ONTAP tools für VMware vSphere konfigurieren

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Inhalt

ONTAP tools für VMware vSphere konfigurieren

Fügen Sie vCenter Serverinstanzen zu ONTAP tools hinzu

Fügen Sie vCenter Server-Instanzen zu ONTAP tools for VMware vSphere hinzu, um Ihre virtuellen Datenspeicher in Ihrer vCenter Server-Umgebung zu konfigurieren, zu verwalten und zu schützen. Beim Hinzufügen mehrerer vCenter Server-Instanzen sind benutzerdefinierte CA-Zertifikate für die sichere Kommunikation zwischen ONTAP tools for VMware und jeder vCenter Server-Instanz erforderlich.

Über diese Aufgabe

ONTAP tools integriert sich mit dem vCenter Server, sodass Speicheraufgaben wie Bereitstellung, Snapshots und Datenschutz direkt über den vSphere Client ausgeführt werden können.

Das Hinzufügen einer vCenter Serverinstanz zu ONTAP tools löst automatisch die folgenden Aktionen aus:

- ONTAP tools registriert das vCenter Client-Plug-in als Remote-Plug-in.
- Benutzerdefinierte Berechtigungen für die Plug-ins und APIs werden auf die vCenter Server-Instanz angewendet.
- Benutzerdefinierte Rollen werden zur Verwaltung der Benutzer erstellt.
- Das Plug-in erscheint als Verknüpfung auf der vSphere Benutzeroberfläche.

Bevor Sie beginnen

- Stellen Sie sicher, dass das vCenter Server-Zertifikat eine gültige Subject Alternative Name (SAN)-Erweiterung mit sowohl DNS- als auch IP-Adresseinträgen enthält. Beispiel:

  ```
  X509v3 extensions:
      X509v3 Subject Alternative Name:
          DNS: vcenter.example.com, DNS: vcenter, IP Address: 192.168.0.50
  ```

  Wenn das Zertifikat keine SAN-Erweiterung enthält oder die SAN-Erweiterung nicht die korrekten DNS- oder IP-Adresswerte enthält, können ONTAP tools-Operationen aufgrund von Zertifikatvalidierungsfehlern fehlschlagen.

- Die primäre Netzwerkkennung (PNID) des vCenter Server muss in den SAN-Details enthalten sein. Die PNID und der DNS-Name müssen identisch und im DNS auflösbar sein.
- Es wird empfohlen, den vCenter Server unter Verwendung seines vollqualifizierten Domainnamens (FQDN) bereitzustellen und sicherzustellen, dass der SAN im Zertifikat DNS Name=machine_FQDN enthält, um optimale Kompatibilität und Unterstützung zu gewährleisten.
- Weitere Informationen finden Sie in der VMware-Dokumentation:
  - "vSphere Certificate Requirements für verschiedene Lösungswege"
  - "Ersetzen Sie das vCenter-Maschinen-SSL-Zertifikat durch ein benutzerdefiniertes, von einer Zertifizierungsstelle signiertes Zertifikat"
  - "Fehler: Das Feld „Subject Alternate Name (SAN)“ enthält keine PNID. Bitte geben Sie ein gültiges Zertifikat an."

Falls kein FQDN verfügbar ist, können Sie die PNID auf die IP-Adresse setzen und die IP-Adresse in das SAN einbinden. Dies wird jedoch von VMware nicht empfohlen.

Schritte

1. Einen Webbrowser öffnen und zur folgenden URL gehen:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **vCenters** > **Hinzufügen**, um die vCenter Serverinstanzen einzubinden. Geben Sie Ihre vCenter IP-Adresse oder Ihren Hostnamen, Ihren Benutzernamen, Ihr Passwort und die Portdetails an.
4. In den erweiterten Optionen wird das vCenter Server-Zertifikat automatisch abgerufen (autorisiert) oder es kann manuell hochgeladen werden.

Sie benötigen kein Administratorkonto, um vCenter Instanzen zu ONTAP tools hinzuzufügen. Eine benutzerdefinierte Rolle mit eingeschränkten Berechtigungen kann auch ohne Administratorkonto erstellt werden. Weitere Informationen sind unter "Verwendung von vCenter Server RBAC mit ONTAP tools for VMware vSphere 10" zu finden.

Registrieren Sie den VASA Provider bei einer vCenter Server-Instanz in ONTAP tools

ONTAP tools für VMware vSphere ermöglichen die Registrierung des VASA Provider bei einer vCenter Server-Instanz. Dadurch werden speicherrichtlinienbasierte Verwaltung, vVols Unterstützung und die Integration mit VMware Live Site Recovery Appliances auf ONTAP Systemen ermöglicht.

Die VASA-Provider-Einstellungen zeigen den Registrierungsstatus für den ausgewählten vCenter Server an.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie unter dem Abschnitt „Plug-ins“ **Shortcuts** > **NetApp ONTAP tools** aus.
3. Wählen Sie **Einstellungen** > **VASA Provider Einstellungen**. Die ONTAP tools zeigen den Registrierungsstatus des VASA Provider als nicht registriert an.
4. Die Schaltfläche **Registrieren** dient zur Registrierung des VASA Provider.
5. Geben Sie einen Namen und die Zugangsdaten für den VASA Provider ein. Der Benutzername darf nur Buchstaben, Zahlen und Unterstriche enthalten. Das Passwort muss zwischen 8 und 256 Zeichen lang sein.
6. **Registrieren** auswählen.
7. Nach erfolgreicher Registrierung und Aktualisierung der Seite zeigen die ONTAP tools den Status, den Namen und die Version des registrierten VASA Provider an.

Was kommt als Nächstes

Es sollte überprüft werden, ob der integrierte VASA Provider unter VASA Provider vom vCenter Client aufgeführt ist:

Schritte

1. Zur vCenter Server-Instanz wechseln.
2. Melden Sie sich mit den Administrator-Zugangsdaten an.
3. Wählen Sie **Speicheranbieter** > **Konfigurieren**. Es sollte überprüft werden, ob der integrierte VASA Provider korrekt aufgeführt ist.

