Konfigurieren Sie ONTAP Tools für VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
November 17, 2025

Inhalt

Konfigurieren Sie ONTAP Tools für VMware vSphere

Fügen Sie vCenter Server-Instanzen hinzu

Fügen Sie vCenter Server-Instanzen zu den ONTAP-Tools für VMware vSphere hinzu, um Ihre virtuellen Datastores in Ihrer vCenter Server-Umgebung zu konfigurieren, zu managen und zu sichern. Wenn Sie mehrere vCenter Server-Instanzen hinzufügen, sind für die sichere Kommunikation zwischen ONTAP-Tools und jedem vCenter Server benutzerdefinierte CA-Zertifikate erforderlich.

Über diese Aufgabe

Durch die Integration mit vCenter können Sie mit ONTAP Tools Storage-Aufgaben wie Bereitstellung, Snapshots und Datensicherung direkt aus dem vSphere Client ausführen, sodass keine separaten Storage-Management-Konsolen mehr erforderlich sind.

Schritte

1. Öffnen Sie einen Webbrowser, und navigieren Sie zur URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie **vCenters** > **Add**, um die vCenter Server-Instanzen zu integrieren. Geben Sie die vCenter-IP-Adresse oder den Hostnamen, den Benutzernamen, das Kennwort und die Portdetails an.

> Sie benötigen kein Administratorkonto, um vCenter Instanzen zu ONTAP Tools hinzuzufügen. Sie können eine benutzerdefinierte Rolle ohne Administratorkonto mit eingeschränkten Berechtigungen erstellen. Weitere Informationen finden Sie unter "Nutzen Sie die RBAC für vCenter Server mit ONTAP Tools für VMware vSphere 10" .

Das Hinzufügen einer vCenter Server-Instanz zu ONTAP Tools löst automatisch die folgenden Aktionen aus:

- Das vCenter Client-Plug-in ist als Remote-Plug-in registriert.
- Benutzerdefinierte Privileges für die Plug-ins und APIs werden auf die vCenter Server Instanz angewendet.
- Zum Verwalten der Benutzer werden benutzerdefinierte Rollen erstellt.
- Das Plug-in wird als Verknüpfung auf der vSphere-Benutzeroberfläche angezeigt.

Registrieren Sie den VASA Provider mit einer vCenter Server-Instanz

Sie können den VASA Provider mit einer vCenter Server-Instanz unter Verwendung von ONTAP Tools für VMware vSphere registrieren. Im Abschnitt VASA Provider-Einstellungen wird der Registrierungsstatus des VASA Providers für den ausgewählten vCenter Server angezeigt. Stellen Sie in einer Multi-vCenter-Bereitstellung sicher, dass Sie für jede vCenter Server-Instanz über benutzerdefinierte CA-Zertifikate verfügen.

Schritte

1. Melden Sie sich beim vSphere-Client an
2. Wählen Sie im Abschnitt Plug-ins **Shortcuts** > **NetApp ONTAP Tools** aus.
3. Wählen Sie **Einstellungen** > **VASA Provider-Einstellungen**. Der Registrierungsstatus des VASA Providers wird als nicht registriert angezeigt.
4. Klicken Sie auf die Schaltfläche **Registrieren**, um den VASA Provider zu registrieren.
5. Geben Sie einen Namen für den VASA Provider ein, und stellen Sie ONTAP Tools für die Anmeldedaten der VMware vSphere-Anwendung bereit. Wählen Sie dann **Registrieren**.
6. Nach einer erfolgreichen Registrierung und Seitenaktualisierung werden der Status, der Name und die Version des registrierten VASA Providers angezeigt. Nach der Registrierung wird die Registrierung aufgehoben.

Nach Ihrer Beendigung

Vergewissern Sie sich, dass der aufgelistete VASA Provider vom vCenter Client unter VASA Provider aufgeführt ist:

Schritte

1. Navigieren Sie zur vCenter Server-Instanz.
2. Melden Sie sich mit den Administratoranmeldeinformationen an.
3. Wählen Sie **Speicheranbieter** > **Konfigurieren** Aus. Vergewissern Sie sich, dass der onboard VASA Provider korrekt aufgeführt ist.

Installieren Sie das NFS VAAI Plug-in

Das NFS vStorage API for Array Integration (NFS VAAI) Plug-in ist eine Softwarekomponente, die VMware vSphere und NFS Storage-Arrays integriert. Installieren Sie das NFS VAAI Plug-in mit ONTAP Tools für VMware vSphere, um die erweiterten Funktionen des NFS-Storage-Arrays nutzen zu können und bestimmte Storage-bezogene Vorgänge von den ESXi Hosts an das Storage Array selbst zu verlagern.

