Dokumentation zu ONTAP Tools für VMware vSphere

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

Inhalt

Dokumentation zu ONTAP Tools für VMware vSphere

Versionshinweise

Versionshinweise für ONTAP tools

Informieren Sie sich über die neuen und verbesserten Funktionen der ONTAP tools for VMware vSphere 10.5.

Eine vollständige Liste der neuen Funktionen und Verbesserungen finden Sie unterWas ist neu in den ONTAP tools for VMware vSphere 10.5 .

Die aktuellsten Informationen zur Kompatibilität finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" .

Die Migration von ONTAP tools for VMware vSphere 9.12D1, 9.13D2 und 9.13P2 auf ONTAP tools for VMware vSphere 10.5 wird unterstützt.

Weitere Informationen finden Sie im "ONTAP tools for VMware vSphere 10.5 – Versionshinweise" . Sie müssen sich mit Ihrem NetApp -Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zugreifen zu können.

Was ist neu in den ONTAP tools for VMware vSphere 10.5

Informieren Sie sich über die neuen Funktionen der ONTAP tools for VMware vSphere 10.5.

- **Plattformqualifikation**

ONTAP tools for VMware vSphere 10.5 bieten Unterstützung für ASA r2-Systeme und sorgen so für Kompatibilität mit den neuesten Hardware- und Softwarekonfigurationen. Diese Version umfasst auch die Integration mit ONTAP 9.16.1 und 9.17.1, wodurch die unterstützten Umgebungen erweitert werden.

- **VMware-Qualifikation und -Zertifizierungen**

ONTAP tools for VMware vSphere 10.5 entsprechen den aktuellen VMware-Zertifizierungsstandards für Interoperabilität und unterstützen sowohl ESXi-Host als auch vCenter Server.

- * MetroCluster Unterstützung*

Diese Version bietet Unterstützung für MetroCluster -Konfigurationen und verbessert so die Hochverfügbarkeit und Notfallwiederherstellungsfunktionen.

- **Sicherheits- und Zertifikatsverwaltung**

Diese Version führt eine optimierte Verwaltung selbstsignierter Zertifikate ein und verbessert so sowohl die Benutzererfahrung als auch die Einhaltung von Sicherheitsstandards. Es bietet verbesserte Workflows zur Zertifikatsvalidierung, um ONTAP und ONTAP tools for VMware vSphere Kommunikation zu sichern.

- **Replikationsverbesserungen**

Diese Version unterstützt die VMFS-Replikation mit hierarchischer Konsistenzgruppe einschließlich SRA und SnapMirror Active Sync in ASA R2-Systemen. Es unterstützt Zero-RPO-Backups zur Verbesserung des Datenschutzes und der Datenwiederherstellung.

- **Upgrade und Migration**

Der Upgrade- und Migrationsprozess von früheren Versionen der ONTAP tools for VMware vSphere auf die ONTAP tools for VMware vSphere 10.5 ist nahtlos und effizient konzipiert, minimiert Ausfallzeiten und gewährleistet einen reibungslosen Übergang.

Unterstützte ONTAP -Plattformen und vCenter Server-Versionen

ONTAP tools for VMware vSphere 10.5 P1 unterstützt vCenter High Availability (HA)-Konfigurationen für SRA- und SnapMirror active sync-Komponenten. vVols wird in dieser Konfiguration nicht unterstützt. Während eines HA-Failovers kann vCenter für mehrere Minuten nicht verfügbar sein. In großen Umgebungen oder wenn ein Fehler auftritt, können die Failover-Zeiten 15 Minuten überschreiten.

Weitere Informationen finden Sie unter "vCenter High Availability-Dokumentation". Bei Fragen zu vCenter HA wenden Sie sich an "Broadcom Support".

Aktuelle Informationen zur Versionskompatibilität finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" .

Vergleich der Funktionen der ONTAP tools for VMware vSphere 9 und 10

Erfahren Sie, ob die Migration von ONTAP tools for VMware vSphere 9 auf ONTAP tools for VMware vSphere 10.2 oder spätere Versionen das Richtige für Sie ist.

Die aktuellsten Informationen zur Kompatibilität finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool" .

Funktion	ONTAP -Tools 9.13	ONTAP -Tools ab 10.2
Wichtigstes Wertversprechen	Optimieren und vereinfachen Sie den Betrieb von Tag 0 bis Tag 2 mit verbesserten Sicherheits-, Compliance- und Automatisierungsfunktionen	Erweiterte Unterstützung um FC für VMFS und NVMe-oF nur für VMFS. Benutzerfreundlichkeit für NetApp SnapMirror, einfache Einrichtung für vSphere Metro Storage-Cluster und VMware Live Site Recovery-Unterstützung für drei Standorte
ONTAP Release-Qualifizierung	ONTAP 9.9.1 bis ONTAP 9.16.1	ONTAP 9.12.1 bis 9.15.1 für ONTAP tools 10.2. ONTAP 9.14.1, 9.15.1, 9.16.0 und 9.16.1 für ONTAP tools 10.3. ONTAP 9.14.1, 9.15.1, 9.16.0 und 9.16.1 für ONTAP tools 10.4. ONTAP 9.16.1P3 und höher ist für ONTAP tools 10.4 bei Verwendung von ASA r2-Systemen erforderlich. ONTAP 9.15.1, 9.16.1 und 9.17.0 für ONTAP tools 10.5.

Funktion	ONTAP -Tools 9.13	ONTAP -Tools ab 10.2
VMware-Release-Unterstützung	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 bis VMware Live Site Recovery 9.0	vSphere 7.x-8.x, vSphere 9.0 ab ONTAP Tools 10.5, VMware Site Recovery Manager (SRM) 8.7 bis VMware Live Site Recovery 9.0 **HINWEIS:** In ONTAP Tools 10.x unterstützt SRM gemeinsam genutzte Standorte, was eine verbesserte Skalierbarkeit und höhere Leistung ermöglicht.
Protokollunterstützung	NFS- und VMFS-Datenspeicher: NFS (v3 und v4.1), VMFS (iSCSI und FCP)	NFS- und VMFS-Datenspeicher: NFS (v3 und v4.1), VMFS (iSCSI/FCP/NVMe-oF)
Skalierbarkeit	Hosts und VMs: 300 Hosts, bis zu 10.000 VMs; Datenspeicher: 600 NFS, bis zu 50 VMFS	Hosts und VMs: 600 Hosts
Beobachtbarkeit	Dashboards zu Leistung, Kapazität und Host-Compliance Dynamische VM- und Datenspeicherberichte	Aktualisierte Dashboards zu Leistung, Kapazität und Host-Compliance. Dynamische VM- und Datenspeicherberichte.
Datenschutz	SRA-Replikation für VMFS und NFS. SCV-Integration und Interoperabilität für Backups.	SRA-Replikation für iSCSI-VMFS- und NFS v3-Datenspeicher, Drei-Site-Schutz durch Kombination von SMAS und VMware Live Site Recovery. SRA-Unterstützung für FCP mit VMFS.
VASA-Anbieterunterstützung	VASA 4,0	VASA 3,0

Konzepte

Erfahren Sie mehr über ONTAP tools

ONTAP tools for VMware vSphere sind ein Satz von Tools für das Lebenszyklusmanagement virtueller Maschinen. Es lässt sich in das VMware-Ökosystem integrieren, um die Bereitstellung von Datenspeichern zu vereinfachen und einen grundlegenden Schutz für virtuelle Maschinen bereitzustellen. Es handelt sich um eine Sammlung horizontal skalierbarer, ereignisgesteuerter Microservices, die als Open Virtual Appliance (OVA) bereitgestellt werden.

ONTAP tools for VMware vSphere unterstützen:

- Kernfunktionen virtueller Maschinen (VM) wie Schutz und Notfallwiederherstellung
- VASA-Anbieter für speicherrichtlinienbasiertes Management
- Richtlinienbasiertes Storage-Management
- Storage Replication Adapter (SRA)

Hohe Verfügbarkeit für ONTAP -Tools für VMware

ONTAP tools for VMware vSphere bieten Hochverfügbarkeitsunterstützung (HA), um bei Ausfällen einen unterbrechungsfreien Betrieb aufrechtzuerhalten.

Die HA-Lösung unterstützt Sie bei der schnellen Wiederherstellung nach den folgenden Arten von Ausfällen:

- Hostausfall – Es wird nur der Ausfall eines einzelnen Knotens unterstützt.
- Netzwerkausfall
- Ausfall der virtuellen Maschine (Gastbetriebssystem)
- Anwendungsfehler (ONTAP -Tools)

Sie müssen keine zusätzliche Konfiguration durchführen, um HA für ONTAP tools for VMware vSphere zu aktivieren.

ONTAP tools for VMware vSphere unterstützen vCenter HA nicht.

Um die HA-Funktion zu verwenden, stellen Sie sicher, dass CPU-Hot-Add und Memory-Hot-Plug während der Bereitstellung oder später in den VM-Einstellungen aktiviert sind.

Schlüsselkonzepte und Begriffe in ONTAP tools

Im folgenden Abschnitt werden die wichtigsten Konzepte und Begriffe beschrieben, die in diesem Dokument verwendet werden.

Zertifizierungsstelle (CA)

CA ist eine vertrauenswürdige Einheit, die SSL-Zertifikate (Secure Sockets Layer) ausgibt.

Konsistenzgruppe

Eine Konsistenzgruppe ist eine Sammlung von Volumes, die als eine Einheit verwaltet werden. Konsistenzgruppen werden zur Gewährleistung der Datenkonsistenz über Speichereinheiten und Datenträger hinweg synchronisiert. In ONTAP bieten sie eine einfache Verwaltung und eine Schutzgarantie für eine Anwendungs-Workload, die sich über mehrere Volumes erstreckt. Erfahren Sie mehr über "Konsistenzgruppen" .

Dual-Stack

Ein Dual-Stack-Netzwerk ist eine Netzwerkumgebung, die die gleichzeitige Verwendung von IPv4- und IPv6-Adressen unterstützt.

Hochverfügbarkeit

Cluster Nodes werden für einen unterbrechungsfreien Betrieb in HA-Paaren konfiguriert.

Logical Unit Number (LUN)

Eine LUN ist eine Zahl, mit der eine logische Einheit innerhalb eines Storage Area Network (SAN) identifiziert wird. Bei diesen adressierbaren Geräten handelt es sich in der Regel um logische Laufwerke, auf die über das SCSI-Protokoll (Small Computer System Interface) oder eines seiner gekapselten Derivate zugegriffen wird.

NVMe-Namespace und -Subsystem

Ein NVMe Namespace ist eine Menge nicht-flüchtiger Speicher, der in logische Blöcke formatiert werden kann. Namespaces sind das Äquivalent von LUNs für FC- und iSCSI-Protokolle, und ein NVMe-Subsystem entspricht einer igroup. Ein NVMe-Subsystem kann Initiatoren zugeordnet werden, damit die zugehörigen Initiatoren auf Namespaces innerhalb des Subsystems zugreifen können.

ONTAP Tools Manager

Der ONTAP Tools Manager bietet ONTAP Tools für VMware vSphere Administratoren mehr Kontrolle über die gemanagten vCenter Server Instanzen und On-Board Storage-Back-Ends. Sie unterstützt das Management von vCenter Server-Instanzen, Storage-Back-Ends, Zertifikaten, Passwörtern und Downloads von Protokollpaketen.

Offene virtuelle Appliance (OVA)

OVA ist ein offener Standard für die Paketierung und Verteilung virtueller Appliances oder Software, die auf virtuellen Maschinen ausgeführt werden müssen.

Recovery-Zeitpunkt (RPO)

RPO misst, wie häufig Sie Daten sichern oder replizieren. Es gibt den genauen Zeitpunkt an, zu dem Sie nach einem Ausfall Daten wiederherstellen müssen, um den Geschäftsbetrieb wieder aufzunehmen. Wenn ein Unternehmen beispielsweise einen RPO von 4 Stunden hat, kann ein Datenverlust bei einem Ausfall von bis zu 4 Stunden toleriert werden.

SnapMirror Active Sync

SnapMirror Active Sync ermöglicht es Business-Services, auch bei einem vollständigen Standortausfall den Betrieb fortzusetzen und Applikationen mithilfe einer sekundären Kopie einen transparenten Failover zu unterstützen. Ein manuelles Eingreifen oder benutzerdefiniertes Scripting ist nicht erforderlich, um ein Failover

mit aktiver SnapMirror Synchronisierung auszulösen. Erfahren Sie mehr über "SnapMirror Active Sync".

Storage-Back-Ends

Storage-Back-Ends sind die zugrunde liegende Storage-Infrastruktur, die der ESXi Host zum Speichern von Virtual Machine-Dateien, Daten und anderen Ressourcen verwendet. Sie ermöglichen es dem ESXi-Host, auf persistente Daten zuzugreifen und diese zu managen, und liefern die erforderliche Storage-Funktionalität und Performance für eine virtualisierte Umgebung.

Globaler Cluster (Storage Back-End)

Globale Storage Back-Ends, die nur mit ONTAP Cluster-Anmeldeinformationen verfügbar sind, werden über die Benutzeroberfläche des ONTAP Tools Managers aufgenommen. Sie können mit minimalem Privileges hinzugefügt werden, um wichtige Cluster-Ressourcen für das Management von VVols aufzufinden. Globale Cluster eignen sich ideal für mandantenfähige Szenarien, in denen ein SVM-Benutzer zum VVols-Management lokal hinzugefügt wird.

Lokales Storage-Back-End

Lokale Storage-Back-Ends mit Cluster- oder SVM-Zugangsdaten werden über die Benutzeroberfläche der ONTAP Tools hinzugefügt und sind auf vCenter beschränkt. Bei lokaler Verwendung der Cluster-Anmeldeinformationen ordnen die zugehörigen SVMs automatisch dem vCenter zu, um VVols oder VMFS zu managen. Für VMFS-Management, einschließlich SRA, unterstützen ONTAP-Tools SVM-Zugangsdaten, ohne dass ein globales Cluster erforderlich ist.

Storage Replication Adapter (SRA)

SRA ist die spezifische Storage-Software, die in der VMware Live Site Recovery-Appliance installiert ist. Der Adapter ermöglicht die Kommunikation zwischen dem Site Recovery Manager und einem Storage Controller auf Storage Virtual Machine (SVM)-Ebene und der Konfiguration auf Cluster-Ebene.

Storage Virtual Machine (SVM)

SVM ist die Einheit der Mandantenfähigkeit in ONTAP. Wie eine Virtual Machine, die auf einem Hypervisor ausgeführt wird, ist SVM eine logische Einheit, die physische Ressourcen abstrahiert. SVM enthält Daten-Volumes und ein oder mehrere LIFs, über die sie Daten an die Clients bereitstellen.

Einheitliche und uneinheitliche Konfiguration

- **Einheitlicher Hostzugriff** bedeutet, dass Hosts von zwei Standorten mit allen Pfaden zu Speicherclustern an beiden Standorten verbunden sind. Standortübergreifende Pfade sind über Entfernungen verteilt.
- **Uneinheitlicher Hostzugriff** bedeutet, dass Hosts an jedem Standort nur mit dem Cluster am selben Standort verbunden sind. Standortübergreifende Pfade und gestreckte Pfade sind nicht miteinander verbunden.

Jeder SnapMirror Active Sync Bereitstellung wird ein einheitlicher Host-Zugriff unterstützt. Ein nicht einheitlicher Host-Zugriff wird nur für symmetrische aktiv/aktiv-Implementierungen unterstützt. Erfahren Sie mehr über "Übersicht über die aktive SnapMirror-Synchronisierung in ONTAP".

Virtual Machine File System (VMFS)

VMFS ist ein geclustertes Dateisystem, das zum Speichern von Dateien von virtuellen Maschinen in VMware vSphere-Umgebungen entwickelt wurde.

Virtuelle Volumes (VVols)

vVols bieten eine Abstraktion auf Volume-Ebene für den von einer virtuellen Maschine verwendeten Speicher. Es bietet mehrere Vorteile und stellt eine Alternative zur Verwendung einer herkömmlichen LUN dar. Ein vVol-Datenspeicher ist normalerweise mit einer einzelnen LUN verknüpft, die als Container für vVols fungiert.

VM-Storage-Richtlinie

VM Storage Policies werden im vCenter Server unter Policies and Profiles erstellt. Für VVols erstellen Sie mithilfe von Regeln des NetApp VVols Storage-Typ-Providers eine Regelsammlung.

VMware Live Site Recovery

VMware Live Site Recovery, früher als Site Recovery Manager (SRM) bekannt, bietet Business Continuity, Disaster Recovery, Standortmigration und unterbrechungsfreie Testfunktionen für virtuelle VMware-Umgebungen.

VMware vSphere APIs für Storage Awareness (VASA)

VASA besteht aus APIs, die Storage-Arrays für Management und Administration mit vCenter Server integrieren. Die Architektur basiert auf mehreren Komponenten, einschließlich dem VASA Provider, der die Kommunikation zwischen VMware vSphere und den Storage-Systemen übernimmt.

VMware vSphere Storage-APIs – Array-Integration (VAAI)

VAAI ist ein Satz von APIs, der die Kommunikation zwischen VMware vSphere ESXi-Hosts und den Speichergeräten ermöglicht. Die APIs enthalten eine Reihe von primitiven Operationen, die von den Hosts zur Auslagerung von Speicheroperationen auf das Array verwendet werden. VAAI kann für Storage-intensive Aufgaben erhebliche Performance-Steigerungen bieten.

VSphere Metro Storage-Cluster

VSphere Metro Storage Cluster (vMSC) ist eine Architektur, die vSphere in einer Stretch-Cluster-Implementierung ermöglicht und unterstützt. VMSC Lösungen werden mit NetApp MetroCluster und SnapMirror Active Sync (ehemals SMBC) unterstützt. Diese Lösungen sorgen für verbesserte Business Continuity bei Domänenausfällen. Das Stabilitätsmodell basiert auf Ihren spezifischen Konfigurationsmöglichkeiten. Erfahren Sie mehr über "VMware vSphere Metro Storage-Cluster".

VVols Datastore

Der VVols Datastore ist eine logische Datastore-Darstellung eines VVols-Containers, der von einem VASA Provider erstellt und verwaltet wird.

Kein RPO

RPO steht für den Recovery Point Objective, die Menge des Datenverlusts, der während eines bestimmten Zeitraums als akzeptabel erachtet wird. Ein RPO von null bedeutet, dass kein Datenverlust akzeptabel ist.

Rollenbasierte Zugriffskontrolle (RBAC)

Erfahren Sie mehr über ONTAP tools RBAC

Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ist ein Sicherheits-

Framework zur Steuerung des Zugriffs auf Ressourcen innerhalb eines Unternehmens. RBAC vereinfacht die Administration, indem Rollen mit bestimmten Berechtigungsstufen für Aktionen definiert werden, anstatt einzelnen Benutzern Berechtigungen zuzuweisen. Die definierten Rollen werden Benutzern zugewiesen, was das Fehlerrisiko reduziert und das Management der Zugriffskontrolle im gesamten Unternehmen vereinfacht.

Das RBAC-Standardmodell besteht aus mehreren Implementierungstechnologien oder Phasen mit zunehmender Komplexität. Als Ergebnis können sich die tatsächlichen RBAC-Implementierungen, basierend auf den Anforderungen der Softwareanbieter und ihrer Kunden, von relativ einfach bis sehr komplex unterscheiden.

RBAC-Komponenten

Prinzipiell gibt es mehrere Komponenten, die in der Regel bei jeder RBAC-Implementierung enthalten sind. Diese Komponenten werden im Rahmen der Definition der Autorisierungsprozesse auf unterschiedliche Weise miteinander verknüpft.

Berechtigungen

Ein Privileg ist eine Aktion oder Fähigkeit, die erlaubt oder verweigert werden kann. Es kann sich um etwas Einfaches wie das Lesen einer Datei oder eine abstraktere Operation handeln, die für ein bestimmtes Softwaresystem spezifisch ist. Privileges können auch definiert werden, um den Zugriff auf REST-API-Endpunkte und CLI-Befehle einzuschränken. Jede RBAC-Implementierung enthält vordefinierte Privilegien und ermöglicht Administratoren möglicherweise auch die Erstellung benutzerdefinierter Privilegien.

Rollen

Eine *Rolle* ist ein Container, der eine oder mehrere Privileges enthält. Rollen werden in der Regel anhand bestimmter Aufgaben oder Tätigkeitsbereiche definiert. Wenn einem Benutzer eine Rolle zugewiesen wird, erhält der Benutzer alle Privileges, die in der Rolle enthalten sind. Wie bei Privileges umfassen Implementierungen auch hier vordefinierte Rollen und ermöglichen in der Regel das Erstellen benutzerdefinierter Rollen.

Objekte

Ein *Object* stellt eine reale oder abstrakte Ressource dar, die innerhalb der RBAC-Umgebung identifiziert wird. Die über die Privileges definierten Aktionen werden für oder mit den zugehörigen Objekten ausgeführt. Je nach Implementierung kann Privileges einem Objekttyp oder einer bestimmten Objektinstanz gewährt werden.

Benutzer und Gruppen

Benutzer werden einer nach der Authentifizierung angewendeten Rolle zugewiesen oder zugeordnet. Bei einigen RBAC-Implementierungen kann einem Benutzer nur eine Rolle zugewiesen werden, während bei anderen Rollen pro Benutzer zulässig sind, wobei möglicherweise nur eine Rolle gleichzeitig aktiv ist. Das Zuweisen von Rollen zu *groups* kann die Sicherheitsverwaltung weiter vereinfachen.

Berechtigungen

Eine *permission* ist eine Definition, die einen Benutzer oder eine Gruppe zusammen mit einer Rolle an ein Objekt bindet. Berechtigungen können bei einem hierarchischen Objektmodell nützlich sein, bei dem sie optional von den untergeordneten Objekten in der Hierarchie geerbt werden können.

Zwei RBAC-Umgebungen

Bei der Arbeit mit ONTAP tools for VMware vSphere 10 müssen zwei unterschiedliche RBAC-Umgebungen berücksichtigt werden. ONTAP tools for VMware vSphere 10 benötigen spezifische Berechtigungen sowohl in vCenter als auch in ONTAP , um ihre Funktionen ausführen zu können. Während ONTAP Tools

Speicherverwaltungsaufgaben automatisieren, erstellen sie weder in vCenter noch in ONTAP Benutzerkonten. Servicekonten müssen bei Bedarf von einem vSphere-Administrator erstellt werden. Diese Dokumentation bietet Administratoren eine Anleitung zur Zuweisung der notwendigen Rollen und Berechtigungen für ein effektives ONTAP Tool-Management.

VMware vCenter Server

Die RBAC-Implementierung in VMware vCenter Server wird verwendet, um den Zugriff auf Objekte einzuschränken, die über die Benutzeroberfläche von vSphere Client zugänglich sind. Im Rahmen der Installation von ONTAP Tools für VMware vSphere 10 wurde die RBAC-Umgebung um zusätzliche Objekte erweitert, die die Funktionen von ONTAP Tools darstellen. Der Zugriff auf diese Objekte erfolgt über das Remote-Plug-in. Weitere Informationen finden Sie unter."RBAC-Umgebung für vCenter Server"

ONTAP-Cluster

Die ONTAP Tools für VMware vSphere 10 sind über die ONTAP-REST-API mit einem ONTAP-Cluster verbunden und ermöglichen so Storage-bezogene Vorgänge. Der Zugriff auf die Storage-Ressourcen wird über eine ONTAP-Rolle gesteuert, die mit dem ONTAP-Benutzer verknüpft ist, der während der Authentifizierung angegeben wurde. Weitere Informationen finden Sie unter "RBAC-Umgebung von ONTAP" .

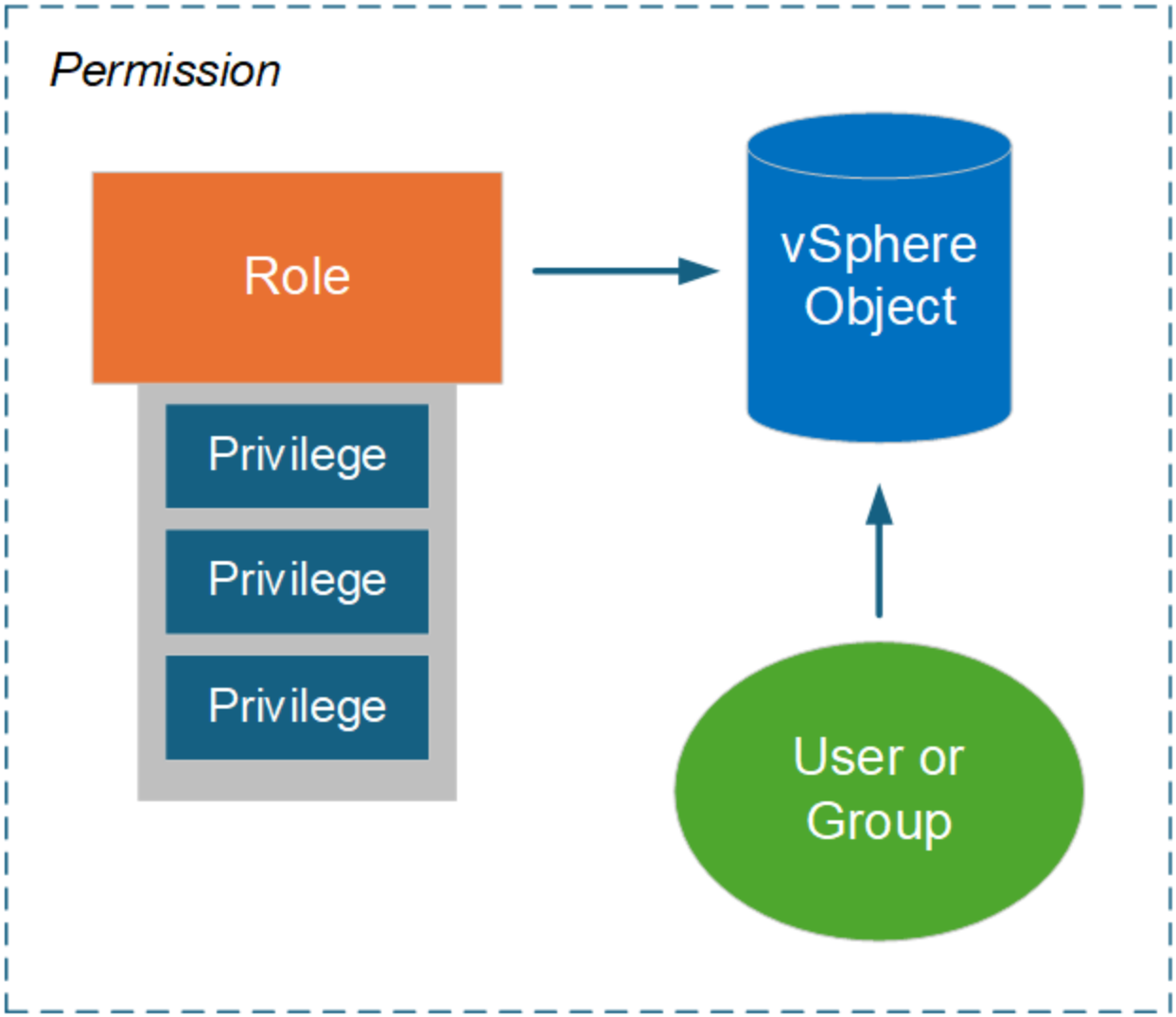
RBAC mit VMware vSphere

Wie vCenter Server-RBAC mit ONTAP tools funktioniert

VMware vCenter Server bietet eine RBAC-Funktion, mit der Sie den Zugriff auf vSphere Objekte steuern können. Dies ist ein wichtiger Teil der zentralisierten Authentifizierungs- und Autorisierungssicherheitsdienste von vCenter.

Abbildung einer vCenter Server-Berechtigung

Eine Berechtigung ist die Grundlage für die Durchsetzung der Zugriffskontrolle in der vCenter Server-Umgebung. Sie wird auf ein vSphere-Objekt mit einem Benutzer oder einer Gruppe angewendet, der in der Berechtigungsdefinition enthalten ist. Die Abbildung unten zeigt eine allgemeine Darstellung einer vCenter-Berechtigung.



Komponenten einer vCenter Server-Berechtigung

Eine vCenter Server-Berechtigung ist ein Paket aus mehreren Komponenten, die bei der Erstellung der Berechtigung miteinander verknüpft sind.

VSphere Objekte

Berechtigungen sind vSphere-Objekten wie vCenter Server, ESXi-Hosts, virtuellen Maschinen, Datastores, Rechenzentren und Ordnern zugeordnet. Anhand der zugewiesenen Berechtigungen des Objekts bestimmt vCenter Server, welche Aktionen oder Aufgaben für das Objekt von jedem Benutzer oder jeder Gruppe ausgeführt werden können. Für die für ONTAP-Tools für VMware vSphere spezifischen Aufgaben werden alle Berechtigungen auf Root- oder Root-Ordnerebene von vCenter Server zugewiesen und validiert. Weitere Informationen finden Sie unter "RBAC mit vCenter Server verwenden" .

Privileges und Rollen

Es gibt zwei Arten von vSphere Privileges, die mit ONTAP-Tools für VMware vSphere 10 verwendet werden. Um die Arbeit mit RBAC in dieser Umgebung zu vereinfachen, bietet ONTAP Tools Rollen, die die erforderlichen nativen und benutzerdefinierten Privileges enthalten. Die Privileges umfassen:

- Native vCenter Server-Berechtigungen

  Dies sind die Privileges, die von vCenter Server bereitgestellt wird.

- Spezifische Berechtigungen für ONTAP-Tools

  Hierbei handelt es sich um individuelle Privileges, die nur bei ONTAP Tools für VMware vSphere üblich sind.

Benutzer und Gruppen

Sie können Benutzer und Gruppen über Active Directory oder die lokale vCenter Server-Instanz definieren. In Kombination mit einer Rolle können Sie eine Berechtigung für ein Objekt in der vSphere-Objekthierarchie erstellen. Die Berechtigung gewährt Zugriff basierend auf den Berechtigungen der zugehörigen Rolle. Beachten Sie, dass Rollen nicht isoliert Benutzern direkt zugewiesen werden. Stattdessen erhalten Benutzer und Gruppen Zugriff auf ein Objekt über Rollenberechtigungen als Teil der umfassenderen vCenter Server-Berechtigung.

vCenter Server-RBAC-Überlegungen für ONTAP tools

Es gibt mehrere Aspekte der ONTAP Tools für die Implementierung von VMware vSphere 10 RBAC mit vCenter Server, die Sie vor Verwendung in einer Produktionsumgebung in Betracht ziehen sollten.

VCenter-Rollen und das Administratorkonto

Sie müssen nur die benutzerdefinierten vCenter Server-Rollen definieren und verwenden, wenn Sie den Zugriff auf die vSphere-Objekte und die zugehörigen administrativen Aufgaben einschränken möchten. Wenn keine Zugriffsbeschränkung erforderlich ist, können Sie stattdessen ein Administratorkonto verwenden. Jedes Administratorkonto wird mit der Administratorrolle auf der obersten Ebene der Objekthierarchie definiert. Dies bietet vollen Zugriff auf die vSphere Objekte, einschließlich derer, die von ONTAP Tools für VMware vSphere 10 hinzugefügt wurden.

VSphere Objekthierarchie

Die vSphere-Objektinventar ist in einer Hierarchie organisiert. Sie können die Hierarchie beispielsweise wie folgt nach unten verschieben:

`vCenter Server --> Datacenter --> Cluster --> Virtual Machine> ESXi host`

Alle Berechtigungen werden in der vSphere-Objekthierarchie mit Ausnahme der VAAI-Plug-in-Vorgänge validiert, die auf dem Ziel-ESXi-Host validiert werden.

In ONTAP Tools für VMware vSphere 10 enthaltene Rollen

Um die Arbeit mit RBAC für vCenter Server zu vereinfachen, bieten die ONTAP Tools für VMware vSphere vordefinierte Rollen, die auf verschiedene Administrationsaufgaben zugeschnitten sind.

> Sie können bei Bedarf neue benutzerdefinierte Rollen erstellen. In diesem Fall sollten Sie eine der vorhandenen Rollen des ONTAP-Tools klonen und sie bei Bedarf bearbeiten. Nachdem Sie die Konfigurationsänderungen vorgenommen haben, müssen sich die betroffenen vSphere-Client-Benutzer ab- und wieder anmelden, um die Änderungen zu aktivieren.

Um die ONTAP tools for VMware vSphere -Rollen anzuzeigen, wählen Sie oben im vSphere Client **Menü** und klicken Sie links auf **Administration** und dann auf **Rollen**. Die folgenden Berechtigungen müssen in der Rolle enthalten sein, die dem vCenter-Benutzer zugewiesen wird, der für die Bereitstellung oder das Onboarding von vCenter verantwortlich ist. Stellen Sie sicher, dass diese Berechtigungen als Voraussetzung für den Bereitstellungs- oder Onboarding-Prozess konfiguriert sind.

- Alarm
  - Alarm bestätigen
- Inhaltsbibliothek
  - Bibliothekselement hinzufügen
  - Vorlage einchecken
  - Schau dir eine Vorlage an
  - Dateien herunterladen
  - Importspeicher
  - Lesespeicher
  - Bibliothekselement synchronisieren
  - Synchronisierung der abonnierten Bibliothek
  - Konfigurationseinstellungen anzeigen
- Datenspeicher
  - Speicherplatz zuweisen
  - Datenspeicher durchsuchen
  - Dateivorgänge auf niedriger Ebene
  - Datei entfernen
  - Aktualisieren der Dateien der virtuellen Maschine
  - Aktualisieren der Metadaten virtueller Maschinen
- ESX Agent Manager
  - Anzeigen
- Ordner
  - Ordner erstellen
- Gastgeber
  - Konfiguration
    - Erweiterte Einstellungen
    - Einstellungen ändern
    - Netzwerkkonfiguration
    - Systemressourcen
    - Konfiguration für den automatischen Start der virtuellen Maschine
  - Lokale Operationen
    - Erstellen einer virtuellen Maschine
    - Virtuelle Maschine löschen

        - Virtuelle Maschine neu konfigurieren
- Netzwerk
    - Netzwerk zuweisen
    - Konfigurieren
- OvfManager
    - Ovf-Verbraucherzugang
- Hostprofil
    - Anzeigen
- Ressource
    - Weisen Sie die virtuelle Maschine dem Ressourcenpool zu.
- Geplante Aufgabe
    - Aufgaben erstellen
    - Aufgabe ändern
    - Aufgabe ausführen
- Aufgaben
    - Aufgabe erstellen
    - Aufgabe aktualisieren
- vApp
    - Virtuelle Maschine hinzufügen
    - Ressourcenpool zuweisen
    - vApp zuweisen
    - Erstellen
    - Import
    - Bewegen
    - Strom aus
    - Strom einschalten
    - Aus URL abrufen
    - OVF-Umgebung anzeigen
- Virtual Machine
    - Konfiguration ändern
        - Vorhandene Festplatte hinzufügen
        - Neue Festplatte hinzufügen
        - Gerät hinzufügen oder entfernen
        - Erweiterte Konfiguration
        - CPU-Anzahl ändern
        - Speicher ändern
        - Einstellungen ändern

        - Ressource ändern
        - Virtuelle Festplatte erweitern
        - Geräteeinstellungen ändern
        - Datenträger entfernen
        - Gastinformationen zurücksetzen
        - Kompatibilität mit virtuellen Maschinen verbessern
    - Inventar bearbeiten
        - Aus bestehenden erstellen
        - Neu erstellen
        - Bewegen
        - Anmeldung
        - Entfernen
        - Abmelden
    - Interaktion
        - Sicherungsvorgang auf virtueller Maschine
        - CD-Medien konfigurieren
        - Diskettenmedien konfigurieren
        - Geräte verbinden
        - Konsoleninteraktion
        - Gastbetriebssystemverwaltung über die VIX-API
        - Strom aus
        - Strom einschalten
        - Zurücksetzen
        - Aussetzen
    - Bereitstellung
        - Festplattenzugriff zulassen
        - Klonvorlage
        - Gäste anpassen
        - Bereitstellungsvorlage
        - Anpassungsspezifikation ändern
        - Lesen Sie die Anpassungsspezifikationen.
    - Snapshot-Verwaltung
        - Snapshot erstellen
        - Snapshot entfernen
        - Snapshot umbenennen
        - Auf Snapshot zurücksetzen

Es gibt drei vordefinierte Rollen, die unten beschrieben werden.

NetApp ONTAP-Tools für VMware vSphere Administrator

Bietet alle nativen vCenter Server Privileges- und ONTAP-Tools-spezifischen Privileges, die für das Ausführen zentraler ONTAP Tools für VMware vSphere Administratoraufgaben erforderlich sind.

NetApp ONTAP-Tools für VMware vSphere schreibgeschützt

Bietet schreibgeschützten Zugriff auf ONTAP Tools. Diese Benutzer können keine ONTAP Tools für VMware vSphere Aktionen ausführen, die zugriffsgesteuert sind.

NetApp ONTAP Tools für VMware vSphere Bereitstellung

Bietet einige der nativen vCenter Server-Berechtigungen und ONTAP-Tools-spezifischen Berechtigungen, die für die Bereitstellung von Speicher erforderlich sind. Sie können die folgenden Aufgaben ausführen:

- Erstellen neuer Datenspeicher
- Managen von Datastores

VSphere Objekte und ONTAP Storage Back-Ends

Die beiden RBAC-Umgebungen arbeiten zusammen. Bei der Ausführung einer Aufgabe in der vSphere-Client-Schnittstelle werden zunächst die für vCenter Server definierten ONTAP-Tools-Rollen aktiviert. Wenn der Vorgang von vSphere zugelassen ist, werden die ONTAP-Rollen-Privileges untersucht. Dieser zweite Schritt basiert auf der ONTAP-Rolle, die dem Benutzer beim Erstellen und Konfigurieren des Storage-Backends zugewiesen wurde.

Arbeiten mit vCenter Server RBAC

Beim Arbeiten mit vCenter Server Privileges und Berechtigungen sind einige Punkte zu beachten.

Erforderliche Berechtigungen

Um auf die Benutzeroberfläche von ONTAP Tools für VMware vSphere 10 zuzugreifen, müssen Sie über die spezifische Berechtigung „Ansicht“ für die ONTAP Tools verfügen. Wenn Sie sich ohne diese Berechtigung bei vSphere anmelden und auf das Symbol NetApp klicken, zeigt ONTAP Tools für VMware vSphere eine Fehlermeldung an und verhindert, dass Sie auf die Benutzeroberfläche zugreifen können.

Die Zuweisungsebene in der vSphere-Objekthierarchie bestimmt, auf welche Teile der Benutzeroberfläche Sie zugreifen können. Wenn Sie dem Stammobjekt die Berechtigung Ansicht zuweisen, können Sie auf ONTAP-Tools für VMware vSphere zugreifen, indem Sie auf das Symbol NetApp klicken.

Sie können stattdessen die Berechtigung View einer anderen niedrigeren vSphere Objektebene zuweisen. Dies beschränkt jedoch die ONTAP Tools für VMware vSphere Menüs, auf die Sie zugreifen können und die Sie verwenden können.

Berechtigungen werden zugewiesen

Sie müssen vCenter Server-Berechtigungen verwenden, wenn Sie den Zugriff auf die vSphere-Objekte und -Aufgaben einschränken möchten. Wenn Sie Berechtigungen in der vSphere-Objekthierarchie zuweisen, bestimmt dies die ONTAP-Tools für VMware vSphere 10-Aufgaben, die Benutzer ausführen können.

Sofern Sie keinen restriktiveren Zugriff definieren müssen, empfiehlt es sich in der Regel, Berechtigungen auf Root-Objekt- oder Root-Ordnerebene zuzuweisen.

Die mit den ONTAP-Tools für VMware vSphere 10 verfügbaren Berechtigungen gelten für benutzerdefinierte nicht-vSphere-Objekte, wie z. B. Speichersysteme. Wenn möglich, sollten Sie diese Berechtigungen ONTAP-

Tools für VMware vSphere-Stammobjekt zuweisen, da es kein vSphere-Objekt gibt, dem Sie es zuweisen können. Beispielsweise sollten alle Berechtigungen, die eine Berechtigung zum Hinzufügen/Ändern/Entfernen von Speichersystemen von ONTAP-Tools für VMware vSphere enthalten, auf der Root-Objektebene zugewiesen werden.

Wenn Sie eine Berechtigung auf einer höheren Ebene in der Objekthierarchie definieren, können Sie die Berechtigung so konfigurieren, dass sie von den untergeordneten Objekten weitergegeben und vererbt wird. Bei Bedarf können Sie den untergeordneten Objekten zusätzliche Berechtigungen zuweisen, die die vom übergeordneten Objekt geerbten Berechtigungen überschreiben.

Sie können eine Berechtigung jederzeit ändern. Wenn Sie eine der Privileges innerhalb einer Berechtigung ändern, müssen sich Benutzer, die mit der Berechtigung verknüpft sind, bei vSphere abmelden und sich erneut anmelden, um die Änderung zu aktivieren.

RBAC mit ONTAP

Wie ONTAP RBAC mit ONTAP tools funktioniert

ONTAP bietet eine robuste und erweiterbare RBAC-Umgebung. Über die RBAC-Funktion kann der Zugriff auf Storage- und Systemvorgänge gesteuert werden, da diese über die REST-API und CLI offengelegt werden. Es ist besonders hilfreich, mit der Umgebung vertraut zu sein, bevor sie mit ONTAP Tools für die Implementierung von VMware vSphere 10 verwendet wird.

Überblick über die administrativen Optionen

Bei der Nutzung von ONTAP RBAC stehen Ihnen je nach Umgebung und Zielen verschiedene Optionen zur Verfügung. Im Folgenden wird ein Überblick über die wichtigsten Verwaltungsentscheidungen gegeben. Weitere Informationen finden Sie unter "ONTAP Automatisierung: Überblick über die RBAC-Sicherheit".

> ONTAP RBAC ist auf eine Speicherumgebung zugeschnitten und einfacher als die mit vCenter Server bereitgestellte RBAC-Implementierung. Mit ONTAP weisen Sie dem Benutzer direkt eine Rolle zu. Das Konfigurieren expliziter Berechtigungen, wie sie beispielsweise bei vCenter Server verwendet werden, ist bei ONTAP RBAC nicht erforderlich.

Rollen- und Privileges-Typen

Beim Definieren eines ONTAP-Benutzers ist eine ONTAP-Rolle erforderlich. Es gibt zwei Arten von ONTAP-Rollen:

- RUHE

  DIE REST-Funktionen wurden mit ONTAP 9.6 eingeführt und werden in der Regel für Benutzer angewendet, die über DIE REST-API auf ONTAP zugreifen. Die in diesen Rollen enthaltenen Privileges werden als Zugriff auf die ONTAP REST-API-Endpunkte und die zugehörigen Aktionen definiert.

- Traditionell

  Hierbei handelt es sich um die älteren Rollen, die vor ONTAP 9.6 enthalten sind. Sie sind weiterhin ein grundlegender Aspekt der RBAC. Die Privileges sind für den Zugriff auf die ONTAP-CLI-Befehle definiert.