Das NFS VAAI Plug-in mit ONTAP tools installieren

Das NFS vStorage API für Array Integration (NFS VAAI) Plug-in verbindet VMware vSphere mit NFS-Speicherarrays. Mit ONTAP tools for VMware vSphere lässt sich das VAAI Plug-in installieren. Dadurch übernimmt das NFS-Speicherarray bestimmte Speicheroperationen anstelle der ESXi-Hosts.

Bevor Sie beginnen

- Laden Sie das "NetApp NFS Plug-in für VMware VAAI" Installationspaket herunter.
- Stellen Sie sicher, dass Sie ESXi-Hosts mit vSphere 7.0 U3 (neuester Patch oder höher) und ONTAP 9.14.1 oder höher verwenden.
- Einen NFS-Datenspeicher einbinden.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Wählen Sie unter dem Abschnitt „Plug-ins“ **Shortcuts** > **NetApp ONTAP tools** aus.
3. **Einstellungen** > **NFS VAAI Tools** auswählen.
4. Wenn Sie das VAAI-Plug-in bereits auf vCenter Server hochgeladen haben, wählen Sie in **Vorhandene Version** die Option **Ändern**. Wenn nicht, wählen Sie **Hochladen**.
5. Durchsuchen und wählen Sie die `.vib` Datei aus und wählen Sie **Hochladen**, um die Datei in ONTAP tools hochzuladen.
6. Wählen Sie **Auf ESXi-Host installieren**, wählen Sie den ESXi-Host aus, auf dem Sie das NFS VAAI Plug-in installieren möchten, und wählen Sie dann **Installieren**.

   Der vSphere Web Client zeigt nur die ESXi-Hosts an, auf denen das Plug-in installiert werden kann. Der Installationsfortschritt ist im Bereich „Letzte Aufgaben“ sichtbar.

7. Der ESXi-Host wird nach der Installation manuell neu gestartet.

   Nach dem Neustart des ESXi-Hosts erkennt ONTAP tools for VMware vSphere das NFS VAAI-Plug-in automatisch und aktiviert es.

Was kommt als Nächstes?

Nach der Installation des NFS VAAI Plug-ins und dem Neustart Ihres ESXi-Hosts sind die NFS-Exportrichtlinien für VAAI Copy Offload zu konfigurieren. Die Exportrichtlinienregeln müssen folgende Anforderungen erfüllen:

- Das entsprechende ONTAP Volume erlaubt NFSv4-Aufrufe.
- Der Root-Benutzer bleibt Root und NFSv4 ist in allen Verbindung Parent-Volumes erlaubt.
- Die Option für die VAAI-Unterstützung ist auf dem entsprechenden NFS-Server festgelegt.

Weitere Informationen finden Sie im "Die korrekten NFS-Exportrichtlinien für VAAI Copy Offload konfigurieren"

KB-Artikel.

Verwandte Informationen

"Unterstützung für VMware vStorage über NFS"

"NFSv4.0 aktivieren oder deaktivieren"

"ONTAP Unterstützung für NFSv4.2"

Konfigurieren der ESXi-Hosteinstellungen in ONTAP tools

Die Konfiguration der Multipath- und Zeitüberschreitungseinstellungen des ESXi Servers trägt zur Aufrechterhaltung der Datenverfügbarkeit und -integrität bei. Dadurch wird ein automatisches Failover auf einen Backup-Speicherpfad ermöglicht, falls der primäre Pfad nicht verfügbar ist.

Multipath- und Zeitüberschreitungseinstellungen des ESXi-Servers konfigurieren

ONTAP tools für VMware vSphere prüfen und konfigurieren die Multipath-Einstellungen des ESXi-Hosts sowie die HBA-Zeitüberschreitungseinstellungen, die am besten mit NetApp Storage-Systemen funktionieren.

Über diese Aufgabe

Dieser Vorgang kann je nach Konfiguration und Systemauslastung einige Zeit in Anspruch nehmen. Der Fortschritt ist im Bereich „Letzte Aufgaben“ einsehbar.

Schritte

1. Wählen Sie auf der Startseite des VMware vSphere Webclients die Option **Hosts und Cluster**.
2. Auf der Seite „Verknüpfungen“ des VMware vSphere Webclients im Abschnitt „Plug-ins“ **NetApp ONTAP tools** auswählen.
3. In der Übersicht (Dashboard) des ONTAP tools for VMware vSphere Plug-ins befindet sich die Karte **ESXi Host compliance**.
4. Den Link **Empfohlene Einstellungen anwenden** auswählen.
5. Im Fenster **Empfohlene Host-Einstellungen anwenden** die Hosts auswählen, die auf die von NetApp empfohlenen Einstellungen aktualisiert werden sollen, und **Weiter** auswählen.

   Sie können den ESXi Host erweitern, um die aktuellen Werte anzuzeigen.

6. Auf der Einstellungsseite können die empfohlenen Werte nach Bedarf ausgewählt werden.
7. Im Zusammenfassungsbereich die Werte überprüfen und **Fertigstellen** auswählen. Der Fortschritt lässt sich im Bereich „Letzte Aufgaben“ verfolgen.

ESXi Hostwerte festlegen

Mit ONTAP tools for VMware vSphere lassen sich Zeitüberschreitungen und andere Werte auf ESXi Hosts für optimale Leistung und Failover festlegen. Diese Werte werden auf Grundlage von NetApp Tests festgelegt.

Auf einem ESXi Host können folgende Werte festgelegt werden:

HBA/CNA Adaptereinstellungen

Legt die folgenden Parameter auf Standardwerte fest:

- Disk.QFullSampleSize
- Disk.QFullThreshold
- Emulex FC HBA Zeitüberschreitungen
- QLogic FC HBA Zeitüberschreitungen

MPIO Einstellungen

Die MPIO-Einstellungen wählen die besten Pfade für NetApp Storage-Systeme aus. Die MPIO-Einstellungen wählen den besten Pfad aus und verwenden ihn.

In Umgebungen mit hohen Leistungsanforderungen oder beim Testen mit einem einzelnen LUN-Datenspeicher sollte die Lastausgleich-Einstellung der Round-Robin (VMW_PSP_RR) Pfadauswahlrichtlinie (PSP) angepasst werden, um die Leistung zu verbessern. Der Standardwert für IOPS ist von 1000 auf 1 zu setzen.

Die MPIO-Einstellungen gelten nicht für die Protokolle NVMe, NVMe/FC und NVMe/TCP.

