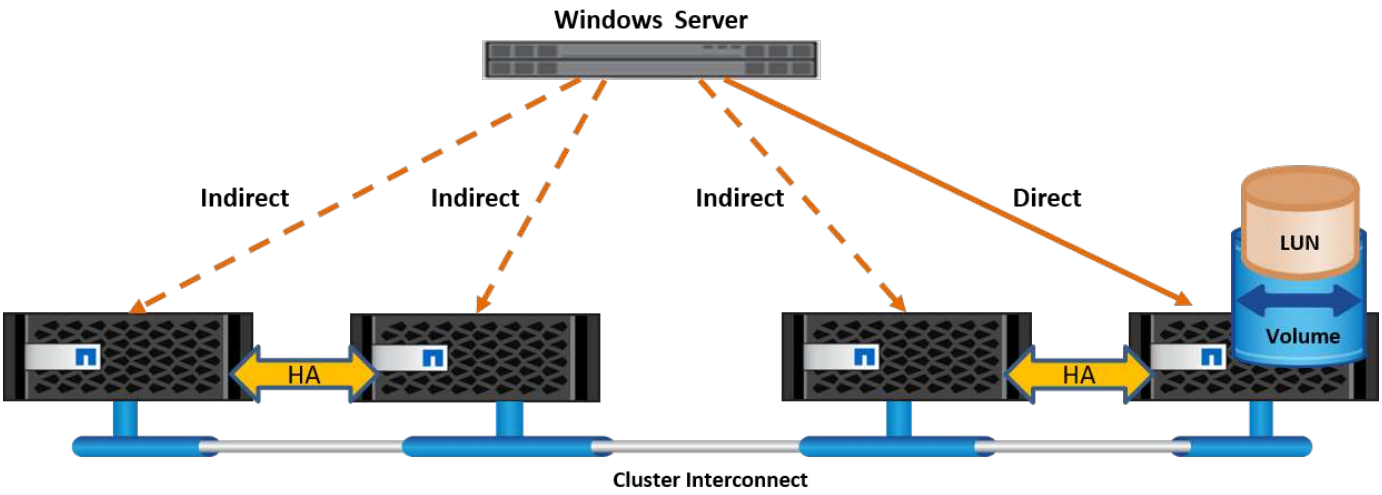
Host-Integration

Windows Server verwendet Asymmetrical Logical Unit Access (ALUA) Extension MPIO, um direkte und indirekte Pfade zu LUNs zu ermitteln. Obwohl jede LIF, die einer SVM gehört, Lese-/Schreibanforderungen für ihre LUNs akzeptiert, sind tatsächlich nur einer der Cluster-Nodes Eigentümer der Festplatten, die diese LUN zu einem beliebigen Zeitpunkt sichern. Dadurch werden die verfügbaren Pfade zu einer LUN in zwei Typen unterteilt, direkt oder indirekt, wie in der folgenden Abbildung dargestellt.

Ein direkter Pfad für eine LUN ist ein Pfad, auf dem sich die LIFs einer SVM und die LUN, auf die zugegriffen wird, auf demselben Node befinden. Um von einem physischen Ziel-Port zur Festplatte zu wechseln, muss das Cluster-Netzwerk nicht durchlaufen werden.

Bei den indirekten Pfaden handelt es sich um Datenpfade, auf denen sich die LIFs einer SVM und die aufgerufene LUN auf unterschiedlichen Nodes befinden. Um von einem physischen Ziel-Port auf die Festplatte

zu gelangen, müssen Daten das Cluster-Netzwerk durchlaufen.



MPIO

NetApp ONTAP bieten hochverfügbaren Storage, bei dem mehrere Pfade vom Storage Controller zum Windows Server existieren können. Multipathing ist die Fähigkeit, mehrere Datenpfade von einem Server zu einem Storage-Array zu haben. Multipathing schützt vor Hardware-Ausfällen (Kabelschnitte, Switch- und Host Bus Adapter- [HBA]-Ausfall usw.) und kann durch die Verwendung der aggregierten Performance mehrerer Verbindungen höhere Performance-Grenzwerte bieten. Wenn ein Pfad oder eine Verbindung nicht mehr verfügbar ist, verschiebt die Multipathing-Software die Last automatisch auf einen der anderen verfügbaren Pfade. Die MPIO-Funktion kombiniert mehrere physische Pfade zum Storage als einen einzigen logischen Pfad, der für den Datenzugriff verwendet wird, um Storage Resiliency und Load Balancing zu ermöglichen. Um diese Funktion verwenden zu können, muss die MPIO-Funktion auf Windows Server aktiviert sein.

Aktivieren Sie MPIO

Führen Sie die folgenden Schritte aus, um MPIO auf Windows Server zu aktivieren:

1. Melden Sie sich bei Windows Server als Mitglied der Administratorgruppe an.
2. Starten Sie Server Manager.
3. Klicken Sie im Abschnitt Verwalten auf Rollen und Funktionen hinzufügen.
4. Wählen Sie auf der Seite Funktionen auswählen die Option Multipath-E/A aus

Konfigurieren Sie MPIO

Wenn Sie das iSCSI-Protokoll verwenden, müssen Sie Windows Server anweisen, Multipath-Unterstützung auf iSCSI-Geräte in den MPIO-Eigenschaften anzuwenden.

Führen Sie die folgenden Schritte aus, um MPIO auf Windows Server zu konfigurieren:

1. Melden Sie sich bei Windows Server als Mitglied der Administratorgruppe an.
2. Starten Sie Server Manager.
3. Klicken Sie im Abschnitt Extras auf MPIO.
4. Wählen Sie unter MPIO-Eigenschaften auf Mehrpfade ermitteln die Option Support für iSCSI-Geräte hinzufügen aus, und klicken Sie auf Hinzufügen. Sie werden anschließend aufgefordert, den Computer neu zu starten.

5. Starten Sie Windows Server neu, um das MPIO-Gerät im Abschnitt MPIO-Geräte der MPIO-Eigenschaften anzuzeigen.

Konfigurieren Sie iSCSI

Führen Sie die folgenden Schritte aus, um iSCSI-Blockspeicher auf Windows Server zu erkennen:

1. Melden Sie sich bei Windows Server als Mitglied der Administratorgruppe an.
2. Starten Sie Server Manager.
3. Klicken Sie im Abschnitt Extras auf iSCSI-Initiator.
4. Klicken Sie auf der Registerkarte Ermittlung auf Portal ermitteln.
5. Geben Sie die IP-Adresse der LIFs für die SVM an, die für das NetApp-Storage-Protokoll für SAN erstellt wurden. Klicken Sie auf Erweitert, konfigurieren Sie die Informationen auf der Registerkarte Allgemein, und klicken Sie auf OK.
6. Der iSCSI-Initiator erkennt das iSCSI-Ziel automatisch und listet es auf der Registerkarte Ziele auf.
7. Wählen Sie das iSCSI-Ziel unter ermittelte Ziele aus. Klicken Sie auf Verbinden, um das Fenster mit Ziel verbinden zu öffnen.
8. Sie müssen mehrere Sitzungen vom Windows Server-Host zu den Ziel-iSCSI-LIFs auf dem NetApp-Storage-Cluster erstellen. Um das zu tun, führen Sie folgende Schritte aus:
9. Wählen Sie im Fenster mit Ziel verbinden die Option MPIO aktivieren aus, und klicken Sie auf Erweitert.
10. Wählen Sie unter Erweiterte Einstellungen auf der Registerkarte Allgemein den lokalen Adapter als Microsoft iSCSI-Initiator aus und wählen Sie Initiator-IP und Zielportal-IP aus.
11. Sie müssen auch über den zweiten Pfad eine Verbindung herstellen. Wiederholen Sie daher Schritt 5 bis Schritt 8, wählen Sie jedoch dieses Mal die Initiator-IP und die Ziel-Portal-IP für den zweiten Pfad aus.
12. Wählen Sie das iSCSI-Ziel im Hauptfenster iSCSI-Eigenschaften unter ermittelte Ziele aus, und klicken Sie auf Eigenschaften.
13. Das Fenster Eigenschaften zeigt an, dass mehrere Sitzungen erkannt wurden. Wählen Sie die Sitzung aus, klicken Sie auf Geräte, und klicken Sie dann auf MPIO, um die Load-Balancing-Richtlinie zu konfigurieren. Alle für das Gerät konfigurierten Pfade werden angezeigt und alle Load-Balancing-Richtlinien werden unterstützt. NetApp empfiehlt im Allgemeinen Round Robin mit Teilmenge. Diese Einstellung ist der Standard für Arrays mit aktiviertem ALUA. Round Robin ist der Standard für aktiv-aktiv-Arrays, die ALUA nicht unterstützen.

Block-Storage erkennen

Führen Sie die folgenden Schritte aus, um iSCSI- oder FC-Blockspeicher auf Windows Server zu erkennen:

1. Klicken Sie im Abschnitt Extras des Server-Managers auf Computerverwaltung.
2. Klicken Sie in der Computerverwaltung im Abschnitt Speicherverwaltung auf Datenträgerverwaltung, und klicken Sie dann auf Weitere Aktionen und Datenträger erneut scannen. Dadurch werden die RAW-iSCSI-LUNs angezeigt.
3. Klicken Sie auf die ermittelte LUN, und stellen Sie sie online. Wählen Sie anschließend Datenträger mit der MBR- oder GPT-Partition initialisieren aus. Erstellen Sie ein neues einfaches Volume, indem Sie die Volume-Größe und den Laufwerksbuchstaben angeben und es mit FAT, FAT32, NTFS oder dem Resilient File System (ReFS) formatieren.

Best Practices in sich vereint

- NetApp empfiehlt die Aktivierung von Thin Provisioning auf den Volumes, auf denen die LUNs gehostet werden.
- Um Multipathing-Probleme zu vermeiden, empfiehlt NetApp, entweder alle 10-GB-Sitzungen oder alle 1-GB-Sitzungen für eine bestimmte LUN zu verwenden.
- NetApp empfiehlt, dass Sie bestätigen, dass ALUA auf dem Storage-System aktiviert ist. ALUA ist auf ONTAP standardmäßig aktiviert.
- Aktivieren Sie auf dem Windows-Server-Host, dem die NetApp-LUN zugeordnet ist, iSCSI-Dienst (TCP-in) für Inbound- und iSCSI-Dienst (TCP-out) für Outbound in den Firewall-Einstellungen. Mit diesen Einstellungen kann iSCSI-Datenverkehr zum und vom Hyper-V-Host und NetApp-Controller geleitet werden.

Bereitstellung von NetApp-LUNs auf dem Nano Server

Voraussetzungen

Zusätzlich zu den im vorherigen Abschnitt genannten Voraussetzungen muss die Speicherrolle von der Nano-Server-Seite aus aktiviert werden. Beispielsweise muss Nano Server mit der Option -Storage bereitgestellt werden. Informationen zum Bereitstellen von Nano Server finden Sie im Abschnitt „"Stellen Sie Nano Server Bereit."„

Einsatz

Gehen Sie wie folgt vor, um NetApp-LUNs auf einem Nano-Server bereitzustellen:

1. Stellen Sie eine Remote-Verbindung zum Nano Server her, indem Sie die Anweisungen im Abschnitt „"Verbindung mit Nano Server herstellen"."
2. Führen Sie zum Konfigurieren von iSCSI die folgenden PowerShell-Cmdlets auf dem Nano Server aus:

```
# Start iSCSI service, if it is not already running
Start-Service msiscsi
```

```
# Create a new iSCSI target portal
New-IscsiTargetPortal â€"TargetPortalAddress <SVM LIF>
```

```
# View the available iSCSI targets and their node address
Get-IscsiTarget
```

```
# Connect to iSCSI target
Connect-IscsiTarget -NodeAddress <NodeAddress>
```

```
# NodeAddress is retrived in above cmdlet Get-IscsiTarget
# OR
Get-IscsiTarget | Connect-IscsiTarget
```

```
# View the established iSCSI session
Get-IscsiSession
```

```
# Note the InitiatorNodeAddress retrieved in the above cmdlet Get-
IscsiSession. This is the IQN for Nano server and this needs to be added
in the Initiator group on NetApp Storage
```

```
# Rescan the disks
Update-HostStorageCache
```

3. Fügen Sie der Initiatorgruppe einen Initiator hinzu.

```
Add the InitiatorNodeAddress retrieved from the cmdlet Get-IscsiSession
to the Initiator Group on NetApp Controller
```

4. Konfigurieren Sie MPIO.

```
# Enable MPIO Feature
Enable-WindowsOptionalFeature -Online -FeatureName MultipathIo
```

```
# Get the Network adapters and their IPs
Get-NetIPAddress â€"AddressFamily IPv4 â€"PrefixOrigin <Dhcp or Manual>
```

```
# Create one MPIO-enabled iSCSI connection per network adapter
Connect-IscsiTarget -NodeAddress <NodeAddress> -IsPersistent $True â
€"IsMultipathEnabled $True â€"InitiatorPortalAddress <IP Address of
ethernet adapter>
```

```
# NodeAddress is retrieved from the cmdlet Get-IscsiTarget
# IPs are retrieved in above cmdlet Get-NetIPAddress
```

```
# View the connections
Get-IscsiConnection
```

5. Block-Storage erkennen

```
# Rescan disks
Update-HostStorageCache
```

```
# Get details of disks
Get-Disk
```

```
# Initialize disk
Initialize-Disk -Number <DiskNumber> -PartitionStyle <GPT or MBR>
```

```
# DiskNumber is retrived in the above cmdlet Get-Disk
# Bring the disk online
Set-Disk -Number <DiskNumber> -IsOffline $false
```

```
# Create a volume with maximum size and default drive letter
New-Partition -DiskNumber <DiskNumber> -UseMaximumSize
-AssignDriveLetter
```

