



ONTAP tools für VMware vSphere Dokumentation

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Inhalt

ONTAP tools für VMware vSphere Dokumentation	1
Versionshinweise	2
Versionshinweise für ONTAP tools	2
Neuerungen in ONTAP tools für VMware vSphere 10.5	2
Unterstützte ONTAP Plattformen und vCenter Serverversionen	3
Vergleich der Funktionen von ONTAP tools for VMware vSphere 9 und 10	3
Konzepte	5
Erfahren Sie mehr über ONTAP tools	5
Schlüsselkonzepte und Begriffe in ONTAP tools	5
Rollenbasierte Zugriffssteuerung (RBAC)	8
Erfahren Sie mehr über ONTAP tools RBAC	8
RBAC mit VMware vSphere	10
RBAC mit ONTAP	17
ONTAP tools für VMware vSphere bereitstellen	21
Schnellstart für ONTAP tools für VMware vSphere	21
Workflow für die Hochverfügbarkeitsbereitstellung von ONTAP tools	23
ONTAP tools für VMware vSphere Anforderungen und Konfigurationsgrenzen	24
Systemvoraussetzungen	24
Minimale Storage- und Applikationsanforderungen	24
Port-Anforderungen	25
Konfigurationsbeschränkungen für die Bereitstellung von ONTAP tools for VMware vSphere für vVols Datenspeicher	27
Konfigurationsbeschränkungen für die Bereitstellung von ONTAP tools for VMware vSphere für VMFS- und NFS-Datenspeicher	28
ONTAP tools für VMware vSphere Storage Replication Adapter (SRA)	28
Anforderungen vor der Bereitstellung von ONTAP tools	29
Bereitstellungsarbeitsblatt	30
Netzwerk Firewall-Konfiguration	31
ONTAP Speichereinstellungen	31
ONTAP tools bereitstellen	31
Fehler bei der Bereitstellung von ONTAP tools beheben	37
Protokolldateien sammeln	37
Bereitstellungsfehlercodes	37
ONTAP tools für VMware vSphere konfigurieren	42
Fügen Sie vCenter Serverinstanzen zu ONTAP tools hinzu	42
Registrieren Sie den VASA Provider bei einer vCenter Server-Instanz in ONTAP tools	43
Das NFS VAAI Plug-in mit ONTAP tools installieren	44
Konfigurieren der ESXi-Hosteinstellungen in ONTAP tools	45
Multipath- und Zeitüberschreitungseinstellungen des ESXi-Servers konfigurieren	45
ESXi Hostwerte festlegen	45
Konfigurieren Sie ONTAP Benutzerrollen und -Berechtigungen für ONTAP tools	46
Anforderungen an die SVM Aggregate-Zuordnung	47
ONTAP Benutzer und Rolle manuell erstellen	48

Upgrade ONTAP tools für VMware vSphere 10.1 Benutzer auf 10.3 Benutzer	56
Upgrade ONTAP tools für VMware vSphere 10.3 Benutzer auf 10.4 Benutzer	58
Fügen Sie ein Speicher-Backend zu ONTAP tools hinzu	58
Verknüpfen Sie ein Storage-Backend mit einer vCenter Server-Instanz in ONTAP tools	61
Konfigurieren Sie Netzwerkzugriff in ONTAP tools	61
Erstellen Sie einen Datenspeicher in ONTAP tools	62
Datenspeicher und virtuelle Maschinen schützen	68
Schützen Sie einen Hostcluster in ONTAP tools	68
Schutz mit SRA-Schutz verwenden	69
Konfigurieren Sie SRA in ONTAP tools, um Datastores zu schützen	69
Konfigurieren Sie SRA in ONTAP tools für VMware vSphere für SAN- und NAS-Umgebungen	70
Konfigurieren Sie SRA in ONTAP tools für hochskalierte Umgebungen	71
Konfigurieren Sie SRA auf der VMware Live Site Recovery Appliance mithilfe von ONTAP tools	72
Aktualisieren Sie die SRA-Anmeldeinformationen in ONTAP tools	73
Konfigurieren von geschützten und Wiederherstellungsstandorten in ONTAP tools	74
Konfiguration von Ressourcen für geschützte und Wiederherstellungsstandorte	76
Überprüfen Sie replizierte Speichersysteme in ONTAP tools	80
Fan-out-Schutz in ONTAP tools	81
ONTAP tools für VMware vSphere verwalten	84
Erfahren Sie mehr über das ONTAP tools-Dashboard	84
Wie ONTAP tools igroups und Exportrichtlinien verwaltet	85
Export-Richtlinien	89
Wie ONTAP tools igroups verwaltet	90
Kurze Verhaltenszusammenfassung	90
Initiatorgruppen-Kontexte	91
Benennungsverhalten	92
Verhalten je nach Szenario	92
Benutzerdefinierte Initiatorgruppen-Wiederverwendung und API-Verhalten	93
Ansicht zur Konvertierung von nativ zu verwaltet	93
Wiederverwendung entdeckter nativer Initiatorgruppen	95
Erfahren Sie mehr über die Benutzeroberfläche des ONTAP tools Manager	95
ONTAP tools Manager-Einstellungen verwalten	97
ONTAP tools AutoSupport-Einstellungen bearbeiten	97
Fügen Sie NTP-Server zu ONTAP tools hinzu	98
VASA-Provider- und SRA-Anmeldeinformationen in ONTAP tools zurücksetzen	98
ONTAP tools-Sicherungseinstellungen bearbeiten	98
ONTAP tools-Dienste aktivieren	99
ONTAP-Tools-Appliance-Einstellungen ändern	99
VMware vSphere-Hosts zu ONTAP tools hinzufügen	101
Datenspeicher verwalten	101
NFS- und VMFS-Datenspeicher in ONTAP tools einbinden	101
NFS- und VMFS-Datenspeicher in ONTAP tools aushängen	102
Einen vVols-Datenspeicher in ONTAP tools einbinden	103
NFS- und VMFS-Datenspeicher in ONTAP tools vergrößern/verkleinern	103
Erweitern Sie vVols Datenspeicher in ONTAP tools	103

Einen vVols Datenspeicher in ONTAP tools verkleinern	104
Datenspeicher in ONTAP tools löschen	104
ONTAP-Speicheransichten für Datenspeicher in ONTAP tools	106
Ansicht des Speichers virtueller Maschinen in ONTAP tools	106
Speicherschwellenwerte in ONTAP tools verwalten	106
Speicher-Backends in ONTAP tools verwalten	107
Speicher entdecken	107
Storage-Backends ändern	107
Storage-Backends entfernen	108
Detaillierte Ansicht des Storage-Backends	108
Verwaltung von vCenter Server-Instanzen in ONTAP tools	109
Speicher-Backends von der vCenter Server-Instanz trennen	109
Eine vCenter Server-Instanz ändern	109
Eine vCenter Server-Instanz entfernen	110
Zertifikat des vCenter Servers erneuern	110
ONTAP tools-Zertifikate verwalten	112
Zugriff auf ONTAP tools für VMware vSphere Wartungskonsole	114
Erfahren Sie mehr über die ONTAP tools maintenance console	114
Konfigurieren Sie den Ferndiagnosezugriff für ONTAP tools	115
Starten Sie SSH auf anderen ONTAP tools-Knoten	116
Aktualisieren Sie die vCenter Server-Anmeldeinformationen in ONTAP tools	116
Ändern Sie das Zertifikatvalidierungsflag in ONTAP tools	116
ONTAP tools Berichte	118
Virtuelle Maschinen verwalten	119
Überlegungen zur Migration und zum Klonen virtueller Maschinen für ONTAP tools	119
Migrieren Sie virtuelle Maschinen zu vVols-Datenspeichern in ONTAP tools	120
Bereinigen Sie die VASA-Konfigurationen in ONTAP tools	121
Eine Datenfestplatte an eine VM in ONTAP tools anhängen oder trennen	121
Speichersysteme und Hosts in ONTAP tools entdecken	122
ESXi-Hosteinstellungen mit ONTAP tools ändern	123
Passwörter verwalten	123
ONTAP tools Manager-Passwort ändern	123
ONTAP tools Manager-Passwort zurücksetzen	124
Anwendungsbenutzerpasswort in ONTAP tools zurücksetzen	124
Passwort der ONTAP tools for VMware vSphere Wartungskonsole zurücksetzen	124
Host-Cluster-Schutz verwalten	126
Ändern eines geschützten Hostclusters in ONTAP tools	126
Hostclusterschutz in ONTAP tools entfernen	129
Wiederherstellung der ONTAP tools Konfiguration	129
ONTAP tools deinstallieren	130
Entfernen Sie FlexVol-Volumes nach der Deinstallation von ONTAP tools	131
Upgrade ONTAP tools für VMware vSphere	132
Upgrade von ONTAP tools für VMware vSphere 10.x auf 10.5	132
ONTAP tools-Upgrade-Fehlercodes	134
Migration von ONTAP tools für VMware vSphere 9.xx auf 10.5	140

Migration von ONTAP tools für VMware vSphere 9.xx auf 10.5	140
Migrieren Sie den VASA Provider und aktualisieren Sie die SRA in ONTAP tools	140
Schritte zur Migration des VASA Provider	140
Schritte zum Aktualisieren des Speicherreplikationsadapters (SRA)	145
Automatisierung mithilfe der REST API	147
Erfahren Sie mehr über die ONTAP tools REST API	147
Grundlagen der REST-Webdienste	147
ONTAP tools Manager Umgebung	147
Details zur Implementierung der ONTAP tools REST API	148
Zugriff auf die REST API	148
HTTP-Details	149
Authentifizierung	150
Synchrone und asynchrone Anfragen	150
Führen Sie Ihren ersten ONTAP tools REST API-Aufruf durch	151
Bevor Sie beginnen	151
Schritt 1: Zugriffstoken abrufen	151
Schritt 2: Den REST API-Aufruf ausführen	152
ONTAP tools REST API-Referenz	152
Rechtliche Hinweise	153
Copyright	153
Marken	153
Patente	153
Datenschutzrichtlinie	153
Open Source	153

ONTAP tools für VMware vSphere Dokumentation

Versionshinweise

Versionshinweise für ONTAP tools

Informationen zu den neuen und erweiterten Funktionen in ONTAP tools for VMware vSphere 10.5.

Eine vollständige Liste der neuen Funktionen und Verbesserungen finden Sie unter [Neuerungen in ONTAP tools für VMware vSphere 10.5](#).

Die aktuellsten Informationen zur Kompatibilität finden Sie unter "[NetApp Interoperabilitätsmatrix-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 sich im "[ONTAP tools für VMware vSphere 10.5 Versionshinweise](#)". Eine Anmeldung mit Ihrem NetApp Account oder die Erstellung eines Accounts ist erforderlich, um auf die Release Notes zuzugreifen.

Neuerungen in ONTAP tools für VMware vSphere 10.5

Informationen zu den neuen Funktionen in ONTAP tools for VMware vSphere 10.5.

- **Plattformqualifizierung**

ONTAP tools for VMware vSphere 10.5 bietet Unterstützung für ASA r2 Systeme und sorgt für Kompatibilität mit den neuesten Hardware- und Softwarekonfigurationen. Diese Version umfasst außerdem die Integration mit ONTAP 9.16.1 und 9.17.1 und erweitert die unterstützten Umgebungen.

- **VMware Qualifizierung und Zertifizierungen**

ONTAP tools for VMware vSphere 10.5 entspricht den aktuellen VMware Interoperabilität Zertifizierungsstandards und unterstützt sowohl ESXi Host als auch vCenter Server.

- **MetroCluster Unterstützung**

Diese Version bietet Unterstützung für MetroCluster Konfigurationen, wodurch die Hochverfügbarkeit und die Funktionen zur Notfallwiederherstellung verbessert werden.

- **Sicherheits- und Zertifikatsverwaltung**

Diese Version bietet eine optimierte Verwaltung selbstsignierter Zertifikate und verbessert so sowohl die Benutzerfreundlichkeit als auch die Einhaltung von Sicherheitsstandards. Es stehen verbesserte Workflows zur Zertifikatsvalidierung zur Verfügung, um die Kommunikation zwischen ONTAP und ONTAP tools for VMware vSphere abzusichern.

- **Verbesserungen der Replikation**

Diese Version unterstützt die VMFS-Replikation mit hierarchischer Konsistenzgruppe einschließlich SRA und SnapMirror active sync in ASA r2-Systemen. Es werden Zero-RPO-Backups zur Verbesserung des Datenschutzes und der Wiederherstellung unterstützt.

• Upgrade und Migration

Der Upgrade- und Migrationsprozess von früheren Versionen der ONTAP tools for VMware vSphere zu ONTAP tools for VMware vSphere 10.5 ist so konzipiert, dass er nahtlos und effizient abläuft, Ausfallzeiten minimiert und einen reibungslosen Übergang gewährleistet.

Unterstützte ONTAP Plattformen und vCenter Serverversionen

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](#)".

Die aktuellsten Informationen zur Versionskompatibilität finden sich unter "[NetApp Interoperabilitätsmatrix-Tool](#)".

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

Es kann festgestellt werden, ob eine Migration von ONTAP tools for VMware vSphere 9 auf ONTAP tools for VMware vSphere 10.2 oder spätere Versionen sinnvoll ist.



Die aktuellsten Informationen zur Kompatibilität finden Sie unter "[NetApp Interoperabilitätsmatrix-Tool](#)".

Funktion	ONTAP tools 9.13	ONTAP tools ab Version 10.2
Wichtigstes Wertversprechen	Abläufe vom ersten bis zum zweiten Tag werden durch erweiterte Sicherheits-, Compliance- und Automatisierungsfunktionen optimiert und vereinfacht.	Erweiterte Unterstützung für FC für VMFS und NVMe-oF nur für VMFS. Benutzerfreundlichkeit für NetApp SnapMirror, einfache Einrichtung für vSphere Metro Storage Cluster und Unterstützung für VMware Live Site Recovery an drei Standorten.
ONTAP 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 Version 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 10K VMs Datenspeicher: 600 NFS, bis zu 50 VMFS	Hosts und VMs: 600 Hosts
Beobachtbarkeit	Dashboards für Leistung, Kapazität und Host-Compliance, dynamische VM- und Datenspeicherberichte	Aktualisierte Dashboards für Leistung, Kapazität und Host-Compliance, dynamische VM- und Datenspeicherberichte
Datenschutz	SRA Replikation für VMFS und NFS. SCV Integration und Interoperabilität für Backup.	SRA Replikation für iSCSI VMFS und NFS v3 Datenspeicher, Drei-Standort-Schutz durch Kombination von SMAS und VMware Live Site Recovery. SRA Unterstützung für FCP mit VMFS.
VASA Provider Unterstützung	VASA 4.0	VASA 3.0

Konzepte

Erfahren Sie mehr über ONTAP tools

ONTAP tools for VMware vSphere ist eine Sammlung von Tools für das Lebenszyklusmanagement virtueller Maschinen. Es integriert sich in das VMware-Ökosystem, um die Bereitstellung von Datenspeichern zu vereinfachen und 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 für VMware vSphere unterstützt:

- Kernfunktionen virtueller Maschinen (VM) wie Schutz und Notfallwiederherstellung
- VASA Provider für speicherrichtlinienbasierte Verwaltung
- Speicherrichtlinienbasierte Verwaltung
- Storage Replication Adapter (SRA)

Hohe Verfügbarkeit für ONTAP tools for VMware

ONTAP tools for VMware vSphere bietet Unterstützung für Hochverfügbarkeit (HA), um einen unterbrechungsfreien Betrieb auch bei Ausfällen zu gewährleisten.

Die HA Lösung hilft Ihnen, sich schnell von folgenden Arten von Ausfällen zu erholen:

- Hostausfall – Nur ein Ausfall eines einzelnen Knotens wird unterstützt.
- Netzwerkausfall
- Fehler der virtuellen Maschine (Gastbetriebssystem)
- Anwendungsfehler (ONTAP tools)

Es sind keine zusätzlichen Konfigurationen erforderlich, um HA für ONTAP tools for VMware vSphere zu aktivieren.



ONTAP tools for VMware vSphere unterstützt keine vCenter HA.

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

Schlüsselkonzepte und Begriffe in ONTAP tools

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

Zertifizierungsstelle (CA)

Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Instanz, die Secure Sockets Layer (SSL)-Zertifikate ausstellt.

Konsistenzgruppe

Eine Konsistenzgruppe ist eine Sammlung von Volumes, die als eine Einheit verwaltet werden. Konsistenzgruppen werden synchronisiert, um Datenkonsistenz über Speichereinheiten und Volumes hinweg zu gewährleisten. In ONTAP bieten sie einfache Verwaltung und Schutzgarantien für einen Anwendungsworkload, der sich über mehrere Volumes erstreckt. Weitere Informationen zu ["Konsistenzgruppen"](#).

Dual Stack

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

Hochverfügbarkeit (HA)

Die Clusterknoten sind in HA Paaren für einen unterbrechungsfreien Betrieb konfiguriert.

Logische Einheitennummer (LUN)

Eine LUN (Logical Unit Number) ist eine Nummer, die zur Identifizierung einer logischen Einheit innerhalb eines Storage Area Network (SAN) verwendet wird. Diese adressierbaren Geräte sind typischerweise logische Datenträger, auf die über das Small Computer System Interface (SCSI) Protokoll oder eine seiner abgeleiteten Varianten zugegriffen wird.

NVMe Namespace und Subsystem

Ein NVMe-Namensraum ist eine Menge nichtflüchtigen Speichers, die in logische Blöcke formatiert werden kann. Namensräume entsprechen den LUNs der FC- und iSCSI-Protokolle, und ein NVMe-Subsystem ist analog zu einer Initiatorgruppe. Ein NVMe-Subsystem kann mit Initiatoren verknüpft werden, sodass die zugehörigen Initiatoren auf Namensräume innerhalb des Subsystems zugreifen können.

ONTAP tools Manager

ONTAP tools Manager bietet ONTAP tools for VMware vSphere-Administratoren mehr Kontrolle über die verwalteten vCenter Serverinstanzen und eingebundene Storage-Backends. Er hilft bei der Verwaltung von vCenter Serverinstanzen, Storage-Backends, Zertifikaten, Passwörtern und Log-Bundles.

Open Virtual Appliance (OVA)

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

Recovery Point Objective (RPO)

RPO misst, wie häufig Sie Daten sichern oder replizieren. Es gibt den genauen Zeitpunkt an, zu dem Daten nach einem Ausfall wiederhergestellt werden müssen, damit der Geschäftsbetrieb fortgesetzt werden kann. Wenn ein Unternehmen beispielsweise einen RPO von 4 Stunden hat, kann es im Katastrophenfall einen Datenverlust von bis zu 4 Stunden tolerieren.

SnapMirror Active Sync

SnapMirror active sync ermöglicht es Unternehmensdiensten, auch bei einem vollständigen Standortausfall weiter zu funktionieren, indem Anwendungen mithilfe einer sekundären Kopie transparent auf ein Failover umschalten. Manuelle Eingriffe oder benutzerdefinierte Skripte sind für die Auslösung eines Failovers mit

SnapMirror active sync nicht erforderlich. Weitere Informationen ["SnapMirror Active Sync"](#).

Storage Backends

Storage Backends bilden die zugrundeliegende Speicherinfrastruktur, die der ESXi Host zum Speichern von Dateien, Daten und anderen Ressourcen virtueller Maschinen nutzt. Sie ermöglichen dem ESXi Host den Zugriff auf und die Verwaltung persistenter Daten und stellen die erforderliche Speicherkapazität und Leistung für eine virtualisierte Umgebung bereit.

Globaler Cluster (Storage-Backend)

Globale Storage-Backends, die nur mit ONTAP Cluster-Anmeldeinformationen verfügbar sind, werden über die ONTAP tools Manager-Oberfläche eingebunden. Sie können mit minimalen Privileges hinzugefügt werden, um die Erkennung der für die vVols-Verwaltung erforderlichen Cluster-Ressourcen zu ermöglichen. Globale Cluster sind ideal für Multitenancy-Szenarien, in denen ein SVM-Benutzer lokal für die vVols-Verwaltung hinzugefügt wird.

Lokaler Storage-Backend

Lokale Storage-Backends mit Cluster- oder SVM-Anmeldeinformationen werden über die ONTAP tools Benutzeroberfläche hinzugefügt und sind auf ein vCenter beschränkt. Bei lokaler Verwendung von Cluster-Anmeldeinformationen werden die zugehörigen SVMs automatisch mit dem vCenter zur Verwaltung von vVols oder VMFS zugeordnet. Für die VMFS-Verwaltung, einschließlich SRA, unterstützen die ONTAP tools SVM-Anmeldeinformationen, ohne dass ein globaler Cluster erforderlich ist.

Storage Replication Adapter (SRA)

SRA ist die herstellerspezifische Speichersoftware, die in der VMware Live Site Recovery Appliance installiert ist. Der Adapter ermöglicht die Kommunikation zwischen dem Site Recovery Manager und einem Speichercontroller auf Ebene der Storage Virtual Machine (SVM) sowie auf Clusterebene.

Storage Virtual Machine (SVM)

SVM ist die Mandantenfähigkeitseinheit in ONTAP. Ähnlich einer virtuellen Maschine auf einem Hypervisor ist SVM eine logische Einheit, die physische Ressourcen abstrahiert. SVM enthält Datenvolumes und eine oder mehrere LIFs, über die Daten an Clients bereitgestellt werden.

Uniforme und nicht-uniforme Konfiguration

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



Einheitlicher Hostzugriff wird für jede SnapMirror active sync-Bereitstellung unterstützt, nicht-einheitlicher Hostzugriff wird nur für symmetrische Aktiv/Aktiv-Bereitstellungen unterstützt. Weitere Informationen zu ["SnapMirror Active Sync Übersicht in ONTAP"](#).

Dateisystem für virtuelle Maschinen (VMFS)

VMFS ist ein Cluster-Dateisystem, das für die Speicherung von Dateien virtueller Maschinen in VMware vSphere-Umgebungen entwickelt wurde.

Virtuelle Volumes (vVols)

vVols bieten eine Abstraktion auf Volumenebene 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 typischerweise mit einer einzelnen LUN verknüpft, die als Container für vVols dient.

VM-Speicherrichtlinie

VM Storage Policies werden im vCenter Server unter Richtlinien und Profile erstellt. Für vVols wird ein Regelset mit Regeln des NetApp vVols Speichertypanbieter erstellt.

VMware Live Site Recovery

VMware Live Site Recovery, ehemals bekannt als Site Recovery Manager (SRM), bietet Funktionen für Geschäftskontinuität, Notfallwiederherstellung, Standortmigration und unterbrechungsfreies Testen in virtuellen VMware-Umgebungen.

VMware vSphere APIs for Storage Awareness (VASA)

VASA ist eine Sammlung von APIs, die Speichersysteme mit dem vCenter Server für Verwaltung und Administration integrieren. Die Architektur basiert auf mehreren Komponenten, darunter dem VASA Provider, der die Kommunikation zwischen VMware vSphere und den Speichersystemen übernimmt.

VMware vSphere Storage APIs – Array Integration (VAAI)

VAAI ist eine Sammlung von APIs, die die Kommunikation zwischen VMware vSphere ESXi Hosts und den Speichergeräten ermöglicht. Die APIs umfassen eine Reihe grundlegender Operationen, die von den Hosts verwendet werden, um Speicheroperationen auf das Array auszulagern. VAAI kann die Leistung bei speicherintensiven Aufgaben deutlich verbessern.

vSphere Metro Storage Cluster

vSphere Metro Storage Cluster (vMSC) ist eine Architektur, die vSphere in einer Stretch-Cluster-Bereitstellung ermöglicht und unterstützt. vMSC-Lösungen werden auf NetApp MetroCluster und SnapMirror active sync (ehemals SMBC) unterstützt. Diese Lösungen bieten verbesserte Geschäftskontinuität im Falle eines Domänenausfalls. Das Resilienzmodell basiert auf Ihren spezifischen Konfigurationsentscheidungen. Weitere Informationen zu ["VMware vSphere Metro Storage Cluster"](#).

vVols Datenspeicher

Der vVols Datenspeicher ist eine logische Repräsentation eines vVols Containers, der von einem VASA Provider erstellt und verwaltet wird.

Zero RPO

RPO steht für Recovery Point Objective, die Menge an Datenverlust, die innerhalb eines bestimmten Zeitraums als akzeptabel gilt. Ein RPO von Null bedeutet, dass kein Datenverlust akzeptabel ist.

Rollenbasierte Zugriffssteuerung (RBAC)

Erfahren Sie mehr über ONTAP tools RBAC

Die rollenbasierte Zugriffskontrolle (RBAC) ist ein Sicherheitsframework zur Steuerung

des Zugriffs auf Ressourcen innerhalb einer Organisation. RBAC vereinfacht die Administration, indem Rollen mit spezifischen Berechtigungsstufen zur Ausführung von Aktionen definiert werden, anstatt einzelnen Benutzern Berechtigungen zuzuweisen. Die definierten Rollen werden Benutzern zugewiesen, was das Fehlerrisiko verringert und die Verwaltung der Zugriffskontrolle in der gesamten Organisation vereinfacht.

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

RBAC-Komponenten

Grundsätzlich gibt es mehrere Komponenten, die in jeder RBAC-Implementierung enthalten sind. Diese Komponenten sind im Rahmen der Definition der Autorisierungsprozesse auf unterschiedliche Weise miteinander verbunden.

Privileges

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

Rollen

Eine Rolle ist ein Container, der ein oder mehrere Privileges umfasst. Rollen werden in der Regel anhand bestimmter Aufgaben oder Funktionen definiert. Wird einem Benutzer eine Rolle zugewiesen, erhält der Benutzer alle in der Rolle enthaltenen Privileges. Wie bei Privileges bieten Implementierungen vordefinierte Rollen und ermöglichen in der Regel auch die Erstellung benutzerdefinierter Rollen.