Bevor Sie beginnen

- Laden Sie das Installationspaket herunter "NetApp NFS Plug-in für VMware VAAI".
- Stellen Sie sicher, dass Sie über den ESXi-Host und vSphere 7.0U3 neuesten Patch oder neuere Versionen und ONTAP 9.14.1 oder höhere Versionen verfügen.
- Mounten Sie einen NFS-Datastore.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie im Abschnitt Plug-ins **Shortcuts** > **NetApp ONTAP Tools** aus.
3. Wählen Sie **Einstellungen** > **NFS VAAI Tools**.
4. Wenn das VAAI-Plug-in auf vCenter Server hochgeladen wird, wählen Sie im Bereich **existing Version Change** aus. Wenn kein VAAI-Plug-in auf den vCenter-Server hochgeladen wird, klicken Sie auf die Schaltfläche **Upload**.

5. Durchsuchen Sie die Datei, wählen `.vib` Sie sie 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** aus.

   Es werden nur die für die Plug-in-Installation geeigneten ESXi-Hosts angezeigt. Sie können den Installationsfortschritt im Abschnitt „Letzte Aufgaben“ des vSphere Web Client überwachen.

7. Starten Sie den ESXi-Host nach der Installation manuell neu.

   Wenn der VMware-Administrator den ESXi-Host neu startet, erkennt und aktiviert ONTAP-Tools für VMware vSphere das NFS VAAI-Plug-in automatisch.

Was kommt als Nächstes?

Nachdem Sie das NFS VAAI Plug-in installiert und Ihren ESXi Host neu gestartet haben, müssen Sie die korrekten NFS-Exportrichtlinien für den VAAI Copy-Offload konfigurieren. Wenn Sie VAAI in einer NFS-Umgebung konfigurieren, konfigurieren Sie die Regeln für die Exportrichtlinie unter Berücksichtigung der folgenden Anforderungen:

- Das entsprechende ONTAP-Volumen muss NFSv4-Aufrufe zulassen.
- Der Root-Benutzer sollte als Root bleiben und NFSv4 in allen übergeordneten Volumes der Verbindung zugelassen werden.
- Die Option für VAAI Support muss auf dem jeweiligen NFS Server eingestellt werden.

Weitere Informationen zum Verfahren finden Sie im "Konfigurieren Sie die richtigen NFS-Exportrichtlinien für den VAAI Copy-Offload" KB-Artikel.

Verwandte Informationen

"Support für VMware vStorage via NFS"

"Aktivieren oder deaktivieren Sie NFSv4.0"

"ONTAP unterstützt NFSv4.2"

Konfigurieren Sie ESXi-Hosteinstellungen

Die Konfiguration der Multipath- und Timeout-Einstellungen des ESXi Servers gewährleistet Hochverfügbarkeit und Datenintegrität, da bei Ausfall eines primären Pfads nahtlos auf einen Backup-Speicherpfad umgeschaltet werden kann.

Konfigurieren Sie die Multipath- und Timeout-Einstellungen des ESXi-Servers

Die ONTAP Tools für VMware vSphere prüfen und legen die Multipath-Einstellungen für ESXi Hosts und die HBA-Zeitüberschreitungseinstellungen fest, die für NetApp Storage-Systeme am besten geeignet sind.

Über diese Aufgabe

Je nach Konfiguration und Systemlast kann dieser Vorgang sehr viel Zeit in Anspruch nehmen. Der Aufgabenfortschritt wird im Fenster Letzte Aufgaben angezeigt.

Schritte

1. Wählen Sie auf der VMware vSphere Web Client-Startseite **Hosts und Cluster** aus.
2. Klicken Sie mit der rechten Maustaste auf einen Host und wählen Sie **NetApp ONTAP Tools** > **Host-Daten aktualisieren**.
3. Wählen Sie auf der Seite Verknüpfungen des VMware vSphere Web-Clients im Abschnitt Plug-ins **NetApp ONTAP-Tools** aus.
4. Gehen Sie in der Übersicht (Dashboard) der ONTAP Tools für VMware vSphere Plug-in zur **ESXi Host Compliance** Karte.
5. Wählen Sie den Link **Empfohlene Einstellungen anwenden**.
6. Wählen Sie im Fenster **Empfohlene Host-Einstellungen anwenden** die Hosts aus, die Sie aktualisieren möchten, um den von NetApp empfohlenen Einstellungen zu entsprechen, und wählen Sie **Weiter**.

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

7. Wählen Sie auf der Einstellungsseite die empfohlenen Werte nach Bedarf aus.
8. Überprüfen Sie im Übersichtsfenster die Werte und wählen Sie **Fertig stellen**. Sie können den Fortschritt im Fenster „Letzte Aufgabe“ verfolgen.