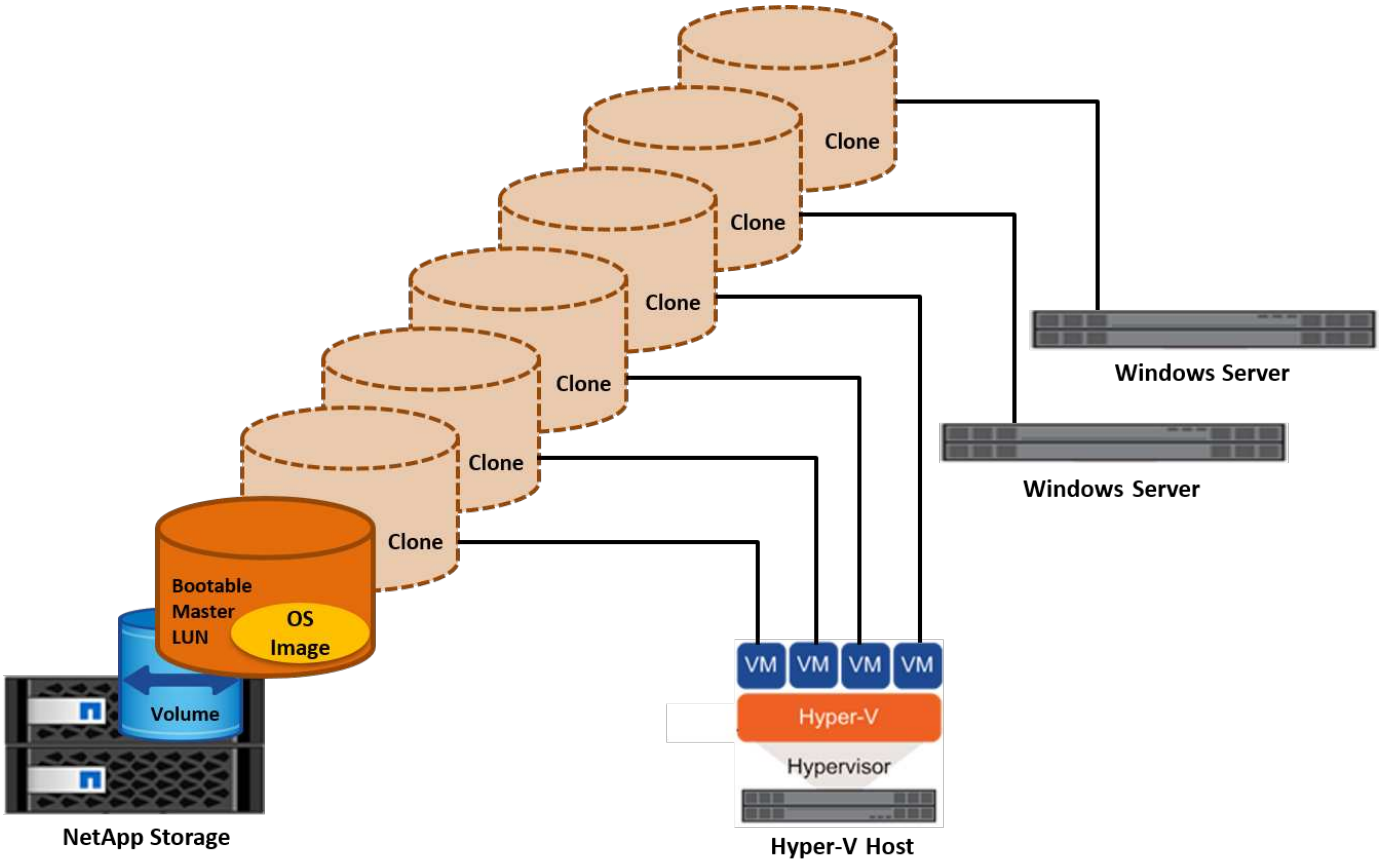
```
# To choose the size and drive letter use -Size and -DriveLetter
parameters
# Format the volume
Format-Volume -DriveLetter <DriveLetter> -FileSystem <FAT32 or NTFS or
REFS>
```

Booten über das SAN

Ein physischer Host (Server) oder eine Hyper-V-VM kann das Windows-Serverbetriebssystem direkt von einer NetApp-LUN starten, anstatt von der internen Festplatte. Beim Ansatz „vom SAN booten“ befindet sich das BS-Image, von dem aus gebootet werden soll, auf einer NetApp-LUN, die mit einem physischen Host oder einer physischen VM verbunden ist. Bei einem physischen Host ist der HBA des physischen Hosts so konfiguriert, dass er die NetApp-LUN zum Booten verwendet. Bei einer VM wird die NetApp-LUN zum Booten als Pass-Through-Disk angehängt.

NetApp FlexClone

Mithilfe der NetApp FlexClone Technologie können Boot-LUNs mit einem Betriebssystem-Image sofort geklont und mit den Servern und VMs verbunden werden, um schnell saubere Betriebssystem-Images zu liefern, wie in der folgenden Abbildung dargestellt.



Booten vom SAN für physischen Host

Voraussetzungen

- Der physische Host (Server) verfügt über einen geeigneten iSCSI- oder FC-HBA.
- Sie haben einen geeigneten HBA-Gerätetreiber für den Server heruntergeladen, der Windows Server unterstützt.
- Der Server verfügt über ein geeignetes CD/DVD-Laufwerk oder ein virtuelles Medium zum Einlegen des Windows Server-ISO-Images, und der HBA-Gerätetreiber wurde heruntergeladen.
- Eine NetApp iSCSI- oder FC-LUN wird auf dem NetApp Storage Controller bereitgestellt.

Einsatz

So konfigurieren Sie das Booten von SAN für einen physischen Host:

1. Aktivieren Sie BootBIOS auf dem Server-HBA.
2. Konfigurieren Sie für iSCSI-HBAs die Initiator-IP, den iSCSI-Knotennamen und den Adapter-Startmodus in den Boot-BIOS-Einstellungen.
3. Wenn Sie auf einem NetApp Storage Controller eine Initiatorgruppe für iSCSI und/oder FC erstellen, fügen Sie der Gruppe den Server-HBA-Initiator hinzu. Der HBA-Initiator des Servers ist der WWPN für den FC-

HBA oder den iSCSI-Knotennamen für iSCSI-HBA.

4. Erstellen Sie eine LUN auf dem NetApp Storage Controller mit der LUN-ID 0 und verknüpfen Sie sie mit der Initiatorgruppe, die im vorherigen Schritt erstellt wurde. Diese LUN dient als Boot-LUN.
5. Beschränken Sie den HBA auf einen einzelnen Pfad zur Boot-LUN. Nach der Installation von Windows Server auf der Boot-LUN können zusätzliche Pfade hinzugefügt werden, um die Multipathing-Funktion auszunutzen.
6. Konfigurieren Sie die LUN mithilfe des HBA-BootBIOS-Dienstprogramms als Startgerät.
7. Starten Sie den Host neu, und rufen Sie das Host-BIOS-Dienstprogramm auf.
8. Konfigurieren Sie das Host-BIOS so, dass die Start-LUN zum ersten Gerät in der Startreihenfolge wird.
9. Starten Sie über die Windows Server-ISO die Installation.
10. Wenn die Installation fragt: „Wo möchten Sie Windows installieren?“, klicken Sie unten im Installationsbildschirm auf Treiber laden, um die Seite Treiber für Installation auswählen zu starten. Geben Sie den Pfad des zuvor heruntergeladenen HBA-Gerätetreibers an, und beenden Sie die Installation des Treibers.
11. Nun muss die zuvor erstellte Boot-LUN auf der Windows-Installationsseite sichtbar sein. Wählen Sie die Start-LUN für die Installation von Windows Server auf der Boot-LUN aus, und beenden Sie die Installation.

Starten Sie von SAN für die virtuelle Maschine

Gehen Sie wie folgt vor, um das Booten über das SAN für eine VM zu konfigurieren:

Einsatz

1. Wenn Sie eine Initiatorgruppe für iSCSI oder FC auf einem NetApp-Speichercontroller erstellen, fügen Sie dem Controller den IQN für iSCSI oder den WWN für FC des Hyper-V-Servers hinzu.
2. Erstellen Sie LUNs oder LUN-Klone auf dem NetApp Storage Controller und verknüpfen Sie sie mit der Initiatorgruppe, die im vorherigen Schritt erstellt wurde. Diese LUNs dienen als Boot-LUNs für die VMs.
3. Erkennen Sie die LUNs auf dem Hyper-V-Server, schalten Sie sie online und initialisieren Sie sie.
4. Versetzen Sie die LUNs in den Offline-Modus.
5. Erstellen Sie VMs mit der Option Virtuelle Festplatte später anhängen auf der Seite Virtuelle Festplatte verbinden.
6. Fügen Sie eine LUN als Pass-Through-Disk zu einer VM hinzu.
   a. Öffnen Sie die VM-Einstellungen.
   b. Klicken Sie auf IDE-Controller 0, wählen Sie Festplatte aus, und klicken Sie auf Hinzufügen. Wenn Sie IDE Controller 0 auswählen, ist diese Festplatte das erste Startgerät für die VM.
   c. Wählen Sie in den Festplattenoptionen physische Festplatte aus, und wählen Sie eine Festplatte aus der Liste als Pass-Through-Disk aus. Bei den Festplatten handelt es sich um die in den vorherigen Schritten konfigurierten LUNs.
7. Installieren Sie Windows Server auf dem Pass-Through-Datenträger.

Best Practices in sich vereint

- Stellen Sie sicher, dass die LUNs offline sind. Andernfalls kann die Festplatte nicht als Pass-Through-Disk zu einer VM hinzugefügt werden.
- Wenn mehrere LUNs vorhanden sind, achten Sie darauf, die Datenträgernummer der LUN in der Datenträgerverwaltung zu notieren. Dies ist notwendig, da für die VM aufgeführte Festplatten mit der

Festplattennummer aufgeführt werden. Außerdem basiert die Auswahl der Festplatte als Pass-Through-Disk für die VM auf dieser Plattennummer.

- NetApp empfiehlt, NIC-Teaming für iSCSI-NICs zu vermeiden.
- NetApp empfiehlt die Verwendung von ONTAP MPIO, das auf dem Host für Storage-Zwecke konfiguriert ist.

Bereitstellung in SMB-Umgebungen

ONTAP bietet unter Verwendung des SMB3-Protokolls einen stabilen und hochperformanten NAS Storage für Hyper-V Virtual Machines.

Wenn eine SVM mit dem CIFS-Protokoll erstellt wird, wird ein CIFS-Server auf der SVM ausgeführt, die Teil der Windows Active Directory Domain ist. SMB-Freigaben können für ein Home Directory verwendet und Hyper-V und SQL Server Workloads hosten. Die folgenden Funktionen von SMB 3.0 werden in ONTAP unterstützt:

- Persistente Handles (kontinuierlich verfügbare Dateifreigaben)
- Witness-Protokoll
- Cluster-Client-Failover
- Erkennung von horizontaler Skalierbarkeit
- ODX
- Remote-VSS

Bereitstellen von SMB-Freigaben auf Windows Server

Voraussetzungen

Für die Verwendung von NetApp Storage in NAS-Umgebungen in Windows Server gelten folgende Anforderungen:

- ONTAP Cluster verfügen über eine gültige CIFS-Lizenz.
- Mindestens ein Aggregat wird erstellt.
- Eine logische Datenschnittstelle (LIF) wird erstellt und die Datenschnittstelle muss für CIFS konfiguriert werden.
- Ein DNS-konfigurierter Windows Active Directory-Domänenserver und Domänenadministratoranmeldeinformationen sind vorhanden.
- Jeder Knoten im NetApp-Cluster ist mit dem Windows-Domänencontroller zeitsynchronisiert.

Active Directory-Domänencontroller

Ein NetApp Storage Controller kann einem Active Directory ähnlich wie einem Windows Server angeschlossen und innerhalb dessen betrieben werden. Während der Erstellung der SVM können Sie den DNS konfigurieren, indem Sie den Domain-Namen und die Details des Name Servers angeben. Die SVM versucht, nach einem Active Directory-Domänencontroller zu suchen, indem sie den DNS nach einem Active Directory-/Lightweight Directory Access Protocol-(LDAP-)Server in einer Weise abfragt, die Windows Server ähnelt.

Damit das CIFS-Setup ordnungsgemäß funktioniert, müssen die NetApp Storage Controller mit dem Windows Domain Controller synchronisiert werden. NetApp empfiehlt eine Zeitskew zwischen dem Windows Domain

Controller und dem NetApp Storage Controller von maximal fünf Minuten. Es empfiehlt sich, den NTP-Server (Network Time Protocol) für die Synchronisierung des ONTAP-Clusters mit einer externen Zeitquelle zu konfigurieren. Führen Sie zum Konfigurieren des Windows-Domänencontrollers als NTP-Server den folgenden Befehl auf dem ONTAP-Cluster aus:

```
$domainControllerIP = "<input IP Address of windows domain controller>"
cluster::> system services ntp server create â€"server $domainControllerIP
```

Einsatz

1. Erstellen Sie eine neue SVM mit aktiviertem NAS-Protokoll CIFS. Eine neue SVM kann mit einer der folgenden Methoden erstellt werden:
   - CLI-Befehle auf NetApp ONTAP
   - System Manager
   - Das NetApp PowerShell Toolkit
2. Konfigurieren Sie das CIFS-Protokoll
   a. Geben Sie den CIFS-Servernamen an.
   b. Geben Sie das Active Directory an, mit dem der CIFS-Server verbunden werden muss. Sie müssen über die Anmeldeinformationen des Domänenadministrators verfügen, um dem CIFS-Server das Active Directory beizutreten.
3. Zuweisung der SVM mit LIFs auf jedem Cluster-Node
4. Starten Sie den CIFS-Service auf der SVM.
5. Erstellen Sie ein Volume mit NTFS-Sicherheitsstil aus dem Aggregat.
6. Erstellen Sie auf dem Volume einen qtree (optional).
7. Erstellen Sie Shares, die dem Volume oder qtree-Verzeichnis entsprechen, sodass über Windows Server auf diese zugegriffen werden kann. Wählen Sie kontinuierliche Verfügbarkeit für Hyper-V während der Erstellung der Freigabe aktivieren, wenn die Freigabe für Hyper-V-Speicher verwendet wird. Auf diese Weise ist Hochverfügbarkeit für Dateifreigaben möglich.
8. Bearbeiten Sie die erstellte Freigabe, und ändern Sie die Berechtigungen, die für den Zugriff auf die Freigabe erforderlich sind. Die Berechtigungen für die SMB-Freigabe müssen so konfiguriert werden, dass sie den Zugriff auf die Computerkonten aller Server gewährt, die auf diese Freigabe zugreifen.

Host-Integration

Das NAS-Protokoll CIFS ist nativ in ONTAP integriert. Aus diesem Grund benötigt Windows Server keine zusätzliche Client-Software für den Zugriff auf die Daten auf NetApp ONTAP. Ein NetApp Storage Controller wird im Netzwerk als nativer File Server angezeigt und unterstützt die Microsoft Active Directory-Authentifizierung.

Führen Sie die folgenden Schritte aus, um die zuvor mit Windows Server erstellte CIFS-Freigabe zu ermitteln:

1. Melden Sie sich bei Windows Server als Mitglied der Administratorgruppe an.
2. Gehen Sie zu run.exe und geben Sie den vollständigen Pfad der CIFS-Freigabe ein, die für den Zugriff auf die Freigabe erstellt wurde.
3. Um die Freigabe dauerhaft auf dem Windows Server zuzuordnen, klicken Sie mit der rechten Maustaste auf Diesen PC, klicken Sie auf Netzwerklaufwerk zuordnen und geben Sie den Pfad der CIFS-Freigabe an.

4. Bestimmte CIFS-Managementaufgaben können mit Microsoft Management Console (MMC) ausgeführt werden. Bevor Sie diese Aufgaben ausführen, müssen Sie die MMC mithilfe der MMC-Menübefehle mit dem NetApp ONTAP-Speicher verbinden.
    a. Um die MMC in Windows Server zu öffnen, klicken Sie im Abschnitt Extras des Server Managers auf Computerverwaltung.
    b. Klicken Sie auf Weitere Aktionen und Verbinden mit einem anderen Computer. Daraufhin wird das Dialogfeld Computer auswählen geöffnet.
    c. Geben Sie den Namen des CIFS-Servers oder die IP-Adresse der SVM-LIF ein, um eine Verbindung zum CIFS-Server herzustellen.
    d. Erweitern Sie System-Tools und freigegebene Ordner, um geöffnete Dateien, Sitzungen und Freigaben anzuzeigen und zu verwalten.