Objekte

Ein Objekt repräsentiert eine reale oder abstrakte Ressource innerhalb der RBAC-Umgebung. Die über die Privileges definierten Aktionen werden an oder mit den zugehörigen Objekten ausgeführt. Je nach Implementierung können Privileges einem Objekttyp oder einer bestimmten Objektinstanz gewährt werden.

Benutzer und Gruppen

Benutzern wird nach der Authentifizierung eine Rolle zugewiesen oder sie werden mit einer Rolle verknüpft. Einige RBAC-Implementierungen erlauben nur eine Rolle pro Benutzer, während andere mehrere Rollen pro Benutzer zulassen, wobei möglicherweise jeweils nur eine Rolle aktiv ist. Die Zuweisung von Rollen zu *Gruppen* kann die Sicherheitsverwaltung zusätzlich vereinfachen.

Berechtigungen

Eine Berechtigung ist eine Definition, die einen Benutzer oder eine Gruppe zusammen mit einer Rolle an ein Objekt bindet. Berechtigungen können in einem hierarchischen Objektmodell nützlich sein, da sie optional von den untergeordneten Elementen in der Hierarchie übernommen werden können.

Zwei RBAC Umgebungen

Bei der Arbeit mit ONTAP tools for VMware vSphere 10 sind zwei unterschiedliche RBAC-Umgebungen zu berücksichtigen. ONTAP tools for VMware vSphere 10 erfordert spezifische Privileges sowohl in vCenter als auch in ONTAP, um die jeweiligen Vorgänge auszuführen. Während ONTAP tools Speicherverwaltungsaufgaben automatisiert, werden keine Benutzerkonten in vCenter oder ONTAP erstellt.

Dienstkonten müssen bei Bedarf von einem vSphere-Administrator erstellt werden. Diese Dokumentation enthält Hinweise für Administratoren zur Zuweisung der erforderlichen Rollen und Berechtigungen für eine effektive Verwaltung von ONTAP tools.

VMware vCenter Server

Die RBAC-Implementierung in VMware vCenter Server wird verwendet, um den Zugriff auf Objekte einzuschränken, die über die vSphere Client-Benutzeroberfläche bereitgestellt werden. Im Rahmen der Installation von ONTAP tools for VMware vSphere 10 wird die RBAC-Umgebung um zusätzliche Objekte erweitert, die die Fähigkeiten der ONTAP tools repräsentieren. Der Zugriff auf diese Objekte erfolgt über das Remote-Plug-in. Weitere Informationen sind unter ["vCenter Server-RBAC-Umgebung"](#) verfügbar.

ONTAP Cluster

ONTAP tools for VMware vSphere 10 stellt über die ONTAP REST API eine Verbindung zu einem ONTAP Cluster her, um speicherbezogene Vorgänge auszuführen. Der Zugriff auf die Speicherressourcen wird durch eine ONTAP Rolle gesteuert, die dem ONTAP Benutzer zugeordnet ist, der während der Authentifizierung angegeben wurde. Siehe ["ONTAP RBAC Umgebung"](#) für weitere Informationen.

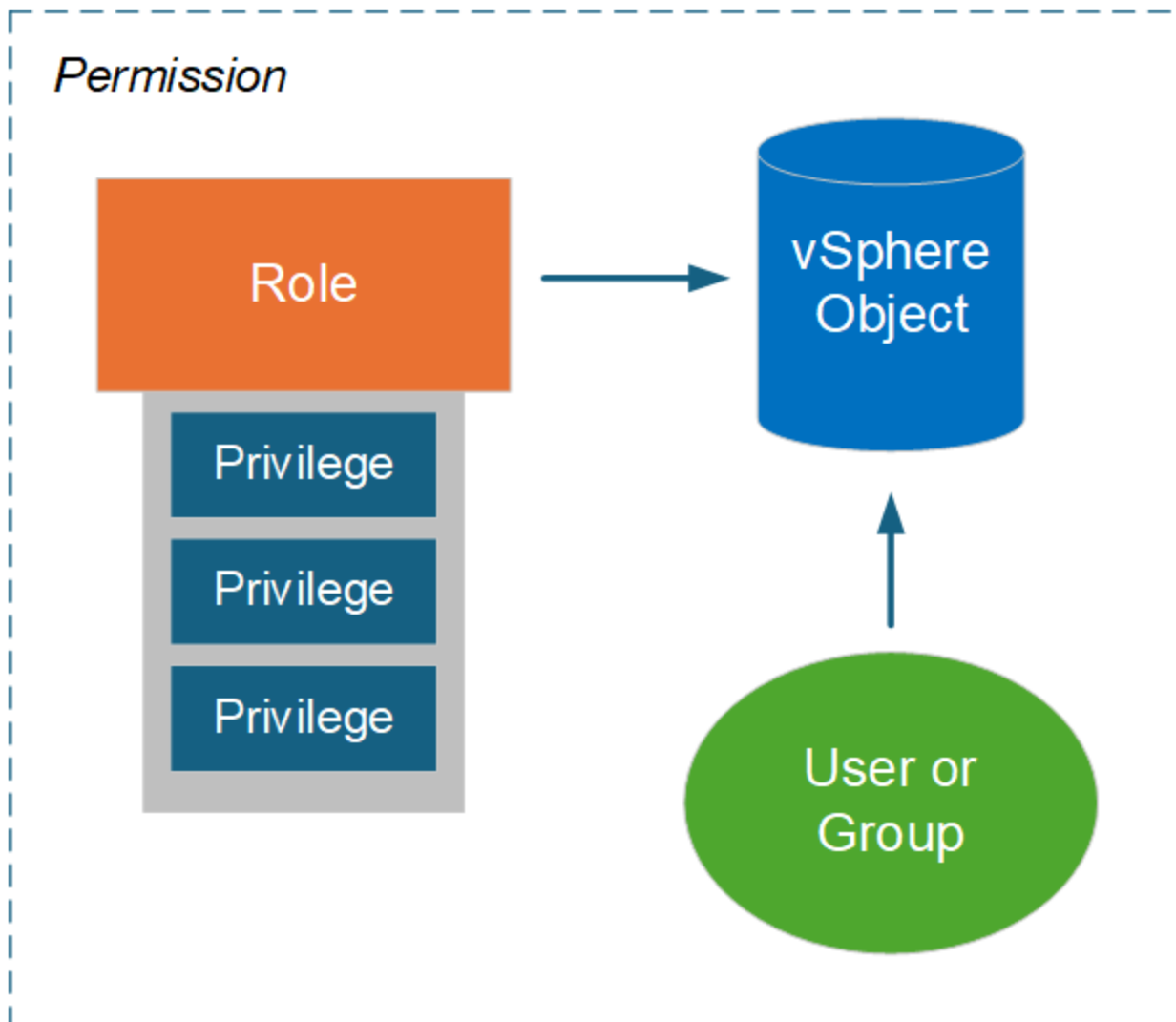
RBAC mit VMware vSphere

Wie vCenter Server-RBAC mit ONTAP tools funktioniert

VMware vCenter Server bietet eine RBAC-Funktion, die die Kontrolle des Zugriffs auf vSphere-Objekte ermöglicht. Dies ist ein wichtiger Bestandteil der zentralisierten Authentifizierungs- und Autorisierungsdienste von vCenter.

Illustration einer vCenter Server-Berechtigung

Eine Berechtigung bildet die Grundlage für die Durchsetzung der Zugriffskontrolle in der vCenter Server-Umgebung. Sie wird auf ein vSphere Objekt angewendet, wobei ein Benutzer oder eine Gruppe in der Berechtigungsdefinition enthalten ist. Eine schematische Darstellung einer vCenter Berechtigung ist in der folgenden Abbildung dargestellt.



Komponenten einer vCenter Server-Berechtigung

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

vSphere Objekte

Berechtigungen werden vSphere-Objekten wie dem vCenter Server, ESXi Hosts, virtuellen Maschinen, Datenspeichern, Rechenzentren und Ordnern zugeordnet. Basierend auf den einem Objekt zugewiesenen Berechtigungen bestimmt der vCenter Server, welche Aktionen oder Aufgaben von den einzelnen Benutzern oder Gruppen an diesem Objekt durchgeführt werden können. Für die spezifischen Aufgaben der ONTAP tools for VMware vSphere werden alle Berechtigungen auf der Stamm- oder Stammordner-Ebene des vCenter Server zugewiesen und validiert. Weitere Informationen sind unter ["RBAC mit vCenter Server verwenden"](#) zu finden.

Privileges und Rollen

Es gibt zwei Arten von vSphere-Privileges, die mit ONTAP tools for VMware vSphere 10 verwendet werden. Zur Vereinfachung der Arbeit mit RBAC in dieser Umgebung stellen die ONTAP tools Rollen mit den

erforderlichen nativen und benutzerdefinierten Privileges bereit. Zu den Privileges gehören:

- Native vCenter Server-Berechtigungen

Dies sind die von vCenter Server bereitgestellten Berechtigungen.

- ONTAP tools-spezifische Privileges

Dies sind benutzerdefinierte Privileges, die ausschließlich für ONTAP tools for VMware vSphere einzigartig sind.

Benutzer und Gruppen

Sie können Benutzer und Gruppen mithilfe von Active Directory oder der lokalen vCenter Server-Instanz definieren. In Kombination mit einer Rolle kann eine Berechtigung für ein Objekt in der vSphere Objekt-Hierarchie erstellt werden. Die Berechtigung gewährt Zugriff basierend auf den Privileges der zugehörigen Rolle. Zu beachten ist, dass Rollen nicht direkt isoliert Benutzern zugewiesen werden. Stattdessen erhalten Benutzer und Gruppen Zugriff auf ein Objekt durch Rollen-Privileges als Teil der umfassenderen vCenter Server-Berechtigung.

vCenter Server-RBAC-Überlegungen für ONTAP tools

Es gibt mehrere Aspekte der ONTAP tools for VMware vSphere 10 RBAC-Implementierung mit vCenter Server, die vor der Verwendung in einer Produktionsumgebung berücksichtigt werden sollten.

vCenter Rollen und das Administratorkonto

Sie müssen benutzerdefinierte vCenter Serverrollen nur dann definieren und verwenden, wenn der Zugriff auf die vSphere Objekte und die zugehörigen administrativen Aufgaben eingeschränkt werden soll. Wenn eine Zugriffsbeschränkung nicht erforderlich ist, kann stattdessen ein Administratorkonto verwendet werden. Jedes Administratorkonto ist mit der Administratorrolle auf oberster Ebene der Objekthierarchie definiert. Dies ermöglicht den vollständigen Zugriff auf die vSphere Objekte, einschließlich der von ONTAP tools for VMware vSphere 10 hinzugefügten Objekte.

vSphere Objekthierarchie

Das vSphere-Objektinventar ist in einer Hierarchie organisiert. Beispielsweise kann in der Hierarchie wie folgt nach unten navigiert werden:

vCenter Server → Datacenter → Cluster → ESXi host → Virtual Machine

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

Mit ONTAP tools for VMware vSphere 10 enthaltene Rollen

Um die Arbeit mit vCenter Server-RBAC zu vereinfachen, stellt ONTAP tools for VMware vSphere vordefinierte Rollen bereit, die auf verschiedene administrative Aufgaben zugeschnitten sind.



Sie können bei Bedarf neue benutzerdefinierte Rollen erstellen. Klonen Sie dazu eine der vorhandenen ONTAP tools-Rollen und bearbeiten Sie diese nach Bedarf. Nach den Konfigurationsänderungen müssen sich die betroffenen vSphere Client-Benutzer ausloggen und wieder anmelden, um die Änderungen zu aktivieren.

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

- Alarme
 - Alarm bestätigen
- Inhaltsbibliothek
 - Bibliothekselement hinzufügen
 - Vorlage einchecken
 - Eine Vorlage kann angesehen werden
 - Dateien herunterladen
 - Storage importieren
 - Lesespeicher
 - Bibliothekselement synchronisieren
 - Synchronisierung der abonnierten Bibliothek
 - Konfigurationseinstellungen anzeigen
- Datenspeicher
 - Speicherplatz zuweisen
 - Datenspeicher durchsuchen
 - Dateioperationen auf niedriger Ebene
 - Datei entfernen
 - Aktualisieren Sie die Dateien der virtuellen Maschine
 - Metadaten der virtuellen Maschine aktualisieren
- ESX Agent Manager
 - Anzeigen
- Ordner
 - Ordner erstellen
- Host
 - Konfiguration
 - Erweiterte Einstellungen
 - Einstellungen ändern
 - Netzwerkkonfiguration
 - Systemressourcen

- Konfiguration für den automatischen Start der virtuellen Maschine
- Lokale Operationen
 - Virtuelle Maschine erstellen
 - Virtuelle Maschine löschen
 - Virtuelle Maschine neu konfigurieren
- Netzwerk
 - Netzwerk zuweisen
 - Konfigurieren
- OvfManager
 - OvfConsumer Zugang
- Hostprofil
 - Anzeigen
- Ressource
 - Virtuelle Maschine einem Ressourcenpool zuweisen
- Geplante Aufgabe
 - Aufgaben erstellen
 - Aufgabe ändern
 - Aufgabe ausführen
- Aufgaben
 - Aufgabe erstellen
 - Aufgabe aktualisieren
- vApp
 - Virtuelle Maschine hinzufügen
 - Ressourcenpool zuweisen
 - Weisen Sie vApp zu
 - Erstellen
 - Importieren
 - Bewegen
 - Ausschalten
 - Einschalten
 - Aus URL abrufen
 - OVF-Umgebung anzeigen
- Virtuelle Maschine
 - 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 der virtuellen Maschine aktualisieren
- Inventar bearbeiten
 - Aus bestehendem erstellen
 - Neu erstellen
 - Bewegen
 - Anmeldung
 - Entfernen
 - Registrierung aufheben
- Interaktion
 - Sicherungsvorgang auf virtueller Maschine
 - CD-Medien konfigurieren
 - Diskettenmedien konfigurieren
 - Geräte verbinden
 - Konsoleninteraktion
 - Systemmanagement des Gastbetriebssystems über die VIX API
 - Ausschalten
 - Einschalten
 - Zurücksetzen
 - Aussetzen
- Bereitstellung
 - Festplattenzugriff zulassen
 - Klonvorlage
 - Gast anpassen
 - Bereitstellungsvorlage
 - Anpassungsspezifikation ändern
 - Anpassungsspezifikationen lesen
- Snapshot Verwaltung
 - Snapshot erstellen

- Snapshot entfernen
- Snapshot umbenennen
- Auf Snapshot zurücksetzen

Es gibt drei vordefinierte Rollen, wie unten beschrieben.

NetApp ONTAP tools für VMware vSphere Administrator

Stellt alle nativen vCenter Server-Berechtigungen und ONTAP tools-spezifischen Berechtigungen bereit, die für die Ausführung der zentralen ONTAP tools für VMware vSphere Administratortasken erforderlich sind.

NetApp ONTAP tools for VMware vSphere Schreibgeschützt

Gewährt Lesezugriff auf ONTAP tools. Diese Benutzer können keine ONTAP tools for VMware vSphere zugriffsbeschränkten Aktionen durchführen.

NetApp ONTAP tools für VMware vSphere Provision

Stellt einige der nativen vCenter Server-Privileges und ONTAP tools-spezifischen Privileges bereit, die für die Bereitstellung von Storage erforderlich sind. Folgende Aufgaben sind möglich:

- Neue Datenspeicher erstellen
- Datenspeicher verwalten

vSphere-Objekte und ONTAP Storage Backends

Die beiden RBAC-Umgebungen arbeiten zusammen. Bei der Ausführung einer Aufgabe in der vSphere Client-Oberfläche werden zunächst die für den vCenter Server definierten ONTAP tools Rollen geprüft. Wenn die Operation von vSphere erlaubt ist, werden anschließend die Privileges der ONTAP Rolle geprüft. Dieser zweite Schritt erfolgt auf Grundlage der ONTAP Rolle, die dem Benutzer bei der Erstellung und Konfiguration des Storage-Backends zugewiesen wurde.

Arbeiten mit vCenter Server-RBAC

Es gibt einige Aspekte, die bei der Arbeit mit den vCenter Server-Berechtigungen und -Rechten zu berücksichtigen sind.

Erforderliche Berechtigungen

Für den Zugriff auf die Benutzeroberfläche von ONTAP tools for VMware vSphere 10 müssen Sie über die für ONTAP tools spezifische Berechtigung „View“ verfügen. Wenn Sie sich ohne diese Berechtigung bei vSphere anmelden und auf das NetApp Symbol klicken, zeigt ONTAP tools for 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. Durch die Zuweisung der Ansichtsberechtigung zum Stammobjekt kann auf ONTAP tools for VMware vSphere zugegriffen werden, indem auf das NetApp-Symbol geklickt wird.

Alternativ kann die Ansichtsberechtigung einer anderen, niedrigeren vSphere Objektebene zugewiesen werden. Dies beschränkt jedoch die ONTAP tools for VMware vSphere Menüs, auf die zugegriffen und die verwendet werden können.

Berechtigungen zuweisen

Sie müssen vCenter Server-Berechtigungen verwenden, wenn Sie den Zugriff auf die vSphere-Objekte und Aufgaben einschränken möchten. Die Stelle, an der die Berechtigung in der vSphere-Objekthierarchie

zugewiesen wird, bestimmt, welche Aufgaben mit den ONTAP tools for VMware vSphere 10 von Benutzern durchgeführt werden können.



Sofern Sie keine restriktiveren Zugriffsrechte definieren müssen, ist es im Allgemeinen eine gute Vorgehensweise, Berechtigungen auf der Ebene des Stammobjekts oder des Stammordners zuzuweisen.

Die mit ONTAP tools for VMware vSphere 10 verfügbaren Berechtigungen gelten für benutzerdefinierte Nicht-vSphere-Objekte, wie zum Beispiel Speichersysteme. Nach Möglichkeit sollten diese Berechtigungen dem ONTAP tools for VMware vSphere Stammobjekt zugewiesen werden, da es kein vSphere-Objekt gibt, dem sie zugewiesen werden könnten. Beispielsweise sollte jede Berechtigung, die das Privileg „Speichersysteme hinzufügen/ändern/entfernen“ für ONTAP tools for VMware vSphere beinhaltet, auf Ebene des Stammobjekts zugewiesen werden.

Wenn eine Berechtigung auf einer höheren Ebene der Objekthierarchie definiert wird, kann diese so konfiguriert werden, dass sie an die untergeordneten Objekte weitergegeben und von diesen geerbt wird. Falls erforderlich, können den untergeordneten Objekten zusätzliche Berechtigungen zugewiesen werden, die die vom übergeordneten Objekt geerbten Berechtigungen überschreiben.

Sie können eine Berechtigung jederzeit ändern. Wenn Sie eine der Berechtigungen innerhalb einer Berechtigung ändern, müssen sich die Benutzer, denen diese Berechtigung zugeordnet ist, aus vSphere ausloggen und wieder anmelden, damit die Änderung wirksam wird.

RBAC mit ONTAP

Wie ONTAP RBAC mit ONTAP tools funktioniert

ONTAP bietet eine robuste und erweiterbare RBAC Umgebung. Die RBAC-Funktionalität ermöglicht die Steuerung des Zugriffs auf Speicher und Systemvorgänge, wie sie über die REST API und CLI bereitgestellt werden. Es ist hilfreich, mit der Umgebung vertraut zu sein, bevor sie mit einer ONTAP tools for VMware vSphere 10 Bereitstellung verwendet wird.

Überblick über die administrativen Optionen

Bei der Verwendung von ONTAP RBAC stehen je nach Ihrer Umgebung und Ihren Zielen verschiedene Optionen zur Verfügung. Nachfolgend ist ein Überblick über die wichtigsten administrativen Entscheidungen dargestellt. Siehe auch ["ONTAP Automatisierung: Überblick über die RBAC-Sicherheit"](#) für weitere Informationen.



ONTAP RBAC ist speziell für Speicherumgebungen entwickelt und einfacher als die mit dem vCenter Server bereitgestellte RBAC-Implementierung. Mit ONTAP wird die Rolle direkt dem Benutzer zugewiesen. Die Konfiguration expliziter Berechtigungen, wie sie mit dem vCenter Server verwendet werden, ist mit ONTAP RBAC nicht erforderlich.

Arten von Rollen und Privileges

Für die Definition eines ONTAP Benutzers ist eine ONTAP Rolle erforderlich. Es gibt zwei Arten von ONTAP Rollen:

- REST

Die REST-Rollen wurden mit ONTAP 9.6 eingeführt und werden im Allgemeinen auf Benutzer angewendet,

die über die REST-API auf ONTAP zugreifen. Die in diesen Rollen enthaltenen Privileges sind im Hinblick auf den Zugriff auf die ONTAP REST API-Endpunkte und die zugehörigen Aktionen definiert.

- Traditionell

Dies sind die Legacy-Rollen, die vor ONTAP 9.6 existierten. Sie sind weiterhin ein grundlegender Bestandteil von RBAC. Die Privileges werden anhand des Zugriffs auf die ONTAP CLI-Befehle definiert.

Obwohl die REST-Rollen erst vor Kurzem eingeführt wurden, bieten die traditionellen Rollen einige Vorteile. Beispielsweise können zusätzliche Abfrageparameter hinzugefügt werden, damit Privileges die Objekte, auf die sie angewendet werden, genauer definieren können.

Umfang

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

Rollendefinitionen

ONTAP bietet eine Reihe vordefinierter Rollen sowohl auf Cluster- als auch auf SVM-Ebene. Es besteht außerdem die Möglichkeit, benutzerdefinierte Rollen zu definieren.

Arbeiten mit ONTAP REST Rollen

Bei der Verwendung der mit ONTAP tools for VMware vSphere 10 enthaltenen ONTAP REST-Rollen sind mehrere Aspekte zu berücksichtigen.

Rollenzuordnung

Unabhängig davon, ob eine traditionelle Rolle oder eine REST-Rolle verwendet wird, werden alle ONTAP-Zugriffsentscheidungen auf Grundlage des zugrunde liegenden CLI-Befehls getroffen. Da die Privileges in einer REST-Rolle jedoch anhand der REST-API-Endpunkte definiert sind, muss ONTAP für jede REST-Rolle eine *zugeordnete* traditionelle Rolle erstellen. Daher ist jede REST-Rolle einer zugrunde liegenden traditionellen Rolle zugeordnet. Dies ermöglicht ONTAP, Zugriffskontrollentscheidungen unabhängig vom Rollentyp konsistent zu treffen. Die parallel zugeordneten Rollen können nicht geändert werden.

Definieren einer REST-Rolle mithilfe von CLI-Privileges

Da ONTAP die Zugriffsrechte grundsätzlich über CLI-Befehle festlegt, lässt sich eine REST-Rolle mithilfe von CLI-Befehlsberechtigungen anstelle von REST-Endpunkten definieren. Ein Vorteil dieses Ansatzes ist die zusätzliche Granularität der traditionellen Rollen.

Administrative Schnittstelle bei der Definition von ONTAP Rollen

Benutzer und Rollen können mit der ONTAP CLI und der REST API erstellt werden. Bequemer ist die Nutzung der System Manager Oberfläche zusammen mit der über den ONTAP tools Manager verfügbaren JSON-Datei. Siehe ["ONTAP RBAC mit ONTAP tools für VMware vSphere 10 verwenden"](#) für weitere Informationen.

ONTAP RBAC-Überlegungen für ONTAP tools

Es sind mehrere Aspekte der ONTAP tools for VMware vSphere 10 RBAC-Implementierung mit ONTAP zu berücksichtigen, bevor diese in einer Produktionsumgebung verwendet werden.

Überblick über den Konfigurationsprozess

ONTAP tools for VMware vSphere umfasst Unterstützung für die Erstellung eines ONTAP Benutzers mit einer benutzerdefinierten Rolle. Die Definitionen sind in einer JSON-Datei zusammengefasst, die in den ONTAP Cluster hochgeladen werden kann. Der Benutzer und die Rolle können entsprechend der jeweiligen Umgebung und Sicherheitsanforderungen erstellt und angepasst werden.

Die wichtigsten Konfigurationsschritte werden im Folgenden grob beschrieben. Weitere Details sind unter ["ONTAP Benutzerrollen und Privileges konfigurieren"](#) zu finden.

1. Vorbereiten

Sie benötigen Administratorrechte sowohl für den ONTAP tools Manager als auch für den ONTAP Cluster.

2. Die JSON-Definitionsdatei herunterladen

Nach der Anmeldung an der ONTAP tools Manager Benutzeroberfläche kann die JSON-Datei mit den RBAC-Definitionen heruntergeladen werden.

3. Einen ONTAP Benutzer mit einer Rolle erstellen

Nach der Anmeldung im System Manager können der Benutzer und die Rolle erstellt werden:

1. Links **Cluster** und dann **Einstellungen** auswählen.
2. Scrollen Sie nach unten zu **Benutzer und Rollen** und klicken Sie auf →.
3. Unter **Benutzer Hinzufügen** auswählen und dann **Virtualisierungsprodukte** auswählen.
4. Wählen Sie die JSON-Datei auf Ihrem lokalen Rechner aus und laden Sie sie hoch.

4. Die Rolle konfigurieren

Im Rahmen der Rollendefinition sind mehrere administrative Entscheidungen erforderlich. Siehe [Die Rolle wird mithilfe von System Manager konfiguriert](#). für weitere Details.

Die Rolle wird mithilfe von System Manager konfiguriert.

Nachdem Sie mit System Manager einen neuen Benutzer und eine neue Rolle erstellt und die JSON-Datei hochgeladen haben, kann die Rolle an Ihre Umgebung und Bedürfnisse angepasst werden.