Legen Sie ESXi-Hostwerte fest

Mit den ONTAP-Tools für VMware vSphere können Sie Timeouts und andere Werte auf den ESXi-Hosts festlegen, um die beste Performance und ein erfolgreiches Failover zu gewährleisten. Die Werte, die ONTAP Tools für VMware vSphere Set bieten, basieren auf internen NetApp-Tests.

Auf einem ESXi-Host können Sie die folgenden Werte festlegen:

HBA/CNA-Adaptereinstellungen

Setzt die folgenden Parameter auf Standardwerte:

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

MPIO-Einstellungen

MPIO-Einstellungen definieren die bevorzugten Pfade für NetApp-Speichersysteme. Sie legen fest, welche der verfügbaren Pfade optimiert sind (im Gegensatz zu nicht optimierten Pfaden, die das Interconnect-Kabel durchlaufen), und legen den bevorzugten Pfad auf einen dieser Pfade fest.

In hochperformanten Umgebungen oder wenn Sie die Performance mit einem einzelnen LUN-Datastore testen, sollten Sie eventuell die Load-Balancing-Einstellung der Round-Robin (VMW_PSP_RR) Path Selection Policy (PSP) von der Standard-IOPS-Einstellung von 1000 auf den Wert 1 ändern.

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

NFS-Einstellungen

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

Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen

Sie können neue Benutzerrollen und -Berechtigungen für das Management von Storage-Back-Ends mit der JSON-Datei konfigurieren, die mit den ONTAP Tools für VMware vSphere und ONTAP System Manager bereitgestellt wird.

Bevor Sie beginnen

- Sie sollten die Datei mit den ONTAP-Berechtigungen von den ONTAP-Tools für VMware vSphere unter Verwendung von *https://<loadbalancerIP>:8443/Virtualization/user-Privileges/users_roles.zip* heruntergeladen haben.
- Sie sollten die ONTAP Privileges-Datei von ONTAP-Tools heruntergeladen haben `https://<loadbalancerIP>:8443/virtualization/user-privileges/users_roles.zip`.

> Benutzer können auf Cluster-Ebene oder direkt auf Storage Virtual Machines (SVMs)-Ebene erstellt werden. Sie können auch Benutzer erstellen, ohne die Datei user_roles.json zu verwenden. Falls dies der Fall ist, müssen Sie über einen Mindestsatz an Berechtigungen auf SVM-Ebene verfügen.

- Sie sollten sich mit Administratorrechten für das Speicher-Back-End angemeldet haben.

Schritte

1. Extrahieren Sie die heruntergeladene Datei *https://<loadbalancerIP>:8443/Virtualization/user-Privileges/users_roles.zip*.
2. Sie können über die Cluster-Management-IP-Adresse des Clusters auf ONTAP System Manager zugreifen.
3. Melden Sie sich mit dem Admin-Privileges beim Cluster an. So konfigurieren Sie einen Benutzer:
   a. Um Cluster-ONTAP-Tools zu konfigurieren, wählen Sie **Cluster** > **Einstellungen** > **Benutzer und Rollen** aus.
   b. Um den Benutzer der SVM-ONTAP-Tools zu konfigurieren, wählen Sie den Bereich **Speicher-SVM** > **Einstellungen** > **Benutzer und Rollen** aus.
   c. Wählen Sie unter Benutzer * Hinzufügen *.
   d. Wählen Sie im Dialogfeld * Benutzer hinzufügen* die Option **Virtualisierungsprodukte** aus.

e. **Browse**, um die JSON-Datei für ONTAP-Berechtigungen auszuwählen und hochzuladen.

   Das Produktfeld wird automatisch ausgefüllt.

f. Wählen Sie die gewünschte Funktion aus dem Dropdown-Menü „Produktfähigkeit“ aus.

   Das Feld **Rolle** wird basierend auf der ausgewählten Produktfähigkeit automatisch ausgefüllt.

g. Geben Sie den erforderlichen Benutzernamen und das erforderliche Passwort ein.

h. Wählen Sie die für den Benutzer erforderliche Privileges (Ermittlung, Speicher erstellen, Speicher ändern, Speicher zerstören, NAS/SAN-Rolle) aus, und wählen Sie dann **Hinzufügen** aus.

Die neue Rolle und der neue Benutzer werden hinzugefügt, und Sie können die detaillierten Berechtigungen unter der von Ihnen konfigurierten Rolle sehen.