Best Practices in sich vereint

- Um sicherzustellen, dass es keine Ausfallzeiten gibt, wenn ein Volume von einem Node auf einen anderen oder im Fall eines Node-Ausfalls verschoben wird, empfiehlt NetApp, die Option für die kontinuierliche Verfügbarkeit der Dateifreigabe zu aktivieren.
- Bei der Bereitstellung von VMs für Hyper-V über SMB-Umgebungen empfiehlt NetApp, den Copy-Offload auf dem Storage-System zu aktivieren. Auf diese Weise wird die Bereitstellungszeit der VMs verkürzt.
- Wenn das Storage-Cluster mehrere SMB-Workloads wie SQL Server, Hyper-V und CIFS-Server hostet, empfiehlt NetApp, verschiedene SMB-Workloads auf separaten SVMs in separaten Aggregaten zu hosten. Diese Konfiguration ist von Vorteil, da für jede dieser Workloads ein einzigartiges Storage-Netzwerk- und Volume-Layout erforderlich ist.
- NetApp empfiehlt, Hyper-V Hosts und NetApp ONTAP Storage mit einem 10-GB-Netzwerk zu verbinden, sofern vorhanden. Bei einer 1-GB-Netzwerkverbindung empfiehlt NetApp die Erstellung einer Schnittstellengruppe, die aus mehreren 1-GB-Ports besteht.
- Wenn VMs von einer SMB 3.0-Freigabe zu einer anderen migriert werden, empfiehlt NetApp die Aktivierung der CIFS-Offloaded-Funktion auf dem Storage-System, damit die Migration schneller erfolgt.

Dinge, die Sie sich merken sollten

- Wenn Sie Volumes für SMB-Umgebungen bereitstellen, müssen die Volumes mit dem NTFS-Sicherheitsstil erstellt werden.
- Die Zeiteinstellungen für Knoten im Cluster sollten entsprechend eingerichtet werden. Verwenden Sie NTP, wenn der NetApp-CIFS-Server an der Windows Active Directory-Domäne teilnehmen muss.
- Persistente Handles funktionieren nur zwischen Nodes in einem HA-Paar.
- Das Witness-Protokoll funktioniert nur zwischen Nodes in einem HA-Paar.
- Kontinuierlich verfügbare File Shares werden nur für Hyper-V und SQL Server Workloads unterstützt.
- Der Multichannel SMB wird ab ONTAP 9.4 unterstützt.
- RDMA wird nicht unterstützt.
- ReFS wird nicht unterstützt.

Bereitstellung von SMB-Freigaben auf Nano Server

Nano Server benötigt keine zusätzliche Client-Software, um auf Daten auf der CIFS-Freigabe auf einem NetApp-Speicher-Controller zuzugreifen.

Um Dateien von Nano Server auf eine CIFS-Freigabe zu kopieren, führen Sie die folgenden Cmdlets auf dem Remote-Server aus:

```
$ip = "<input IP Address of the Nano Server>"
```

```
# Create a New PS Session to the Nano Server
$session = New-PSSession -ComputerName $ip -Credential ~\Administrator
```

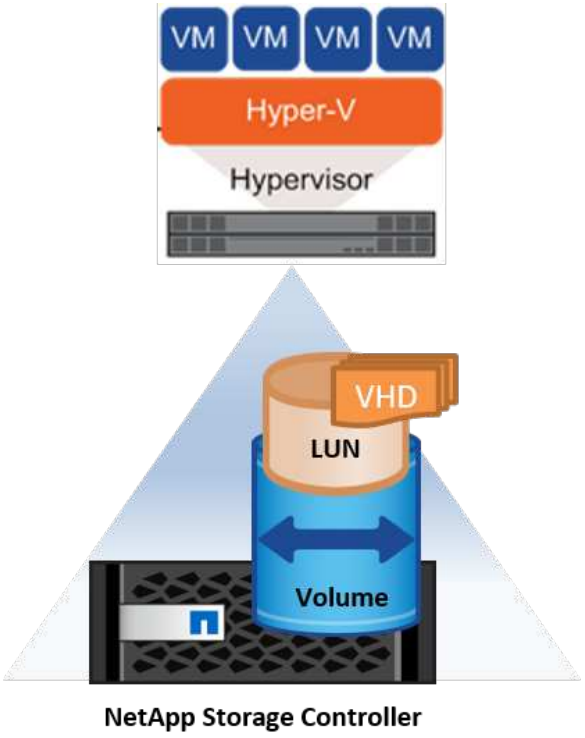
```
 Copy-Item -FromSession $s -Path C:\Windows\Logs\DISM\dism.log
-Destination \\cifsshare
* `cifsshare` Ist die CIFS-Freigabe auf dem NetApp-Speicher-Controller.
* Führen Sie das folgende Cmdlet aus, um Dateien in Nano Server zu
kopieren:
```

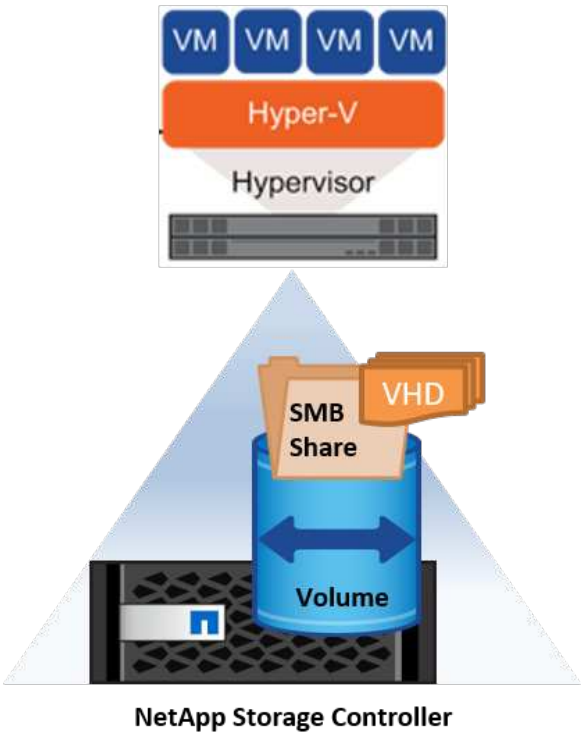
+
Copy-Item -ToSession $s -Path \\cifsshare\<file> -Destination C:\

Um den gesamten Inhalt eines Ordners zu kopieren, geben Sie den Ordnernamen an und verwenden Sie den Parameter -Recurse am Ende des Cmdlet.

Hyper-V Storage-Infrastruktur auf NetApp

Eine Hyper-V Storage-Infrastruktur kann auf ONTAP Storage-Systemen gehostet werden. Speicher für Hyper-V zur Speicherung der VM-Dateien und ihrer Festplatten kann mithilfe von NetApp-LUNs oder NetApp-CIFS-Freigaben bereitgestellt werden, wie in der folgenden Abbildung dargestellt.





Hyper-V-Speicher auf NetApp-LUNs

- Stellen Sie eine NetApp-LUN auf dem Hyper-V-Servercomputer bereit. Weitere Informationen finden Sie im Abschnitt „"Bereitstellung in SAN-Umgebungen".“
- Öffnen Sie Hyper-V Manager im Abschnitt Tools von Server Manager.
- Wählen Sie den Hyper-V-Server aus, und klicken Sie auf Hyper-V-Einstellungen.
- Geben Sie den Standardordner an, in dem die VM und ihre Festplatte als LUN gespeichert werden sollen. Dadurch wird der Standardpfad als LUN für den Hyper-V-Speicher festgelegt. Wenn Sie den Pfad für eine VM explizit angeben möchten, können Sie dies bei der Erstellung der VM tun.

Hyper-V-Speicher auf NetApp CIFS

Bevor Sie mit den in diesem Abschnitt aufgeführten Schritten beginnen, lesen Sie den Abschnitt „"Bereitstellung in SMB-Umgebungen".“ Gehen Sie wie folgt vor, um Hyper-V-Speicher auf der NetApp-CIFS-Freigabe zu konfigurieren:

1. Öffnen Sie Hyper-V Manager im Abschnitt Tools von Server Manager.
2. Wählen Sie den Hyper-V-Server aus, und klicken Sie auf Hyper-V-Einstellungen.
3. Geben Sie den Standardordner an, in dem die VM und ihr Laufwerk als CIFS-Freigabe gespeichert werden sollen. Dadurch wird der Standardpfad als CIFS-Freigabe für den Hyper-V-Speicher festgelegt. Wenn Sie den Pfad für eine VM explizit angeben möchten, können Sie dies bei der Erstellung der VM tun.

Jede VM in Hyper-V kann wiederum mit den NetApp LUNs und CIFS-Freigaben bereitgestellt werden, die dem physischen Host zur Verfügung gestellt wurden. Dieses Verfahren ist das gleiche wie für jeden physischen Host. Mit den folgenden Methoden kann Storage für eine VM bereitgestellt werden:

- Hinzufügen einer Storage-LUN mithilfe des FC-Initiators in der VM
- Hinzufügen einer Storage-LUN mithilfe des iSCSI-Initiators in der VM

- Hinzufügen einer physischen Pass-Through-Festplatte zu einer VM
- Hinzufügen von VHD/VHDX zu einer VM vom Host aus

Best Practices in sich vereint

- Wenn eine VM und die zugehörigen Daten im NetApp Storage gespeichert sind, empfiehlt NetApp, die NetApp Deduplizierung regelmäßig auf Volume-Ebene durchzuführen. Wenn identische VMs auf einer CSV- oder SMB-Freigabe gehostet werden, lassen sich erhebliche Platzeinsparungen erzielen. Die Deduplizierung wird auf dem Storage-Controller ausgeführt und das Host-System und die VM-Performance werden nicht beeinträchtigt.
- Wenn Sie iSCSI-LUNs für Hyper-V verwenden, stellen Sie sicher, dass aktiviert ist `iSCSI Service (TCP-In) for Inbound` Und `iSCSI Service (TCP-Out) for Outbound` In den Firewall-Einstellungen auf dem Hyper-V-Host. Auf diese Weise kann iSCSI-Datenverkehr zum und vom Hyper-V-Host und dem NetApp-Controller geleitet werden.
- NetApp empfiehlt, die Option Verwaltungs-Betriebssystem zulassen, diesen Netzwerkadapter für den virtuellen Hyper-V-Switch gemeinsam zu nutzen, zu deaktivieren. Dadurch wird ein dediziertes Netzwerk für die VMs erstellt.

Dinge, die Sie sich merken sollten

- Die Bereitstellung einer VM mithilfe von virtuellem Fibre Channel erfordert einen N_Port ID Virtualizationâ€“enabled FC HBA. Es werden maximal vier FC-Ports unterstützt.
- Wenn das Hostsystem mit mehreren FC-Ports konfiguriert und der VM vorgelegt wird, muss MPIO in der VM installiert werden, um Multipathing zu aktivieren.
- Pass-Through-Festplatten können nicht auf dem Host bereitgestellt werden, wenn MPIO auf diesem Host verwendet wird, da Pass-Through-Festplatten MPIO nicht unterstützen.
- Für VHD/VHDX-Dateien verwendete Festplatten sollten zur Zuweisung eine 64-KB-Formatierung verwenden.

Weitere Informationen

- Weitere Informationen zu FC-HBAs finden Sie im "NetApp Interoperabilitätsmatrix".
- Weitere Informationen zu virtuellem Fibre Channel finden Sie unter Microsoft "Hyper-V Virtual Fibre Channel – Überblick" Seite.

Verlagerte Datenübertragung

Microsoft ODX, auch als Copy Offload bezeichnet, ermöglicht direkte Datentransfers innerhalb eines Speichergeräts oder zwischen kompatiblen Speichergeräten, ohne die Daten über den Hostcomputer zu übertragen. NetApp ONTAP unterstützt die ODX Funktion für CIFS- und SAN-Protokolle. ODX kann potenziell die Performance verbessern, wenn Kopien sich innerhalb desselben Volumes befinden, senkt die Auslastung von CPU und Arbeitsspeicher im Client und reduziert die Auslastung der Netzwerk-I/O-Bandbreite.

Mit ODX ist es schneller und effizienter, Dateien innerhalb der SMB-Freigaben, innerhalb der LUNs sowie zwischen SMB-Freigaben und LUNs zu kopieren, wenn sich diese sich in demselben Volume befinden. Dieser Ansatz ist insbesondere in Szenarien hilfreich, in denen mehrere Kopien des Golden Image eines Betriebssystems (VHD/VHDX) innerhalb desselben Volumes erforderlich sind. Es können mehrere Kopien desselben goldenen Images in deutlich kürzerer Zeit erstellt werden, wenn sich Kopien innerhalb desselben Volumes befinden. ODX wird auch bei der Hyper-V Storage Live Migration für die Verschiebung von VM Storage eingesetzt.

Wenn Kopien über Volumes hinweg erstellt werden, ergeben sich möglicherweise keine nennenswerten Performance-Steigerungen im Vergleich zu hostbasierten Kopien.

Führen Sie die folgenden CLI-Befehle auf dem NetApp-Speichercontroller aus, um die ODX-Funktion auf CIFS zu aktivieren:

1. Aktivieren Sie ODX für CIFS.
   #Setzen Sie die Berechtigungsebene auf Diagnose
   Cluster::> set -Privilege Diagnostics

   ```
   #enable the odx feature
   cluster::> vserver cifs options modify -vserver <vserver_name> -copy
   -offload-enabled true
   ```

   ```
   #return to admin privilege level
   cluster::> set privilege admin
   ```

2. Führen Sie zum Aktivieren der ODX-Funktion auf dem SAN die folgenden CLI-Befehle auf dem NetApp-Speicher-Controller aus:
   #Setzen Sie die Berechtigungsebene auf Diagnose
   Cluster::> set -Privilege Diagnostics

   ```
   #enable the odx feature
   cluster::> copy-offload modify -vserver <vserver_name> -scsi enabled
   ```

   ```
   #return to admin privilege level
   cluster::> set privilege admin
   ```

Dinge, die Sie sich merken sollten

- Für CIFS ist ODX nur verfügbar, wenn sowohl der Client als auch der Speicherserver SMB 3.0 und die ODX-Funktion unterstützen.
- In SAN-Umgebungen ist ODX nur verfügbar, wenn sowohl der Client als auch der Speicherserver die ODX-Funktion unterstützen.

Weitere Informationen

Informationen zu ODX finden Sie unter "Verbesserung Der Microsoft Remote Copy Performance" Und "Microsoft Offloaded Data Transfers" .