Kernbenutzer und Rollenkonfiguration

Die RBAC-Definitionen sind in verschiedenen Produktfunktionen zusammengefasst, darunter Kombinationen aus VSC, VASA Provider und SRA. Die Umgebung oder Umgebungen, in denen RBAC-Unterstützung benötigt wird, sollten ausgewählt werden. Wenn beispielsweise Rollen die Remote Plug-in-Funktion unterstützen sollen, ist VSC auszuwählen. Auch der Benutzername und das zugehörige Passwort müssen ausgewählt werden.

Privileges

Die Rollenberechtigungen sind in vier Gruppen unterteilt, basierend auf dem für ONTAP Storage benötigten Zugriffsniveau. Die den Rollen zugrunde liegenden Privileges umfassen:

- Entdeckung

Diese Rolle ermöglicht es Ihnen, Speichersysteme hinzuzufügen.

- Speicher erstellen

Diese Rolle ermöglicht Ihnen das Erstellen von Storage. Sie umfasst außerdem alle Privileges, die mit der

Discovery-Rolle verbunden sind.

- Speicher ändern

Diese Rolle ermöglicht Ihnen, Speicher zu ändern. Sie umfasst außerdem alle Privileges, die mit den Rollen „Speicher ermitteln“ und „Speicher erstellen“ verbunden sind.

- Speicher zerstören

Diese Rolle ermöglicht Ihnen, Speicher zu zerstören. Sie umfasst außerdem alle Privileges, die mit den Rollen „Speicher ermitteln“, „Speicher erstellen“ und „Speicher ändern“ verbunden sind.

Den Benutzer mit einer Rolle generieren

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

- Konstanter Präfixwert, der in der JSON-Datei definiert ist (zum Beispiel "OTV_10")
- Die 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.

ONTAP tools für VMware vSphere bereitstellen

Schnellstart für ONTAP tools für VMware vSphere

ONTAP tools für VMware vSphere lassen sich mit diesem Schnellstartabschnitt einrichten.

Zunächst sind diese Kernaufgaben abzuschließen, damit ONTAP tools für das Management und die Bereitstellung am Tag 0 betriebsbereit sind. Danach folgen die optionalen Aufgaben, abhängig von Ihrer Umgebung und den Schutzanforderungen.

Zunächst wird ONTAP tools for VMware vSphere als kleine Einzelknoten-Konfiguration bereitgestellt, die Kerndienste zur Unterstützung von NFS- und VMFS-Datenspeichern bietet. Für eine Erweiterung der Konfiguration um zusätzliche Container pro Dienst, erhöhte Ausfallsicherheit oder die Nutzung von vVols Datenspeichern und Hochverfügbarkeit (HA) ist zunächst dieser Workflow abzuschließen, bevor die Erweiterungsschritte erfolgen. Weitere Informationen sind in der ["HA Bereitstellungsworkflow"](#) zu finden.

1

Planung Ihrer Bereitstellung

Bestätigen Sie, dass Ihre Umgebung für eine unterstützte Bereitstellung bereit ist. Überprüfen Sie, ob Ihre vSphere-, ONTAP- und ESXi-Hostversionen mit der ONTAP tools Version kompatibel sind. Es sollte ausreichend CPU-, Arbeitsspeicher- und Festplattenspeicher zugewiesen werden. Abhängig von Ihren Sicherheitsrichtlinien kann es erforderlich sein, Firewalls oder andere Sicherheitstools einzurichten, um Netzwerkverkehr zuzulassen.

Es ist sicherzustellen, dass der vCenter Server installiert und erreichbar ist.

- ["Interoperabilitätsmatrix-Tool"](#)
- ["ONTAP tools für VMware vSphere Anforderungen und Konfigurationsgrenzen"](#)
- ["Bevor Sie beginnen"](#)

2

ONTAP tools für VMware vSphere bereitstellen

Die ONTAP tools Appliance wird bereitgestellt, um Basisdienste für NFS und VMFS Datenspeicher bereitzustellen.

Zunächst wird ONTAP tools for VMware vSphere als kleine Einzelknotenkonfiguration bereitgestellt. Falls die Konfiguration auf die Nutzung von vVols Datenspeichern und Hochverfügbarkeit (HA) erweitert werden soll, geschieht dies nach Abschluss dieses Workflows. Für die Erweiterung auf eine HA-Konfiguration ist sicherzustellen, dass CPU-Hot-Add und Memory-Hot-Plug aktiviert sind.

Während der Bereitstellung sollten die Felder **Vorlage anpassen** sorgfältig geprüft werden, insbesondere Hostname, Verwendung der ONTAP tools IP-Adresse und DNS-Anforderungen.

- ["ONTAP tools für VMware vSphere bereitstellen"](#)

3

Registrierung und Installation des vCenter Client-Plug-ins

Eine vCenter Server-Instanz wird hinzugefügt, um das vCenter Client-Plug-in zu registrieren und die

erforderlichen Berechtigungen und Rollen anzuwenden. Beim Hinzufügen einer vCenter Server-Instanz registrieren die ONTAP tools das Remote-Plug-in, wenden benutzerdefinierte Plug-in- und API-Berechtigungen an, erstellen benutzerdefinierte Rollen und fügen eine Plug-in-Verknüpfung in der vSphere Benutzeroberfläche hinzu.

- ["Fügen Sie vCenter Serverinstanzen zu ONTAP tools hinzu"](#)

4

Die Storage-Backends konfigurieren

ONTAP-Speicherressourcen werden verbunden, damit ONTAP tools Datenspeicher bereitstellen und verwalten kann. Ein Storage-Backend wird zu einem ONTAP Cluster hinzugefügt. In mandantenfähigen Umgebungen, in denen ein vCenter Server einer Tenant-SVM zugeordnet ist, wird ONTAP tools Manager verwendet, um den Cluster hinzuzufügen. Anschließend wird das Storage-Backend dem vCenter Server zugeordnet, um eine globale Zuordnung für diese vCenter Instanz zu erstellen.

Die lokalen Storage-Backends werden mit Cluster- oder SVM-Anmeldeinformationen über die ONTAP tools Benutzeroberfläche hinzugefügt. Diese Storage-Backends sind auf ein einzelnes vCenter beschränkt. Bei lokaler Verwendung von Cluster-Anmeldeinformationen werden die zugehörigen SVMs automatisch dem vCenter zugeordnet, um vVols oder VMFS zu verwalten. Für die VMFS-Verwaltung, einschließlich SRA, unterstützen die ONTAP tools SVM-Anmeldeinformationen, ohne dass ein globaler Cluster erforderlich ist.

- ["Ein Storage-Backend hinzufügen"](#)
- ["Das Storage-Backend mit einer vCenter Server-Instanz verknüpfen"](#)

Optionale nächste Aufgaben

1

ONTAP Benutzerrollen und -Berechtigungen konfigurieren

Benutzerdefinierte ONTAP-Rollen für den Zugriff nach dem Prinzip der minimalen Berechtigungen anstelle des standardmäßigen Administratorkontos konfigurieren.

- ["ONTAP Benutzerrollen und Privileges konfigurieren"](#)

2

Zertifikate für mehrere vCenter Server-Instanzen aktualisieren

Zertifikate werden aktualisiert, um eine vertrauenswürdige, zertifikatsbasierte Kommunikation über mehrere vCenter Server-Instanzen hinweg zu ermöglichen.

- ["Zertifikate verwalten"](#)

3

SRA-Schutz konfigurieren

Die SRA-Funktion ermöglicht das Einrichten von Notfallwiederherstellungsschutz für NFS- und VMFS-Datenspeicher.

- ["ONTAP tools für VMware vSphere Dienste aktivieren"](#)
- ["SRA auf der VMware Live Site Recovery Appliance konfigurieren"](#)

4

Aktiver SnapMirror Active Sync-Schutz

Hostclusterschutz mit SnapMirror active sync einrichten, um VMFS-Datenspeicher zu schützen. In ONTAP-Systemen den erforderlichen Cluster und die SVM koppeln und anschließend den Hostclusterschutz in ONTAP tools for VMware vSphere konfigurieren. Diese Option gilt nur für VMFS-Datenspeicher.

- ["Schutz mithilfe von Host-Cluster-Schutz"](#)

5

Backup und Recovery für Ihre ONTAP tools Bereitstellung einrichten

Backup und Recovery einrichten, um die ONTAP tools Konfiguration zu schützen und eine schnelle Wiederherstellung nach Ausfällen zu ermöglichen.

Die Datensicherung ist in ONTAP tools for VMware vSphere 10.5 standardmäßig aktiviert und erfolgt alle 10 Minuten. Backups der ONTAP tools for VMware vSphere Installation können so geplant werden, dass die Wiederherstellung der Installation im Fehlerfall möglich ist.

- ["Die Sicherungseinstellungen bearbeiten"](#)
- ["Wiederherstellung der ONTAP tools Konfiguration"](#)

Workflow für die Hochverfügbarkeitsbereitstellung von ONTAP tools

Um die Ausfallsicherheit zu erhöhen und mehr Container pro Dienst zu unterstützen, kann die ursprüngliche ONTAP tools Bereitstellung auf eine Hochverfügbarkeitskonfiguration (HA) erweitert werden. Die Aktivierung des VASA Provider Dienstes ist für vVols Datenspeicher in einer HA-Konfiguration erforderlich.

1

Die Bereitstellung skalieren

Die ONTAP tools for VMware vSphere Konfiguration kann skaliert werden, um die Anzahl der Knoten in der Bereitstellung zu erhöhen und die Konfiguration auf eine HA-Konfiguration umzustellen.

- ["Konfiguration der ONTAP tools for VMware vSphere ändern"](#)

2

Dienste aktivieren

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

Die SRA-Dienste werden aktiviert, damit ONTAP tools Storage Replication Adapter (SRA) für VMware Site Recovery Manager (SRM) oder VMware Live Site Recovery (VLSR) verwendet werden kann.

- ["VASA Provider und SRA Services aktivieren"](#)

3

Zertifikate aktualisieren

Wenn Sie vVol Datenspeicher mit mehreren vCenter Serverinstanzen verwenden, sollte das selbstsignierte Zertifikat durch ein von einer Zertifizierungsstelle (CA) signiertes Zertifikat ersetzt werden.

- "Zertifikate verwalten"

ONTAP tools für VMware vSphere Anforderungen und Konfigurationsgrenzen

Vor der Bereitstellung der ONTAP tools für VMware vSphere sollten die Speicherplatzanforderungen für das Bereitstellungspaket sowie einige grundlegende Anforderungen an das Hostsystem bekannt sein.

Sie können ONTAP tools für VMware vSphere mit VMware vCenter Server Virtual Appliance (vCSA) verwenden. Sie sollten ONTAP tools für VMware vSphere in einer unterstützten vSphere Umgebung bereitstellen, die ESXi-Hosts umfasst.

Systemvoraussetzungen

- **Speicherplatzbedarf für das Installationspaket pro Knoten**
 - 15 GB für Thin Provisioned-Installationen
 - 348 GB für Installationen mit Thick Provisioning
- **Anforderungen an die Dimensionierung des Hostsystems** Die folgende Tabelle zeigt den empfohlenen Arbeitsspeicher für jede Bereitstellungsgröße. Für Hochverfügbarkeitsbereitstellungen (HA) ist die dreifache Appliance-Größe erforderlich.

Art der Bereitstellung	CPUs pro Knoten	Speicher (GB) pro Knoten	Festplattenspeicher (GB) Thick Provisioned pro Node
Klein	9	18	350
Mittel	13	26	350
Großer HINWEIS: Die große Bereitstellung ist nur für die HA-Konfiguration vorgesehen.	17	34	350



Wenn die Datensicherung aktiviert ist, benötigt jeder ONTAP tools Cluster zusätzliche 50 GB Speicherplatz auf dem Datenspeicher, auf dem die VMs bereitgestellt sind. Daher erfordert Non-HA insgesamt 400 GB und HA insgesamt 1100 GB Speicherplatz.

Minimale Storage- und Applikationsanforderungen

Speicher, Host und Applikationen	Versionsanforderungen
ONTAP	9.15.1, 9.16.1 und 9.17.0
ONTAP tools unterstützte ESXi Hosts	7.0.3 und höher
ONTAP tools unterstützte vCenter Server	7.0U3 und höher
VASA Provider	3,0
OVA Anwendung	10,5

Speicher, Host und Applikationen	Versionsanforderungen
ESXi Host zur Bereitstellung der ONTAP tools virtuellen Maschine	7.0U3 und 8.0U3
vCenter Server zur Bereitstellung der ONTAP tools Virtual Machine	7.0 und 8.0



Ab ONTAP tools for VMware vSphere 10.4 wird die Hardware der virtuellen Maschine von Version 10 auf 17 geändert.

Das Interoperability Matrix Tool (IMT) enthält die aktuellsten Informationen zu den unterstützten Versionen von ONTAP, vCenter Server, ESXi Hosts und Plug-in-Anwendungen.

["Interoperabilitätsmatrix-Tool"](#)

Port-Anforderungen

Die folgende Tabelle beschreibt die von NetApp verwendeten Netzwerkports und deren Zweck. Es gibt drei verschiedene Porttypen:

- **Externe Ports:** Diese Ports sind von außerhalb des Kubernetes-Clusters oder Knotens zugänglich. Sie ermöglichen Diensten die Kommunikation mit externen Netzwerken oder Benutzern und damit die Integration mit Systemen außerhalb der Clusterumgebung.
- **Inter-node-Ports:** Diese Ports ermöglichen die Kommunikation zwischen den Knoten innerhalb des Kubernetes-Clusters. Sie sind für Clusteraufgaben wie das Teilen von Daten und die Zusammenarbeit erforderlich. Bei Einzelknoten-Bereitstellungen werden Inter-node-Ports nur innerhalb des Knotens verwendet und benötigen keinen externen Zugriff. Inter-node-Ports können Datenverkehr von außerhalb des Clusters empfangen. Inter-node-Ports sollten mit Firewall-Regeln vom Internetzugriff abgeschirmt werden.
- **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.



Alle ONTAP tools-Knoten sollten sich im selben Subnetz befinden, um eine unterbrechungsfreie Kommunikation untereinander sicherzustellen.

Zum Ein- oder Ausblenden der Tabelle mit den Portanforderungen klicken.

Dienst-/Komponentenname	Port	Protokoll	Anschlusstyp	Beschreibung
ntv-gateway-svc (LB)	443, 8443	TCP	Extern	Durchleitungsport für eingehende Kommunikation für den VASA Provider Service. Das selbstsignierte Zertifikat des VASA Provider und das benutzerdefinierte CA-Zertifikat werden auf diesem Port 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	Network Time Protocol (NTP) zur Zeitsynchronisation.
etcd	2379, 2380, 2381	TCP	Zwischenknoten	Schlüsselwertspeicher für Clusterdaten.

Dienst-/Komponentenna me	Port	Protokoll	Anschlusstyp	Beschreibung
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
calico-node	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 den Pods über die Knoten hinweg, eine Blockierung unterbricht die Netzwerkverbindung zwischen den Knoten.

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
Nicht-HA	Klein (S)	bis zu 12K	32
Nicht-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 Small	200	80	32
Nicht-HA Medium	250	100	32
HA Small	350	200	64
HA Medium	600	200	128
HA Large	1024	250	256

ONTAP tools für VMware vSphere Storage Replication Adapter (SRA)

Die folgende Tabelle zeigt die unterstützten Zahlen pro VMware Live Site Recovery Instanz bei Verwendung von ONTAP tools for VMware vSphere.

vCenter Bereitstellungsgröße	Klein	Mittel
Gesamtzahl der für den Schutz mittels Array-basierter Replikation konfigurierten virtuellen Maschinen	2000	5000
Gesamtzahl der arraybasierten Replikationsschutzgruppen	250	250
Gesamtzahl der Schutzgruppen pro Wiederherstellungsplan	50	50

vCenter Bereitstellungsgröße	Klein	Mittel
Anzahl der replizierten Datenspeicher	255	255
Anzahl der VMs	4000	7000

Die folgende Tabelle zeigt die Anzahl der VMware Live Site Recovery-Instanzen und die entsprechenden ONTAP tools für VMware vSphere-Bereitstellungsgröße.

Anzahl der VMware Live Site Recovery Instanzen	ONTAP tools Bereitstellungsgröße
Bis zu 4	Klein
4 bis 8	Mittel
Mehr als 8	Groß

Weitere Informationen finden Sie unter ["Betriebsgrenzen von VMware Live Site Recovery"](#).

Anforderungen vor der Bereitstellung von ONTAP tools

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

Anforderungen	Ihr Status
vSphere Version, ONTAP Version und ESXi Host Version sind mit der ONTAP tools Version kompatibel.	☐ Ja ☐ Nein
vCenter Server-Umgebung ist eingerichtet und konfiguriert	☐ Ja ☐ Nein
Der Browsercache wurde gelöscht.	☐ Ja ☐ Nein
Sie verfügen über die Anmeldeinformationen des übergeordneten vCenter Servers.	☐ Ja ☐ Nein
Sie verfügen über die Anmeldeinformationen für die vCenter Serverinstanz, mit der sich die ONTAP tools for VMware vSphere nach der Bereitstellung zur Registrierung verbinden.	☐ Ja ☐ Nein
Der Domänenname, auf dem das Zertifikat ausgestellt ist, wird in einer Multi-vCenter-Bereitstellung, in der benutzerdefinierte CA-Zertifikate obligatorisch sind, der virtuellen IP-Adresse zugeordnet.	☐ Ja ☐ Nein
Sie haben die nslookup-Prüfung für den Domainnamen durchgeführt, um zu überprüfen, ob die Domain auf die beabsichtigte IP-Adresse aufgelöst wird.	☐ Ja ☐ Nein
Das Zertifikat wird mit dem Domännennamen und der IP-Adresse der ONTAP tools erstellt.	☐ Ja ☐ Nein
ONTAP tools Anwendung und interne Dienste sind vom vCenter Server aus erreichbar.	☐ Ja ☐ Nein

Anforderungen	Ihr Status
Bei der Verwendung von mandantenfähigen SVMs gibt es auf jeder SVM eine SVM-Management-LIF.	☐ Ja ☐ Nein

Bereitstellungsarbeitsblatt

Für die Bereitstellung auf einem einzelnen Knoten

Verwenden Sie das folgende Arbeitsblatt, um die erforderlichen Informationen für ONTAP tools for VMware vSphere Erstbereitstellung zu sammeln:

Anforderung	Ihr Wert
IP-Adresse für die ONTAP tools Anwendung. Dies ist die IP-Adresse für den Zugriff auf die ONTAP tools Manager Managementoberfläche (Load Balancer) unter <code>https://<ip>:8443/virtualization/ui/</code>	
Virtuelle IP-Adresse von ONTAP tools für interne Kommunikation. Diese IP-Adresse wird für die interne Kommunikation in einem Setup mit mehreren ONTAP tools Instanzen verwendet. Diese IP-Adresse sollte nicht dieselbe sein wie die IP-Adresse für die ONTAP tools Anwendung. (Die Kubernetes Control Plane)	
DNS-Hostname für den ONTAP tools Management-Node	
Primärer DNS-Server	
Sekundärer DNS-Server	
DNS-Suchdomäne	
IPv4-Adresse für den ONTAP tools Verwaltungsknoten. Es ist eine eindeutige IPv4-Adresse für die Managementoberfläche des Knotens im Managementnetzwerk. Diese wird verwendet, um eine Verbindung zur ONTAP tools Appliance für den Remote-Diagnosezugriff über SSH herzustellen.	
Subnetzmaske für die IPv4-Adresse	
Standardgateway 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. Ordnen Sie diese vor der Vergabe von Hostnamen den freien IP-Adressen im DNS zu. Alle IP-Adressen müssen sich im selben VLAN befinden, das für die Bereitstellung ausgewählt wurde.

Für High availability (HA) Deployment

Zusätzlich zu den Anforderungen für die Bereitstellung auf einem einzelnen Knoten werden für die HA-Bereitstellung die folgenden Informationen benötigt:

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

Netzwerk Firewall-Konfiguration

Stellen Sie sicher, dass die erforderlichen Firewall-Ports für alle relevanten IP-Adressen geöffnet sind. ONTAP tools benötigen Zugriff auf die LIF über Port 443. Eine vollständige Liste der erforderlichen Ports befindet sich im Abschnitt Portanforderungen unter ["ONTAP tools für VMware vSphere Anforderungen und Konfigurationsgrenzen"](#).

ONTAP Speichereinstellungen

Für eine nahtlose Integration von ONTAP Storage mit ONTAP tools for VMware vSphere sind die folgenden Einstellungen zu berücksichtigen:

- Wenn Sie Fibre Channel (FC) für die Speicherkonnektivität verwenden, sollte die Zonierung auf den FC-Switches so konfiguriert werden, dass die ESXi-Hosts mit den FC-LIFs der SVM verbunden sind.
["Informationen zu FC- und FCoE-Zoning mit ONTAP Systemen"](#)
- Um von ONTAP tools verwaltete SnapMirror Replikation zu verwenden, sollte der ONTAP Storage-Administrator ["ONTAP Cluster Peer-Beziehungen"](#) und ["ONTAP Intercluster SVM Peer-Beziehungen"](#) in ONTAP erstellen, bevor SnapMirror verwendet wird.

ONTAP tools bereitstellen

Das ONTAP tools for VMware vSphere Appliance wird als kleiner Einzelknoten mit Kerndiensten zur Unterstützung von NFS- und VMFS-Datenspeichern bereitgestellt. Der Bereitstellungsprozess der ONTAP tools kann bis zu 45 Minuten dauern.

Bevor Sie beginnen

Bei der Bereitstellung eines kleinen einzelnen Knotens ist eine Inhaltsbibliothek optional. Für Bereitstellungen mit mehreren Knoten oder Hochverfügbarkeit ist eine Inhaltsbibliothek erforderlich. In VMware speichert eine Inhaltsbibliothek VM-Vorlagen, vApp-Vorlagen und andere Dateien. Die Bereitstellung mit einer Inhaltsbibliothek bietet eine nahtlose Erfahrung, da sie nicht von der Netzwerkverbindung abhängig ist.

Vor dem Erstellen einer Inhaltsbibliothek ist Folgendes zu beachten:

- Die Bibliothek sollte auf einem gemeinsam genutzten Datenspeicher erstellt werden, sodass alle Hosts im Cluster darauf zugreifen können.
- Die Inhaltsbibliothek sollte eingerichtet werden, bevor die ONTAP tools for VMware vSphere OVA bereitgestellt wird.
- Die Bibliothek muss erstellt sein, bevor das Gerät für HA konfiguriert wird.



Die OVA-Vorlage sollte nach der Bereitstellung nicht aus der Inhaltsbibliothek gelöscht werden.



Um zukünftig eine HA-Bereitstellung zu ermöglichen, vermeiden Sie die direkte Bereitstellung der virtuellen Maschine der ONTAP tools direkt auf einem ESXi-Host. Stellen Sie sie stattdessen innerhalb eines ESXi-Host-Clusters oder Ressourcenpools bereit.

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

1. Laden Sie die Datei herunter, die die Binärdateien (.ova) und signierten Zertifikate für ONTAP tools for VMware vSphere von der ["NetApp Support Site"](#) enthält.
2. Melden Sie sich beim vSphere Client an.
3. Das vSphere Client-Menü auswählen und **Inhaltsbibliotheken** auswählen.
4. Rechts auf der Seite befindet sich die Option **Erstellen**.
5. Einen Namen für die Bibliothek angeben und die Inhaltsbibliothek erstellen.
6. Wechseln Sie zur von Ihnen erstellten Inhaltsbibliothek.
7. Wählen Sie auf der rechten Seite **Aktionen**, dann **Element importieren** 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 auf „Konservativ“ ein. Dadurch wird sichergestellt, dass VMs während der Installation nicht migriert werden.

Die ONTAP tools für VMware vSphere werden zunächst als Nicht-HA-Setup bereitgestellt. Um auf eine HA-Bereitstellung zu skalieren, müssen Sie das CPU-Hot-Add und das Memory-Hot-Plug aktivieren. Sie können diesen Schritt als Teil des Bereitstellungsprozesses durchführen oder die VM-Einstellungen nach der Bereitstellung bearbeiten.

Schritte

1. Laden Sie die Datei herunter, die die Binärdateien (.ova) und signierten Zertifikate für die ONTAP tools for VMware vSphere von der ["NetApp Support Site"](#) enthält. Wenn die OVA-Datei bereits in die Inhaltsbibliothek importiert wurde, kann dieser Schritt übersprungen und mit dem nächsten Schritt fortgefahren werden.
2. Melden Sie sich am vSphere Server an.
3. Zum Ressourcenpool, Cluster oder Host wechseln, auf dem die OVA bereitgestellt werden soll.



Speichern Sie die ONTAP tools for VMware vSphere Virtual Machine niemals auf vVols Datenspeichern, die sie verwaltet.

4. Sie können die OVA aus der Bibliothek oder vom lokalen System bereitstellen.

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

5. Im Feld **Name und Ordner auswählen** den Namen der virtuellen Maschine eingeben und den Speicherort auswählen.

- Wenn Sie die vCenter Server 8.0.3 Version verwenden, wählen Sie die Option **Hardware dieser virtuellen Maschine anpassen**, wodurch ein zusätzlicher Schritt namens **Hardware anpassen** aktiviert wird, bevor Sie zum Fenster **Bereit zum Abschließen** gelangen.
- Wenn Sie die vCenter Server Version 7.0.3 verwenden, befolgen Sie die Schritte im Abschnitt **Was kommt als Nächstes?** am Ende der Bereitstellung.

netapp-ontap-tools-for-vmware-vsphere-10.5-1740090540 - New Virtual Machine from Content Library

- 1 Select a creation type
- 2 Select a template
- 3 Select a name and folder
- 4 Select a compute resource
- 5 Review details
- 6 Select storage
- 7 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: demootv

Select a location for the virtual machine.