NFS-Einstellungen

Parameter	Diesen Wert auf … festlegen.
Net.TcpipHeapSize	32
Net.TcpipHeapMax	1024 MB
NFS.MaxVolumes	256
NFS41.MaxVolumes	256
NFS.MaxQueueDepth	128 oder höher
NFS.HeartbeatMaxFailures	10
NFS.HeartbeatFrequency	12
NFS.HeartbeatTimeout	5

Konfigurieren Sie ONTAP Benutzerrollen und -Berechtigungen für ONTAP tools

In diesem Abschnitt werden ONTAP-Benutzerrollen und Privileges für Storage-Backends mit ONTAP tools for VMware vSphere und ONTAP System Manager konfiguriert. Rollen können mithilfe der bereitgestellten JSON-Dateien zugewiesen, Benutzer und Rollen manuell erstellt und die minimal erforderlichen Privileges für Nicht-Admin-Konten angewendet werden.

Bevor Sie beginnen

- Die ONTAP Privileges Datei aus ONTAP tools for VMware vSphere kann über *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* heruntergeladen werden. Nach dem Herunterladen der ZIP-Datei sind zwei JSON-Dateien enthalten. Die ASA r2-spezifische JSON-Datei

ist bei der Konfiguration eines ASA r2-Systems zu verwenden.

> Sie können Benutzer auf Clusterebene oder direkt auf Ebene der Storage Virtual Machines (SVMs) erstellen. Wenn die Datei user_roles.json nicht verwendet wird, ist sicherzustellen, dass der Benutzer über die minimal erforderlichen SVM-Berechtigungen verfügt.

- Mit Administratorrechten für das Storage-Backend anmelden.

Schritte

1. Extrahieren Sie die Datei *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*, die Sie heruntergeladen haben.
2. Auf den ONTAP System Manager wird über die Cluster-Management-IP-Adresse des Clusters zugegriffen.
3. Melden Sie sich mit Administratorrechten am Cluster an. Zur Konfiguration eines Benutzers:
   a. Zur Konfiguration eines Cluster ONTAP tools Benutzers die Seite **Cluster** > **Einstellungen** > **Benutzer und Rollen** auswählen.
   b. Zur Konfiguration eines SVM ONTAP tools Benutzers wird der Bereich **Storage SVM** > **Einstellungen** > **Benutzer und Rollen** ausgewählt.
   c. Unter Benutzer **Hinzufügen** auswählen.
   d. Im Dialogfeld **Benutzer hinzufügen** die Option **Virtualisierungsprodukte** auswählen.
   e. **Durchsuchen** auswählen, um die ONTAP Privileges JSON-Datei auszuwählen und hochzuladen. Für Systeme ohne ASA r2 die Datei users_roles.json auswählen und für ASA r2-Systeme die Datei users_roles_ASAr2.json auswählen.

      ONTAP tools füllt das Produktfeld automatisch aus.

   f. Die Produktfunktionalität **VSC, VASA Provider und SRA** ist aus der Dropdown-Liste auszuwählen.

      ONTAP tools füllt das Feld **Rolle** automatisch basierend auf der ausgewählten Produktfunktion aus.

   g. Den erforderlichen Benutzernamen und das Passwort eingeben.
   h. Wählen Sie die Privileges (Discovery, Create Storage, Modify Storage, Destroy Storage, NAS/SAN Role) aus, die der Benutzer benötigt, und wählen Sie dann **Hinzufügen**.

ONTAP tools fügt die neue Rolle und den neuen Benutzer hinzu. Die Privileges der konfigurierten Rolle sind einsehbar.

Anforderungen an die SVM Aggregate-Zuordnung

Bei der Bereitstellung von Datenspeichern mithilfe von SVM-Benutzeranmeldeinformationen erstellt ONTAP tools for VMware vSphere Volumes auf dem in der Datastores-POST-API angegebenen Aggregat. ONTAP verhindert, dass SVM-Benutzer Volumes auf Aggregaten erstellen, die der SVM nicht zugeordnet sind. Vor dem Erstellen von Volumes ist die SVM den erforderlichen Aggregaten mithilfe der ONTAP REST API oder CLI zuzuordnen.

REST API:

```
PATCH "/api/svm/svms/f16f0935-5281-11e8-b94d-005056b46485"
'{"aggregates":{"name":["aggr1","aggr2","aggr3"]}}'
```

ONTAP CLI:

```
sti115_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver        Aggregate      State         Size Type    SnapLock
Type-------------- -------------- ------- ---------- -------
--------------svm_test       sti115_vsim_ucs630f_aggr1
online     10.11GB vmdisk  non-snaplock
```

ONTAP Benutzer und Rolle manuell erstellen

Benutzer und Rollen manuell ohne die JSON-Datei erstellen.

1. Auf den ONTAP System Manager wird über die Cluster-Management-IP-Adresse des Clusters zugegriffen.
2. Melden Sie sich mit Administratorrechten im Cluster an.
   a. Zur Konfiguration der ONTAP tools Rollen im Cluster **Cluster** > **Einstellungen** > **Benutzer und Rollen** auswählen.
   b. Zur Konfiguration der Cluster-SVM-ONTAP-Tools-Rollen in ONTAP **Storage SVM** > **Einstellungen** > **Benutzer und Rollen** auswählen.
3. Rollen erstellen:
   a. Unter der Tabelle **Rollen Hinzufügen** auswählen.
   b. Die Details zu **Rollenname** und **Rollenattributen** eingeben.

      Fügen Sie den **REST API-Pfad** hinzu und wählen Sie den Zugriff aus der Dropdown-Liste aus.

   c. Alle benötigten APIs hinzufügen und die Änderungen speichern.
4. Benutzer erstellen:
   a. Wählen Sie unter der Tabelle **Benutzer** die Option **Hinzufügen**.
   b. Im Dialogfeld **Benutzer hinzufügen System Manager** auswählen.
   c. Den **Benutzernamen** eingeben.
   d. **Rolle** aus den im Schritt **Rollen erstellen** erstellten Optionen auswählen.
   e. Geben Sie die Anwendungen an, denen Sie Zugriff gewähren möchten, sowie das Authentifizierungsverfahren. ONTAPI und HTTP sind die erforderlichen Anwendungen, und der Authentifizierungstyp ist **Passwort**.
   f. Das **Passwort für den Benutzer** festlegen und den Benutzer **speichern**.