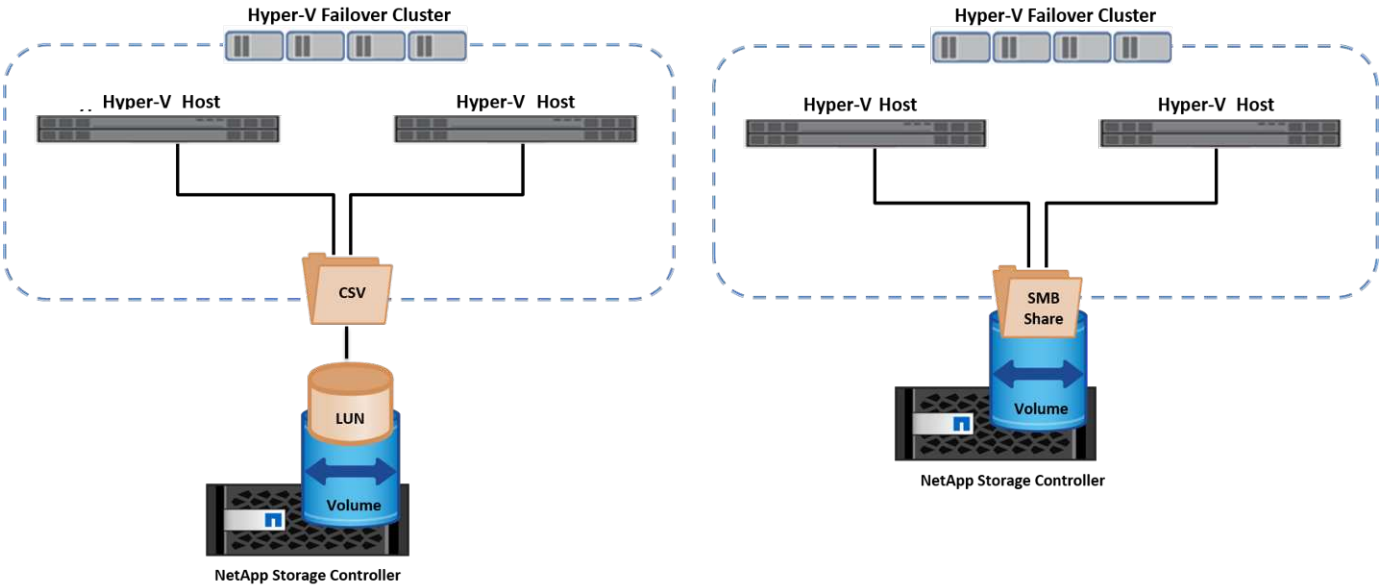
Hyper-V Clustering: Hohe Verfügbarkeit und Skalierbarkeit für virtuelle Maschinen

Failover-Cluster bieten Hochverfügbarkeit und Skalierbarkeit für Hyper-V Server. Ein Failover-Cluster ist eine Gruppe unabhängiger Hyper-V Server, die gemeinsam die Verfügbarkeit und Skalierbarkeit der VMs erhöhen.

Hyper-V Cluster-Server (sogenannte Nodes) werden über das physische Netzwerk und über Cluster-Software verbunden. Diese Nodes verwenden Shared Storage zur Speicherung der VM-Dateien, darunter Konfiguration, VHD-Dateien (virtuelle Festplatte) und Snapshot-Kopien. Beim gemeinsam genutzten Storage kann es sich um eine NetApp SMB/CIFS-Freigabe oder einen CSV auf einer NetApp-LUN handeln, wie in Abbildung 6 dargestellt. Dieser Shared-Storage bietet einen konsistenten und verteilten Namespace, auf den alle Nodes im Cluster gleichzeitig zugreifen können. Wenn daher ein Node im Cluster ausfällt, stellt der andere Node Services für den Prozess Failover bereit. Failover-Cluster können mithilfe des Failover Cluster Manager Snap-ins und der Windows PowerShell Cmdlets für Failover-Clustering gemanagt werden.

Cluster Shared Volumes

CSVs ermöglichen mehreren Knoten in einem Failover-Cluster gleichzeitig Lese-/Schreibzugriff auf dieselbe NetApp-LUN, die als NTFS- oder ReFS-Volume bereitgestellt wird. Mit CSVs können geclusterte Rollen schnell ein Failover von einem Node auf einen anderen durchführen, ohne dass eine Änderung des Festplatteneigentums erforderlich ist oder ein Volume aus- und wieder gemountet werden muss. CSVs vereinfachen außerdem das Management einer potenziell großen Anzahl von LUNs in einem Failover-Cluster. CSVs stellen ein universell einsetzbare Cluster-Dateisystem bereit, das über NTFS oder ReFS geschichtet ist.



Best Practices in sich vereint

- NetApp empfiehlt, die Cluster-Kommunikation im iSCSI-Netzwerk zu deaktivieren, um zu verhindern, dass interne Cluster-Kommunikation und CSV-Datenverkehr über dasselbe Netzwerk übertragen werden.
- NetApp empfiehlt zur Gewährleistung von Ausfallsicherheit und QoS redundante Netzwerkpfade (mehrere Switches).

Dinge, die Sie sich merken sollten

- Für CSV verwendete Laufwerke müssen mit NTFS oder ReFS partitioniert werden. Mit FAT oder FAT32 formatierte Festplatten können nicht für CSV verwendet werden.
- Für CSVs verwendete Festplatten sollten eine 64K-Formatierung für die Zuweisung verwenden.

Weitere Informationen

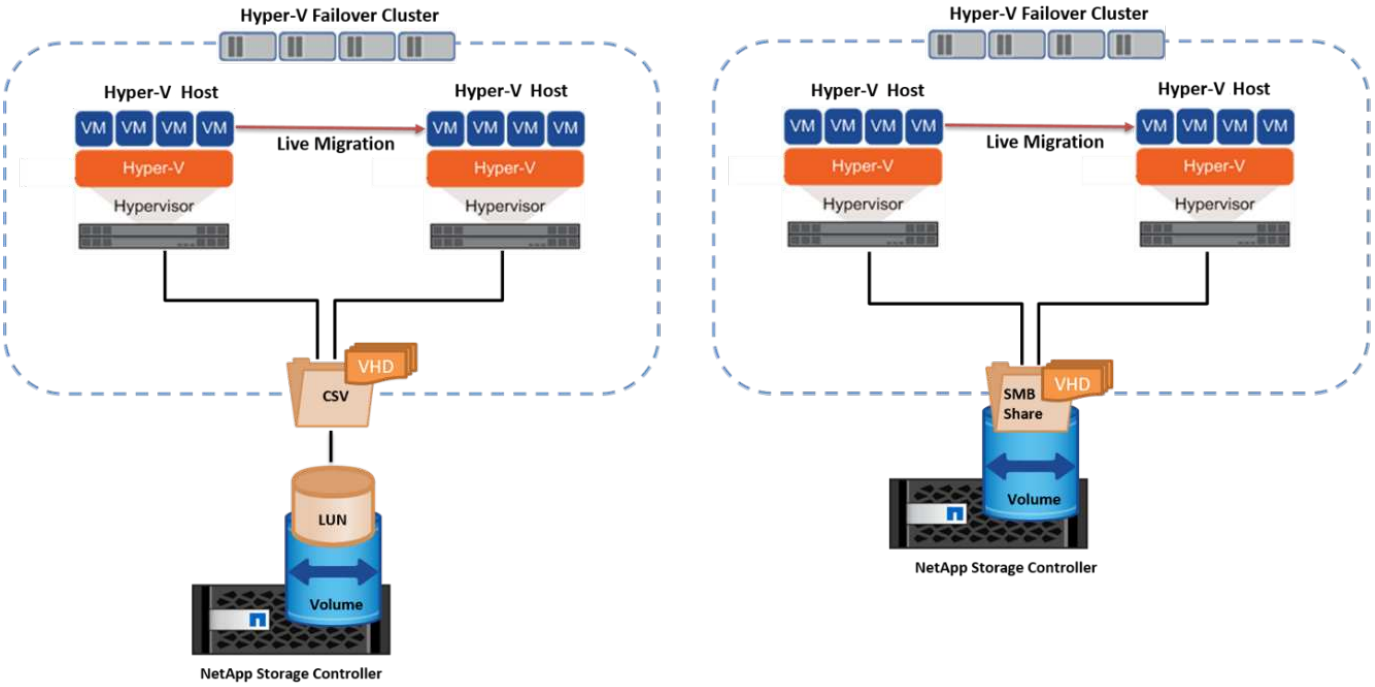
Informationen zum Bereitstellen eines Hyper-V-Clusters finden Sie in Anhang B: "Implementieren Sie Hyper-V Cluster".

Hyper-V Live Migration: Migration von VMs

Manchmal ist es während der Lebensdauer der VMs erforderlich, sie auf einen anderen Host auf dem Windows-Cluster zu verschieben. Dies kann erforderlich sein, wenn dem Host die Systemressourcen ausgehen oder der Host aus Wartungsgründen neu gestartet werden muss. Gleichermaßen kann es erforderlich sein, eine VM auf eine andere LUN- oder SMB-Freigabe zu verschieben. Dies kann erforderlich sein, wenn die aktuelle LUN oder Share über zu viel Speicherplatz verfügt oder eine niedrigere Performance erzielt als erwartet. Live-Migration mit Hyper-V verschiebt laufende VMs von einem physischen Hyper-V Server auf einen anderen, ohne dass die VM-Verfügbarkeit für Benutzer darunter ist. Sie können VMs zwischen Hyper-V-Servern, die Teil eines Failover-Clusters sind, oder zwischen unabhängigen Hyper-V-Servern, die nicht Teil eines Clusters sind, live migrieren.

Live-Migration in einer Cluster-Umgebung

VMs können nahtlos zwischen den Nodes eines Clusters verschoben werden. Die VM-Migration erfolgt unmittelbar, da alle Nodes im Cluster denselben Storage teilen und Zugriff auf die VM und die Festplatte haben. Die folgende Abbildung zeigt die Live-Migration in einer Cluster-Umgebung.



Best Practices in sich

- Verfügen über einen dedizierten Port für den Datenverkehr von Live-Migrationen.
- Nutzen Sie ein dediziertes Host-Live-Migrationsnetzwerk, um netzwerkbezogene Probleme während der Migration zu vermeiden.

Weitere Informationen

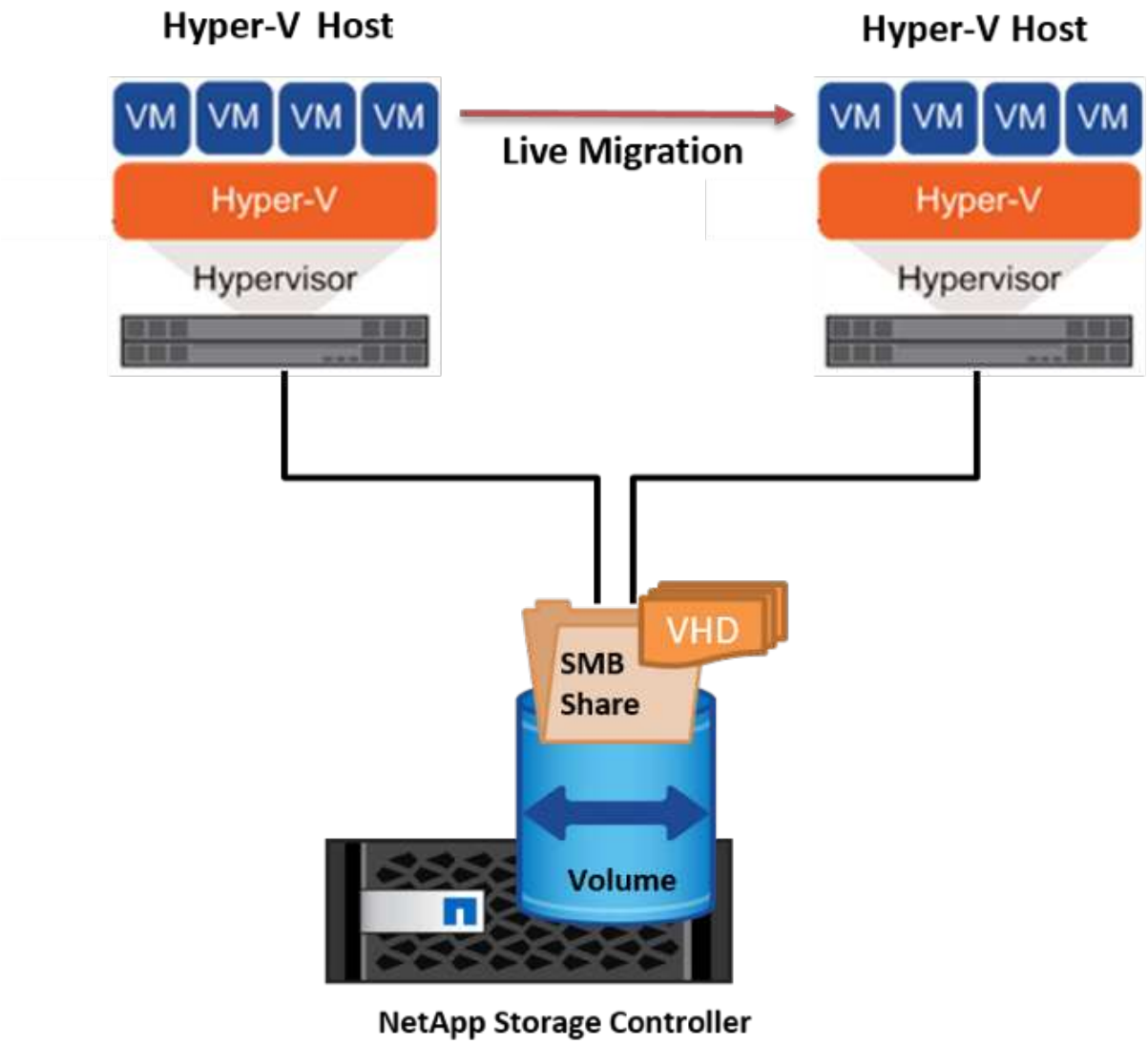
Informationen zur Bereitstellung von Live-Migration in einer Cluster-Umgebung finden Sie unter "Anhang C: Bereitstellung von Hyper-V Live-Migration in einer Cluster-Umgebung".