- vcf-vc01.ontappmtme.openenglab.netapp.com
 - Raleigh

- ☐ Customize the operating system
- ☐ Customize this virtual machine's hardware

CANCEL

BACK

NEXT

6. Eine Computerressource auswählen und auf **Weiter** klicken. Optional das Kontrollkästchen **Bereitgestellte VM automatisch einschalten** aktivieren.

7. Die Details der Vorlage werden angezeigt, anschließend ist **Weiter** auszuwählen.

8. Die Lizenzvereinbarung muss gelesen und akzeptiert werden, anschließend ist **Weiter** auszuwählen.

9. Den Speicher für die Konfiguration und das Festplattenformat auswählen und **Weiter** wählen.
10. Für jedes Quellnetzwerk das Zielnetzwerk auswählen und **Weiter** wählen.
11. Im Fenster **Vorlage anpassen** füllen Sie die erforderlichen Felder aus.

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template**
- Customize hardware
- Ready to complete

Customize template

ONTAP tools IP address

ONTAP tools virtual IP address*

vCenter Server configuration for ONTAP tools deployment 3 settings

vCenter Server hostname*

vCenter Server username (user@domain.com)*

vCenter Server password*

ONTAP tools uses this IP address for internal communication

Enter the hostname of the target vCenter Server for ONTAP tools deployment.

Enter the user principal name of the vCenter Server account (for example, username@vsphere.local).
backup@vsphere.local

Enter the vCenter Server password to authenticate your login.

Password

Confirm Password

CANCEL BACK NEXT

Die Werte auf der Seite **Vorlage anpassen** sind für eine erfolgreiche Bereitstellung erforderlich.

Achten Sie besonders auf diese Felder:



- **Host name:** Geben Sie den Hostnamen der ONTAP tools VM ein. Ein gültiges Hostnamenformat ist zu verwenden.
- **ONTAP tools IP-Adresse:** Dies ist die primäre Managementoberfläche für den Zugriff auf ONTAP tools.
- **IPv4-Adresse:** Dies ist die Knoten-IP-Adresse, die für den Zugriff auf die Diagnoseschale und per SSH zur Fehlerbehebung und Wartung verwendet wird.

Wenn Sie DNS-Namen für den Host oder vCenter verwenden, muss sichergestellt sein, dass diese Namen im DNS korrekt aufgelöst werden.



Der vCenter Hostname ist der Name der vCenter Serverinstanz, auf der die ONTAP tools Appliance bereitgestellt ist.

Wenn Sie ONTAP tools in einer Zwei-vCenter-Server-Topologie bereitstellen – 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 die für die OVF-Vorlagenbereitstellung erforderlichen Berechtigungen besitzt. Weitere Informationen finden Sie in der Liste der Rollen ["Mit ONTAP tools for VMware vSphere 10 enthaltene Rollen"](#).

Für die vCenter Instanz, die von ONTAP tools verwaltet wird, muss das vCenter Benutzerkonto über Administratorrechte verfügen.

- Hostnamen müssen Buchstaben (A-Z, a-z), Ziffern (0-9) und Bindestriche (-) enthalten. Für die Konfiguration von Dual Stack ist der Hostname anzugeben, der der IPv6-Adresse zugeordnet ist.



Reines IPv6 wird nicht unterstützt. Gemischter Modus wird unterstützt, wenn das VLAN sowohl IPv6- als auch IPv4-Adressen enthält.

- Die IP-Adresse der ONTAP tools ist die primäre Schnittstelle für die Kommunikation mit ONTAP tools.
- IPv4 ist die IP-Adresskomponente der Knotenkonfiguration, die genutzt werden kann, um den Zugriff auf die Diagnose-Shell und SSH auf dem Knoten zum Zwecke der Fehlersuche und Wartung zu ermöglichen.

12. Bei Verwendung der vCenter Serverversion 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.

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

- 1 Select a name and folder
- 2 Select a compute resource
- 3 Review details
- 4 License agreements
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Customize hardware**
- 9 Ready to complete

Customize hardware

Configure the virtual machine hardware

Virtual Hardware VM Options Advanced Parameters

ADD NEW DEVICE ▾

▼ CPU * 9 ⓘ

Cores per Socket 1 ▾
Sockets: 9

CPU Hot Plug ☒ Enable CPU Hot Add

Reservation 10305 ▾ MHz ▾

Limit Unlimited ▾ MHz ▾

Shares Normal ▾ 1000 ▾

Hardware virtualization ☐ Expose hardware assisted virtualization to the guest OS

Performance Counters ☐ Enable virtualized CPU performance counters

Scheduling Affinity ⓘ

CANCEL BACK NEXT

netapp-ontap-tools-for-vmware-vsphere-10.5-1773361740 - New Virtual Machine from Content Library

- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks
- Customize template
- Customize hardware**
- Ready to complete

Customize hardware

Limit

Unlimited

MB

Shares

Normal

1000

Hardware virtualization

☐

Expose hardware assisted virtualization to the guest OS

Performance Counters

☐

Enable virtualized CPU performance counters

Scheduling Affinity

I/O MMU

☐

Enabled

Memory *

18

GB

Reservation

9

GB

☐

Reserve all guest memory (All locked)

Limit

Unlimited

MB

Shares

Normal

368640

Memory Hot Plug

☒

Enable

Hard disks *

5 total | 348 GB

CANCEL

BACK

NEXT

13. Die Details im Fenster **Bereit zum Abschließen** können überprüft und mit **Fertigstellen** abgeschlossen werden.

Während der Bereitstellungsaufgabe erstellt wird, wird der Fortschritt in der vSphere Aufgabenleiste angezeigt.

14. Die VM wird nach Abschluss der Aufgabe eingeschaltet, wenn die Option zum automatischen Einschalten der VM nicht ausgewählt wurde.

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

Wenn es Unstimmigkeiten im OVF-Formular gibt, fordert ein Dialogfeld zur Korrekturmaßnahme auf. Mit der Tabulatortaste kann navigiert, die erforderlichen Änderungen vorgenommen und **OK** ausgewählt werden. Es stehen drei Versuche zur Verfügung, um etwaige Probleme zu beheben. Wenn nach drei Versuchen weiterhin Probleme bestehen, wird der Installationsprozess gestoppt und es wird empfohlen, die Installation auf einer neuen virtuellen Maschine zu wiederholen.

Was kommt als Nächstes?

Wenn Sie ONTAP tools für VMware vSphere mit vCenter Server 7.0.3 bereitgestellt haben, befolgen Sie nach der Bereitstellung diese Schritte.

- Melden Sie sich beim vCenter Client an.
- Den ONTAP tools Node ausschalten.
- Gehen Sie zur ONTAP tools for VMware vSphere Virtual Machine unter **Inventare** und wählen Sie die Option **Einstellungen bearbeiten**.
- Unter den **CPU**-Optionen das Kontrollkästchen **CPU-Hot-Add aktivieren** aktivieren
- Unter den **Speicher**-Optionen das Kontrollkästchen **Aktivieren** bei **Speicher-Hot-Plug** aktivieren.

Fehler bei der Bereitstellung von ONTAP tools beheben

Wenn Bereitstellungsprobleme auftreten, sollten die Protokolle und Fehlercodes überprüft werden, um Probleme zu diagnostizieren und zu beheben. Ab ONTAP tools for VMware vSphere 10.5 enthalten 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 bestehenden ONTAP tools Serviceprotokollen bereitgestellt und verbessern die Supportfähigkeit und Fehlerbehebung.

Protokolldateien sammeln

Sie können Protokolldateien für ONTAP tools for VMware vSphere über die Optionen in der ONTAP tools Manager-Benutzeroberfläche erfassen. Der technische Support kann Sie bitten, die Protokolldateien zur Fehlerbehebung zu sammeln.



Die Protokollgenerierung über den ONTAP tools Manager umfasst alle Protokolle aller vCenter Serverinstanzen. Die Protokollgenerierung über die vCenter Client-Benutzeroberfläche ist auf den ausgewählten vCenter Server beschränkt.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. **Protokollpakete** in der Seitenleiste auswählen.

Dieser Vorgang kann mehrere Minuten dauern.

4. **Generieren** auswählen, um die Protokolldateien zu generieren.
5. Die Bezeichnung für das Protokollpaket eingeben und **Generieren** auswählen.

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

Führen Sie die folgenden Schritte aus, um mithilfe der vCenter Client-Benutzeroberfläche ein Protokollpaket zu generieren:

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Auf der vSphere Client-Startseite zu **Support > Protokollpaket > Generieren** wechseln.
3. Die Bezeichnung des Protokollpakets angeben und das Protokollpaket generieren. Die Download-Option ist sichtbar, wenn die Dateien generiert wurden. Das Herunterladen kann einige Zeit in Anspruch nehmen.



Das neu erstellte Protokollpaket ersetzt das Protokollpaket, das innerhalb der letzten 3 Tage oder 72 Stunden erstellt wurde.

Bereitstellungsfehlercodes

Während der Bereitstellung, des Neustarts und der Wiederherstellung von ONTAP tools for VMware vSphere

können Fehlercodes auftreten. Die Fehlercodes sind fünfstellig, wobei die ersten beiden Ziffern das Skript kennzeichnen, in dem das Problem aufgetreten 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` gespeichert, 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, falls der Fehler weiterhin besteht oder keine Lösung genannt wird.

Die folgende Tabelle listet die Fehlercodes und die zugehörigen Dateinamen auf.

Fehlercode	Skriptname
00	firstboot-network-config.pl, Modus Deploy
01	firstboot-network-config.pl, Modus Upgrade
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, reboot
06	firstboot-deploy-otv-ng.pl, Upgrade, HA
07	firstboot-deploy-otv-ng.pl, Upgrade, non-HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Die letzten drei Ziffern des Fehlercodes geben den spezifischen Workflow-Fehler innerhalb des Skripts an:

Bereitstellungsfehlercode	Arbeitsablauf	Auflösung
049	Für Netzwerk und Validierung wird das Perl-Skript diese ebenfalls in Kürze zuweisen.	-
050	SSH-Schlüsselgenerierung fehlgeschlagen	Die primäre virtuelle Maschine (VM) wird neu gestartet.
053	Fehler bei der Installation von RKE2	Entweder wird Folgendes ausgeführt und die primäre VM neu gestartet oder eine erneute Bereitstellung vorgenommen: <code>sudo rke2-killall.sh</code> (alle VMs) <code>sudo rke2-uninstall.sh</code> (alle VMs).
054	Fehler beim Festlegen von kubeconfig	Erneut bereitstellen

055	Fehler beim Bereitstellen der Registrierung	Wenn der Registry-Pod vorhanden ist, warten Sie, bis der Pod bereit ist, und starten Sie dann die primäre VM neu oder stellen Sie sie erneut bereit.
059	KubeVip Bereitstellung ist fehlgeschlagen	Stellen Sie sicher, dass die virtuelle IP-Adresse für die Kubernetes-Steuerungsebene und die während der Bereitstellung angegebene ONTAP tools IP-Adresse zum selben VLAN gehören und freie IP-Adressen sind. Starten Sie neu, wenn alle vorherigen Punkte korrekt sind. Andernfalls führen Sie eine erneute Bereitstellung durch.
060	Die Bereitstellung des Operators ist fehlgeschlagen	Neustart
061	Die Bereitstellung der Services ist fehlgeschlagen.	Grundlegende Kubernetes-Debugging-Maßnahmen wie <code>get pods</code> , <code>get rs</code> , <code>get svc</code> usw. im <code>ntv-system</code> -Namespace liefern weitere Details und Fehlerprotokolle unter <code>/var/log/ansible-perl-errors.log</code> und <code>/var/log/ansible-run.log</code> ; anschließend kann eine erneute Bereitstellung erfolgen.
062	Die Bereitstellung der ONTAP tools Services ist fehlgeschlagen.	Weitere Details finden sich in den Fehlerprotokollen unter <code>/var/log/ansible-perl-errors.log</code> , und eine erneute Bereitstellung ist erforderlich.
065	Die Swagger-Seiten-URL ist nicht erreichbar	Erneut bereitstellen
066	Die Schritte nach der Bereitstellung des Gateway-Zertifikats sind fehlgeschlagen	Führen Sie folgende Schritte aus, um das Upgrade wiederherzustellen/abzuschließen: • Diagnose-Shell aktivieren. • Führen Sie den Befehl <code>'sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy'</code> aus. • Überprüfen Sie die Protokolle unter <code>/var/log/post-deploy-upgrade.log</code>.

088	Die Konfiguration der Protokollrotation für journald ist fehlgeschlagen.	Prüfen Sie, ob die Netzwerkeinstellungen der VM mit dem Host kompatibel sind, auf dem die VM ausgeführt wird. Es besteht die Möglichkeit, auf einen anderen Host zu migrieren und die VM neu zu starten.
089	Die Änderung der Besitzverhältnisse der Konfigurationsdatei für die Rotation des Zusammenfassungsprotokolls ist fehlgeschlagen.	Die primäre VM wird neu gestartet.
096	Dynamischen Speicherbereitsteller installieren	-
108	Seeding-Skript fehlgeschlagen	-
114	Interne Zertifikatsaktualisierung in der MongoDB-Collection fehlgeschlagen	Falls die Bereitstellung mit dem Fehlercode 114 fehlschlägt, führen Sie die folgenden Schritte aus: • Aktivieren Sie die Diagnose-Shell. • Führen Sie folgenden Befehl aus: <code>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --internal_cert_update_collection</code> • Überprüfen Sie die Protokolle unter <code>/var/log/otvng/post-deploy-upgrade.log</code>

Neustartfehlercode	Arbeitsablauf	Auflösung
067	Die Wartezeit auf rke2-server ist abgelaufen.	-
101	Das Zurücksetzen des Maint-/Console-Benutzerpassworts ist fehlgeschlagen.	-
102	Fehler beim Löschen der Passwortdatei während des Zurücksetzens des Wartungs-/Konsolenbenutzerpassworts.	-
103	Das Passwort des neuen Wartungs-/Konsolenbenutzers konnte im Vault nicht aktualisiert werden.	-

088	Die Konfiguration der Protokollrotation für journald ist fehlgeschlagen.	Prüfen Sie, ob die Netzwerkeinstellungen der VM mit dem Host kompatibel sind, auf dem die VM ausgeführt wird. Es besteht die Möglichkeit, auf einen anderen Host zu migrieren und die VM neu zu starten.
089	Die Änderung des Besitzverhältnisses der Konfigurationsdatei für die Rotation des Zusammenfassungsprotokolls ist fehlgeschlagen.	Die VM wird neu gestartet.

ONTAP tools für VMware vSphere konfigurieren

Fügen Sie vCenter Serverinstanzen zu ONTAP tools hinzu

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

Über diese Aufgabe

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

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

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

Bevor Sie beginnen

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

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

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

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



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

Schritte

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



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

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

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

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

Schritte

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

Was kommt als Nächstes

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

Schritte

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

Das NFS VAAI Plug-in mit ONTAP tools installieren

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

Bevor Sie beginnen

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

Schritte

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

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

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

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

Was kommt als Nächstes?

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

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

Weitere Informationen finden Sie im ["Die korrekten NFS-Exportrichtlinien für VAAI Copy Offload konfigurieren"](#)

Verwandte Informationen

["Unterstützung für VMware vStorage über NFS"](#)

["NFSv4.0 aktivieren oder deaktivieren"](#)

["ONTAP Unterstützung für NFSv4.2"](#)

Konfigurieren der ESXi-Hosteinstellungen in ONTAP tools

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

Multipath- und Zeitüberschreitungseinstellungen des ESXi-Servers konfigurieren

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

Über diese Aufgabe

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

Schritte

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



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

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

ESXi Hostwerte festlegen

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

Auf einem ESXi Host können folgende Werte festgelegt werden:

HBA/CNA Adaptoreinstellungen

Legt die folgenden Parameter auf Standardwerte fest:

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

MPIO Einstellungen

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

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



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

NFS-Einstellungen

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

Konfigurieren Sie ONTAP Benutzerrollen und -Berechtigungen für ONTAP tools

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

Bevor Sie beginnen

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

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



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

- Mit Administratorrechten für das Storage-Backend anmelden.

Schritte

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

ONTAP tools füllt das Produktfeld automatisch aus.

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

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

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

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

Anforderungen an die SVM Aggregate-Zuordnung

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

REST API:

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

ONTAP CLI:

```
still15_vsim_ucs630f_aggr1 vserver show-aggregates
AvailableVserver      Aggregate      State      Size Type      SnapLock
Type-----
-----svm_test      still15_vsim_ucs630f_aggr1
online      10.11GB vmdisk  non-snaplock
```

ONTAP Benutzer und Rolle manuell erstellen

Benutzer und Rollen manuell ohne die JSON-Datei erstellen.

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

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

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

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

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

Auf Funktionen kann über APIs zugegriffen werden:

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

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



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

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

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

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

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

```

/api/private/cli/snapmirror -access all

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

```

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

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

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

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

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

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

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

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

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

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

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

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

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

```

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

```

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

```

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

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

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

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

```
security login rest-role create -role <role-name> -api  
/api/application/consistency-groups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/private/cli/snapmirror -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nfs/export-policies -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystem-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/subsystems -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/igroups -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/lun-maps -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/vvol-bindings -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/snapmirror/relationships -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/storage/volumes -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
"/api/storage/volumes/*/snapshots" -access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api /api/storage/luns  
-access all -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api
```

```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

```

name>

```
security login rest-role create -role <role-name> -api  
/api/protocols/nvme/interfaces -access readonly -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/fcp/services -access readonly -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/protocols/san/iscsi/services -access readonly -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/security/accounts -access readonly -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api /api/security/roles  
-access readonly -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api /api/storage/qtrees  
-access readonly -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/storage/quota/reports -access readonly -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api  
/api/storage/snapshot-policies -access readonly -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api /api/svm/peers  
-access readonly -vserver <vserver-name>  
  
security login rest-role create -role <role-name> -api /api/svm/svms  
-access readonly -vserver <vserver-name>
```

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

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

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

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

Beispiel:

```
security login create -user-or-group-name testvpsraall -application http  
-authentication-method password -role  
OTV_10_VP_SRA_Discovery_Create_Modify_Destroy -vserver Cl_stil60-cluster_
```

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

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

Beispiel:

```
security login unlock -username testvpsraall -vserver Cl_stil60-cluster
```

Upgrade ONTAP tools für VMware vSphere 10.1 Benutzer auf 10.3 Benutzer

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

Zu den Produktfunktionen:

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

Cluster-Privileges:

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

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

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

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

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

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

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

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

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

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

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

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

SVM Privileges:

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

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

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

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

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

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

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

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

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

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

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

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