Während die ÜBRIGEN Rollen in jüngster Zeit eingeführt wurden, haben die traditionellen Rollen einige Vorteile. So können optional zusätzliche Abfrageparameter einbezogen werden, damit die Privileges die

Objekte genauer definieren, auf die sie angewendet werden.

Umfang

ONTAP-Rollen können mit einem von zwei verschiedenen Bereichen definiert werden. Sie können auf eine bestimmte Daten-SVM (SVM-Ebene) oder auf das gesamte ONTAP-Cluster (Cluster-Ebene) angewendet werden.

Rollendefinitionen

ONTAP bietet vordefinierte Rollen auf Cluster- und SVM-Ebene. Sie können auch benutzerdefinierte Rollen definieren.

Arbeiten mit ONTAP-REST-Rollen

Bei der Verwendung der in ONTAP Tools für VMware vSphere 10 enthaltenen ONTAP REST-Rollen müssen verschiedene Aspekte berücksichtigt werden.

Rollenzuordnung

Alle Entscheidungen für den ONTAP-Zugriff basierend auf dem zugrunde liegenden CLI-Befehl werden unabhängig davon getroffen, ob sie eine klassische Rolle oder eine REST-Rolle verwenden. Da die Privileges in einer REST-Rolle jedoch in Bezug auf die REST-API-Endpunkte definiert sind, muss ONTAP für jede der REST-Rollen eine traditionelle *Mapping* Rolle erstellen. Daher wird jede REST-Rolle einer zugrunde liegenden herkömmlichen Rolle zugeordnet. Dadurch kann ONTAP unabhängig vom Rollentyp Entscheidungen zur Zugriffssteuerung konsistent treffen. Sie können die parallel zugeordneten Rollen nicht ändern.

Definieren einer REST-Rolle mithilfe von CLI-Privileges

Da ONTAP immer die CLI-Befehle verwendet, um den Zugriff auf Basisebene zu bestimmen, kann eine REST-Rolle über den CLI-Befehl Privileges anstelle von REST-Endpunkten ausgedrückt werden. Ein Vorteil dieses Ansatzes ist die zusätzliche Granularität, die mit den herkömmlichen Rollen verfügbar ist.

Administratorschnittstelle beim Definieren von ONTAP-Rollen

Sie können Benutzer und Rollen mit der ONTAP-CLI und REST-API erstellen. Es empfiehlt sich jedoch, die Benutzeroberfläche von System Manager zusammen mit der JSON-Datei zu verwenden, die über den ONTAP Tools Manager verfügbar ist. Weitere Informationen finden Sie unter "Nutzen Sie die rollenbasierte Zugriffssteuerung von ONTAP mit ONTAP-Tools für VMware vSphere 10" .

ONTAP RBAC-Überlegungen für ONTAP tools

Es gibt verschiedene Aspekte der ONTAP Tools für die Implementierung der rollenbasierten Zugriffssteuerung von VMware vSphere 10 mit ONTAP, die Sie vor dem Einsatz in einer Produktionsumgebung in Betracht ziehen sollten.

Überblick über den Konfigurationsprozess

ONTAP tools for VMware vSphere umfassen Unterstützung für die Erstellung eines ONTAP Benutzers mit einer benutzerdefinierten Rolle. Die Definitionen sind in einer JSON-Datei verpackt, die Sie in den ONTAP Cluster hochladen können. Sie können den Benutzer erstellen und die Rolle an Ihre Umgebung und Sicherheitsanforderungen anpassen.

Die wichtigsten Konfigurationsschritte werden auf einer der folgenden Ebenen beschrieben. "Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen"Weitere Informationen finden Sie unter.

1. Vorbereiten

Sie müssen über Administratoranmeldeinformationen sowohl für den ONTAP Tools Manager als auch für den

ONTAP Cluster verfügen.

2. Laden Sie die JSON-Definitionsdatei herunter

Nachdem Sie sich bei der Benutzeroberfläche von ONTAP Tools Manager angemeldet haben, können Sie die JSON-Datei mit den RBAC-Definitionen herunterladen.

3. Erstellen Sie einen ONTAP-Benutzer mit einer Rolle

Nach der Anmeldung bei System Manager können Sie den Benutzer und die Rolle erstellen:

1. Wählen Sie **Cluster** auf der linken Seite und dann **Einstellungen**.
2. Scrollen Sie nach unten zu **Benutzer und Rollen** und klicken Sie auf –→.
3. Wählen Sie **Add** unter **Users** und wählen Sie **Virtualization products** aus.
4. Wählen Sie die JSON-Datei auf Ihrer lokalen Workstation aus, und laden Sie sie hoch.

4. Konfigurieren Sie die Rolle

Im Rahmen der Definition der Rolle müssen Sie mehrere administrative Entscheidungen treffen. Weitere Informationen finden Sie unterKonfigurieren Sie die Rolle mit System Manager.

Konfigurieren Sie die Rolle mit System Manager

Nachdem Sie mit dem Erstellen eines neuen Benutzers und einer neuen Rolle mit System Manager begonnen und die JSON-Datei hochgeladen haben, können Sie die Rolle auf Ihre Umgebung und Ihre Anforderungen abstimmen.

Konfiguration von Kernbenutzern und -Rollen

Die RBAC-Definitionen sind in Form von verschiedenen Produktfunktionen gebündelt, darunter Kombinationen von VSC, VASA Provider und SRA. Wählen Sie die Umgebung oder die Umgebungen aus, in denen die RBAC-Unterstützung benötigt wird. Wenn Rollen beispielsweise die Remote Plug-in-Funktion unterstützen sollen, wählen Sie VSC aus. Außerdem müssen Sie den Benutzernamen und das zugehörige Kennwort auswählen.

Berechtigungen

Die Rolle Privileges sind in vier Sets basierend auf der Zugriffsebene angeordnet, die für den ONTAP Storage erforderlich ist. Zu den Privileges, auf denen die Rollen basieren, gehören:

- Ermitteln

  Diese Rolle ermöglicht es Ihnen, Storage-Systeme hinzuzufügen.

- Storage erstellen

  Mit dieser Rolle können Sie Speicher erstellen. Er umfasst außerdem alle Privileges, die der Erkennungsrolle zugeordnet sind.

- Speicher ändern

  Mit dieser Rolle können Sie Speicher ändern. Er umfasst auch alle Privileges, die der Ermittlung zugeordnet sind und Storage-Rollen erstellen.

- Zerstören Sie den Speicher

Mit dieser Rolle können Sie Speicher zerstören. Sie umfasst auch alle Privileges, die der Ermittlung zugeordnet sind, Speicher erstellen und Speicherrollen ändern.

Benutzer mit einer Rolle generieren

Nachdem Sie die Konfigurationsoptionen für Ihre Umgebung ausgewählt haben, klicken Sie auf **Hinzufügen** und ONTAP erstellt den Benutzer und die Rolle. Der Name der generierten Rolle ist eine Verkettung der folgenden Werte:

- In der JSON-Datei definierter konstanter Präfixwert (z.B. „OTV_10“)
- Ausgewählte Produktfunktion
- Liste der Berechtigungssätze.

Beispiel

```
OTV_10_VSC_Discovery_Create
```

Der neue Benutzer wird der Liste auf der Seite "Benutzer und Rollen" hinzugefügt. Beachten Sie, dass sowohl HTTP- als auch ONTAPI-Benutzeranmeldemethoden unterstützt werden.

Implementieren Sie ONTAP-Tools für VMware vSphere

Schnellstart für ONTAP-Tools für VMware vSphere

Richten Sie mit diesem Schnellstartabschnitt ONTAP tools for VMware vSphere ein.

Zunächst stellen Sie ONTAP tools for VMware vSphere als kleine Einzelknotenkonfiguration bereit, die Kerndienste zur Unterstützung von NFS- und VMFS-Datenspeichern bereitstellt. Um Ihre Konfiguration für zusätzliche Container pro Dienst, verbesserte Ausfallsicherheit oder die Verwendung von vVols -Datenspeichern und Hochverfügbarkeit (HA) zu erweitern, schließen Sie zuerst diesen Workflow ab und fahren Sie dann mit den Erweiterungsschritten fort. Weitere Informationen finden Sie im "HA-Implementierungs-Workflow" .

Planen Sie Ihre Implementierung

Stellen Sie sicher, dass Ihre vSphere-, ONTAP und ESXi-Hostversionen mit der ONTAP Toolversion kompatibel sind. Stellen Sie ausreichend CPU-, Arbeitsspeicher- und Festplattenspeicher bereit. Abhängig von Ihren Sicherheitsregeln müssen Sie möglicherweise Firewalls oder andere Sicherheitstools einrichten, um Netzwerkverkehr zuzulassen.

Stellen Sie sicher, dass vCenter Server installiert ist und zugänglich ist.

- "Interoperabilitäts-Matrix-Tool"
- "ONTAP-Tools für VMware vSphere – Anforderungen und Konfigurationsgrenzen"
- "Bevor Sie beginnen"

Implementieren Sie ONTAP-Tools für VMware vSphere

Zunächst implementieren Sie ONTAP tools for VMware vSphere als kleine Einzelknotenkonfiguration, die Kerndienste zur Unterstützung von NFS- und VMFS-Datenspeichern bereitstellt. Wenn Sie Ihre Konfiguration um vVols Datenspeicher und Hochverfügbarkeit (HA) erweitern möchten, tun Sie dies nach Abschluss dieses Workflows. Stellen Sie für die Erweiterung auf ein HA-Setup sicher, dass CPU-Hot-Add und Memory-Hot-Plug aktiviert sind.

- "Implementieren Sie ONTAP-Tools für VMware vSphere"

Fügen Sie vCenter Server-Instanzen hinzu

Fügen Sie vCenter Server-Instanzen zu ONTAP tools for VMware vSphere hinzu, um virtuelle Datenspeicher in der vCenter Server-Umgebung zu konfigurieren, zu verwalten und zu schützen.

- "Fügen Sie vCenter Server-Instanzen hinzu"

Konfigurieren Sie ONTAP-Benutzerrollen und Privileges

Konfigurieren Sie neue Benutzerrollen und Privileges für das Management von Storage-Back-Ends mit der JSON-Datei, die in den ONTAP Tools für VMware vSphere bereitgestellt wird.

- "Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen"

5 **Konfigurieren Sie die Speicher-Back-Ends**

Hinzufügen eines Storage-Back-End zu einem ONTAP Cluster Wenn vCenter für mandantenfähige Konfigurationen als Mandant mit einer entsprechenden SVM fungiert, fügen Sie das Cluster mithilfe des ONTAP Tools Manager hinzu. Verknüpfen Sie das Storage-Backend mit dem vCenter Server, um es global der eingenommenen vCenter Server-Instanz zuzuordnen.

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.

- "Fügen Sie ein Storage-Back-End hinzu"
- "Ordnen Sie das Storage-Back-End einer vCenter Server-Instanz zu"

6 **Aktualisieren Sie die Zertifikate, wenn Sie mit mehreren vCenter Server-Instanzen arbeiten**

Wenn Sie mit mehreren vCenter Server-Instanzen arbeiten, aktualisieren Sie das selbstsignierte Zertifikat auf ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat.

- "Verwalten von Zertifikaten"

7 **(Optional) Konfigurieren des SRA-Schutzes**

Stellen Sie die SRA-Funktionen bereit, um Disaster Recovery zu konfigurieren und NFS- oder VMFS-Datastores zu schützen.

- "Aktivieren Sie ONTAP-Tools für VMware vSphere-Services"
- "Konfigurieren Sie SRA auf der VMware Live Site Recovery-Appliance"

8 **(Optional) Aktivieren Sie den SnapMirror-Schutz für aktive Synchronisierung**

Konfigurieren Sie ONTAP-Tools für VMware vSphere, um den Schutz des Host-Clusters für die aktive SnapMirror-Synchronisierung zu managen. Führen Sie das ONTAP-Cluster- und SVM-Peering in ONTAP-Systemen durch, um SnapMirror Active Sync zu verwenden. Dies gilt nur für VMFS Datastores.

- "Schützen mit Host-Cluster-Schutz"

9 **Richten Sie Backup und Recovery für Ihre ONTAP Tools zur Implementierung von VMware vSphere ein**

Die Sicherung ist in den ONTAP tools for VMware vSphere 10.5 standardmäßig aktiviert und erfolgt alle 10 Minuten. Planen Sie Backups Ihrer ONTAP tools for VMware vSphere -Setup, mit denen Sie das Setup im Fehlerfall wiederherstellen können.

- "Bearbeiten der Sicherungseinstellungen"

- "Wiederherstellen des ONTAP Tools-Setups"

Workflow für die Hochverfügbarkeitsbereitstellung von ONTAP tools

Um die Ausfallsicherheit zu erhöhen und mehr Container pro Dienst zu unterstützen, erweitern Sie Ihre anfängliche ONTAP Toolbereitstellung auf eine Hochverfügbarkeitskonfiguration (HA). Für vVols Datenspeicher in einem HA-Setup ist die Aktivierung des VASA-Provider-Dienstes erforderlich.

Vertikale Skalierung der Implementierung

Sie können die Konfiguration der ONTAP Tools für VMware vSphere vertikal skalieren, um die Anzahl der Nodes in der Implementierung zu erhöhen und die Konfiguration zu einem HA-Setup zu ändern.

- "Ändern Sie ONTAP-Tools für die VMware vSphere Konfiguration"

Aktivieren Sie Services

Um vVols Datenspeicher zu konfigurieren, müssen Sie den VASA Provider-Dienst aktivieren. Registrieren Sie den VASA-Anbieter bei vCenter und stellen Sie sicher, dass Ihre Speicherrichtlinien die HA-Anforderungen erfüllen, einschließlich der richtigen Netzwerk- und Speicherkonfigurationen.

Aktivieren Sie die SRA-Dienste zur Verwendung von ONTAP-Tools Storage Replication Adapter (SRA) für VMware Site Recovery Manager (SRM) oder VMware Live Site Recovery (VLSR).

- "Aktivieren Sie VASA Provider- und SRA-Services"

Aktualisieren Sie die Zertifikate

Wenn Sie vVol-Datastores mit mehreren vCenter Server-Instanzen verwenden, aktualisieren Sie das selbstsignierte Zertifikat auf ein signiertes Zertifikat einer Zertifizierungsstelle (CA).

- "Verwalten von Zertifikaten"

ONTAP-Tools für VMware vSphere – Anforderungen und Konfigurationsgrenzen

Vor der Bereitstellung der ONTAP Tools für VMware vSphere sollten Sie mit den Speicherplatzanforderungen für das Deployment-Paket und einigen grundlegenden Anforderungen an das Host-System vertraut sein.

Sie können ONTAP-Tools für VMware vSphere mit der virtuellen VMware vCenter Server-Appliance (vCSA) verwenden. Sie sollten ONTAP-Tools für VMware vSphere auf einem unterstützten vSphere-Client mit ESXi-System implementieren.

Systemanforderungen

- **Platzanforderungen für Installationspaket pro Knoten**
  - 15 GB bei Thin Provisioning-Installationen
  - 348 GB für Thick Provisioning-Installationen
- **Anforderungen an die Dimensionierung des Hostsystems** Die folgende Tabelle zeigt den empfohlenen Arbeitsspeicher für jede Bereitstellungsgröße. Für Bereitstellungen mit hoher Verfügbarkeit (HA) benötigen Sie die dreifache Appliance-Größe, die angegeben ist.

Art der Bereitstellung	CPUs pro Knoten	Arbeitsspeicher (GB) pro Node	Speicherplatz (GB) Thick Provisioning pro Knoten
Klein	9	18	350
Mittel	13	26	350
HINWEIS: Bei der großen Implementierung geht es nur um die HA-Konfiguration.	17	34	350

Wenn Backup aktiviert ist, benötigt jeder Cluster mit ONTAP Tools weitere 50 GB Speicherplatz auf dem Datenspeicher, auf dem die VMs implementiert werden. Daher sind für nicht-HA 400 GB und für HA insgesamt 1100 GB Speicherplatz erforderlich.

Mindestanforderungen hinsichtlich Storage und Applikationen

Storage, Host und Applikationen	Versionsanforderungen
ONTAP	9.15.1, 9.16.1 und 9.17.0
Von ONTAP Tools unterstützte ESXi-Hosts	Ab 7.0.3
ONTAP Tools unterstützten vCenter Server	7.0U3 ab
VASA Provider	3.0
OVA-Anwendung	10,5
ESXi-Host zur Implementierung der virtuellen Maschine mit ONTAP-Tools	7.0U3 und 8.0U3
VCenter Server zur Bereitstellung einer virtuellen Maschine mit ONTAP-Tools	7.0 und 8.0

Ab ONTAP-Tools für VMware vSphere 10.4 wird die Hardware der virtuellen Maschine von Version 10 auf 17 geändert.

Das Interoperabilitäts-Matrix-Tool (IMT) enthält aktuelle Informationen zu den unterstützten Versionen von ONTAP, vCenter Server, ESXi-Hosts und Plug-in-Applikationen.

"Interoperabilitäts-Matrix-Tool"

Port-Anforderungen

Die folgende Tabelle zeigt die von NetApp verwendeten Netzwerkports und deren Zweck. Es gibt drei verschiedene Arten von Anschlüssen:

- Externe Ports: Diese Ports sind von außerhalb des Kubernetes-Clusters oder -Knotens zugänglich. Sie ermöglichen es Diensten, mit externen Netzwerken oder Benutzern zu kommunizieren und so die Integration mit Systemen außerhalb der Clusterumgebung zu ermöglichen.
- Inter-Node-Ports: Diese Ports ermöglichen die Kommunikation zwischen den Knoten innerhalb des Kubernetes-Clusters. Sie werden für Clusteraufgaben wie den Datenaustausch und die Zusammenarbeit benötigt. Bei Einzelknoten-Bereitstellungen werden die Inter-Node-Ports nur innerhalb des Knotens verwendet und benötigen keinen externen Zugriff. Inter-Node-Ports können Datenverkehr von außerhalb des Clusters akzeptieren. Sperren Sie den Internetzugang zwischen den Knoten mithilfe von Firewall-Regeln.
- Interne Ports: Diese Ports kommunizieren innerhalb des Kubernetes-Clusters über ClusterIP-Adressen. Sie sind nicht extern zugänglich und müssen nicht zu Firewall-Regeln hinzugefügt werden.

Stellen Sie sicher, dass sich alle ONTAP Tool-Knoten im selben Subnetz befinden, um eine unterbrechungsfreie Kommunikation untereinander aufrechtzuerhalten.

Klicken Sie, um die Tabelle mit den Portanforderungen ein- oder auszublenden.

Dienst-/Komponentenname	Port	Protokoll	Anschlusstyp	Beschreibung
ntv-gateway-svc (LB)	443, 8443	TCP	Extern	Durchgangsport für eingehende Kommunikation für den VASA-Provider-Dienst. Auf diesem Port werden das selbstsignierte Zertifikat des VASA-Anbieters und das benutzerdefinierte CA-Zertifikat gehostet.
SSH	22	TCP	Extern	Secure Shell für die Anmeldung am Remote-Server und die Ausführung von Befehlen.
rke2-Server	9345	TCP	Zwischenknoten	RKE2 Supervisor API (Beschränkung auf vertrauenswürdige Netzwerke).
kube-apiserver	6443	TCP	Zwischenknoten	Kubernetes API-Server-Port (auf vertrauenswürdige Netzwerke beschränken).
rpcbind/portmapper	111	TCP/UDP	Zwischenknoten	Wird für die RPC-Kommunikation zwischen Diensten verwendet.
coredns (DNS)	53	TCP/UDP	Zwischenknoten	Domain Name System (DNS)-Dienst zur Namensauflösung innerhalb des Clusters.
NTP	123	UDP	Zwischenknoten	Netzwerkzeitprotokoll (NTP) zur Zeitsynchronisation.

Dienst-/Komponentenname	Port	Protokoll	Anschlusstyp	Beschreibung
etcd	2379, 2380, 2381	TCP	Zwischenknoten	Schlüsselwertspeicher für Clusterdaten.
kube-vip	2112	TCP	Zwischenknoten	Kubernetes API-Server-Port.
kubelet	10248, 10250	TCP	Zwischenknoten	Kubernetes-Komponente
kube-controller	10257	TCP	Zwischenknoten	Kubernetes-Komponente
Cloud-Controller	10258	TCP	Zwischenknoten	Kubernetes-Komponente
kube-scheduler	10259	TCP	Zwischenknoten	Kubernetes-Komponente
kube-proxy	10249, 10256	TCP	Zwischenknoten	Kubernetes-Komponente
Kaliko-Knoten	9091, 9099	TCP	Zwischenknoten	Calico-Netzwerkkomponente.
containerd	10010	TCP	Zwischenknoten	Container-Daemon-Dienst.
VXLAN (Flannel)	8472	UDP	Zwischenknoten	Overlay-Netzwerk für die Pod-Kommunikation.

Bei HA-Bereitstellungen muss sichergestellt werden, dass der UDP-Port 8472 zwischen allen Knoten geöffnet ist. Dieser Port ermöglicht die Kommunikation zwischen Pods über verschiedene Knoten hinweg; durch Blockierung wird die Netzwerkverbindung zwischen den Knoten unterbrochen.

Konfigurationsbeschränkungen für die Bereitstellung von ONTAP tools for VMware vSphere für vVols Datenspeicher

Sie können die folgende Tabelle als Leitfaden für die Konfiguration von ONTAP tools for VMware vSphere verwenden.

* Bereitstellung*	Typ	Anzahl der VVols	Anzahl der Hosts
Ohne HA	Klein (S)	bis zu 12K	32
Ohne HA	Mittel (M)	bis zu 24K	64
Hochverfügbarkeit	Klein (S)	bis zu 24K	64
Hochverfügbarkeit	Mittel (M)	bis zu 50k	128

Hochverfügbarkeit	Groß (L)	bis zu 100k	256

Die Host-Zahlen in der Tabelle stellen die kombinierte Gesamtzahl über alle verbundenen vCenters dar.

Konfigurationsbeschränkungen für die Bereitstellung von ONTAP tools for VMware vSphere für VMFS- und NFS-Datenspeicher

Die in diesem Abschnitt aufgeführten Konfigurationsgrenzen sind von NetApp validiert und unterstützt. Die tatsächlichen Grenzen können je nach Umgebung und Arbeitslast variieren. Eine Überschreitung dieser Grenzen kann die Leistung oder die Supportfähigkeit beeinträchtigen und wird nicht empfohlen. Beachten Sie Folgendes bei der Durchsicht der Tabelle:

- Die Notfallwiederherstellung (Disaster Recovery, DR) virtueller Maschinen wird mithilfe von synchronen, asynchronen oder strikten Sync-Richtlinien konfiguriert. DR wird für das NVMe-Protokoll nicht unterstützt.
- Der ESXi-Hostclusterschutz verwendet SnapMirror Active Sync, welches keine Multi-vCenter-Bereitstellungen unterstützt.
- ONTAP tools beschränkt lediglich die Anzahl der ESXi-Hosts und Datenspeicher basierend auf der Bereitstellungsgröße. Es gibt keine Beschränkungen hinsichtlich der Anzahl der vCenter Server, die mit ONTAP tools verbunden werden können.
- ONTAP tools führt eine parallele Erkennung aller Speicherobjekte durch. Konfigurationsbeschränkungen für ONTAP-Speicherobjekte gelten unabhängig von der Anzahl der aktiv verwendeten Objekte.
- ONTAP tools legt keine Beschränkung hinsichtlich der Anzahl der vCenter Servers fest, die integriert werden können. Die Konfigurationsbeschränkungen werden durch die Anzahl der unterstützten Hosts und Datenspeicher bestimmt, wie in der folgenden Tabelle aufgeführt.

Bereitstellung	Anzahl der VMFS- und NFS-Datenspeicher	Anzahl der DR-fähigen VMFS-Datenspeicher	Anzahl der Hosts
Nicht-HA klein	200	80	32
Non-HA Medium	250	100	32
HA klein	350	200	64
HA Mittel	600	200	128
HA groß	1024	250	256

ONTAP Tools für VMware vSphere – Storage Replication Adapter (SRA)

In der folgenden Tabelle sind die Zahlen aufgeführt, die pro VMware Live Site Recovery-Instanz mithilfe von ONTAP Tools für VMware vSphere unterstützt werden.

VCenter-Bereitstellungsgröße	Klein	Mittel
Gesamtzahl der virtuellen Maschinen, die für den Schutz mithilfe einer Array-basierten Replikation konfiguriert wurden	2000	5000
Gesamtzahl der Array-basierten Replikationsschutzgruppen	250	250

VCenter-Bereitstellungsgröße	Klein	Mittel
Gesamtzahl der Schutzgruppen pro Wiederherstellungsplan	50	50
Anzahl replizierter Datastores	255	255
Anzahl der VMs	4000	7000

In der folgenden Tabelle sind die Anzahl der VMware Live Site Recovery und die entsprechenden ONTAP Tools für die VMware vSphere Implementierungsgröße aufgeführt.

Anzahl der VMware Live Site Recovery Instanzen	Größe der Bereitstellung von ONTAP-Tools
Bis Zu 4	Klein
4 bis 8	Mittel
Mehr als 8	Groß

Weitere Informationen finden Sie unter "Betriebsgrenzen der VMware Live Site Recovery".

Anforderungen vor der Bereitstellung von ONTAP tools

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie mit der Implementierung fortfahren:

Anforderungen	Ihr Status
Die Version von vSphere, die Version von ONTAP und die Version des ESXi Hosts sind mit der Version der ONTP Tools kompatibel.	□ Ja □ Nein
VCenter Server-Umgebung ist eingerichtet und konfiguriert	□ Ja □ Nein
Browser-Cache wird gelöscht	□ Ja □ Nein
Sie verfügen über die übergeordneten vCenter Server-Anmeldeinformationen	□ Ja □ Nein
Sie verfügen über die Anmeldeinformationen für die vCenter Server-Instanz, mit der die ONTAP-Tools für VMware vSphere nach der Bereitstellung zur Registrierung verbunden werden	□ Ja □ Nein
Der Domänenname, auf dem das Zertifikat ausgestellt wird, wird der virtuellen IP-Adresse in einer Multi-vCenter-Bereitstellung zugeordnet, in der benutzerdefinierte CA-Zertifikate erforderlich sind.	□ Ja □ Nein
Sie haben die nslookup-Prüfung für den Domänennamen ausgeführt, um zu überprüfen, ob die Domäne auf die beabsichtigte IP-Adresse aufgelöst wird.	□ Ja □ Nein
Das Zertifikat wird mit dem Domänennamen und der IP-Adresse des ONTAP Tools erstellt.	□ Ja □ Nein

Anforderungen	Ihr Status
Die Anwendung der ONTAP-Tools und die internen Dienste sind vom vCenter-Server aus erreichbar.	□ Ja □ Nein
Wenn Sie mandantenfähige SVMs verwenden, finden Sie auf jeder SVM eine LIF zum SVM-Management.	□ Ja □ Nein

Arbeitsblatt für die Bereitstellung

Für Single-Node-Implementierung

Verwenden Sie das folgende Arbeitsblatt, um die erforderlichen Informationen für ONTAP-Tools für die Erstbereitstellung von VMware vSphere zu sammeln:

Anforderungen	Ihr Wert
IP-Adresse für die ONTAP -Tools-Anwendung. Dies ist die IP-Adresse für den Zugriff auf die Weboberfläche der ONTAP Tools (Load Balancer).	
Virtuelle IP-Adresse der ONTAP -Tools für die interne Kommunikation. Diese IP-Adresse wird für die interne Kommunikation in einem Setup mit mehreren ONTAP -Tools-Instanzen verwendet. Diese IP-Adresse darf nicht mit der IP-Adresse für die ONTAP -Tools -Anwendung identisch sein. (Die Kubernetes-Steuerebene)	
DNS-Hostname für den Verwaltungsknoten der ONTAP -Tools	
Primärer DNS-Server	
Sekundärer DNS-Server	
DNS-Suchdomäne	
IPv4-Adresse für den Verwaltungsknoten der ONTAP Tools. Es handelt sich um eine eindeutige IPv4-Adresse für die Knotenverwaltungsschnittstelle im Verwaltungsnetzwerk.	
Subnetzmaske für die IPv4-Adresse	
Standard-Gateway für die IPv4-Adresse	
IPv6-Adresse (optional)	
IPv6-Präfixlänge (optional)	
Gateway für die IPv6-Adresse (optional)	

Erstellen Sie DNS-Einträge für alle oben genannten IP-Adressen. Bevor Sie Hostnamen zuweisen, ordnen Sie sie den freien IP-Adressen auf dem DNS zu. Alle IP-Adressen sollten sich im gleichen VLAN befinden, das für die Bereitstellung ausgewählt wurde.

Für hochverfügbare Implementierungen

Zusätzlich zu den Implementierungsanforderungen für einen Node benötigen Sie für die HA-Implementierung die folgenden Informationen:

Anforderungen	Ihr Wert
Primärer DNS-Server	
Sekundärer DNS-Server	
DNS-Suchdomäne	
DNS-Hostname für den zweiten Knoten	
IP-Adresse für den zweiten Node	
DNS-Hostname für den dritten Knoten	
IP-Adresse für den dritten Knoten	

Konfiguration der Netzwerk-Firewall

Stellen Sie sicher, dass die erforderlichen Firewall-Ports für alle relevanten IP-Adressen geöffnet sind. ONTAP -Tools erfordern Zugriff auf das LIF über Port 443. Eine vollständige Liste der erforderlichen Ports finden Sie im Abschnitt „Portanforderungen“ unter"ONTAP-Tools für VMware vSphere – Anforderungen und Konfigurationsgrenzen" .

ONTAP Storage-Einstellungen

Um eine nahtlose Integration von ONTAP Storage mit ONTAP Tools für VMware vSphere zu gewährleisten, sollten folgende Einstellungen durchgeführt werden:

- Wenn Sie Fibre Channel (FC) für die Speicherkonnektivität verwenden, konfigurieren Sie die Zoning auf Ihren FC-Switches, um die ESXi-Hosts mit den FC-LIFs der SVM zu verbinden. "Erfahren Sie mehr über FC- und FCoE-Zoning mit ONTAP Systemen"
- Um ONTAP Tools-gemanagte SnapMirror-Replizierung zu verwenden, sollte der ONTAP Storage-Administrator vor Verwendung von SnapMirror und "Intercluster SVM-Peer-Beziehungen mit ONTAP" in ONTAP erstellen "ONTAP Cluster Peer-Beziehungen".

ONTAP tools bereitstellen

Die ONTAP tools for VMware vSphere Appliance werden als kleiner Einzelknoten mit Kerndiensten zur Unterstützung von NFS- und VMFS-Datenspeichern bereitgestellt. Die Bereitstellung der ONTAP Tools kann bis zu 45 Minuten dauern.

Bevor Sie beginnen

Wenn Sie einen kleinen Einzelknoten bereitstellen, ist eine Inhaltsbibliothek optional. Für Multi-Node- oder HA-Bereitstellungen ist eine Inhaltsbibliothek erforderlich. In VMware speichert eine Inhaltsbibliothek VM-Vorlagen, vApp-Vorlagen und andere Dateien. Die Bereitstellung mit einer Inhaltsbibliothek bietet ein nahtloses Erlebnis, da sie nicht von der Netzwerkkonnektivität abhängig ist.

Beachten Sie Folgendes, bevor Sie eine Inhaltsbibliothek erstellen:

- Erstellen Sie die Inhaltsbibliothek auf einem gemeinsam genutzten Datenspeicher, damit alle Hosts im Cluster darauf zugreifen können.
- Richten Sie die Inhaltsbibliothek ein, bevor Sie die ONTAP tools for VMware vSphere OVA bereitstellen.
- Stellen Sie sicher, dass die Inhaltsbibliothek erstellt wird, bevor Sie das Gerät für HA konfigurieren.

Löschen Sie die OVA-Vorlage nach der Bereitstellung nicht in der Inhaltsbibliothek.

Um die HA-Bereitstellung in Zukunft zu ermöglichen, vermeiden Sie die Bereitstellung der virtuellen Maschine mit den ONTAP Tools direkt auf einem ESXi-Host. Stellen Sie es stattdessen in einem ESXi-Hostcluster oder Ressourcenpool bereit.

Führen Sie die folgenden Schritte aus, um eine Inhaltsbibliothek zu erstellen:

1. Laden Sie die Datei mit den Binärdateien (*.ova*) und signierten Zertifikaten für ONTAP tools for VMware vSphere von der "NetApp Support Website" .
2. Melden Sie sich beim vSphere-Client an
3. Wählen Sie das vSphere-Client-Menü aus und wählen Sie **Inhaltsbibliotheken** aus.
4. Wählen Sie auf der rechten Seite die Option **Erstellen**.
5. Geben Sie einen Namen für die Bibliothek ein, und erstellen Sie die Inhaltsbibliothek.
6. Gehen Sie zu der von Ihnen erstellten Inhaltsbibliothek.
7. Wählen Sie **actions** rechts auf der Seite aus und wählen Sie **Import item** und importieren Sie die OVA-Datei.

Weitere Informationen finden Sie im "Erstellen und Verwenden der Inhaltsbibliothek" Blog.

Bevor Sie mit der Bereitstellung fortfahren, stellen Sie den Distributed Resource Scheduler (DRS) des Clusters im Inventar auf „Konservativ“ ein. Dadurch wird sichergestellt, dass während der Installation keine VMs migriert werden.

Die ONTAP tools for VMware vSphere werden zunächst als Nicht-HA-Setup bereitgestellt. Für die Skalierung auf HA-Bereitstellung müssen Sie CPU-Hotplug und Speicher-Hotplug aktivieren. Sie können diesen Schritt im Rahmen des Bereitstellungsprozesses ausführen oder die VM-Einstellungen nachträglich bearbeiten.

Schritte

1. Laden Sie die Datei herunter, die die Binärdateien (*.ova*) und signierten Zertifikate für die ONTAP tools for VMware vSphere enthält. Wenn Sie die OVA in die Inhaltsbibliothek importiert haben, können Sie diesen Schritt überspringen und mit dem nächsten Schritt fortfahren
2. Melden Sie sich beim vSphere-Server an.
3. Gehen Sie zum Ressourcenpool, Cluster oder Host, auf dem Sie die OVA bereitstellen möchten.

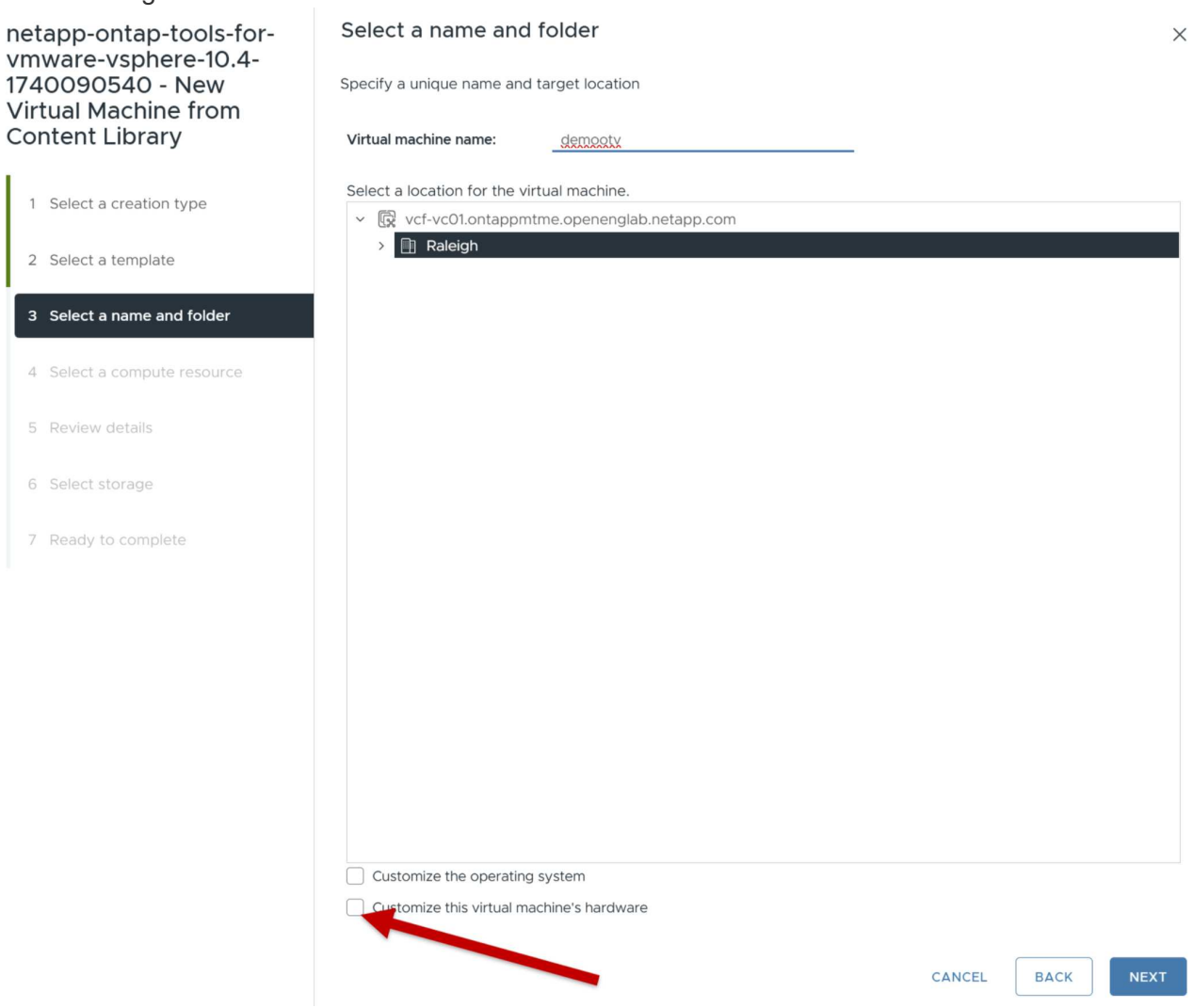
Speichern Sie niemals ONTAP Tools für VMware vSphere Virtual Machine auf von ihm gemanagten VVols Datastores.

4. Sie können die OVA aus der Inhaltsbibliothek oder aus dem lokalen System bereitstellen.

Aus dem lokalen System	Aus der Inhaltsbibliothek

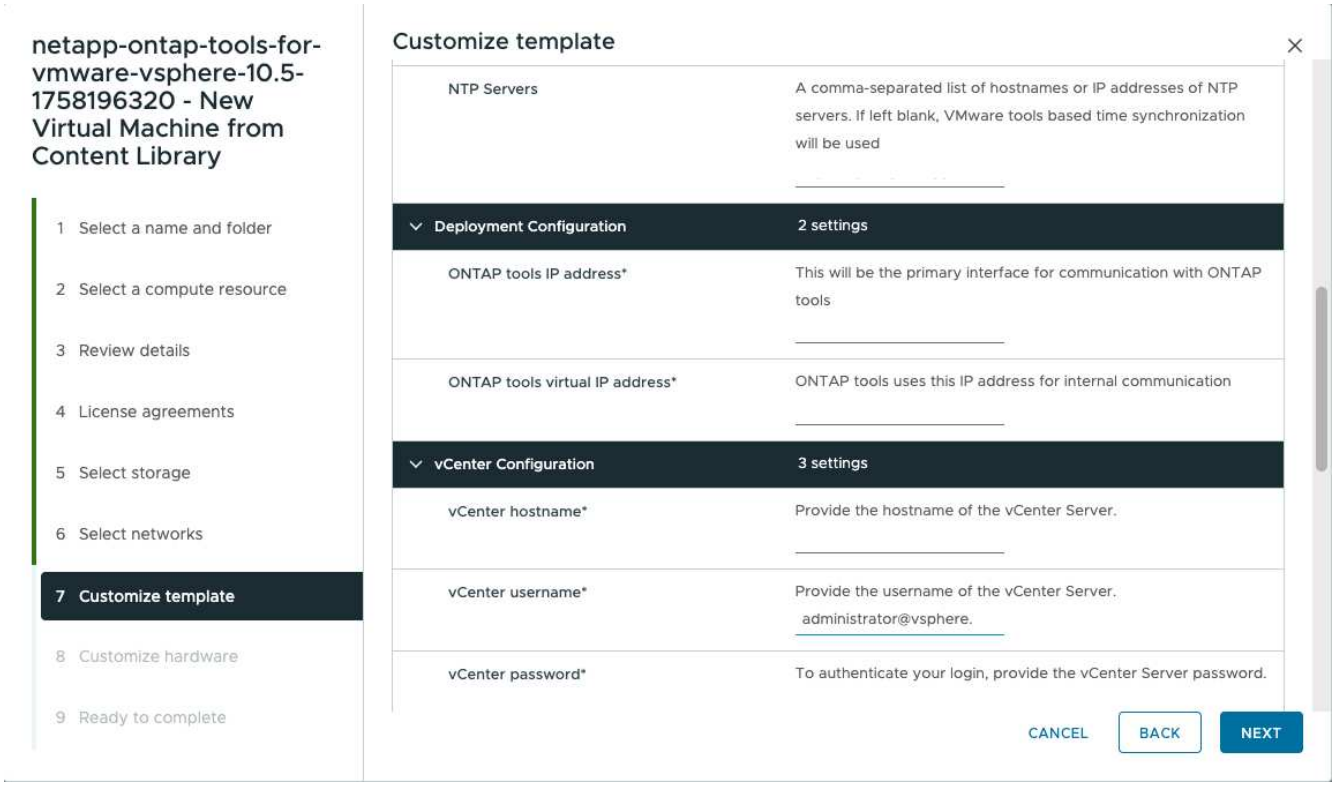
a. Klicken Sie mit der rechten Maustaste, und wählen Sie **OVF-Vorlage bereitstellen…**. b. Wählen Sie die OVA-Datei aus der URL aus, oder navigieren Sie zu ihrem Speicherort, und wählen Sie dann **Weiter** aus.	a. Gehen Sie zu Ihrer Inhaltsbibliothek und wählen Sie das Bibliothekselement aus, das Sie bereitstellen möchten. b. Wählen Sie **Aktionen** > **Neue VM aus dieser Vorlage**

5. Geben Sie im Feld **Namen und Ordner auswählen** den Namen der virtuellen Maschine ein und wählen Sie deren Speicherort.
   - Wenn Sie die vCenter Server 8.0.3-Version verwenden, wählen Sie die Option **Hardware dieser virtuellen Maschine anpassen** aus, die einen zusätzlichen Schritt mit dem Namen **Hardware anpassen** aktiviert, bevor Sie zum Fenster **Ready to Complete** gehen.
   - Wenn Sie die Version 7.0.3 von vCenter Server verwenden, befolgen Sie die Schritte im Abschnitt **Was kommt als Nächstes?** am Ende der Bereitstellung.



6. Wählen Sie eine Computerressource aus und wählen Sie **Weiter**. Aktivieren Sie optional das Kontrollkästchen, um die bereitgestellte VM automatisch einzuschalten*.
7. Überprüfen Sie die Details der Vorlage und wählen Sie **Weiter**.
8. Lesen und akzeptieren Sie die Lizenzvereinbarung und wählen Sie **Weiter**.
9. Wählen Sie den Speicher für die Konfiguration und das Festplattenformat aus und wählen Sie **Weiter**.