Live-Migration außerhalb einer Cluster-Umgebung

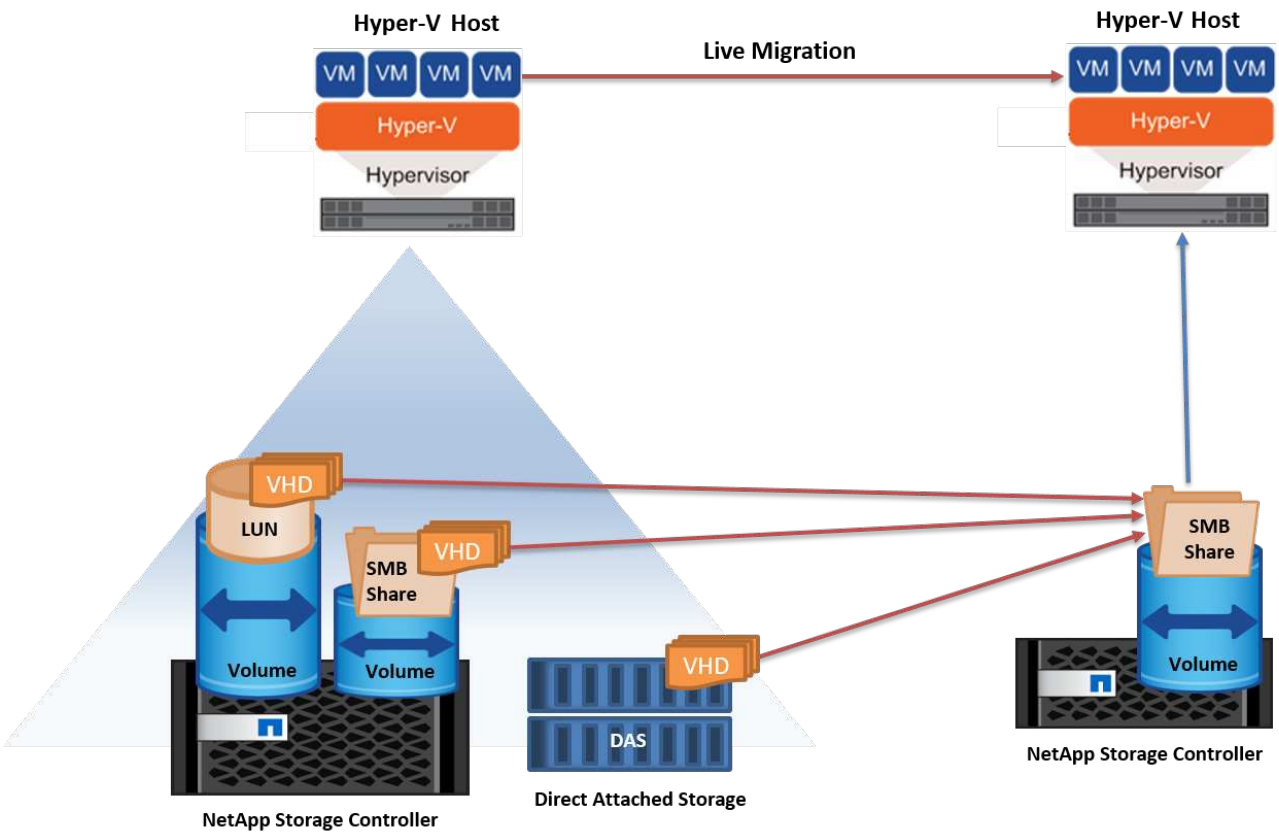
Sie können eine VM zwischen zwei nicht geclusterten, unabhängigen Hyper-V Servern migrieren. Bei diesem Prozess kann entweder eine Live-Migration ohne gemeinsame Nutzung oder ohne gemeinsame Nutzung

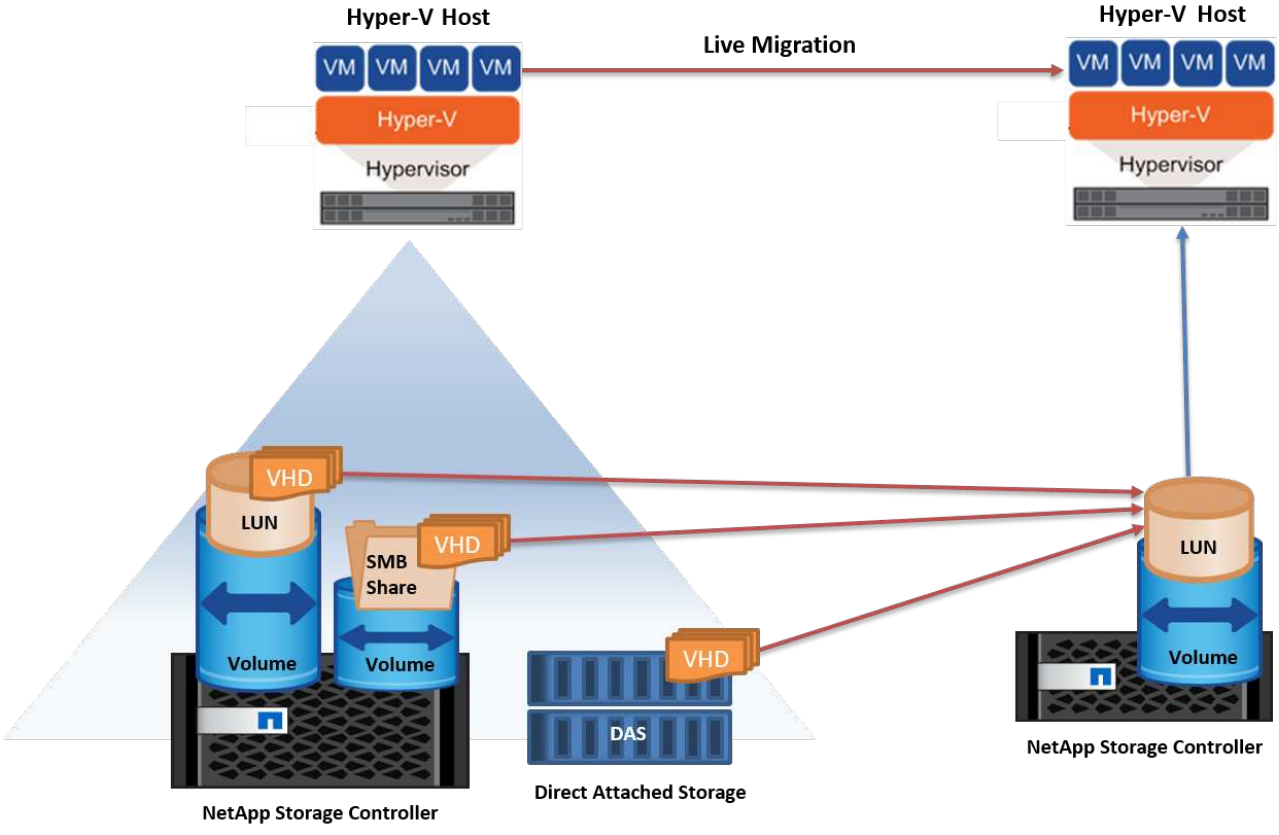
verwendet werden.

- Bei der gemeinsam genutzten Live-Migration wird die VM auf einer SMB-Freigabe gespeichert. Wenn Sie eine VM live migrieren, bleibt der Storage der VM auf der zentralen SMB Freigabe für sofortigen Zugriff durch den anderen Node, wie in der folgenden Abbildung dargestellt.



- Bei der Live-Migration ohne Shared-Ressourcen verfügt jeder Hyper-V-Server über einen eigenen lokalen Storage (ein SMB-Share, eine LUN oder das), und der Storage der VM befindet sich lokal auf seinem Hyper-V Server. Bei der Live-Migration einer VM wird der Storage der VM über das Client-Netzwerk auf den Zielserver gespiegelt und dann die VM migriert. Die auf das, einer LUN oder einer SMB/CIFS-Freigabe gespeicherte VM kann zu einem SMB/CIFS-Share auf einem anderen Hyper-V Server verschoben werden, wie in der folgenden Abbildung dargestellt. Sie kann auch auf eine LUN verschoben werden, wie in der zweiten Abbildung dargestellt.


Hyper-V Host
Live Migration
Hyper-V Host
VM VM VM VM
Hyper-V
Hypervisor
VM VM VM VM
Hyper-V
Hypervisor
VHD
LUN
SMB Share
VHD
Volume
Volume
VHD
DAS
SMB Share
Volume
NetApp Storage Controller
Direct Attached Storage
NetApp Storage Controller


Hyper-V Host
Live Migration
Hyper-V Host
VM VM VM VM
Hyper-V
Hypervisor
VM VM VM VM
Hyper-V
Hypervisor
VHD
LUN
SMB Share
VHD
Volume
Volume
VHD
DAS
LUN
Volume
NetApp Storage Controller
Direct Attached Storage
NetApp Storage Controller

Weitere Informationen

Informationen zur Bereitstellung von Live-Migration außerhalb einer Cluster-Umgebung finden Sie unter "Anhang D: Implementierung von Hyper-V Live-Migration außerhalb einer Cluster-Umgebung".

Hyper-V Storage Live-Migration

Während der Nutzungsdauer einer VM müssen Sie möglicherweise den VM Storage (VHD/VHDX) auf eine andere LUN oder SMB-Freigabe verschieben. Dies kann erforderlich sein, wenn die aktuelle LUN oder Share über zu viel Speicherplatz verfügt oder eine niedrigere Performance erzielt als erwartet.

Die LUN oder die Freigabe, die derzeit als Host für die VM fungiert, kann jedoch nicht mehr genügend Speicherplatz haben, mit einer neuen Verwendung zugewiesen werden oder die Performance beeinträchtigen. Unter diesen Umständen kann die VM ohne Ausfallzeit auf eine andere LUN oder auf eine andere Share in einem anderen Volume, Aggregat oder Cluster verschoben werden. Dieser Prozess läuft schneller ab, wenn das Storage-System Copy-Offload-Funktionen verfügt. NetApp Storage-Systeme sind in CIFS- und SAN-Umgebungen standardmäßig für die Copy-Offload-Funktion aktiviert.

Die ODX-Funktion erstellt Kopien von vollständigen oder untergeordneten Dateien zwischen zwei Verzeichnissen auf Remote-Servern. Eine Kopie wird durch Kopieren von Daten zwischen den Servern (oder dem gleichen Server, wenn sich sowohl die Quell- als auch die Zieldateien auf demselben Server befinden) erstellt. Die Kopie wird erstellt, ohne dass der Client die Daten von der Quelle liest oder auf das Ziel schreibt. Dieser Prozess reduziert die Prozessor- und Speichernutzung für den Client oder Server und minimiert die Netzwerk-I/O-Bandbreite. Die Kopie ist schneller, wenn sie sich innerhalb des gleichen Volumes befindet. Wenn Kopien über Volumes hinweg erstellt werden, ergeben sich möglicherweise keine nennenswerten Performance-Steigerungen im Vergleich zu hostbasierten Kopien. Bevor Sie mit einem Kopiervorgang auf dem Host fortfahren, vergewissern Sie sich, dass die Einstellungen für den Copy-Offload im Storage-System konfiguriert sind.

Wenn die VM Storage Live-Migration von einem Host aus initiiert wird, werden Quelle und Ziel identifiziert und die Kopieraktivität wird zum Storage-System verlagert. Da die Aktivität vom Storage-System durchgeführt wird, wird die Host-CPU, der Arbeitsspeicher oder das Netzwerk nicht wesentlich genutzt.

NetApp Storage Controller unterstützen die folgenden ODX Szenarien:

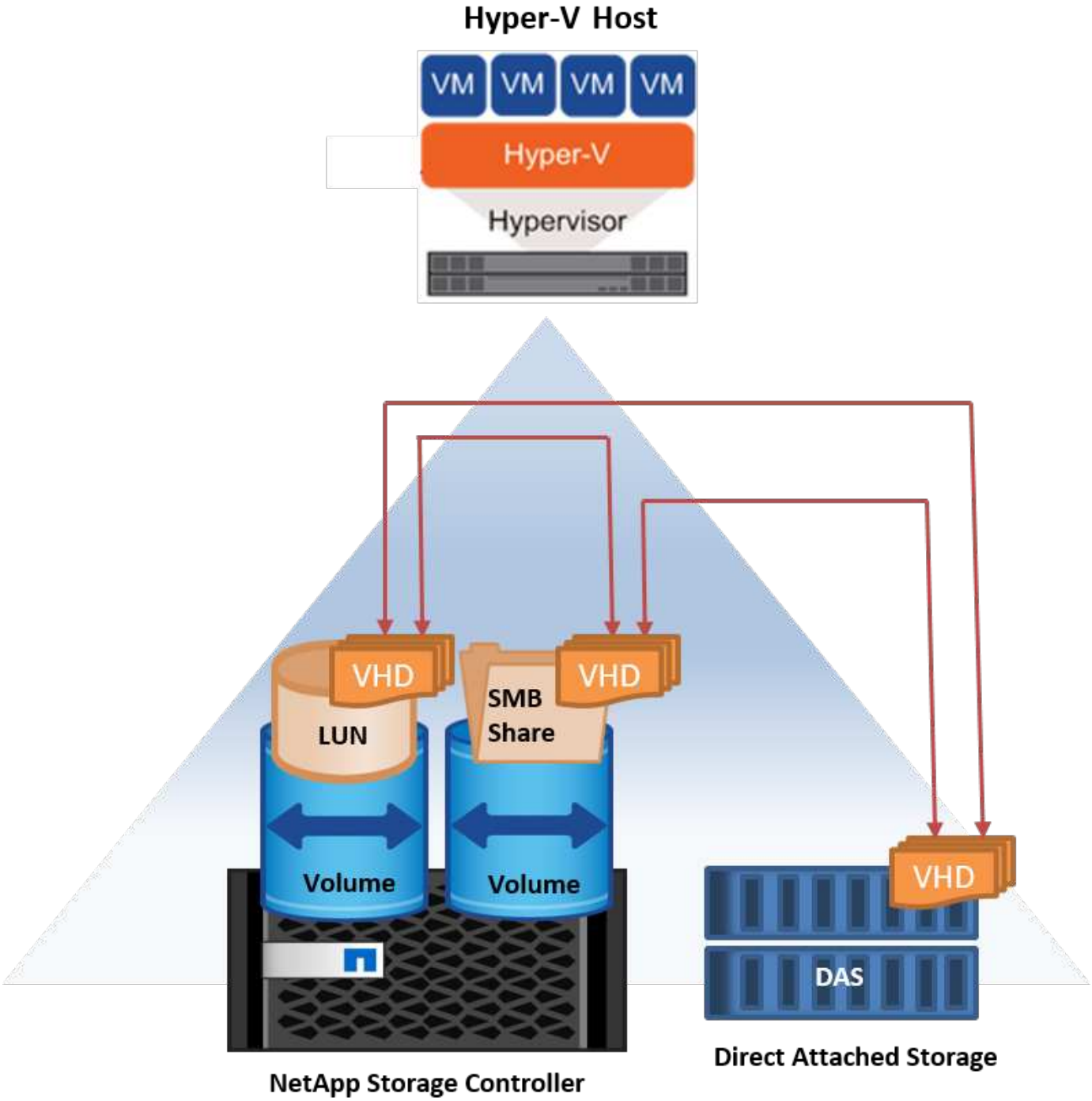
- **IntraSVM.** die Daten befinden sich im Besitz derselben SVM:
- **Intravolume, Intranode.** die Quell- und Zieldateien oder LUNs befinden sich innerhalb des gleichen Volumes. Die FlexClone Dateitechnologie ermöglicht die Erstellung der Kopie. Damit profitieren Sie von weiteren Performance-Vorteilen bei Remote-Kopien.
- **Intervolume, Intranode.** die Quell- und Zieldateien bzw. LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Knoten befinden.
- **Intervolume, Internodes.** die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf verschiedenen Knoten befinden.
- **InterSVM.** die Daten sind Eigentum verschiedener SVMs.
- **Intervolume, Intranode.** die Quell- und Zieldateien bzw. LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Knoten befinden.
- **Intervolume, Internodes.** die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf verschiedenen Knoten befinden.
- **Intercluster.** ab ONTAP 9.0 wird ODX auch für Cluster-LUN-Transfers in SAN-Umgebungen unterstützt. Intercluster ODX wird nur für SAN-Protokolle unterstützt, nicht für SMB.

Nach Abschluss der Migration müssen die Backup- und Replizierungsrichtlinien neu konfiguriert werden, um

das neue Volume, in dem die VMs enthalten sind, zu berücksichtigen. Alle zuvor erstellten Backups können nicht verwendet werden.