```
vserver nvme namespace create  
  
vserver nvme namespace modify  
  
vserver nvme subsystem create  
  
vserver nvme subsystem modify
```

Upgrade ONTAP tools für VMware vSphere 10.3 Benutzer auf 10.4 Benutzer

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

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

Zu den Produktfunktionen:

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

Cluster-Privileges:

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

Fügen Sie ein Speicher-Backend zu ONTAP tools hinzu

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

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

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

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

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

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

Bevor Sie beginnen

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

Verwendung von ONTAP tools Manager



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

Schritte

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



IPv4- und IPv6-Adressverwaltungs-LIFs sind unterstützt.

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



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

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



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

Verwendung der vSphere Client-Benutzeroberfläche



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

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



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

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

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

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



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

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

Verwandte Informationen

["OTV 10: Was ist der globale und lokale Gültigkeitsbereich des Storage-Backends"](#)

["Konfiguration der Cluster zu einer MetroCluster Konfiguration"](#)

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

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

Schritte

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

Konfigurieren Sie Netzwerkzugriff in ONTAP tools

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

Schritte

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

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

4. **Speichern** auswählen.

Erstellen Sie einen Datenspeicher in ONTAP tools

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

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

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

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

Einen vVols Datenspeicher erstellen

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

Bevor Sie beginnen

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

Schritte

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



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

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



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

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

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

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

Einen NFS Datenspeicher erstellen

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

Schritte

1. Melden Sie sich beim vSphere Client an.

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



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

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



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

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

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

Einen VMFS Datenspeicher erstellen

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

Auf einem geschützten Cluster:

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

Bevor Sie beginnen

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

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



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

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

Informationen zur Konfiguration einer ONTAP SVM für das FC-Protokoll finden Sie unter ["Eine SVM für FC konfigurieren"](#).

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

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

Schritte

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

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

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

6. Aus dem Bereich **Speicherattribute**:

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



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

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



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

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

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

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



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



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

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



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

Ergebnis

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

Datenspeicher und virtuelle Maschinen schützen

Schützen Sie einen Hostcluster in ONTAP tools

ONTAP tools for VMware vSphere verwaltet den Schutz von Host-Clustern. Alle Datenspeicher, die zur ausgewählten SVM gehören und auf einem oder mehreren Hosts des Clusters eingebunden sind, werden unter einem Host-Cluster geschützt.

Bevor Sie beginnen

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

- Der Host-Cluster enthält Datenspeicher nur von einer einzigen SVM.
- Datenspeicher auf dem Host-Cluster werden nicht auf Hosts außerhalb des Clusters eingebunden.
- Die auf dem Hostcluster eingebundenen Datenspeicher sind VMFS-Datenspeicher mit iSCSI- oder FC-Protokoll. Die Verwendung von vVols, NFS- oder VMFS-Datenspeichern mit NVMe/FC- und NVMe/TCP-Protokollen ist nicht möglich.
- Datenspeicher, die auf FlexVol/LUN-Volumes basieren und auf einem Host eingebunden sind, sind nicht Teil einer Konsistenzgruppe.
- Datenspeicher, die auf FlexVol/LUN-Volumes basieren und auf einem Host eingebunden sind, sind nicht Teil einer SnapMirror-Beziehung.
- Der Host-Cluster 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 > Protect Cluster**.
3. Im Fenster „Cluster schützen“ werden der Datentyp und die Details der Storage Virtual Machine (VM) des Quellspeichers automatisch ausgefüllt. Der Link „Datenspeicher“ zeigt die geschützten Datenspeicher an.
4. **Beziehung hinzufügen** auswählen.
5. Im Fenster **SnapMirror Beziehung hinzufügen** werden die **Ziel-Storage-VM** und der **Richtlinientyp** ausgewählt.

Der Richtlinientyp kann asynchron oder AutomatedFailOverDuplex sein.

Wenn Sie die SnapMirror Beziehung als AutomatedFailOverDuplex Typ-Richtlinie hinzufügen, müssen Sie die Ziel-Speicher-VM als Speicher-Backend zu demselben vCenter hinzufügen, auf dem ONTAP tools for VMware vSphere bereitgestellt ist.

Im AutomatedFailOverDuplex-Richtlinientyp gibt es einheitliche und nicht einheitliche Hostkonfigurationen. Wenn Sie die Umschalttaste **Einheitliche Hostkonfiguration** auswählen, wird die Konfiguration der Host-Initiatorgruppe implizit auf dem Zielstandort repliziert. Weitere Informationen finden sich unter ["Schlüsselkonzepte und Begriffe"](#).

6. Wenn Sie eine nicht einheitliche Hostkonfiguration wählen, wählen Sie den Hostzugriff (Quelle/Ziel) für jeden Host innerhalb dieses Clusters aus.
7. Wählen Sie **Add**.

8. Sie können den Hostclusterschutz mit der Operation **Hostclusterschutz ändern** bearbeiten. Sie können die Beziehungen mit den Menüoptionen mit den Auslassungspunkten bearbeiten oder löschen.
9. Die Schaltfläche **Schützen** auswählen.

Das System erstellt eine vCenter Aufgabe mit den Details der Auftrags-ID und zeigt deren Fortschritt im Bereich „Letzte Aufgaben“ an. Dies ist eine asynchrone Aufgabe, die Benutzeroberfläche zeigt nur den Status der Anfrageübermittlung an und wartet nicht auf den Abschluss der Aufgabe.

10. Die geschützten Host-Cluster sind unter **NetApp ONTAP tools > Protection > Host cluster relationships** zu finden. Für eine Konsistenzgruppe werden deren Kapazität, zugehörige Datenspeicher und untergeordnete Konsistenzgruppen angezeigt.



Wenn der Schutz innerhalb einer Stunde nach der Erstellung entfernt werden muss, sollte zuerst die Speichererkennung durchgeführt werden.

Verwandte Informationen

["VMware vSphere Metro Storage Cluster \(vMSC\)"](#)

Schutz mit SRA-Schutz verwenden

Konfigurieren Sie SRA in ONTAP tools, um Datastores zu schützen

ONTAP tools for VMware vSphere bietet die Möglichkeit, die SRA-Funktionalität zu aktivieren, um die Notfallwiederherstellung zu konfigurieren.

Bevor Sie beginnen

- Sie sollten Ihre vCenter Server-Instanz eingerichtet und die ESXi-Hosts konfiguriert haben.
- Sie sollten ONTAP tools for VMware vSphere bereitgestellt haben.
- Sie sollten die SRA Adapter `.tar.gz` Datei von der ["NetApp Support Site"](#) heruntergeladen haben.
- Auf beiden ONTAP-Clustern (Quell- und Zielcluster) sollten die gleichen benutzerdefinierten SnapMirror-Zeitpläne vorhanden sein, bevor die SRA-Workflows ausgeführt werden.
- ["ONTAP tools für VMware vSphere Dienste aktivieren"](#) um die SRA-Funktionalität zu aktivieren.

Schritte

1. Melden Sie sich an der Managementoberfläche der VMware Live Site Recovery Appliance über die URL `https://<srm_ip>:5480` an und gehen Sie dann zu Storage Replication Adapters in der Managementoberfläche der VMware Live Site Recovery Appliance.
2. **Neuer Adapter** auswählen.
3. Das `.tar.gz` Installationsprogramm für das SRA Plug-in in VMware Live Site Recovery hochladen.
4. Die Adapter werden erneut gescannt, um zu überprüfen, ob die Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ aktualisiert sind.



Nach einem Failover sind Aktionen wie Erweitern, Einbinden und Löschen für Datenspeicher möglicherweise nicht verfügbar. Eine Datenspeichererkennung aktualisiert und zeigt die entsprechenden Kontextmenüaktionen an.



Nach jedem Reprotect Vorgang ist eine Speicherermittlung an beiden Standorten erforderlich.

In einer neuen Konfiguration mit SRA-Schutz wird empfohlen, stets ein Test-Failover durchzuführen. Das Überspringen des Test-Failovers kann dazu führen, dass der Reprotect-Vorgang fehlschlägt.

In einer Fan-Out-Konfiguration, nach einem SnapMirror Active Sync Failover, bei dem die SnapMirror Quelle für Automated Failover Duplex und asynchrones SnapMirror auf Standort B wechselt, sollte ein Test-Failover zwischen den Standorten B und C durchgeführt werden. Das Überspringen dieses Schritts kann zu einem fehlgeschlagenen Reprotect-Vorgang führen.

Verwandte Informationen

["Die Notfallwiederherstellung für NFS-Datenspeicher mit VMware Site Recovery Manager konfigurieren"](#)

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

Die Speichersysteme sind vor der Ausführung des Storage Replication Adapter (SRA) für VMware Live Site Recovery einzurichten.

SRA für SAN-Umgebungen konfigurieren



Konsistenzgruppen in SRA-Workflows werden nur mit SAN-Protokollen (iSCSI und Fibre Channel) auf Unified- und ASA r2 Storage-Systemen unterstützt.

Bevor Sie beginnen

Auf dem geschützten Standort und dem Wiederherstellungsstandort sollten die folgenden Programme installiert sein:

- VMware Live Site Recovery: Die VMware Website stellt Installationsdokumentation für VMware Live Site Recovery bereit.

["Über VMware Live Site Recovery"](#)

- SRA: Der Adapter wird auf VMware Live Site Recovery installiert.

Beachten Sie bei der Konfiguration des iSCSI-Protokolls vor dem Ausführen von SRA-Workflows Folgendes:

- **Geschützter Bereich:** iSCSI-Speicheradapter und Daten-LIF-Details werden bei der Bereitstellung von Datenspeichern automatisch konfiguriert. Keine manuelle Konfiguration ist erforderlich.
- **Wiederherstellungsstandort:** iSCSI-Speicheradapter müssen auf jedem ESXi-Host, der in die Ressourcenzuordnung für die Notfallwiederherstellung einbezogen ist, manuell konfiguriert werden. Um die individuelle Konfiguration der Adapter auf jedem Host zu vermeiden, erstellen Sie auf dem Wiederherstellungsstandort mithilfe der SVM, auf der die SRA-Workflows konfiguriert sind, einen Platzhalter-Datenspeicher vom Typ iSCSI. Dadurch werden der iSCSI-Adapter und die erforderlichen Daten-LIF-IP-Adressen automatisch allen zugeordneten ESXi-Hosts hinzugefügt. Weitere Informationen finden Sie unter ["Platzhalterdatenspeicher in ONTAP tools konfigurieren"](#).

Schritte

1. Es wird sichergestellt, dass die primären ESXi Hosts mit den LUNs im primären Storage-System am geschützten Standort verbunden sind.
2. Überprüfen Sie, ob sich die LUNs in igroups befinden, bei denen die `ostype` Option auf *VMware* auf dem primären Storage-System gesetzt ist.
3. Es ist sicherzustellen, dass die ESXi Hosts am Wiederherstellungsstandort über die erforderliche iSCSI-

und Fibre Channel-Konnektivität zur Storage Virtual Machine (SVM) verfügen. Die ESXi Hosts am sekundären Standort sollten Zugriff auf den Speicher des sekundären Standorts haben, und die ESXi Hosts am primären Standort sollten Zugriff auf den Speicher des primären Standorts haben.

Dies kann entweder durch Überprüfung erfolgen, ob die ESXi-Hosts lokale LUNs haben, die auf der SVM verbunden sind, oder durch den `iscsi show initiators` Befehl auf den SVMs. Der LUN-Zugriff für die zugeordneten LUNs im ESXi-Host dient zur Verifizierung der iSCSI-Konnektivität.

SRA für NAS-Umgebungen konfigurieren



Konsistenzgruppen werden für NFS in SRA-Workflows nicht unterstützt. Wenn NFS-Datenspeichervolumen einer Konsistenzgruppe zugeordnet und geschützt werden, schlägt der Vorgang „Geräte ermitteln“ fehl. Verwenden Sie keine Konsistenzgruppen, wenn Sie NFS-Datenspeicher mit SRA schützen.

Bevor Sie beginnen

Auf dem geschützten Standort und dem Wiederherstellungsstandort sollten die folgenden Programme installiert sein:

- VMware Live Site Recovery: Die Installationsdokumentation für VMware Live Site Recovery befindet sich auf der VMware Website "[Über VMware Live Site Recovery](#)"
- SRA: Der Adapter ist auf VMware Live Site Recovery und dem SRA Server zu installieren.

Schritte

1. Es sollte sichergestellt sein, dass die Datenspeicher am geschützten Standort virtuelle Maschinen enthalten, die beim vCenter Server registriert sind.
2. Überprüfen Sie, ob die ESXi-Hosts am geschützten Standort die NFS-Exportvolumen der Storage Virtual Machine (SVM) eingebunden haben.
3. Stellen Sie sicher, dass im Feld **NFS Addresses** gültige IP-Adressen angegeben sind, unter denen die NFS-Exporte vorhanden sind, wenn Sie den Array Manager-Assistenten zum Hinzufügen von Arrays zu VMware Live Site Recovery verwenden. Verwenden Sie im Feld **NFS Addresses** nicht den NFS-Hostnamen oder den FQDN.
4. Der `ping` Befehl ist auf jedem ESXi Host am Wiederherstellungsstandort zu verwenden, um zu überprüfen, ob der Host über einen VMkernel Port verfügt, der auf die IP-Adressen zugreifen kann, die zum Bereitstellen von NFS-Exporten von der SVM verwendet werden.

Konfigurieren Sie SRA in ONTAP tools für hochskalierte Umgebungen

Die Zeitüberschreitungsintervalle für den Speicher sollten gemäß den empfohlenen Einstellungen konfiguriert werden, damit der Storage Replication Adapter (SRA) in hochskalierten Umgebungen optimal arbeitet.

Einstellungen des Speicheranbieters

Für skalierte Umgebungen in VMware Live Site Recovery sind die folgenden Zeitüberschreitungswerte festzulegen:

Erweiterte Einstellungen	Timeout-Werte
--------------------------	---------------

<code>StorageProvider.resignatureTimeout</code>	Der Wert der Einstellung wird von 900 Sekunden auf 12000 Sekunden erhöht.
<code>storageProvider.hostRescanDelaySec</code>	60
<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Ein hoher Wert festlegen (zum Beispiel: 99999)

Die Option `StorageProvider.autoResignatureMode` sollte ebenfalls aktiviert werden.

Weitere Informationen zum Ändern der Einstellungen des Speicheraanbieters finden Sie unter ["Speicheraanbieter-Einstellungen ändern"](#).

Speichereinstellungen

Wenn eine Zeitüberschreitung auftritt, die Werte von `storage.commandTimeout` und `storage.maxConcurrentCommandCnt` auf einen höheren Wert erhöhen.



Das angegebene Zeitüberschreitungsintervall ist der Maximalwert. Sie müssen nicht warten, bis die maximale Zeitüberschreitung erreicht ist. Die meisten Befehle werden innerhalb des festgelegten maximalen Zeitüberschreitungsintervalls abgeschlossen.

Siehe ["Speichereinstellungen ändern"](#) zum Ändern der SAN-Provider-Einstellungen.

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

Nach der Bereitstellung der VMware Live Site Recovery Appliance wird der Storage Replication Adapter (SRA) konfiguriert, um das Disaster Recovery Management zu ermöglichen.

Die Konfiguration von SRA auf der VMware Live Site Recovery Appliance speichert die ONTAP tools for VMware vSphere Anmeldeinformationen innerhalb der Appliance und ermöglicht so die Kommunikation zwischen VMware Live Site Recovery und SRA.

Bevor Sie beginnen

- Die `.tar.gz`-Datei kann von der ["NetApp Support Site"](#) heruntergeladen werden.
- Aktivieren Sie die SRA-Dienste im ONTAP tools Manager. Weitere Informationen finden Sie im ["Dienste aktivieren"](#) Abschnitt.
- Fügen Sie vCenter Server zur ONTAP tools for VMware vSphere Appliance hinzu. Weitere Informationen finden Sie im ["Fügen Sie vCenter Server hinzu"](#) Abschnitt.
- Fügen Sie Speicher-Backends zu ONTAP tools for VMware vSphere hinzu. Weitere Informationen finden Sie im ["Storage-Backends hinzufügen"](#) Abschnitt.



Wenn der vCenter-Zertifikatspatch von ONTAP tools angewendet wurde, sollte die vCenter-Konfiguration in der VMware Live Site Recovery Appliance über den Port (:5480) aktualisiert werden. Anleitungen finden sich unter ["Die Site Recovery Manager Appliance neu konfigurieren"](#).

Schritte

1. Auf dem Bildschirm der VMware Live Site Recovery Appliance **Storage Replication Adapter > New Adapter** auswählen.
2. Die `.tar.gz`-Datei in VMware Live Site Recovery hochladen.
3. Melden Sie sich mit einem Administratorkonto über einen SSH-Client wie PuTTY bei der VMware Live Site Recovery Appliance an.
4. Zum Root-Benutzer mit folgendem Befehl wechseln: `su root`
5. Führen Sie den Befehl `cd /var/log/vmware/srm` aus, um zum Protokollverzeichnis zu wechseln.
6. Geben Sie am Speicherort des Protokolls den Befehl ein, um die von SRA verwendete docker id zu erhalten: `docker ps -l`
7. Um sich bei der Container-ID anzumelden, den folgenden Befehl eingeben: `docker exec -it -u srm <container id> sh`
8. VMware Live Site Recovery mit ONTAP tools for VMware vSphere IP-Adresse und Passwort wird mit folgendem Befehl konfiguriert: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Das Passwort ist in einfache Anführungszeichen zu setzen, damit das Perl-Skript Sonderzeichen als Teil des Passworts und nicht als Trennzeichen behandelt.
 - Sie können den Benutzernamen und das Kennwort für die Anwendung (VASA Provider/SRA) im ONTAP tools Manager festlegen, wenn diese Dienste zum ersten Mal aktiviert werden. Mit diesen Anmeldeinformationen lässt sich SRA bei VMware Live Site Recovery registrieren.
 - Um die vCenter GUID zu finden, gehen Sie nach dem Hinzufügen Ihrer vCenter Instanz auf die vCenter Serverseite im ONTAP tools Manager. Siehe ["Fügen Sie vCenter Server hinzu"](#) Abschnitt.
9. Die Adapter werden erneut gescannt, sodass die aktualisierten Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ angezeigt werden.

Ergebnis Es erscheint eine Bestätigungsmeldung, die anzeigt, dass die Speicherzugangsdaten gespeichert wurden. Sie können SRA nun verwenden, um mit dem SRA Server über die angegebene IP-Adresse, den Port und die Zugangsdaten 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, falls Sie die Anmeldeinformationen geändert haben.

Bevor Sie beginnen

Sie sollten die im Thema genannten Schritte ["Konfiguration von SRA auf der VMware Live Site Recovery Appliance"](#) ausgeführt haben.

Schritte

1. Führen Sie die folgenden Befehle aus, um die zwischengespeicherten ONTAP tools-Anmeldeinformationen von der VMware Live Site Recovery-Maschine 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 -l --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv -password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`` Es muss ein einfaches Anführungszeichen um den Passwortwert gesetzt werden.

Es wird eine Erfolgsmeldung angezeigt, die bestätigt, dass die Speicherzugangsdaten gespeichert wurden. SRA kann über die angegebene IP-Adresse, den Port und die Zugangsdaten mit dem SRA-Server kommunizieren.