Anforderungen für die SVM-Aggregatzuordnung

Um SVM-Benutzeranmeldeinformationen für die Bereitstellung von Datastores zu verwenden, erstellt das interne ONTAP-Tool für VMware vSphere Volumes auf dem Aggregat, das in der POST-API für Datastores angegeben ist. Die ONTAP ermöglicht nicht die Erstellung von Volumes auf Aggregaten ohne Zuweisung auf einer SVM mit SVM-Benutzeranmeldeinformationen. Um das zu lösen, müssen Sie die SVMs wie hier beschrieben mit den Aggregaten zuordnen. Dazu verwenden Sie entweder die ONTAP REST-API oder die CLI.

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
```

Erstellen Sie ONTAP-Benutzer und -Rolle manuell

Befolgen Sie die Anweisungen in diesem Abschnitt, um den Benutzer und die Rollen manuell zu erstellen, ohne die JSON-Datei zu verwenden.

1. Sie können über die Cluster-Management-IP-Adresse des Clusters auf ONTAP System Manager zugreifen.
2. Melden Sie sich mit dem Admin-Privileges beim Cluster an.
   a. Um Cluster-ONTAP-Tools-Rollen zu konfigurieren, wählen Sie **Cluster** > **Einstellungen** > **Benutzer und Rollen** aus.
   b. Um die Rollen der Cluster-SVM-ONTAP-Tools zu konfigurieren, wählen Sie **Speicher-SVM** >

Einstellungen > **Benutzer und Rollen** aus

3. Rollen Erstellen:
   a. Wählen Sie **Hinzufügen** unter **Rollen** Tabelle.
   b. Geben Sie die Details **Rollenname** und **Rollenattribute** ein.

      Fügen Sie den **REST API Path** und den entsprechenden Zugriff aus dem Drop-Down-Menü hinzu.

   c. Fügen Sie alle benötigten APIs hinzu und speichern Sie die Änderungen.
4. Benutzer Erstellen:
   a. Wählen Sie **Hinzufügen** unter **Benutzer** Tabelle.
   b. Wählen Sie im Dialogfeld **Benutzer hinzufügen System Manager** aus.
   c. Geben Sie den Benutzernamen * ein.
   d. Wählen Sie **Rolle** aus den Optionen aus, die im Schritt **Rollen erstellen** oben erstellt wurden.
   e. Geben Sie die Anwendungen ein, auf die Zugriff gewährt werden soll, und geben Sie die Authentifizierungsmethode ein. ONTAPI und HTTP sind die erforderlichen Anwendungen, und der Authentifizierungstyp ist **Password**.
   f. Legen Sie das **Passwort für den Benutzer** und **Speichern** für den Benutzer fest.

Liste der Mindestberechtigungen, die für einen nicht-Administrator-Cluster mit globalem Umfang erforderlich sind

In diesem Abschnitt werden die Mindestberechtigungen aufgeführt, die für Benutzer mit globalem Clusterbereich, die ohne Verwendung der JSON-Datei des Benutzers erstellt wurden, erforderlich sind. Wenn Sie einen Cluster mit lokalem Umfang hinzufügen, empfehlen wir, zum Erstellen der Benutzer die JSON-Datei zu verwenden, da für ONTAP Tools für VMware vSphere mehr als nur die Leseberechtigungen für das Provisioning auf ONTAP erforderlich sind.

Verwenden von APIs:

API	Zugangsstufe	Verwendet für
/API/Cluster	Schreibgeschützt	Erkennung Der Clusterkonfiguration
/API/Cluster/Lizenzierung/Lizenzen	Schreibgeschützt	Lizenzprüfung für protokollspezifische Lizenzen
/API/Cluster/Nodes	Schreibgeschützt	Erkennung des Plattformtyps
/API/Sicherheit/Konten	Schreibgeschützt	Ermittlung Von Berechtigungen
/API/Sicherheit/Funktionen	Schreibgeschützt	Ermittlung Von Berechtigungen
/API/Storage/Aggregate	Schreibgeschützt	Speicherplatzüberprüfung von Aggregaten während der Bereitstellung von Datastores/Volumes
/API/Storage/Cluster	Schreibgeschützt	Um Speicherplatz auf Cluster-Ebene und Effizienzdaten zu erhalten

/API/Storage/Festplatten	Schreibgeschützt	Um die in einem Aggregat zugeordneten Festplatten zu erhalten
/API/Storage/qos/Richtlinien	Lesen/Erstellen/Ändern	QoS- und VM-Richtlinienmanagement
/API/svm/svms	Schreibgeschützt	Um die SVM-Konfiguration für den Fall zu erhalten, dass das Cluster lokal hinzugefügt wird.
/API/Netzwerk/ip/Schnittstellen	Schreibgeschützt	Storage Back-end hinzufügen: Zur Identifizierung des Management-LIF-Umfangs ist Cluster/SVM

Erstellen Sie ONTAP Tools für VMware vSphere ONTAP API-basierten Cluster Scoped User

Privileges müssen erkannt, erstellt, geändert und zerstört werden, damit bei Ausfällen in Datastores PATCHVORGÄNGE und automatische Rollbacks durchgeführt werden können. Das Fehlen dieser Privileges führt zu Unterbrechungen des Workflows und Problemen bei der Bereinigung.

Erstellen von ONTAP-Tools für VMware vSphere ONTAP API-basierte Benutzer mit Erkennung, Erstellung von Speicher, Änderung von Speicher, Zerstörung von Speicher Privileges ermöglicht die Initiierung von Ermittlungen und Management von ONTAP-Tools Workflows.

Führen Sie die folgenden Befehle aus, um einen Cluster-scoped-Benutzer mit allen oben genannten Privileges zu erstellen:

```
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
```

Außerdem führen Sie für ONTAP-Versionen 9.16.0 und höher den folgenden Befehl aus:

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

ONTAP Tools für VMware vSphere ONTAP API-basierten SVM-Scoped User erstellen

Führen Sie die folgenden Befehle aus, um einen für den SVM-Scoped-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>
```

Außerdem führen Sie für ONTAP-Versionen 9.16.0 und höher den 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 mit den oben erstellten API-basierten Rollen zu erstellen, führen Sie den 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_
```

Um das Konto zu entsperren, führen Sie den folgenden Befehl aus, um 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 von ONTAP Tools für VMware vSphere 10.1 Benutzer auf 10.3 Benutzer

Wenn es sich bei den ONTAP-Tools für VMware vSphere 10.1-Benutzer um einen Cluster-scoped-Benutzer handelt, der mit der json-Datei erstellt wurde, führen Sie die folgenden Befehle auf der ONTAP-CLI mit dem Admin-Benutzer aus, um ein Upgrade auf Version 10.3 durchzuführen.

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

Wenn es sich bei den ONTAP Tools für VMware vSphere 10.1 Benutzer um einen im SVM-Umfang enthaltenen Benutzer handelt, der mit der json-Datei erstellt wurde, führen Sie die folgenden Befehle an der ONTAP-CLI aus, wobei Sie den Admin-Benutzer zum Upgrade auf Version 10.3 verwenden.

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>

Durch Hinzufügen des Befehls *vserver nvme Namespace show* und *vserver nvme-Subsystem show* zu der vorhandenen Rolle werden die folgenden Befehle hinzugefügt.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Fügen Sie ein Storage-Back-End hinzu

Durch das Hinzufügen eines Storage-Backends können Sie ein ONTAP Cluster integrieren.

Über diese Aufgabe

Bei mandantenfähige Konfigurationen, bei denen vCenter als Mandant mit einer entsprechenden SVM fungiert, können Sie das Cluster mit dem ONTAP Tools Manager hinzufügen. Verknüpfen Sie das Storage-Backend mit dem vCenter Server, um es global der eingenommenen vCenter Server-Instanz zuzuordnen. Der vCenter Mandant muss die gewünschten Storage Virtual Machines (SVMs) integriert haben. Dadurch kann ein SVM-Benutzer VVols Datastore bereitstellen. Sie können Storage in vCenter mithilfe der SVM hinzufügen.

Fügen Sie über die Benutzeroberfläche von ONTAP Tools lokale Storage-Back-Ends mit Cluster- oder SVM-Anmeldedaten hinzu. Diese Storage Back-Ends sind auf nur ein vCenter beschränkt. Bei lokaler Verwendung der Cluster-Anmeldedaten werden die zugehörigen SVMs automatisch dem vCenter zugeordnet, um VVols oder VMFS zu managen. Für VMFS-Management, einschließlich SRA, unterstützen ONTAP-Tools SVM-

Zugangsdaten, ohne dass ein globales Cluster erforderlich ist.

Verwenden des ONTAP Tools Managers

In einer mandantenfähigen Einrichtung können Sie ein Storage-Back-End-Cluster global und eine lokale SVM hinzufügen, um die SVM-Benutzeranmeldedaten zu verwenden.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste **Speicher-Backends** aus.
4. Fügen Sie das Speicher-Back-End hinzu und geben Sie die IP-Adresse oder den FQDN, den Benutzernamen und das Kennwort des Servers an.

   IPv4- und IPv6-Adressenmanagement-LIFs werden unterstützt.

Die vSphere-Client-Benutzeroberfläche wird verwendet

Bei der Konfiguration eines Storage-Backend über die vSphere Client-Benutzeroberfläche ist zu beachten, dass der VVols-Datastore das direkte Hinzufügen eines SVM-Benutzers nicht unterstützt.

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie auf der Shortcuts-Seite unter dem Plug-ins-Abschnitt **NetApp ONTAP Tools** aus.
3. Wählen Sie in der Seitenleiste **Speicher-Backends** aus.
4. Fügen Sie das Speicher-Back-End hinzu, und geben Sie die IP-Adresse, den Benutzernamen, das Kennwort und die Portdetails des Servers an.