VM Storage (VHD/VHDX) kann zwischen den folgenden Storage-Typen migriert werden:

- DAS und die SMB-Freigabe
- DAS und LUN
- Eine SMB-Freigabe und eine LUN
- Zwischen LUNs durchgeführt
- Zwischen SMB-Freigaben

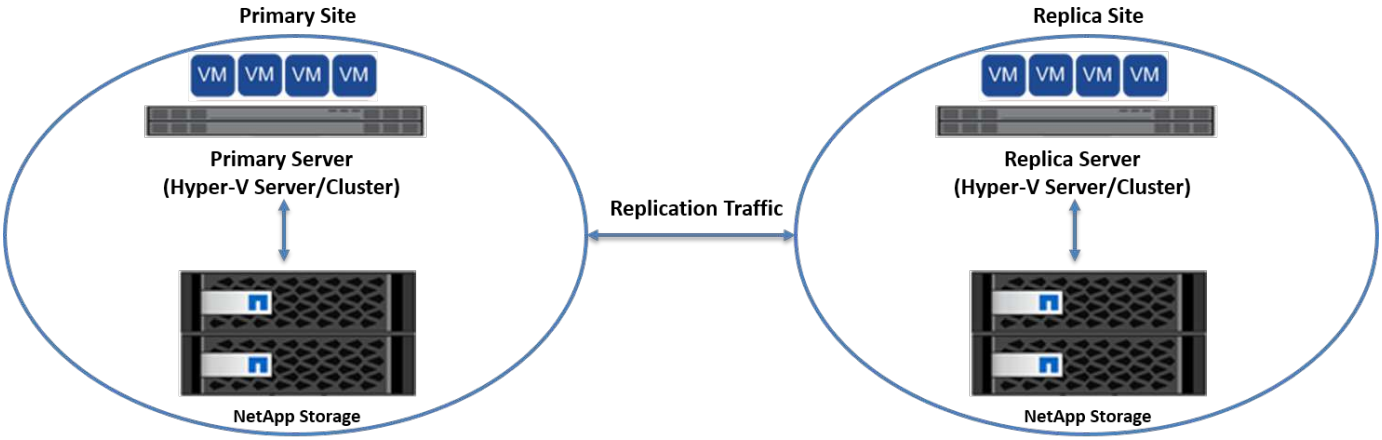


Weitere Informationen

Informationen zur Bereitstellung der Live-Migration von Speicher finden Sie unter "Anhang E: Implementieren von Hyper-V Storage Live-Migration".

Hyper-V Replica: Disaster Recovery für virtuelle Maschinen

Hyper-V Replica repliziert die Hyper-V VMs von einem primären Standort auf die VMs an einem sekundären Standort und stellt so das Disaster Recovery für die VMs asynchron zur Verfügung. Der Hyper-V-Server am primären Standort, der die VMs hostet, wird als primärer Server bezeichnet; der Hyper-V-Server am sekundären Standort, der replizierte VMs empfängt, wird als Replikatserver bezeichnet. Ein Beispielszenario für Hyper-V-Replika wird in der folgenden Abbildung dargestellt. Sie können Hyper-V Replica für VMs zwischen Hyper-V-Servern verwenden, die Teil eines Failover-Clusters sind, oder zwischen unabhängigen Hyper-V-Servern, die nicht Teil eines Clusters sind.



Replizierung

Nachdem das Hyper-V-Replikat für eine VM auf dem primären Server aktiviert wurde, erstellt die erste Replikation eine identische VM auf dem Replikatserver. Nach der ersten Replikation verwaltet Hyper-V Replica eine Protokolldatei für die VHDs der VM. Die Protokolldatei wird in umgekehrter Reihenfolge auf die Replikat-VHD in Übereinstimmung mit der Replikationsfrequenz wiedergegeben. Dieses Protokoll und die Verwendung der umgekehrten Reihenfolge stellen sicher, dass die neuesten Änderungen gespeichert und asynchron repliziert werden. Wenn die Replikation nicht der erwarteten Häufigkeit entspricht, wird eine Warnmeldung ausgegeben.

Erweiterte Replizierung

Hyper-V Replica unterstützt erweiterte Replikation, bei der ein sekundärer Replikatserver für die Disaster Recovery konfiguriert werden kann. Ein sekundärer Replikatserver kann so konfiguriert werden, dass der Replikatserver die Änderungen an den Replikat-VMs empfängt. In einem erweiterten Replikationsszenario werden die Änderungen an den primären VMs auf dem primären Server auf den Replikatserver repliziert. Anschließend werden die Änderungen auf den erweiterten Replikatserver repliziert. Die VMs können nur dann ein Failover auf den erweiterten Replikatserver durchgeführt werden, wenn sowohl der primäre als auch der Replikatserver ausfallen.

Failover

Failover ist nicht automatisch; der Prozess muss manuell ausgelöst werden. Es gibt drei Arten von Failover:

- **Test Failover.** dieser Typ wird verwendet, um zu überprüfen, ob eine ReplikatVM erfolgreich auf dem

Replikatserver gestartet werden kann und auf der ReplikatVM initiiert wird. Durch diesen Prozess wird während des Failovers eine Test-VM doppelt erstellt und die regelmäßige Produktionsreplikation wird nicht beeinträchtigt.

- **Geplante Ausfallsicherung.** dieser Typ wird verwendet, um VMs während geplanter Ausfallzeiten oder erwarteter Ausfälle zu überführen. Dieser Prozess wird auf der primären VM gestartet, die auf dem primären Server ausgeschaltet werden muss, bevor ein geplantes Failover ausgeführt wird. Nach dem Failover der Maschine startet Hyper-V Replica die Replikat-VM auf dem Replikatserver.
- **Ungeplantes Failover.** dieser Typ wird verwendet, wenn unerwartete Ausfälle auftreten. Dieser Prozess wird auf der Replikat-VM initiiert und sollte nur verwendet werden, wenn der primäre Computer ausfällt.

Recovery

Wenn Sie die Replikation für eine VM konfigurieren, können Sie die Anzahl der Wiederherstellungspunkte angeben. Wiederherstellungspunkte stellen Zeitpunkte dar, aus denen Daten von einem replizierten Rechner wiederhergestellt werden können.

Weitere Informationen

- Informationen zur Bereitstellung von Hyper-V Replica außerhalb einer Cluster-Umgebung finden Sie im Abschnitt „"Bereitstellung von Hyper-V Replica außerhalb einer Cluster-Umgebung".“
- Informationen zur Bereitstellung von Hyper-V Replica in einer Cluster-Umgebung finden Sie im Abschnitt „"Bereitstellung von Hyper-V Replica in einer Cluster-Umgebung".“

Storage-Effizienz

ONTAP bietet branchenführende Storage-Effizienz für virtualisierte Umgebungen, einschließlich Microsoft Hyper-V. NetApp bietet darüber hinaus Garantie-Programme für Storage-Effizienz.

NetApp Deduplizierung

NetApp Deduplizierung entfernt Blockduplikate auf Storage Volume-Ebene und speichert nur eine physische Kopie, unabhängig von der Anzahl der logischen Kopien. Daher erzeugt die Deduplizierung die Illusion, dass es mehrere Kopien dieses Blocks gibt. Deduplizierung entfernt automatisch doppelte Datenblöcke auf 4-KB-Blockebene über ein gesamtes Volume. Bei diesem Prozess wird Storage neu beansprucht, um Speicherplatz und potenzielle Performance-Einsparungen zu erzielen, indem die Anzahl der physischen Schreibvorgänge auf die Festplatte reduziert wird. Die Deduplizierung kann in Hyper-V Umgebungen zu einer Platzeinsparung von mehr als 70 % führen.

Thin Provisioning

Thin Provisioning bietet eine effiziente Möglichkeit, Storage bereitzustellen, da der Storage nicht vorab zugewiesen wird. Das bedeutet, dass bei der Erstellung eines Volume oder einer LUN mit Thin Provisioning der Speicherplatz im Storage-System nicht genutzt wird. Der Speicherplatz bleibt ungenutzt, bis die Daten auf die LUN oder das Volume geschrieben werden und nur so viel Speicherplatz verwendet wird, wie zur Speicherung der Daten notwendig ist. NetApp empfiehlt die Aktivierung von Thin Provisioning auf dem Volume und die Deaktivierung der LUN-Reservierung.

Quality of Service

Mit Storage QoS in Clustered ONTAP können Sie Storage-Objekte gruppieren und Durchsatzbegrenzungen in

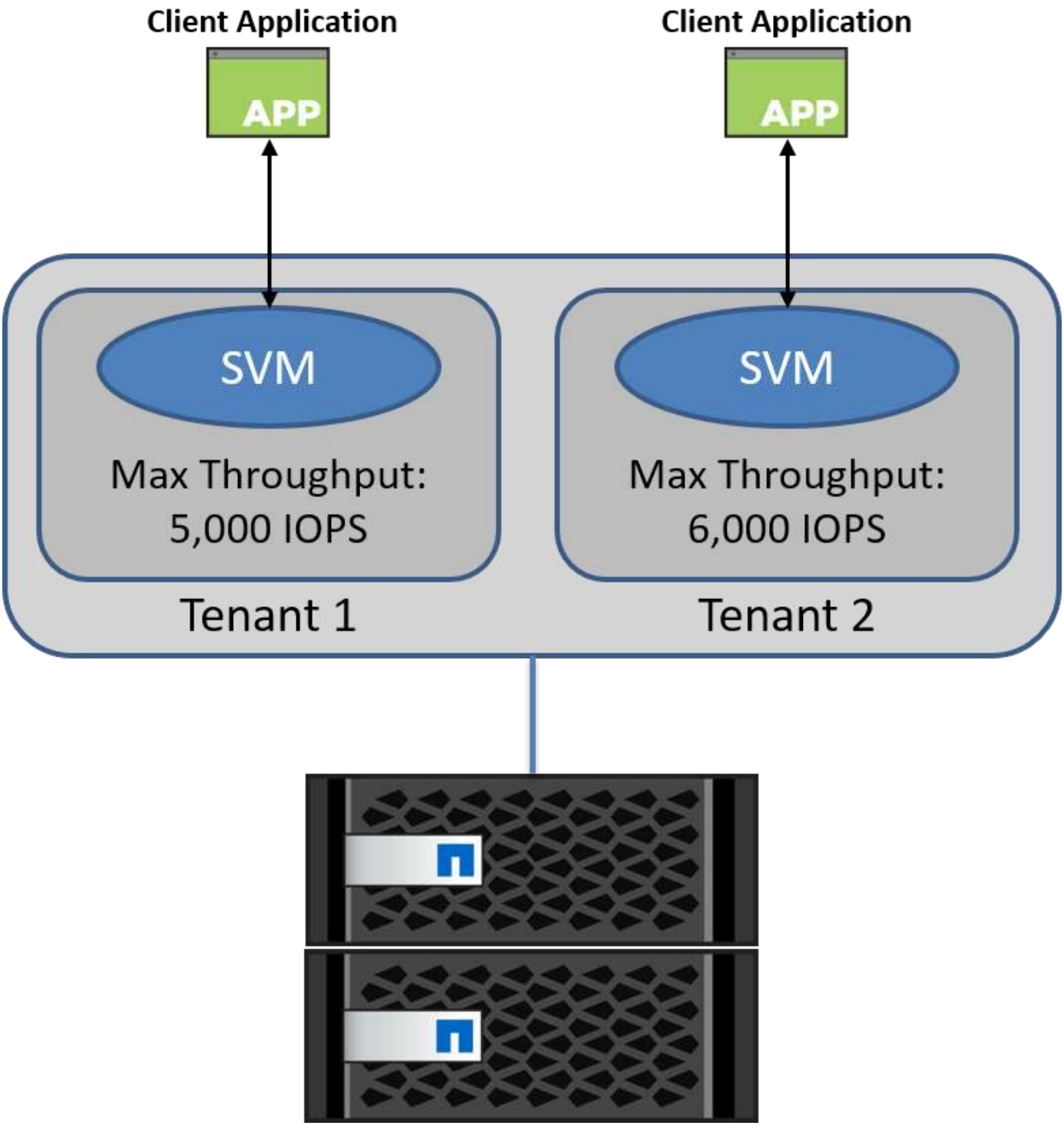
der Gruppe festlegen. Storage QoS kann verwendet werden, um den Durchsatz auf Workloads zu begrenzen und die Workload-Performance zu überwachen. Storage-Administratoren können so Workloads je nach Organisation, Applikation, Geschäftsbereich oder Produktions- oder Entwicklungsumgebung trennen.

In Enterprise-Umgebungen bietet Storage QoS folgende Vorteile:

- Verhindert, dass sich Benutzer-Workloads gegenseitig beeinträchtigen
- Sichert kritische Applikationen mit spezifischen Reaktionszeiten, die in IT-als-Service-Umgebungen (ITaaS) erfüllt werden müssen.
- Verhindert, dass sich Mandanten gegenseitig beeinträchtigen.
- Vermeidung von Performance-Einbußen durch Hinzufügen neuer Mandanten

Mit QoS können Sie die Menge der an eine SVM, ein flexibles Volume, eine LUN oder eine Datei gesendeten I/O begrenzen. Die I/O-Operationen können durch die Anzahl der Operationen oder den Datendurchsatz begrenzt werden.

In der folgenden Abbildung wird SVM mit einer eigenen QoS-Richtlinie dargestellt, die ein maximales Durchsatzlimit durchsetzt.



Führen Sie zum Konfigurieren einer SVM mit einer eigenen QoS-Richtlinie und für das Monitoring der Richtliniengruppe die folgenden Befehle auf Ihrem ONTAP-Cluster aus:

```
# create a new policy group pg1 with a maximum throughput of 5,000 IOPS
cluster::> qos policy-group create pg1 -vserver vs1 -max-throughput
5000iops
```

```
# create a new policy group pg2 without a maximum throughput
cluster::> qos policy-group create pg2 -vserver vs2
```

```
# monitor policy group performance
cluster::> qos statistics performance show
```

```
# monitor workload performance
cluster::> qos statistics workload performance show
```

Sicherheit

ONTAP stellt ein sicheres Storage-System für das Windows Betriebssystem bereit.

Windows Defender Antivirus

Windows Defender ist eine Anti-Malware-Software, die standardmäßig auf Windows Server installiert und aktiviert ist. Diese Software schützt Windows Server aktiv vor bekannter Malware und kann Malwaredefinitionen regelmäßig über Windows Update aktualisieren. NetApp-LUNs und SMB-Freigaben können mit Windows Defender gescannt werden.

Weitere Informationen

Weitere Informationen finden Sie im "Windows Defender – Übersicht".

BitLocker

Die BitLocker-Laufwerkverschlüsselung ist eine Datenschutzfunktion, die von Windows Server 2012 fortgesetzt wird. Diese Verschlüsselung schützt physische Festplatten, LUNs und CSVs.

Best Practices in sich

Vor der Aktivierung von BitLocker muss die CSV-Datei in den Wartungsmodus versetzt werden. Daher empfiehlt NetApp, vor dem Erstellen von VMs auf der CSV-Datei Entscheidungen zur BitLocker-basierten Sicherheit zu treffen, um Ausfallzeiten zu vermeiden.

Einsatz von Nano-Server

Erfahren Sie mehr über die Bereitstellung von Microsoft Windows Nano Server.

Einsatz

Um einen Nano-Server als Hyper-V-Host bereitzustellen, führen Sie die folgenden Schritte aus:

1. Melden Sie sich bei Windows Server als Mitglied der Administratorgruppe an.
2. Kopieren Sie den Ordner NanoServerImageGenerator aus dem Ordner \NanoServer im Windows Server

ISO auf die lokale Festplatte.