Konfigurieren Sie vCenter in der VMware Live Site Recovery Appliance nach einer Zertifikatsänderung neu

Wenn sich das vCenter-Zertifikat ändert, beispielsweise nach einem vCenter-Upgrade, kann bei der Site Recovery-Erweiterung ein Fehler aufgrund eines nicht übereinstimmenden Fingerabdrucks auftreten. Führen Sie die folgenden Schritte aus, um das Problem zu beheben.

Schritte

1. Neukonfiguration vCenter in der VMware Live Site Recovery Appliance

- a. Öffnen Sie die VMware Live Site Recovery Appliance Managementoberfläche in einem Browser:
`https://<SRM_IP>:5480`
- b. Wählen Sie die Registerkarte **Zusammenfassung**.
- c. Wählen Sie **Neu konfigurieren** für die vCenter Serververbindung.

Dies ruft den neuesten Zertifikatfingerabdruck von vCenter ab und akzeptiert ihn.

2. Stellen Sie die Standortkopplung erneut her (falls der Fehler weiterhin besteht)

Wenn der Fehler mit der Fingerabdruckabweichung auch nach der Neukonfiguration weiterhin besteht:

- a. Melden Sie sich bei der vCenter Benutzeroberfläche an.
- b. Navigieren Sie zur Erweiterung **Site Recovery**.
- c. Suchen Sie den Abschnitt **Site Pairing**.
- d. Wählen Sie **Neu verbinden**, um die Standortkopplung mit dem aktualisierten Zertifikat wiederherzustellen.

Konfigurieren von geschützten und Wiederherstellungsstandorten in ONTAP tools

Es empfiehlt sich, Schutzgruppen zu erstellen, um eine Gruppe virtueller Maschinen auf

der geschützten Site zu schützen.

Beim Hinzufügen eines neuen Datenspeichers kann dieser in die bestehende Datenspeichergruppe aufgenommen oder ein neuer Datenspeicher hinzugefügt und ein neues Volume oder eine neue Konsistenzgruppe zum Schutz erstellt werden. Nach dem Hinzufügen eines neuen Datenspeichers zu einer geschützten Konsistenzgruppe oder einem geschützten Volume sollten SnapMirror aktualisiert und die Speichererkennung sowohl am geschützten als auch am Wiederherstellungsstandort durchgeführt werden. Die Erkennung kann manuell oder nach einem Zeitplan ausgeführt werden, um sicherzustellen, dass der neue Datenspeicher erkannt und geschützt ist.

Geschützte und Wiederherstellungsstandorte paaren

Sie sollten die mit Ihrem vSphere Client erstellten geschützten und Wiederherstellungsstandorte koppeln, damit der Storage Replication Adapter (SRA) die Speichersysteme erkennen kann.



Der Storage Replication Adapter (SRA) unterstützt Fan-Out mit einer synchronen Beziehung vom Typ Automated Failover Duplex und einer asynchronen SnapMirror-Beziehung in einer Konsistenzgruppe. Fan-Out mit zwei asynchronen SnapMirror-Beziehungen in Konsistenzgruppen oder Fan-Out SnapMirror-Beziehungen auf Volumes wird jedoch nicht unterstützt. Vault-Typ SnapMirror-Beziehungen werden bei diesen Fan-Out-Beschränkungen nicht berücksichtigt. Die Unterstützung von Konsistenzgruppen im SRA ist auf SAN-Protokolle (iSCSI und Fibre Channel) auf Unified- und ASA r2-Speichersystemen beschränkt. Konsistenzgruppen werden für NFS nicht unterstützt. Wenn NFS-Datenspeichervolumen einer Konsistenzgruppe zugeordnet werden, schlägt die Geräteerkennung fehl.

Bevor Sie beginnen

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

Schritte

1. Auf der Startseite des vSphere Clients auf das Symbol **Site Recovery** doppelklicken und anschließend **Sites** auswählen.
2. **Objekte > Aktionen > Standorte koppeln** auswählen.
3. Im Dialogfeld **Pair Site Recovery Manager Servers** die Adresse des Platform Services Controllers der geschützten Site eingeben und anschließend **Weiter** auswählen.
4. Führen Sie im Abschnitt vCenter Server auswählen die folgenden Schritte aus:
 - a. Es sollte überprüft werden, ob der vCenter Server der geschützten Site als passender Kandidat für die Kopplung angezeigt wird.
 - b. Geben Sie die SSO-Administratoranmeldeinformationen ein und wählen Sie anschließend **Fertigstellen** aus.
5. Falls Sie dazu aufgefordert werden, **Ja** auswählen, um die Sicherheitszertifikate zu akzeptieren.

Ergebnis

Im Dialogfeld **Objekte** werden sowohl die geschützten als auch die Wiederherstellungs-Sites angezeigt.

Schutzgruppen konfigurieren

Bevor Sie beginnen

Es sollte sichergestellt sein, dass sowohl die Quell- als auch die Zielseite für Folgendes konfiguriert sind:

- Dieselbe Version von VMware Live Site Recovery ist installiert
- Virtuelle Maschinen
- Gepaarte geschützte und Wiederherstellungsstandorte
- Quell- und Zieldatenspeicher sollten an den jeweiligen Standorten eingebunden sein.

Schritte

1. Melden Sie sich beim vCenter Server an und wählen Sie **Site Recovery > Protection Groups**.
2. Im Bereich **Schutzgruppen** auf **Neu** auswählen.
3. Einen Namen und eine Beschreibung für die Schutzgruppe sowie die Richtung angeben und **Weiter** auswählen.
4. Wählen Sie im Feld **Typ** die Option **Typfeld...** als Datenspeichergruppen (Array-basierte Replikation) für NFS- und VMFS-Datenspeicher aus. Die Fehlerdomäne besteht aus SVMs mit aktivierter Replikation. Die SVMs, die ausschließlich Peering implementiert haben und keine Probleme aufweisen, werden angezeigt.
5. Auf der Registerkarte Replikationsgruppen entweder das aktivierte Array-Paar oder die Replikationsgruppen auswählen, die die konfigurierte virtuelle Maschine enthalten, und anschließend **Weiter** auswählen.

Alle virtuellen Maschinen der Replikationsgruppe werden der Schutzgruppe hinzugefügt.

6. Sie können entweder den bestehenden Wiederherstellungsplan auswählen oder einen neuen erstellen, indem Sie **Zu neuem Wiederherstellungsplan hinzufügen** auswählen.
7. Auf der Registerkarte „Bereit zum Abschließen“ werden die Details der erstellten Schutzgruppe angezeigt, anschließend kann **Fertigstellen** ausgewählt werden.

Konfiguration von Ressourcen für geschützte und Wiederherstellungsstandorte

Netzwerkzuordnungen in ONTAP tools konfigurieren

Ihre Ressourcenzuordnungen wie VM-Netzwerke, ESXi Hosts und Ordner an beiden Standorten sind so zu konfigurieren, dass die Zuordnung jeder Ressource vom geschützten Standort zur entsprechenden Ressource am Wiederherstellungsstandort möglich ist.

Die folgenden Ressourcenkonfigurationen sollten abgeschlossen werden:

- Netzwerkzuordnungen
- Ordnerzuordnungen
- Ressourcenzuordnungen
- Platzhalter Datenspeicher

Bevor Sie beginnen

Die geschützten und die Wiederherstellungsstandorte sollten verbunden sein.

Schritte

1. Melden Sie sich am vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Website aus und wählen Sie **Verwalten**.

3. Im Tab „Verwalten“ unter **Netzwerkzuordnungen** > **Neu** kann eine neue Netzwerkzuordnung erstellt werden.
4. Im Assistenten zum Erstellen einer Netzwerkzuordnung sind folgende Schritte auszuführen:
 - a. **Automatisch Zuordnungen für Netzwerke mit übereinstimmenden Namen vorbereiten** auswählen und **Weiter** auswählen.
 - b. Wählen Sie die benötigten Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
 - c. **Weiter** auswählen, nachdem die Zuordnungen erfolgreich erstellt wurden.
 - d. Wählen Sie das Objekt aus, das zuvor zum Erstellen der umgekehrten Zuordnung verwendet wurde, und dann **Fertigstellen**.

Ergebnis

Auf der Seite „Netzwerkzuordnungen“ werden die Ressourcen des geschützten Standorts und die Ressourcen des Wiederherstellungsstandorts angezeigt. Für andere Netzwerke in Ihrer Umgebung sind die gleichen Schritte möglich.

Ordnerzuordnungen in ONTAP tools konfigurieren

Ihre Ordner auf der geschützten Site und der Wiederherstellungs-Site sollten einander zugeordnet werden, damit die Kommunikation zwischen ihnen möglich ist.

Bevor Sie beginnen

Die geschützten und die Wiederherstellungsstandorte sollten verbunden sein.

Schritte

1. Melden Sie sich am vCenter Server an und wählen Sie **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Website aus und wählen Sie **Verwalten**.
3. **Ordnerzuordnungen** > **Ordner**-Symbol in der Registerkarte „Verwalten“ auswählen, um eine neue Ordnerzuordnung zu erstellen.
4. Im Assistenten zum Erstellen von Ordnerzuordnungen sind die folgenden Schritte auszuführen:
 - a. **Automatische Zuordnung für Ordner mit übereinstimmenden Namen vorbereiten** auswählen und **Weiter** auswählen.
 - b. Wählen Sie die benötigten Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
 - c. **Weiter** auswählen, nachdem die Zuordnungen erfolgreich erstellt wurden.
 - d. Wählen Sie das Objekt aus, das zuvor zum Erstellen der umgekehrten Zuordnung verwendet wurde, und dann **Fertigstellen**.

Ergebnis

Auf der Seite „Ordnerzuordnungen“ werden die geschützten Site-Ressourcen und die Ressourcen der Wiederherstellungssite angezeigt. Sie können die gleichen Schritte für andere Ordner in Ihrer Umgebung ausführen.

Ressourcenzuordnungen in ONTAP tools konfigurieren

Ihre Ressourcen auf dem geschützten Standort und dem Wiederherstellungsstandort sollten so zugeordnet werden, dass virtuelle Maschinen so konfiguriert sind, dass sie bei

einem Failover in die eine oder andere Gruppe von Hosts wechseln.

Bevor Sie beginnen

Die geschützten und die Wiederherstellungsstandorte sollten verbunden sein.



In VMware Live Site Recovery können Ressourcen Ressourcenpools, ESXi Hosts oder vSphere Clustern sein.

Schritte

1. Melden Sie sich am vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Website aus und wählen Sie **Verwalten**.
3. Im Tab „Verwalten“ **Ressourcenzuordnungen > Neu** auswählen, um eine neue Ressourcenzuordnung zu erstellen.
4. Im Assistenten zum Erstellen von Ressourcenzuordnungen sind die folgenden Schritte auszuführen:
 - a. Wählen Sie **Automatisch Zuordnungen für Ressourcen mit übereinstimmenden Namen vorbereiten** und wählen Sie **Weiter**.
 - b. Wählen Sie die benötigten Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
 - c. **Weiter** auswählen, nachdem die Zuordnungen erfolgreich erstellt wurden.
 - d. Wählen Sie das Objekt aus, das zuvor zum Erstellen der umgekehrten Zuordnung verwendet wurde, und dann **Fertigstellen**.

Ergebnis

Auf der Seite „Ressourcenzuordnungen“ werden die geschützten Standortressourcen und die Ressourcen des Wiederherstellungsstandorts angezeigt. Sie können die gleichen Schritte für andere Ressourcen in Ihrer Umgebung ausführen.

Platzhalterdatenspeicher in ONTAP tools konfigurieren

Ein Platzhalterdatenspeicher wird konfiguriert, um Speicherplatz im vCenter-Inventar am Wiederherstellungsstandort für geschützte virtuelle Maschinen (VMs) zu reservieren. Platzhalterdatenspeicher benötigen nur minimale Kapazität, da Platzhalter-VMs klein sind und typischerweise nur wenige hundert Kilobyte belegen.

Bevor Sie beginnen

- Es ist sicherzustellen, dass die geschützten Standorte und die Wiederherstellungsstandorte miteinander verbunden sind.
- Es sollte überprüft werden, ob die Ressourcenzuordnungen konfiguriert wurden.

Schritte

1. Melden Sie sich am vCenter Server an und wählen Sie **Site Recovery > Sites**.
2. Wählen Sie Ihre geschützte Website aus und wählen Sie **Verwalten**.
3. Im Tab „Verwalten“ **Placeholder Datastores > Neu** auswählen, um einen neuen Platzhalter-Datenspeicher zu erstellen.
4. Den entsprechenden Datenspeicher auswählen und **OK** wählen.



Platzhalterdatenspeicher können sich auf lokalem oder entferntem Speicher befinden, erfordern jedoch keine Replikation.

- Schritte 3 bis 5 werden wiederholt, um einen Platzhalter-Datenspeicher für den Wiederherstellungsstandort zu konfigurieren.

Konfigurieren Sie SRA mithilfe des Array-Managers in ONTAP tools

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

Bevor Sie beginnen

- Die geschützten Standorte und die Wiederherstellungsstandorte sollten in VMware Live Site Recovery gekoppelt sein.
- Der integrierte Speicher sollte vor der Konfiguration des Array-Managers konfiguriert worden sein.
- Die SnapMirror Beziehungen zwischen den geschützten Standorten und den Wiederherstellungsstandorten sollten konfiguriert und repliziert sein.
- Die SVM Management-LIFs sollten aktiviert sein, um Mandantenfähigkeit zu ermöglichen.

SRA unterstützt die Verwaltung auf Cluster-Ebene und SVM-Ebene. Wenn Speicher auf Cluster-Ebene hinzugefügt wird, können alle SVMs im Cluster erkannt und Operationen an ihnen durchgeführt werden. Wenn Speicher auf SVM-Ebene hinzugefügt wird, kann nur diese spezifische SVM verwaltet werden.

Schritte

- In VMware Live Site Recovery **Array Manager > Array Manager hinzufügen** auswählen.
- Folgende Informationen beschreiben das Array in VMware Live Site Recovery:
 - Im Feld **Anzeigename** einen Namen zur Identifizierung des Array Managers eingeben.
 - Im Feld **SRA-Typ** ist **NetApp Storage Replication Adapter für ONTAP** auszuwählen.
 - Geben Sie die Informationen ein, um eine Verbindung zum Cluster oder zur SVM herzustellen:
 - Wenn Sie eine Verbindung zu einem Cluster herstellen, sollte die Cluster-Management-LIF eingegeben werden.
 - Wenn Sie eine direkte Verbindung zu einer SVM herstellen, sollte die IP-Adresse des SVM Management-LIF eingegeben werden.



Bei der Konfiguration des Array-Managers sollte dieselbe Verbindung (IP-Adresse) für das Speichersystem verwendet werden, die auch für das Onboarding des Speichersystems in ONTAP tools for VMware vSphere verwendet wurde. Wenn die Konfiguration des Array-Managers beispielsweise auf SVM-Ebene erfolgt, sollte der Speicher unter ONTAP tools for VMware vSphere auf SVM-Ebene hinzugefügt werden.

- Wenn eine Verbindung zu einem Cluster hergestellt wird, ist der SVM-Name im Feld **SVM-Name** anzugeben oder das Feld bleibt leer, um alle SVMs im Cluster zu verwalten.
- Geben Sie die zu ermittelnden Volumes im Feld **Volume-Einschlussliste** ein.

Am geschützten Standort kann das Quellvolume und am Wiederherstellungsstandort das replizierte

Zielvolume eingegeben werden.

Wenn beispielsweise das Volume `src_vol1` ermittelt werden soll, das sich in einer SnapMirror Beziehung mit dem Volume `dst_vol1` befindet, ist `src_vol1` im Feld „geschützter Standort“ und `dst_vol1` im Feld „Wiederherstellungsstandort“ anzugeben.

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

Am geschützten Standort kann das Quellvolume und am Wiederherstellungsstandort das replizierte Zielvolume eingegeben werden.

Wenn beispielsweise das Volume `src_vol1` ausgeschlossen werden soll, das sich in einer SnapMirror Beziehung mit dem Volume `dst_vol1` befindet, ist `src_vol1` im Feld „geschützter Standort“ und `dst_vol1` im Feld „Wiederherstellungsstandort“ anzugeben.

3. **Weiter** auswählen.

4. Es sollte überprüft werden, ob das Array erkannt und unten im Fenster „Add Array Manager“ angezeigt wird, und anschließend **Finish** ausgewählt werden.

Die gleichen Schritte können für den Wiederherstellungsstandort unter Verwendung der entsprechenden SVM-Management-IP-Adressen und Anmeldedaten durchgeführt werden. Auf dem Bildschirm „Array-Paare aktivieren“ des Assistenten zum Hinzufügen eines Array-Managers sollte überprüft werden, ob das richtige Array-Paar ausgewählt ist und als aktivierungsbereit angezeigt wird.

Überprüfen Sie replizierte Speichersysteme in ONTAP tools

Nach der Konfiguration des Storage Replication Adapter (SRA) sollte überprüft werden, ob der geschützte Standort und der Wiederherstellungsstandort erfolgreich gekoppelt sind. Das replizierte Storage-System sollte sowohl vom geschützten Standort als auch vom Wiederherstellungsstandort aus auffindbar sein.

Bevor Sie beginnen

- Sie sollten Ihr Speichersystem konfiguriert haben.
- Der geschützte Standort und der Wiederherstellungsstandort sollten mithilfe des VMware Live Site Recovery Array Managers gekoppelt worden sein.
- Die FlexClone Lizenz und die SnapMirror Lizenz sollten vor der Durchführung des Test-Failover-Vorgangs und des Failover-Vorgangs für SRA aktiviert worden sein.
- An Quell- und Zielstandorten sollten die gleichen SnapMirror Richtlinien und Zeitpläne vorhanden sein.
- Wenn Sie benutzerdefinierte SnapMirror-Richtlinien mit einem benutzerdefinierten Zeitplan verwenden, müssen Sie denselben Zeitplan und dieselbe Richtlinie sowohl auf dem geschützten als auch auf dem Wiederherstellungsstandort konfigurieren.
- Wenn Sie benutzerdefinierte SnapMirror-Richtlinien verwenden (mit einem Standard- oder benutzerdefinierten Zeitplan), müssen Sie die Speichererkennung von ONTAP tools durchführen, damit die neue Richtlinie erkannt wird. Ohne dies schlagen SRA-Workflows, einschließlich Test-Failover und Failover, fehl. Führen Sie die Speichererkennung an den folgenden Punkten durch:
 - Nach dem Erstellen der benutzerdefinierten Richtlinie auf der Wiederherstellungsseite.
 - Nach einer Reprotect-Operation, bei der die Richtlinie auf der geschützten Site wiederhergestellt wird.

Schritte

1. Melden Sie sich bei Ihrem vCenter Server an.
2. Zu **Site Recovery > Array Based Replication** wechseln.
3. Das erforderliche Array Pair auswählen und die entsprechenden Details überprüfen.

Die Speichersysteme sollten am geschützten Standort und am Wiederherstellungsstandort mit dem Status **Enabled** erkannt werden.

Fan-out-Schutz in ONTAP tools

In einem Fan-Out-Schutzszenario ist die Konsistenzgruppe doppelt geschützt: mit synchroner Beziehung auf dem ersten Ziel-ONTAP Cluster und mit asynchroner Beziehung auf dem zweiten Ziel-ONTAP Cluster. Die Workflows zum Erstellen, Bearbeiten und Löschen von SnapMirror Active Sync-Schutz erhalten den synchronen Schutz. Die Workflows für Failover und Reprotect der VMware Live Site Recovery Appliance erhalten den asynchronen Schutz.



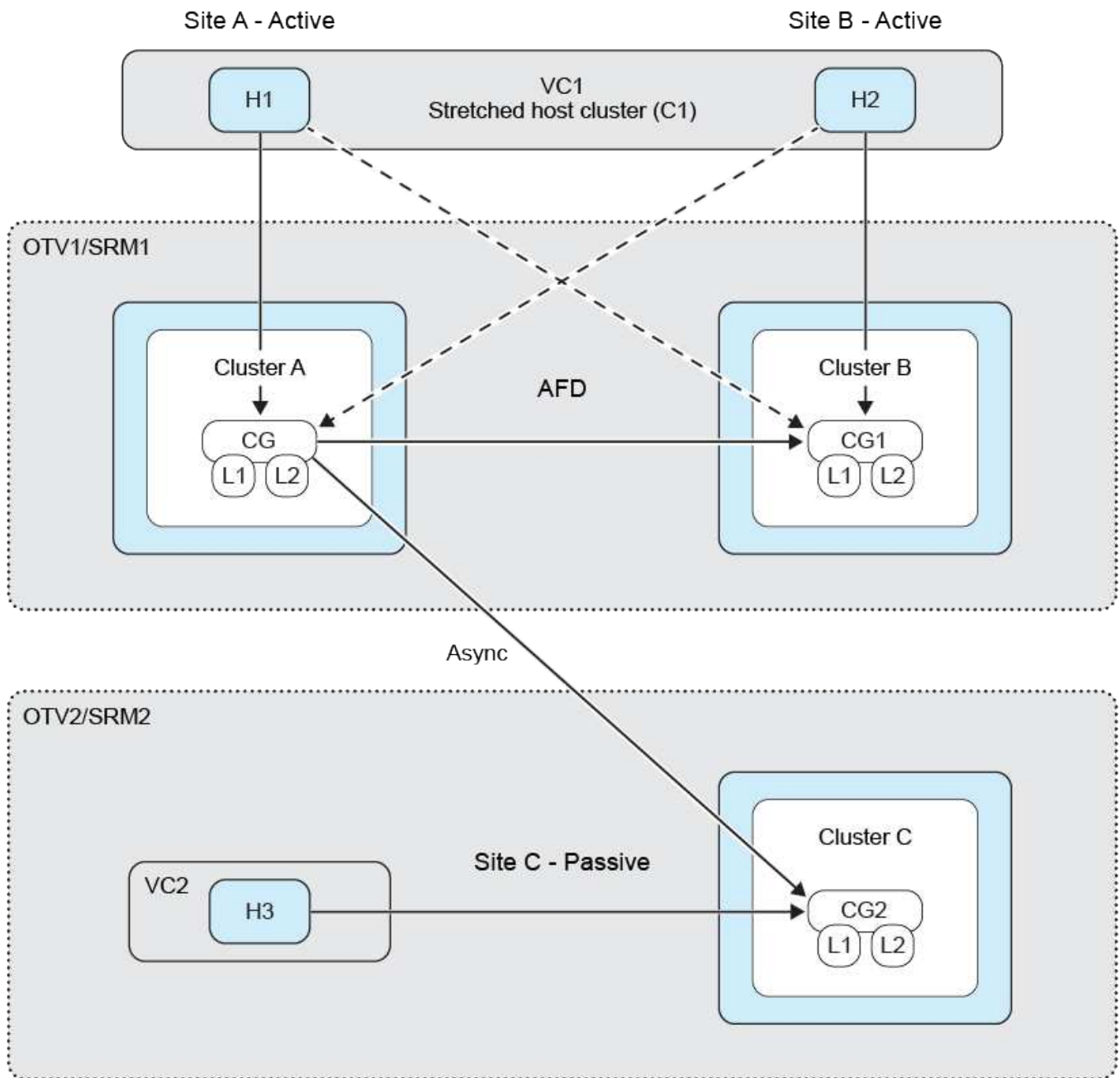
Fan-Out wird für SVM-Benutzer nicht unterstützt.

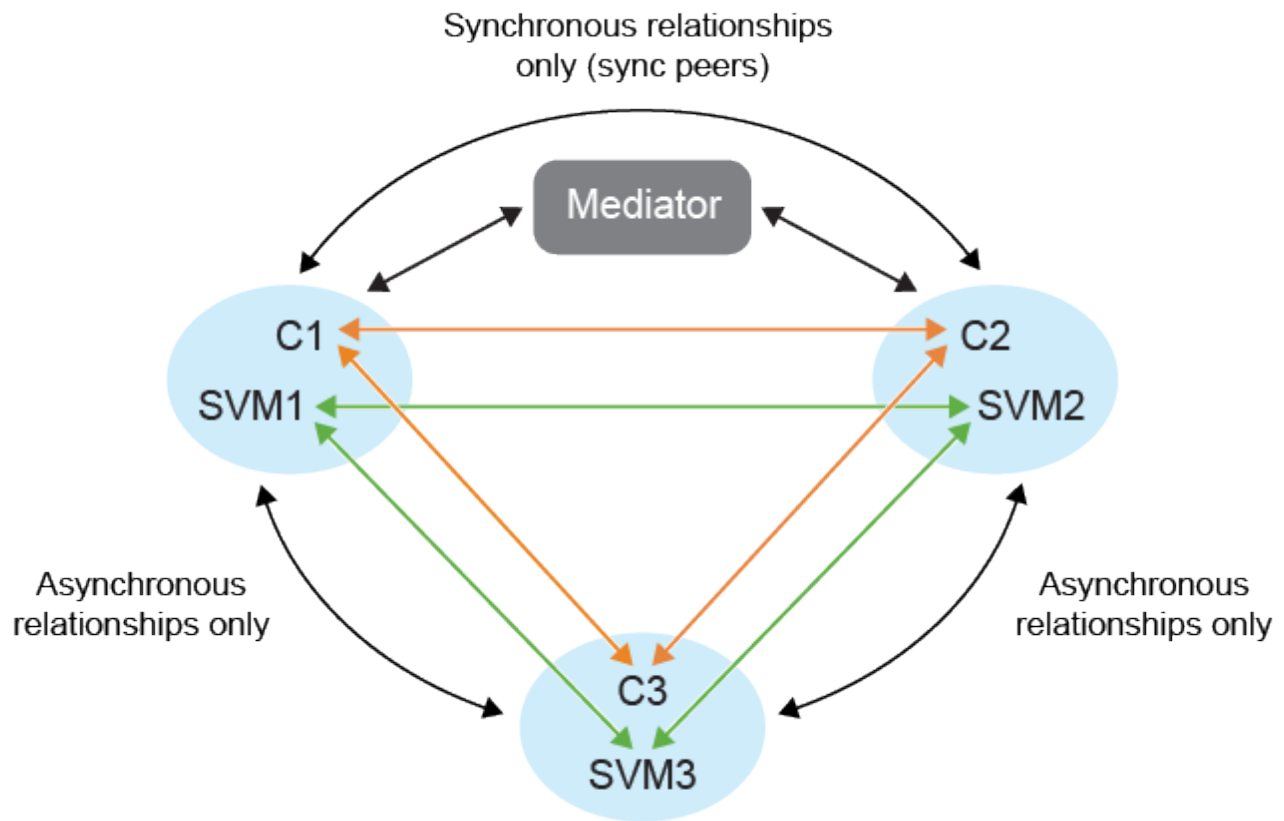
Zum Einrichten des Fan-Out-Schutzes werden die drei Standort-Cluster und SVMs miteinander gekoppelt.

Beispiel:

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

Das folgende Diagramm zeigt die Fan-Out-Schutzkonfiguration:





Schritte

1. Wählen Sie einen neuen Platzhalterdatenspeicher aus. Die Auswahlkriterien für den Platzhalterdatenspeicher im Rahmen des phasenweisen Schutzes lauten:
 - Der Platzhalterdatenspeicher sollte nicht im Hostcluster platziert werden, den Sie schützen.
 - Wenn Sie den Platzhalterdatenspeicher in den Hostcluster einbinden müssen, fügen Sie ihn der VMware Live Site Recovery Appliance hinzu, bevor Sie SnapMirror active sync-Schutz einrichten. Mit dieser Konfiguration können Sie den Platzhalterdatenspeicher vom Schutz ausnehmen.

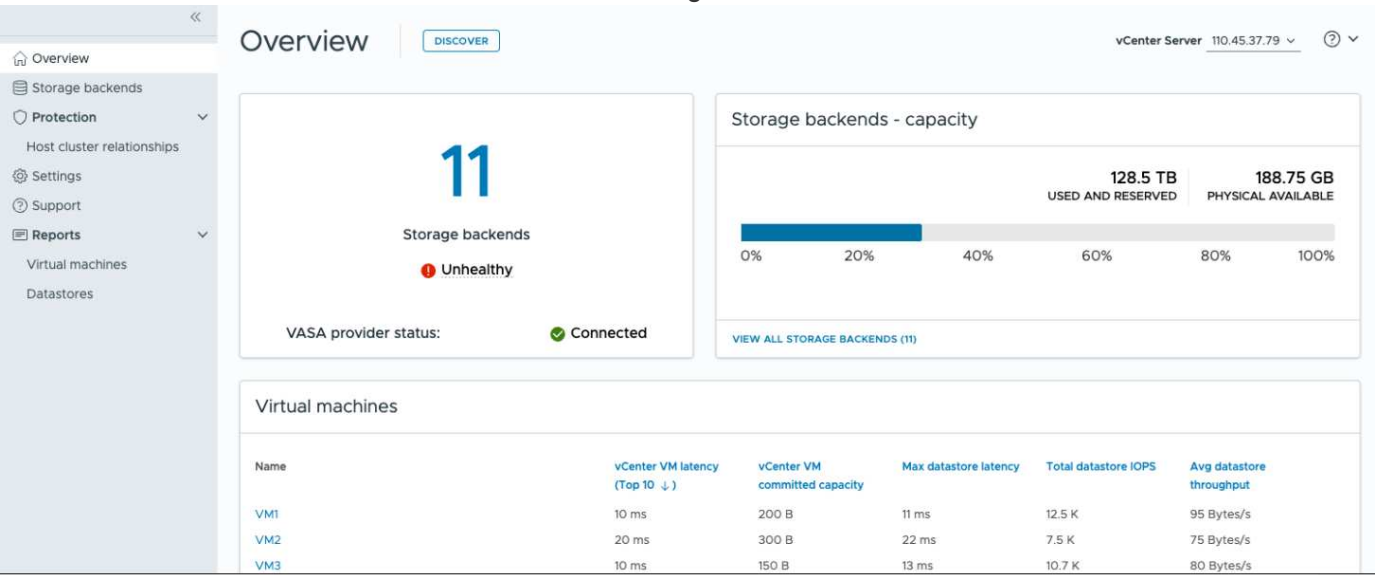
Weitere Informationen finden Sie unter ["Einen Platzhalter-Datenspeicher auswählen"](#)
2. Fügen Sie Datenspeicher zum Hostclusterschutz hinzu, indem Sie ["Geschützten Host-Cluster modifizieren"](#) folgen. Fügen Sie sowohl asynchrone als auch synchrone Richtlinientypen hinzu.

ONTAP tools für VMware vSphere verwalten

Erfahren Sie mehr über das ONTAP tools-Dashboard

Die Auswahl des ONTAP tools for VMware vSphere Plug-in-Symbols im Bereich „Verknüpfungen“ des vCenter Clients öffnet die Übersichtsseite. Dieses Dashboard bietet eine Zusammenfassung des ONTAP tools for VMware vSphere Plug-ins.

Im erweiterten Verknüpfungsmodus (ELM) wird das vCenter Server Dropdown-Menü angezeigt. Ein vCenter Server kann ausgewählt werden, um dessen Daten anzuzeigen. Das Dropdown-Menü ist in allen Listenansichten des Plug-ins verfügbar. Wird auf einer Seite ein vCenter Server ausgewählt, bleibt diese Auswahl auch beim Wechsel zwischen den Tabs im Plug-in erhalten.



Auf der Übersichtsseite kann die **Discovery**-Aktion ausgeführt werden. Die Discovery-Aktion erkennt neu hinzugefügte oder aktualisierte Storage-Backends, Hosts, Datenspeicher sowie den Schutzstatus oder Beziehungen auf vCenter-Ebene. Eine bedarfsgesteuerte Erkennung ist möglich, ohne auf die geplante Erkennung zu warten.



Die Schaltfläche **Discovery** ist nur dann aktiviert, wenn Sie über die erforderliche Privilege zur Durchführung der Discovery verfügen.

Nachdem die Discovery-Anfrage abgeschickt wurde, lässt sich der Fortschritt der Aktion im Bereich „Letzte Aufgaben“ nachverfolgen.

Das Dashboard enthält 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-Backends sowie den allgemeinen Zustand der Speicher-Backends und des VASA Provider an. Der Status der Speicher-Backends wird als Healthy angezeigt, wenn alle Speicher-Backends einen normalen Status haben, und als Unhealthy , wenn ein Speicher-Backend ein Problem hat (Status: Unknown/Nicht erreichbar/Beeinträchtigt). Wählen Sie das Tooltip aus, um die Statusdetails der Speicher-Backends zu öffnen. Sie können ein beliebiges Speicher-Backend für weitere Details auswählen. Der Link Other VASA Provider states zeigt den aktuellen Status des im vCenter Server registrierten VASA Provider an.
Storage Backends Kapazität	Diese Karte zeigt die aggregierte genutzte und verfügbare Kapazität aller Storage-Backends für die ausgewählte vCenter Server-Instanz an. Für ASA r2 Storage-Systeme werden die Kapazitätsdaten nicht angezeigt, da der Storage disaggregiert ist.