10. Wählen Sie für jedes Quellnetzwerk das Zielnetzwerk aus und wählen Sie **Weiter**.
11. Im Fenster **Vorlage anpassen** füllen Sie die erforderlichen Felder aus.



Der vCenter-Hostname ist der Name der vCenter Server-Instanz, auf der die ONTAP Tools Appliance bereitgestellt wird.

Wenn Sie ONTAP Tools in einer Topologie mit zwei vCenter Servern einsetzen – wobei die Appliance in einer vCenter-Instanz gehostet wird und eine andere verwaltet –, können Sie der vCenter-Instanz, die die ONTAP Tools hostet, eine eingeschränkte Rolle zuweisen. Sie können einen dedizierten vCenter-Benutzer und eine Rolle erstellen, die nur über die für die OVF-Vorlagenbereitstellung erforderlichen Berechtigungen verfügen. Für Einzelheiten siehe die aufgeführten Rollen in "In ONTAP Tools für VMware vSphere 10 enthaltene Rollen"Die

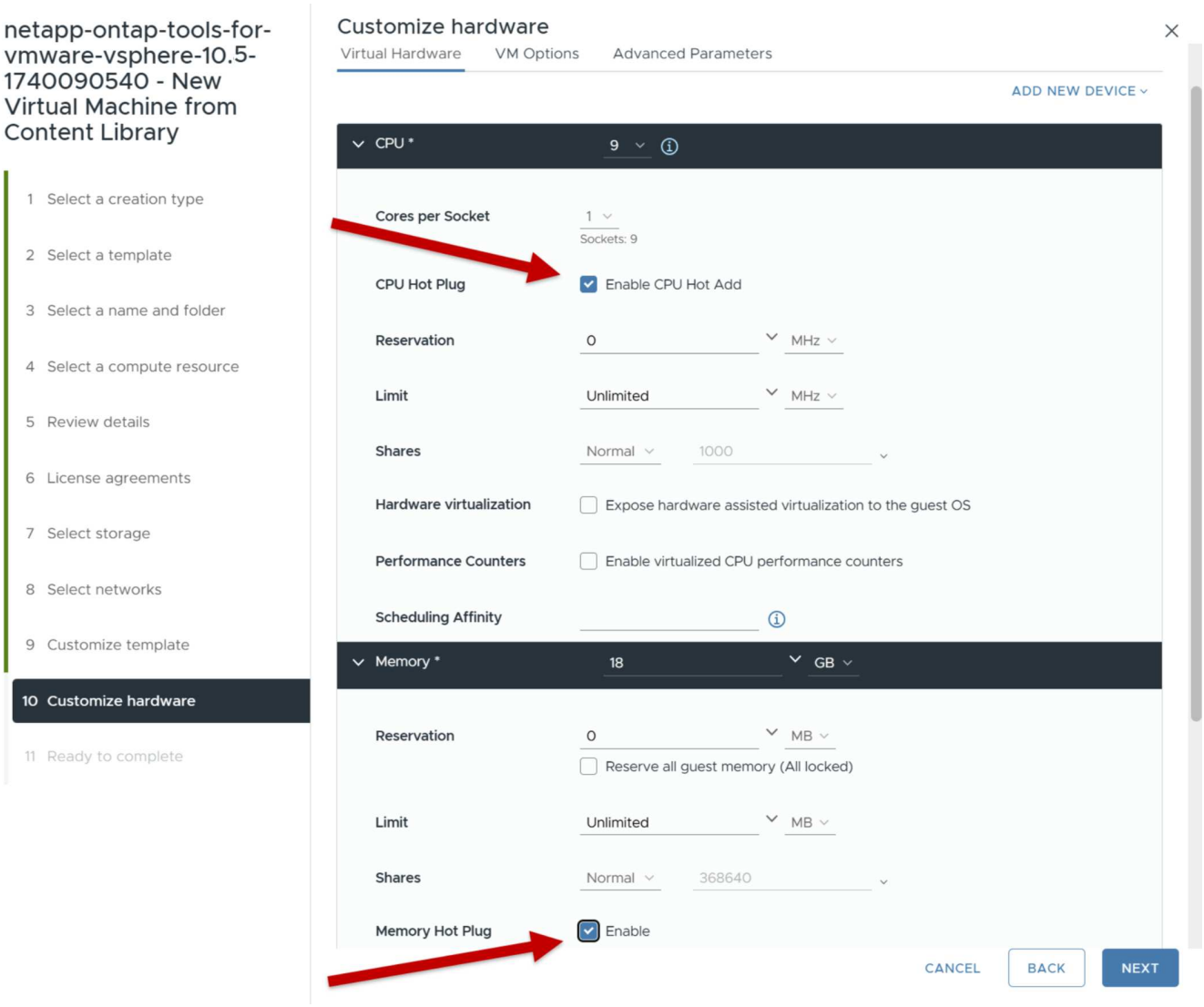
Stellen Sie für die vCenter-Instanz, die von ONTAP -Tools verwaltet wird, sicher, dass das vCenter-Benutzerkonto über Administratorrechte verfügt.

- Hostnamen müssen Buchstaben (A–Z, a–z), Ziffern (0–9) und Bindestriche (-) enthalten. Geben Sie zum Konfigurieren von Dual-Stack den Hostnamen an, der der IPv6-Adresse zugeordnet ist.

  Pure IPv6 wird nicht unterstützt. Der gemischte Modus wird mit VLAN unterstützt, das sowohl IPv6- als auch IPv4-Adressen enthält.

- Die IP-Adresse des ONTAP Tools ist die primäre Schnittstelle zur Kommunikation mit ONTAP Tools.
- IPv4 ist die IP-Adresskomponente der Knotenkonfiguration, die zur Aktivierung von Diagnose-Shell und SSH-Zugriff auf den Knoten für Debugging und Wartung verwendet werden kann.

12. Bei Verwendung der vCenter Server Version 8.0.3 müssen Sie im Fenster **Hardware anpassen** die Optionen **CPU Hot-Add** und **Speicher Hot-Plug** aktivieren, um die HA-Funktionalität zu ermöglichen.



13. Überprüfen Sie die Details im Fenster **Ready to Complete**, wählen Sie **Finish**.

    Wenn die Bereitstellungsaufgabe erstellt wird, wird der Fortschritt in der vSphere-Taskleiste angezeigt.

14. Schalten Sie die VM nach Abschluss der Aufgabe ein, wenn die Option zum automatischen Einschalten der VM nicht ausgewählt wurde.

Sie können den Fortschritt der Installation in der Webkonsole der VM verfolgen.

Wenn im OVF-Formular Unstimmigkeiten auftreten, werden Sie in einem Dialogfeld aufgefordert, Korrekturmaßnahmen zu ergreifen. Navigieren Sie mit der Tabulatortaste, nehmen Sie die erforderlichen Änderungen vor und wählen Sie **OK**. Sie haben drei Versuche, etwaige Probleme zu lösen. Wenn die Probleme nach drei Versuchen weiterhin bestehen, wird der Installationsvorgang abgebrochen und es wird empfohlen, die Installation auf einer neuen virtuellen Maschine erneut zu versuchen.

Was kommt als Nächstes?

Wenn Sie ONTAP-Tools für VMware vSphere mit vCenter Server 7.0.3 bereitstellen, führen Sie diese Schritte nach der Bereitstellung aus.

1. Melden Sie sich beim vCenter Client an
2. Schalten Sie den Knoten „ONTAP Tools“ aus.

3. Gehen Sie zu den ONTAP tools for VMware vSphere Maschine unter **Inventar** und wählen Sie die Option **Einstellungen bearbeiten**.
4. Aktivieren Sie unter den Optionen **CPU** das Kontrollkästchen **CPU Hot add aktivieren**
5. Aktivieren Sie unter den **Memory**-Optionen das Kontrollkästchen **enable** gegen **Memory Hot Plug**.

Fehler bei der Bereitstellung von ONTAP tools beheben

Wenn bei der Bereitstellung Probleme auftreten, überprüfen Sie die Protokolle und Fehlercodes, um die Probleme zu diagnostizieren und zu beheben. Ab ONTAP tools for VMware vSphere 10.5 umfassen die von den Pods gesammelten Protokollpakete Protokolle von MongoDB, RabbitMQ und Vault sowie den Status und die Beschreibungen aller Pods. Diese werden zusätzlich zu den vorhandenen Serviceprotokollen der ONTAP Tools bereitgestellt und verbessern die Supportfähigkeit und Fehlerbehebung.

Sammeln Sie die Protokolldateien

Sie können Protokolldateien für ONTAP-Tools für VMware vSphere über die in der Benutzeroberfläche von ONTAP Tools Manager verfügbaren Optionen sammeln. Der technische Support fordert Sie möglicherweise auf, die Protokolldateien zu sammeln, damit Sie Probleme beheben können.

> Die Generierung von Protokollen über den ONTAP-Tools-Manager umfasst alle Protokolle für alle vCenter-Serverinstanzen. Die Generierung von Protokollen über die vCenter-Client-Benutzeroberfläche ist für den ausgewählten vCenter-Server vorgesehen.

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 **Log Bundles** aus.

   Dieser Vorgang kann mehrere Minuten dauern.
4. Wählen Sie **Generate**, um die Protokolldateien zu generieren.
5. Geben Sie die Bezeichnung für das Log Bundle ein und wählen Sie **Generate**.

   Laden Sie die Datei tar.gz herunter, und senden Sie sie an den technischen Support.

Führen Sie die folgenden Schritte aus, um Protokollbündel über die vCenter Client-Benutzeroberfläche zu generieren:

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Gehen Sie auf der vSphere Client-Homepage zu **Support** > **Log Bundle** > **Generate**.
3. Geben Sie die Bezeichnung des Protokollpakets an und generieren Sie das Protokollpaket. Die Download-Option wird angezeigt, wenn die Dateien generiert werden. Der Download kann einige Zeit dauern.

Das erzeugte Log-Bundle ersetzt das Log-Bundle, das innerhalb der letzten 3 Tage oder 72 Stunden erzeugt wurde.

Fehlercodes für die Bereitstellung

Während der Bereitstellung, des Neustarts und der Wiederherstellungsvorgänge von ONTAP-Tools für VMware vSphere können Fehlercodes auftreten.
Die Fehlercodes sind fünf Ziffern lang, wobei die ersten beiden Ziffern das Skript darstellen, das auf das Problem gestoßen ist, und die letzten drei Ziffern den spezifischen Workflow innerhalb dieses Skripts darstellen.

Alle Fehlerprotokolle werden in der Datei ansible-perl-errors.log im Verzeichnis /var/log aufgezeichnet, um die einfache Verfolgung und Lösung von Problemen zu ermöglichen. Diese Protokolldatei enthält den Fehlercode und die fehlgeschlagene Ansible-Aufgabe.

Die auf dieser Seite angegebenen Fehlercodes dienen nur als Referenz. Wenden Sie sich an das Support-Team, wenn der Fehler weiterhin besteht oder wenn keine Lösung erwähnt wird.

In der folgenden Tabelle sind die Fehlercodes und die entsprechenden Dateinamen aufgeführt.

Fehlercode	Skriptname
00	firstboot-network-config.pl, Mode Deployment
01	firstboot-network-config.pl, Modusaktualisierung
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, Deploy, HA
04	firstboot-deploy-otv-ng.pl, Deploy, non-HA
05	firstboot-deploy-otv-ng.pl, Neustart
06	firstboot-deploy-otv-ng.pl, Upgrade, HA
07	firstboot-deploy-otv-ng.pl, Upgrade, nicht HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Die letzten drei Ziffern des Fehlercodes zeigen den spezifischen Workflow-Fehler im Skript an:

Deployment-Fehlercode	Arbeitsablauf	* Auflösung*
049	Für Netzwerk und Validierung wird Perl Skript sie auch in Kürze zuweisen	-
050	Generierung des SSH-Schlüssels fehlgeschlagen	Starten Sie die primäre virtuelle Maschine (VM) neu.

053	RKE2 konnte nicht installiert werden	Führen Sie entweder Folgendes aus und starten Sie die primäre VM neu, oder starten Sie Neuimplementierung: Sudo rke2-killall.sh (alle VMs) Sudo rke2-uninstall.sh (alle VMs).
054	Einstellung von kubeconfig fehlgeschlagen	Neuimplementierung
055	Fehler beim Bereitstellen der Registrierung	Wenn der Registrierungs-Pod vorhanden ist, warten Sie, bis der Pod bereit ist, starten Sie dann die primäre VM neu oder starten Sie es andernfalls neu.
059	Die KubeVip-Bereitstellung ist fehlgeschlagen	Vergewissern Sie sich, dass die während der Implementierung angegebene virtuelle IP-Adresse für die Kubernetes-Kontrollebene und die ONTAP-Tools die IP-Adresse im selben VLAN und freien IP-Adressen sind. Neu starten, wenn alle vorherigen Punkte korrekt sind. Ansonsten Neuimplementierung.
060	Die Benutzerbereitstellung ist fehlgeschlagen	Neu Starten
061	Die Bereitstellung der Dienste ist fehlgeschlagen	Führen Sie einfache Kubernetes-Fehlerbehebungen wie get Pods, get rs, get svc usw. im ntv-System-Namespace durch, um weitere Details und Fehlerprotokolle unter /var/log/ansible-perl-errors.log und /var/log/ansible-run.log zu erhalten und Neuimplementierungen durchzuführen.
062	Die Bereitstellung der ONTAP Tools Services ist fehlgeschlagen	Weitere Informationen und Neuimplementierungen finden Sie in den Fehlerprotokollen unter /var/log/ansible-perl-errors.log.
065	Die URL der Swagger-Seite ist nicht erreichbar	Neuimplementierung
066	Fehler bei den Schritten nach der Bereitstellung für das Gateway-Zertifikat	Gehen Sie wie folgt vor, um das Upgrade wiederherzustellen/abzuschließen: * Diagnostic Shell aktivieren. * Führen Sie den Befehl 'sudo perl /Home/maint/scripts/post-deploy-upgrade.pl --postDeploy' aus. * Überprüfen Sie die Protokolle unter /var/log/post-deploy-Upgrade.log.

088	Die Konfiguration der Protokollrotation für journald ist fehlgeschlagen	Überprüfen Sie die VM-Netzwerkeinstellungen, die mit dem Host kompatibel sind, auf dem die VM gehostet wird. Sie können versuchen, auf einen anderen Host zu migrieren und die VM neu zu starten.
089	Ändern der Eigentumsrechte für die Konfigurationsdatei „Zusammenfassung Protokoll drehen“ ist fehlgeschlagen	Starten Sie die primäre VM neu.
096	Installieren Sie die dynamische Storage-provisionierung	-
108	Das Seeding des Skripts ist fehlgeschlagen	-

Fehlercode für Neustart	**Arbeitsablauf**	* Auflösung*
067	Zeitüberschreitung beim Warten auf Rke2-Server.	-
101	Fehler beim Zurücksetzen des Benutzerpassworts für Wartung/Konsole.	-
102	Fehler beim Löschen der Kennwortdatei beim Zurücksetzen des Benutzerpassworts für Wartung/Konsole.	-
103	Fehler beim Aktualisieren des neuen Benutzerpassworts für Wartung/Konsole im Tresor.	-
088	Die Konfiguration der Protokollrotation für journald ist fehlgeschlagen.	Überprüfen Sie die VM-Netzwerkeinstellungen, die mit dem Host kompatibel sind, auf dem die VM gehostet wird. Sie können versuchen, auf einen anderen Host zu migrieren und die VM neu zu starten.
089	Ändern der Eigentumsrechte für die Konfigurationsdatei „Zusammenfassung Protokoll drehen“ ist fehlgeschlagen.	Starten Sie den VM neu.

Konfigurieren Sie ONTAP Tools für VMware vSphere

vCenter Server-Instanzen zu ONTAP -Tools hinzufügen

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

ONTAP -Tools lassen sich in vCenter Server integrieren, um Speicheraufgaben wie Bereitstellung, Snapshots und Datenschutz direkt vom vSphere-Client aus durchzuführen.

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. Zum 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. Öffnen Sie einen Webbrowser und rufen Sie die URL auf:
   `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.
4. Rufen Sie in den erweiterten Optionen das vCenter Server-Zertifikat automatisch ab (autorisieren Sie es) oder laden Sie es manuell hoch.

> 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:

- ONTAP -Tools registrieren das vCenter-Client-Plug-In als Remote-Plug-In.
- 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 bei einer vCenter Server-Instanz in ONTAP tools

Verwenden Sie ONTAP tools for VMware vSphere, um den VASA-Anbieter bei einer vCenter Server-Instanz zu registrieren. Dies ermöglicht eine speicherrichtlinienbasierte Verwaltung, vVols Unterstützung und die Integration mit VMware Live Site Recovery-Geräten auf ONTAP -Systemen.

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 im Abschnitt Plug-ins **Shortcuts** > **NetApp ONTAP Tools** aus.
3. Wählen Sie **Einstellungen** > **VASA-Anbietereinstellungen**. Die ONTAP -Tools zeigen den Registrierungsstatus des VASA-Anbieters als „nicht registriert“ an.
4. Klicken Sie auf die Schaltfläche **Registrieren**, um den VASA Provider zu registrieren.
5. Geben Sie einen Namen und Anmeldeinformationen für den VASA-Anbieter ein. Der Benutzername darf nur Buchstaben, Zahlen und Unterstriche enthalten. Legen Sie die Passwortlänge zwischen 8 und 256 Zeichen fest.
6. Wählen Sie **Registrieren**.
7. Nach einer erfolgreichen Registrierung und Seitenaktualisierung zeigen die ONTAP -Tools den Status, den Namen und die Version des registrierten VASA-Anbieters an.

Wie es weiter geht

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

Schritte

1. Gehen 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 mit ONTAP -Tools

Das Plug-In NFS vStorage API for Array Integration (NFS VAAI) verbindet VMware vSphere mit NFS-Speicher-Arrays. Verwenden Sie ONTAP tools for VMware vSphere , um das VAAI-Plug-In zu installieren. Dadurch kann das NFS-Speicherarray bestimmte Speichervorgänge anstelle von ESXi-Hosts verarbeiten.

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 Sie das VAAI-Plug-In bereits auf vCenter Server hochgeladen haben, wählen Sie **Ändern** unter **Vorhandene Version**. Wenn nicht, wählen Sie **Hochladen**.
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.

   Der vSphere Web Client zeigt nur die ESXi-Hosts an, die das Plug-in installieren können. Sie können den Installationsfortschritt im Abschnitt „Letzte Aufgaben“ verfolgen.

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

   Nach dem Neustart des ESXi-Hosts erkennen und aktivieren die ONTAP tools for 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, konfigurieren Sie die NFS-Exportrichtlinien für die VAAI-Kopierauslagerung. Stellen Sie sicher, dass die Exportrichtlinienregeln diese Anforderungen erfüllen:

- Das entsprechende ONTAP Volume ermöglicht NFSv4-Aufrufe.
- Der Root-Benutzer bleibt Root und NFSv4 ist in allen übergeordneten Junction-Volumes zulässig.
- Die Option für die VAAI-Unterstützung wird auf dem jeweiligen NFS-Server eingestellt.

Weitere Informationen finden Sie unter "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 der ESXi-Hosteinstellungen in ONTAP tools

Durch die Konfiguration der Multipath- und Timeout-Einstellungen des ESXi-Servers können Sie die Datenverfügbarkeit und -integrität aufrechterhalten. Es ermöglicht ein automatisches Failover auf einen Backup-Speicherpfad, wenn der primäre Pfad nicht mehr verfügbar ist.

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

Dieser Vorgang kann je nach Konfiguration und Systemauslastung einige Zeit in Anspruch nehmen. Sie können den Fortschritt im Bereich „Letzte Aufgaben“ anzeigen.

Schritte

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

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

6. Wählen Sie auf der Einstellungsseite die empfohlenen Werte nach Bedarf aus.
7. 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

Verwenden Sie ONTAP tools for VMware vSphere, um Timeouts und andere Werte auf ESXi-Hosts für optimale Leistung und Failover festzulegen. Diese Werte werden auf Grundlage von NetApp -Tests festgelegt.

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 wählen die besten Pfade für NetApp -Speichersysteme aus. Wählen Sie in den MPIO-Einstellungen den besten Pfad aus und verwenden Sie ihn.

Passen Sie für Hochleistungsumgebungen oder beim Testen mit einem einzelnen LUN-Datenspeicher die Lastausgleichseinstellung der Round-Robin-Pfadauswahlrichtlinie (VMW_PSP_RR) an, um die Leistung zu verbessern. Setzen Sie den Standard-IOPS-Wert von 1000 auf 1.

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 für ONTAP tools

In diesem Abschnitt konfigurieren Sie ONTAP -Benutzerrollen und -Berechtigungen für Speichersysteme mit ONTAP tools for VMware vSphere und ONTAP System Manager. Sie können Rollen mithilfe der bereitgestellten JSON-Dateien zuweisen, Benutzer und Rollen manuell erstellen und die minimal erforderlichen Berechtigungen für Nicht-Administratorkonten anwenden.

Bevor Sie beginnen

- Laden Sie die ONTAP Privileges von den ONTAP tools for VMware vSphere mit *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* herunter. Nach dem Herunterladen der ZIP-Datei finden Sie zwei JSON-Dateien. Verwenden Sie die ASA r2-spezifische JSON-

Datei, wenn Sie ein ASA r2-System konfigurieren.

> Sie können Benutzer auf Clusterebene oder direkt auf der Ebene der virtuellen Speichermaschinen (SVMs) erstellen. Wenn Sie die Datei user_roles.json nicht verwenden, stellen Sie sicher, dass der Benutzer über die erforderlichen Mindestberechtigungen für SVM verfügt.

- Melden Sie sich mit Administratorrechten für das Speicher-Backend an.

Schritte

1. Extrahieren Sie die heruntergeladene Datei *https://<ONTAPtoolsIP>: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 Administratorrechten beim Cluster an. So konfigurieren Sie einen Benutzer:
   a. Um einen Cluster ONTAP Tools-Benutzer zu konfigurieren, wählen Sie den Bereich **Cluster** > **Einstellungen** > **Benutzer und Rollen**.
   b. Um einen SVM ONTAP -Tools-Benutzer zu konfigurieren, wählen Sie den Bereich **Storage SVM** > **Einstellungen** > **Benutzer und Rollen**.
   c. Wählen Sie unter Benutzer * Hinzufügen *.
   d. Wählen Sie im Dialogfeld * Benutzer hinzufügen* die Option **Virtualisierungsprodukte** aus.
   e. **Durchsuchen**, um die JSON-Datei mit den ONTAP Privileges auszuwählen und hochzuladen. Wählen Sie für Nicht- ASA R2-Systeme die Datei users_roles.json und für ASA R2-Systeme die Datei users_roles_ASAr2.json aus.

      ONTAP -Tools füllen das Produktfeld automatisch aus.

   f. Wählen Sie aus der Dropdown-Liste die Produktfunktion „VSC, VASA Provider und SRA“ aus.

      ONTAP -Tools füllen das Feld **Rolle** automatisch basierend auf der von Ihnen ausgewählten Produktfunktion aus.

   g. Geben Sie den erforderlichen Benutzernamen und das erforderliche Passwort ein.
   h. Wählen Sie die Berechtigungen (Erkennung, Speicher erstellen, Speicher ändern, Speicher zerstören, NAS/SAN-Rolle) aus, die der Benutzer benötigt, und wählen Sie dann **Hinzufügen**.

ONTAP -Tools fügen die neue Rolle und den neuen Benutzer hinzu. Sie können die Berechtigungen unter der von Ihnen konfigurierten Rolle anzeigen.

Anforderungen für die SVM-Aggregatzuordnung

Beim Bereitstellen von Datenspeichern mithilfe von SVM-Benutzeranmeldeinformationen erstellen ONTAP tools for VMware vSphere Volumes auf dem in der POST-API des Datenspeichers angegebenen Aggregat. ONTAP verhindert, dass SVM-Benutzer Volumes auf Aggregaten erstellen, die nicht dem SVM zugeordnet sind. Ordnen Sie die SVM mithilfe der ONTAP REST API oder CLI den erforderlichen Aggregaten zu, bevor Sie Volumes erstellen.

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

Erstellen Sie Benutzer und Rollen manuell ohne die JSON-Datei.

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 die Rollen der Cluster ONTAP Tools zu konfigurieren, wählen Sie **Cluster** > **Einstellungen** > **Benutzer und Rollen**.
   b. Um die Rollen der Cluster-SVM ONTAP -Tools zu konfigurieren, wählen Sie **Storage-SVM** > **Einstellungen** > **Benutzer und Rollen**.
3. Rollen erstellen:
   a. Wählen Sie **Hinzufügen** unter **Rollen** Tabelle.
   b. Geben Sie die Details **Rollenname** und **Rollenattribute** ein.

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

   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

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,

verwenden Sie die JSON-Datei zum Erstellen von Benutzern, da ONTAP tools for VMware vSphere mehr als nur Leseberechtigungen für die Bereitstellung auf ONTAP benötigen.

Sie können über APIs auf die Funktionen zugreifen:

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	Berechtigungsermittlung
/API/Sicherheit/Funktionen	Schreibgeschützt	Berechtigungsermittlung
/API/Storage/Aggregate	Schreibgeschützt	Überprüfung des Gesamtspeicherplatzes während der Bereitstellung von Datenspeichern/Volumes
/API/Storage/Cluster	Schreibgeschützt	So erhalten Sie Speicherplatz- und Effizienzdaten auf Clusterebene
/API/Storage/Festplatten	Schreibgeschützt	So erhalten Sie die in einem Aggregat verknüpften Datenträger
/API/Storage/qos/Richtlinien	Lesen/Erstellen/Ändern	QoS- und VM-Richtlinienverwaltung
/API/svm/svms	Schreibgeschützt	Um die SVM-Konfiguration abzurufen, wenn der Cluster lokal hinzugefügt wird.
/API/Netzwerk/ip/Schnittstellen	Schreibgeschützt	Speicher-Backend hinzufügen – Um zu identifizieren, dass der Verwaltungs-LIF-Bereich Cluster/SVM ist
/API/Storage/Verfügbarkeitszonen	Schreibgeschützt	SAZ-Entdeckung. Gilt für ONTAP Versionen ab 9.16.1 und ASA r2-Systeme.
/api/cluster/metrocluster	Schreibgeschützt	Ruft den Status und die Konfigurationsdetails von MetroCluster ab.

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

Für PATCH-Vorgänge und automatische Rollbacks auf Datenspeichern sind Berechtigungen zum Ermitteln, Erstellen, Ändern und Löschen erforderlich. Fehlende Berechtigungen können zu Problemen beim Workflow und bei der Bereinigung führen.

Ein auf der ONTAP -API basierender Benutzer mit den Berechtigungen zum Erkennen, Erstellen, Ändern und Löschen kann die Workflows der ONTAP -Tools verwalten.

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

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

Führen Sie für ASA r2-Systeme mit ONTAP Version 9.16.1 und höher den folgenden Befehl aus:

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

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

Führen Sie die folgenden Befehle aus, um einen SVM-Benutzer mit allen Berechtigungen 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_
```

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

Verwenden Sie für Benutzer von ONTAP Tools für VMware vSphere 10.1, die über einen Cluster-scoped-Benutzer erstellt haben, die über die JSON-Datei erstellt wurden, zum Upgrade auf Version 10.3 die folgenden ONTAP-CLI-Befehle mit dem Benutzer-Admin-Privileges.

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

Verwenden Sie für ONTAP Tools für Benutzer von VMware vSphere 10.1 mit einem im SVM-Umfang enthaltenen Benutzer, die mit der json-Datei erstellt wurden, zum Upgrade auf Version 10.3 die ONTAP-CLI-Befehle mit Admin-Benutzer Privileges.

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, fügen Sie der vorhandenen Rolle die Befehle *vserver nvme namespace show* und *vserver nvme subsystem show* hinzu.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Upgrade von ONTAP Tools für VMware vSphere 10.3 Benutzer auf 10.4 Benutzer

Ab ONTAP 9.16.1 aktualisieren Sie die ONTAP tools for VMware vSphere 10.3-Benutzer auf 10.4-Benutzer.

Verwenden Sie für ONTAP Tools für VMware vSphere 10.3 Benutzer mit einem über Cluster erstellten Benutzer, der über die JSON-Datei und ONTAP Version 9.16.1 oder höher erstellt wurde, den ONTAP-CLI-Befehl mit dem Admin-Benutzer Privileges, um ein Upgrade auf den Release 10.4 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 "storage
availability-zone show" -access all
```

Fügen Sie ein Speicher-Backend zu ONTAP tools hinzu

Verwenden Sie ONTAP tools for VMware vSphere, um Speicher-Backends für Ihre ESXi-Hosts hinzuzufügen und zu verwalten. Sie können Cluster oder SVMs einbinden, die MetroCluster Unterstützung aktivieren und Zertifikate für eine sichere Verbindung validieren. Sie können Speicher-Backends mit dem ONTAP Tools Manager oder dem vSphere Client konfigurieren, den Zertifikatsstatus überwachen und Ressourcen nach Clusteränderungen manuell neu erkennen.

Um ein lokales Speicher-Backend hinzuzufügen, verwenden Sie Cluster- oder SVM-Anmeldeinformationen in der ONTAP -Tools-Oberfläche. Lokale Speicher-Backends stehen nur dem ausgewählten vCenter Server zur Verfügung. ONTAP -Tools ordnen SVMs dem vCenter Server für die Verwaltung von vVols oder VMFS-

Datenspeichern zu. Für VMFS-Datenspeicher und SRA-Workflows können Sie SVM-Anmeldeinformationen verwenden, ohne einen Cluster global zuzuordnen.

Um ein globales Speicher-Backend hinzuzufügen, verwenden Sie die ONTAP Cluster-Anmeldeinformationen im ONTAP Tools Manager. Globale Speicher-Backends ermöglichen Discovery-Workflows zur Identifizierung der für die vVol-Verwaltung erforderlichen Clusterressourcen. In Multitenant-Umgebungen können Sie einen SVM-Benutzer lokal hinzufügen, um vVols Datenspeicher zu verwalten.

Wenn die MetroCluster Unterstützung in ONTAP aktiviert ist, werden sowohl Quell- als auch Zielcluster als lokale oder globale Speicher-Backends eingebunden.

Bevor Sie beginnen

Überprüfen Sie, ob das Zertifikat ein gültiges Feld „Subject Alternative Name“ (SAN) enthält. ONTAP -Systeme verwenden das SAN-Feld, um Cluster- und SVM-Management-LIFs zu identifizieren.

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.

5. Rufen Sie die ONTAP Cluster-Zertifikate automatisch ab und autorisieren Sie das Zertifikat oder laden Sie es manuell hoch, indem Sie zu seinem Speicherort navigieren.

   Bei Bedarf können Sie die SAN-Validierung (Subject Alternative Name) über die Wartungskonsole deaktivieren. Anweisungen hierzu finden Sie unter"Zertifikatvalidierungsflag ändern" .

6. Wenn das von Ihnen hinzugefügte Speicher-Backend Teil einer MetroCluster -Konfiguration ist, zeigt der ONTAP Tools Manager eine Popup-Meldung zum Hinzufügen des Peered-Clusters an. Wählen Sie **Hinzufügen** und geben Sie die Details für das MetroCluster Peer-Storage-Backend ein.

   Nachdem das ONTAP -System ein Switchover und Switchback durchgeführt hat, führen Sie die Erkennung der ONTAP Tools manuell aus.

Die vSphere-Client-Benutzeroberfläche wird verwendet

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

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.

   Sie können ein Speicher-Backend mithilfe clusterbasierter Anmeldeinformationen mit IPv4- oder IPv6-Verwaltungs-LIFs hinzufügen. Um einen SVM-Benutzer direkt hinzuzufügen, geben Sie SVM-basierte Anmeldeinformationen zusammen mit einem SVM-Verwaltungs-LIF an. Wenn ein Cluster bereits integriert ist, können Sie keinen SVM-Benutzer aus diesem Cluster erneut integrieren.

5. Rufen Sie die ONTAP Cluster-Zertifikate automatisch ab und autorisieren Sie das Zertifikat oder laden

Sie es manuell hoch, indem Sie zu seinem Speicherort navigieren.

6. Wenn das hinzugefügte Speicher-Backend Teil der MetroCluster -Konfiguration ist, zeigen die ONTAP Tools den Bildschirm * MetroCluster Peer hinzufügen* an. Wählen Sie **Peer hinzufügen**, um das Peer-Speicher-Backend hinzuzufügen.

> Nachdem das ONTAP -System ein Switchover und Switchback durchgeführt hat, führen Sie die Erkennung der ONTAP Tools manuell aus.

Was kommt als Nächstes?

ONTAP -Tools aktualisieren die Liste, um das neue Speicher-Backend anzuzeigen.

ONTAP -Tools listen das neu hinzugefügte Speicher-Backend auf der Seite **Speicher-Backends** auf. Wenn ein Zertifikat in 30 Tagen oder weniger abläuft, zeigen die ONTAP Tools in der Spalte mit dem Ablaufdatum des Zertifikats eine Warnung an. Nach Ablauf markieren die ONTAP -Tools das Speicher-Backend als unbekannt, da es keine Verbindung zum Speichersystem herstellen kann.

Verwandte Informationen

"Konfigurieren der Cluster in einer MetroCluster -Konfiguration"

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

Ordnen Sie einer vCenter Server-Instanz ein Speicher-Backend zu, um den Zugriff für alle vCenter Server-Instanzen zu ermöglichen. Stellen Sie bei der MetroCluster -Konfiguration sicher, dass Sie beim Zuordnen eines Storage-Backend-Clusters auch dessen Peer-Cluster mit dem vCenter Server zuordnen.

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 Auslassungspunkte neben der vCenter Server-Instanz aus, die Sie mit den Speicher-Backends verbinden möchten.
5. Wählen Sie aus dem Dropdown-Menü das Speicher-Backend aus, das Sie mit der ausgewählten vCenter Server-Instanz verknüpfen 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 den Netzwerkzugriff. Sie können die Exportrichtlinie so ändern, dass der Zugriff nur von bestimmten IP-Adressen aus erlaubt ist. Wenn ein ausgeschlossener ESXi-Host versucht, einen Mount-Vorgang durchzuführen, 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. Gehen Sie im linken Bereich der ONTAP -Tools zu **Einstellungen** > **Netzwerkzugriff 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 Sie einen Datenspeicher in ONTAP tools

Wenn Sie einen Datenspeicher auf Hostclusterebene erstellen, mounten ONTAP Tools ihn auf allen Zielhosts und aktivieren die Aktion nur, wenn Sie über die erforderlichen Berechtigungen verfügen.

Interoperabilität zwischen nativen Datenspeichern mit vCenter Server und von ONTAP-Tools verwalteten Datenspeichern

Ab ONTAP tools for VMware vSphere 10.4 erstellen ONTAP Tools verschachtelte igroups für Datenspeicher, wobei übergeordnete igroups spezifisch für Datenspeicher und untergeordnete igroups den Hosts zugeordnet sind. Sie können flache igroups vom ONTAP System Manager aus erstellen und diese zum Erstellen von VMFS-Datenspeichern verwenden, ohne ONTAP Tools zu verwenden. Siehe "Verwalten von SAN-Initiatoren und igroups" für weitere Informationen.

Nachdem Sie den Speicher integriert und die Datenspeichererkennung ausgeführt haben, ändern ONTAP -Tools flache Igroups in VMFS-Datenspeichern in verschachtelte Igroups. Sie können frühere flache igroups nicht zum Erstellen neuer Datenspeicher verwenden. Verwenden Sie die ONTAP Tools-Schnittstelle oder die REST-API, um verschachtelte igroups wiederzuverwenden.

Erstellen Sie einen VVols-Datastore

Ab den ONTAP tools for VMware vSphere 10.3 können Sie einen vVols Datenspeicher auf ASA R2-Systemen mit platzsparender Speicherkapazität als thin.vVol erstellen. Der VASA-Anbieter erstellt beim Erstellen des vVol-Datenspeichers einen Container und die gewünschten Protokollendpunkte. Der VASA-Anbieter weist diesem Container keine Sicherungsvolumes zu.

Bevor Sie beginnen

- Stellen Sie sicher, dass Root-Aggregate nicht auf SVM abgebildet sind.
- 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* > **Datastore erstellen**.
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. Unter Erweiterte Optionen:
   - Wenn Sie die **Benutzerdefinierte Exportrichtlinie** auswählen, stellen Sie sicher, dass Sie die Erkennung in vCenter für alle Objekte ausführen. Es wird empfohlen, diese Option nicht zu verwenden.
   - Sie können für die iSCSI- und FC-Protokolle **Custom Initiator Group**-Name 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 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 QoS im Datenspeicher aktivieren. Standardmäßig wird für jede LUN-Erstellungsanforderung ein Volume erstellt. Überspringen Sie diesen Schritt für vVols -Datenspeicher auf ASA R2-Speichersystemen.

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

Erstellen Sie einen NFS-Datastore

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. 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. Wenn Sie unter den erweiterten Optionen **Benutzerdefinierte Exportrichtlinie** auswählen, führen Sie die Erkennung in vCenter für alle Objekte aus. Es wird empfohlen, diese Option nicht zu verwenden.

   Sie können keinen NFS-Datenspeicher mithilfe der Standard- oder 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 im Plattform-Dropdown-Menü die Option **Beliebig** auswählen, können Sie alle SVMs im vCenter sehen. Plattform und asymmetrische Flagge beeinträchtigen die Sicht nicht.
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**.

ONTAP -Tools erstellen den NFS-Datenspeicher und mounten ihn auf allen Hosts.

Erstellen Sie einen VMFS-Datastore

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

In einem geschützten Cluster:

- Sie können nur VMFS-Datenspeicher erstellen. Durch das Hinzufügen eines VMFS-Datenspeichers zu einem geschützten Cluster wird dieser automatisch geschützt.
- Sie können keinen Datastore in einem Rechenzentrum mit einem oder mehreren geschützten Host-Clustern erstellen.
- Sie können keinen Datenspeicher auf einem ESXi-Host erstellen, wenn der übergeordnete Hostcluster durch eine „Automated Failover Duplex Policy“ (einheitliche oder nicht einheitliche Konfiguration) geschützt ist.
- 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 neuere Versionen unterstützen das NVMe/TCP-Protokoll. VMware vSphere 8.0 und neuere Versionen werden jedoch empfohlen.

b. Überprüfen Sie, ob der Anbieter der Netzwerkschnittstellenkarte (NIC) ESXi NIC mit dem NVMe/TCP-Protokoll unterstützt.

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

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 für die Version VMware vSphere 8, "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. Falls noch nicht aktiviert, 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 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**.
3. Wählen Sie den VMFS-Datastore-Typ 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 vorhandenen VMFS-Cluster hinzuzufügen, wählen Sie den Datenspeicher-Cluster in den erweiterten Optionen 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.

Wenn das NVMe/FC- oder NVMe/TCP-Protokoll ausgewählt wird, wird ein neues Namespace-Subsystem erstellt und für die Namespace-Zuordnung verwendet. ONTAP -Tools erstellen das Namespace-Subsystem mithilfe des automatisch generierten Namens, der den Datenspeichernamen enthält. Sie können das Namespace-Subsystem im Feld **Benutzerdefinierter Namespace-Subsystemname** in den erweiterten Optionen des Bereichs **Speicher** umbenennen.

6. Im Bereich **Storage attributes**:

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

   Bei ASA r2-Speichersystemen wird die Option **Aggregat** nicht angezeigt, da der Speicher disaggregiert ist. Wenn Sie einen ASA R2-Speichersystemtyp „SVM“ auswählen, werden auf der Seite mit den Speicherattributen die Optionen zum Aktivieren von QoS angezeigt.

   b. ONTAP -Tools erstellen basierend auf dem ausgewählten Protokoll eine Speichereinheit (LUN/Namespace) mit einer Thin-Space-Reserve.

   Ab ONTAP 9.16.1 unterstützen ASA r2 Storage-Systeme bis zu 12 Nodes pro Cluster.

   c. Wählen Sie das **Performance Service Level** für ASA r2 Speichersysteme mit 12 Knoten SVM, die ein heterogener Cluster ist. Diese Option ist nicht verfügbar, wenn die ausgewählte SVM ein homogenes Cluster ist oder einen SVM-Benutzer verwendet.

   „Beliebig“ ist der Standard-PSL-Wert (Performance Service Level). Diese Einstellung erstellt die Speichereinheit mithilfe des ONTAP-Algorithmus für die ausgewogene Platzierung. Sie können jedoch nach Bedarf die Option „Performance“ oder „Extreme“ auswählen.

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

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

   Sie können das vorhandene Volume nicht zum Erstellen eines VMFS-Datenspeichers mit NVMe/FC- oder NVMe/TCP-Protokoll verwenden. Erstellen Sie ein neues Volume für den VMFS-Datenspeicher.

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

ONTAP -Tools erstellen den VMFS-Datenspeicher und mounten ihn auf allen Hosts.

Sicherung von Data Stores und Virtual Machines

Schützen Sie einen Hostcluster in ONTAP tools

ONTAP Tools für VMware vSphere managen den Schutz von Host-Clustern. Alle Datastores, die zur ausgewählten SVM gehören und auf einem oder mehreren Hosts des Clusters gemountet werden, werden unter einem Host-Cluster geschützt.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie einen Hostcluster schützen:

- Der Hostcluster enthält nur Datenspeicher von einer einzigen SVM.
- Datenspeicher auf dem Hostcluster werden nicht auf Hosts außerhalb des Clusters gemountet.
- Auf dem Hostcluster gemountete Datenspeicher sind VMFS-Datenspeicher mit iSCSI- oder FC-Protokoll. Sie können keine vVols, NFS- oder VMFS-Datenspeicher mit NVMe/FC- und NVMe/TCP-Protokollen verwenden.
- Datenspeicher, die auf auf einem Host gemounteten FlexVol/LUN-Volumes basieren, sind nicht Teil einer Konsistenzgruppe.
- Datenspeicher, die auf auf einem Host gemounteten FlexVol/LUN-Volumes basieren, sind nicht Teil einer SnapMirror -Beziehung.
- Der Hostcluster enthält mindestens einen Datenspeicher.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie * NetApp ONTAP -Tools* > **Cluster schützen**.
3. Im Fenster „Cluster schützen“ trägt das System automatisch den Datenspeichertyp und die Details der virtuellen Maschine (VM) des Quellspeichers ein. Wählen Sie den Link „Datenspeicher“ aus, um die geschützten Datenspeicher anzuzeigen.
4. Wählen Sie **Beziehung Hinzufügen**.
5. Wählen Sie im Fenster **SnapMirror-Beziehung hinzufügen** den Typ **Zielspeicher-VM** und den Typ **Richtlinie** aus.

   Der Richtlinientyp kann „asynchron“ oder „AutomaticatedFailOverDuplex“ sein.

   Wenn Sie die SnapMirror Beziehung als Richtlinie vom Typ AutomatedFailOverDuplex hinzufügen, müssen Sie die Ziel-Storage VM als Storage-Backend zum gleichen vCenter hinzufügen, in dem ONTAP Tools für VMware vSphere implementiert werden.