Liste der Mindestberechtigungen, die für einen globalen Clusterbenutzer ohne Administratorrechte erforderlich sind

Diese Seite listet die Mindestberechtigungen auf, die für einen globalen Clusterbenutzer ohne Administratorrechte und ohne JSON-Datei erforderlich sind. Wenn sich ein Cluster im lokalen Bereich befindet, sollte die JSON-Datei zur Erstellung von Benutzern verwendet werden, da ONTAP tools for VMware vSphere für die Bereitstellung auf ONTAP mehr als nur die Leseberechtigungen benötigt.

Auf Funktionen kann über APIs zugegriffen werden:

API	Zugriffsebene	Wird verwendet für
/api/cluster	Schreibgeschützt	Cluster-Konfigurationsentdeckung
/api/cluster/licensing/licenses	Schreibgeschützt	Lizenzprüfung für protokollspezifische Lizenzen
/api/cluster/nodes	Schreibgeschützt	Plattformtyperkennung
/api/security/accounts	Schreibgeschützt	Ermittlung von Privilegien
/api/security/roles	Schreibgeschützt	Ermittlung von Privilegien
/api/storage/aggregates	Schreibgeschützt	Überprüfung des Aggregatspeicherplatzes während der Datenspeicher-/Volume-Bereitstellung
/api/storage/cluster	Schreibgeschützt	Um die Speicherplatz- und Effizienzdaten auf Clusterebene abzurufen
/api/storage/disks	Schreibgeschützt	Die mit einem Aggregat verbundenen Festplatten abrufen
/api/storage/qos/policies	Lesen/Erstellen/Ändern	QoS und VM-Richtlinienverwaltung
/api/svm/svms	Schreibgeschützt	Die SVM-Konfiguration wird abgerufen, wenn der Cluster lokal hinzugefügt wird.
/api/network/ip/interfaces	Schreibgeschützt	Storage-Backend hinzufügen, um den Management-LIF-Bereich als Cluster/SVM zu identifizieren
/api/storage/availability-zones	Schreibgeschützt	SAZ-Erkennung. Gültig ab ONTAP 9.16.1 und für ASA r2 Systeme.
/api/cluster/metrocluster	Schreibgeschützt	Zeigt MetroCluster Status- und Konfigurationsdetails an.

ONTAP tools für VMware vSphere ONTAP API-basierter, clusterbezogener Benutzer erstellen

Für PATCH-Operationen und automatische Rollbacks auf Datenspeichern sind Privileges zum Ermitteln, Erstellen, Ändern und zerstören erforderlich. Fehlende Berechtigungen können zu Problemen im Workflow und bei der Datenbereinigung führen.

Ein auf ONTAP API basierender Benutzer mit Berechtigungen für Discovery, Erstellen, Ändern und Zerstören kann ONTAP tools Workflows verwalten.

Zum Erstellen eines Clusterbenutzers mit allen oben genannten Berechtigungen sind die folgenden Befehle auszuführen:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all

security login rest-role create -role <role-name> -api
```

```
/api/private/cli/snapmirror -access all

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all

security login rest-role create -role <role-name> -api /api/storage/luns
-access all

security login rest-role create -role <role-name> -api
/api/storage/namespaces -access all

security login rest-role create -role <role-name> -api
/api/storage/qos/policies -access all

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create
```

```
security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify

security login rest-role create -role <role-name> -api /api/cluster
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/licensing/licenses -access readonly

security login rest-role create -role <role-name> -api /api/cluster/nodes
-access readonly

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly

security login rest-role create -role <role-name> -api
/api/network/fc/ports -access readonly

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly
```

```
security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/aggregates -access readonly

security login rest-role create -role <role-name> -api
/api/storage/cluster -access readonly

security login rest-role create -role <role-name> -api /api/storage/disks
-access readonly

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly

security login rest-role create -role <role-name> -api
/api/cluster/metrocluster -access readonly
```

Führen Sie für ONTAP-Versionen 9.16.0 und höher zusätzlich folgenden Befehl aus:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all
```

Für ASA r2-Systeme mit ONTAP Versionen 9.16.1 und höher führen Sie den folgenden Befehl aus:

```
security login rest-role create -role <role-name> -api
/api/storage/availability-zones -access readonly
```

Erstellung eines ONTAP tools for VMware vSphere ONTAP API-basierten, SVM-beschränkten Benutzers

Führen Sie die folgenden Befehle aus, um einen SVM-Benutzer mit allen Privileges zu erstellen:

```
security login rest-role create -role <role-name> -api
/api/application/consistency-groups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/private/cli/snapmirror -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/igroups -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/lun-maps -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/relationships -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/volumes -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/luns
-access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
```

```
/api/storage/namespaces -access all -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/cluster/schedules -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/snapmirror/policies -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/clone -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/file/copy -access read_create -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/support/ems/application-logs -access read_create -vserver <vserver-
name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/services -access read_modify -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/jobs
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/cluster/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/name-
services/name-mappings -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ethernet/ports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/fc/logins -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/network/ip/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/nfs/kerberos/interfaces -access readonly -vserver <vserver-
```

```
name>

security login rest-role create -role <role-name> -api
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/security/accounts -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/security/roles
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/storage/qtrees
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/quota/reports -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/peers
-access readonly -vserver <vserver-name>

security login rest-role create -role <role-name> -api /api/svm/svms
-access readonly -vserver <vserver-name>
```

Führen Sie für ONTAP-Versionen 9.16.0 und höher zusätzlich folgenden Befehl aus:

```
security login rest-role create -role <role-name> -api
/api/storage/storage-units -access all -vserver <vserver-name>
```

Um einen neuen API-basierten Benutzer mithilfe der zuvor erstellten API-basierten Rollen zu erstellen, führen Sie folgenden Befehl aus:

```
security login create -user-or-group-name <user-name> -application http
-authentication-method password -role <role-name> -vserver <cluster-or-
vserver-name>
```

Beispiel:

```
security login create -user-or-group-name testvpsraall -application http
-authentication-method password -role
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver C1_sti160-cluster_
```

Führen Sie den folgenden Befehl aus, um das Konto zu entsperren und den Zugriff auf die Managementoberfläche zu aktivieren:

```
security login unlock -user <user-name> -vserver <cluster-or-vserver-name>
```

Beispiel:

```
security login unlock -username testvpsraall -vserver C1_sti160-cluster
```

Upgrade ONTAP tools für VMware vSphere 10.1 Benutzer auf 10.3 Benutzer

Für ONTAP tools for VMware vSphere 10.1 Benutzer mit einem Cluster-Benutzer, der mithilfe der JSON-Datei erstellt wurde, können die folgenden ONTAP CLI-Befehle mit Benutzer-Admin-Privileges zum Upgrade auf die Version 10.3 verwendet werden.