   Zum direkten Hinzufügen eines SVM-Benutzers können Cluster-basierte Anmeldedaten und logische Schnittstellen für das IPv4- und IPv6-Adressmanagement hinzugefügt oder SVM-basierte Anmeldedaten mit einer SVM-Management-LIF bereitgestellt werden.

Was kommt als Nächstes?

Die Liste wird aktualisiert, und das neu hinzugefügte Storage-Back-End wird in der Liste angezeigt.

Ordnen Sie ein Storage-Back-End einer vCenter Server-Instanz zu

Verknüpfen Sie ein Storage-Backend mit dem vCenter Server, um eine Zuordnung zwischen dem Storage-Backend und der eingeboard vCenter Server Instanz global zu erstellen.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Randleiste vCenter aus.
4. Wählen Sie die vertikalen Ellipsen für die vCenter Server-Instanz aus, die Sie mit den Speicher-Back-Ends verknüpfen möchten.
5. Wählen Sie das Storage-Back-End aus der Dropdown-Liste aus, um die vCenter Server-Instanz dem erforderlichen Storage-Back-End zuzuordnen.

Konfigurieren Sie den Netzwerkzugriff

Wenn Sie den Netzwerkzugriff nicht konfiguriert haben, werden standardmäßig alle vom ESXi-Host ermittelten IP-Adressen zur Exportrichtlinie hinzugefügt. Sie können ihn so konfigurieren, dass der Exportrichtlinie einige spezifische IP-Adressen hinzugefügt und der Rest ausgeschlossen wird. Wenn Sie jedoch einen Mount-Vorgang auf den ausgeschlossenen ESXi-Hosts durchführen, schlägt der Vorgang fehl.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie **NetApp ONTAP Tools** auf der Shortcuts-Seite unter dem Plug-ins-Bereich.
3. Navigieren Sie im linken Bereich der ONTAP-Tools zu **Einstellungen** > **Netzwerkzugang verwalten** > **Bearbeiten**.

   Um mehrere IP-Adressen hinzuzufügen, trennen Sie die Liste durch Kommas, Bereich, klassenloses Inter-Domain Routing (CIDR) oder eine Kombination aller drei.

4. Wählen Sie **Speichern**.

Erstellen eines Datenspeichers

Wenn Sie einen Datastore auf Host-Cluster-Ebene erstellen, wird der Datastore auf allen Hosts des Ziels erstellt und gemountet. Die Aktion wird nur aktiviert, wenn der aktuelle Benutzer über die Berechtigung zur Ausführung verfügt.

Erstellen Sie einen VVols-Datastore

Ab der Nutzung von ONTAP Tools für VMware vSphere 10.3 können Sie auf ASA r2 Systemen mit Platzeffizienz wie Thin.vVol einen VVols Datastore erstellen. Der VASA Provider erstellt bei der Erstellung des vVol Datastore einen Container und die gewünschten Protokollendpunkte. Dieser Container verfügt nicht über Sicherungsvolumes.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Root-Aggregate nicht der SVM zugeordnet sind.
- Stellen Sie sicher, dass der VASA Provider beim ausgewählten vCenter registriert ist.
- Im ASA r2 Storage-System sollte die SVM dem Aggregat für 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** > **Datastore erstellen** aus.
3. Wählen Sie VVols **Datenspeichertyp** aus.
4. Geben Sie die Informationen **Datastore Name** und **Protocol** ein.

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

5. Wählen Sie die Storage-VM aus, auf der der Datastore erstellt werden soll.
6. Wählen Sie in den **Erweiterten Optionen** eine benutzerdefinierte Exportrichtlinie für das NFS-Protokoll oder einen benutzerdefinierten Initiatorgruppennamen für die iSCSI- und FC-Protokolle aus.

   Beim Typ SVM des ASA r2 Storage-Systems werden Storage-Einheiten (LUN/Namespace) nicht erstellt, da der Datastore nur ein logischer Container ist.

7. Im Bereich **Speicherattribute** können Sie neue Volumes erstellen oder die vorhandenen Volumes verwenden. Sie können diese beiden Volume-Typen jedoch nicht kombinieren, um einen VVols-Datastore zu erstellen.

   Beim Erstellen eines neuen Volumes können Sie die QoS auf dem Datastore aktivieren. Standardmäßig wird für jede Anforderung, die eine LUN erstellt hat, ein Volume erstellt. Dieser Schritt gilt nicht für VVols-Datastores, die ASA r2 Storage-Systeme verwenden.