   Beim Richtlinientyp „AutomatedFailOverDuplex“ gibt es einheitliche und nicht einheitliche Hostkonfigurationen. Wenn Sie die Umschalttaste **einheitliche Hostkonfiguration** auswählen, wird die Konfiguration der Hostinitiatorgruppe implizit auf der Zielsite repliziert. Weitere Informationen finden Sie unter "Schlüsselkonzepte und -Begriffe" .
6. Wenn Sie sich für eine nicht einheitliche Hostkonfiguration entscheiden, wählen Sie den Hostzugriff (Quelle/Ziel) für jeden Host innerhalb dieses Clusters aus.
7. Wählen Sie **Hinzufügen**.

8. Sie können den Hostclusterschutz mit dem Vorgang **Hostclusterschutz ändern** bearbeiten. Sie können die Beziehungen mithilfe der Auslassungspunkte-Menüoptionen bearbeiten oder löschen.
9. Wählen Sie die Schaltfläche **protect**.

   Das System erstellt eine vCenter-Aufgabe mit Job-ID-Details und zeigt ihren Fortschritt im Bereich „Letzte Aufgaben“ an. Dies ist eine asynchrone Aufgabe. Die Benutzeroberfläche zeigt nur den Status der Anforderungsübermittlung an und wartet nicht auf den Abschluss der Aufgabe.

10. Um die geschützten Host-Cluster anzuzeigen, gehen Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**. Wählen Sie eine Konsistenzgruppe aus, um ihre Kapazität, die zugehörigen Datenspeicher und die untergeordneten Konsistenzgruppen anzuzeigen.

> Wenn Sie den Schutz innerhalb einer Stunde nach der Erstellung entfernen müssen, führen Sie zuerst die Speichererkennung aus.

Verwandte Informationen

"VMware vSphere Metro Storage Cluster (vMSC)"

Schutz mit SRA-Sicherung

Konfigurieren Sie SRA in ONTAP tools, um Datastores zu schützen

ONTAP Tools für VMware vSphere bieten die Option zur Aktivierung der SRA-Funktionen zur Konfiguration der Disaster Recovery.

Bevor Sie beginnen

- Sie sollten Ihre vCenter Server-Instanz eingerichtet und den ESXi-Host konfiguriert haben.
- Sie sollten ONTAP Tools für VMware vSphere implementiert haben.
- Sie sollten die SRA Adapter- `.tar.gz`Datei von der heruntergeladen haben "NetApp Support Website".
- Sie sollten auf den Quell- und Ziel ONTAP -Clustern dieselben benutzerdefinierten SnapMirror -Zeitpläne haben, bevor Sie die SRA-Workflows ausführen.
- "Aktivieren Sie ONTAP-Tools für VMware vSphere-Services" um die SRA-Funktion zu aktivieren.

Schritte

1. Melden Sie sich über die URL: An der VMware Live Site Recovery Appliance Management Interface an `https://:<srm_ip>:5480`, und wechseln Sie dann zu Storage Replication Adapters in VMware Live Site Recovery Appliance Management Interface.
2. Wählen Sie **New Adapter**.
3. Laden Sie das Installationsprogramm *.tar.gz* für das SRA-Plug-in auf VMware Live Site Recovery hoch.
4. Überprüfen Sie die Adapter erneut, um sicherzustellen, dass die Details auf der Seite VMware Live Site Recovery Storage Replication Adapters aktualisiert werden.

> Nach einem Failover sind Aktionen wie Erweitern, Mounten und Löschen für Datenspeicher möglicherweise nicht verfügbar. Führen Sie eine Datenspeichererkennung durch, um die entsprechenden Kontextmenüaktionen zu aktualisieren und anzuzeigen.

Nach jedem erneuten Schutzvorgang müssen Sie auf beiden Sites eine Speichererkennung durchführen.

Führen Sie bei einer neuen Konfiguration mit SRA-Schutz immer ein Test-Failover durch. Das Überspringen des Test-Failovers kann dazu führen, dass der Vorgang zum erneuten Schützen fehlschlägt.

Führen Sie in einer Fan-Out-Konfiguration nach einem SnapMirror Active Sync-Failover, bei dem die SnapMirror Quelle für Automated Failover Duplex und Asynchronous SnapMirror zu Site B wechselt, ein Test-Failover zwischen Site B und C aus. Das Überspringen dieses Schritts kann zu einem fehlgeschlagenen Vorgang zum erneuten Schützen führen.

Verwandte Informationen

"Konfigurieren der Notfallwiederherstellung für NFS-Datenspeicher mit VMware Site Recovery Manager"

Konfigurieren Sie SRA in ONTAP tools for VMware vSphere für SAN- und NAS-Umgebungen

Sie sollten die Speichersysteme einrichten, bevor Sie Storage Replication Adapter (SRA) für die VMware Live Site Recovery ausführen.

Konfiguration von SRA für SAN-Umgebungen

Bevor Sie beginnen

Die folgenden Programme sollten auf dem geschützten Standort und dem Wiederherstellungsstandort installiert sein:

- VMware Live Site Recovery: Die VMware-Site bietet Installationsdokumentation für VMware Live Site Recovery.

  "Über VMware Live Site Recovery"

- SRA: Installieren Sie den Adapter auf VMware Live Site Recovery.

Schritte

1. Vergewissern Sie sich, dass die primären ESXi-Hosts mit den LUNs im primären Speichersystem am geschützten Standort verbunden sind.
2. Vergewissern Sie sich, dass die LUNS in Initiatorgruppen vorhanden sind, die über die verfügen `ostype` Option auf dem primären Storage-System auf *VMware* eingestellt.
3. Stellen Sie sicher, dass die ESXi-Hosts am Wiederherstellungsstandort über eine entsprechende iSCSI- und Fibre Channel-Konnektivität zur Storage Virtual Machine (SVM) verfügen. Die ESXi-Hosts des sekundären Standorts sollten Zugriff auf den Speicher des sekundären Standorts haben und die ESXi-Hosts des primären Standorts sollten Zugriff auf den Speicher des primären Standorts haben.

   Dazu können Sie entweder überprüfen, ob die ESXi-Hosts über lokale LUNs auf der SVM oder auf der verfügen `iscsi show initiators` Befehl auf den SVMs.
   Überprüfen Sie den LUN-Zugriff auf die zugeordneten LUNs auf dem ESXi-Host, um die iSCSI-Konnektivität zu überprüfen.

Konfiguration von SRA für NAS-Umgebungen

Bevor Sie beginnen

Die folgenden Programme sollten auf dem geschützten Standort und dem Wiederherstellungsstandort installiert sein:

- VMware Live Site Recovery: Installationsdokumentation für VMware Live Site Recovery finden Sie auf der VMware-Site – "Über VMware Live Site Recovery"
- SRA: Installieren Sie den Adapter auf VMware Live Site Recovery und dem SRA-Server.

Schritte

1. Überprüfen Sie, ob die Datenspeicher am geschützten Standort virtuelle Maschinen enthalten, die bei vCenter Server registriert sind.
2. Überprüfen Sie, ob die ESXi-Hosts am geschützten Standort die NFS-Exporte-Volumes von der Storage Virtual Machine (SVM) gemountet haben.
3. Stellen Sie sicher, dass gültige Adressen wie die IP-Adresse oder der FQDN, unter dem die NFS-Exporte vorliegen, im Feld **NFS-Adressen** angegeben sind, wenn Sie den Array Manager-Assistenten zum Hinzufügen von Arrays zu VMware Live Site Recovery verwenden. Verwenden Sie im Feld **NFS-Adressen** nicht den NFS-Hostnamen.
4. Verwenden Sie die `ping` Führen Sie einen Befehl auf jedem ESXi Host am Recovery-Standort aus, um zu überprüfen, ob der Host über einen VMkernel-Port verfügt, der auf die IP-Adressen zugreifen kann, die für NFS-Exporte von der SVM verwendet werden.

Konfigurieren Sie SRA in ONTAP tools für hochskalierte Umgebungen

Sie sollten die Storage-Timeout-Intervalle gemäß den empfohlenen Einstellungen für Storage Replication Adapter (SRA) so konfigurieren, dass sie in stark skalierten Umgebungen optimal funktionieren.

Einstellungen für Speicheranbieter

Sie sollten die folgenden Zeitüberschreitungswerte auf VMware Live Site Recovery für eine skalierte Umgebung festlegen:

Erweiterte Einstellungen	Timeout-Werte
`StorageProvider.resignatureTimeout`	Erhöhen Sie den Wert der Einstellung von 900 Sekunden auf 12000 Sekunden.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Legen Sie einen hohen Wert fest (z. B. 99999).

Sie sollten auch die aktivieren `StorageProvider.autoResignatureMode` Option.

Weitere Informationen zum Ändern von Speicheranbietereinstellungen finden Sie unter "Ändern Sie Die Einstellungen Des Speicheranbieters".

Speichereinstellungen

Wenn Sie auf ein Timeout klicken, erhöhen Sie die Werte von `storage.commandTimeout` Und `storage.maxConcurrentCommandCnt` Zu einem höheren Wert.

> Das angegebene Timeout-Intervall ist der Maximalwert. Sie müssen nicht warten, bis das maximale Timeout erreicht ist. Die meisten Befehle werden innerhalb des festgelegten maximalen Timeout-Intervalls abgeschlossen.

Informationen zum Ändern der SAN-Provider-Einstellungen finden Sie unter "Ändern Sie Die Speichereinstellungen".

Konfigurieren Sie SRA auf der VMware Live Site Recovery Appliance mithilfe von ONTAP tools

Konfigurieren Sie nach der Bereitstellung der VMware Live Site Recovery-Appliance den Storage Replication Adapter (SRA), um die Notfallwiederherstellungsverwaltung zu aktivieren.

Durch die Konfiguration von SRA auf der VMware Live Site Recovery-Appliance werden die ONTAP tools for VMware vSphere -Anmeldeinformationen innerhalb der Appliance gespeichert, wodurch die Kommunikation zwischen VMware Live Site Recovery und SRA ermöglicht wird.

Bevor Sie beginnen

- Laden Sie die Datei *.tar.gz* von der "NetApp Support Website" .
- Aktivieren Sie SRA-Dienste im ONTAP Tools Manager. Weitere Informationen finden Sie im "Dienste aktivieren" Abschnitt.
- Fügen Sie vCenter-Server zu den ONTATP-Tools für die VMware vSphere-Appliance hinzu. Weitere Informationen finden Sie im "vCenter-Server hinzufügen" Abschnitt.
- Fügen Sie den ONTAP tools for VMware vSphere Speicher-Backends hinzu. Weitere Informationen finden Sie im "Speicher-Backends hinzufügen" Abschnitt.

> Wenn Sie den vCenter-Zertifikatpatch von ONTAP -Tools angewendet haben, aktualisieren Sie die vCenter-Konfiguration im VMware Live Site Recovery-Gerät mithilfe des Ports (:5480). Anweisungen hierzu finden Sie unter "Neukonfigurieren der Site Recovery Manager Appliance" .

Schritte

1. Wählen Sie auf dem Bildschirm VMware Live Site Recovery Appliance **Storage Replication Adapter** > **New Adapter** aus.
2. Laden Sie die Datei *.tar.gz* in die VMware Live Site Recovery hoch.
3. Melden Sie sich mit einem Administratorkonto über einen SSH-Client wie PuTTY bei der VMware Live Site Recovery-Appliance an.
4. Wechseln Sie mit dem Befehl zum Root-Benutzer: `su root`
5. Führen Sie den Befehl aus `cd /var/log/vmware/srm` um zum Protokollverzeichnis zu gelangen.
6. Geben Sie am Protokollspeicherort den Befehl ein, um die von SRA verwendete Docker-ID abzurufen: `docker ps -l`
7. Um sich bei der Container-ID anzumelden, geben Sie den Befehl ein: `docker exec -it -u srm`

`<container id> sh`

8. Konfigurieren Sie VMware Live Site Recovery mit ONTAP tools for VMware vSphere IP-Adresse und das Kennwort mithilfe des folgenden Befehls: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv -username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - Geben Sie das Kennwort in einfachen Anführungszeichen ein, damit das Perl-Skript Sonderzeichen als Teil des Kennworts und nicht als Trennzeichen behandelt.
   - Sie können den Benutzernamen und das Kennwort der Anwendung (VASA Provider/SRA) im ONTAP Tools Manager festlegen, wenn Sie diese Dienste zum ersten Mal aktivieren. Verwenden Sie diese Anmeldeinformationen, um SRA bei VMware Live Site Recovery zu registrieren.
   - Um die vCenter-GUID zu finden, gehen Sie nach dem Hinzufügen Ihrer vCenter-Instanz zur vCenter-Server-Seite im ONTAP Tools Manager. Siehe"vCenter-Server hinzufügen" Abschnitt.
9. Scannen Sie die Adapter erneut, um zu bestätigen, dass die aktualisierten Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ angezeigt werden.

Ergebnisse Es wird eine Bestätigungsmeldung angezeigt, die angibt, dass die Speicheranmeldeinformationen gespeichert wurden. Sie können jetzt SRA verwenden, um mit dem SRA-Server unter Verwendung der angegebenen IP-Adresse, des Ports und der Anmeldeinformationen zu kommunizieren.

Aktualisieren Sie die SRA-Anmeldeinformationen in ONTAP tools

Damit VMware Live Site Recovery mit SRA kommunizieren kann, sollten Sie die SRA-Anmeldeinformationen auf dem VMware Live Site Recovery-Server aktualisieren, wenn Sie die Anmeldeinformationen geändert haben.

Bevor Sie beginnen

Sie sollten die im Thema genannten Schritte ausgeführt haben "Konfigurieren von SRA auf einer VMware Live Site Recovery-Appliance".

Schritte

1. Führen Sie die folgenden Befehle aus, um den Ordner des VMware Live Site Recovery-Rechners im Cache gespeicherte ONTAP-Tools username password zu löschen:
   a. `sudo su <enter root password>`
   b. `docker ps`
   c. `docker exec -it <container_id> sh`
   d. `cd conf/`
   e. `rm -rf *`
2. Führen Sie den Perl-Befehl aus, um SRA mit den neuen Anmeldeinformationen zu konfigurieren:
   a. `cd ..`
   b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` Sie benötigen ein einziges Angebot um den Passwortwert herum.

      Eine Erfolgsmeldung, die bestätigt, dass die Speicher-Anmeldedaten gespeichert werden, wird angezeigt. SRA kann mit dem SRA-Server unter Verwendung der angegebenen IP-Adresse, des Ports und der Anmeldeinformationen kommunizieren.

Konfigurieren von geschützten und Wiederherstellungsstandorten in ONTAP tools

Sie sollten Schutzgruppen erstellen, um eine Gruppe virtueller Maschinen am geschützten Standort zu schützen.

Wenn Sie einen neuen Datenspeicher hinzufügen, können Sie ihn in die bestehende Datenspeichergruppe aufnehmen oder einen neuen Datenspeicher hinzufügen und ein neues Volume oder eine neue Konsistenzgruppe zum Schutz erstellen. Nachdem Sie einen neuen Datenspeicher zu einer geschützten Konsistenzgruppe oder einem geschützten Volume hinzugefügt haben, aktualisieren Sie SnapMirror und führen Sie die Speichererkennung sowohl auf dem geschützten als auch auf dem Wiederherstellungsstandort durch. Sie können die Erkennung manuell oder nach Zeitplan durchführen, um sicherzustellen, dass der neue Datenspeicher erkannt und geschützt wird.

Kombinieren Sie geschützte Standorte und Recovery-Standorte

Sie sollten die geschützten und Recovery-Standorte, die mit Ihrem vSphere Client erstellt wurden, koppeln, um Storage Replication Adapter (SRA) zur Erkennung der Speichersysteme zu aktivieren.

> Storage Replication Adapter (SRA) unterstützt Fan-Out mit einer Synchronisierungsbeziehung vom Typ „Automated Failover Duplex“ und der asynchronen Beziehung SnapMirror auf der Konsistenzgruppe. Allerdings wird Fan-Out mit zwei asynchronen SnapMirror auf einer Konsistenzgruppe oder Fan-Out-SnapMirrors auf einem Volume nicht unterstützt. SnapMirror -Beziehungen vom Vault-Typ werden bei diesen Fan-Out-Einschränkungen nicht berücksichtigt.

Bevor Sie beginnen

- VMware Live Site Recovery sollte auf den geschützten und Recovery-Standorten installiert sein.
- SRA sollte auf den geschützten und den Recovery-Standorten installiert sein.

Schritte

1. Doppelklicken Sie auf der Startseite des vSphere-Clients auf das Symbol **Site Recovery** und wählen Sie dann **Sites** aus.
2. Wählen Sie **Objects** > **Actions** > **Pair Sites**.
3. Geben Sie im Dialogfeld **Pair Site Recovery Manager Servers** die Adresse des Platform Services Controllers des geschützten Standorts ein, und wählen Sie dann **Next**.
4. Gehen Sie im Abschnitt vCenter Server auswählen folgendermaßen vor:
   a. Stellen Sie sicher, dass der vCenter Server des geschützten Standorts als übereinstimmender Kandidat für das Pairing angezeigt wird.
   b. Geben Sie die SSO-Administratoranmeldedaten ein, und wählen Sie dann **Finish**.
5. Wenn Sie dazu aufgefordert werden, wählen Sie **Ja**, um die Sicherheitszertifikate zu akzeptieren.

Ergebnis

Im Dialogfeld **Objekte** werden sowohl die geschützten als auch die Wiederherstellungssites angezeigt.

Konfigurieren Sie Schutzgruppen

Bevor Sie beginnen

Stellen Sie sicher, dass die Quell- und Zielstandorte für Folgendes konfiguriert sind:

- Dieselbe Version von VMware Live Site Recovery ist installiert

- Virtual Machines
- Gepaarte geschützte Standorte und Recovery-Standorte
- Quell- und Ziel-Datastores sollten auf den jeweiligen Sites gemountet werden

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery** > **Schutzgruppen**.
2. Wählen Sie im Bereich **Schutzgruppen Neu** aus.
3. Geben Sie einen Namen und eine Beschreibung für die Schutzgruppe, Richtung und wählen Sie **Weiter**.
4. Wählen Sie im Feld **Typ** die Option **Typfeldoption…** als Datenspeichergruppen (Array-basierte Replikation) für NFS- und VMFS-Datenspeicher aus. Die Fehlerdomäne besteht ausschließlich aus SVMs mit aktivierter Replikation. Es werden die SVMs angezeigt, die nur Peering implementiert haben und keine Probleme aufweisen.
5. Wählen Sie auf der Registerkarte Replikationsgruppen entweder das aktivierte Array-Paar oder die Replikationsgruppen aus, für die die virtuelle Maschine konfiguriert ist, und wählen Sie dann **Weiter** aus.

   Alle virtuellen Maschinen auf der Replikationsgruppe werden der Schutzgruppe hinzugefügt.
6. Sie können entweder den vorhandenen Wiederherstellungsplan auswählen oder einen neuen erstellen, indem Sie **Zum neuen Wiederherstellungsplan hinzufügen** auswählen.
7. Überprüfen Sie auf der Registerkarte bereit zur Fertigstellung die Details der von Ihnen erstellten Schutzgruppe, und wählen Sie dann **Fertig stellen** aus.

Konfigurieren Sie geschützte Ressourcen und Recovery-Standortressourcen

Netzwerkzuordnungen in ONTAP tools konfigurieren

Sie sollten Ihre Ressourcenzuordnungen wie VM-Netzwerke, ESXi-Hosts und Ordner an beiden Standorten konfigurieren, um die Zuordnung jeder Ressource vom geschützten Standort zur entsprechenden Ressource am Recovery-Standort zu ermöglichen.

Sie sollten die folgenden Ressourcenkonfigurationen abschließen:

- Netzwerkzuordnungen
- Ordnerzuordnungen
- Ressourcen-Zuordnungen
- Platzhalter-Datenspeicher

Bevor Sie beginnen

Sie sollten die geschützten und Recovery-Standorte verbunden haben.

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie **Netzwerkzuordnungen** > **Neu** auf der Registerkarte Verwalten, um eine neue Netzwerkzuordnung zu erstellen.
4. Führen Sie im Assistenten zum Erstellen von Netzwerkzuordnungen die folgenden Schritte aus:

a. Wählen Sie **Zuordnungen für Netzwerke mit übereinstimmenden Namen automatisch vorbereiten** aus und wählen Sie **Weiter** aus.

b. Wählen Sie die gewünschten Rechenzentrumsobjekte für die geschützten und Recovery-Standorte aus und wählen Sie **Zuordnungen hinzufügen**.

c. Wählen Sie **Weiter**, nachdem Zuordnungen erfolgreich erstellt wurden.

d. Wählen Sie das zuvor verwendete Objekt aus, um eine umgekehrte Zuordnung zu erstellen, und wählen Sie dann **Fertig stellen**.

Ergebnis

Auf der Seite Netzwerkzuordnungen werden die geschützten Standortressourcen und die Ressourcen des Recovery-Standorts angezeigt. Sie können die gleichen Schritte für andere Netzwerke in Ihrer Umgebung befolgen.

Ordnerzuordnungen in ONTAP tools konfigurieren

Sie sollten Ihre Ordner auf dem geschützten Standort und dem Wiederherstellungsstandort zuordnen, um die Kommunikation zwischen ihnen zu ermöglichen.

Bevor Sie beginnen

Sie sollten die geschützten und Recovery-Standorte verbunden haben.

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie auf der Registerkarte Verwalten das Symbol **Ordnerzuordnungen** > **Ordner**, um eine neue Ordnerzuordnung zu erstellen.
4. Führen Sie im Assistenten zum Erstellen der Ordnerzuordnung folgende Schritte aus:
   a. Wählen Sie **automatisch Zuordnungen für Ordner mit übereinstimmenden Namen vorbereiten** aus und wählen Sie **Weiter** aus.
   b. Wählen Sie die gewünschten Rechenzentrumsobjekte für die geschützten und Recovery-Standorte aus und wählen Sie **Zuordnungen hinzufügen**.
   c. Wählen Sie **Weiter**, nachdem Zuordnungen erfolgreich erstellt wurden.
   d. Wählen Sie das zuvor verwendete Objekt aus, um eine umgekehrte Zuordnung zu erstellen, und wählen Sie dann **Fertig stellen**.

Ergebnis

Auf der Seite Ordnerzuordnungen werden die geschützten Site-Ressourcen und die Ressourcen des Recovery-Standorts angezeigt. Sie können die gleichen Schritte für andere Netzwerke in Ihrer Umgebung befolgen.

Ressourcenzuordnungen in ONTAP tools konfigurieren

Sie sollten Ihre Ressourcen am geschützten Standort und am Recovery-Standort zuordnen, damit Virtual Machines für Failover auf eine oder mehrere Host-Gruppen konfiguriert sind.

Bevor Sie beginnen

Sie sollten die geschützten und Recovery-Standorte verbunden haben.

> In VMware Live Site Recovery können Ressourcen Ressourcen-Pools, ESXi-Hosts oder vSphere-Cluster sein.

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie **Ressourcenzuordnungen** > **Neu** auf der Registerkarte Verwalten, um eine neue Ressourcenzuordnung zu erstellen.
4. Führen Sie im Assistenten „Ressourcenzuordnung erstellen“ folgende Schritte aus:
   a. Wählen Sie **Zuordnungen automatisch für Ressource mit übereinstimmenden Namen vorbereiten** und wählen Sie **Weiter**.
   b. Wählen Sie die gewünschten Rechenzentrumsobjekte für die geschützten und Recovery-Standorte aus und wählen Sie **Zuordnungen hinzufügen**.
   c. Wählen Sie **Weiter**, nachdem Zuordnungen erfolgreich erstellt wurden.
   d. Wählen Sie das zuvor verwendete Objekt aus, um eine umgekehrte Zuordnung zu erstellen, und wählen Sie dann **Fertig stellen**.

Ergebnis

Auf der Seite Ressourcenzuordnungen werden die geschützten Standortressourcen und die Ressourcen des Recovery-Standorts angezeigt. Sie können die gleichen Schritte für andere Netzwerke in Ihrer Umgebung befolgen.

Platzhalterdatenspeicher in ONTAP tools konfigurieren

Konfigurieren Sie einen Platzhalterdatenspeicher, um im vCenter-Inventar am Wiederherstellungsstandort Speicherplatz für geschützte virtuelle Maschinen (VMs) zu reservieren. Platzhalter-Datenspeicher erfordern nur minimale Kapazität, da Platzhalter-VMs klein sind und normalerweise nur einige hundert Kilobyte verwenden.

Bevor Sie beginnen

- Stellen Sie sicher, dass die geschützten Sites und die Wiederherstellungssites verbunden sind.
- Überprüfen Sie, ob die Ressourcenzuordnungen konfiguriert wurden.

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie **Platzhalter-Datenspeicher** > **Neu** auf der Registerkarte Verwalten aus, um einen neuen Platzhalter-Datenspeicher zu erstellen.
4. Wählen Sie den entsprechenden Datastore aus und wählen Sie **OK**.

> Platzhalter-Datenspeicher können sich auf einem lokalen oder Remote-Speicher befinden, erfordern jedoch keine Replikation.

5. Wiederholen Sie die Schritte 3 bis 5, um einen Platzhalterdatenspeicher für den Recovery-Standort zu

konfigurieren.

Konfigurieren Sie SRA mithilfe des Array-Managers in ONTAP tools

Sie können Storage Replication Adapter (SRA) mithilfe des Array Manager-Assistenten von VMware Live Site Recovery konfigurieren, um Interaktionen zwischen VMware Live Site Recovery und Storage Virtual Machines (SVMs) zu ermöglichen.

Bevor Sie beginnen

- Sie sollten die geschützten Standorte und Recovery-Standorte in VMware Live Site Recovery gekoppelt haben.
- Sie sollten Ihren Onboarding Storage konfiguriert haben, bevor Sie den Array Manager konfigurieren.
- Die SnapMirror Beziehungen zwischen den geschützten Standorten und den Recovery-Standorten sollten konfiguriert und repliziert werden.
- Sie sollten die SVM-Management-LIFs aktivieren, um die Mandantenfähigkeit zu aktivieren.

SRA unterstützt das Management auf Cluster-Ebene und das Management der SVM. Wenn Sie Storage auf Cluster-Ebene hinzufügen, können Sie Vorgänge für alle SVMs im Cluster erkennen und ausführen. Wenn Sie Storage auf SVM-Ebene hinzufügen, können Sie nur die spezifische SVM managen.

Schritte

1. Wählen Sie in VMware Live Site Recovery **Array Manager** > **Array Manager hinzufügen** aus.
2. Geben Sie die folgenden Informationen ein, um das Array in VMware Live Site Recovery zu beschreiben:

   a. Geben Sie einen Namen ein, um den Array-Manager im Feld **Anzeigename** zu identifizieren.

   b. Wählen Sie im Feld **SRA Typ NetApp Storage Replication Adapter für ONTAP** aus.

   c. Geben Sie die Informationen ein, die für eine Verbindung zum Cluster oder zur SVM benötigen:

      - Wenn Sie eine Verbindung zu einem Cluster herstellen, sollten Sie das LIF zur Clusterverwaltung eingeben.
      - Wenn Sie eine direkte Verbindung zu einem SVM herstellen, sollten Sie die IP-Adresse des SVM-Verwaltungs-LIF eingeben.

      > Beim Konfigurieren des Array Managers sollten Sie dieselbe Verbindung (IP-Adresse) für das Speichersystem verwenden, mit dem das Storage-System in ONTAP Tools für VMware vSphere integriert wurde. Wenn beispielsweise die Array Manager-Konfiguration im Umfang der SVM konfiguriert ist, sollte der Storage unter den ONTAP Tools für VMware vSphere auf SVM-Ebene hinzugefügt werden.

   d. Wenn Sie eine Verbindung zu einem Cluster herstellen, geben Sie den SVM-Namen im Feld **SVM-Name** an oder lassen Sie es leer, um alle SVMs im Cluster zu verwalten.

   e. Geben Sie die Volumes ein, die im Feld **Liste der Volumes include** erkannt werden sollen.

      Sie können das Quell-Volume am geschützten Standort und das replizierte Ziel-Volume am Recovery-Standort eingeben.

      Wenn Sie beispielsweise Volume src_vol1 ermitteln möchten, das sich in einer SnapMirror-Beziehung zu Volume dst_vol1 befindet, sollten Sie im Feld geschützter Standort src_vol1 und im Feld Wiederherstellungsstandort dst_vol1 angeben.

f. **(Optional)** Geben Sie im Feld **Volume exclude list** die Volumes ein, die von der Ermittlung ausgeschlossen werden sollen.

   Sie können das Quell-Volume am geschützten Standort und das replizierte Ziel-Volume am Recovery-Standort eingeben.

Wenn Sie beispielsweise Volume *src_vol1* aus einer SnapMirror-Beziehung mit Volume *dst_vol1* ausschließen möchten, sollten Sie *src_vol1* im Feld geschützter Standort und *dst_vol1* im Feld Wiederherstellungsstandort angeben.

3. Wählen Sie **Weiter**.
4. Überprüfen Sie, ob das Array erkannt und unten im Fenster Array-Manager hinzufügen angezeigt wird, und wählen Sie **Fertig stellen**.

Sie können dieselben Schritte für den Recovery-Standort befolgen, indem Sie die entsprechenden SVM-Management-IP-Adressen und Anmeldedaten verwenden. Auf dem Bildschirm Array-Paare aktivieren des Assistenten zum Hinzufügen von Array-Manager sollten Sie überprüfen, ob das richtige Array-Paar ausgewählt ist und dass es als bereit für die Aktivierung angezeigt wird.

Überprüfen Sie replizierte Speichersysteme in ONTAP tools

Sie sollten überprüfen, ob der geschützte Standort und der Recovery-Standort nach der Konfiguration des Storage Replication Adapter (SRA) erfolgreich gepaart wurden. Das replizierte Storage-System sollte sowohl vom geschützten Standort als auch vom Wiederherstellungsstandort erkannt werden können.

Bevor Sie beginnen

- Sie sollten Ihr Storage-System konfiguriert haben.
- Sie sollten den geschützten Standort und den Recovery-Standort mit dem VMware Live Site Recovery Array Manager gekoppelt haben.
- Bevor Sie den Test-Failover und den Failover-Vorgang für SRA durchführen, sollten Sie die FlexClone Lizenz und die SnapMirror Lizenz aktiviert haben.
- Auf Quell- und Zielstandorten sollten dieselben SnapMirror-Richtlinien und Zeitpläne eingehalten werden.

Schritte

1. Melden Sie sich bei Ihrem vCenter Server an.
2. Gehen Sie zu **Site Recovery** > **Array-basierte Replikation**.
3. Wählen Sie das erforderliche Array Pair aus, und überprüfen Sie die entsprechenden Details.

   Die Speichersysteme sollten am geschützten Standort und am Recovery-Standort mit dem Status „`enabled`“ erkannt werden.

Fan-out-Schutz in ONTAP tools

In einem Fan-Out-Schutzszenario ist die Konsistenzgruppe doppelt geschützt, mit einer synchronen Beziehung auf dem ersten Ziel ONTAP Cluster und mit einer asynchronen Beziehung auf dem zweiten Ziel ONTAP Cluster. Die Workflows zum Erstellen, Bearbeiten und Löschen des SnapMirror Active Sync-Schutzes gewährleisten den

synchronen Schutz. Failover- und Reprotect-Workflows der VMware Live Site Recovery-Appliance gewährleisten den asynchronen Schutz.

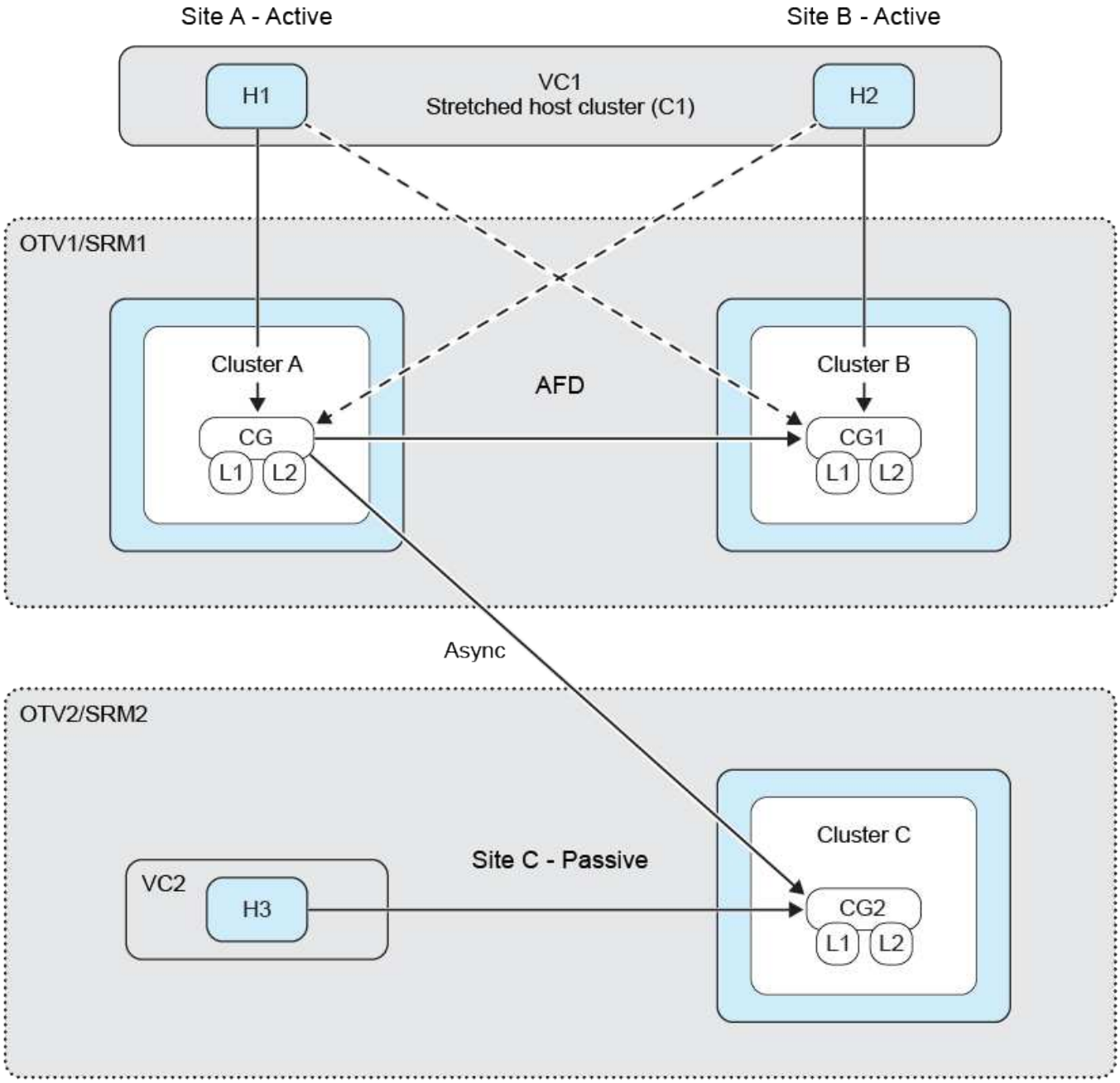
Fan-Out wird für SVM-Benutzer nicht unterstützt.

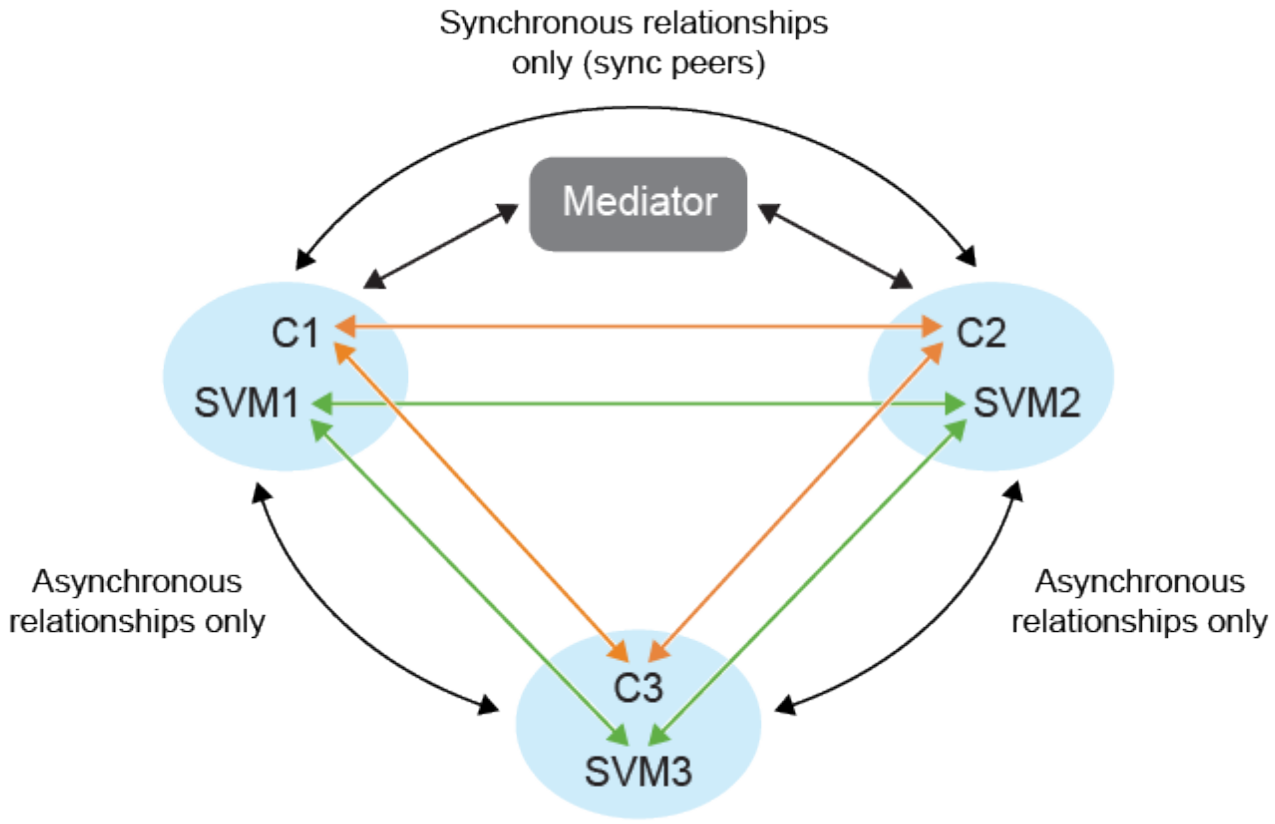
Um den Fan-Out-Schutz einzurichten, führen Sie ein Peering der drei Site-Cluster und SVMs durch.

Beispiel:

Wenn	Dann
• Die Konsistenzgruppe der Quelle befindet sich auf Cluster c1 und SVM svm1 • Die erste Ziel-Konsistenzgruppe befindet sich auf Cluster c2 und SVM svm2 und • Die zweite Ziel-Konsistenzgruppe befindet sich auf Cluster c3 und SVM svm3	• Der Cluster-Peering auf dem Quell-ONTAP-Cluster ist (C1, C2) und (C1, C3). • Der Cluster-Peering auf dem ersten Ziel-ONTAP-Cluster ist (C2, C1) und (C2, C3) • Der Cluster-Peering auf dem zweiten Ziel-ONTAP-Cluster sind (C3, C1) und (C3, C2). • SVM-Peering auf Quell-SVM wird (svm1, svm2) und (svm1, svm3) sein. • SVM-Peering auf der ersten Ziel-SVM wird (svm2, svm1) und (svm2, svm3) und sein • SVM-Peering auf zweite Ziel-SVM wird (svm3, svm1) und (svm3, svm2) sein.

Das folgende Diagramm zeigt die Fan-Out-Schutzkonfiguration:


Site A - Active
Site B - Active
VC1
Stretched host cluster (C1)
H1
H2
OTV1/SRM1
Cluster A
AFD
Cluster B
CG
L1
L2
CG1
L1
L2
Async
OTV2/SRM2
Cluster C
Site C - Passive
VC2
H3
CG2
L1
L2



Schritte

1. Wählen Sie einen neuen Platzhalter-Datenspeicher aus. Die Auswahlkriterien für den Platzhalterdatenspeicher für den stufenweisen Schutz sind:
   - Platzieren Sie den Platzhalter-Datenspeicher nicht im Hostcluster, den Sie schützen.
   - Wenn Sie den Platzhalter-Datenspeicher in den Hostcluster aufnehmen müssen, fügen Sie ihn der VMware Live Site Recovery-Appliance hinzu, bevor Sie den SnapMirror Active Sync-Schutz einrichten. Mit diesem Setup können Sie den Platzhalterdatenspeicher vom Schutz ausnehmen.

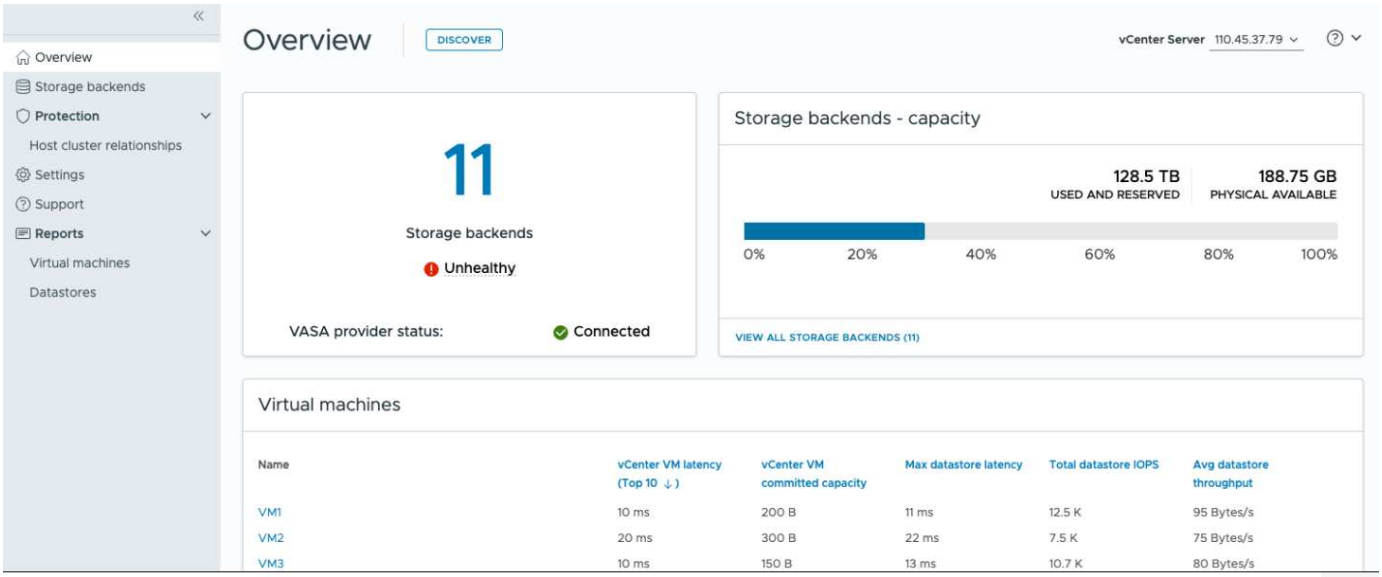
     Weitere Informationen finden Sie unter "Wählen Sie einen Platzhalter Datastore aus"
2. Fügen Sie dem Hostclusterschutz einen Datenspeicher hinzu, indem Sie Folgendes tun:"Geschütztes Host-Cluster ändern" . Fügen Sie sowohl asynchrone als auch synchrone Richtlinientypen hinzu.