Zu den Produktfunktionen:

- VSC
- VSC und VASA Provider
- VSC und SRA
- VSC, VASA Provider und SRA.

Cluster-Privileges:

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all

Für Benutzer von ONTAP tools for VMware vSphere 10.1, die einen SVM-benutzer mit Hilfe der json-Datei erstellt haben, können die ONTAP CLI-Befehle mit Administratorrechten verwendet werden, um auf die Version 10.3 zu aktualisieren.

SVM Privileges:

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map show" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme show-interface" -access read -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map add" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme namespace delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem delete" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem host remove" -access all -vserver <vserver-name>

security login role create -role <existing-role-name> -cmddirname "vserver nvme subsystem map remove" -access all -vserver <vserver-name>

Um die folgenden Befehle zu aktivieren, müssen die Befehle *vserver nvme namespace show* und *vserver nvme subsystem show* zur bestehenden Rolle hinzugefügt werden.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Upgrade ONTAP tools für VMware vSphere 10.3 Benutzer auf 10.4 Benutzer

Ab ONTAP 9.16.1 wird der ONTAP tools for VMware vSphere 10.3 Benutzer auf 10.4 Benutzer aktualisiert.

Für ONTAP tools for VMware vSphere 10.3 Benutzer mit einem cluster-scoped Benutzer, der mit der JSON-Datei erstellt wurde, und ONTAP Version 9.16.1 oder höher empfiehlt sich die Verwendung des ONTAP CLI-Befehls mit Admin-Benutzerrechten für das Upgrade auf die Version 10.4.

Zu den Produktfunktionen:

- VSC
- VSC und VASA Provider
- VSC und SRA
- VSC, VASA Provider und SRA.

Cluster-Privileges:

```
security login role create -role <existing-role-name> -cmddirname "storage
availability-zone show" -access all
```

Fügen Sie ein Speicher-Backend zu ONTAP tools hinzu

Mit ONTAP tools für VMware vSphere lassen sich Storage-Backends für Ihre ESXi-Hosts hinzufügen und verwalten. Cluster oder SVMs können eingebunden, MetroCluster-Support aktiviert und Zertifikate für eine sichere Verbindung validiert werden. Storage-Backends lassen sich mit ONTAP tools Manager oder dem vSphere Client konfigurieren, der Zertifikatsstatus kann überwacht und Ressourcen nach Clusteränderungen manuell erneut erkannt werden.

Um ein lokales Storage-Backend hinzuzufügen, werden Cluster- oder SVM-Anmeldeinformationen in der ONTAP tools-Oberfläche verwendet. Lokale Storage-Backends sind nur für den ausgewählten vCenter Server verfügbar. ONTAP tools ordnet SVMs dem vCenter Server für vVols oder die VMFS-Datenspeicherverwaltung zu. Für VMFS-Datenspeicher und SRA-Workflows können SVM-Anmeldeinformationen verwendet werden, ohne einen Cluster global zuzuordnen.

Zum Hinzufügen eines globalen Storage-Backends werden ONTAP Cluster-Anmeldeinformationen im ONTAP tools Manager verwendet. Globale Storage-Backends ermöglichen Erkennungs-Workflows zur Identifizierung der für die vVol-Verwaltung benötigten Clusterressourcen. In mandantenfähigen Umgebungen kann ein SVM-

Benutzer lokal hinzugefügt werden, um vVols-Datenspeicher zu verwalten.

Weitere Informationen zu globalen und lokalen Speichersystemen finden Sie im KB-Artikel: "OTV 10: Was ist der globale und lokale Gültigkeitsbereich des Storage-Backends".

Wenn die MetroCluster Unterstützung in ONTAP aktiviert ist, sind sowohl Quell- als auch Zielcluster als lokale oder globale Storage Backends einzubinden.

Bevor Sie beginnen

Es sollte überprüft werden, ob das Zertifikat ein gültiges Subject Alternative Name (SAN)-Feld enthält. ONTAP Systeme verwenden das SAN-Feld zur Identifizierung von Cluster- und SVM-Management-LIFs.

Verwendung von ONTAP tools Manager

In einer mandantenfähigen Umgebung kann ein Storage Backend Cluster global und SVM lokal hinzugefügt werden, um die SVM-Benutzeranmeldeinformationen zu verwenden.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. **Storage Backends** in der Seitenleiste auswählen.
4. Das Speicher-Backend wird hinzugefügt, wobei die Server-IP-Adresse oder der FQDN, der Benutzername und das Passwort anzugeben sind.

   IPv4- und IPv6-Adressverwaltungs-LIFs sind unterstützt.

5. Die ONTAP Cluster-Zertifikate werden automatisch abgerufen und das Zertifikat autorisiert, oder es kann manuell hochgeladen werden, indem zu seinem Speicherort navigiert wird.

   Bei Bedarf kann die Validierung des Subject Alternative Name (SAN) über die Wartungskonsole deaktiviert werden. Anleitungen finden sich unter "Zertifikatvalidierungsflag ändern".

6. Wenn das hinzugefügte Storage-Backend Teil einer MetroCluster Konfiguration ist, zeigt ONTAP tools Manager eine Pop-up-Meldung an, um das Peered Cluster hinzuzufügen. **Add** auswählen und die Details für das MetroCluster Peer-Storage-Backend angeben.

   Nachdem das ONTAP System einen Switchover und Switchback durchgeführt hat, sollte die ONTAP tools discovery manuell ausgeführt werden.

Verwendung der vSphere Client-Benutzeroberfläche

vVols Datenspeicher unterstützen das direkte Hinzufügen eines SVM-Benutzers über die vSphere Client-Benutzeroberfläche nicht.