8. Überprüfen Sie Ihre Auswahl im Fenster **Zusammenfassung** und wählen Sie **Fertig stellen**.

Erstellen Sie einen NFS-Datastore

Ein Datastore des VMware Network File System (NFS) verwendet das NFS-Protokoll, um ESXi-Hosts über ein Netzwerk mit einem Shared Storage-Gerät zu verbinden. NFS-Datastores werden häufig in VMware vSphere Umgebungen verwendet und bieten verschiedene Vorteile, z. B. Einfachheit und Flexibilität.

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** > **Datastore erstellen** aus.
3. Wählen Sie NFS im Feld **Datastore type** aus.

4. Geben Sie den Namen, die Größe und die Protokollinformationen des Datastore im Bereich **Name und Protokoll** ein. Wählen Sie in den erweiterten Optionen **Datastore Cluster** und **Kerberos-Authentifizierung** aus.

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

5. Wählen Sie **Plattform** und **Storage VM** im Bereich **Storage** aus.
6. Wählen Sie **Custom Export Policy** unter Advanced options, falls erforderlich, aber es wird nicht empfohlen. Falls verwendet, stellen Sie sicher, dass Sie die Erkennung in vCenter für alle Objekte ausführen.

   Sie können keinen NFS-Datastore mit der Standard-/Root-Volume-Richtlinie der SVM erstellen.

   - In den erweiterten Optionen ist die Umschalttaste **Asymmetric** nur sichtbar, wenn Leistung oder Kapazität in der Dropdown-Liste Plattform ausgewählt ist.
   - Wenn Sie die Option **any** in der Dropdown-Liste der Plattform wählen, sehen Sie die SVMs, die Teil des vCenter sind, unabhängig von der Plattform oder dem asymmetrischen Flag.
7. Wählen Sie im Bereich **Speicherattribute** das Aggregat für die Volume-Erstellung aus. Wählen Sie in den erweiterten Optionen je nach Bedarf **Space Reserve** und **Enable QoS** aus.
8. Überprüfen Sie die Auswahl im Fenster **Zusammenfassung** und wählen Sie **Fertig stellen**.

Der NFS Datastore wird auf allen Hosts erstellt und gemountet.

Erstellen Sie einen VMFS-Datastore

Virtual Machine File System (VMFS) ist ein geclustertes Dateisystem, das Dateien von virtuellen Maschinen in VMware vSphere Umgebungen speichert. Mit VMFS können mehrere ESXi-Hosts gleichzeitig auf dieselben VM-Dateien zugreifen, wodurch Funktionen wie vMotion und Hochverfügbarkeit aktiviert werden.

In einem geschützten Cluster:

- Sie können nur VMFS-Datastores erstellen. Wenn Sie einem geschützten Cluster einen VMFS Datastore hinzufügen, wird dieser automatisch gesichert.
- Sie können keinen Datastore in einem Rechenzentrum mit einem oder mehreren geschützten Host-Clustern erstellen.
- Sie können keinen Datastore auf dem ESXi-Host erstellen, wenn der übergeordnete Host-Cluster durch eine Beziehung des Typs „automatisierte Failover-Duplex-Richtlinie“ geschützt ist (einheitliche/uneinheitliche Konfiguration).
- Sie können einen VMFS-Datastore nur auf einem ESXi-Host erstellen, der durch eine asynchrone Beziehung geschützt ist. Sie können keinen Datastore auf einem ESXi-Host erstellen und mounten, der Teil eines Host-Clusters ist, der durch die Richtlinie „Automatischer Failover-Duplex“ geschützt ist.

Bevor Sie beginnen

- Aktivieren Sie Services und LIFs für jedes Protokoll auf der ONTAP Storage-Seite.
- SVM-Aggregat für 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 Compatibility Guide"

> VMware vSphere 7.0 U3 und höher unterstützen das NVMe/TCP-Protokoll. Es wird jedoch VMware vSphere 8.0 und eine neuere Version empfohlen.

b. Überprüfen Sie, ob der NIC-Anbieter (Network Interface Card) ESXi NIC mit NVMe/TCP-Protokoll unterstützt.

c. Konfigurieren Sie die ESXi-NIC für NVMe/TCP gemäß den Spezifikationen des NIC-Anbieters.