Managen Sie ONTAP Tools für VMware vSphere

Erfahren Sie mehr über das ONTAP tools-Dashboard

Wenn Sie im vCenter-Client im Abschnitt „Verknüpfungen“ das Plug-in-Symbol „ONTAP tools for VMware vSphere“ auswählen, wird die Übersichtsseite geöffnet. Dieses Dashboard bietet eine Zusammenfassung der ONTAP tools for VMware vSphere Plug-in.

Im Enhanced Linked Mode (ELM) wird das Dropdown-Menü „vCenter Server“ angezeigt. Wählen Sie einen vCenter Server aus, um seine Daten anzuzeigen. Das Dropdown-Menü ist in allen Listenansichten des Plug-Ins verfügbar. Wenn Sie auf einer Seite einen vCenter Server auswählen, bleibt dieser beim Wechseln der Registerkarten im Plug-In
unverändert.



Von der Übersichtsseite aus können Sie die Aktion **Discovery** ausführen. Die Erkennungsaktion erkennt neu hinzugefügte oder aktualisierte Speicher-Backends, Hosts, Datenspeicher und Schutzstatus oder -beziehungen auf vCenter-Ebene. Führen Sie die Erkennung nach Bedarf aus, ohne auf die geplante Erkennung zu warten.

Die Aktionsschaltfläche **Erkennung** ist nur aktiviert, wenn Sie über die erforderliche Berechtigung zum Ausführen der Erkennungsaktion verfügen.

Nachdem die Ermittlungsanfrage übermittelt wurde, können Sie den Fortschritt der Aktion im Bereich „Letzte Aufgaben“ verfolgen.

Das Dashboard verfügt über mehrere Karten, die verschiedene Elemente des Systems anzeigen. Die folgende Tabelle zeigt die verschiedenen Karten und was sie darstellen.

Karte	Beschreibung

Status	Die Statuskarte zeigt die Anzahl der Speicher-Back-Ends und den allgemeinen Integritätsstatus der Speicher-Back-Ends und des VASA Providers an. Speicher-Back-Ends-Status zeigt **gesund** an, wenn der gesamte Speicher-Back-Ends-Status normal ist und es **ungesund** anzeigt, wenn eines der Speicher-Backends ein Problem hat (Unbekannt/Unerreichbar/herabgesetzt). Wählen Sie die QuickInfo aus, um die Statusdetails der Speicherbackends zu öffnen. Für weitere Details können Sie ein beliebiges Storage-Back-End auswählen. **Andere VASA Provider-Zustände** Link zeigt den aktuellen Status des VASA Providers an, der im vCenter Server registriert ist.
Storage Back-Ends – Kapazität	Diese Karte zeigt die aggregierte genutzte und verfügbare Kapazität aller Speicher-Backends für die ausgewählte vCenter Server-Instanz. Bei ASA R2-Speichersystemen werden die Kapazitätsdaten nicht angezeigt, da es sich um ein disaggregiertes System handelt.
Virtual Machines	Diese Karte zeigt die 10 wichtigsten VMs nach Performance-Metrik. Sie können die Kopfzeile auswählen, um die 10 wichtigsten VMs für die ausgewählte Metrik nach aufsteigender oder absteigender Reihenfolge zu erhalten. Die auf der Karte vorgenommenen Änderungen beim Sortieren und Filtern bleiben bestehen, bis Sie den Browser-Cache ändern oder löschen.
Datenspeicher	Diese Karte zeigt die 10 besten Datenspeicher, sortiert nach einer Performance-Metrik. Sie können die Kopfzeile auswählen, um die 10 wichtigsten Datastores für die ausgewählte Metrik nach aufsteigender oder absteigender Reihenfolge zu erhalten. Die auf der Karte vorgenommenen Änderungen beim Sortieren und Filtern bleiben bestehen, bis Sie den Browser-Cache ändern oder löschen. Zum Auswählen des Typs der Datastores – NFS, VMFS oder VVols – existiert ein Dropdown-Menü zum Datenspeichertyp.
ESXi-Host-Compliance-Karte	Diese Karte zeigt, ob alle ESXi-Hosts (für das ausgewählte vCenter) den empfohlenen NetApp Hosteinstellungen nach Gruppe oder Kategorie folgen. Sie können den Link **Empfohlene Einstellungen anwenden** auswählen, um die empfohlenen Einstellungen anzuwenden. Sie können den Konformitätsstatus der Hosts auswählen, um die Liste der Hosts anzuzeigen.

Wie ONTAP tools igroups und Exportrichtlinien verwaltet

Initiatorgruppen (igroups) sind Tabellen mit World Wide Port Names (WWPNs) des FC-Protokollhosts oder qualifizierten Knotennamen des iSCSI-Hosts. Sie können Initiatorgruppen definieren und sie LUNs zuordnen, um zu steuern, welche Initiatoren Zugriff auf LUNs haben.

In ONTAP tools for VMware vSphere 9.x wurden igroups in einer flachen Struktur erstellt und verwaltet, wobei jeder Datenspeicher in vCenter einer einzelnen igroup zugeordnet war. Dieses Modell schränkte die Flexibilität und Wiederverwendung von igroups über mehrere Datenspeicher hinweg ein. ONTAP tools for VMware vSphere führen verschachtelte igroups ein, bei denen jeder Datenspeicher in vCenter einer übergeordneten igroup zugeordnet ist, während jeder Host mit einer untergeordneten igroup unter dieser übergeordneten igroup verknüpft ist. Sie können benutzerdefinierte übergeordnete igroups mit benutzerdefinierten Namen zur Wiederverwendung in allen Datenspeichern definieren, um die igroup-Verwaltung zu vereinfachen. Verstehen Sie den igroup-Workflow zum Verwalten von LUNs und Datenspeichern in ONTAP tools for VMware vSphere. Verschiedene Workflows erzeugen unterschiedliche igroup-Konfigurationen, wie in den folgenden Beispielen gezeigt:

Die genannten Namen dienen nur zu Illustrationszwecken und beziehen sich nicht auf echte igroup-Namen. Von ONTAP -Tools verwaltete igroups verwenden das Präfix „otv_“. Benutzerdefinierten igroups kann ein beliebiger Name zugewiesen werden.

Begriff	Beschreibung
DS<Nummer>	Datenspeicher
iqn<Nummer>	Initiator-IQN
Host<Nummer>	Gastgeber MoRef
lun<Nummer>	LUN-ID
<DSName>Igroup<Nummer>	Standardmäßige (von ONTAP-Tools verwaltete) übergeordnete igroup
<Host-Moref>Igroup<Nummer>	Untergeordnete igroup
CustomIgroup<Nummer>	Benutzerdefinierte benutzerdefinierte übergeordnete igroup
ClassicIgroup<Nummer>	In den Versionen 9.x der ONTAP-Tools verwendete Igroup.

Beispiel 1:

Erstellen Sie einen Datenspeicher auf einem einzelnen Host mit einem Initiator

Workflow: [Erstellen] DS1 (lun1): host1 (iqn1)

Ergebnis:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)

ONTAP erstellt die übergeordnete Igroup DS1Igroup für DS1 und ordnet die untergeordnete Igroup host1Igroup lun1 zu. Das System ordnet LUNs immer untergeordneten igroups zu.

Beispiel 2:

Mounten Sie den vorhandenen Datenspeicher auf einem zusätzlichen Host

Workflow: [Mount] DS1 (lun1): host2 (iqn2)

Ergebnis:

- DS1Igroup:
  - host1Igroup → (iqn1: lun1)
  - host2Igroup → (iqn2: lun1)

ONTAP tools for VMware vSphere erstellen eine untergeordnete igroup host2Igroup und fügen sie der vorhandenen übergeordneten igroup DS1Igroup hinzu.

Beispiel 3:

Unmounten eines Datenspeichers von einem Host

Workflow: [Unmount] DS1 (lun1): host1 (iqn1)

Ergebnis:

- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

ONTAP tools for VMware vSphere entfernen host1Igroup aus der Hierarchie. Das System löscht untergeordnete igroups nicht explizit. Sie werden unter diesen beiden Bedingungen gelöscht:

- Wenn keine LUNs zugeordnet sind, löscht das ONTAP-System die untergeordnete igroup.
- Ein geplanter Bereinigungsauftrag entfernt die nicht mehr vorhandenen untergeordneten Igroups ohne LUN-Zuordnungen. Diese Szenarien gelten nur für von ONTAP-Tools verwaltete Igroups, nicht für benutzerdefinierte Igroups.

Beispiel 4:

Datenspeicher löschen

Workflow: [Löschen] DS1 (lun1): host2 (iqn2)

Ergebnis:

- DS1Igroup:
  - host2Igroup → (iqn2: lun1)

Übergeordnete und untergeordnete Igroups werden entfernt, sofern nicht ein anderer Datenspeicher die übergeordnete Igroup wiederverwendet. Untergeordnete igroups werden nicht explizit gelöscht

Beispiel 5:

Erstellen Sie mehrere Datenspeicher unter einer benutzerdefinierten übergeordneten igroup

Arbeitsablauf:

- [Erstellen] DS2 (lun2): host1 (iqn1), host2 (iqn2)
- [Erstellen] DS3 (lun3): host1 (iqn1), host3 (iqn3)

Ergebnis:

- CustomIgroup1:
  - host1Igroup → (iqn1: lun2, lun3)
  - host2Igroup → (iqn2: lun2)
  - host3Igroup → (iqn3: lun3)

CustomIgroup1 wird für DS2 erstellt und für DS3 wiederverwendet. Untergeordnete Igroups werden unter dem gemeinsamen übergeordneten Element erstellt oder aktualisiert, wobei jede untergeordnete Igroup den entsprechenden LUNs zugeordnet wird.

Beispiel 6:
Löschen Sie einen Datenspeicher unter einer benutzerdefinierten übergeordneten Igroup.

Workflow: [Löschen] DS2 (lun2): host1 (iqn1), host2 (iqn2)

Ergebnis:

- CustomIgroup1:
  - host1Igroup → (iqn1: lun3)
  - host3Igroup → (iqn3: lun3)
- Obwohl CustomIgroup1 nicht wiederverwendet wird, wird es nicht gelöscht.
- Wenn keine LUNs zugeordnet sind, löscht das ONTAP-System host2Igroup.
- Die Host1-Igroup wird nicht gelöscht, da sie der Lun3 von DS3 zugeordnet ist. Benutzerdefinierte Igroups werden unabhängig vom Wiederverwendungsstatus nie gelöscht.

Beispiel 7:
Erweitern Sie den vVols-Datenspeicher (Volume hinzufügen)

Arbeitsablauf:

Vor der Erweiterung:

[Erweitern] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

Nach der Erweiterung:

[Erweitern] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

Eine neue LUN wird erstellt und der vorhandenen untergeordneten Igroup „host4Igroup“ zugeordnet.

Beispiel 8:
vVols-Datenspeicher verkleinern (Volume entfernen)

Arbeitsablauf:

Vor dem Schrumpfen:

[Verkleinern] DS4 (lun4, lun5): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4, lun5)

Nach dem Schrumpfen:

[Verkleinern] DS4 (lun4): host4 (iqn4)

- DS4Igroup: host4Igroup → (iqn4: lun4)

Die Zuordnung der angegebenen LUN (lun5) zur untergeordneten Igroup wird aufgehoben. Die Igroup bleibt aktiv, solange sie mindestens eine zugeordnete LUN hat.

Beispiel 9:

Migration von ONTAP Tools 9 auf 10 (igroup-Normalisierung)

Arbeitsablauf

ONTAP -Tools für VMware vSPhere 9.x-Versionen unterstützen keine hierarchischen igroups. Während der Migration auf Version 10.3 oder höher müssen igroups in die hierarchische Struktur normalisiert werden.

Vor der Migration:

[Migration] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

Die Logik der ONTAP Tools 9.x ermöglicht mehrere Initiatoren pro Igroup, ohne eine Eins-zu-eins-Hostzuordnung zu erzwingen.

Nach der Migration:

[Migration] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → ClassicIgroup1: otv_ClassicIgroup1 (iqn6 & iqn7 : lun6, lun7)

Während der Migration:

- Eine neue übergeordnete Igroup (ClassicIgroup1) wird erstellt.
- Die ursprüngliche Igroup wird mit dem Präfix „otv_“ umbenannt und wird zu einer untergeordneten Igroup.

Dadurch wird die Einhaltung des hierarchischen Modells sichergestellt.

Verwandte Themen

"Allgemeines zu Initiatorgruppen"

Exportrichtlinien

Exportrichtlinien steuern den Zugriff auf NFS-Datenspeicher und die Clientberechtigungen in ONTAP tools for VMware vSphere. Exportrichtlinien werden in ONTAP -Systemen erstellt und verwaltet und können mit NFS-Datenspeichern verwendet werden, um die Zugriffskontrolle durchzusetzen. Jede Exportrichtlinie besteht aus Regeln, die die Clients (IP-Adressen oder Subnetze) angeben, denen Zugriff gewährt wird, und die erteilten Berechtigungen (schreibgeschützt oder Lese-/Schreibzugriff).

Beim Erstellen eines NFS-Datenspeichers in ONTAP Tools für VMware vSphere können Sie eine vorhandene Exportrichtlinie auswählen oder eine neue erstellen. Die Exportrichtlinie wird dann auf den Datenspeicher angewendet und stellt sicher, dass nur autorisierte Clients darauf zugreifen können.

Wenn Sie einen NFS-Datenspeicher auf einem neuen ESXi-Host mounten, fügen ONTAP Tools für VMware vSphere die IP-Adresse des Hosts der bestehenden Exportrichtlinie des Datenspeichers hinzu. Dadurch kann der neue Host auf den Datenspeicher zugreifen, ohne eine neue Exportrichtlinie erstellen zu müssen.

Wenn Sie einen NFS-Datenspeicher von einem ESXi-Host löschen oder aushängen, entfernen die ONTAP tools for VMware vSphere die IP-Adresse des Hosts aus der Exportrichtlinie. Wenn keine anderen Hosts diese Exportrichtlinie verwenden, wird sie gelöscht. Wenn Sie einen NFS-Datenspeicher löschen, entfernen die ONTAP tools for VMware vSphere die mit diesem Datenspeicher verknüpfte Exportrichtlinie, wenn sie nicht von anderen Datenspeichern wiederverwendet wird. Wenn die Exportrichtlinie wiederverwendet wird, bleibt die Host-IP-Adresse erhalten und ändert sich nicht. Wenn Sie die Datenspeicher löschen, hebt die Exportrichtlinie die Zuweisung der Host-IP-Adresse auf und weist eine Standardexportrichtlinie zu, sodass die ONTAP -Systeme bei Bedarf darauf zugreifen können.

Die Zuweisung der Exportrichtlinie unterscheidet sich, wenn sie in verschiedenen Datenspeichern wiederverwendet wird. Bei der Wiederverwendung der Exportrichtlinie können Sie die neue Host-IP-Adresse anhängen. Beim Löschen oder Unmounten eines Datenspeichers mit einer freigegebenen Exportrichtlinie wird die Richtlinie nicht gelöscht. Sie bleibt unverändert, und die Host-IP-Adresse wird nicht entfernt, da sie mit den anderen Datenspeichern gemeinsam genutzt wird. Die Wiederverwendung von Exportrichtlinien wird nicht empfohlen, da dies zu Zugriffs- und Latenzproblemen führen kann.

Verwandte Themen

"Erstellen Sie eine Exportrichtlinie"

Wie ONTAP tools igroups verwaltet

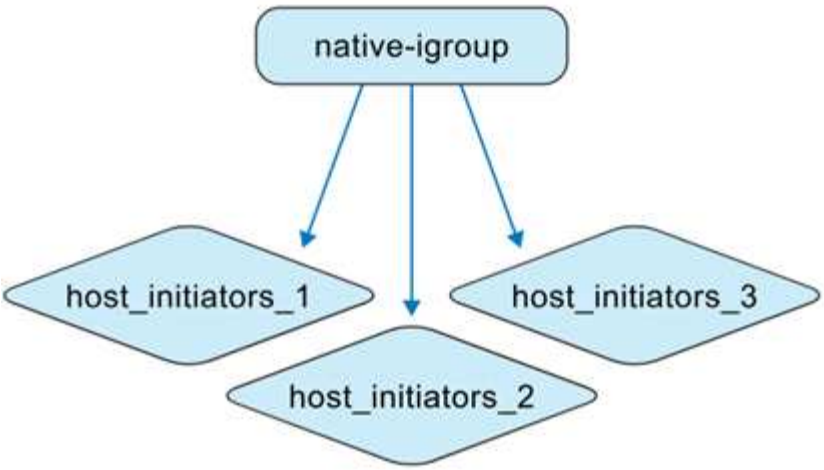
Wenn Sie sowohl VMs mit ONTAP -Tools als auch ONTAP Speichersysteme verwalten, ist es wichtig zu verstehen, wie sich igroups verhalten, insbesondere beim Verschieben von Datenspeichern aus Umgebungen, die nicht mit ONTAP -Tools verwaltet werden, in Umgebungen, die mit ONTAP-Tools verwaltet werden. Diese Seite erklärt, wie igroups während dieses Prozesses aktualisiert werden.

ONTAP tools for VMware vSphere 10.4 und höhere Versionen erstellen und verwalten automatisch ONTAP und vCenter-Objekte, um die Datenspeicherverwaltung in VMware-Rechenzentrumsumgebungen zu vereinfachen.

ONTAP tools for VMware vSphere interpretieren igroups in zwei verschiedenen Kontexten:

Von Nicht- ONTAP -Tools verwaltete igroups

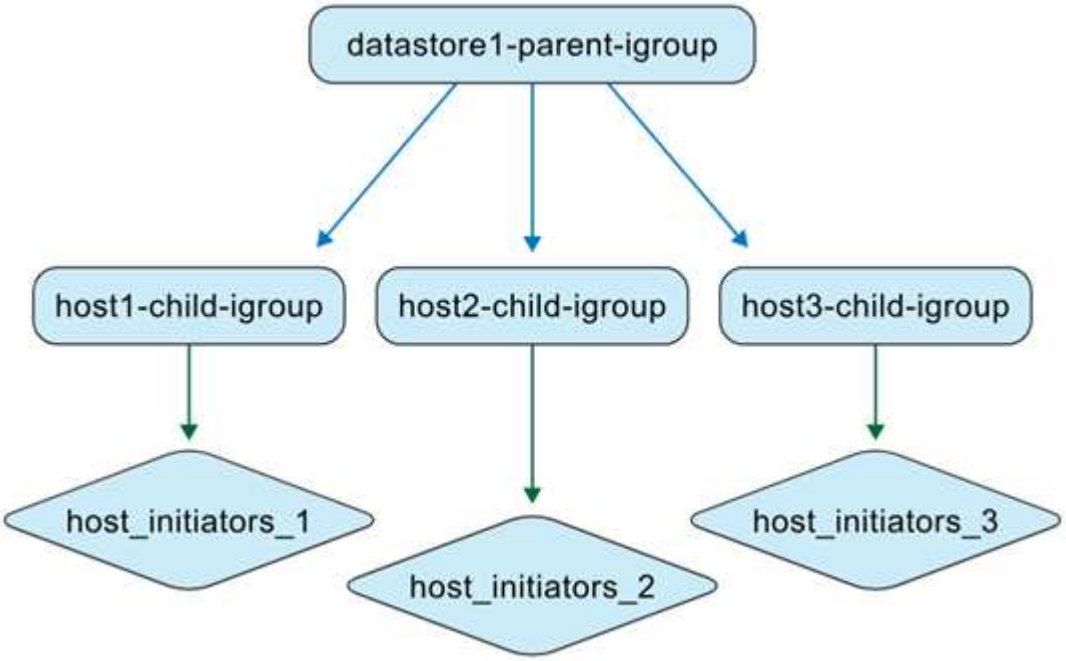
Als Speicheradministrator können Sie igroups auf dem ONTAP -System als flache oder verschachtelte Strukturen erstellen. Die Abbildung zeigt eine flache igroup, die im ONTAP -System erstellt wurde.

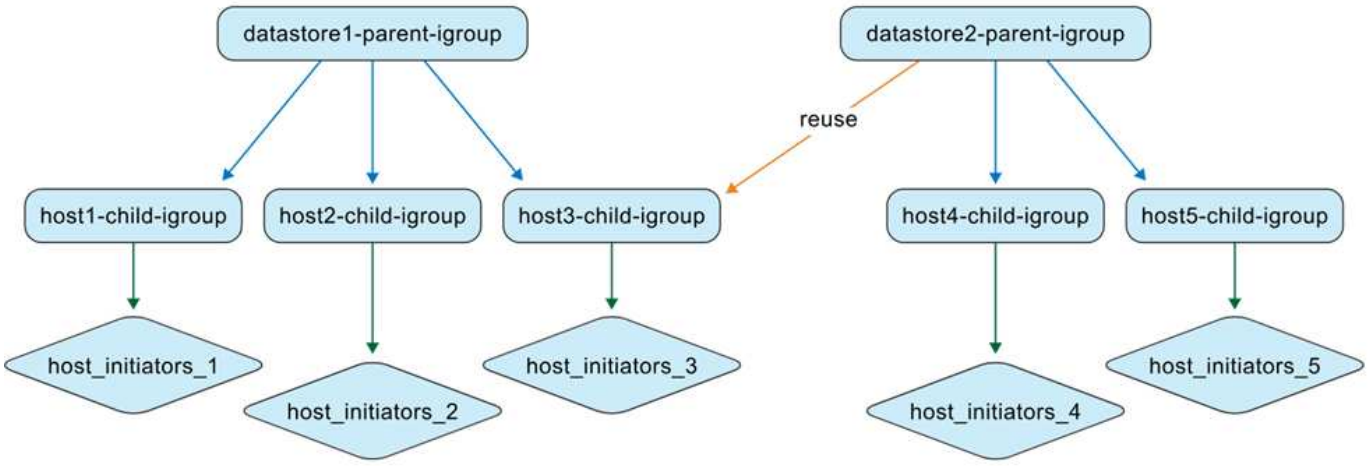


Von ONTAP -Tools verwaltete igroups

Wenn Sie Datenspeicher erstellen, erstellen ONTAP tools for VMware vSphere automatisch igroups mithilfe einer verschachtelten Struktur für eine einfachere LUN-Zuordnung.

Wenn beispielsweise Datastore1 erstellt und auf den Hosts 1, 2 und 3 gemountet wird und ein neuer Datastore (Datastore2) erstellt und auf den Hosts 3, 4 und 5 gemountet wird, verwenden ONTAP -Tools die igroup auf Hostebene für eine effiziente Verwaltung erneut.





Hier sind einige Fälle für ONTAP tools for VMware vSphere unterstützte igroups.

Wenn Sie einen Datenspeicher mit Standard-Igroup-Einstellungen erstellen

Wenn Sie einen Datenspeicher erstellen und das Feld „igroup“ leer lassen (Standardeinstellung), generieren ONTAP -Tools automatisch eine verschachtelte igroup-Struktur für diesen Datenspeicher. Die übergeordnete igroup auf Datenspeicherebene wird nach folgendem Muster benannt: otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>. Jede untergeordnete igroup auf Hostebene folgt dem Muster: otv_<hostMoref>_<vcguid>. Sie können die Zuordnung zwischen übergeordneten (Datenspeicherebene) und untergeordneten (Hostebene) igroups im Abschnitt **Parent Initiator Group** der ONTAP Speicherschnittstelle anzeigen.

Beim Ansatz mit verschachtelten igroups werden LUNs nur den untergeordneten igroups zugeordnet. Das vCenter Server-Inventar zeigt dann den neuen Datenspeicher an.

Wenn Sie einen Datenspeicher mit einem benutzerdefinierten igroup-Namen erstellen

Während der Datenspeichererstellung in ONTAP -Tools können Sie einen benutzerdefinierten Igroup-Namen eingeben, anstatt ihn aus der Dropdown-Liste auszuwählen. Anschließend erstellen die ONTAP -Tools eine übergeordnete igroup auf Datenspeicherebene mit dem von Ihnen angegebenen Namen. Wenn derselbe Host für mehrere Datenspeicher verwendet wird, wird die vorhandene (untergeordnete) igroup auf Hostebene wiederverwendet. Infolgedessen wird die LUN für den neuen Datenspeicher dieser vorhandenen untergeordneten Igroup zugeordnet, die jetzt möglicherweise mit mehreren übergeordneten Igroups verknüpft ist (eine für jeden Datenspeicher). Sie können den neuen Datenspeicher mit dem benutzerdefinierten Igroup-Namen in der vCenter Server-Schnittstelle sehen.

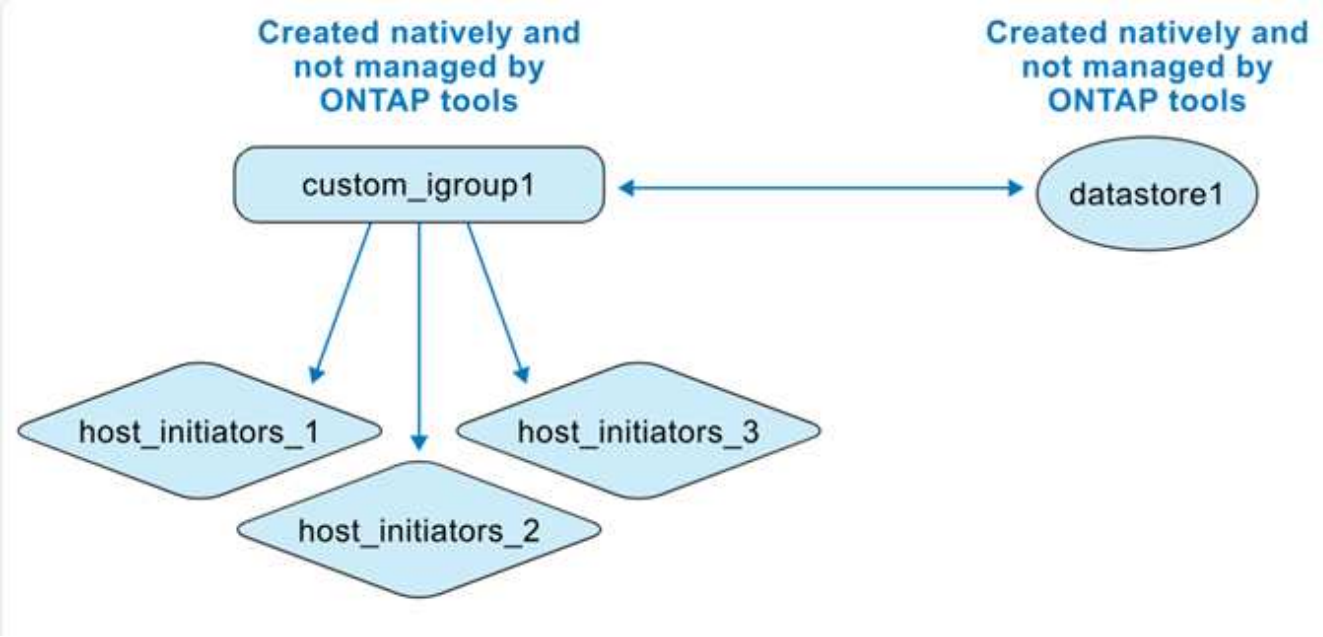
Wenn Sie den Igroup-Namen während der Datenspeichererstellung wiederverwenden

Wenn Sie einen Datenspeicher mithilfe der Benutzeroberfläche der ONTAP -Tools erstellen, können Sie eine vorhandene benutzerdefinierte übergeordnete igroup aus der Dropdown-Liste auswählen. Nachdem Sie die übergeordnete igroup zum Erstellen eines anderen Datenspeichers wiederverwendet haben, zeigt die Benutzeroberfläche des ONTAP -Systems diese Zuordnung an. Der neue Datenspeicher wird auch in der Benutzeroberfläche von vCenter Server angezeigt.

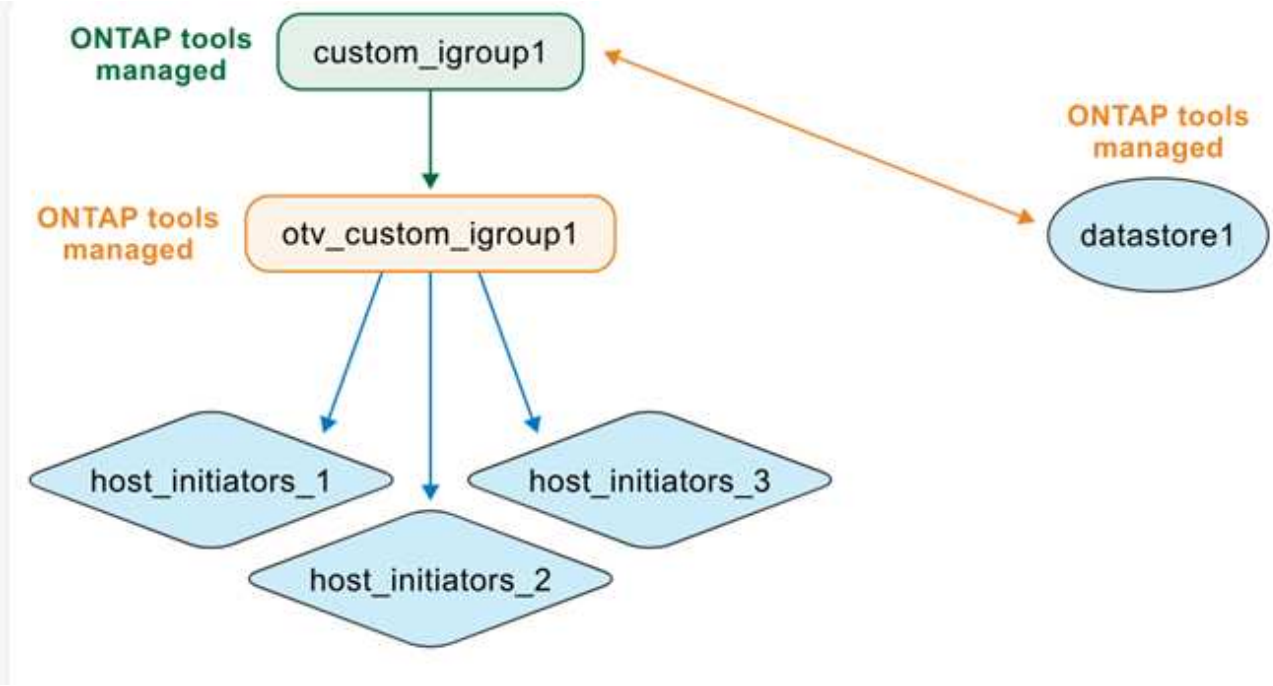
Dieser Vorgang kann auch mithilfe der API durchgeführt werden. Um eine vorhandene Igroup während der Datenspeichererstellung wiederzuverwenden, geben Sie die Igroup-UUID in der Nutzlast der API-Anforderung an.

Wenn Sie einen Datastore und eine igroup nativ von ONTAP und vCenter erstellen

Wenn Sie die igroup und den Datenspeicher direkt in ONTAP -Systemen und VMware-Umgebungen erstellen, verwalten die ONTAP Tools diese Objekte zunächst nicht. Dadurch entsteht eine flache Igroup-Struktur.



Um einen vorhandenen Datenspeicher und eine vorhandene igroup mit ONTAP Tools zu verwalten, sollten Sie eine Datenspeichererkennung durchführen. ONTAP -Tools identifizieren und registrieren den Datenspeicher und die Igroup und konvertieren sie in eine verschachtelte Struktur in ihrer Datenbank. Eine neue übergeordnete Igroup wird mit dem benutzerdefinierten Namen erstellt, während die vorhandene Igroup mit dem Präfix „otv_“ umbenannt wird und zur untergeordneten Igroup wird. Die Initiatorzuordnungen bleiben unverändert. Während der Erkennung werden nur den Datenspeichern zugeordnete Igroups konvertiert. Danach sieht die Igroup-Struktur wie in der folgenden Abbildung aus.



Nachdem Sie die Datenspeichererkennung in ONTAP -Tools ausgeführt haben, konvertieren ONTAP Tools die flache Igroup in eine verschachtelte Struktur. ONTAP -Tools verwalten dann die igroup und benennen sie mit dem Präfix „otv_“ um. Die LUN bleibt während des gesamten Vorgangs derselben Igroup zugeordnet.

Wie ONTAP -Tools nativ erstellte igroups wiederverwenden

Sie können einen Datenspeicher in ONTAP -Tools mithilfe einer Igroup erstellen, die zuerst in ONTAP Systemen erstellt wurde, nachdem ONTAP Tools sie verwaltet haben. Diese Igroups werden in der Dropdown-Liste mit den benutzerdefinierten Initiatorgruppennamen angezeigt. Die neue LUN für den Datenspeicher wird dann der entsprechenden normalisierten untergeordneten Igroup zugeordnet, beispielsweise „otv_NativeIgroup1“.

ONTAP tools for VMware vSphere erkennen oder verwenden keine im ONTAP System erstellten Igroups, die nicht von ONTAP Tools verwaltet oder mit einem Datenspeicher verknüpft werden.

Erfahren Sie mehr über die Benutzeroberfläche des ONTAP tools Manager

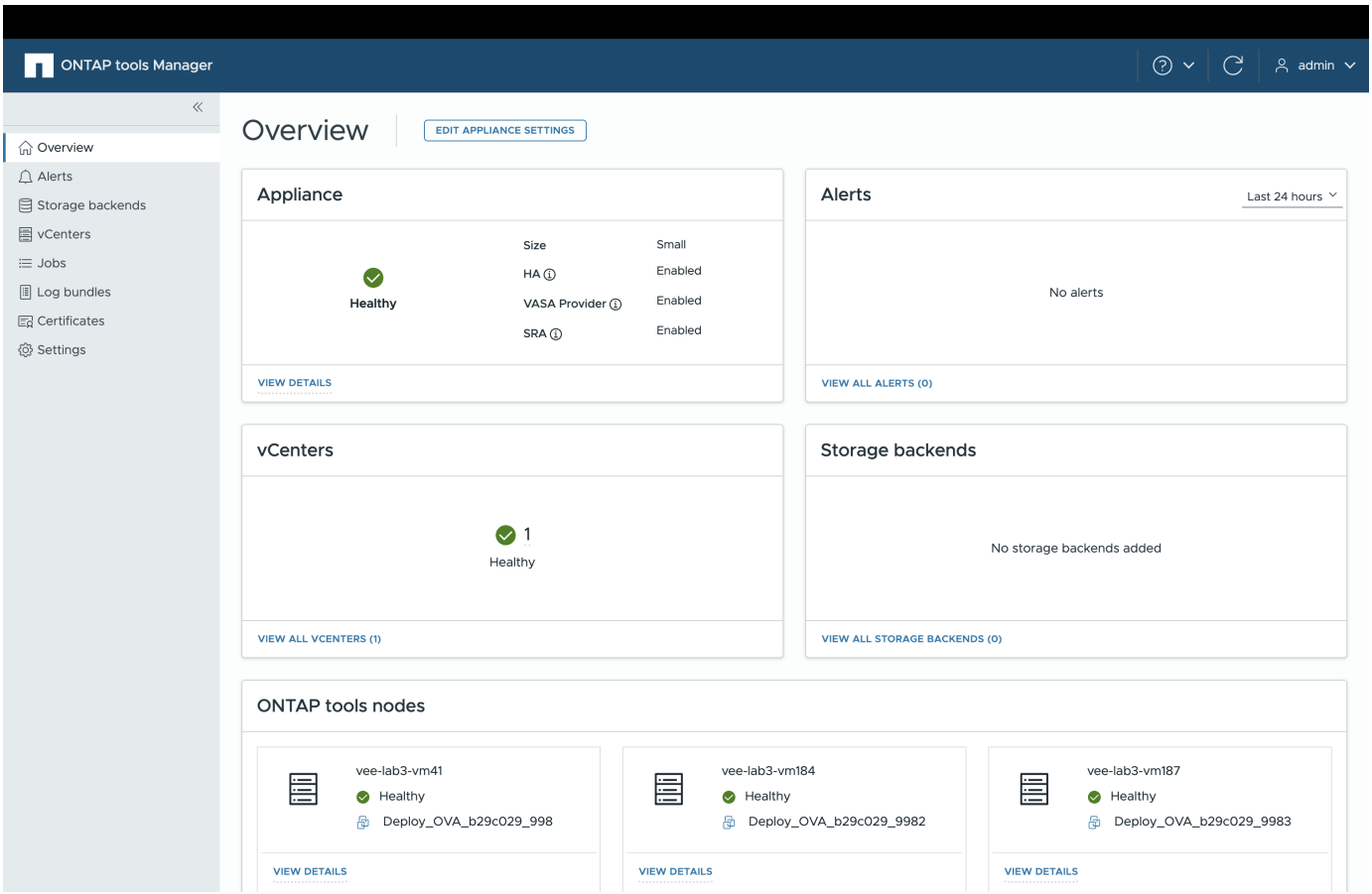
ONTAP tools for VMware vSphere unterstützen Multi-Tenancy und ermöglichen die Verwaltung mehrerer vCenter Server-Instanzen.

ONTAP Tools Manager ist eine webbasierte Konsole zum Verwalten von ONTAP tools for VMware vSphere, vCenter Server-Instanzen, Speicher-Backends und Appliance-Konfigurationen wie Hochverfügbarkeit (HA) und Knotenskalierung.

Der ONTAP Tools Manager bietet die folgenden Funktionen:

- Warnungen verwalten – Zeigen Sie von ONTAP tools for VMware vSphere generierte Warnungen an und filtern Sie sie.
- Speicher-Backends verwalten – Fügen Sie ONTAP Speichercluster hinzu, verwalten Sie sie und ordnen Sie sie global vCenter Server-Instanzen zu.
- vCenter Server-Instanzen verwalten – Fügen Sie vCenter Server-Instanzen innerhalb der ONTAP Tools hinzu und verwalten Sie sie.
- Jobs überwachen – Überwachen und debuggen Sie asynchrone Jobs, die sowohl über die Plug-in-Schnittstelle der ONTAP Tools als auch über die Manager-Schnittstelle der ONTAP -Tools initiiert wurden. Sie können Aufträge nach Zeitraum filtern, die Seitengröße anpassen und Auftragsdetails anzeigen, einschließlich Fehlern und Unteraufgaben. Klicken Sie auf einen fehlgeschlagenen Status, um Fehlerdetails anzuzeigen. Erweitern Sie bei Jobs mit Unteraufgaben die Zeile, um Beschreibungen und Status anzuzeigen. Verwenden Sie für Unteraufträge die Drilldown-Funktion des Auftrags, um die Details anzuzeigen.
- Laden Sie Protokollpakete herunter – Sammeln Sie Protokolldateien zur Fehlerbehebung bei ONTAP tools for VMware vSphere.
- Zertifikate verwalten – Ersetzen Sie das selbstsignierte Zertifikat durch ein benutzerdefiniertes CA-Zertifikat und erneuern oder aktualisieren Sie Zertifikate für VASA Provider und ONTAP Tools.
- Passwörter zurücksetzen – Ändern Sie das Passwort für den VASA-Anbieter und SRA.
- Appliance-Einstellungen verwalten – Konfigurieren Sie die ONTAP -Tools-Appliance, einschließlich der Aktivierung von HA und der Skalierung der Knotengrößen.

Um auf den ONTAP Tools Manager zuzugreifen, starten Sie `https://<ONTAPtoolsIP>:8443/virtualization/ui/` ihn über den Browser und melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.



Karte	Beschreibung
Gerätekarte	Die Appliance-Karte zeigt den Gesamtstatus der ONTAP Tools-Appliance, Konfigurationsdetails und den Status aktivierter Dienste. Um weitere Informationen anzuzeigen, wählen Sie den Link **Details anzeigen**. Wenn Sie eine Geräteeinstellung ändern, werden auf der Karte der Auftragsstatus und die Details angezeigt, bis die Änderung abgeschlossen ist.
Warnkarte	Auf der Karte „Warnungen“ werden Warnungen der ONTAP -Tools nach Typ kategorisiert angezeigt, einschließlich Warnungen auf HA-Knotenebene. Sie können detaillierte Warnungen anzeigen, indem Sie auf den Hyperlink „Zählen“ klicken. Dadurch gelangen Sie zur Warnungsseite, die nach dem ausgewählten Warnungstyp gefiltert ist.
vCenters-Karte	Die vCenters-Karte zeigt den Integritätsstatus aller von ONTAP -Tools verwalteten vCenter Server-Instanzen. Sie können Details zu jedem vCenter anzeigen, indem Sie den entsprechenden Link auswählen, der zu einer Seite mit weiteren Informationen zur ausgewählten Instanz führt.

Karte	Beschreibung
Speicher-Backends-Karte	Die Karte „Storage-Backends“ zeigt den Integritäts- und Konnektivitätsstatus aller in ONTAP -Tools konfigurierten ONTAP -Speichercluster an. Sie können Details zu jedem Speicher-Backend anzeigen, indem Sie den entsprechenden Link auswählen, der zu einer Seite mit weiteren Informationen zum ausgewählten Cluster führt.
Karte der ONTAP-Tools-Knoten	Die Knotenkarte des ONTAP -Tools zeigt alle Knoten im Gerät an, einschließlich Knotenname, VM-Name, Status und Netzwerkinformationen. Wählen Sie **Details anzeigen** aus, um weitere Details zu einem bestimmten Knoten anzuzeigen. [HINWEIS] In einer Nicht-HA-Konfiguration wird nur ein einzelner Knoten angezeigt. In einer HA-Konfiguration werden drei Knoten angezeigt.

Verwalten der ONTAP Tools Manager-Einstellungen

ONTAP tools AutoSupport-Einstellungen bearbeiten

Bei der erstmaligen Konfiguration von ONTAP tools for VMware vSphere ist AutoSupport standardmäßig aktiviert. Es sendet 24 Stunden nach der Aktivierung Nachrichten an den technischen Support.

Deaktivieren Sie AutoSupport

Wenn Sie AutoSupport deaktivieren, erhalten Sie keinen proaktiven Support und keine Überwachung mehr.

> Es wird empfohlen, AutoSupport aktiviert zu lassen, da es die Problemerkennung und -lösung beschleunigt. Auch wenn AutoSupport deaktiviert ist, sammelt und speichert das System weiterhin lokal Informationen, sendet jedoch keine Berichte über das Netzwerk.

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 die Option **Einstellungen** > **Telemetrie** > **Bearbeiten**.
4. Deaktivieren Sie die Option **AutoSupport** und speichern Sie die Änderungen.