3. Gehen Sie wie folgt vor, um eine Nano Server VHD/VHDX zu erstellen:
   a. Starten Sie Windows PowerShell als Administrator, navigieren Sie zum kopierten NanoServerImageGenerator-Ordner auf der lokalen Festplatte und führen Sie das folgende Cmdlet aus:

```
Set-ExecutionPolicy RemoteSigned
Import-Module .\NanoServerImageGenerator -Verbose
```

   b. Erstellen Sie eine VHD für den Nano Server als Hyper-V-Host, indem Sie das folgende PowerShell-Cmdlet ausführen. Mit diesem Befehl werden Sie zur Eingabe eines Administratorkennworts für die neue VHD aufgefordert.

```
 New-NanoServerImage -Edition Standard -DeploymentType Guest
-MediaPath <"input the path to the root of the contents of Windows
Server 2016 ISO"> -TargetPath <"input the path, including the
filename and extension where the resulting VHD/VHDX will be created">
-ComputerName <"input the name of the nano server computer you are
about to create"> -Compute
.. Im folgenden Beispiel erstellen wir eine Nano Server VHD mit der
Funktion Hyper-V Host mit aktiviertem Failover Clustering. In diesem
Beispiel wird eine Nano Server VHD von einem ISO erstellt, das bei
f:\ gemountet ist. Die neu erstellte VHD wird in einem Ordner namens
NanoServer im Ordner abgelegt, von dem aus das Cmdlet ausgeführt
wird. Der Computername ist NanoServer und die resultierende VHD
enthält die Standard-Edition von Windows Server.
```

```
 New-NanoServerImage -Edition Standard -DeploymentType Guest
-MediaPath f:\ -TargetPath .\NanoServer.vhd -ComputerName NanoServer
-Compute -Clustering
.. Konfigurieren Sie mit dem Cmdlet New-NanoServerImage Parameter,
die die IP-Adresse, die Subnetzmaske, das Standard-Gateway, den DNS-
Server, den Domänennamen, und so weiter.
```

4. Verwenden Sie die VHD in einer VM oder einem physischen Host, um Nano Server als Hyper-V-Host bereitzustellen:
   a. Erstellen Sie für die Bereitstellung auf einer VM eine neue VM im Hyper-V Manager, und verwenden Sie die in Schritt 3 erstellte VHD.
   b. Kopieren Sie zur Bereitstellung auf einem physischen Host die VHD auf den physischen Computer, und konfigurieren Sie sie so, dass sie von dieser neuen VHD gestartet wird. Zuerst mounten Sie die VHD, führen Sie bcdboot e:\Windows (wo die VHD unter E:\ gemountet ist), unmounten Sie die VHD, starten Sie den physischen Computer neu, und starten Sie den Nano Server.
5. Verbinden Sie den Nano Server mit einer Domain (optional):

a. Melden Sie sich an einem beliebigen Computer in der Domäne an und erstellen Sie einen Daten-Blob, indem Sie das folgende PowerShell Cmdlet ausführen:

```
$domain = "<input the domain to which the Nano Server is to be
joined>"
$nanoserver = "<input name of the Nano Server>"
```

```
 djoin.exe /provision /domain $domain /machine $nanoserver /savefile
C:\temp\odjblob /reuse
.. Kopieren Sie die odjBLOB-Datei auf den Nano Server, indem Sie die
folgenden PowerShell-Cmdlets auf einem Remote-Computer ausführen:
```

```
$nanoserver = "<input name of the Nano Server>"
$nanouname = ""<input username of the Nano Server>"
$nanopwd = ""<input password of the Nano Server>"
```

```
$filePath = 'c:\temp\odjblob'
$fileContents = Get-Content -Path $filePath -Encoding Unicode
```

```
$securenanopwd = ConvertTo-SecureString -AsPlainText -Force $nanopwd
$nanosecurecred = new-object management.automation.pscredential
$nanouname, $securenanopwd
```

```
Invoke-Command -VMName $nanoserver -Credential $nanosecurecred
-ArgumentList @($filePath,$fileContents) -ScriptBlock \{
    param($filePath,$data)
    New-Item -ItemType directory -Path c:\temp
    Set-Content -Path $filePath -Value $data -Encoding Unicode
    cd C:\temp
    djoin /requestodj /loadfile c:\temp\odjblob /windowspath
c:\windows /localos
}
```

b. Starten Sie den Nano Server neu.

Verbindung mit Nano Server herstellen

Gehen Sie wie folgt vor, um eine Remote-Verbindung mit dem Nano Server über PowerShell herzustellen:

1. Fügen Sie den Nano Server als vertrauenswürdigen Host auf dem Remotecomputer hinzu, indem Sie das

folgende Cmdlet auf dem Remoteserver ausführen:

```
 Set-Item WSMan:\LocalHost\Client\TrustedHosts "<input IP Address of the
Nano Server>"
. Wenn die Umgebung sicher ist und Sie alle hinzuzufügenden Hosts als
vertrauenswürdige Hosts auf einem Server festlegen möchten, führen Sie
den folgenden Befehl aus:
```

```
 Set-Item WSMan:\LocalHost\Client\TrustedHosts *
. Starten Sie die Remote-Sitzung, indem Sie das folgende Cmdlet auf dem
Remote-Server ausführen. Geben Sie das Passwort für den Nano Server an,
wenn Sie dazu aufgefordert werden.
```

```
Enter-PSSession -ComputerName "<input IP Address of the Nano Server>"
-Credential ~\Administrator
```

Um eine Remote-Verbindung mit dem Nano Server über GUI-Verwaltungstools von einem Remote-Windows-Server herzustellen, führen Sie die folgenden Befehle aus:

1. Melden Sie sich beim Windows Server als Mitglied der Administratorgruppe an.
2. Starten Sie Server Manager.
3. Um einen Nano Server Remote vom Server Manager aus zu verwalten, klicken Sie mit der rechten Maustaste auf Alle Server, klicken Sie auf Server hinzufügen, geben Sie die Informationen des Nano Servers an und fügen Sie sie hinzu. Der Nano Server ist nun in der Serverliste aufgelistet. Wählen Sie den Nano Server aus, klicken Sie mit der rechten Maustaste darauf, und beginnen Sie mit der Verwaltung mit den verschiedenen verfügbaren Optionen.
4. Um Dienste auf einem Nano Server Remote zu verwalten, führen Sie die folgenden Schritte aus:
   a. Öffnen Sie Services im Abschnitt „Tools“ von Server Manager.
   b. Klicken Sie mit der rechten Maustaste auf Dienste (Lokal).
   c. Klicken Sie auf mit Server verbinden.
   d. Geben Sie die Details des Nano-Servers an, um die Dienste auf dem Nano-Server anzuzeigen und zu verwalten.
5. Wenn die Hyper-V-Rolle auf dem Nano Server aktiviert ist, führen Sie die folgenden Schritte aus, um sie Remote vom Hyper-V Manager zu verwalten:
   a. Öffnen Sie Hyper-V Manager im Abschnitt Tools von Server Manager.
   b. Klicken Sie mit der rechten Maustaste auf Hyper-V Manager.
   c. Klicken Sie auf mit Server verbinden und geben Sie die Details zum Nano Server ein. Jetzt kann der Nano Server als Hyper-V Server verwaltet werden, um darüber hinaus VMs zu erstellen und zu verwalten.
6. Wenn die Failover Clustering-Rolle auf dem Nano Server aktiviert ist, führen Sie die folgenden Schritte aus, um sie vom Failover Cluster Manager aus Remote zu verwalten:

a. Öffnen Sie Failover Cluster Manager im Abschnitt „Tools“ von Server Manager.

b. Führen Sie mit dem Nano Server Cluster-bezogene Vorgänge durch.

Implementieren des Hyper-V-Clusters

In diesem Anhang wird das Bereitstellen eines Hyper-V-Clusters beschrieben.

Voraussetzungen

- Mindestens zwei Hyper-V-Server sind miteinander verbunden.
- Auf jedem Hyper-V-Server ist mindestens ein virtueller Switch konfiguriert.
- Die Failover-Cluster-Funktion ist auf jedem Hyper-V-Server aktiviert.
- SMB-Freigaben oder CSVs werden als Shared Storage verwendet, um VMs und ihre Festplatten für das Hyper-V Clustering zu speichern.
- Storage sollte nicht zwischen verschiedenen Clustern gemeinsam genutzt werden. Pro Cluster sollte nur eine CSV-/CIFS-Freigabe vorhanden sein.
- Wenn die SMB-Freigabe als freigegebener Speicher verwendet wird, müssen Berechtigungen für die SMB-Freigabe konfiguriert werden, um Zugriff auf die Computerkonten aller Hyper-V-Server im Cluster zu gewähren.

Einsatz

1. Melden Sie sich bei einem der Windows Hyper-V-Server als Mitglied der Administratorgruppe an.
2. Starten Sie Server Manager**.**
3. Klicken Sie im Abschnitt Extras auf Failover Cluster Manager.
4. Klicken Sie im Menü Aktionen auf Cluster erstellen.
5. Geben Sie Details für den Hyper-V-Server an, der Teil dieses Clusters ist.
6. Validieren der Cluster-Konfiguration. Wählen Sie Ja, wenn Sie zur Validierung der Cluster-Konfiguration aufgefordert werden, und wählen Sie die erforderlichen Tests aus, um zu überprüfen, ob die Hyper-V-Server die Voraussetzungen erfüllen, um Teil des Clusters zu sein.
7. Nachdem die Validierung erfolgreich war, wird der Assistent Cluster erstellen gestartet. Geben Sie im Assistenten den Cluster-Namen und die Cluster-IP-Adresse für das neue Cluster an. Anschließend wird ein neuer Failover-Cluster für den Hyper-V-Server erstellt.
8. Klicken Sie im Failover Cluster Manager auf den neu erstellten Cluster, und verwalten Sie ihn.
9. Definieren Sie den gemeinsam genutzten Storage, der für das Cluster verwendet werden soll. Es kann sich entweder um eine SMB-Freigabe oder ein CSV handeln.
10. Die Verwendung einer SMB-Freigabe als Shared Storage erfordert keine besonderen Schritte.
    - Konfigurieren Sie eine CIFS-Freigabe auf einem NetApp-Speicher-Controller. Hierzu siehe Abschnitt „"Bereitstellung in SMB-Umgebungen"„.
11. Führen Sie die folgenden Schritte aus, um ein CSV als gemeinsam genutzten Speicher zu verwenden:
    a. Konfigurieren Sie LUNs auf einem NetApp Storage Controller. Hierzu finden Sie im Abschnitt „Provisionierung in SAN-Umgebungen“.
    b. Stellen Sie sicher, dass alle Hyper-V-Server im Failover Cluster die NetApp-LUNs sehen können. Um dies für alle Hyper-V-Server zu tun, die Teil des Failover-Clusters sind, stellen Sie sicher, dass ihre

Initiatoren der Initiatorgruppe im NetApp Storage hinzugefügt werden. Stellen Sie auch sicher, dass ihre LUNs erkannt werden, und stellen Sie sicher, dass MPIO aktiviert ist.

c. Führen Sie auf einem der Hyper-V-Server im Cluster die folgenden Schritte aus:

   i. Nehmen Sie die LUN online, initialisieren Sie die Festplatte, erstellen Sie ein neues einfaches Volume und formatieren Sie sie mit NTFS oder ReFS.

   ii. Erweitern Sie in Failover Cluster Manager den Cluster, erweitern Sie Speicher, klicken Sie mit der rechten Maustaste auf Festplatten, und klicken Sie dann auf Festplatten hinzufügen. Dadurch wird der Assistent Festplatten zu einem Cluster hinzufügen geöffnet, in dem die LUN als Festplatte angezeigt wird. Klicken Sie auf OK, um die LUN als Festplatte hinzuzufügen.

   iii. Nun wird die LUN mit dem Namen „Cluster Disk“ bezeichnet und unter „Disks“ als „Available Storage“ angezeigt.

d. Klicken Sie mit der rechten Maustaste auf die LUN (Cluster Disk) und klicken Sie auf Add to Cluster Shared Volumes. Nun wird die LUN als CSV angezeigt.

e. Der CSV ist von allen Hyper-V Servern des Failover-Clusters an seinem lokalen Standort C:\ClusterStorage\ gleichzeitig sichtbar und zugänglich.

12. Erstellen einer hochverfügbaren VM:

    a. Wählen Sie in Failover Cluster Manager den zuvor erstellten Cluster aus, und erweitern Sie ihn.

    b. Klicken Sie auf Rollen und anschließend auf Virtuelle Maschinen in Aktionen. Klicken Sie Auf Neue Virtuelle Maschine.

    c. Wählen Sie den Node aus dem Cluster aus, auf dem sich die VM befinden soll.

    d. Stellen Sie im Assistenten für die Erstellung virtueller Maschinen den gemeinsam genutzten Speicher (SMB-Freigabe oder CSV) als Pfad zum Speichern der VM und ihrer Festplatten bereit.

    e. Verwenden Sie Hyper-V Manager, um den gemeinsam genutzten Speicher (SMB-Freigabe oder CSV) als Standardpfad festzulegen, um die VM und ihre Festplatten für einen Hyper-V-Server zu speichern.

13. Testen Sie das geplante Failover. Verschieben Sie VMs mithilfe von Live-Migration, schneller Migration oder Storage-Migration (Verschieben) auf einen anderen Node. Prüfen "Live-Migration in einer Cluster-Umgebung" Entnehmen.

14. Testen Sie ein ungeplantes Failover. Stoppen Sie den Cluster-Service auf dem Server, auf dem die VM gehört.

Bereitstellung von Hyper-V Live Migration in einer Cluster-Umgebung

In diesem Anhang wird die Bereitstellung von Live-Migration in einer Cluster-Umgebung beschrieben.

Voraussetzungen

Für die Bereitstellung der Live-Migration müssen Hyper-V-Server in einem Failover-Cluster mit Shared Storage konfiguriert sein. Prüfen "Implementieren Sie Hyper-V Cluster" Entnehmen.

Einsatz

Gehen Sie wie folgt vor, um die Live-Migration in einer Cluster-Umgebung zu nutzen:

1. Wählen Sie in Failover Cluster Manager den Cluster aus, und erweitern Sie ihn. Wenn der Cluster nicht

angezeigt wird, klicken Sie auf Failover Cluster Manager, klicken Sie auf mit Cluster verbinden, und geben Sie den Cluster-Namen ein.

2. Klicken Sie auf Rollen, in der alle in einem Cluster verfügbaren VMs aufgeführt sind.
3. Klicken Sie mit der rechten Maustaste auf die VM und klicken Sie auf Verschieben. Dadurch stehen Ihnen drei Optionen zur Verfügung:
   - **Live Migration.** Sie können einen Knoten manuell auswählen oder dem Cluster erlauben, den besten Knoten auszuwählen. Bei der Live-Migration kopiert das Cluster den von der VM verwendeten Arbeitsspeicher vom aktuellen Node auf einen anderen Node. Wenn die VM zu einem anderen Node migriert wird, sind die von der VM benötigten Arbeitsspeicher- und Statusinformationen bereits für die VM vorhanden. Diese Migrationsmethode erfolgt nahezu ohne Verzögerung, aber nur eine VM kann gleichzeitig live migriert werden.
   - **Schnelle Migration.** Sie können einen Knoten manuell auswählen oder dem Cluster erlauben, den besten Knoten auszuwählen. Bei einer schnellen Migration kopiert das Cluster den von einer VM genutzten Speicher auf eine Festplatte im Storage. Wenn die VM zu einem anderen Node migriert wird, können daher die von der VM benötigten Arbeitsspeicher- und Statusinformationen schnell von der Festplatte des anderen Node gelesen werden. Durch die schnelle Migration können mehrere VMs gleichzeitig migriert werden.
   - **Migration des virtuellen Maschinenspeichers.** Diese Methode verwendet den Assistenten zum Verschieben des virtuellen Maschinenspeichers. Mit diesem Assistenten können Sie die VM-Festplatte zusammen mit anderen Dateien auswählen, die an einen anderen Speicherort verschoben werden sollen. Dabei kann es sich um eine CSV- oder SMB-Freigabe handeln.