1. Melden Sie sich beim vSphere Client an.
2. Auf der Seite „Shortcuts“ im Abschnitt „Plug-ins“ ist **NetApp ONTAP tools** auszuwählen.
3. **Storage Backends** in der Seitenleiste auswählen.
4. Das Speicher-Backend hinzufügen und die Server-IP-Adresse, den Benutzernamen, das Passwort und die Portdetails angeben.

   Sie können ein Storage-Backend mithilfe clusterbasierter Anmeldeinformationen mit entweder IPv4- oder IPv6-Management-LIFs hinzufügen. Zum direkten Hinzufügen eines SVM-Benutzers sind SVM-basierte Anmeldeinformationen zusammen mit einem SVM-Management-LIF bereitzustellen. Ist ein Cluster bereits eingebunden, kann ein SVM-Benutzer aus diesem Cluster nicht erneut eingebunden werden.

5. Die ONTAP Cluster-Zertifikate werden automatisch abgerufen und das Zertifikat autorisiert, oder es

kann manuell hochgeladen werden, indem zu seinem Speicherort navigiert wird.

6. Wenn das hinzugefügte Storage-Backend Teil der MetroCluster Konfiguration ist, zeigt ONTAP tools den Bildschirm **Add MetroCluster peer** an. **Add peer** auswählen, um das Peer-Storage-Backend hinzuzufügen.

> Nachdem das ONTAP System einen Switchover und Switchback durchgeführt hat, sollte die ONTAP tools discovery manuell ausgeführt werden.

ONTAP tools listet das neu hinzugefügte Storage Backend auf der Seite **Storage backends** auf. Läuft ein Zertifikat in 30 Tagen oder weniger ab, zeigt ONTAP tools eine Warnung in der Spalte für das Ablaufdatum des Zertifikats an. Nach Ablauf markiert ONTAP tools das Storage Backend als unbekannt, da keine Verbindung zum Storage System hergestellt werden kann.

Verwandte Informationen

"OTV 10: Was ist der globale und lokale Gültigkeitsbereich des Storage-Backends"

"Konfiguration der Cluster zu einer MetroCluster Konfiguration"

Verknüpfen Sie ein Storage-Backend mit einer vCenter Server-Instanz in ONTAP tools

Ein Storage-Backend wird mit einer vCenter Server-Instanz verknüpft, um den Zugriff für alle vCenter Server-Instanzen zu ermöglichen. Bei einer MetroCluster Konfiguration ist beim Verknüpfen eines Storage-Backend-Clusters sicherzustellen, dass auch dessen Peer-Cluster mit dem vCenter Server verknüpft wird.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie vCenter aus der Seitenleiste.
4. Wählen Sie die vertikalen Auslassungspunkte neben der vCenter Serverinstanz aus, die Sie mit den Speicher-Backends verbinden möchten.
5. Wählen Sie im Dropdown-Menü das Speichersystem aus, das Sie der ausgewählten vCenter Server-Instanz zuordnen möchten.

Konfigurieren Sie Netzwerkzugriff in ONTAP tools

Standardmäßig werden alle vom ESXi-Host ermittelten IP-Adressen automatisch zur Exportrichtlinie hinzugefügt, es sei denn, Sie konfigurieren Netzwerkzugriff. Die Exportrichtlinie kann so angepasst werden, dass der Zugriff nur von bestimmten IP-Adressen zugelassen wird. Wenn ein ausgeschlossener ESXi-Host versucht, einen Mount-Vorgang durchzuführen, schlägt der Vorgang fehl.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. **NetApp ONTAP tools** auf der Seite „Shortcuts“ im Abschnitt „Plug-ins“ auswählen.
3. Im linken Bereich von ONTAP tools zu **Einstellungen** > **Netzwerkzugriff verwalten** > **Bearbeiten** wechseln.

   Um mehrere IP-Adressen hinzuzufügen, die Liste mit Kommas, Bereichen, Classless Inter-Domain Routing (CIDR) oder einer Kombination aus allen drei trennen.

4. **Speichern** auswählen.

Erstellen Sie einen Datenspeicher in ONTAP tools

Wenn ein Datenspeicher auf Hostclusterebene erstellt wird, bindet ONTAP tools ihn auf allen Zielhosts ein und die Aktion wird nur ermöglicht, wenn die erforderlichen Berechtigungen vorhanden sind.

Interoperabilität zwischen nativen Datenspeichern mit vCenter Server und ONTAP tools verwalteten Datenspeichern

Ab ONTAP tools für VMware vSphere 10.4 erstellt ONTAP tools verschachtelte igroups für Datenspeicher, wobei übergeordnete igroups spezifisch für die Datenspeicher sind und untergeordnete igroups den Hosts zugeordnet werden. Flache igroups können im ONTAP System Manager erstellt und zur Erstellung von VMFS Datenspeichern verwendet werden, ohne ONTAP tools zu nutzen. Weitere Informationen sind unter "SAN-Initiatoren und iGroups verwalten" verfügbar.

Nach dem Onboarding des Speichers und der Ausführung der Datenspeichererkennung ändert ONTAP tools flache Igroups in VMFS-Datenspeichern in verschachtelte Igroups. Die früheren flachen Igroups können nicht mehr zur Erstellung neuer Datenspeicher verwendet werden. Die ONTAP tools-Oberfläche oder die REST API kann genutzt werden, um verschachtelte Igroups wiederzuverwenden.

Einen vVols Datenspeicher erstellen

Ab ONTAP tools for VMware vSphere 10.3 ist es möglich, auf ASA r2 Systemen einen vVols Datastore mit Platzersparnis als thin.vVol zu erstellen. Der VASA Provider erstellt beim Anlegen des vVol Datastores einen Container und die gewünschten Protokollendpunkte. Der VASA Provider weist diesem Container keine Backing Volumes zu.

Bevor Sie beginnen

- Stellen Sie sicher, dass keine Root-Aggregate auf die SVM abgebildet werden.
- Stellen Sie sicher, dass der VASA Provider beim ausgewählten vCenter registriert ist.
- Im ASA r2 Speichersystem sollte die SVM dem Aggregat für den SVM-Benutzer zugeordnet werden.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem, einen Hostcluster oder ein Rechenzentrum und wählen Sie **NetApp ONTAP tools** > **Datenspeicher erstellen**.
3. Wählen Sie vVols als **Datenspeichertyp** aus.
4. Den **Datenspeichernamen** und das **Protokoll** angeben.