Aktualisieren Sie die AutoSupport-Proxy-URL

Aktualisieren Sie die AutoSupport -Proxy-URL, damit die AutoSupport Funktion Daten zur sicheren Übertragung über den Proxy-Server leitet.

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 **Einstellungen** aus.
4. Wählen Sie die Option **Einstellungen** > **Telemetrie** > **Bearbeiten**.
5. Geben Sie eine gültige **Proxy-URL** ein und speichern Sie die Änderungen.

   Wenn Sie AutoSupport deaktivieren, ist auch die Proxy-URL deaktiviert.

Fügen Sie NTP-Server zu ONTAP tools hinzu

Geben Sie die NTP-Serverdetails ein, um die Zeituhren der ONTAP Tools-Appliance zu synchronisieren.

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 die Option **Einstellungen** > **NTP-Server** > **Bearbeiten**.
4. Geben Sie den vollständig qualifizierten Domänennamen (FQDN), IPv4- oder IPv6-Adressen durch Komma getrennt ein.

   Aktualisieren Sie den Bildschirm, um die aktualisierten Werte anzuzeigen.

VASA-Provider- und SRA-Anmeldeinformationen in ONTAP tools zurücksetzen

Wenn Sie Ihre VASA-Provider- oder SRA-Anmeldeinformationen vergessen, können Sie sie mithilfe der ONTAP Tools Manager-Schnittstelle auf ein neues Kennwort zurücksetzen. Das neue Passwort muss zwischen 8 und 256 Zeichen lang sein.

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 die Option **Einstellungen** > **VASA-Anbieter-/SRA-Anmeldeinformationen** > **Passwort zurücksetzen**.
4. Geben Sie das neue Passwort ein und bestätigen Sie es.
5. Wählen Sie **Speichern**, um die Änderungen zu übernehmen.

ONTAP tools-Sicherungseinstellungen bearbeiten

Ab ONTAP tools for VMware vSphere 10.5 ist die Backup-Funktion standardmäßig aktiviert und alle 10 Minuten wird ein Backup erstellt. Sie können die Sicherung

deaktivieren oder die Häufigkeit der Sicherung bearbeiten.

Deaktivieren Sie die Sicherung nicht, da dies die ONTAP -Tools daran hindert, einen niedrigen RPO aufrechtzuerhalten. Durch das Deaktivieren der Sicherung werden die vorhandenen Sicherungsdateien nicht gelöscht. Sie können die Häufigkeit der Sicherung auf einen Wert zwischen 10 und 60 Minuten ändern.

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 die Option **Einstellungen** > **Sicherung** > **Bearbeiten**.
4. Im Bearbeitungsfenster können Sie die Sicherung deaktivieren oder die Sicherungshäufigkeit bearbeiten.

ONTAP tools-Dienste aktivieren

Mithilfe von ONTAP Tools Manager kann das Administratorpasswort geändert werden, um Services wie VASA Provider, den Import der VVols-Konfiguration und die Disaster Recovery (SRA) mithilfe von ONTAP Tools Manager zu aktivieren.

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 im Übersichtsbereich die Option **Geräteeinstellungen bearbeiten** aus.
4. Im Abschnitt **Services** können Sie bei Bedarf optionale Dienste wie VASA Provider, den Import der vVols -Konfiguration und Disaster Recovery (SRA) aktivieren.

   Wenn Sie die Services zum ersten Mal aktivieren, müssen Sie die VASA Provider- und SRA-Anmeldeinformationen erstellen. Diese werden verwendet, um die VASA Provider- und SRA-Dienste auf dem vCenter Server zu registrieren oder zu aktivieren. Der Benutzername darf nur Buchstaben, Ziffern und Unterstriche enthalten. Das Passwort muss zwischen 8 und 256 Zeichen lang sein.

   Stellen Sie vor dem Deaktivieren optionaler Dienste sicher, dass die von ONTAP -Tools verwalteten vCenter-Server diese nicht verwenden.

   Die Option **Import der vVols -Konfiguration zulassen** wird nur angezeigt, wenn der VASA-Provider-Dienst aktiviert ist. Diese Option ermöglicht die vVols Datenmigration von ONTAP Tools 9.xx zu ONTAP Tools 10.5.

ONTAP-Tools-Appliance-Einstellungen ändern

Verwenden Sie den ONTAP Tools Manager, um die ONTAP tools for VMware vSphere Konfiguration zu skalieren, indem Sie entweder die Anzahl der Knoten erhöhen oder die Hochverfügbarkeit (HA) aktivieren. Standardmäßig werden die ONTAP tools for VMware vSphere Appliance als Einzelknotenkonfiguration ohne Hochverfügbarkeit bereitgestellt.

Bevor Sie beginnen

- Stellen Sie sicher, dass Ihre OVA-Vorlage die gleiche OVA-Version wie Knoten 1 hat. Knoten 1 ist der Standardknoten, auf dem die ONTAP-Tools für VMware vSphere OVA ursprünglich bereitgestellt werden.
- Stellen Sie sicher, dass der CPU-Hot-Plug-Speicher und der Hot-Plug-Speicher aktiviert sind.
- Stellen Sie im vCenter Server die Automatisierungsstufe des Disaster Recovery Service (DRS) auf „Teilautomatisiert“ ein. Setzen Sie sie nach der HA-Bereitstellung wieder auf „Vollautomatisiert“ zurück.
- Knoten-Hostnamen im HA-Setup sollten in Kleinbuchstaben geschrieben sein.

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 im Übersichtsbereich die Option **Geräteeinstellungen bearbeiten** aus.
4. Im Abschnitt **Konfiguration** können Sie die Knotengröße erhöhen und die HA-Konfiguration aktivieren. Verwenden Sie die Anmeldeinformationen des vCenter Servers, um Änderungen vorzunehmen.

   In der HA-Konfiguration können Sie Details zur Inhaltsbibliothek ändern. Geben Sie für jede Bearbeitung das Passwort an.

   In ONTAP tools for VMware vSphere können Sie die Knotengröße nur erhöhen, nicht jedoch verringern. In einem Nicht-HA-Setup wird nur eine mittelgroße Konfiguration unterstützt. In einem HA-Setup werden mittlere und große Konfigurationen unterstützt.

5. Aktivieren Sie die HA-Konfiguration mit der HA-Toggle-Taste. Stellen Sie auf der Seite **HA settings** Folgendes sicher:
   - Die Inhaltsbibliothek gehört zum gleichen vCenter Server, auf dem die ONTAP Tools-Knoten-VMs ausgeführt werden. VCenter Server-Anmeldeinformationen werden verwendet, um die OVA-Vorlage für Appliance-Änderungen zu validieren und herunterzuladen.
   - Die virtuelle Maschine, die die ONTAP-Tools hostet, wird nicht direkt auf einem ESXi-Host bereitgestellt. Die VM sollte auf einem Cluster oder einem Ressourcen-Pool bereitgestellt werden.

   Nachdem die HA-Konfiguration aktiviert wurde, können Sie nicht mehr zu einer Einzelknotenkonfiguration ohne HA zurückkehren.

6. Im Abschnitt **HA-Einstellungen** des Fensters **Appliance-Einstellungen bearbeiten** können Sie die Details der Knoten 2 und 3 eingeben. Die ONTAP Tools für VMware vSphere unterstützen drei Nodes im HA-Setup.

   Die ONTAP -Tools füllen die meisten Eingabefelder automatisch mit Netzwerkdetails von Knoten 1 aus, um den Arbeitsablauf zu vereinfachen. Sie können die Eingabedaten bearbeiten, bevor Sie zur letzten Seite des Assistenten gelangen. Sie können IPv6-Adressdetails für die anderen beiden Knoten nur eingeben, wenn die IPv6-Adresse auf dem Verwaltungsknoten der ONTAP -Tools aktiviert ist.

   Stellen Sie sicher, dass ein ESXi-Host nur eine VM mit ONTAP Tools enthält. Die Eingaben werden jedes Mal validiert, wenn Sie zum nächsten Fenster wechseln.

7. Überprüfen Sie die Details im Abschnitt **Zusammenfassung** und speichern Sie die Änderungen.

Was kommt als Nächstes?

Auf der Seite **Übersicht** wird der Status der Bereitstellung angezeigt. Sie können den Status des Auftrags „Geräteeinstellungen bearbeiten“ auch in der Auftragsansicht mithilfe der Auftrags-ID verfolgen.

Falls die HA-Bereitstellung fehlschlägt und der Status des neuen Knotens „Neu“ lautet, löschen Sie die neue VM in vCenter, bevor Sie versuchen, HA erneut zu aktivieren.

Auf der Registerkarte **Alerts** im linken Bereich werden Warnungen für ONTAP-Tools für VMware vSphere aufgelistet.

VMware vSphere-Hosts zu ONTAP tools hinzufügen

Fügen Sie neue VMware vSphere-Hosts zu den ONTAP tools for VMware vSphere hinzu, um die Datenspeicher auf den Hosts zu verwalten und zu schützen.

Schritte

1. Fügen Sie Ihrem VMware vSphere-Cluster einen Host gemäß dem Workflow auf Seite 1 hinzu: "So fügen Sie Ihrem vSphere-Cluster mithilfe des Schnellstart-Workflows einen ESX-Host hinzu"
2. Nach dem Hinzufügen des Hosts gehen Sie zum Hauptmenü der ONTAP -Tools und wählen im Übersichtsfenster **Discover** aus. Warten Sie, bis der Erkennungsprozess abgeschlossen ist. Alternativ können Sie warten, bis die geplante Host-Erkennung abgeschlossen ist.

Ergebnis

Der neue Host wird nun von den ONTAP tools for VMware vSphere erkannt und verwaltet. Sie können nun mit der Verwaltung des Datenspeichers auf dem neuen Host fortfahren.

Verwandte Themen

- "Mounten Sie einen VVols Datastore"auf neuen Hosts.
- "Mounten Sie NFS- und VMFS-Datastore"auf neuen Hosts.

Managen von Datastores

NFS- und VMFS-Datenspeicher in ONTAP tools einbinden

Durch das Mounten eines Datenspeichers können zusätzliche Hosts auf den Speicher zugreifen. Nachdem Sie die Hosts der VMware Umgebung hinzugefügt haben, können Sie den Datastore auf den zusätzlichen Hosts einbinden.

> Wenn Sie einen neuen ESXi-Host hinzufügen, indem Sie "Fügen Sie Ihrem vSphere-Cluster-Workflow einen ESX-Host hinzu" Warten Sie, bis die geplante Host-Erkennung abgeschlossen ist, bevor der Host in den ONTAP -Tools angezeigt wird. Alternativ können Sie die Erkennung manuell über die Übersichtsseite der NetApp ONTAP -Tools starten.

Über diese Aufgabe

- Einige Rechtsklick-Aktionen sind abhängig von der vSphere-Client-Version und dem ausgewählten Datastore-Typ deaktiviert oder nicht verfügbar.
  - Wenn Sie vSphere Client 8.0 oder höher verwenden, sind einige der Optionen mit der rechten Maustaste ausgeblendet.

- Von vSphere 7.0U3 bis vSphere 8.0, obwohl die Optionen angezeigt werden, wird die Aktion deaktiviert.

- vSphere deaktiviert die Option "Mount Datastore", wenn der Host-Cluster mit einheitlichen Konfigurationen geschützt ist.

Schritte

1. Wählen Sie auf der vSphere Client-Startseite **Hosts und Cluster** aus.
2. Wählen Sie im linken Navigationsbereich die Rechenzentren aus, die die Hosts enthalten.
3. Um NFS/VMFS-Datenspeicher auf einem Host oder einem Hostcluster einzubinden, klicken Sie mit der rechten Maustaste und wählen Sie * NetApp ONTAP Tools* > **Datenspeicher einbinden**.
4. Wählen Sie die Datenspeicher aus, die Sie mounten möchten, und wählen Sie **Mount**.

Was kommt als Nächstes?

Sie können den Fortschritt im Fenster „Letzte Aufgabe“ verfolgen.

Verwandtes Thema

"Neue VMware vSphere-Hosts hinzufügen"

NFS- und VMFS-Datenspeicher in ONTAP tools aushängen

Die Aktion „Datenspeicher aushängen“ entfernt einen NFS- oder VMFS-Datenspeicher von ESXi-Hosts. Es ist für Datenspeicher verfügbar, die von ONTAP tools for VMware vSphere erkannt oder verwaltet werden.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Klicken Sie mit der rechten Maustaste auf ein NFS- oder VMFS-Datenspeicherobjekt und wählen Sie **Datenspeicher aushängen**.

   Der vSphere-Client öffnet ein Dialogfeld und listet die ESXi-Hosts auf, die den Datenspeicher einbinden. Wenn der Vorgang auf einem geschützten Datenspeicher ausgeführt wird, wird eine Warnmeldung auf dem Bildschirm angezeigt.

3. Wählen Sie einen oder mehrere ESXi-Hosts aus, um die Bereitstellung des Datastore aufzuheben.

   Sie können den Datastore nicht von allen Hosts abladen. Die Benutzeroberfläche schlägt vor, dass Sie stattdessen den Vorgang zum Löschen von Datenspeichern verwenden.

4. Wählen Sie die Schaltfläche **Unmount**.

   Wenn der Datastore Teil eines geschützten Host-Clusters ist, wird eine Warnmeldung angezeigt.

> Wenn der geschützte Datenspeicher ausgehängt wird, kann die bestehende Schutzeinstellung zu einem teilweisen Schutz führen. Siehe "Geschütztes Host-Cluster ändern" um einen umfassenden Schutz zu ermöglichen.

Was kommt als Nächstes?

Sie können den Fortschritt im Fenster „Letzte Aufgaben“ verfolgen.

Einen vVols-Datenspeicher in ONTAP tools einbinden

Sie können einen VMware Virtual Volumes (VVols)-Datastore auf einen oder mehrere zusätzliche Hosts mounten, um zusätzlichen Hosts den Storage-Zugriff zu ermöglichen. Sie können das Mounten von VVols-Datastores nur über die APIs aufheben.

> Wenn Sie einen neuen ESXi-Host hinzufügen, indem Sie "Fügen Sie Ihrem vSphere-Cluster-Workflow einen ESX-Host hinzu" Warten Sie, bis die geplante Host-Erkennung abgeschlossen ist, bevor der Host in den ONTAP -Tools angezeigt wird. Alternativ können Sie die Erkennung manuell über die Übersichtsseite der NetApp ONTAP -Tools starten.

Schritte

1. Wählen Sie auf der vSphere Client-Startseite **Hosts und Cluster** aus.
2. Wählen Sie im Navigationsbereich das Rechenzentrum aus, das den Datastore enthält.
3. Klicken Sie mit der rechten Maustaste auf den Datastore und wählen Sie **NetApp ONTAP Tools** > **Datastore mounten**.
4. Wählen Sie im Dialogfeld **Datastores auf Hosts mounten** die Hosts aus, auf denen Sie den Datastore mounten möchten, und wählen Sie dann **Mount** aus.

Im Bereich „Letzte Aufgaben“ wird der Fortschritt angezeigt.

Verwandtes Thema

"Neue VMware vSphere-Hosts hinzufügen"

NFS- und VMFS-Datenspeicher in ONTAP tools vergrößern/verkleinern

Durch die Größenänderung eines Datenspeichers können Sie den Speicher für die Dateien Ihrer virtuellen Maschine erhöhen. Sie können die Größe eines Datastores ändern, wenn sich Ihre Infrastrukturanforderungen ändern.

Über diese Aufgabe

Sie können die Größe von NFS- und VMFS-Datenspeichern erhöhen. Ein FlexVol volume in diesen Datenspeichern kann nicht unter seine aktuelle Größe verkleinert werden, aber auf bis zu 120 % anwachsen.

Schritte

1. Wählen Sie auf der vSphere Client-Startseite **Hosts und Cluster** aus.
2. Wählen Sie im Navigationsbereich das Rechenzentrum aus, das den Datastore enthält.
3. Klicken Sie mit der rechten Maustaste auf den NFS- oder VMFS-Datastore und wählen Sie **NetApp ONTAP Tools** > **Datastore skalieren** aus.
4. Geben Sie im Dialogfeld „Größe ändern“ eine neue Größe für den Datenspeicher ein und wählen Sie **OK**.

Erweitern Sie vVols Datenspeicher in ONTAP tools

Wenn Sie in der vCenter-Objektansicht mit der rechten Maustaste auf das Datenspeicherobjekt klicken, werden im Abschnitt „Plug-ins“ die unterstützten Aktionen für ONTAP tools for VMware vSphere angezeigt. Abhängig vom Datenspeichertyp und den aktuellen Benutzerberechtigungen werden bestimmte Aktionen aktiviert.

Das erweitern des VVols-Datastore ist nicht für systembasierte VVols Datastores in ASA r2 anwendbar.

Schritte

1. Wählen Sie auf der vSphere Client-Startseite **Hosts und Cluster** aus.
2. Wählen Sie im Navigationsbereich das Rechenzentrum aus, das den Datastore enthält.
3. Klicken Sie mit der rechten Maustaste auf den Datastore und wählen Sie **NetApp ONTAP Tools** > **Speicher zum Datastore hinzufügen**.
4. Im Fenster „Volumes erstellen oder auswählen“ können Sie entweder neue Volumes erstellen oder aus den vorhandenen Volumes auswählen. Folgen Sie den Anweisungen auf dem Bildschirm, um Ihre Auswahl zu treffen.
5. Überprüfen Sie im Fenster **Summary** die Auswahl und wählen Sie **Expand**. Sie können den Fortschritt im Fenster „Letzte Aufgaben“ verfolgen.

Einen vVols Datenspeicher in ONTAP tools verkleinern

Diese Seite erklärt, wie man Volumes aus einem vVols -Datenspeicher entfernt.

Verwenden Sie die Aktion "Speicher aus Datenspeicher entfernen" für jeden vVols -Datenspeicher, der von ONTAP Tools in vCenter Server verwaltet wird.

Sie können keinen Speicher von einem Volume entfernen, wenn es vVols enthält. Die Option zum Entfernen wird für solche Volumes deaktiviert. Beim Entfernen von Volumes aus dem Datenspeicher haben Sie auch die Möglichkeit, die ausgewählten Volumes aus dem ONTAP Speicher zu löschen.

Der Vorgang zum Verkleinern von vVols Datenspeichern wird für vVols Datenspeicher, die auf ASA R2-Systemen basieren, nicht unterstützt.

Schritte

1. Wählen Sie auf der vSphere Client-Startseite **Hosts und Cluster** aus.
2. Wählen Sie im Navigationsbereich das Rechenzentrum aus, das den Datastore enthält.
3. Klicken Sie mit der rechten Maustaste auf den vVol Datastore und wählen Sie **NetApp ONTAP Tools** > **Speicher aus Datastore entfernen**.
4. Wählen Sie die Volumes aus, die keine vVols haben, und wählen Sie **Entfernen**.

   Die Option zum Auswählen des Volumes, auf dem sich vVols befindet, ist deaktiviert.

5. Aktivieren Sie im Popup-Fenster **Speicher entfernen** das Kontrollkästchen **Volumes aus ONTAP-Cluster löschen**, um die Volumes aus dem Datastore und aus dem ONTAP-Speicher zu löschen, und wählen Sie **Löschen** aus.

Datenspeicher in ONTAP tools löschen

Diese Seite beschreibt, wie man NFS-, VMFS- oder vVols -Datenspeicher mithilfe von ONTAP Tools im vCenter Server löscht.

Wenn Sie einen Datenspeicher löschen, werden je nach Datenspeichertyp die folgenden Aktionen ausgeführt:

- Der vVol-Container ist ausgehängt.
- Wenn die Igroup nicht verwendet wird, wird iqn aus der Igroup entfernt.
- Der vVol-Container wird gelöscht.
- Flex-Volumes verbleiben auf dem Speicherarray.

Sie können den Datenspeicher nur löschen, wenn auf dem ausgewählten Datenspeicher keine vVols vorhanden sind.

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 löschen**.

   Sie können einen von virtuellen Maschinen verwendeten Datenspeicher nicht löschen. Verschieben Sie virtuelle Maschinen vor dem Löschen in einen anderen Datenspeicher. Sie können das Volume nicht löschen, wenn es Teil eines geschützten Hostclusters ist.

   a. Bei einem NFS- oder VMFS-Datenspeicher wird ein Dialogfeld mit der Liste der VMs angezeigt, die den Datenspeicher verwenden.
   b. Wenn einem VMFS-Datenspeicher keine virtuellen Maschinen zugeordnet sind, wird ein Bestätigungsdialogfeld angezeigt. Wenn der Hostclusterschutz aktiviert ist und eine AFD-Beziehung besteht, können Sie sekundäre Speicherelemente bereinigen.
   c. Bei geschützten VMFS-Datenspeichern auf ASA r2-Systemen muss der Schutz vor dem Löschen entfernt werden. Ab ONTAP 9.17.1 und ONTAP tools for VMware vSphere 10.5 können Sie einen geschützten Datenspeicher löschen. Wenn es sich um den einzigen Datenspeicher in der Schutzgruppe handelt, wird dieser vom Hostclusterschutz automatisch entfernt.
   d. Bei vVols -Datenspeichern können Sie den Datenspeicher nur löschen, wenn keine vVols vorhanden sind. Das Dialogfeld **Datenspeicher löschen** enthält eine Option zum Entfernen von Volumes aus dem ONTAP Cluster.
   e. Bei vVols Datenspeichern auf ASA r2-Systemen können Sie die Sicherungsvolumes nicht mit der Option **Datenspeicher löschen** aus ONTAP löschen.
3. Um die Backing Volumes auf dem ONTAP-Speicher zu löschen, wählen Sie **Delete Volumes on ONTAP Cluster** aus.

   Bei VMFS-Datenspeichern auf Unified ONTAP -Speicher, die Teil eines geschützten Hostclusters sind, können Sie das Volume nicht aus dem ONTAP Cluster löschen.

Wenn Sie einen NFS-, VMFS- oder vVols -Datenspeicher löschen, verbleiben die übergeordneten igroups auf dem ONTAP System. Untergeordnete igroups, die keinen LUNs zugeordnet sind, werden automatisch gelöscht. ONTAP -Tools führen eine tägliche Bereinigung durch, um nicht zugeordnete übergeordnete Standard-igroups zu entfernen. Löschen Sie die benutzerdefinierten übergeordneten iGroups manuell in ONTAP. ONTAP Tools können veraltete übergeordnete iGroups nicht wiederverwenden.

ONTAP-Speicheransichten für Datenspeicher in ONTAP tools

ONTAP Tools für VMware vSphere zeigt die ONTAP Storage-Seitenansicht der Datastores und ihrer Volumes auf der Registerkarte „Konfigurieren“.

Schritte

1. Gehen Sie vom vSphere-Client zum Datenspeicher.
2. Wählen Sie im rechten Fensterbereich die Registerkarte **Configure** aus.
3. Wählen Sie * NetApp ONTAP -Tools* > * ONTAP Speicher*. Die Ansicht ändert sich je nach Datenspeichertyp. Siehe die folgende Tabelle:

Datenspeichertyp	Informationen verfügbar
NFS-Datastore	Die Seite **Storage Details** enthält Speicher-Back-Ends, Aggregat- und Volume-Informationen. Die Seite **NFS Details** enthält Daten zum NFS Datastore.
VMFS-Datastores	Die Seite **Storage Details** enthält Details zu Speicher-Backend, Aggregat, Volume und Storage Availability Zone (SAZ). Die Seite **Storage unit Details** enthält Details zur Speichereinheit.
VVols Datastores	Listet alle Bände auf. Sie können Speicher im ONTAP Speicherbereich erweitern oder entfernen. ONTAP Tools unterstützen diese Ansicht nicht für ASA r2-System-basierte vVols Datenspeicher.

Ansicht des Speichers virtueller Maschinen in ONTAP tools

Die Speicheransicht zeigt die Liste der vVols an, die die virtuelle Maschine erstellt.

Diese Ansicht gilt für VMs mit mindestens einer Festplatte aus einem von ONTAP tools for VMware vSphere verwalteten vVols Datenspeicher.

Schritte

1. Gehen Sie vom vSphere-Client zur virtuellen Maschine.
2. Wählen Sie im rechten Fensterbereich die Registerkarte **Monitor** aus.
3. Wählen Sie **NetApp ONTAP Tools** > **Speicher**. Die **Speicher**-Details werden im rechten Fensterbereich angezeigt. Sie können die Liste der VVols anzeigen, die auf der VM vorhanden sind.

   Sie können die Option „Spalten verwalten“ verwenden, um verschiedene Spalten ein- oder auszublenden.

Speicherschwellenwerte in ONTAP tools verwalten

Sie können den Schwellenwert für den Empfang von Benachrichtigungen in vCenter Server festlegen, wenn das Volume und die Gesamtkapazität des Aggregats bestimmte Ebenen erreichen.

Schritte

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. Gehen Sie im linken Bereich der ONTAP -Tools zu **Einstellungen** > **Schwellenwerteinstellungen** > **Bearbeiten**.

4. Geben Sie im Fenster **Schwellenwert bearbeiten** die gewünschten Werte in die Felder **Fast voll** und **Voll** ein und wählen Sie **Speichern**. Sie können die Schwellenwerte auf die empfohlenen Standardwerte zurücksetzen: 80 für Fast voll und 90 für Voll.

Speicher-Backends in ONTAP tools verwalten

Storage-Back-Ends sind Systeme, die die ESXi Hosts zum Speichern von Daten verwenden.

Storage erkennen

Sie können die Erkennung eines Speicher-Backends bei Bedarf ausführen, ohne auf eine geplante Erkennung warten zu müssen, um die Speicherdetails sofort zu aktualisieren. Führen Sie bei MetroCluster -Konfigurationen die Erkennung der ONTAP Tools nach einem Switchover manuell aus.

Führen Sie die folgenden Schritte aus, um die Speicher-Back-Ends zu ermitteln.

Schritte

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. Gehen Sie im linken Bereich der ONTAP -Tools zu **Storage Backends** und wählen Sie ein Storage Backend aus.
4. Wählen Sie das Menü Vertikale Ellipsen und dann **Speicher entdecken**

Sie können den Fortschritt im Fenster „Letzte Aufgaben“ verfolgen.

Speicherbackends ändern

Sie können die Anmeldeinformationen des Speicher-Backends oder den Portnamen ändern. Sie können das Speicher-Backend für globale ONTAP Cluster auch mit dem ONTAP Tools Manager ändern. Wenn das Zertifikat in 30 Tagen oder weniger abläuft, zeigen die ONTAP Tools eine Warnung an. Ändern Sie das Speicher-Backend und laden Sie das neue Zertifikat vom ONTAP Administrator hoch.

Wenn Sie das Speicher-Backend ändern, führen ONTAP tools for VMware vSphere eine Erkennung des Speicher-Backends durch, um die Speicherdetails zu aktualisieren.

Befolgen Sie die Schritte in diesem Abschnitt, um ein Speicher-Back-End zu ändern.

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. Gehen Sie im linken Bereich der ONTAP -Tools zu **Storage Backends** und wählen Sie ein Storage Backend aus.
4. Wählen Sie das vertikale Ellipsenmenü aus und wählen Sie **Ändern**, um die Anmeldeinformationen oder den Anschlussnamen zu ändern. Sie können den Fortschritt im Fenster „Letzte Aufgaben“ verfolgen.

Ändern Sie globale ONTAP Cluster mit dem ONTAP -Tools-Manager wie folgt.

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-Back-Ends aus.
4. Wählen Sie das zu ändernde Speicher-Back-End aus.
5. Wählen Sie das Menü Vertikale Ellipsen und dann **Ändern**.
6. Sie können die Anmeldeinformationen oder den Port ändern. Geben Sie den **Username** und das **Passwort** ein, um das Speicher-Backend zu ändern.

Entfernen Sie die Speicher-Back-Ends

Sie müssen alle an das Speicher-Backend angeschlossenen Datenspeicher entfernen, bevor Sie es entfernen. Führen Sie die folgenden Schritte aus, um ein Speicher-Backend zu entfernen.

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. Gehen Sie im linken Bereich der ONTAP -Tools zu **Storage Backends** und wählen Sie ein Storage Backend aus.
4. Wählen Sie das vertikale Auslassungsmenü und wählen Sie **Entfernen**. Stellen Sie sicher, dass das Speicher-Backend keine Datenspeicher enthält. Sie können den Fortschritt im Bereich „Letzte Aufgaben“ verfolgen.

Sie können den Vorgang zum Entfernen globaler ONTAP-Cluster mit dem ONTAP-Tools-Manager ausführen.

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. Wählen Sie das Storage-Backend aus, das Sie entfernen möchten
5. Wählen Sie das Menü Vertikale Ellipsen und dann **Entfernen**.

Drilldown-Ansicht des Storage-Back-End

Auf der Speicher-Backend-Seite sind alle Speicher-Backends aufgelistet. Sie können Vorgänge zum Erkennen, Ändern und Entfernen von Speicher auf den von Ihnen hinzugefügten Speicher-Backends ausführen, jedoch nicht auf den einzelnen untergeordneten SVMs unter dem Cluster.

Wählen Sie den übergeordneten oder untergeordneten Cluster aus, um die Komponentenübersicht anzuzeigen. Verwenden Sie für den übergeordneten Cluster das Dropdown-Menü „Aktionen“, um Speicher zu ermitteln und das Speicher-Backend zu ändern oder zu entfernen.

Die Übersichtsseite enthält folgende Details:

- Status des Storage-Backends
- Kapazitätsinformationen
- Grundlegende Informationen zur VM
- Zertifikatsdetails wie Zertifikatsstatus und Ablaufdatum.

- Netzwerkinformationen wie IP-Adresse und Port des Netzwerks. Für die untergeordnete SVM sind die Informationen dieselben wie für das übergeordnete Speicher-Backend.
- Erlaubte und eingeschränkte Privileges für das Speicher-Backend. Für die untergeordnete SVM sind die Informationen dieselben wie für das übergeordnete Speicher-Backend. ONTAP -Tools zeigen Berechtigungen nur für die clusterbasierten Speicher-Backends an. Wenn Sie SVM als Speicher-Backend hinzufügen, werden keine Berechtigungsinformationen angezeigt.
- Die Drilldown-Ansicht des ASA R2-Systemclusters enthält keine Registerkarte „Lokale Ebenen“, wenn die disaggregierte Eigenschaft für die SVM oder den Cluster auf „true“ gesetzt ist.
- Bei ASA r2 SVM-Systemen wird das Portlet „Capacity“ nicht angezeigt. Das Kapazitätsportal ist nur erforderlich, wenn die disaggregierte Eigenschaft für die SVM oder den Cluster als „true“ festgelegt ist.
- Für ASA r2 SVM-Systeme wird im Abschnitt grundlegende Informationen der Plattformtyp angezeigt.

Die Registerkarte Schnittstelle enthält detaillierte Informationen zur Schnittstelle.

Auf der Registerkarte „Lokale Ebenen“ finden Sie detaillierte Informationen zur Aggregatliste.

Verwalten von vCenter Server-Instanzen in ONTAP -Tools

VCenter Server-Instanzen sind zentrale Management-Plattformen, mit denen Sie Hosts, Virtual Machines und Storage-Back-Ends steuern können.

Trennen Sie Storage Back-Ends von der vCenter Server-Instanz

Auf der Listingseite des vCenter-Servers wird die zugehörige Anzahl von Speicher-Back-Ends angezeigt. Jede vCenter Server-Instanz hat die Möglichkeit, ein Storage-Back-End zuzuordnen oder die Zuordnung zu aufheben.

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 die erforderliche vCenter Server-Instanz aus.
4. Wählen Sie die vertikalen Ellipsen für den vCenter Server aus, den Sie mit Speicher-Back-Ends verknüpfen oder trennen möchten.
5. Wählen Sie **Speicher-Backend trennen**.

Ändern Sie eine vCenter Server-Instanz

Führen Sie die folgenden Schritte aus, um eine vCenter Server-Instanz zu ändern.

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 die entsprechende vCenter Server-Instanz aus
4. Wählen Sie die vertikalen Ellipsen für den vCenter Server aus, den Sie ändern möchten, und wählen Sie

Ändern.

5. Geben Sie im Fenster **vCenter ändern** den Benutzernamen, das Kennwort und die Portdetails ein.
6. Laden Sie das Zertifikat hoch und wählen Sie **Ändern**.

Entfernen einer vCenter Server-Instanz

Entfernen Sie alle Speicher-Backends vom vCenter Server, bevor Sie ihn entfernen.

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 die entsprechenden vCenter Server-Instanzen aus
4. Wählen Sie die vertikalen Auslassungspunkte neben dem vCenter Server aus, den Sie entfernen möchten, und wählen Sie **Entfernen**.

> Nachdem Sie vCenter Server-Instanzen entfernt haben, werden sie nicht mehr von der Anwendung verwaltet.

Wenn Sie vCenter Server-Instanzen in ONTAP-Tools entfernen, werden die folgenden Aktionen automatisch ausgeführt:

- Die Registrierung des Plug-ins wurde aufgehoben.
- Plug-in-Berechtigungen und Plug-in-Rollen werden entfernt.

vCenter Server-Zertifikat erneuern

ONTAP tools benachrichtigt Sie, wenn das vCenter-Zertifikat bald abläuft oder bereits abgelaufen ist. Nach der Erneuerung des vCenter-Zertifikats laden Sie das neue Zertifikat mithilfe der folgenden Schritte in die ONTAP Tools hoch:

1. Melden Sie sich bei der Remote-Diagnose-Shell der ONTAP Tools an.
2. Das erneuerte vCenter-Zertifikat erhalten Sie über die Diagnoseshell:

```
echo | openssl s_client connect <vcenter>:443 2>&1 | sed -n '/-BEGIN
CERTIFICATE/,/END CERTIFICATE/p'
```

3. Stellen Sie sicher, dass das Zertifikat im Base64-ASCII-Format vorliegt und die Anfangs- und Endzeile enthält, zum Beispiel:

```
---{}BEGIN CERTIFICATE{}---
MIIFUzCCA7ugAwIBAgIJANOgLapcl5oSMA0GCSqGSIb3DQEBCwUAMIGJMQwwCgYD
VQQDDAN2YzExFDASBgoJkiaJk/IsZAEZFgRkZW1vMRUwEwYKCZImiZPyLGQBGRYF
bG9jYWwxCzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRwwGgYDVQQK
DBN2YzEuZGVtby5uZXRhcHAuY29tMQwwCgYDVQQLDANMT0QwHhcNMjQwNDA1MTgw
NTE4WhcNMjYwNDA1MTgwNTE4WjBzMRwwGgYDVQQDDBN2YzEuZGVtby5uZXRhcHAu
Y29tMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTESMBAGA1UEBwwJ
UGFsbyBBbHRvMQ8wDQYDVQQKDAZOZXRBcHAxDDAKBgNVBAsMA0xPRDCCAaIwDQYJ
KoZIhvcNAQEBBQADggGPADCCAYoCggGBALU8OCWMtA2gvIC/OTw/7xucvPVuM+b8
DhzvNpQ2phjfr6ctEhbntPpqPdu+t2CKK7l0mzg3D9cJ/rvMvdDDXr0tgaD1oi2u
ZDW0CaF0QhLOpNfRXMoogBZ66csEhViAy3CHTcOse770mA/PyoHgrCPZngVlZIiQ
TIWpdQMbEEzFIkrLfC70UW2MzfublrsH7Dn/kOu/iCSlVJWixKf7SmZtVQ5ZxBTD
UlJSiqoX1eRXGyunArEvrIpOY9kkKXUElm3hGnk/ZmiuBJ+HqUYqYW+H+7vE3lKa
6NEqDX+tZotxTx2bXMjeiIWU30ZbshgeXlIG9qc49clBoC9iGjavhctOcaXg/W3h
dLKK5ds3rpRERgMg6VMkrfiqAJuiq+b3sTvXMAul/3hL7hz5QABAE/hP4ZvIHV02
WWDQRLiuVFAcDAyvCrO9Irx0Gk1RyRShKYakdWxZ3hhMdLuGq0yvRXqo1Ib94zwO
JfBJHjFToA/GqwromZgiTzJkKq5xbN8MFwIDAQABo4HSMIHPMAsGA1UdDwQEAwIF
4DA7BgNVHREENDAygRVlbWFpbEBkZW1vLm5ldGFwcC5jb22HBMCoAB+CE3ZjMS5k
ZW1vLm5ldGFwcC5jb20wHQYDVR0OBBYEFJ0V0zY+JRpFrEt31ovAY4BLFXmAMB8G
A1UdIwQYMBaAFENf6fRxWF3OJQNTPIdUpK6kjA78MEMGCCsGAQUFBwEBBDcwNTAz
BggrBgEFBQcwAoYnaHR0cHM6Ly92YzEuZGVtby5uZXRhcHAuY29tL2FmZC92ZWNz
L2NhMA0GCSqGSIb3DQEBCwUAA4IBgQBaDfk7GBM4vmhzYCqGrr6KB+h3qeTJ+Y0Y
5nIPRP1HucawDQ8QTay605ddJ8gFGoxkOQDn9tdXWXGjnTRFOT8R+Hw/nUfVSiDP
sYienb16copzUNwtqh+m9Ifow74Gf+ulRzEC0EAVO1X/nTEYH6NKM6Wy7y7F8g5J
lrpM3JY90ZChMqHO3Av/88rbErfQ/gU1brJ3u9Gks4e20Z7Ff312ZKhWRuJDlN2Z
0tc/gp90N9GxaVvELovq/pdjaZ8xiXCxa6piicrJd9WnqMH1gmxP2PIBDxMDBWBG
gwsfs5H7VG9MJYks6lViNsGclo0EwEdF0MfoB3JtsWpPWq6+jBua0Jm7/aFCU+Ht
mykr0gaV7muegoiBQuDma4EkAI31D7ZlUgJQaw157NTk4RW3TFcbtViBHJkM54Hr
iVm0cl+2BZNi/QTMh/MkWV2dYXJ3NuNlqqfzFY+bUfkzkR4SneMk0HX3joNNYDJv
siO7bL+k/Pxql27NVIhuCoVJAlcI7ak=
---{}END CERTIFICATE{}---
```

4. Kopieren Sie die Ausgabe und speichern Sie sie als Textdatei mit dem Namen `.pem` Erweiterung auf Ihrem Desktop.
5. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
6. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
7. Wählen Sie in der Seitenleiste die entsprechende vCenter Server-Instanz aus
8. Wählen Sie die vertikalen Ellipsen für den vCenter Server aus, den Sie ändern möchten, und wählen Sie **Ändern**.
9. Geben Sie im Fenster **vCenter ändern** den Benutzernamen, das Kennwort und die Portdetails ein.
10. Laden Sie das Zertifikat hoch und wählen Sie **Ändern**.

Verwandte Informationen

"Konfigurieren Sie den Zugriff auf die Remote-Diagnose"

ONTAP tools-Zertifikate verwalten

Für ONTAP -Tools und den VASA-Provider wird während der Bereitstellung standardmäßig ein selbstsigniertes Zertifikat generiert. Über die ONTAP Tools Manager-Oberfläche können Sie dieses Zertifikat erneuern oder durch ein benutzerdefiniertes CA-Zertifikat ersetzen. Bei Multi-vCenter-Bereitstellungen ist die Verwendung benutzerdefinierter CA-Zertifikate erforderlich.

Bevor Sie beginnen

Folgendes sollten Sie vor Beginn bereithalten:

- Der Domänenname wurde der virtuellen IP-Adresse zugeordnet.
- Erfolgreicher nslookup des Domainnamens, was bestätigt, dass er zur korrekten IP-Adresse aufgelöst wird.
- Zertifikate, die mit dem Domänennamen und der IP-Adresse der ONTAP -Tools erstellt wurden.

Eine IP-Adresse für ONTAP-Tools sollte einem vollständig qualifizierten Domänennamen (FQDN) zugeordnet werden. Zertifikate sollten denselben FQDN enthalten, der der IP-Adresse des ONTAP-Tools in alternativen Namen des Subjekts oder des Subjekts zugeordnet ist.

Sie können nicht von einem mit einer Zertifizierungsstelle signierten zu einem selbstsignierten Zertifikat wechseln.

Upgrade ONTAP Tools Zertifikat

Auf der Registerkarte „ONTAP Tools“ werden Details wie der Zertifikatstyp (selbstsigniert/CA-signiert) und der Domänenname angezeigt. Während der Bereitstellung wird standardmäßig ein selbstsigniertes Zertifikat generiert. Sie können das Zertifikat erneuern oder das Zertifikat auf CA aktualisieren.

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 **Zertifikate** > **ONTAP Tools** > **erneuern**, um die Zertifikate zu erneuern.

   Sie können das Zertifikat erneuern, wenn es abgelaufen ist oder sich seinem Ablaufdatum nähert. Die Option „erneuern“ ist verfügbar, wenn der Zertifikatstyp CA-signiert ist. Geben Sie im Popup-Fenster das Serverzertifikat, den privaten Schlüssel, die Stammzertifizierungsstelle und die Details zum Zwischenzertifikat an.

   Das System ist offline, bis das Zertifikat erneuert wird, und Sie werden von der Benutzeroberfläche des ONTAP Tools Managers abgemeldet.

4. Um das selbstsignierte Zertifikat auf ein benutzerdefiniertes CA-Zertifikat zu aktualisieren, wählen Sie **Zertifikate** > **ONTAP-Tools** > **Upgrade auf CA**.
   a. Laden Sie im Popup-Fenster das Serverzertifikat, den privaten Schlüssel des Serverzertifikats, das Stammzertifizierungsstellenzertifikat und die Zwischenzertifikatdateien hoch.
   b. Geben Sie den FQDN der Load Balancer IP-Adresse ein, für die Sie dieses Zertifikat generiert haben, und aktualisieren Sie das Zertifikat.

      Das System ist bis zum Abschluss des Upgrades offline und Sie werden von der Oberfläche des ONTAP Tools Managers abgemeldet.

Upgrade des VASA Provider-Zertifikats

ONTAP Tools für VMware vSphere werden mit einem selbstsignierten Zertifikat für VASA Provider implementiert. Dadurch kann nur eine vCenter Server-Instanz für VVols-Datastores gemanagt werden. Wenn Sie mehrere vCenter Server-Instanzen managen und VVols-Funktionen darauf aktivieren möchten, müssen Sie das selbstsignierte Zertifikat in ein benutzerdefiniertes CA-Zertifikat ändern.

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 **Certificates** > **VASA Provider** oder **ONTAP Tools** > **Renew**, um die Zertifikate zu erneuern.
4. Wählen Sie **Certificates** > **VASA Provider** oder **ONTAP Tools** > **Upgrade auf CA**, um das selbstsignierte Zertifikat auf ein benutzerdefiniertes CA-Zertifikat zu aktualisieren.
   a. Laden Sie im Popup-Fenster das Serverzertifikat, den privaten Schlüssel des Serverzertifikats, das Stammzertifizierungsstellenzertifikat und die Zwischenzertifikatdateien hoch.

b. Geben Sie den FQDN der Load Balancer IP-Adresse ein, für die Sie dieses Zertifikat generiert haben, und aktualisieren Sie das Zertifikat.

Das System ist bis zum Abschluss des Upgrades offline und Sie werden von der Oberfläche des ONTAP Tools Managers abgemeldet.