Implementierung von Hyper-V Live Migration außerhalb einer Cluster-Umgebung

In diesem Abschnitt wird die Bereitstellung der Hyper-V Live-Migration außerhalb einer Cluster-Umgebung beschrieben.

Voraussetzungen

- Standalone Hyper-V Server mit unabhängigem Storage oder Shared SMB Storage.
- Die Hyper-V-Rolle, die sowohl auf den Quell- als auch auf den Zielservern installiert ist.
- Beide Hyper-V-Server gehören zur gleichen Domäne oder zu Domänen, die sich gegenseitig vertrauen.

Einsatz

Um eine Live-Migration in einer Umgebung ohne Cluster durchzuführen, konfigurieren Sie Hyper-V Quell- und Zielserver so, dass sie Live-Migrationsvorgänge senden und empfangen können. Führen Sie auf beiden Hyper-V-Servern die folgenden Schritte aus:

1. Öffnen Sie Hyper-V Manager im Abschnitt Tools von Server Manager.
2. Klicken Sie unter Aktionen auf Hyper-V-Einstellungen.
3. Klicken Sie auf Live-Migrationen, und wählen Sie eingehende und ausgehende Live-Migrationen aktivieren aus.
4. Wählen Sie aus, ob Live-Migrationsverkehr auf einem beliebigen verfügbaren Netzwerk oder nur in bestimmten Netzwerken zugelassen werden soll.
5. Optional können Sie das Authentifizierungsprotokoll und die Leistsoptionen im Abschnitt „Erweitert“ von

Live-Migrationen konfigurieren.

6. Wenn CredSSP als Authentifizierungsprotokoll verwendet wird, müssen Sie sich vom Hyper-V-Zielserver beim Hyper-V-Quellserver anmelden, bevor Sie die VM verschieben.
7. Wenn Kerberos als Authentifizierungsprotokoll verwendet wird, konfigurieren Sie die eingeschränkte Delegierung. Hierfür ist der Zugriff auf den Active Directory-Domänencontroller erforderlich. Führen Sie zum Konfigurieren der Delegierung die folgenden Schritte aus:
   a. Melden Sie sich beim Active Directory-Domänencontroller als Administrator an.
   b. Starten Sie Server Manager.
   c. Klicken Sie im Abschnitt Extras auf Active Directory-Benutzer und -Computer.
   d. Erweitern Sie die Domäne, und klicken Sie auf Computer.
   e. Wählen Sie den Hyper-V-Quellserver aus der Liste aus, klicken Sie mit der rechten Maustaste darauf, und klicken Sie auf Eigenschaften.
   f. Wählen Sie auf der Registerkarte Delegation die Option Diesen Computer nur für die Delegation an bestimmte Dienste vertrauen aus.
   g. Wählen Sie Nur Kerberos Verwenden Aus.
   h. Klicken Sie auf Hinzufügen, um den Assistenten zum Hinzufügen von Services zu öffnen.
   i. Klicken Sie unter Dienste hinzufügen auf Benutzer und Computer, um Benutzer oder Computer auswählen **zu öffnen.**
   j. Geben Sie den Hyper-V-Zielservernamen ein, und klicken Sie auf OK.
      - Um VM-Speicher zu verschieben, wählen Sie CIFS aus.
      - Um VMs zu verschieben, wählen Sie den Microsoft Virtual System Migration Service aus.
   k. Klicken Sie auf der Registerkarte Delegation auf OK.
   l. Wählen Sie im Ordner Computer den Hyper-V-Zielserver aus der Liste aus, und wiederholen Sie den Vorgang. Geben Sie unter Benutzer oder Computer auswählen den Hyper-V-Quellservernamen an.
8. Verschieben Sie die VM.
   a. Öffnen Sie Hyper-V Manager.
   b. Klicken Sie mit der rechten Maustaste auf eine VM und klicken Sie auf Verschieben.
   c. Wählen Sie „Virtuelle Maschine verschieben“.
   d. Geben Sie den Hyper-V-Zielserver für die VM an.
   e. Wählen Sie die Optionen zum Verschieben. Wählen Sie für Shared Live Migration nur die virtuelle Maschine verschieben. Wählen Sie für „Shared Nothing Live Migration“ je nach Ihren Einstellungen eine der beiden anderen Optionen aus.
   f. Geben Sie den Speicherort für die VM auf dem Hyper-V-Zielserver basierend auf Ihren Einstellungen an.
   g. Überprüfen Sie die Zusammenfassung, und klicken Sie auf OK, um die VM zu verschieben.

Bereitstellung von Hyper-V Storage Live Migration

Erfahren Sie, wie Sie die Hyper-V-Speicher-Live-Migration konfigurieren

Voraussetzungen

- Sie müssen über einen Standalone-Hyper-V-Server mit unabhängigem Storage (das oder LUN) oder SMB-Storage (lokal oder von anderen Hyper-V Servern gemeinsam genutzt) verfügen.
- Der Hyper-V-Server muss für die Live-Migration konfiguriert sein. Lesen Sie den Abschnitt zur Bereitstellung in "Live-Migration außerhalb einer Cluster-Umgebung".

Einsatz

1. Öffnen Sie Hyper-V Manager.
2. Klicken Sie mit der rechten Maustaste auf eine VM und klicken Sie auf Verschieben.
3. Wählen Sie Speicher der virtuellen Maschine verschieben.
4. Wählen Sie Optionen zum Verschieben des Speichers nach Ihren Präferenzen aus.
5. Geben Sie den neuen Speicherort für die VM-Elemente an.
6. Überprüfen Sie die Zusammenfassung, und klicken Sie auf OK, um den VM-Speicher zu verschieben.

Bereitstellung von Hyper-V Replica außerhalb einer Cluster-Umgebung

In diesem Anhang wird die Bereitstellung von Hyper-V Replica außerhalb einer Clusterumgebung beschrieben.

Voraussetzungen

- Sie benötigen eigenständige Hyper-V-Server, die sich an demselben oder einem anderen geografischen Standort befinden und als primäre und Replikatserver dienen.
- Wenn separate Standorte verwendet werden, muss die Firewall an jedem Standort so konfiguriert werden, dass die Kommunikation zwischen dem primären und dem Replikatserver möglich ist.
- Der Replikatserver muss über genügend Speicherplatz zum Speichern der replizierten Workloads verfügen.

Einsatz

1. Konfigurieren Sie den Replikatserver.
    a. Führen Sie das folgende PowerShell-Cmdlet aus, damit die Regeln der eingehenden Firewall eingehenden Replikationsverkehr zulassen:

```
 Enable-Netfirewallrule -displayname "Hyper-V Replica HTTP Listener
(TCP-In)"
.. Öffnen Sie Hyper-V Manager im Abschnitt Tools von Server Manager.
.. Klicken Sie in Aktionen auf Hyper-V-Einstellungen.
.. Klicken Sie auf Replikationskonfiguration und wählen Sie Diesen
Computer als Replikatserver aktivieren aus.
.. Wählen Sie im Abschnitt Authentifizierung und Ports die
Authentifizierungsmethode und den Port aus.
.. Geben Sie im Abschnitt Autorisierung und Speicher den Speicherort
für die replizierten VMs und Dateien an.
```

2. Aktivieren Sie die VM-Replikation für VMs auf dem primären Server. VM-Replikation wird pro VM und nicht für den gesamten Hyper-V-Server aktiviert.
   a. Klicken Sie in Hyper-V Manager mit der rechten Maustaste auf eine VM, und klicken Sie auf Replikation aktivieren, um den Assistenten Replikation aktivieren zu öffnen.
   b. Geben Sie den Namen des Replikatservers an, auf dem die VM repliziert werden muss.
   c. Geben Sie den Authentifizierungstyp und den Port des Replikatservers an, der für den Empfang von Replikationsdatenverkehr auf dem Replikatserver konfiguriert wurde.
   d. Wählen Sie die zu replizierenden VHDs aus.
   e. Wählen Sie die Häufigkeit (Dauer), mit der die Änderungen an den Replikatserver gesendet werden.
   f. Konfigurieren Sie Wiederherstellungspunkte, um die Anzahl der Wiederherstellungspunkte anzugeben, die auf dem Replikatserver beibehalten werden sollen.
   g. Wählen Sie Initial Replication Method, um die Methode anzugeben, mit der die erste Kopie der VM-Daten auf den Replikatserver übertragen werden soll.
   h. Überprüfen Sie die Zusammenfassung, und klicken Sie auf Fertig stellen.
   i. Durch diesen Prozess wird ein VM-Replikat auf dem Replikatserver erstellt.

Replizierung

1. Führen Sie einen Test-Failover aus, um sicherzustellen, dass die Replikat-VM auf dem Replikatserver ordnungsgemäß funktioniert. Der Test erstellt eine temporäre VM auf dem Replikatserver.
   a. Melden Sie sich beim Replikatserver an.
   b. Klicken Sie in Hyper-V Manager mit der rechten Maustaste auf eine Replikat-VM, klicken Sie auf Replikation, und klicken Sie auf Failover testen.
   c. Wählen Sie den zu verwendenden Wiederherstellungspunkt aus.
   d. Bei diesem Vorgang wird eine VM mit dem gleichen Namen erstellt, die mit -Test angehängt wird.
   e. Überprüfung der VM zur Gewährleistung der guten Funktionsweise
   f. Nach dem Failover wird die Test-VM des Replikats gelöscht, wenn Sie für sie die Option „Test-Failover anhalten“ auswählen.
2. Führen Sie ein geplantes Failover aus, um die letzten Änderungen an der primären VM auf die Replikat-VM zu replizieren.
   a. Melden Sie sich beim primären Server an.

b. Schalten Sie die VM aus, für die ein Failover durchgeführt werden soll.

c. Klicken Sie in Hyper-V Manager mit der rechten Maustaste auf die ausgeschalteten VM, klicken Sie auf Replikation, und klicken Sie auf geplante Failover.

d. Klicken Sie auf Failover, um die letzten VM-Änderungen auf den Replikatserver zu übertragen.

3. Führen Sie bei Ausfall der primären VM ein ungeplantes Failover aus.

a. Melden Sie sich beim Replikatserver an.

b. Klicken Sie in Hyper-V Manager mit der rechten Maustaste auf eine Replikat-VM, klicken Sie auf Replikation und dann auf Failover.

c. Wählen Sie den zu verwendenden Wiederherstellungspunkt aus.

d. Klicken Sie auf Failover, um ein Failover der VM durchzuführen.

Bereitstellung von Hyper-V-Replikaten in einer Cluster-Umgebung

Erfahren Sie, wie Sie Hyper-V-Replikate mit Windows Server Failover Cluster bereitstellen und konfigurieren.

Voraussetzungen

- Sie müssen Hyper-V-Cluster auf demselben oder an verschiedenen geografischen Standorten haben, die als primäre und Replikatcluster dienen. Prüfen "Implementieren Sie Hyper-V Cluster" Entnehmen.
- Wenn separate Standorte verwendet werden, muss die Firewall an jedem Standort so konfiguriert werden, dass die Kommunikation zwischen dem primären und dem Replikatcluster möglich ist.
- Das Replikat-Cluster muss über genügend Speicherplatz zum Speichern der replizierten Workloads verfügen.

Einsatz

1. Aktivieren Sie Firewall-Regeln für alle Knoten eines Clusters. Führen Sie das folgende PowerShell-Cmdlet mit Administratorrechten auf allen Knoten sowohl im primären als auch im Replikatcluster aus.

```
# For Kerberos authentication
get-clusternode | ForEach-Object \{Invoke-command -computername $_.name
-scriptblock \{Enable-Netfirewallrule -displayname "Hyper-V Replica HTTP
Listener (TCP-In)"}}
```

```
# For Certificate authentication
get-clusternode | ForEach-Object \{Invoke-command -computername $_.name
-scriptblock \{Enable-Netfirewallrule -displayname "Hyper-V Replica
HTTPS Listener (TCP-In)"}}
```

2. Konfigurieren Sie das Replikat-Cluster.

a. Konfigurieren Sie den Hyper-V Replica Broker mit einem NetBIOS-Namen und einer IP-Adresse, die

als Verbindungspunkt zu dem Cluster verwendet werden sollen, der als Replikatcluster verwendet wird.

i. Öffnen Sie Failover Cluster Manager.

ii. Erweitern Sie den Cluster, klicken Sie auf Rollen, und klicken Sie im Bereich Aktionen auf Rolle konfigurieren.

iii. Wählen Sie auf der Seite Rolle auswählen die Option Hyper-V Replica Broker aus.

iv. Geben Sie den NetBIOS-Namen und die IP-Adresse an, die als Verbindungspunkt zum Cluster (Client-Zugriffspunkt) verwendet werden sollen.

v. Dieser Prozess erstellt eine Hyper-V Replica Broker-Rolle. Stellen Sie sicher, dass sie erfolgreich online ist.

b. Konfigurieren Sie die Replikationseinstellungen.

i. Klicken Sie mit der rechten Maustaste auf den Replikatbroker, der in den vorherigen Schritten erstellt wurde, und klicken Sie auf Replikationseinstellungen.

ii. Wählen Sie Diesen Cluster als Replikatserver aktivieren aus.

iii. Wählen Sie im Abschnitt Authentifizierung und Ports die Authentifizierungsmethode und den Port aus.

iv. Wählen Sie im Abschnitt Autorisierung und Speicher die Server aus, die VMs auf dieses Cluster replizieren dürfen. Geben Sie außerdem den Standardspeicherort an, an dem die replizierten VMs gespeichert werden.

Replizierung

Die Replikation ähnelt dem im Abschnitt beschriebenen Prozess "Replikat außerhalb einer Cluster-Umgebung".

Wo Sie weitere Informationen finden

Zusätzliche Ressourcen für Microsoft Windows und Hyper-V

- ONTAP-Konzepte
  https://docs.netapp.com/us-en/ontap/concepts/introducing-data-management-software-concept.html
- Best Practices für modernes SAN
  https://www.netapp.com/media/10680-tr4080.pdf
- Datenverfügbarkeit und Integrität von All-SAN-Arrays der NetApp mit der NetApp ASA
  https://www.netapp.com/pdf.html?item=/media/85671-tr-4968.pdf
- SMB-Dokumentation
  https://docs.netapp.com/us-en/ontap/smb-admin/index.html
- Erste Schritte mit Nano Server
  https://technet.microsoft.com/library/mt126167.aspx
- Was ist neu in Hyper-V auf Windows Server
  https://technet.microsoft.com/windows-server-docs/compute/hyper-v/what-s-new-in-hyper-v-on-windows