Virtuelle Maschinen	Diese Karte zeigt die Top 10 VMs, sortiert nach Leistungsmetrik. Die Überschrift kann ausgewählt werden, um die Top 10 VMs für die ausgewählte Metrik entweder aufsteigend oder absteigend sortiert anzuzeigen. Die auf der Karte vorgenommenen Sortier- und Filteränderungen bleiben erhalten, bis der Browser-Cache geändert oder geleert wird.
Datenspeicher	Diese Karte zeigt die Top 10 Datenspeicher, sortiert nach einer Leistungsmetrik. Die Überschrift kann ausgewählt werden, um die Top 10 Datenspeicher für die ausgewählte Metrik in aufsteigender oder absteigender Reihenfolge anzuzeigen. Die auf der Karte vorgenommenen Sortier- und Filteränderungen bleiben erhalten, bis der Browser-Cache geändert oder geleert wird. Es gibt ein Datenspeichertyp-Drop-down zur Auswahl des Typs der Datenspeicher: NFS, VMFS oder vVols.
ESXi Host Konformitätskarte	Diese Karte zeigt an, ob alle ESXi-Hosts (für das ausgewählte vCenter) die empfohlenen NetApp Host-Einstellungen nach Gruppe oder Kategorie einhalten. Sie können den Link Empfohlene Einstellungen anwenden auswählen, um die empfohlenen Einstellungen zu übernehmen. 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 FC-Protokoll-Host-World-Wide-Port-Namen (WWPNs) oder iSCSI-Host-qualifizierten Knotennamen. Es besteht die Möglichkeit, igroups zu definieren und sie LUNs zuzuordnen, um zu steuern, welche Initiatoren Zugriff

auf LUNs haben.

In ONTAP tools for VMware vSphere 9.x wurden Initiatorgruppen in einer flachen Struktur erstellt und verwaltet, wobei jeder Datenspeicher in vCenter einer einzelnen Initiatorgruppe zugeordnet war. Dieses Modell schränkte die Flexibilität und Wiederverwendbarkeit von Initiatorgruppen über mehrere Datenspeicher hinweg ein. ONTAP tools for VMware vSphere führt verschachtelte Initiatorgruppen ein, bei denen jeder Datenspeicher in vCenter einer übergeordneten Initiatorgruppe zugeordnet ist, während jeder Host mit einer untergeordneten Initiatorgruppe unter dieser übergeordneten Initiatorgruppe verknüpft ist. Benutzerdefinierte übergeordnete Initiatorgruppen mit frei wählbaren Namen können für die Wiederverwendung über mehrere Datenspeicher hinweg definiert werden, um die Verwaltung der Initiatorgruppen zu erleichtern. Der Initiatorgruppen-Workflow ermöglicht die Verwaltung von LUNs und Datenspeichern in ONTAP tools for VMware vSphere. Unterschiedliche Workflows erzeugen verschiedene Initiatorgruppen-Konfigurationen, wie in den folgenden Beispielen dargestellt:



Die genannten Namen dienen lediglich der Veranschaulichung und beziehen sich nicht auf tatsächliche Initiatorgruppen-Namen. ONTAP tools verwaltete Initiatorgruppen verwenden das Präfix „otv_“. Benutzerdefinierte Initiatorgruppen können beliebige Namen erhalten.

Begriff	Beschreibung
DS<number>	Datenspeicher
iqn<number>	Initiator-IQN
Host<number>	Host-MoRef
LUN<number>	LUN-ID
<DSName>Initiatorgruppe<number>	Standard (ONTAP tools verwaltete) übergeordnete Initiatorgruppe
<Host-Moref>Initiatorgruppe<number>	Child Initiatorgruppe
CustomIgroup<number>	Benutzerdefinierte übergeordnete Initiatorgruppe
ClassicIgroup<number>	Igroup wird in ONTAP tools Version 9.x verwendet.

Beispiel 1:

Datenspeicher auf einem einzelnen Host mit einem Initiator erstellen

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

Ergebnis:

- DS1Igroup:
 - host1Igroup → (iqn1: lun1)

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

Beispiel 2:

Vorhandenen Datenspeicher auf einem zusätzlichen Host einbinden

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

Ergebnis:

- DS1lgroup:
 - host1lgroup → (iqn1: lun1)
 - host2lgroup → (iqn2: lun1)

ONTAP tools für VMware vSphere erstellen eine untergeordnete Initiatorgruppe host2lgroup und fügen sie der bestehenden übergeordneten Initiatorgruppe DS1lgroup hinzu.

Beispiel 3:

Einen Datenspeicher von einem Host trennen

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

Ergebnis:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

ONTAP tools for VMware vSphere entfernen die host1lgroup aus der Hierarchie. Das System löscht untergeordnete Initiatorgruppen nicht explizit. Sie werden unter diesen beiden Bedingungen gelöscht:

- Wenn keine LUNs zugeordnet sind, löscht das ONTAP System die untergeordnete Initiatorgruppe.
- Ein geplanter Bereinigungsauftrag entfernt die verwaisten untergeordneten Initiatorgruppen ohne LUN-Zuordnungen. Diese Szenarien gelten nur für von ONTAP tools verwaltete Initiatorgruppen, nicht für benutzerdefinierte.

Beispiel 4:

Datenspeicher löschen

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

Ergebnis:

- DS1lgroup:
 - host2lgroup → (iqn2: lun1)

Übergeordnete und untergeordnete Initiatorgruppen werden entfernt, es sei denn, ein anderer Datenspeicher verwendet die übergeordnete Initiatorgruppe. Untergeordnete Initiatorgruppen werden nicht explizit gelöscht.

Beispiel 5:

Mehrere Datenspeicher unter einer benutzerdefinierten übergeordneten Initiatorgruppe erstellen

Arbeitsablauf:

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

Ergebnis:

- Customlgroup1:
 - host1lgroup → (iqn1: lun2, lun3)
 - host2-Initiatorgruppe → (iqn2: lun2)

- host3Initiatorgruppe → (iqn3: lun3)

Customlgroup1 wird für DS2 erstellt und für DS3 wiederverwendet. Unter dem gemeinsamen übergeordneten Element werden untergeordnete Initiatorgruppen erstellt oder aktualisiert, wobei jede untergeordnete Initiatorgruppe ihren relevanten LUNs zugeordnet wird.

Beispiel 6:

Einen Datenspeicher unter einer benutzerdefinierten übergeordneten Initiatorgruppe löschen.

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

Ergebnis:

- Customlgroup1:
 - host1-Initiatorgruppe → (iqn1: lun3)
 - host3Initiatorgruppe → (iqn3: lun3)
- Auch wenn Customlgroup1 nicht wiederverwendet wird, wird sie nicht gelöscht.
- Wenn keine LUNs zugeordnet sind, löscht das ONTAP System host2lgroup.
- host1lgroup wird nicht gelöscht, da sie lun3 von DS3 zugeordnet ist. Benutzerdefinierte Initiatorgruppen werden unabhängig vom Wiederverwendungsstatus niemals gelöscht.

Beispiel 7:

Datenspeicher für vVols erweitern (Volume hinzufügen)

Arbeitsablauf:

Vor der Erweiterung:

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

- DS4Initiatorgruppe: host4Initiatorgruppe → (iqn4: lun4)

Nach der Erweiterung:

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

- DS4Initiatorgruppe: host4Initiatorgruppe → (iqn4: lun4, lun5)

Eine neue LUN wird erstellt und der bestehenden untergeordneten Initiatorgruppe host4lgroup zugeordnet.

Beispiel 8:

Datenspeicher für vVols verkleinern (Volume entfernen)

Arbeitsablauf:

Vor dem Schrumpfen:

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

- DS4Initiatorgruppe: host4Initiatorgruppe → (iqn4: lun4, lun5)

Nach dem Schrumpfen:

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

- DS4Initiatorgruppe: host4Initiatorgruppe → (iqn4: lun4)

Die angegebene LUN (lun5) ist aus der untergeordneten Initiatorgruppe entfernt. Die Initiatorgruppe bleibt aktiv, solange ihr mindestens eine LUN zugeordnet ist.

Beispiel 9:

Migration von ONTAP tools 9 zu 10 (Initiatorgruppe-Normalisierung)

Arbeitsablauf

ONTAP tools for VMware vSphere 9.x Versionen unterstützen keine hierarchischen Initiatorgruppen. Während der Migration auf Version 10.3 oder höher müssen Initiatorgruppen in die hierarchische Struktur normalisiert werden.

Vor der Migration:

[Migration] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → ClassicInitiatorgruppe1 (iqn6 & iqn7 : lun6, lun7)

Die Logik von ONTAP tools 9.x erlaubt mehrere Initiatoren pro Initiatorgruppe, ohne eine Eins-zu-Eins-Hostzuordnung zu erzwingen.

Nach der Migration:

[Migration] DS6 (lun6, lun7): host6 (iqn6), host7 (iqn7) → Classicgroup1: otv_Classicgroup1 (iqn6 & iqn7 : lun6, lun7)

Während der Migration:

- Eine neue übergeordnete Initiatorgruppe (Classicgroup1) wird erstellt.
- Die ursprüngliche Initiatorgruppe wird mit dem Präfix otv_ umbenannt und wird zu einer untergeordneten Initiatorgruppe.

Dies gewährleistet die Einhaltung des hierarchischen Modells.

Ab ONTAP tools 10.5P2 werden migrierte Initiatorgruppen gelöscht, sobald sie nicht mehr verwendet werden. In früheren Versionen wurden migrierte Initiatorgruppen nie entfernt. Dabei ist Folgendes zu beachten:

- Migrierte igroups können nicht in mehreren Datastores wiederverwendet werden.
- Benutzerdefinierte igroups (benutzerdefiniert) werden niemals gelöscht und können weiterhin wiederverwendet werden.

Verwandte Themen

["Über Initiatorgruppen"](#)

Export-Richtlinien

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 zur Durchsetzung der Zugriffskontrolle verwendet werden. Jede Exportrichtlinie besteht aus Regeln, die die Clients (IP-Adressen oder Subnetze) mit Zugriffsberechtigung und die gewährten Berechtigungen (nur lesend oder lesend/schreibend) festlegen.

Beim Erstellen eines NFS-Datenspeichers in ONTAP tools for VMware vSphere können eine vorhandene Exportrichtlinie ausgewählt oder eine neue erstellt werden. Die Exportrichtlinie wird dann auf den Datenspeicher angewendet, sodass nur autorisierte Clients darauf zugreifen können.

Wenn ein NFS-Datenspeicher auf einem neuen ESXi-Host eingebunden wird, fügt ONTAP tools for VMware vSphere die IP-Adresse des Hosts der bestehenden, dem Datenspeicher zugeordneten Exportrichtlinie hinzu. Dies ermöglicht dem neuen Host den Zugriff auf den Datenspeicher, ohne dass eine neue Exportrichtlinie erstellt werden muss.

Wenn ein NFS-Datenspeicher von einem ESXi-Host gelöscht oder ausgehängt wird, entfernt ONTAP tools for VMware vSphere die IP-Adresse des Hosts aus der Exportrichtlinie. Wenn keine anderen Hosts diese Exportrichtlinie verwenden, wird sie gelöscht. Beim Löschen eines NFS-Datenspeichers entfernt ONTAP tools for VMware vSphere die mit diesem Datenspeicher verknüpfte Exportrichtlinie, sofern sie nicht von anderen Datenspeichern wiederverwendet wird. Wird die Exportrichtlinie wiederverwendet, bleibt die Host-IP-Adresse erhalten und es erfolgt keine Änderung. Beim Löschen der Datenspeicher wird die Zuordnung der Host-IP-Adresse durch die Exportrichtlinie aufgehoben und eine Standard-Exportrichtlinie zugewiesen, sodass die ONTAP Systeme bei Bedarf darauf zugreifen können.

Die Zuweisung der Exportrichtlinie unterscheidet sich, wenn sie für verschiedene Datenspeicher wiederverwendet wird. Bei der Wiederverwendung der Exportrichtlinie kann die Richtlinie um die neue Host-IP-Adresse ergänzt werden. Wenn ein Datenspeicher gelöscht oder ausgehängt wird, der eine gemeinsam genutzte Exportrichtlinie verwendet, 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 ONTAP tools-VMs als auch ONTAP-Speichersysteme verwalten, ist es wichtig, das Verhalten von Initiatorgruppen zu verstehen, insbesondere beim Verschieben von Datenspeichern aus Umgebungen, die nicht von ONTAP tools verwaltet werden, in solche, die es werden. Diese Seite erläutert, wie ONTAP tools für VMware vSphere Initiatorgruppen darstellt und verwaltet. Es handelt sich um konzeptionelle Informationen zum Verständnis der Verhaltensunterschiede zwischen früheren Versionen und dem aktuellen verschachtelten Initiatorgruppenmodell.

Ab ONTAP tools for VMware vSphere 10.4 werden ONTAP- und vCenter-Objekte automatisch erstellt und verwaltet, wodurch die Datenspeicherverwaltung in VMware-Rechenzentrumsumgebungen vereinfacht wird. Ab ONTAP tools for VMware vSphere 10.5 P2 werden migrierte Initiatorgruppen zudem automatisch gelöscht, sobald sie nicht mehr verwendet werden.

Kurze Verhaltenszusammenfassung

- ONTAP Tools-verwaltete VMFS-Datenspeicher verwenden verschachtelte Initiatorgruppen: eine übergeordnete Initiatorgruppe pro Datenspeicherkontext und untergeordnete Initiatorgruppen pro Host.
- LUN-Zuordnungen werden auf untergeordnete Initiatorgruppen angewendet.
- Benutzerdefinierte übergeordnete Initiatorgruppen können datenspeicherübergreifend wiederverwendet werden.

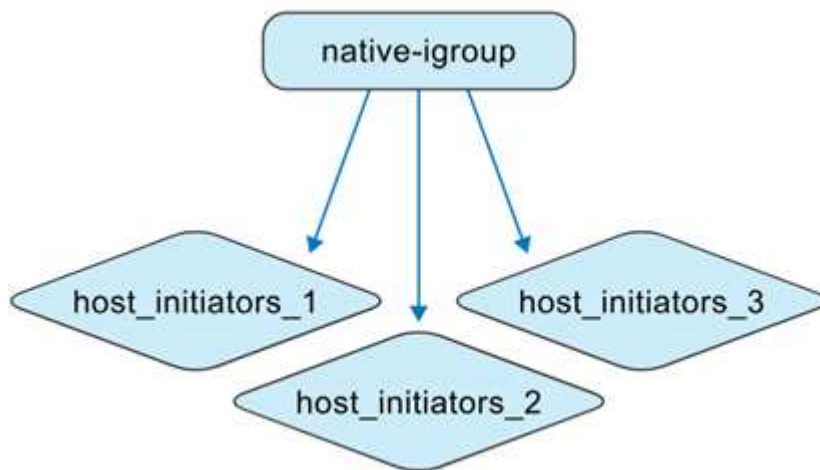
- Migrierte Initiatorgruppen aus ONTAP tools 9.x können nicht wiederverwendet werden.

Initiatorgruppen-Kontexte

ONTAP tools for VMware vSphere verarbeitet Initiatorgruppen in zwei Kontexten.

Nicht-ONTAP Tools verwaltete Initiatorgruppen

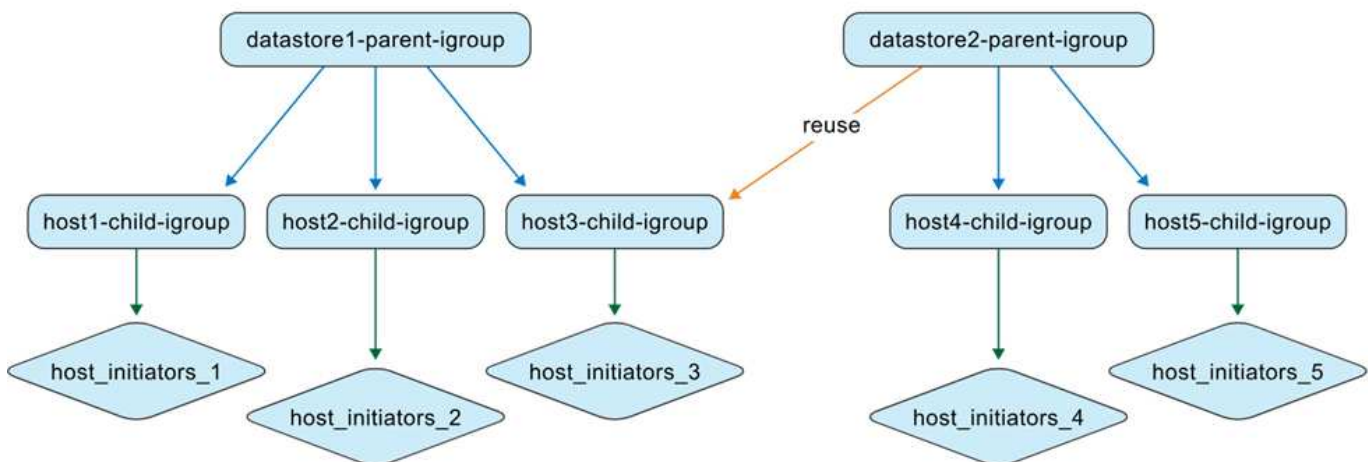
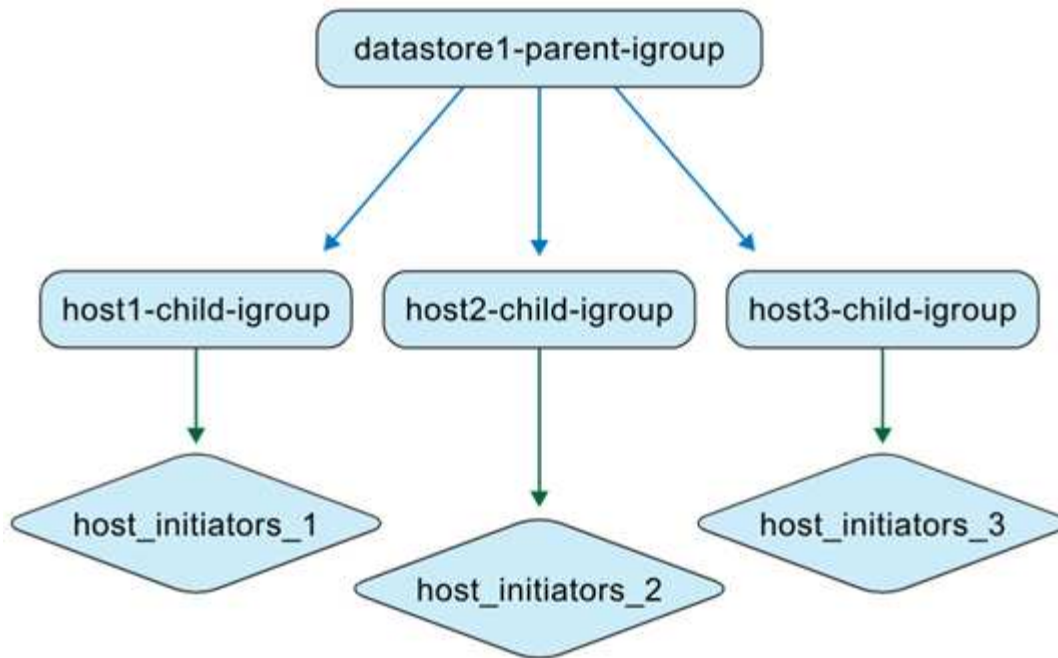
Als Speicheradministrator können Sie auf dem ONTAP-System Initiatorgruppen als flache oder verschachtelte Strukturen erstellen. Die folgende Abbildung zeigt eine flache Initiatorgruppe, die direkt in ONTAP erstellt wurde.



ONTAP tools verwaltete Initiatorgruppen

Wenn Sie Datenspeicher erstellen, erstellt ONTAP tools for VMware vSphere Initiatorgruppen in einer verschachtelten Struktur.

Wenn beispielsweise datastore1 erstellt und auf den Hosts 1, 2 und 3 eingebunden wird und ein neuer datastore (datastore2) erstellt und auf den Hosts 3, 4 und 5 eingebunden wird, verwenden die ONTAP tools die Host-Level-Initiatorgruppe für eine effiziente Verwaltung erneut.



Benennungsverhalten

Wenn Sie einen Datenspeicher erstellen und das Feld Initiatorgruppe leer lassen, erstellt ONTAP tools eine standardmäßige verschachtelte Initiatorgruppe-Struktur.

- Namensmuster der übergeordneten Initiatorgruppe:
`otv_<vcguid>_<host_parent_datacenterMoref>_<datastore_name>`
- Namensmuster für untergeordnete Initiatorgruppen: `otv_<hostMoref>_<vcguid>`

Die ONTAP Benutzeroberfläche der ONTAP-Systeme zeigt die Beziehung zwischen übergeordneten und untergeordneten Initiatorgruppen im Feld **Übergeordnete Initiatorgruppe** an.

Verhalten je nach Szenario

Szenario	Elterngruppenverhalten der Initiatorgruppe	Verhalten von untergeordneten Initiatorgruppen	LUN-Zuordnung und -Sichtbarkeit
Datenspeicher mit Standard-Initiatorgruppe-Einstellung erstellt	Eine standardmäßige, von ONTAP tools verwaltete übergeordnete Initiatorgruppe wird erstellt.	Bei Bedarf werden untergeordnete Initiatorgruppen auf Hostebene erstellt.	LUNs werden untergeordneten Initiatorgruppen zugeordnet. Der Datenspeicher wird im vCenter Server-Inventar angezeigt.
Datenspeicher mit benutzerdefiniertem Initiatorgruppen-Namen erstellt	Es wird eine benutzerdefinierte übergeordnete Initiatorgruppe mit dem angegebenen Namen erstellt.	Vorhandene untergeordnete Initiatorgruppen auf Hostebene werden wiederverwendet, wenn sich Hosts überschneiden.	Die neue Datenspeicher-LUN wird der wiederverwendeten oder neu erstellten untergeordneten Initiatorgruppe zugeordnet. Der Datenspeicher wird im vCenter Server angezeigt.
Vorhandene benutzerdefinierte Initiatorgruppe wird bei der Datenspeichererstellung wiederverwendet	Eine vorhandene benutzerdefinierte übergeordnete Initiatorgruppe wird ausgewählt und wiederverwendet.	Untergeordnete Initiatorgruppen werden basierend auf der Host-Mitgliedschaft wiederverwendet oder erweitert.	Die neue Datenspeicher-LUN wird über die zugehörige untergeordnete Initiatorgruppe zugeordnet. Der Datenspeicher wird im vCenter Server angezeigt.
Datenspeicher und Initiatorgruppe wurden nativ in ONTAP und vCenter erstellt und anschließend von ONTAP tools erkannt.	ONTAP tools erstellt eine übergeordnete Initiatorgruppe in seinem Verwaltungskontext und behält den ursprünglichen Initiatorgruppenamen bei.	ONTAP tools benennt die ursprüngliche Initiatorgruppe mit dem <code>otv_</code> Präfix um und stellt sie als untergeordnete Initiatorgruppe in der Hierarchie dar.	Die Initiatorzuordnungen bleiben unverändert. Nur die Datenspeichern zugeordneten Initiatorgruppen werden während der Erkennung konvertiert.

Benutzerdefinierte Initiatorgruppen-Wiederverwendung und API-Verhalten

In der Benutzeroberfläche der ONTAP tools können Sie beim Erstellen eines Datenspeichers eine vorhandene benutzerdefinierte übergeordnete Initiatorgruppe aus der Dropdown-Liste wiederverwenden.

Das gleiche Verhalten wird über die API unterstützt. Um eine vorhandene Initiatorgruppe bei der Datenspeichererstellung wiederzuverwenden, geben Sie die Initiatorgruppen-UUID in der API-Nutzlast an.

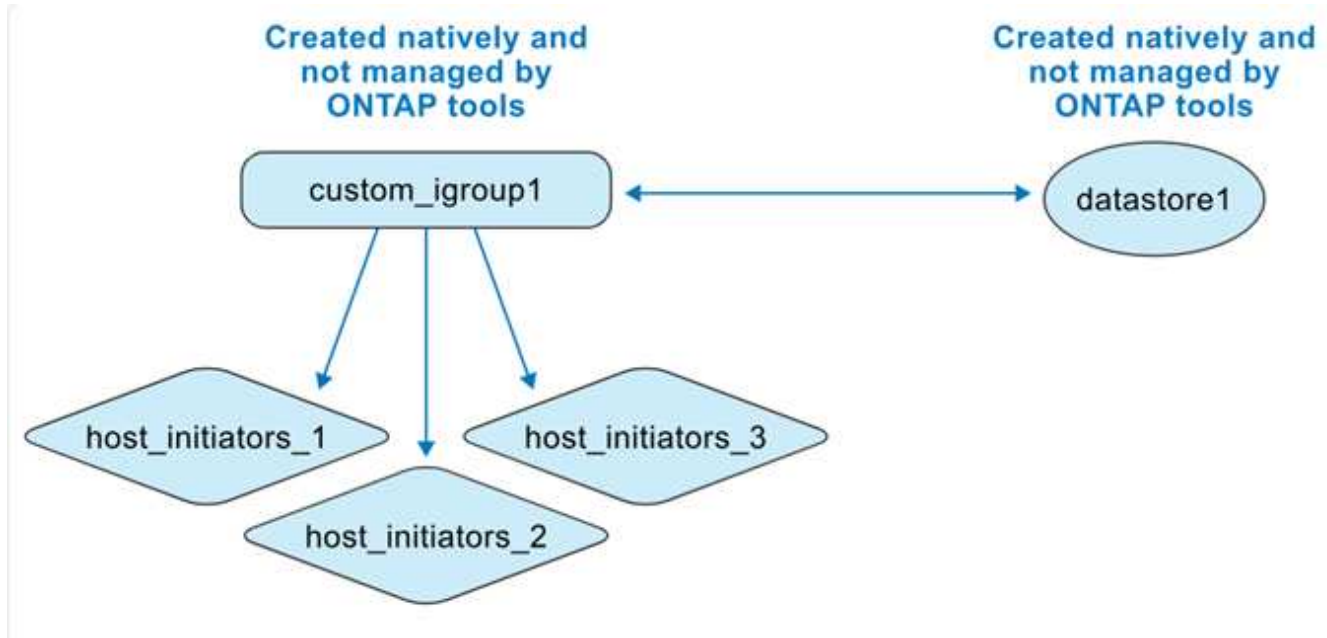


Nur benutzerdefinierte Initiatorgruppen können wiederverwendet werden. Migrierte Initiatorgruppen aus ONTAP tools 9.x können nicht wiederverwendet werden und werden ab ONTAP tools 10.5 P2 automatisch gelöscht, sobald sie nicht mehr verwendet werden.

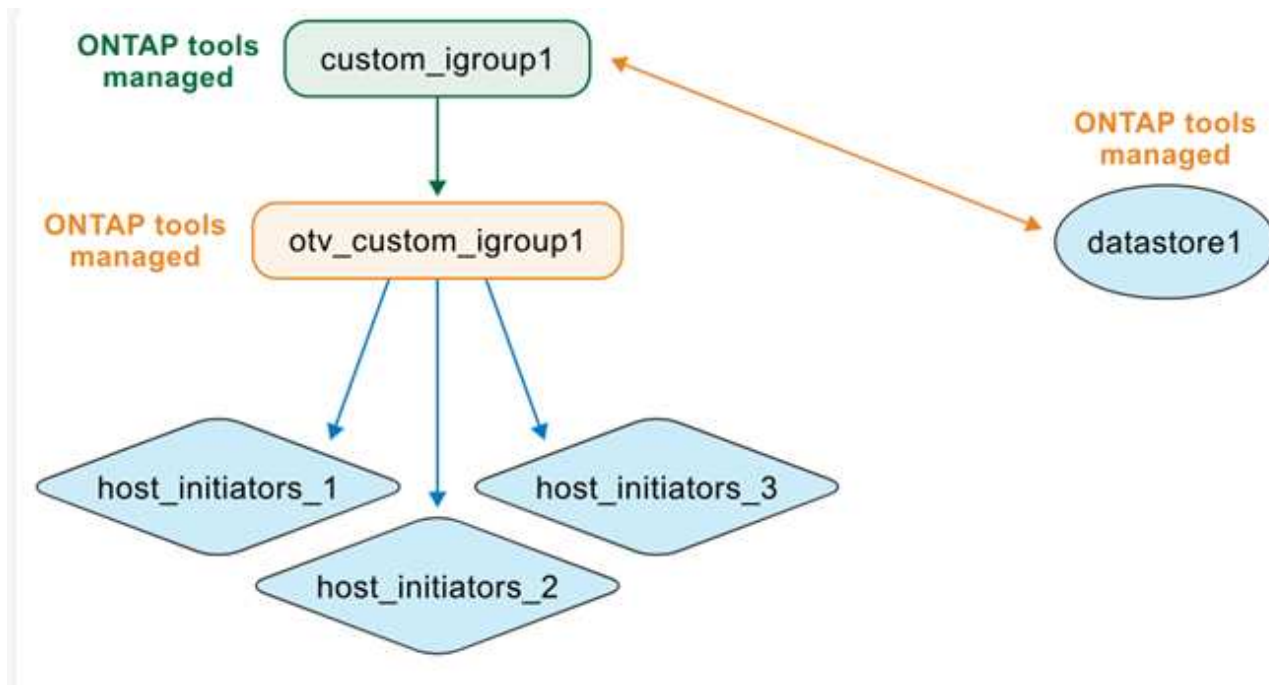
Ansicht zur Konvertierung von nativ zu verwaltet

Wenn Sie die Initiatorgruppe und den Datenspeicher direkt in ONTAP-Systemen und VMware-Umgebungen

erstellen, werden diese Objekte von den ONTAP tools zunächst nicht verwaltet. Dies führt zu einer flachen Initiatorgruppenstruktur.



Nach der Datenspeichererkennung identifiziert und registriert ONTAP tools die datenspeicherzugeordneten Initiatorgruppen und stellt sie anschließend in einem verschachtelten Modell dar. Die übergeordnete Initiatorgruppe wird auf Datensepeicherebene abgebildet, die bestehende Initiatorgruppe wird mit dem `otv_` Präfix als untergeordnete Initiatorgruppe umbenannt, und die Initiatorzuordnungen bleiben unverändert.



ONTAP tools for VMware vSphere erkennen oder verwalten keine Initiatorgruppen, die in ONTAP-Systemen erstellt wurden, aber keinem Datenspeicher zugeordnet oder mit ONTAP tools verknüpft sind. Während der Erkennung konvertieren ONTAP tools nur die Initiatorgruppen, die erkannten Datenspeichern zugeordnet sind; andere Initiatorgruppen bleiben unverwaltet.

Wiederverwendung entdeckter nativer Initiatorgruppen

Nachdem ONTAP tools eine erkannte native Initiatorgruppe verwaltet, steht diese Initiatorgruppe in der Dropdown-Liste für benutzerdefinierte Initiatorgruppennamen zur Erstellung von Datenspeichern zur Verfügung.

Die neue Datastore-LUN wird der normalisierten Child-Initiatorgruppe zugeordnet, zum Beispiel `otv_NativeIgroup1`.

ONTAP tools for VMware vSphere erkennt oder verwendet keine Initiatorgruppen, die in ONTAP-Systemen erstellt wurden, die nicht von ONTAP tools verwaltet werden oder nicht mit einem Datenspeicher verknüpft sind.

Erfahren Sie mehr über die Benutzeroberfläche des ONTAP tools Manager

ONTAP tools for VMware vSphere unterstützt Mandantenfähigkeit, wodurch die Verwaltung mehrerer vCenter Server-Instanzen möglich ist.

ONTAP tools Manager ist eine webbasierte Konsole zur Verwaltung von ONTAP tools für VMware vSphere, vCenter Server-Instanzen, Storage-Backends und Appliance-Konfigurationen wie High Availability (HA) und Node-Scaling.

ONTAP tools Manager bietet folgende Funktionen:

- Warnmeldungen verwalten – Warnmeldungen anzeigen und filtern, die von ONTAP tools for VMware vSphere generiert wurden.
- Speicher-Backends verwalten – ONTAP-Speichercluster hinzufügen und verwalten sowie diese vCenter Server-Instanzen global zuordnen.
- vCenter Server-Instanzen verwalten, vCenter Server-Instanzen innerhalb von ONTAP tools hinzufügen und verwalten.
- Jobs überwachen – Überwachen und debuggen Sie asynchrone Jobs, die sowohl über die ONTAP tools Plug-in-Oberfläche als auch die ONTAP tools Manager-Oberfläche gestartet wurden. Sie können Jobs nach Zeitraum filtern, die Seitengröße anpassen und Jobdetails, einschließlich Fehlern und Unteraufgaben, anzeigen. Klicken Sie auf den Fehlerstatus, um die Fehlerdetails anzuzeigen. Bei Jobs mit Unteraufgaben erweitern Sie die Zeile, um Beschreibungen und Status anzuzeigen. Verwenden Sie für Unterjobs die Drilldown-Funktion des Jobs, um die Details anzuzeigen.
- Protokollpakete herunterladen, Protokolldateien zur Fehlerbehebung von ONTAP tools for VMware vSphere sammeln.
- Zertifikate verwalten: Das selbstsignierte Zertifikat kann durch ein benutzerdefiniertes CA-Zertifikat ersetzt werden, ebenso ist das Erneuern oder Aktualisieren von Zertifikaten für VASA Provider und ONTAP tools möglich.
- Passwörter zurücksetzen: Das Passwort für den VASA Provider und die SRA ändern.
- Geräteeinstellungen verwalten: Die ONTAP tools Appliance konfigurieren, einschließlich der Aktivierung von HA und der Skalierung der Node-Größen.

Um auf ONTAP tools Manager zuzugreifen, `https://<ONTAPtoolsIP>:8443/virtualization/ui/` im Browser starten und sich mit den ONTAP tools for VMware vSphere Administratoranmeldeinformationen anmelden, die während der Bereitstellung angegeben wurden.

ONTAP tools Manager

?

↺

↻

admin

Overview

Alerts

Storage backends

vCenters

Jobs

Log bundles

Certificates

Settings

Overview

EDIT APPLIANCE SETTINGS

Appliance

✓

Healthy

Size

HA ①

VASA Provider ①

SRA ①

Small

Enabled

Enabled

Enabled

VIEW DETAILS

Alerts

Last 24 hours ▾

No alerts

VIEW ALL ALERTS (0)

vCenters

✓ 1

Healthy

VIEW ALL VCENTERS (1)

Storage backends

No storage backends added

VIEW ALL STORAGE BACKENDS (0)

ONTAP tools nodes

vee-lab3-vm41

✓

Healthy

Deploy_OVA_b29c029_998

VIEW DETAILS

vee-lab3-vm184

✓

Healthy

Deploy_OVA_b29c029_9982