Zugriff auf ONTAP Tools für die VMware vSphere Wartungskonsole

Erfahren Sie mehr über die ONTAP tools maintenance console

Die Wartungskonsole für ONTAP tools for VMware vSphere ermöglicht die Verwaltung von Anwendungs-, System- und Netzwerkeinstellungen. Sie können Administrator- und Wartungspasswörter aktualisieren, Support-Bundles generieren, Protokollierungsstufen konfigurieren, TLS-Einstellungen verwalten und die Ferndiagnose aktivieren.

Nach der Bereitstellung der ONTAP tools for VMware vSphere und falls die Wartungskonsole nicht erreichbar ist, installieren Sie die VMware-Tools vom vCenter Server aus. Melden Sie sich mit dem `maint` Benutzername und das während der Bereitstellung festgelegte Passwort. Verwenden Sie **nano**, um Dateien in der Wartungskonsole oder der Root-Login-Konsole zu bearbeiten.

Sie sollten ein Kennwort für das festlegen `diag` Benutzer, während die Ferndiagnose aktiviert wird.

Sie sollten die Registerkarte **Zusammenfassung** Ihrer bereitgestellten ONTAP-Tools für VMware vSphere verwenden, um auf die Wartungskonsole zuzugreifen. Wenn Sie auswählen  , wird die Wartungskonsole gestartet.

Konsolenmenü	Optionen
Anwendungskonfiguration	1. Zeigt eine Zusammenfassung des Serverstatus an 2. Ändern Sie die LOG-Ebene für ONTAP -Tools -Dienste 3. Zertifikatsvalidierungsflag ändern
Systemkonfiguration	1. Starten Sie die virtuelle Maschine neu 2. Virtuelle Maschine herunterfahren 3. Ändern Sie das Benutzerpasswort „Wartung“ 4. Zeitzone ändern 5. Erhöhen der Größe der Jail-Festplatte (/jail) 6. Upgrade 7. Installation der VMware Tools

Netzwerkkonfiguration	1. Zeigt die Einstellungen für die IP-Adresse an 2. Zeigen Sie die Einstellungen für die Suche nach Domain-Namen an 3. Ändern Sie die Einstellungen für die DNS-Suche 4. Statische Routen anzeigen 5. Ändern Sie statische Routen 6. Änderungen speichern 7. Ping an einen Host 8. Standardeinstellungen wiederherstellen
Support und Diagnose	1. Zugriff auf die Diagnoseschale 2. Remote-Diagnosezugriff aktivieren 3. Geben Sie die vCenter-Anmeldeinformationen für das Backup an 4. Sichern Sie sich

Konfigurieren Sie den Ferndiagnosezugriff für ONTAP tools

Sie können ONTAP Tools für VMware vSphere konfigurieren, um den SSH-Zugriff für den Diagnosebenutzer zu aktivieren.

Bevor Sie beginnen

Aktivieren Sie die VASA Provider-Erweiterung für Ihre vCenter Server-Instanz.

Über diese Aufgabe

Die Verwendung von SSH für den Zugriff auf das Diagnose-Benutzerkonto weist folgende Einschränkungen auf:

- Sie dürfen pro SSH-Aktivierung nur ein Anmeldekonto verwenden.
- SSH-Zugriff auf das Diagnose-Benutzerkonto ist deaktiviert, wenn eines der folgenden Ereignisse eintritt:
  - Die Zeit läuft ab.

    Die Anmeldesitzung läuft am nächsten Tag um Mitternacht ab.
  - Sie melden sich erneut als Diagnose-Benutzer mit SSH an.

Schritte

1. Öffnen Sie über den vCenter Server eine Konsole für VASA Provider.
2. Melden Sie sich als Wartungbenutzer an.
3. Geben Sie ein `4`, um **Support und Diagnose** auszuwählen.
4. Eingeben `2` , um **Zugriff auf Remotediagnose aktivieren** auszuwählen.
5. Eingabe `y` Im Dialogfeld „Bestätigung“ können Sie den Remote-Diagnosezugriff aktivieren.
6. Geben Sie ein Kennwort für den Remote-Diagnosezugriff ein.

Starten Sie SSH auf anderen ONTAP tools-Knoten

Sie müssen SSH auf anderen Nodes vor dem Upgrade starten.

Bevor Sie beginnen

Aktivieren Sie die VASA Provider-Erweiterung für Ihre vCenter Server-Instanz.

Über diese Aufgabe

Wiederholen Sie diesen Vorgang auf jedem Knoten vor dem Upgrade.

Schritte

1. Öffnen Sie über den vCenter Server eine Konsole für VASA Provider.
2. Melden Sie sich als Wartungbenutzer an.
3. Eingabe `4` Wählen Sie Support und Diagnose aus.
4. Eingabe `1` Wählen Sie Access Diagnostic Shell aus.
5. Eingabe `y` Fortfahren.
6. Führen Sie den Befehl *sudo systemctl restart ssh* aus.

Aktualisieren Sie die vCenter Server-Anmeldeinformationen in ONTAP tools

Sie können die Anmeldeinformationen der vCenter Server-Instanz über die Wartungskonsole aktualisieren.

Bevor Sie beginnen

Sie müssen über Anmeldedaten für Wartungsbenutzer verfügen.

Über diese Aufgabe

Wenn Sie die Anmeldeinformationen für den vCenter Server nach der Bereitstellung geändert haben, aktualisieren Sie diese mit diesem Verfahren.

Schritte

1. Öffnen Sie über den vCenter Server eine Konsole für VASA Provider.
2. Melden Sie sich als Wartungbenutzer an.
3. Geben Sie ein `2` , um das Menü Systemkonfiguration auszuwählen.
4. Eingeben `8` um die vCenter-Anmeldeinformationen zu ändern.

Ändern Sie das Zertifikatvalidierungsflag in ONTAP tools

Standardmäßig ist das Flag zur Zertifikatsvalidierung aktiviert (auf „true“ gesetzt). Sie können das Zertifikatvalidierungsflag des ONTAP -Speicher-Backends auf „false“ setzen, wenn Sie SAN-Zertifikatsprüfungen umgehen müssen. Diese Einstellung ist nicht auf vCenter Server-Zertifikate anwendbar.

Bevor Sie beginnen

Sie müssen über Anmeldedaten für Wartungsbenutzer verfügen.

Schritte

1. Öffnen Sie im vCenter Server eine Konsole für ONTAP Tools.
2. Melden Sie sich als Wartungbenutzer an.
3. Eingeben `1` um das Menü **Anwendungskonfiguration** auszuwählen.
4. Eingeben `3` um das Zertifikatvalidierungsflag zu ändern.

   Die Wartungskonsole zeigt den Status des Zertifikatvalidierungsflags an und fordert Sie auf, ihn zu ändern.

5. Geben Sie „y“ ein, um die Flagge umzuschalten, oder „n“, um abzubrechen.

Wenn Sie das Flag für die Zertifikatsvalidierung aktivieren (auf „true“ setzen), überprüft ONTAP Tools, ob alle Speicher-Backends Zertifikate mit einem Subject Alternative Name (SAN) verwenden. Wenn ein Backend ein Zertifikat ohne SAN verwendet, kann die Zertifikatsvalidierung nicht aktiviert werden. Bevor Sie dieses Flag aktivieren, vergewissern Sie sich, dass alle Speichersysteme SAN-basierte Zertifikate verwenden. Wenn Sie das Flag für die Zertifikatsvalidierung deaktivieren (auf „false“ setzen), umgeht ONTAP tools die Zertifikatsvalidierung für alle konfigurierten Speicher-Backends.

Berichte zu ONTAP Tools

ONTAP Tools für das VMware vSphere Plug-in bieten Berichte für Virtual Machines und Datastores. Wenn Sie im Abschnitt „Verknüpfungen“ des vCenter-Clients das Symbol „NetApp ONTAP-Tools für VMware vSphere“ auswählen, wechselt die Benutzeroberfläche zur Seite „Übersicht“. Wählen Sie die Registerkarte Berichte aus, um die virtuelle Maschine und den Bericht Datastores anzuzeigen.

Der Bericht „Virtuelle Maschinen“ zeigt die Liste der erkannten virtuellen Maschinen (sollte mindestens eine Festplatte aus ONTAP Speicher-basierten Datenspeichern haben) mit Leistungsmetriken. Wenn Sie den VM-Datensatz erweitern, zeigt die Benutzeroberfläche alle datenspeicherbezogenen Informationen zum Datenträger an.

Der Datenspeicherbericht listet die von ONTAP tools for VMware vSphere erkannten oder identifizierten Datenspeicher auf, die ONTAP -Speicher verwenden, und gibt Leistungskennzahlen an.

Mit der Option Spalten verwalten können Sie verschiedene Spalten ein- oder ausblenden.

Management von Virtual Machines

Überlegungen zur Migration und zum Klonen virtueller Maschinen für ONTAP tools

Bei der Migration bestehender virtueller Maschinen in Ihrem Rechenzentrum sollten Sie einige Überlegungen beachten.

Migrieren Sie geschützte Virtual Machines

Sie können die geschützten virtuellen Maschinen migrieren in:

- Derselbe VVols-Datastore auf einem anderen ESXi-Host
- Unterschiedliche kompatible VVols-Datastores auf demselben ESXi-Host
- Unterschiedliche kompatible VVols-Datastores auf einem anderen ESXi-Host

Wenn Sie die virtuelle Maschine auf ein anderes FlexVol volume migrieren, aktualisiert das System die Metadatendatei für dieses Volume mit den Informationen zur virtuellen Maschine. Wenn eine virtuelle Maschine auf einen anderen ESXi-Host, aber denselben Speicher migriert wird, wird die zugrunde liegende Metadatendatei des FlexVol volume nicht geändert.

Klonen geschützter Virtual Machines

Sie können geschützte Virtual Machines folgendermaßen klonen:

- Derselbe Container desselben FlexVol Volumes mithilfe der Replizierungsgruppe

  Die Metadatendatei dieses FlexVol Volume wird mit den geklonten Virtual Machines aktualisiert.

- Derselbe Container eines anderen FlexVol Volumes unter Verwendung der Replizierungsgruppe

  Das FlexVol Volume, auf dem die geklonte Virtual Machine gespeichert wird, wird die Metadatendatei mit den Details der geklonten Virtual Machine aktualisiert.

- Unterschiedlicher Container oder VVols Datastore

  Dem FlexVol Volume, auf dem die geklonte Virtual Machine gespeichert wird, werden die Metadatendatei die Details der Virtual Machine aktualisiert.

VMware unterstützt derzeit keine virtuellen Maschinen, die in eine VM-Vorlage geklont wurden.

Der Klon einer geschützten Virtual Machine wird unterstützt.

Weitere Informationen finden Sie unter "Erstellen einer virtuellen Maschine zum Klonen".

Snapshots Von Virtual Machines

Derzeit werden nur Snapshots virtueller Maschinen ohne Speicher unterstützt. Wenn auf einer virtuellen Maschine Snapshot mit Arbeitsspeicher vorhanden ist, wird die virtuelle Maschine nicht als Schutz betrachtet.

Sie können auch keine ungeschützten virtuellen Maschinen schützen, die über einen Speicher-Snapshot verfügen. Bei dieser Version müssen Sie den Speicher-Snapshot löschen, bevor Sie den Schutz für die virtuelle Maschine aktivieren.

Bei einer Windows-VM mit dem Speichertyp ASA r2 ist ein Snapshot der virtuellen Maschine schreibgeschützt. Beim Einschalten der VM erstellt der VASA Provider eine LUN aus dem schreibgeschützten Snapshot und aktiviert IOPS. Wenn Sie die VM ausschalten, löscht der VASA Provider die LUN und deaktiviert IOPS.

Migrieren Sie virtuelle Maschinen zu vVols-Datenspeichern in ONTAP tools

Sie können Virtual Machines von NFS- und VMFS-Datastores auf Virtual Volumes (VVols) Datastores migrieren, um die Vorteile des richtlinienbasierten VM-Managements und anderer VVols Funktionen zu nutzen. VVols Datastores ermöglichen es, steigende Workload-Anforderungen zu erfüllen.

Bevor Sie beginnen

Vergewissern Sie sich, dass VASA Provider auf keiner der virtuellen Maschinen ausgeführt wird, die Sie migrieren möchten. Wenn Sie eine Virtual Machine migrieren, auf der VASA Provider ausgeführt wird, zu einem VVols Datastore, können Sie keine Managementvorgänge ausführen. Das gilt auch das Hochfahren der

Virtual Machines auf VVols Datastores.

Über diese Aufgabe

Bei der Migration von einem NFS- und VMFS-Datastore zu einem VVols-Datastore verwendet vCenter Server vStorage APIs for Array Integration (VAAI), wenn Daten aus VMFS-Datastores, nicht jedoch aus einer NFS VMDK-Datei verschoben werden. VAAI-Entlastung verringert normalerweise die Last des Hosts.

Schritte

1. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, die Sie migrieren möchten, und wählen Sie **Migrate**.
2. Wählen Sie **nur Speicher ändern** und dann **Weiter**.
3. Wählen Sie ein virtuelles Datenträgerformat, eine VM-Speicherrichtlinie und einen vVol-Datenspeicher aus, der den Funktionen des Datenspeichers entspricht, den Sie migrieren.
4. Überprüfen Sie die Einstellungen und wählen Sie **Fertig stellen**.

Bereinigen Sie die VASA-Konfigurationen in ONTAP tools

Um den VASA-Bereinigungsprozess abzuschließen, befolgen Sie diese Schritte.

Es wird empfohlen, vor Beginn der VASA-Bereinigung alle vVols -Datenspeicher zu entfernen.

Schritte

1. Heben Sie die Registrierung des Plug-ins auf, indem Sie zu https://OTV_IP:8143/Register.html gehen
2. Vergewissern Sie sich, dass das Plug-in nicht mehr auf dem vCenter Server verfügbar ist.
3. Fahren Sie die ONTAP Tools für VMware vSphere VM herunter.
4. Löschen Sie ONTAP Tools für VMware vSphere VM.

Eine Datenfestplatte an eine VM in ONTAP tools anhängen oder trennen

Befolgen Sie diese Schritte, um Datenträger an virtuelle Maschinen in vSphere anzuhängen oder zu trennen und deren Speicherressourcen zu verwalten.

Verbinden Sie eine Datenfestplatte mit einer virtuellen Maschine

Schließen Sie eine Datenfestplatte an eine virtuelle Maschine an, um mehr Speicherplatz hinzuzufügen.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine im Inventar und wählen Sie **Einstellungen bearbeiten**.
3. Wählen Sie auf der Registerkarte **Virtual Hardware existing Hard Disk** aus.
4. Wählen Sie die virtuelle Maschine aus, auf der das Laufwerk vorhanden ist.
5. Wählen Sie die Festplatte aus, die Sie anschließen möchten, und klicken Sie auf die Schaltfläche **OK**.

Ergebnis

Die Festplatte wird in der Liste Virtuelle Hardwaregeräte angezeigt.

Trennen Sie ein Datenlaufwerk von der virtuellen Maschine

Trennen Sie eine Datenfestplatte von einer virtuellen Maschine, wenn Sie sie nicht mehr benötigen. Die Festplatte wird nicht gelöscht; sie verbleibt im ONTAP -Speichersystem.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine im Inventar und wählen Sie **Einstellungen bearbeiten**.
3. Bewegen Sie den Mauszeiger über die Scheibe und wählen Sie **Entfernen**.

> Der Datenträger wird aus der virtuellen Maschine entfernt. Wenn andere virtuelle Maschinen den Datenträger gemeinsam nutzen, werden die Datenträgerdateien nicht gelöscht.

Verwandte Informationen

"Fügen Sie einer virtuellen Maschine eine neue Festplatte hinzu"

"Fügen Sie einer virtuellen Maschine eine vorhandene Festplatte hinzu"

Speichersysteme und Hosts in ONTAP tools entdecken

Wenn ONTAP tools for VMware vSphere zum ersten Mal im vSphere Client gestartet wird, werden automatisch ESXi-Hosts, die zugehörigen LUNs und NFS-Exporte sowie die NetApp -Speichersysteme, denen diese Ressourcen gehören, erkannt.

Bevor Sie beginnen

- Stellen Sie sicher, dass alle ESXi-Hosts eingeschaltet und verbunden sind.
- Stellen Sie sicher, dass alle zu erkennenden Storage Virtual Machines (SVMs) ausgeführt werden und dass auf jedem Clusterknoten mindestens eine Daten-LIF für das verwendete Speicherprotokoll (NFS oder iSCSI) konfiguriert ist.

Über diese Aufgabe

Sie können neue Speichersysteme entdecken oder bestehende aktualisieren, um die neuesten Kapazitäts- und Konfigurationsdetails zu erhalten. Sie können die ONTAP tools for VMware vSphere Anmeldeinformationen für den Zugriff auf das Speichersystem ändern.

Bei der Erkennung der Speichersysteme erfasst ONTAP-Tools für VMware vSphere Informationen von den ESXi-Hosts, die von der vCenter Server-Instanz gemanagt werden.

Schritte

1. Wählen Sie auf der vSphere Client-Startseite **Hosts und Cluster** aus.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Rechenzentrum und wählen Sie * NetApp ONTAP -Tools* > **Hostdaten aktualisieren**.

   Bestätigen Sie im Dialogfeld **Bestätigen** Ihre Auswahl.

3. Wählen Sie die ermittelten Speicher-Controller aus, die den Status haben `Authentication Failure`, und wählen Sie **actions** > **Modify** aus.
4. Geben Sie die erforderlichen Informationen in das Dialogfeld * Speichersystem ändern* ein.

5. Wiederholen Sie die Schritte 4 und 5 für alle Speicher-Controller mit `Authentication Failure` Status:

Führen Sie nach Abschluss des Erkennungsvorgangs die folgenden Schritte aus:

- Verwenden Sie ONTAP-Tools für VMware vSphere, um ESXi-Hosteinstellungen für Hosts zu konfigurieren, die das Warnsymbol in der Spalte für die Adaptereinstellungen, die Spalte für die MPIO-Einstellungen oder die Spalte für NFS-Einstellungen anzeigen.
- Geben Sie die Anmeldeinformationen des Speichersystems an.

Ändern Sie ESXi Hosteinstellungen mithilfe von ONTAP Tools

Nutzen Sie das ONTAP -Tools-Dashboard in VMware vSphere, um Konfigurationsprobleme zu identifizieren, ESXi-Hosts auszuwählen, die von NetApp empfohlenen Einstellungen zu überprüfen und diese anzuwenden.

Bevor Sie beginnen

Das ESXi-Hostsystem-Portlet zeigt Probleme mit den ESXi-Hosteinstellungen an. Wählen Sie ein Problem aus, um den Hostnamen oder die IP-Adresse anzuzeigen.

Schritte

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. Gehen Sie in der Übersicht (Dashboard) des ONTAP Tools for VMware vSphere Plug-ins zum Portlet **ESXi Host Compliance**.
4. Wählen Sie den Link **Empfohlene Einstellungen anwenden**.
5. Im Fenster **Empfohlene Hosteinstellungen anwenden** wählen Sie die Hosts aus, für die Sie die von NetApp empfohlenen Hosteinstellungen verwenden möchten, und klicken Sie auf **Weiter**.

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

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

Verwandte Informationen

"Konfigurieren Sie ESXi-Hosteinstellungen"

Passwörter verwalten

Ändern Sie das Kennwort des ONTAP Tools Managers

Sie können das Administratorkennwort mit dem ONTAP Tools Manager ändern.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`

2. Melden Sie sich mit Ihren ONTAP tools for VMware vSphere Administratoranmeldeinformationen an.
3. Wählen Sie das Symbol **Administrator** in der oberen rechten Ecke des Bildschirms und wählen Sie **Passwort ändern**.
4. Geben Sie im Popup-Fenster zum Ändern des Passworts das alte und das neue Passwort ein. Auf dem Bildschirm der Benutzeroberfläche werden die Passwortanforderungen angezeigt.
5. Wählen Sie **Ändern**, um die Änderungen anzuwenden.

Kennwort des ONTAP Tools Managers zurücksetzen

Falls Sie das Passwort des ONTAP Tools Managers vergessen haben, können Sie den Administratorzugriff wiederherstellen, indem Sie ein Reset-Token verwenden, das von der ONTAP tools for VMware vSphere Wartungskonsole generiert wurde.

Schritte

1. Öffnen Sie einen Webbrowser und navigieren Sie zu `https://<ONTAPtoolsIP>:8443/virtualization/ui/` um auf den ONTAP Tools Manager zuzugreifen.
2. Wählen Sie auf der Anmeldeseite die Option **Passwort zurücksetzen**.
3. Generieren Sie ein Token zum Zurücksetzen des Kennworts mithilfe der ONTAP tools for VMware vSphere Wartungskonsole:
   a. Melden Sie sich beim vCenter Server an und öffnen Sie die Wartungskonsole.
   b. Eingeben `2` Um die **Systemkonfiguration** auszuwählen, wählen Sie diese bitte aus.
   c. Eingeben `3` **Passwort des Wartungsbenutzers ändern**.
4. Geben Sie im Dialogfeld zum Zurücksetzen des Passworts das Reset-Token, den Benutzernamen und das neue Passwort ein.
5. Wählen Sie **Zurücksetzen**, um die Anmeldeinformationen zu aktualisieren.
6. Melden Sie sich mit dem neuen Passwort beim ONTAP Tools Manager an.

Anwendungsbenutzerpasswort in ONTAP tools zurücksetzen

Führen Sie diese Schritte aus, um das für die SRA- und VASA-Provider-Registrierung bei vCenter Server erforderliche Anwendungsbenutzerkennwort mithilfe der ONTAP tools for VMware vSphere zurückzusetzen.

Schritte

1. Öffnen Sie einen Webbrowser und navigieren Sie zu: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen an, die während der Bereitstellung der ONTAP -Tools konfiguriert wurden.
3. Wählen Sie in der Seitenleiste **Einstellungen** aus.
4. Auf der Seite **VASA/SRA-Zugangsdaten** wählen Sie **Passwort zurücksetzen**.
5. Geben Sie das neue Passwort ein und bestätigen Sie es.
6. Wählen Sie **Zurücksetzen**, um das neue Passwort anzuwenden.

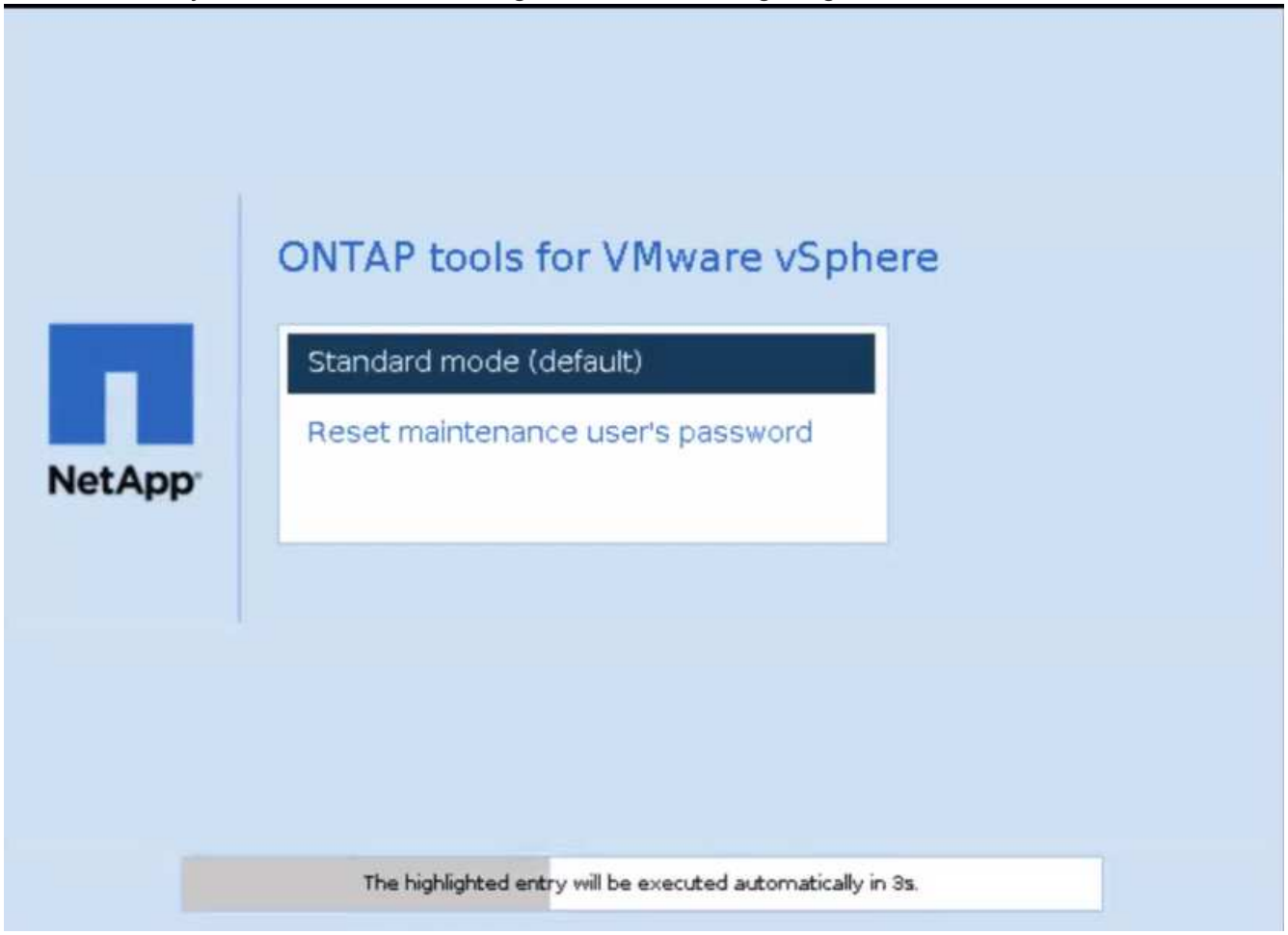
Passwort der ONTAP tools for VMware vSphere Wartungskonsole zurücksetzen

Während des Neustartvorgangs des Gastbetriebssystems wird im GRUB-Menü eine Option zum Zurücksetzen des Benutzerpassworts der Wartungskonsole angezeigt. Mit dieser Option können Sie das Benutzerkennwort der Wartungskonsole auf der VM aktualisieren. Nach dem Zurücksetzen des Passworts wird die VM neu gestartet, um das neue Passwort festzulegen. Im HA-Bereitstellungsszenario wird das Kennwort nach dem Neustart der VM automatisch auf den beiden anderen VMs aktualisiert.

Für ONTAP tools for VMware vSphere HA-Bereitstellung sollten Sie das Benutzerkennwort der Wartungskonsole auf dem Verwaltungsknoten der ONTAP Tools (Knoten1) ändern.

Schritte

1. Melden Sie sich bei Ihrem vCenter-Server an
2. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **Power** > **Gast-OS neu starten** Während des Systemneustarts wird der folgende Bildschirm angezeigt:



   Sie haben 5 Sekunden Zeit, um Ihre Option auszuwählen. Drücken Sie eine beliebige Taste, um den Fortschritt zu stoppen und das GRUB-Menü einzufrieren.

3. Wählen Sie die Option **Passwort des Wartungsbenutzers zurücksetzen**. Die Wartungskonsole wird geöffnet.
4. Geben Sie in der Konsole das neue Passwort ein und bestätigen Sie es. Sie haben drei Versuche. Das

System startet neu, nachdem Sie das neue Passwort erfolgreich eingegeben haben.

5. Drücken Sie die **Eingabetaste**, um fortzufahren. Das System aktualisiert das Passwort auf der VM.

> Das gleiche GRUB-Menü wird auch beim Einschalten der VM angezeigt. Die Option zum Zurücksetzen des Passworts sollten Sie jedoch nur in Verbindung mit der Option **Gastbetriebssystem neu starten** verwenden.

Verwalten Sie den Schutz des Host-Clusters

Ändern eines geschützten Hostclusters in ONTAP tools

Sie können die Schutzeinstellungen für einen Hostcluster in einem einzigen Workflow ändern. Die folgenden Änderungen werden unterstützt:

- Fügen Sie dem geschützten Cluster neue Datastores oder Hosts hinzu.
- Fügen Sie den Sicherungseinstellungen neue SnapMirror-Beziehungen hinzu.
- Löschen Sie vorhandene SnapMirror-Beziehungen aus den Sicherungseinstellungen.
- Ändern Sie eine vorhandene SnapMirror-Beziehung.

> Sie müssen eine Speichererkennung durchführen, nachdem Sie den Schutz für einen Hostcluster erstellt, bearbeitet oder gelöscht haben, um die Änderungen widerzuspiegeln. Wenn Sie die Speichererkennung nicht durchführen, werden die Änderungen nach dem Auslösen der regelmäßigen Speichererkennung angezeigt.

Überwachen Sie den Schutz des Host-Clusters

Überwachen Sie den Schutzstatus, die SnapMirror -Beziehungen, die Datenspeicher und den SnapMirror -Status für jeden geschützten Hostcluster.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Gehen Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**.

   In der Schutzspalte wird ein Symbol angezeigt, das den Schutzstatus anzeigt.

3. Bewegen Sie den Mauszeiger über das Symbol, um weitere Details anzuzeigen.

Fügen Sie neue Datastores oder Hosts hinzu

Fügen Sie mithilfe der vCenter-Benutzeroberfläche Hosts hinzu oder erstellen Sie Datenspeicher auf dem geschützten Cluster.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Um die Eigenschaften eines geschützten Clusters zu bearbeiten, können Sie eine der beiden Optionen wählen
   a. Gehen Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**, wählen Sie das Auslassungsmenü neben dem Cluster und wählen Sie **Bearbeiten** oder

b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie * NetApp ONTAP -Tools* > **Cluster schützen**.

3. Wenn Sie in der vCenter-Benutzeroberfläche einen Datenspeicher erstellen, wird dieser als ungeschützt angezeigt. Sie können alle Datenspeicher im Cluster und ihren Schutzstatus in einem Dialogfeld anzeigen. Wählen Sie die Schaltfläche **Schützen**, um den Schutz zu aktivieren.

> Nachdem Sie in der Benutzeroberfläche von vCenter Server einen Datenspeicher erstellt haben, wählen Sie auf der Übersichtsseite **Erkennen** aus, um den Datenspeicher als Kandidat für den Schutz im Hostcluster anzuzeigen. Der Schutzstatus wird nach der nächsten regelmäßigen Schutzerkennung auf „Geschützt“ aktualisiert.

4. Wenn Sie einen neuen ESXi-Host hinzufügen, wird der Schutzstatus als teilweise geschützt angezeigt. Wählen Sie das Auslassungsmenü unter den SnapMirror -Einstellungen und wählen Sie **Bearbeiten**, um die Nähe des neu hinzugefügten ESXi-Hosts festzulegen.

> Bei asynchronen Beziehungen wird die Bearbeitung in ONTAP -Tools nicht unterstützt, da die Ziel-SVM für einen tertiären Standort nicht derselben Instanz hinzugefügt werden kann. Um die Beziehungskonfiguration zu ändern, verwenden Sie System Manager oder die CLI auf der Ziel-SVM.

5. Wählen Sie nach dem Vornehmen von Änderungen **Speichern**.
6. Sie können die Änderungen im Fenster **Protect Cluster** sehen.

ONTAP -Tools erstellen eine vCenter-Aufgabe und Sie können ihren Fortschritt im Bereich **Letzte Aufgabe** verfolgen.

Fügen Sie eine neue SnapMirror-Beziehung hinzu

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Um die Eigenschaften eines geschützten Clusters zu bearbeiten, können Sie eine der beiden Optionen wählen
   a. Gehen Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**, wählen Sie das Auslassungsmenü neben dem Cluster und wählen Sie **Bearbeiten** oder
   b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie * NetApp ONTAP -Tools* > **Cluster schützen**.
3. Wählen Sie **Beziehung hinzufügen**.
4. Fügen Sie eine neue Beziehung als Richtlinientyp **Asynchronous** oder **AutomatedFailOverDuplex** hinzu.
5. Wählen Sie **Schutz**.

   Sie können die Änderungen im Fenster **Protect Cluster** sehen.

ONTAP -Tools erstellen eine vCenter-Aufgabe und Sie können ihren Fortschritt im Bereich **Letzte Aufgabe** verfolgen.

Löschen einer vorhandenen SnapMirror-Beziehung

Um eine asynchrone SnapMirror -Beziehung zu löschen, stellen Sie sicher, dass die SVM oder der Cluster des sekundären Standorts als Speicher-Backend in den ONTAP tools for VMware vSphere hinzugefügt wird. Sie

können nicht alle SnapMirror -Beziehungen auf einmal löschen. Durch das Löschen einer Beziehung wird auch die entsprechende Beziehung aus dem ONTAP Cluster entfernt. Wenn Sie eine automatisierte Failover-Duplex SnapMirror -Beziehung löschen, hebt das System die Zuordnung der Zieldatenspeicher auf und löscht die Konsistenzgruppe, LUNs, Volumes und igroups aus dem Ziel ONTAP Cluster.

Wenn Sie die Beziehung löschen, scannt das System den sekundären Standort erneut, um die nicht zugeordnete LUN als aktiven Pfad von den Hosts zu entfernen.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Um die Eigenschaften eines geschützten Clusters zu bearbeiten, können Sie eine der beiden Optionen wählen
   a. Gehen Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**, wählen Sie das Auslassungsmenü neben dem Cluster und wählen Sie **Bearbeiten** oder
   b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie * NetApp ONTAP -Tools* > **Cluster schützen**.
3. Wählen Sie unter den SnapMirror-Einstellungen das Auslassungsmenü aus und wählen Sie **Löschen**.
   - Wenn Sie eine asynchrone, auf dem Richtlinientyp basierende Beziehung eines geschützten Hostclusters löschen, müssen Sie die Speicherelemente manuell aus dem tertiären Speichercluster entfernen. Zu den Speicherelementen gehören Konsistenzgruppen, Volumes (für ONTAP -Systeme), Speichereinheiten (LUNs/Namespaces) und Snapshots.
   - Wenn Sie eine auf einer richtliniebasierte Automated Failover Duplex (AFD)-Beziehung eines geschützten Hostclusters löschen, können Sie die zugehörigen Speicherelemente auf dem sekundären Speicher direkt aus der Schnittstelle entfernen.
   - Wenn Sie eine auf einer richtliniebasierte Beziehung für Automated Failover Duplex (AFD) löschen und die Konsistenzgruppe nun für Sicherungen auf Anwendungsebene hierarchisch ist, wird eine Warnung bezüglich der Auswirkungen auf die Sicherung angezeigt. Bestätigen Sie, um fortzufahren. Nach der Bestätigung löschen Sie die zugehörigen Speicherelemente auf dem Sekundärspeicher. Wenn Sie sie nicht entfernen, verbleiben sie auf der sekundären Site.

ONTAP -Tools erstellen eine vCenter-Aufgabe und Sie können ihren Fortschritt im Bereich **Letzte Aufgabe** verfolgen.

Ändern Sie eine vorhandene SnapMirror-Beziehung

Um eine asynchrone SnapMirror -Beziehung zu ändern, stellen Sie sicher, dass der SVM oder Cluster des sekundären Standorts als Speicher-Backend in den ONTAP tools for VMware vSphere hinzugefügt wird. Für automatisierte Failover-Duplex- SnapMirror Beziehungen können Sie die Hostnähe für einheitliche Konfigurationen oder den Hostzugriff für nicht einheitliche Konfigurationen aktualisieren. Das Wechseln zwischen den Richtlinientypen „Asynchrones Failover-Duplex“ und „Automatisches Failover-Duplex“ wird nicht unterstützt. Sie können Näherungs- oder Zugriffseinstellungen für neu erkannte Hosts im Cluster konfigurieren.

Sie können eine vorhandene asynchrone SnapMirror -Beziehung nicht bearbeiten.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Um die Eigenschaften eines geschützten Clusters zu bearbeiten, können Sie eine der beiden Optionen wählen
   a. Gehen Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**, wählen Sie das Auslassungsmenü neben dem Cluster und wählen Sie **Bearbeiten** oder

b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie * NetApp ONTAP -Tools* > **Cluster schützen**.

3. Wenn der Richtlinientyp „AutomatedFailOverDuplex“ ausgewählt ist, fügen Sie Details zur Hostnähe oder zum Hostzugriff hinzu.
4. Wählen Sie die Schaltfläche **protect**.

ONTAP -Tools erstellen eine vCenter-Aufgabe. Verfolgen Sie den Fortschritt im Bereich **Letzte Aufgaben**.

Hostclusterschutz in ONTAP tools entfernen

Wenn Sie den Host-Cluster-Schutz entfernen, werden die Datastores ungeschützt.

Schritte

1. Um die Liste der geschützten Host-Cluster anzuzeigen, gehen Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**.

   Überwachen Sie auf dieser Seite geschützte Hostcluster, den Schutzstatus, die SnapMirror -Beziehung und den Status. Wählen Sie Konsistenzgruppen aus, um Kapazität, zugehörige Datenspeicher und untergeordnete Gruppen anzuzeigen.

2. Wählen Sie im Fenster **Hostclusterschutz** das Auslassungsmenü neben dem Cluster und wählen Sie **Schutz entfernen**.
   - Wenn Sie den Schutz von einem Hostcluster mit nur einer asynchronen SnapMirror -Beziehung entfernen, müssen Sie die Speicherelemente manuell löschen. Zu den Speicherelementen gehören Konsistenzgruppen, Volumes (für ONTAP -Systeme), Speichereinheiten (LUNs) und Snapshots.
   - Wenn Sie den Schutz von einem Hostcluster mit nur einer automatisierten, auf Failover-Duplex basierenden SnapMirror -Richtlinienbeziehung und einer nicht hierarchischen Konsistenzgruppe entfernen, können Sie die zugehörigen Speicherelemente auf dem sekundären Speicher direkt vom selben Bildschirm aus löschen.
   - Wenn Sie den Schutz eines Hostclusters sowohl mit SnapMirror -Richtlinien als auch mit einer hierarchischen Konsistenzgruppe für Sicherungen entfernen, wird eine Warnung zu den Auswirkungen auf die Sicherung angezeigt. Bestätigen Sie, um fortzufahren. Nach der Bestätigung löschen Sie die zugehörigen Speicherelemente auf dem Sekundärspeicher. Wenn Sie keine Bereinigung durchführen, verbleiben die Speicherelemente auf dem sekundären Standort.

Wiederherstellen des ONTAP Tools-Setups

Ab ONTAP tools for VMware vSphere 10.5 ist die Backup-Funktion standardmäßig aktiviert.

Der Datenspeicher, in dem Sie ONTAP tools for VMware vSphere Maschinen bereitstellen, speichert die Sicherungsdateien. Ein Ordner, der nach der IP-Adresse des ONTAP -Tools benannt ist (Punkte durch Unterstriche ersetzt und mit *OTV_backup* angehängt), enthält die beiden aktuellsten Sicherungsdateien (*OTV_backup_1.tar.enc* und *OTV_backup_2.tar.enc*) und eine Infodatei (*OTV_backup_info.txt*), die den Namen der aktuellsten Sicherung enthält.

Stellen Sie sicher, dass die neue virtuelle Maschine dieselbe IP-Adresse der ONTAP Tools verwendet und mit der ursprünglichen Systemkonfiguration übereinstimmt, einschließlich aktivierter Dienste, Knotengröße und HA-Modus.

Schritte

1. Laden Sie die Sicherungsdateien aus dem Datenspeicher der ursprünglichen virtuellen Maschine auf Ihr lokales System herunter.
   a. Gehen Sie zum Speicherbereich und wählen Sie den Datenspeicher aus, der die Sicherungsdateien für die virtuelle Maschine enthält.
   b. Wählen Sie den Abschnitt **Dateien** aus.
   c. Laden Sie das erforderliche Sicherungsverzeichnis herunter.
2. Schalten Sie die vorhandene virtuelle Maschine aus. Stellen Sie dann eine neue virtuelle Maschine bereit, indem Sie dieselbe OVA-Datei wie bei der ursprünglichen Bereitstellung verwenden.
3. Öffnen Sie vom vCenter Server aus die Wartungskonsole.
4. Melden Sie sich als Wartungbenutzer an.
5. Geben Sie ein `4`, um **Support und Diagnose** auszuwählen.
6. Geben Sie ein `2`, um die Option **Ferndiagnosezugriff aktivieren** auszuwählen, und erstellen Sie ein neues Passwort für den Diagnosezugriff.
7. Wählen Sie eine Sicherungsdatei aus dem heruntergeladenen Verzeichnis. Informationen zum neuesten Backup finden Sie in der Datei *OTV_backup_info.txt*.
8. Verwenden Sie den folgenden Befehl, um die Sicherungsdatei auf die neue virtuelle Maschine zu übertragen. Geben Sie bei der entsprechenden Aufforderung das Diagnosekennwort ein.

   ```
   scp <OTV_backup_X.tar.enc>
   diag@<node_ip>:/home/diag/system_recovery.tar.enc
   ```

   Ändern Sie nicht den im Befehl angegebenen Zielpfad und Dateinamen (/home/diag/system_recovery.tar.enc).

9. Nachdem die Sicherungsdatei übertragen wurde, melden Sie sich bei der Diagnose-Shell an und führen Sie den folgenden Befehl aus:

   ```
   sudo perl /home/maint/scripts/post-deploy-upgrade.pl -recovery
   ```

   Die Protokolle werden in der Datei */var/log/post-deploy-Upgrade.log* aufgezeichnet.

Nachdem Sie die Wiederherstellung abgeschlossen haben, stellen die ONTAP Tools Dienste und vCenter-Objekte wieder her.

ONTAP tools deinstallieren

Durch das Deinstallieren der ONTAP-Tools für VMware vSphere werden alle Daten in den Tools gelöscht.

Schritte

1. Entfernen oder verschieben Sie alle virtuellen Maschinen aus den ONTAP-Tools für von VMware vSphere gemanagte Datastores.
   - Informationen zum Entfernen der virtuellen Maschinen finden Sie unter "Entfernen Sie VMs und VM-

Vorlagen und registrieren Sie sie erneut"

- Informationen zum Verschieben in einen nicht verwalteten Datenspeicher finden Sie unter "So migrieren Sie Ihre virtuelle Maschine mit Storage vMotion"

2. "Löschen Sie Datastores" Auf ONTAP Tools für VMware vSphere erstellt.
3. Wenn Sie den VASA-Provider aktiviert haben, wählen Sie in den ONTAP-Tools **Einstellungen** > **VASA-Provider-Einstellungen** > **Registrierung aufheben** aus, um die Registrierung der VASA-Anbieter von allen vCenter-Servern aufzuheben.
4. Aufheben der Zuordnung aller Speicher-Back-Ends zur vCenter Server-Instanz. Siehe "Trennen Sie Storage Back-Ends von der vCenter Server-Instanz".
5. Löschen Sie alle Speicher-Back-Ends. Siehe "Managen von Storage-Back-Ends".
6. Entfernen Sie den SRA-Adapter aus VMware Live Site Recovery:
   a. Melden Sie sich als Administrator an der VMware Live Site Recovery-Appliance-Managementschnittstelle über Port 5480 an.
   b. Wählen Sie **Storage Replication Adapter** Aus.
   c. Wählen Sie die entsprechende SRA-Karte aus, und wählen Sie im Dropdown-Menü **Löschen** aus.
   d. Bestätigen Sie, dass Sie die Ergebnisse des Löschens des Adapters kennen, und wählen Sie **Löschen**.
7. Löschen Sie die in den ONTAP Tools für VMware vSphere gespeicherten vCenter Server-Instanzen. Siehe "Verwalten von vCenter Server-Instanzen".
8. Schalten Sie die ONTAP-Tools für VMware vSphere-VMs vom vCenter-Server aus und löschen Sie die VMs.