   Das ASA r2 System unterstützt die iSCSI und FC Protokolle für vVols.

5. Die Storage-VM auswählen, auf der der Datenspeicher erstellt werden soll.
6. Unter den erweiterten Optionen:
   - Wenn Sie die **Benutzerdefinierte Exportrichtlinie** auswählen, ist sicherzustellen, dass die Erkennung in vCenter für alle Objekte durchgeführt wird. Die Verwendung dieser Option wird nicht empfohlen.
   - Sie können einen **benutzerdefinierten Initiatorgruppen**-Namen für die iSCSI- und FC-Protokolle auswählen.

     Im ASA r2 Speichersystemtyp SVM werden keine Speichereinheiten (LUN/Namespace) erstellt, da der Datenspeicher nur ein logischer Container ist.

7. Im Bereich **Speicherattribute** können neue Volumes erstellt oder vorhandene Volumes verwendet werden. Es ist jedoch nicht möglich, diese beiden Volume-Typen zu einem vVols Datenspeicher zu kombinieren.

   Beim Erstellen eines neuen Volumes können Sie QoS für den Datenspeicher aktivieren. Standardmäßig wird für jede LUN-Erstellungsanforderung ein Volume erstellt. Überspringen Sie diesen Schritt für vVols Datenspeicher auf ASA r2-Speichersystemen.

8. Die Auswahl im Bereich **Übersicht** kann im **Summary**-Bereich überprüft werden, anschließend steht **Fertigstellen** zur Verfügung.

Einen NFS Datenspeicher erstellen

Ein NFS-Datenspeicher verbindet ESXi Hosts über das NFS-Protokoll mit gemeinsam genutztem Speicher. Sie sind einfach und flexibel und werden in VMware vSphere Umgebungen verwendet.

Schritte

1. Melden Sie sich beim vSphere Client an.

2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem, einen Hostcluster oder ein Rechenzentrum und wählen Sie **NetApp ONTAP tools** > **Datenspeicher erstellen**.
3. Im Feld **Datenspeichertyp** NFS auswählen.
4. Im Bereich **Name und Protokoll** werden der Name, die Größe und die Protokollinformationen des Datenspeichers eingegeben. In den erweiterten Optionen werden **Datenspeichercluster** und **Kerberos-Authentifizierung** ausgewählt.

   Die Kerberos-Authentifizierung ist nur verfügbar, wenn das NFS 4.1 Protokoll ausgewählt ist.

5. Im Bereich **Speicher** sind **Plattform** und **Speicher-VM** auszuwählen.
6. Wenn unter den erweiterten Optionen **Benutzerdefinierte Exportrichtlinie** ausgewählt wird, erfolgt die Erkennung in vCenter für alle Objekte. Es wird empfohlen, diese Option nicht zu verwenden.

   Es ist nicht möglich, einen NFS-Datenspeicher mit der Standard- oder Root-Volume-Richtlinie der SVM zu erstellen.

   - In den erweiterten Optionen ist die Umschaltfläche **Asymmetrisch** nur sichtbar, wenn im Plattform-Dropdown Leistung oder Kapazität ausgewählt ist.
   - Wenn im Dropdown-Menü „Plattform“ die Option „**Beliebig**“ ausgewählt wird, sind alle SVMs im vCenter sichtbar. Plattform und Asymmetrie-Flag haben keinen Einfluss auf die Sichtbarkeit.
7. Im Bereich **Speicherattribute** das Aggregat für die Volume-Erstellung auswählen. In den erweiterten Optionen **Speicherplatzreservierung** und **QoS aktivieren** nach Bedarf auswählen.
8. Die Auswahlen im Bereich **Zusammenfassung** werden angezeigt, anschließend ist **Fertigstellen** auszuwählen.

ONTAP tools erstellt den NFS-Datenspeicher und bindet ihn auf allen Hosts ein.

Einen VMFS Datenspeicher erstellen

VMFS ist ein Cluster-Dateisystem zum Speichern von Dateien virtueller Maschinen. Mehrere ESXi-Hosts können gleichzeitig auf dieselben VM-Dateien zugreifen, um vMotion und Hochverfügbarkeitsfunktionen zu ermöglichen.

Auf einem geschützten Cluster:

- Sie können nur VMFS-Datenspeicher erstellen. Das Hinzufügen eines VMFS-Datenspeichers zu einem geschützten Cluster schützt diesen automatisch.
- Es kann kein Datenspeicher in einem Rechenzentrum mit einem oder mehreren geschützten Host-Clustern erstellt werden.
- Es ist nicht möglich, einen Datenspeicher auf einem ESXi-Host zu erstellen, wenn der übergeordnete Host-Cluster durch eine „Automated Failover Duplex policy“ (uniform oder non-uniform configuration) geschützt ist.
- Sie können einen VMFS-Datenspeicher nur auf einem ESXi-Host erstellen, der durch eine asynchrone Beziehung geschützt ist. Es ist nicht möglich, einen Datenspeicher auf einem ESXi-Host zu erstellen und einzubinden, der Teil eines Hostclusters ist, der durch die Richtlinie "Automated Failover Duplex" geschützt ist.

Bevor Sie beginnen

- Dienste und LIFs für jedes Protokoll auf der ONTAP-Speicherseite aktivieren.