d. Wenn Sie VMware vSphere 7-Version verwenden, befolgen Sie die Anweisungen auf der VMware-Site "Konfigurieren Sie die VMkernel Bindung für den NVMe over TCP Adapter", um die NVMe/TCP-Portbindung zu konfigurieren. Wenn Sie VMware vSphere 8 Version verwenden, folgen Sie "Konfiguration von NVMe over TCP auf ESXi", um die NVMe/TCP-Portbindung zu konfigurieren.

e. Folgen Sie für VMware vSphere 7 Release den Anweisungen auf Seite "Aktivieren Sie NVMe over RDMA oder NVMe over TCP-Softwareadapter", um NVMe/TCP-Softwareadapter zu konfigurieren. Folgen Sie bei VMware vSphere 8 Version, "Fügen Sie Software-NVMe-over-RDMA- oder NVMe-over-TCP-Adapter hinzu" um die NVMe/TCP-Softwareadapter zu konfigurieren.

f. Führen Sie "Erkennen von Storage-Systemen und Hosts"eine Aktion auf dem ESXi-Host aus. Weitere Informationen finden Sie unter "Konfigurieren von NVMe/TCP mit vSphere 8.0 Update 1 und ONTAP 9.13.1 für VMFS-Datenspeicher".

- Wenn Sie das NVME/FC-Protokoll verwenden, führen Sie die folgenden Schritte aus, um den ESXi-Host zu konfigurieren:

  a. Aktivieren Sie NVMe over Fabrics (NVMe-of) auf Ihren ESXi Hosts.

  b. Vollständiges SCSI-Zoning

  c. Stellen Sie sicher, dass ESXi-Hosts und das ONTAP-System auf einer physischen und einer logischen Ebene verbunden sind.

Informationen zum Konfigurieren einer ONTAP SVM für das FC-Protokoll finden Sie unter "Konfigurieren Sie eine SVM für FC".

Weitere Informationen zur Nutzung des NVMe/FC-Protokolls mit VMware vSphere 8.0 finden Sie unter "NVMe-of Host-Konfiguration 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** > **Datastore erstellen** aus.
3. Wählen Sie den VMFS-Datastore-Typ aus.
4. Geben Sie den Namen, die Größe und die Protokollinformationen des Datastore im Bereich **Name und Protokoll** ein. Wenn Sie den neuen Datastore zu einem vorhandenen VMFS Datastore-Cluster hinzufügen möchten, wählen Sie unter Erweiterte Optionen die Datastore-Cluster-Auswahl aus.
5. Wählen Sie Speicher-VM im Bereich **Speicher** aus. Geben Sie den **Custom Initiator Group Name** im Abschnitt **Advanced options** nach Bedarf an. Sie können eine vorhandene Initiatorgruppe für den Datastore auswählen oder eine neue Initiatorgruppe mit einem benutzerdefinierten Namen erstellen.

Bei Auswahl des NVMe/FC- oder NVMe/TCP-Protokolls wird ein neues Namespace-Subsystem erstellt und für die Namespace-Zuordnung verwendet. Das Namespace-Subsystem wird mit dem automatisch generierten Namen erstellt, der den Datastore-Namen enthält. Sie können das Namespace-Subsystem im Feld **Custom Namespace Subsystem Name** in den erweiterten Optionen des Fensters **Storage** umbenennen.

6. Im Bereich **Storage attributes**:

   a. Wählen Sie aus den Dropdown-Optionen **Aggregate** aus.

   Bei ASA r2-Speichersystemen wird die Option **Aggregate** nicht angezeigt, da es sich bei ASA r2-Speicher um einen disaggregierten Speicher handelt. Wenn Sie eine ASA r2 Storage-System-Typ SVM auswählen, werden auf der Seite Storage-Attribute die Optionen zur Aktivierung der QoS angezeigt.

   b. Nach dem ausgewählten Protokoll wird eine Storage-Einheit (LUN/Namespace) mit einer Platzreserve des Typs Thin erstellt.

   c. Wählen Sie **vorhandenes Volume verwenden**, **QoS**-Optionen nach Bedarf aktivieren und geben Sie die Details an.

   Im ASA r2-Speichertyp ist die Volume-Erstellung oder -Auswahl für die Erstellung von Speichereinheiten (LUN/Namespace) nicht anwendbar. Daher werden diese Optionen nicht angezeigt.

   Bei der Erstellung eines VMFS-Datastore mit einem NVMe/FC- oder NVMe/TCP-Protokoll können Sie das vorhandene Volume nicht verwenden, sondern müssen ein neues Volume erstellen.

7. Überprüfen Sie die Datastore-Details im Bereich **Summary** und wählen Sie **Finish**.

   Wenn Sie den Datastore auf einem geschützten Cluster erstellen, wird eine schreibgeschützte Meldung angezeigt: „Der Datastore wird auf einem geschützten Cluster gemountet.“

Ergebnis

Der VMFS Datastore wird auf allen Hosts erstellt und gemountet.