Was kommt als Nächstes?

"Entfernen Sie FlexVol Volumes"

Entfernen Sie FlexVol-Volumes nach der Deinstallation von ONTAP tools

Wenn Sie einen dedizierten ONTAP Cluster für ONTAP Tools zur VMware Implementierung verwenden, werden viele nicht genutzte FlexVol Volumes erstellt. Nach dem Entfernen von ONTAP-Tools für VMware vSphere sollten Sie die FlexVol-Volumes entfernen, um mögliche Performance-Auswirkungen zu vermeiden.

Schritte

1. Ermitteln Sie den ONTAP tools for VMware vSphere -Bereitstellungstyp über die VM des ONTAP Tools-Verwaltungsknotens. Führen Sie folgenden Befehl aus, um den Bereitstellungstyp zu überprüfen: *cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol*

   Wenn es sich um eine iSCSI-Bereitstellung handelt, löschen Sie auch die igroups.

2. Rufen Sie die Liste der FlexVol -Volumes ab. *kubectl beschreibe persistente Volumes | grep internalName | awk -F'=' '{print $2}'*
3. Entfernen Sie die VMs vom vCenter Server. Siehe "Entfernen Sie VMs und VM-Vorlagen und registrieren Sie sie erneut".
4. Löschen Sie FlexVol -Volumes. Siehe "Löschen Sie ein FlexVol Volume" . Geben Sie den genauen FlexVol volume Namen im CLI-Befehl ein, um ein Volume zu löschen.

5. Löschen Sie im Falle einer iSCSI-Bereitstellung SAN-Initiatorgruppen aus dem ONTAP-Speichersystem. Siehe "Zeigen Sie SAN-Initiatoren und -Initiatorgruppen an und verwalten Sie sie".

Upgrade der ONTAP Tools für VMware vSphere

Upgrade von ONTAP tools for VMware vSphere 10.x auf 10.5

Sie können von ONTAP tools for VMware vSphere 10.3 oder 10.4 auf 10.5 aktualisieren. Um jedoch von ONTAP Tools 10.0, 10.1 oder 10.2 auf 10.5 zu aktualisieren, müssen Sie zuerst auf 10.3 oder 10.4 aktualisieren, bevor Sie mit 10.5 fortfahren.

- Stellen Sie bei ASA R2-Systemen sicher, dass Sie ein Upgrade auf ONTAP tools for VMware vSphere auf 10.5 und ONTAP auf 9.16.1 durchführen, bevor Sie weitere Storage Availability Zones (SAZs) einrichten.
- Wenn das Upgrade von ONTAP tools for VMware vSphere 10.3 oder 10.4 auf 10.5 fehlschlägt, ist ein Rollback nicht möglich. Verwenden Sie ein niedriges RPO oder eine Snapshot-Wiederherstellung, um das Setup wiederherzustellen. Verwenden Sie für ONTAP tools for VMware vSphere 10.2 und früher Zero-RPO, um das Setup wiederherzustellen.

Bevor Sie beginnen

- Stellen Sie sicher, dass alle Knoten aktiv sind.
- Stellen Sie sicher, dass das ONTAP -Systemzertifikat und die integrierten vCenter-Zertifikate mindestens 5 Tage gültig sind. Wenn die Zertifikate früher ablaufen, schlägt das Upgrade fehl.
- Stellen Sie sicher, dass Sie auf allen Knoten über eine fünfte Festplatte mit einer Kapazität von 100 GB verfügen.
- Überprüfen Sie, ob die Knotenkonfiguration den Spezifikationen in der folgenden Tabelle entspricht.

Bereitstellungstyp	CPU (Core) pro Node	Arbeitsspeicher (GB) pro Node	Festplattenspeicher (GB) pro Node	CPU gesamt (Core)	Arbeitsspeicher (GB)	Gesamter Festplattenspeicher (GB)
Nicht-HA klein	9	18	350	9	18	350
Non-HA Medium	13	26	350	13	26	350
HA klein	9	18	350	27	54	1050
HA Mittel	13	26	350	39	78	1050
HA groß	17	34	350	51	102	1050

- Stellen Sie sicher, dass das Hot-Plug-in für CPU und RAM aktiviert ist.
- Aktivieren Sie die Sicherung mit niedrigem RPO und stellen Sie sicher, dass eine Sicherung in der vCenter Client-Oberfläche sichtbar ist. Laden Sie den Sicherungsordner vor dem Upgrade herunter.
- Es wird eine Datensicherung mit niedrigem RPO empfohlen. Bei einer Bereitstellung ohne Hochverfügbarkeit können Sie jedoch vor dem Upgrade einen statischen Snapshot der virtuellen Maschine der ONTAP -Tools erstellen.

  Siehe "Backup-Einstellungen bearbeiten" Und "Wiederherstellen des ONTAP Tools-Setups" Weitere Informationen zu Datensicherung und -wiederherstellung finden Sie hier.

Schritte

1. Laden Sie ONTAP-Tools für VMware vSphere hoch, aktualisieren Sie ISO in die Content Library.
2. Wählen Sie auf der primären VM-Seite **Aktionen** > **Einstellungen bearbeiten**. Um den primären VM-Namen zu ermitteln:
   a. Aktivieren Sie die Diagnose-Shell auf einem beliebigen Knoten.
   b. Führen Sie folgenden Befehl aus:
   `grep sourceHost /opt/netapp/meta/ansible_vars.yaml`
3. Wählen Sie im Fenster „Einstellungen bearbeiten“ unter dem Feld „CD/DVD-Laufwerk“ die **ISO-Datei der Inhaltsbibliothek** aus.
4. Wählen Sie die ISO-Datei aus, aktivieren Sie das Kontrollkästchen **Verbunden** für das Feld **CD/DVD-Laufwerk** und klicken Sie auf **OK**.
5. Öffnen Sie im vCenter Server eine Konsole für ONTAP Tools.
6. Melden Sie sich als Wartungbenutzer an.
7. Geben Sie **2** ein, um das Menü **Systemkonfiguration** auszuwählen.
8. Geben Sie **7** ein, um die Option **Upgrade** auszuwählen.
9. Geben Sie die vCenter-Anmeldeinformationen an, wenn Sie dazu aufgefordert werden. Dies ist die vCenter-Instanz, auf der die ONTAP Tools gehostet werden.

   Wenn Sie ONTAP Tools in einer Topologie mit zwei vCenter Servern verwenden – wobei die Appliance in einer vCenter-Instanz gehostet wird und eine andere verwaltet –, können Sie der vCenter-Instanz, die die ONTAP Tools hostet, eine eingeschränkte Rolle zuweisen. Sie können einen dedizierten vCenter-Benutzer und eine Rolle erstellen, die nur über die für die OVF-Vorlagenbereitstellung erforderlichen Berechtigungen verfügen. Für Einzelheiten siehe die aufgeführten Rollen in "In ONTAP Tools für VMware vSphere 10 enthaltene Rollen"Die

   Stellen Sie für die vCenter-Instanz, die von ONTAP -Tools verwaltet wird, sicher, dass das vCenter-Benutzerkonto über Administratorrechte verfügt.

   Wenn während des Upgrades in integrierten Speicher-Backend-Zertifikaten SAN-Einträge (Subject Alternative Name) fehlen, erhalten Sie eine Meldung mit dem Hinweis auf den fehlenden SAN. Wenn Sie ohne Validierung des SAN fortfahren, wird das Upgrade fortgesetzt. Dies wird jedoch aufgrund potenzieller Sicherheitsrisiken nicht empfohlen.

10. Wenn Sie ein Upgrade durchführen, werden die folgenden Aktionen automatisch ausgeführt:
    a. Das Gateway-Zertifikat wird mit einer Gültigkeitsdauer von 1 Jahr erneuert. Wenn Sie den vorherigen SRA-Adapter entfernen und den neuen 10.5-Adapter hochladen, ändert sich die Gültigkeit des SRA-Zertifikats von 10 Jahren auf 1 Jahr.
    b. Remote-Plug-In wird aktualisiert
    c. ONTAP und vCenter Server-Zertifikate werden validiert und zu ONTAP -Tools hinzugefügt
    d. Sicherung ist aktiviert

Wie es weiter geht

Nach dem Upgrade auf ONTAP tools for VMware vSphere 10.5:

- Überwachen Sie Systemwarnungen und planen Sie die Erneuerung des Gateway-Zertifikats, bevor es in einem Jahr abläuft.
- Entfernen Sie den SRA-Adapter der ONTAP Tools 10.4 oder 10.3 und laden Sie die TAR-Datei des SRA-Adapters 10.5 hoch.

- Führen Sie den Installationsbefehl nach dem Hochladen des SRA-Adapter-Tar-Archivs aus. Scannen Sie anschließend die SRA-Adapter erneut, um die Seite „VMware Site Recovery Storage Replication Adapters“ zu aktualisieren.

Nach dem Upgrade können Sie:

- Deaktivieren Sie die Dienste über die Benutzeroberfläche des Managers
- Wechseln Sie von einer Einrichtung ohne HA-Konfiguration zu einer HA-Einrichtung
- Skalieren Sie eine kleine Konfiguration ohne HA auf eine mittlere Konfiguration ohne HA oder auf eine mittlere oder große HA-Konfiguration.

Verwandte Informationen

"Migrieren Sie von ONTAP tools for VMware vSphere 9.xx auf 10.5"

ONTAP tools-Upgrade-Fehlercodes

Während der Aktualisierung von ONTAP Tools für VMware vSphere können Sie auf Fehlercodes stoßen.
Die Fehlercodes sind fünf Ziffern lang, wobei die ersten beiden Ziffern das Skript darstellen, das auf das Problem gestoßen ist, und die letzten drei Ziffern den spezifischen Workflow innerhalb dieses Skripts darstellen.

Alle Fehlerprotokolle werden in der Datei ansible-perl-errors.log aufgezeichnet, um die Nachverfolgung und Behebung von Problemen zu erleichtern. Diese Protokolldatei enthält den Fehlercode und die fehlgeschlagene Ansible-Aufgabe.

Die auf dieser Seite angegebenen Fehlercodes dienen nur als Referenz. Wenden Sie sich an das Support-Team, wenn der Fehler weiterhin besteht oder wenn keine Lösung erwähnt wird.

In der folgenden Tabelle sind die Fehlercodes und die entsprechenden Dateinamen aufgeführt.

Fehlercode	Skriptname
00	firstboot-network-config.pl, Mode Deployment
01	firstboot-network-config.pl, Modusaktualisierung
02	firstboot-inputs-validation.pl
03	firstboot-deploy-otv-ng.pl, Deploy, HA
04	firstboot-deploy-otv-ng.pl, Deploy, non-HA
05	firstboot-deploy-otv-ng.pl, Neustart
06	firstboot-deploy-otv-ng.pl, Upgrade, HA
07	firstboot-deploy-otv-ng.pl, Upgrade, nicht HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Die letzten drei Ziffern des Fehlercodes zeigen den spezifischen Workflow-Fehler im Skript an:

Upgrade-Fehlercode	Arbeitsablauf	* Auflösung*
052	Die ISO-Datei kann mit der aktuellen Version identisch sein oder zwei Versionen über der aktuellen Version liegen.	Verwenden Sie eine kompatible ISO-Version, um von Ihrer aktuellen Version zu aktualisieren.
068	Das Rollback von Debian-Paketen ist fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
069	Wiederherstellung der Dateien fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
070	Backup konnte nicht gelöscht werden	-
071	Das Kubernetes-Cluster war in keinem ordnungsgemäßen Zustand	-
074	Mount-ISO ist fehlgeschlagen	Prüfen Sie /var/log/upgrade-run.log, und versuchen Sie die Aktualisierung erneut.
075	Die Vorabprüfungen für die Aktualisierung sind fehlgeschlagen	Wiederholen Sie die Aktualisierung.
076	Aktualisierung der Registrierung fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
077	Fehler beim Zurücksetzen der Registrierung	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
078	Upgrade des Bedieners fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
079	Rollback des Benutzers fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
080	Aktualisierung der Dienste ist fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
081	Rollback der Dienste ist fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
082	Löschen alter Bilder aus Container fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
083	Löschen des Backups ist fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen

Upgrade-Fehlercode	Arbeitsablauf	* Auflösung*
084	JobManager konnte nicht wieder in die Produktion geändert werden	Führen Sie die folgenden Schritte aus, um das Upgrade wiederherzustellen/abzuschließen. 1. Aktivieren Sie Diagnostic Shell 2. Führen Sie den Befehl *sudo perl /Home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3 aus. Überprüfen Sie die Protokolle unter /var/log/post-deploy-upgrade.log
087	Schritte nach dem Upgrade fehlgeschlagen.	Führen Sie die folgenden Schritte aus, um das Upgrade wiederherzustellen bzw. abzuschließen. 1. Aktivieren Sie Diagnostic Shell 2. Führen Sie *sudo perl /Home/maint/scripts/post-deploy-upgrade.pl --postupgrade* Befehl 3 aus. Überprüfen Sie die Protokolle unter /var/log/post-deploy-upgrade.log
088	Die Konfiguration der Protokollrotation für journald ist fehlgeschlagen	Überprüfen Sie die VM-Netzwerkeinstellungen, die mit dem Host kompatibel sind, auf dem die VM gehostet wird. Sie können versuchen, die VM auf einen anderen Host zu migrieren und neu zu starten.
089	Ändern der Eigentumsrechte für die Konfigurationsdatei „Zusammenfassung Protokoll drehen“ ist fehlgeschlagen	Wiederholen Sie die Aktualisierung.
095	Fehler beim Upgrade des Betriebssystems	Kein Recovery für OS Upgrade. Die ONTAP Tools Services wurden aktualisiert und neue Pods laufen.
096	Installieren Sie die dynamische Storage-provisionierung	Prüfen Sie die Upgrade-Protokolle, und versuchen Sie das Upgrade erneut.
097	Die Deinstallation der Dienste für das Upgrade ist fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
098	Das Kopieren des dockercred Secret von ntv-System in den Namespace für die dynamische Storage-bereitstellung ist fehlgeschlagen	Prüfen Sie die Upgrade-Protokolle, und versuchen Sie das Upgrade erneut.

Upgrade-Fehlercode	Arbeitsablauf	* Auflösung*
099	Die neue HDD-Ergänzung konnte nicht validiert werden	Fügen Sie im Falle von HA alle Nodes hinzu und bei einer Implementierung ohne HA-System einem Node.
109	Das Backup von persistenten Volume-Daten ist fehlgeschlagen	Prüfen Sie die Upgrade-Protokolle, und versuchen Sie das Upgrade erneut.
110	Die Wiederherstellung von persistenten Volume-Daten ist fehlgeschlagen	Recovery auf Basis von RPOs oder Snapshots ohne RPO und Upgrade erneut versuchen
111	Die Aktualisierung der etcd-Timeout-Parameter für RKE2 ist fehlgeschlagen	Prüfen Sie die Upgrade-Protokolle, und versuchen Sie das Upgrade erneut.
112	Die dynamische speicherbereitstellung konnte nicht deinstalliert werden	-
113	Die Aktualisierung der Ressourcen auf sekundären Nodes ist fehlgeschlagen	Prüfen Sie die Upgrade-Protokolle, und versuchen Sie das Upgrade erneut.
104	Der Neustart des sekundären Knotens ist fehlgeschlagen	Starten Sie die Knoten manuell nacheinander neu
100	Kernel-Rollback ist fehlgeschlagen	-
051	Das Upgrade der dynamischen speicherbereitstellung ist fehlgeschlagen	Upgrade-Protokolle prüfen und Upgrade wiederholen.
056	Löschen der Migrationssicherung fehlgeschlagen	NA
090	Zertifikatsvalidierung für Speicher-Backends und vCenter fehlgeschlagen	Überprüfen Sie die Upgrade-Protokolle und die Protokolldatei unter /var/log/cert_validation_error.log und versuchen Sie das Upgrade erneut.

Ab ONTAP-Tools für VMware vSphere 10.3 werden Zero RPO nicht unterstützt.

Weitere Informationen zu "So stellen Sie ONTAP-Tools für VMware vSphere wieder her, wenn das Upgrade von Version 10.0 auf 10.1 fehlschlägt"

Migrieren Sie ONTAP tools for VMware vSphere 9.xx auf 10.5

Migrieren Sie von ONTAP tools for VMware vSphere 9.xx auf 10.5

Die Migration der NetApp ONTAP tools for VMware vSphere -Setup von Version 9.xx auf 10.5 erfordert aufgrund der erheblichen Produktaktualisierungen und -verbesserungen in den Versionen einen Migrationsprozess.

Sie können von den ONTAP tools for VMware vSphere 9.12D1, 9.13D2 und 9.13P2 auf die ONTAP tools for VMware vSphere 10.5 migrieren.

Wenn Sie in Ihrem Setup NFS- und VMFS-Datenspeicher und keine vVols Datenspeicher haben, deinstallieren Sie einfach ONTAP Tools 9.xx und stellen Sie ONTAP Tools 10.5 bereit. Wenn Ihr Setup jedoch vVols Datenspeicher enthält, müssen Sie den VASA-Provider und den SRA migrieren.

Die folgende Tabelle skizziert den Migrationsprozess in diesen beiden unterschiedlichen Szenarien.

Wenn das Setup über vVols-Datenspeicher verfügt	Wenn das Setup nur NFS- und VMFS-Datenspeicher enthält
Schritte: 1. "Migrieren des VASA-Anbieters" 2. "Erstellen von VM-Speicherrichtlinien"	Schritte: 1. Entfernen Sie ONTAP Tools 9.xx aus Ihrer Umgebung. Siehe "So entfernen Sie OTV 9.xx aus Ihrer Umgebung" NetApp Knowledge Base-Artikel. 2. "Bereitstellen und Konfigurieren von ONTAP tools for VMware vSphere 10.5" 3. "Aktualisieren Sie das SRA" 4. "Erstellen von VM-Speicherrichtlinien"

Nach der Migration von ONTAP tools for VMware vSphere 9.xx auf 10.5 sind vVols Datenspeicher, die das NVMe/FC-Protokoll verwenden, nicht mehr betriebsbereit, da ONTAP Tools 10.5 das NVMe-oF-Protokoll nur mit VMFS-Datenspeichern unterstützt.

Migrieren Sie den VASA Provider und aktualisieren Sie die SRA in ONTAP tools

Befolgen Sie die Schritte in diesem Abschnitt, um den VASA Provider von ONTAP tools for VMware vSphere 9.xx auf ONTAP tools for VMware vSphere 10.5 zu migrieren und den Storage Replication Adapter (SRA) auf der VMware Live Site Recovery Appliance zu aktualisieren.

Schritte zur Migration des VASA-Anbieters

1. Um Derby-PORT 1527 auf den vorhandenen ONTAP-Tools für VMware vSphere zu aktivieren, aktivieren Sie den Root-Benutzer und melden Sie sich über SSH an der CLI an. Führen Sie dann den folgenden Befehl aus:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Stellen Sie OVA für ONTAP tools for VMware vSphere 10.5 bereit.
3. Fügen Sie die vCenter Server-Instanz hinzu, die Sie zu ONTAP tools for VMware vSphere 10.5 Release migrieren möchten. Weitere Informationen finden Sie unter "Fügen Sie eine vCenter Server-Instanz hinzu" für weitere Informationen.
4. Binden Sie das Speicher-Backend lokal über die vCenter Server-APIs für das ONTAP -Tools-Plug-in ein. Siehe dazu"Fügen Sie ein Speicher-Backend über die vSphere-Clientschnittstelle hinzu." für weitere Informationen.
5. Sie benötigen ein Zugriffstoken, um REST-API-Anfragen zu authentifizieren. Verwenden Sie das folgende Beispiel und ersetzen Sie die Variablen durch Werte, die für Ihre Umgebung spezifisch sind.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login” \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

   Kopieren und speichern Sie das in der Antwort zurückgegebene Zugriffstoken.

6. Geben Sie die folgende API von Swagger oder in Postman zur Migration aus.

```
curl -X POST
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migra
tion-jobs`
```

   Sie können über diese URL auf Swagger zugreifen: `https://$FQDN_IP_PORT/` , Zum Beispiel: `https://10.67.25.33:8443/` .

HTTP-Methode und Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/v1

Verarbeitungsart

Asynchron

Beispiel für Curl

```
curl -X POST 'https://<OTV-NG-
IP>:8443/virtualization/api/v1/vcenters/<vcguid>/migration-jobs' \
--header 'x-auth: <auth_token>' \
--header 'Content-Type: application/json' \
--data '{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "******"
  },
  "database_password": "******"
}'
```

Request Body für andere Release-Migration:

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*******"
  }
}
```

JSON-Ausgabebeispiel

Das System gibt ein Jobobjekt zurück. Speichern Sie die Auftragskennung, um sie im nächsten Schritt zu verwenden.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

7. Verwenden Sie den folgenden URI in Swagger, um den Status zu überprüfen:

```
curl
`\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<migra
tion_id>?includeSubJobsAndTasks=true`
```

   Überprüfen Sie nach Abschluss des Auftrags den Migrationsbericht in der Auftragsantwort.

8. Fügen Sie die ONTAP tools for VMware vSphere -Speicheranbieter zum vCenter Server hinzu.
9. Registrieren Sie den VASA-Provider mit ONTAP tools for VMware vSphere. Anweisungen finden Sie unter"Registrieren Sie den VASA Provider" .
10. Überprüfen Sie nach der Registrierung den Namen des VASA-Anbieters und seinen Status im vSphere Client unter **Speicheranbieter**. Der VASA-Anbieter sollte online erscheinen und die erfolgreiche Registrierung bestätigen.
11. "Aktivieren Sie VASA Provider"Dienst auf ONTAP tools for VMware vSphere 10.5.
12. Beenden Sie die ONTAP tools for VMware vSphere Storage Provider 9.10/9.11/9.12/9.13 VASA Provider-Dienst mit den folgenden Schritten:
    a. Öffnen Sie in ONTAP tools 9.x die Webkonsole.
    b. Greifen Sie auf die Wartungskonsole zu.
    c. Eingeben `1` um das Menü **Anwendungskonfiguration** auszuwählen.
    d. Eingeben `5` um die VASA Provider- und SRA-Dienste zu stoppen.
    e. Navigieren Sie im vSphere Client zu **Inventar** > **Speicheranbieter**.
    f. Wählen Sie im Speicher-Backend den ONTAP tools 9.x VASA Provider aus und klicken Sie auf **Entfernen**.

       Nachdem der alte VASA-Provider gestoppt wurde, führt der vCenter Server ein Failover auf ONTAP tools for VMware vSphere durch. Alle Datenspeicher und VMs sind nun über ONTAP tools for VMware vSphere zugänglich und werden von diesen bedient.

13. Migrierte NFS- und VMFS-Datenspeicher werden in ONTAP tools for VMware vSphere 10.5 nach dem Datenspeichererkennungsjob angezeigt, der bis zu 30 Minuten dauern kann. Überprüfen Sie ihre Sichtbarkeit auf der Übersichtsseite.
14. Führen Sie die Patch-Migration mit der folgenden API in Swagger oder in Postman durch:

HTTP-Methode und Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
PATCH	/API/v1

Verarbeitungsart

Asynchron

Verwenden Sie die folgende URI in Swagger:

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_i
d>/migration-jobs/<migration_id>`
```

Beispiel für Curl

```
curl  -X PATCH
`\https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-
4163-44f9-a872-9adabb008ca9/migration-jobs/d50073ce-35b4-4c51-9d2e-
4ce66f802c35`
```

JSON-Ausgabebeispiel

Ein Jobobjekt wird zurückgegeben. Sie sollten die Jobkennung speichern, um sie im nächsten Schritt zu verwenden.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

Der Anforderungskörper ist für den Patchvorgang leer.

UUID ist die Migrations-UUID, die als Antwort auf die API nach der Migration zurückgegeben wird.

Nach Ausführung der Patch-Migrations-API halten alle VMs die Storage-Richtlinie ein.

Wie es weiter geht

Nachdem Sie die Migration abgeschlossen und ONTAP Tools 10.5 beim vCenter Server registriert haben,

führen Sie die folgenden Schritte aus:

- Warten Sie, bis die **Erkennung** abgeschlossen ist. Das System aktualisiert die Zertifikate auf allen Hosts automatisch.
- Warten Sie, bevor Sie mit dem Starten von Datenspeicher- und virtuellen Maschinenvorgängen beginnen. Die Wartezeit hängt von der Anzahl der Hosts, Datenspeicher und virtuellen Maschinen ab. Wenn Sie nicht warten, kann es gelegentlich zu Fehlern kommen.

Wenn der Compliance-Zustand der virtuellen Maschine nach dem Upgrade veraltet ist, wenden Sie die Speicherrichtlinie erneut an, indem Sie die folgenden Schritte ausführen:

1. Gehen Sie zum Datenspeicher und wählen Sie **Zusammenfassung** > **VM-Speicherrichtlinien**.

   Das System zeigt den Compliance-Status unter **VM-Speicherrichtlinien-Compliance** als **Veraltet** an.

2. Wählen Sie die Storage-VM-Richtlinie und die entsprechende VM aus.
3. Wählen Sie **Übernehmen**.

   Der Konformitätsstatus unter **VM-Speicherrichtlinienkonformität** wird als konform angezeigt.

Verwandte Informationen

- "Erfahren Sie mehr über ONTAP Tools für die rollenbasierte Zugriffssteuerung von VMware vSphere 10"
- "Upgrade von ONTAP tools for VMware vSphere 10.x auf 10.5"

Schritte zum Aktualisieren des Storage Replication Adapters (SRA)

Bevor Sie beginnen

Im Wiederherstellungsplan bezeichnet der geschützte Standort den Ort, an dem die VMs aktuell ausgeführt werden, während der Wiederherstellungsstandort der Ort ist, an dem die VMs wiederhergestellt werden. Die Schnittstelle der VMware Live Site Recovery-Appliance zeigt den Status des Wiederherstellungsplans mit Details zu den geschützten und Wiederherstellungs-Sites an. Im Wiederherstellungsplan sind die Schaltflächen „Bereinigen“ und „Neu schützen“ deaktiviert, während die Schaltflächen „Testen“ und „Ausführen“ aktiviert bleiben. Dies zeigt an, dass der Standort für die Datenwiederherstellung vorbereitet ist. Stellen Sie vor der Migration des SRA sicher, dass sich ein Standort im geschützten Zustand und der andere im Wiederherstellungszustand befindet.

> Beginnen Sie nicht mit der Migration, wenn das Failover abgeschlossen ist, der erneute Schutz jedoch noch aussteht. Stellen Sie sicher, dass der erneute Schutzvorgang abgeschlossen ist, bevor Sie mit der Migration fortfahren. Wenn ein Test-Failover läuft, bereinigen Sie das Test-Failover und starten Sie die Migration.

1. Führen Sie diese Schritte aus, um den SRA-Adapter für ONTAP-Tools für VMware vSphere 9.xx in der VMware-Standortwiederherstellung zu löschen:
   a. Wechseln Sie zur Seite VMware Live Site Recovery Configuration Management
   b. Gehen Sie zum Abschnitt **Storage Replication Adapter**.
   c. Wählen Sie im Auslassungsmenü **Konfiguration zurücksetzen**.
   d. Wählen Sie im Auslassungsmenü **Löschen**.
2. Führen Sie diese Schritte sowohl an Sicherungs- als auch an Recovery-Standorten aus.
   a. "Aktivieren Sie ONTAP-Tools für VMware vSphere-Services"

b. Konfigurieren Sie ONTAP tools for VMware vSphere 10.5 SRA-Adapter mit den Schritten in"Konfigurieren Sie SRA auf der VMware Live Site Recovery-Appliance" .

c. Führen Sie auf der VMware Live Site Recovery-Schnittstelle **Discover Arrays** und **Discover Devices** aus. Bestätigen Sie, dass die Geräte wie vor der Migration angezeigt werden.

Automatisierung mit der REST-API

Erfahren Sie mehr über die ONTAP tools REST API

ONTAP Tools für VMware vSphere 10 ist eine Sammlung von Tools für das Lifecycle Management von Virtual Machines. Sie umfasst eine zuverlässige REST-API, die Sie als Teil Ihrer Automatisierungsprozesse nutzen können.

REST-Web-Services-Grundlage

Representational State Transfer (REST) ist ein Stil zur Erstellung verteilter Webanwendungen, einschließlich des Designs von Webservices-APIs. Es wird eine Reihe von Technologien zur Offenlegung serverbasierter Ressourcen und zur Verwaltung ihrer Zustände eingeführt.

Ressourcen- und Zustandsdarstellung

Ressourcen sind die grundlegenden Komponenten einer REST-Web-Services-Anwendung. Beim Entwurf einer REST-API gibt es zwei wichtige Anfangsaufgaben:

- Ermitteln Sie die System- oder serverbasierten Ressourcen
- Definieren Sie den Ressourcenstatus und die zugehörigen Statusübergangsvorgänge

Client-Anwendungen können die Ressourcenzustände über genau definierte Nachrichtenflüsse anzeigen und ändern.

HTTP-Meldungen

Hypertext Transfer Protocol (HTTP) ist das Protokoll, das vom Web Services-Client und -Server zum Austausch von Nachrichten über die Ressourcen verwendet wird. Es folgt dem CRUD-Modell auf der Grundlage der generischen Vorgänge Erstellen, Lesen, Aktualisieren und Löschen. Das HTTP-Protokoll enthält Anforderungs- und Antwortheader sowie Antwortstatuscodes.

JSON-Datenformatierung

Obwohl mehrere Nachrichtenformate verfügbar sind, ist die beliebteste Option JavaScript Object Notation (JSON). JSON ist ein Industriestandard für die Darstellung einfacher Datenstrukturen im Klartext und dient zur Übertragung von Statusinformationen, die die Ressourcen und gewünschten Aktionen beschreiben.

Sicherheit

Sicherheit ist ein wichtiger Aspekt einer REST-API. Zusätzlich zum TLS-Protokoll (Transport Layer Security) zum Schutz des HTTP-Datenverkehrs über das Netzwerk verwendet die ONTAP Tools für die VMware vSphere 10 REST API auch Zugriffstoken für die Authentifizierung. Sie müssen ein Zugriffstoken erwerben und für nachfolgende API-Aufrufe verwenden.

Unterstützung für asynchrone Anfragen

Die ONTAP-Tools für VMware vSphere 10 REST API führen die meisten Anfragen synchron aus und geben einen Statuscode zurück, sobald der Vorgang abgeschlossen ist. Sie unterstützt auch die asynchrone Verarbeitung für Aufgaben, die eine längere Zeit benötigen.

ONTAP Tools Manager-Umgebung

Es gibt mehrere Aspekte der ONTAP Tools Manager Umgebung, die Sie berücksichtigen sollten.

Virtual Machine

ONTAP tools for VMware vSphere 10 werden mithilfe der vSphere-Remote-Plug-In-Architektur bereitgestellt. Die Software, einschließlich der Unterstützung für die REST-API, wird in einer separaten virtuellen Maschine ausgeführt.

IP-Adresse des ONTAP Tools

Die ONTAP Tools für VMware vSphere 10 bieten eine einzige IP-Adresse, die ein Gateway für die Funktionen der Virtual Machine bereitstellt. Sie müssen die Adresse während der Erstkonfiguration angeben und sie ist einer internen Komponente des Load Balancers zugewiesen. Die Adresse wird von der Benutzeroberfläche des ONTAP Tools Managers sowie für den direkten Zugriff auf die Dokumentationsseite und die REST-API von Swagger verwendet.

Zwei REST-APIs

Zusätzlich zu den ONTAP-Tools für die VMware vSphere 10-REST-API verfügt der ONTAP-Cluster über eine eigene REST-API. Der ONTAP-Tools-Manager verwendet die ONTAP-REST-API als Client, um Storage-bezogene Aufgaben auszuführen. Es ist wichtig, daran zu denken, dass diese beiden APIs separat und eindeutig sind. Weitere Informationen finden Sie unter "ONTAP-Automatisierung".

Details zur Implementierung der ONTAP tools REST API

IM REST werden einheitliche Technologien und Best Practices eingeführt, aber die genaue Implementierung jeder API kann je nach Designauswahl variieren. Sie sollten vor der Verwendung der ONTAP-Tools für VMware vSphere 10 REST-API vertraut sein.

Die REST-API umfasst mehrere Ressourcenkategorien wie vCenter und Aggregate. Im "API-Referenz" finden Sie weitere Informationen.

So erhalten Sie Zugriff auf die REST API

Sie können über die IP-Adresse des ONTAP Tools und den Port auf die ONTAP Tools für die VMware vSphere 10 REST-API zugreifen. Es gibt mehrere Teile der vollständigen URL, einschließlich:

- ONTAP Tools IP-Adresse und Port
- API-Version
- Ressourcenkategorie
- Bestimmte Ressource

Sie müssen die IP-Adresse während der Ersteinrichtung konfigurieren, während der Port fest auf 8443 bleibt. Der erste Teil der URL ist für jede ONTAP tools for VMware vSphere 10-Instanz konsistent; nur die Ressourcenkategorie und die spezifische Ressource ändern sich zwischen den Endpunkten.

> Die IP-Adresse und die Portwerte in den folgenden Beispielen dienen nur der Veranschaulichung. Sie müssen diese Werte für Ihre Umgebung ändern.

Beispiel für den Zugriff auf Authentifizierungsdienste

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Diese URL kann verwendet werden, um ein Zugriffstoken mit der POST-Methode anzufordern.

Beispiel für die Auflistung der vCenter-Server

```
https://10.61.25.34:8443/virtualization/api/v1/vcenters
```

Über diese URL kann mit der GET-Methode eine Liste der definierten vCenter-Serverinstanzen angefordert werden.

HTTP – Details

Die ONTAP-Tools für die REST-API von VMware vSphere 10 verwenden HTTP und verwandte Parameter, um auf die Ressourceninstanzen und -Sammlungen zu reagieren. Einzelheiten zur HTTP-Implementierung finden Sie unten.

HTTP-Methoden

Die HTTP-Methoden oder Verben, die von der REST-API unterstützt werden, sind in der folgenden Tabelle aufgeführt.

Methode	CRUD	Beschreibung
GET	Lesen	Ruft Objekteigenschaften für eine Ressourceninstanz oder -Sammlung ab. Bei Verwendung mit einer Sammlung gilt dies als Listenoperation.
POST	Erstellen	Erstellt eine neue Ressourceninstanz basierend auf den Eingabeparametern.
PUT	Aktualisieren	Aktualisiert eine gesamte Ressourceninstanz mit dem bereitgestellten JSON-Anforderungstext. Nicht vom Benutzer änderbare Schlüsselwerte bleiben erhalten.
PATCH	Aktualisieren	Fordert eine Reihe ausgewählter Änderungen in der Anforderung an, die auf die Ressourceninstanz angewendet werden.
Löschen	Löschen	Löscht eine vorhandene Ressourceninstanz.

Header für Anfragen und Antworten

In der folgenden Tabelle sind die wichtigsten HTTP-Header zusammengefasst, die mit der REST-API verwendet werden.

Kopfzeile	Typ	Nutzungshinweise
Akzeptieren	Anfrage	Dies ist der Inhaltstyp, den die Client-Anwendung akzeptieren kann. Gültige Werte sind '*/*` oder `application/json`.
X-auth	Anfrage	Enthält ein Zugriffstoken, das den Benutzer identifiziert, der die Anforderung über die Clientanwendung ausgibt.
Inhaltstyp	Antwort	Wird vom Server basierend auf dem Anforderungsheader zurückgegeben `Accept`.

HTTP-Statuscodes

Die HTTP-Statuscodes, die von der REST-API verwendet werden, werden im Folgenden beschrieben.

Codieren	Bedeutung	Beschreibung
200	OK	Zeigt den Erfolg von Aufrufen an, die keine neue Ressourceninstanz erstellen.

Codieren	Bedeutung	Beschreibung
201	Erstellt	Ein Objekt mit einer eindeutigen Kennung für die Ressourceninstanz wurde erfolgreich erstellt.
202	Akzeptiert	Die Anforderung wurde angenommen und ein Hintergrundjob erstellt, um die Anforderung auszuführen.
204	Kein Inhalt	Die Anfrage war erfolgreich, obwohl kein Inhalt zurückgegeben wurde.
400	Schlechte Anfrage	Die Eingabe der Anfrage ist nicht erkannt oder nicht angemessen.
401	Nicht Autorisiert	Der Benutzer ist nicht autorisiert und muss sich authentifizieren.
403	Verboten	Der Zugriff wird aufgrund eines Autorisierungsfehlers verweigert.
404	Nicht gefunden	Die in der Anfrage genannte Ressource existiert nicht.
409	Konflikt	Der Versuch, ein Objekt zu erstellen, ist fehlgeschlagen, weil das Objekt bereits vorhanden ist.
500	Interner Fehler	Ein allgemeiner interner Fehler ist auf dem Server aufgetreten.

Authentifizierung

Die Authentifizierung eines Clients für die REST-API wird mit einem Zugriffstoken durchgeführt. Zu den relevanten Merkmalen des Token- und Authentifizierungsprozesses gehören:

- Der Client muss ein Token mit den Admin-Anmeldedaten des ONTAP Tools Managers (Benutzername und Passwort) anfordern.
- Token werden als JSON Web Token (JWT) formatiert.
- Jedes Token läuft nach 60 Minuten ab.
- API-Anforderungen eines Clients müssen das Token in der Anforderungsheader enthalten `x-auth`.

Ein Beispiel für das anfordern und Verwenden eines Zugriffstoken finden Sie unter"Ihr erster REST-API-Aufruf".

Synchrone und asynchrone Anfragen

Die meisten REST-API-Aufrufe sind schnell abgeschlossen und werden daher synchron ausgeführt. Das heißt, sie geben einen Statuscode (z. B. 200) zurück, nachdem eine Anfrage abgeschlossen wurde. Anforderungen, die länger dauern, werden asynchron mit einem Hintergrundjob ausgeführt.

Nach der Ausgabe eines API-Aufrufs, der asynchron ausgeführt wird, gibt der Server einen HTTP-Statuscode 202 zurück. Dies zeigt an, dass die Anforderung angenommen, aber noch nicht abgeschlossen wurde. Sie können den Hintergrundjob abfragen, um seinen Status einschließlich Erfolg oder Fehlschlag zu bestimmen.

Die asynchrone Verarbeitung wird für verschiedene Arten von Vorgängen mit langen Ausführungsvorgängen verwendet, einschließlich Datastore- und vVol-Vorgängen. Weitere Informationen finden Sie in der Kategorie „Job Manager“ der REST-API auf der Seite „Swagger“.

Führen Sie Ihren ersten ONTAP tools REST API-Aufruf durch

Sie können einen API-Aufruf mit Curl ausgeben, um mit den ONTAP-Tools für die REST-API von VMware vSphere 10 zu beginnen.

Bevor Sie beginnen

In den Curl-Beispielen sollten Sie die erforderlichen Informationen und Parameter überprüfen.

Erforderliche Informationen

Sie benötigen Folgendes:

- ONTAP-Tools für VMware vSphere 10 IP-Adresse oder FQDN sowie den Port
- Zugangsdaten für den ONTAP Tools Manager Admin (Benutzername und Passwort)

Parameter und Variablen

Die folgenden Curl-Beispiele enthalten Bash-Style-Variablen. Sie können diese Variablen in der Bash-Umgebung festlegen oder sie vor der Ausgabe der Befehle manuell aktualisieren. Wenn Sie die Variablen festlegen, ersetzt die Shell die Werte in jeden Befehl, bevor er ausgeführt wird. Die Variablen sind in der folgenden Tabelle beschrieben.

Variabel	Beschreibung
FQDN_IP_PORT VON US-DOLLAR	Der vollständig qualifizierte Domänenname oder die IP-Adresse des ONTAP Tools Managers zusammen mit der Portnummer.
MYUSER	Benutzername für das ONTAP Tools Manager-Konto.
„MEIN KENNWORT“	Kennwort für den Benutzernamen des ONTAP Tools Managers.
ACCESS_TOKEN IN HÖHE VON USD	Das vom ONTAP Tools Manager ausgegebene Zugriffstoken.

Die folgenden Befehle und die Ausgabe an der Linux CLI veranschaulichen, wie eine Variable eingestellt und angezeigt werden kann:

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

Schritt 1: Erwerben Sie ein Zugriffstoken

Sie müssen ein Zugriffstoken erwerben, um die REST-API verwenden zu können. Ein Beispiel, wie Sie ein Zugriffstoken anfordern, finden Sie unten. Sie sollten die entsprechenden Werte für Ihre Umgebung ersetzen.

```
curl --request POST \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/login” \
--header "Content-Type: application/json" \
--header "Accept: */*" \
-d "{"username": "$MYUSER", "password": "$MYPASSWORD"}"
```

Kopieren und speichern Sie das in der Antwort angegebene Zugriffstoken.

Schritt 2: Geben Sie den REST API-Aufruf aus

Nachdem Sie über ein Zugriffstoken verfügen, können Sie Curl verwenden, um einen REST-API-Aufruf auszustellen. Fügen Sie das im ersten Schritt erworbene Zugriffstoken hinzu.

Beispiel für die Wellung

```
curl --request GET \
--location "https://$FQDN_IP_PORT/virtualization/api/v1/vcenters" \
--header "Accept: */*" \
--header "x-auth: $ACCESS_TOKEN"
```

Die JSON-Antwort enthält eine Liste der VMware vCenter Instanzen, die für den ONTAP Tools Manager konfiguriert wurden.

ONTAP tools REST API-Referenz

Die Referenz zu den ONTAP Tools für VMware vSphere 10 REST API enthält Details zu allen API-Aufrufen. Diese Referenz ist bei der Entwicklung von Automatisierungsapplikationen hilfreich.

Sie können online über die Swagger-Benutzeroberfläche auf die ONTAP-Tools für die VMware vSphere 10-REST-API-Dokumentation zugreifen. Sie benötigen die IP-Adresse oder den FQDN der ONTAP-Tools für den VMware vSphere 10 Gateway-Dienst sowie den Port.

Schritte

1. Geben Sie die folgende URL in Ihren Browser ein, um die entsprechende IP-Adresse und Port-Kombination für die Variable zu ersetzen, und drücken Sie **Enter**.

   `https://$FQDN_IP_PORT/`

   Beispiel

   `https://10.61.25.33:8443/`

2. Scrollen Sie als Beispiel für einen einzelnen API-Aufruf nach unten in die Kategorie **vCenters** und wählen Sie neben dem Endpunkt **GET** `/virtualization/api/v1/vcenters`

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweis zu ONTAP tools for VMware vSphere 10.5"