- SVM einem Aggregat für den SVM-Benutzer im ASA r2 Storage-System zuordnen.
- Konfigurieren Sie den ESXi Host, wenn Sie das NVMe/TCP Protokoll verwenden:
  a. Überprüfen Sie die "VMware Kompatibilitätsleitfaden"

> VMware vSphere 7.0 U3 und spätere Versionen unterstützen das NVMe/TCP-Protokoll. Es werden jedoch VMware vSphere 8.0 und spätere Versionen empfohlen.

  b. Es sollte geprüft werden, ob der Hersteller der Netzwerkkarte (NIC) ESXi NIC mit dem NVMe/TCP-Protokoll unterstützt.
  c. Die ESXi-Netzwerkkarte ist für NVMe/TCP gemäß den Spezifikationen des Netzwerkkartenherstellers einzurichten.
  d. Bei Verwendung von VMware vSphere 7 befolgen Sie die Anweisungen auf der VMware-Website "VMkernel-Bindung für den NVMe over TCP Adapter konfigurieren", um die NVMe/TCP-Portbindung zu konfigurieren. Bei Verwendung von VMware vSphere 8 befolgen Sie "Konfiguration von NVMe über TCP auf ESXi", um die NVMe/TCP-Portbindung zu konfigurieren.
  e. Für VMware vSphere 7 Release siehe die Anweisungen auf Seite "NVMe über RDMA oder NVMe über TCP Softwareadapter aktivieren" zur Konfiguration der NVMe/TCP Softwareadapter. Für das VMware vSphere 8 Release siehe "Software-NVMe-over-RDMA- oder NVMe-over-TCP-Adapter hinzufügen" zur Konfiguration der NVMe/TCP Softwareadapter.
  f. Führen Sie "Speichersysteme und Hosts erkennen" die Aktion auf dem ESXi-Host aus. Weitere Informationen finden Sie unter "Konfiguration von NVMe/TCP mit vSphere 8.0 Update 1 und ONTAP 9.13.1 für VMFS Datenspeicher".
- Wenn Sie das NVME/FC-Protokoll verwenden, sind die folgenden Schritte zur Konfiguration des ESXi-Hosts erforderlich:
  a. Falls NVMe over Fabrics (NVMe-oF) noch nicht aktiviert ist, sollte es auf dem oder den ESXi-Hosts aktiviert werden.
  b. Vollständige SCSI Zonierung.
  c. Es muss sichergestellt sein, dass die ESXi-Hosts und das ONTAP System auf physischer und logischer Ebene verbunden sind.

Informationen zur Konfiguration einer ONTAP SVM für das FC-Protokoll finden Sie unter "Eine SVM für FC konfigurieren".

Weitere Informationen zur Verwendung des NVMe/FC-Protokolls mit VMware vSphere 8.0 finden Sie unter "NVMe-oF Hostkonfiguration für ESXi 8.x mit ONTAP".

Weitere Informationen zur Verwendung von NVMe/FC mit VMware vSphere 7.0 finden Sie unter "ONTAP NVMe/FC Host-Konfigurationsleitfaden" und "TR-4684".

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem, einen Hostcluster oder ein Rechenzentrum und wählen Sie **NetApp ONTAP tools** > **Datenspeicher erstellen**.
3. Wählen Sie den VMFS-Datenspeichertyp aus.
4. Geben Sie im Bereich **Name und Protokoll** den Namen, die Größe und die Protokollinformationen des Datenspeichers ein. Um den neuen Datenspeicher zu einem bestehenden VMFS Cluster hinzuzufügen, in den erweiterten Optionen den Datenspeichercluster auswählen.

5. Wählen Sie im Bereich **Speicher** eine Speicher-VM aus. Im Abschnitt **Erweiterte Optionen** bei Bedarf den **Namen der benutzerdefinierten Initiatorgruppe** angeben. Es besteht die Möglichkeit, eine vorhandene Initiatorgruppe für den Datenspeicher auszuwählen oder eine neue Initiatorgruppe mit einem benutzerdefinierten Namen zu erstellen.

   Bei Auswahl des NVMe/FC- oder NVMe/TCP-Protokolls wird ein neues Namespace-Subsystem erstellt und für die Namespace-Zuordnung verwendet. ONTAP tools erstellt das Namespace-Subsystem mit dem automatisch generierten Namen, der den Datenspeichernamen enthält. Eine Umbenennung des Namespace-Subsystems ist im Feld **Benutzerdefinierter Namespace-Subsystemname** in den erweiterten Optionen des **Storage**-Bereichs möglich.

6. Aus dem Bereich **Speicherattribute**:

   a. **Aggregate** aus den Dropdown-Optionen auswählen.

      Für ASA r2 Storage-Systeme wird die Option **Aggregate** nicht angezeigt, da der Storage disaggregiert ist. Bei Auswahl eines ASA r2 Storage-Systems vom Typ SVM werden auf der Seite mit den Storage-Attributen die Optionen zur Aktivierung von QoS angezeigt.

   b. ONTAP tools erstellt eine Speichereinheit (LUN/Namespace) mit einer dünnen Speicherplatzreserve basierend auf dem ausgewählten Protokoll.

      Ab ONTAP 9.16.1 unterstützen ASA r2 Speichersysteme bis zu 12 Knoten pro Cluster.

   c. Wählen Sie die **Performance-Servicelevel** für ASA r2 Storage-Systeme mit 12-Node SVM, die ein heterogenes Cluster ist. Diese Option ist nicht verfügbar, wenn die ausgewählte SVM ein homogenes Cluster ist oder ein SVM-Benutzer verwendet wird.

      'Any' ist der Standardwert für den Performance Service Level (PSL). Diese Einstellung erstellt die Storage-Einheit mithilfe des ONTAP Balanced-Placement-Algorithmus. Sie können jedoch bei Bedarf die Option 'Performance' oder 'Extreme' auswählen.

   d. Je nach Bedarf können die Optionen **Vorhandenes Volume verwenden** und **QoS aktivieren** ausgewählt und die entsprechenden Details angegeben werden.

      Im ASA r2 Speichertyp gilt die Erstellung oder Auswahl von Volumes nicht für die Erstellung von Speichereinheiten (LUN/Namespace). Daher werden diese Optionen nicht angezeigt.

   Das vorhandene Volume kann nicht zur Erstellung eines VMFS-Datenspeichers mit NVMe/FC- oder NVMe/TCP-Protokoll verwendet werden. Für den VMFS-Datenspeicher ist ein neues Volume zu erstellen.

7. Die Datenspeicherdetails sind im Bereich **Zusammenfassung** einsehbar, anschließend ist **Fertigstellen** auszuwählen.

   Wenn Sie den Datenspeicher auf einem geschützten Cluster erstellen, erscheint eine schreibgeschützte Meldung: „Der Datenspeicher wird auf einem geschützten Cluster eingebunden.“

Ergebnis

ONTAP tools erstellt den VMFS Datenspeicher und bindet ihn auf allen Hosts ein.