VIEW DETAILS

vee-lab3-vm187

✓

Healthy

Deploy_OVA_b29c029_9983

VIEW DETAILS

Karte	Beschreibung
Gerätekarte	Die Appliance-Karte zeigt den Gesamtstatus der ONTAP tools Appliance, Konfigurationsdetails und den Status aktivierter Dienste an. Weitere Informationen sind über den Link View details verfügbar. Wenn eine Appliance-Einstellung geändert wird, zeigt die Karte den Auftragsstatus und die Details an, bis die Änderung abgeschlossen ist.
Benachrichtigungskarte	Die Warnmeldungskarte zeigt ONTAP tools Warnmeldungen, kategorisiert nach Typ, einschließlich HA Node-Name-Ebene-Warnungen. Detaillierte Warnmeldungen werden durch Klicken auf den Anzahl-Hyperlink angezeigt, der zur Warnmeldungsseite führt, gefiltert nach dem ausgewählten Warnmeldungstyp.
vCenters Karte	Die vCenters-Karte zeigt den Status aller von ONTAP tools verwalteten vCenter Serverinstanzen an. Details zu jeder vCenter Instanz sind über den entsprechenden Link einsehbar, der zu einer Seite mit weiteren Informationen zur ausgewählten Instanz führt.

96

Karte	Beschreibung
Storage-Backend-Karte	Die Karte „Storage backends“ zeigt den Zustand und die Konnektivität aller in ONTAP tools konfigurierten ONTAP Storage Cluster an. Details zu jedem Storage backend sind über den entsprechenden Link einsehbar, der zu einer Seite mit weiteren Informationen zum ausgewählten Cluster führt.
ONTAP tools Knotenkarte	Die ONTAP tools Knotenkarte zeigt alle Knoten im Appliance an, einschließlich Node-Name, VM-Name, Status und Netzwerkinformationen. Details anzeigen zeigt weitere Details zu einem bestimmten Knoten an. [HINWEIS] In einer Nicht-HA-Konfiguration erscheint nur ein einzelner Knoten. In einer HA-Konfiguration werden drei Knoten angezeigt.

ONTAP tools Manager-Einstellungen verwalten

ONTAP tools AutoSupport-Einstellungen bearbeiten

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

Deaktivieren AutoSupport

Wenn AutoSupport deaktiviert wird, erfolgt keine proaktive Unterstützung und Überwachung mehr.



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

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Die Option **Einstellungen > Telemetrie > Bearbeiten** auswählen.
4. Deaktivieren Sie die Option **AutoSupport** und speichern Sie die Änderungen.

Proxy-URL für AutoSupport aktualisieren

Die AutoSupport Proxy-URL wird aktualisiert, sodass die AutoSupport Funktion Daten zur sicheren Übertragung über den Proxyserver leitet.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie

während der Bereitstellung angegeben haben.

3. In der Seitenleiste ist **Einstellungen** auszuwählen.
4. Die Option **Einstellungen > Telemetrie > Bearbeiten** auswählen.
5. Eine gültige **Proxy-URL** eingeben und die Änderungen speichern.

Wenn Sie AutoSupport deaktivieren, wird 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. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Die Option **Einstellungen > NTP server > Bearbeiten** auswählen.
4. Geben Sie die durch Kommas getrennten vollqualifizierten Domainnamen (FQDN), IPv4- oder IPv6-Adressen ein.

Aktualisieren Sie die Seite, um die aktualisierten Werte zu sehen.

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

Falls Sie Ihre VASA Provider- oder SRA-Zugangsdaten vergessen, können diese über die ONTAP tools Manager-Oberfläche auf ein neues Passwort zurückgesetzt werden. Das neue Passwort muss zwischen 8 und 256 Zeichen lang sein.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Die Option **Einstellungen > VASA Provider / SRA Anmeldeinformationen > Passwort zurücksetzen** auswählen.
4. Das neue Passwort eingeben und bestätigen.
5. **Speichern** auswählen, um die Änderungen zu übernehmen.

ONTAP tools-Sicherungseinstellungen bearbeiten

Ab ONTAP tools for VMware vSphere 10.5 ist die Backup-Funktion standardmäßig aktiviert und es wird alle 10 Minuten ein Backup erstellt. Das Backup kann deaktiviert oder die Häufigkeit des Backups angepasst werden.

Die Datensicherung sollte nicht deaktiviert werden, da dies ONTAP tools daran hindert, einen niedrigen RPO

aufrechtzuerhalten. Das Deaktivieren der Datensicherung löscht die vorhandenen Sicherungsdateien nicht. Die Häufigkeit der Datensicherung kann auf einen Wert zwischen 10 und 60 Minuten geändert werden.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Die Option **Einstellungen > Sicherung > Bearbeiten** auswählen.
4. Im Bearbeitungsfenster können Sie die Datensicherung deaktivieren oder die Sicherungshäufigkeit bearbeiten.

ONTAP tools-Dienste aktivieren

Das Administratorkennwort kann mit ONTAP tools Manager geändert werden, um Dienste wie VASA Provider, den Import der vVols Konfiguration und Disaster Recovery (SRA) mit ONTAP tools Manager zu ermöglichen.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Im Abschnitt „Übersicht“ ist **Geräteeinstellungen bearbeiten** auszuwählen.
4. Im Abschnitt **Services** lassen sich optionale Dienste wie VASA Provider, Import der vVols Konfiguration und Disaster Recovery (SRA) bei Bedarf aktivieren.

Bei der erstmaligen Aktivierung der Dienste müssen die VASA Provider- und SRA-Zugangsdaten erstellt werden. Diese werden verwendet, um die VASA Provider- und SRA-Dienste auf dem vCenter Server zu registrieren oder zu aktivieren. Der Benutzername darf nur Buchstaben, Zahlen und Unterstriche enthalten. Die Passwortlänge muss zwischen 8 und 256 Zeichen liegen.



Bevor optionale Dienste deaktiviert werden, ist sicherzustellen, dass die von ONTAP tools verwalteten vCenter Server diese nicht verwenden.

Die Option **Import von 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 ONTAP tools Manager, um die ONTAP tools for VMware vSphere Konfiguration zu skalieren, entweder durch Erhöhung der Anzahl der Knoten oder durch Aktivierung von Hochverfügbarkeit (HA). Standardmäßig wird die ONTAP tools for VMware vSphere Appliance als Einzelknoten-, nicht-HA-Konfiguration bereitgestellt.

Bevor Sie beginnen

- Stellen Sie sicher, dass Ihre OVA-Vorlage die gleiche OVA-Version wie Node 1 aufweist. Node 1 ist der Standardknoten, auf dem die ONTAP tools for VMware vSphere OVA initial bereitgestellt wird.
- Sicherstellen, dass CPU Hot Add und Speicher Hot Plug aktiviert sind.
- Im vCenter Server den Automatisierungsgrad des Disaster Recovery Service (DRS) auf teilweise automatisiert setzen. Nach der Bereitstellung von HA wieder auf vollständig automatisiert zurücksetzen.
- Die Hostnamen der Knoten in der HA-Konfiguration sollten in Kleinbuchstaben sein.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Im Abschnitt „Übersicht“ ist **Geräteeinstellungen bearbeiten** auszuwählen.
4. Im Abschnitt **Konfiguration** die Knotengröße erhöhen und die HA-Konfiguration aktivieren. Mit den vCenter Server-Anmeldeinformationen Änderungen vornehmen.

In der HA Konfiguration können die Details der Inhaltsbibliothek geändert werden. Für jede Änderung ist das Passwort anzugeben.



In ONTAP tools for VMware vSphere ist nur eine Vergrößerung der Knotengröße zulässig, eine Verkleinerung ist nicht möglich. In einer Non-HA-Konfiguration wird nur eine mittlere Konfiguration unterstützt. In einer HA-Konfiguration werden mittlere und große Konfigurationen unterstützt.

5. Verwenden Sie den HA-Umschalter, um die HA-Konfiguration zu aktivieren. Auf der Seite **HA-Einstellungen** ist Folgendes sicherzustellen:
 - Die Bibliothek befindet sich auf demselben vCenter Server, auf dem die ONTAP tools Node-VMs ausgeführt werden. vCenter Server-Anmeldeinformationen werden verwendet, um die OVA-Vorlage für Appliance-Änderungen zu validieren und herunterzuladen.
 - Die virtuelle Maschine, auf der die ONTAP tools laufen, wird nicht direkt auf einem ESXi Host bereitgestellt. Die VM sollte in einem Cluster oder einem Ressourcenpool bereitgestellt werden.



Nach der Aktivierung der HA-Konfiguration ist eine Rückkehr zu einer Nicht-HA Single Node Konfiguration nicht mehr möglich.

6. Im Abschnitt **HA-Einstellungen** des Fensters **Geräteeinstellungen bearbeiten** können die Details der Knoten 2 und 3 eingegeben werden. ONTAP tools for VMware vSphere unterstützt drei Knoten in einer HA-Konfiguration.



ONTAP tools füllt die meisten Eingabeoptionen automatisch mit den Netzwerkdetails von Node 1 aus, um den Workflow zu vereinfachen. Die Eingabedaten können vor dem Wechsel zur letzten Seite des Assistenten bearbeitet werden. IPv6-Adressdetails für die beiden anderen Nodes können nur eingegeben werden, wenn die IPv6-Adresse auf dem ONTAP tools Management-Node aktiviert ist.

Stellen Sie sicher, dass jeder ESXi-Host nur eine ONTAP tools VM enthält. Die Eingaben werden bei jedem Wechsel zum nächsten Fenster validiert.

7. Die Details im Abschnitt **Zusammenfassung** sowie die Änderungen unter **Speichern** lassen sich

überprüfen.

Was kommt als Nächstes?

Die Seite **Übersicht** zeigt den Status der Bereitstellung an. Der Status des Auftrags zum Bearbeiten der Geräteeinstellungen kann auch in der Auftragsansicht anhand der Auftrags-ID nachverfolgt werden.

Falls die HA-Bereitstellung fehlschlägt und der Status des neuen Knotens „Neu“ ist, sollte die neue VM in vCenter gelöscht werden, bevor HA erneut aktiviert wird.

Die Registerkarte **Warnungen** im linken Bereich listet Warnungen für ONTAP tools for VMware vSphere auf.

VMware vSphere-Hosts zu ONTAP tools hinzufügen

Neue VMware vSphere Hosts zu ONTAP tools for VMware vSphere hinzufügen, um die Datenspeicher auf den Hosts zu verwalten und zu schützen.

Schritte

1. Einen Host zum VMware vSphere Cluster entsprechend dem Workflow auf Seite "[Hinzufügen eines ESX-Hosts zu Ihrem vSphere Cluster mithilfe des Quickstart-Workflows](#)" hinzufügen.
2. Nach dem Hinzufügen des Hosts im Hauptmenü der ONTAP tools die Option **Discover** im Übersichtsbereich auswählen. Warten, bis der Erkennungsvorgang abgeschlossen ist. Alternativ kann auf den Abschluss der geplanten Host-Erkennung gewartet werden.

Ergebnis

Der neue Host wird nun von ONTAP tools for VMware vSphere erkannt und verwaltet. Die Verwaltung des Datenspeichers auf dem neuen Host ist möglich.

Verwandte Themen

- "[Einen vVols Datenspeicher einbinden](#)" auf neuen Hosts.
- "[NFS und VMFS Datenspeicher einbinden](#)" auf neuen Hosts.

Datenspeicher verwalten

NFS- und VMFS-Datenspeicher in ONTAP tools einbinden

Durch das Einbinden eines Datenspeichers erhalten zusätzliche Hosts Zugriff auf den Speicher. Der Datenspeicher kann auf den zusätzlichen Hosts eingebunden werden, nachdem diese Ihrer VMware Umgebung hinzugefügt wurden.



Wenn ein neuer ESXi-Host mit dem "[Einen ESX-Host zum vSphere Cluster-Workflow hinzufügen](#)" hinzugefügt wird, sollte abgewartet werden, bis die geplante Hosterkennung abgeschlossen ist, bevor er in ONTAP tools erscheint. Alternativ lässt sich die Erkennung manuell über die NetApp ONTAP tools Übersichtsseite ausführen.

Über diese Aufgabe

- Je nach vSphere Client-Version und ausgewähltem Datenspeichertyp sind einige Rechtsklick-Aktionen deaktiviert oder nicht verfügbar.
 - Wenn der vSphere Client 8.0 oder eine spätere Version verwendet wird, sind einige der Rechtsklick-Optionen ausgeblendet.

- Von vSphere 7.0U3 bis vSphere 8.0 Versionen werden die Optionen zwar angezeigt, die Aktion ist jedoch deaktiviert.
- vSphere deaktiviert die Option "Mount Datastore", wenn der Host-Cluster mit einheitlichen Konfigurationen geschützt ist.

Schritte

1. Auf der vSphere Client-Startseite **Hosts und Cluster** auswählen.
2. Wählen Sie im linken Navigationsbereich die Rechenzentren aus, die die Hosts enthalten.
3. Zum Einbinden von NFS/VMFS-Datenspeichern auf einem Host oder einem Host-Cluster mit der rechten Maustaste klicken und **NetApp ONTAP tools > Mount Datastores** auswählen.
4. Wählen Sie die Datenspeicher aus, die eingebunden werden sollen, und wählen Sie **Einbinden**.

Was kommt als Nächstes?

Der Fortschritt ist im Bereich „Letzte Aufgaben“ nachverfolgbar.

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. Sie 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, erscheint eine Warnmeldung auf dem Bildschirm.

3. Wählen Sie einen oder mehrere ESXi-Hosts aus, um den Datenspeicher auszuhängen.

Sie können den Datenspeicher nicht von allen Hosts aushängen. Die Benutzeroberfläche schlägt stattdessen die Verwendung der Operation „Datenspeicher löschen“ vor.

4. Die Schaltfläche **Aushängen** auswählen.

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



Wird der geschützte Datenspeicher ausgehängt, kann die bestehende Schutzeinstellung zu einem teilweisen Schutz führen. Siehe ["Geschützten Host-Cluster modifizieren"](#) zum Aktivieren des vollständigen Schutzes.

Was kommt als Nächstes?

Der Fortschritt kann im Bereich „Letzte Aufgaben“ verfolgt werden.

Einen vVols-Datenspeicher in ONTAP tools einbinden

Ein VMware Virtual Volumes (vVols) Datenspeicher kann auf einem oder mehreren zusätzlichen Hosts eingebunden werden, um diesen Hosts Speicherzugriff bereitzustellen. Das Aushängen eines vVols Datenspeichers ist ausschließlich über die APIs möglich.



Wenn ein neuer ESXi-Host mit dem ["Einen ESX-Host zum vSphere Cluster-Workflow hinzufügen"](#) hinzugefügt wird, sollte abgewartet werden, bis die geplante Hosterkennung abgeschlossen ist, bevor er in ONTAP tools erscheint. Alternativ lässt sich die Erkennung manuell über die NetApp ONTAP tools Übersichtsseite ausführen.

Schritte

1. Auf der vSphere Client-Startseite **Hosts und Cluster** auswählen.
2. Im Navigationsbereich das Rechenzentrum auswählen, das den Datenspeicher enthält.
3. Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **NetApp ONTAP tools > Datenspeicher einbinden**.
4. Im Dialogfeld **Datenspeicher auf Hosts einbinden** die Hosts auswählen, auf denen der Datenspeicher eingebunden werden soll, und anschließend **Einbinden** auswählen.

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 Anpassung der Größe eines Datenspeichers kann der Speicherplatz für die Dateien Ihrer virtuellen Maschinen vergrößert werden. Die Größe eines Datenspeichers kann angepasst werden, wenn sich die Anforderungen Ihrer Infrastruktur 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 bis zu 120 % wachsen.

Schritte

1. Auf der vSphere Client-Startseite **Hosts und Cluster** auswählen.
2. Im Navigationsbereich das Rechenzentrum auswählen, das den Datenspeicher enthält.
3. Klicken Sie mit der rechten Maustaste auf den NFS- oder VMFS-Datenspeicher und wählen Sie **NetApp ONTAP tools > Datenspeichergröße ändern**.
4. Im Dialogfeld „Größe ändern“ eine neue Größe für den Datenspeicher eingeben und **OK** auswählen.

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-in“ die unterstützten Aktionen für ONTAP tools for VMware vSphere angezeigt. Je nach Datenspeichertyp und den

aktuellen Benutzerrechten sind bestimmte Aktionen aktiviert.



Die Funktion „vVols Datastore erweitern“ ist für ASA r2 System-basierte vVols Datastores nicht anwendbar.

Schritte

1. Auf der vSphere Client-Startseite **Hosts und Cluster** auswählen.
2. Im Navigationsbereich das Rechenzentrum auswählen, das den Datenspeicher enthält.
3. Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie **NetApp ONTAP tools > Add storage to datastore**.
4. Im Fenster „Volumes erstellen oder auswählen“ besteht die Möglichkeit, entweder neue Volumes zu erstellen oder aus den vorhandenen Volumes auszuwählen. Die Auswahl erfolgt anhand der Anweisungen auf dem Bildschirm.
5. Im Fenster **Zusammenfassung** können die Auswahlen überprüft und **Erweitern** ausgewählt werden. Der Fortschritt lässt sich im Bereich „Letzte Aufgaben“ nachverfolgen.

Einen vVols Datenspeicher in ONTAP tools verkleinern

Diese Seite erklärt, wie Datenträger aus einem vVols Datenspeicher entfernt werden.

Die Aktion „Speicher aus Datenspeicher entfernen“ kann für jeden von ONTAP tools verwalteten vVols Datenspeicher im vCenter Server verwendet werden.

Sie können keinen Speicher von einem Volume entfernen, wenn es vVols enthält; die Option zum Entfernen ist für solche Volumes deaktiviert. Beim Entfernen von Volumes aus dem Datenspeicher besteht außerdem die Möglichkeit, die ausgewählten Volumes aus dem ONTAP Storage zu löschen.



Die Verkleinerungsoperation für vVols-Datenspeicher wird für vVols-Datenspeicher, die auf ASA r2 Systemen basieren, nicht unterstützt.

Schritte

1. Auf der vSphere Client-Startseite **Hosts und Cluster** auswählen.
2. Im Navigationsbereich das Rechenzentrum auswählen, das den Datenspeicher enthält.
3. Mit der rechten Maustaste auf den vVol Datenspeicher klicken und **NetApp ONTAP tools > Speicher aus dem Datenspeicher entfernen** auswählen.
4. Volumes ohne vVols auswählen und **Entfernen** wählen.



Die Option zur Auswahl des Volumes, auf dem vVols sich befindet, ist deaktiviert.

5. Im Popup **Speicher entfernen** das Kontrollkästchen **Volumes aus ONTAP Cluster löschen** aktivieren, um die Volumes aus dem Datenspeicher und aus dem ONTAP Storage zu löschen, und **Löschen** auswählen.

Datenspeicher in ONTAP tools löschen

Diese Seite beschreibt, wie NFS-, VMFS- oder vVols Datenspeicher mithilfe von ONTAP tools im vCenter Server gelöscht werden.

Beim Löschen eines Datenspeichers werden je nach Datenspeichertyp die folgenden Aktionen ausgeführt:

- Der vVol Container ist ausgehängt.
- Wenn die Initiatorgruppe nicht verwendet wird, werden ihre Initiatoren aus der Initiatorgruppe entfernt.
- Der vVol Container wurde gelöscht.
- FlexVol volumes bleiben auf dem Storage-Array erhalten.

Sie können den Datenspeicher nur löschen, wenn sich keine vVols auf dem ausgewählten Datenspeicher befinden.

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**.



Ein von virtuellen Maschinen verwendeter Datenspeicher kann nicht gelöscht werden. Vor dem Löschen sind die virtuellen Maschinen auf einen anderen Datenspeicher zu verschieben. Das Volume kann nicht gelöscht werden, wenn es Teil eines geschützten Hostclusters ist.

- a. Im Falle eines NFS- oder VMFS-Datenspeichers erscheint ein Dialogfeld mit der Liste der VMs, die den Datenspeicher verwenden.
 - b. Sind keine virtuellen Maschinen mit einem VMFS-Datenspeicher verknüpft, erscheint ein Bestätigungsdialog. Wenn der Hostcluster-Schutz aktiviert ist und eine AFD-Beziehung besteht, ist eine Bereinigung sekundärer Speicherelemente möglich.
 - c. Bei geschützten VMFS-Datenspeichern auf ASA r2 Systemen muss der Schutz vor dem Löschen aufgehoben werden. Ab ONTAP 9.17.1 und ONTAP tools for VMware vSphere 10.5 ist das Löschen eines geschützten Datenspeichers möglich. Handelt es sich um den einzigen Datenspeicher in der Schutzgruppe, wird der Hostcluster-Schutz automatisch entfernt.
 - d. Für vVols Datenspeicher kann der Datenspeicher nur gelöscht werden, wenn keine vVols vorhanden sind. Das Dialogfeld **Datenspeicher löschen** enthält eine Option, um Volumes aus dem ONTAP Cluster zu entfernen.
 - e. Für vVols Datenspeicher auf ASA r2 Systemen können die zugrunde liegenden Volumes nicht mit der Option **Datenspeicher löschen** aus ONTAP gelöscht werden.
3. Zum Löschen der Sicherungsvolumes auf ONTAP Storage ist **Volumes auf ONTAP Cluster löschen** auszuwählen.



Bei VMFS-Datenspeichern auf einheitlichem ONTAP Speicher, die Teil eines geschützten Hostclusters sind, kann das Volume nicht aus dem ONTAP Cluster gelöscht werden.

Beim Löschen eines NFS-, VMFS- oder vVols Datenspeichers bleiben übergeordnete igroups auf dem ONTAP System erhalten. Untergeordnete igroups, die keiner LUN zugeordnet sind, werden automatisch gelöscht. ONTAP tools führen täglich eine Bereinigung durch, um nicht zugeordnete Standard-Parent-igroups zu entfernen. Benutzerdefinierte übergeordnete igroups sind manuell in ONTAP zu löschen. ONTAP tools können veraltete übergeordnete igroups nicht wiederverwenden.

ONTAP-Speicheransichten für Datenspeicher in ONTAP tools

ONTAP tools for VMware vSphere zeigt auf der Registerkarte „Konfigurieren“ die ONTAP-Speicherseitenansicht der Datastores und ihrer Volumes.

Schritte

1. Im vSphere Client zum Datenspeicher wechseln.
2. Im rechten Bereich die Registerkarte **Konfigurieren** auswählen.
3. **NetApp ONTAP tools > ONTAP Storage** auswählen. Die Ansicht ändert sich je nach Datenspeichertyp. Die folgende Tabelle gibt Auskunft:

Datenspeichertyp	Informationen verfügbar
NFS Datenspeicher	Die Seite Speicherdetails enthält Informationen zu Speicher-Backends, Aggregaten und Volumes. Die Seite NFS-Details enthält Daten zum NFS-Datenspeicher.
VMFS-Datenspeicher	Die Seite Speicherdetails enthält Informationen zum Storage-Backend, Aggregat, Volume und zur Storage Availability Zone (SAZ). Die Seite Speichereinheitendetails enthält Details zur Speichereinheit.
vVols Datenspeicher	Hier werden alle Volumes aufgelistet. Speicher kann im ONTAP Speicherbereich erweitert oder entfernt werden. ONTAP tools unterstützen diese Ansicht nicht für ASA r2 systembasierte vVols Datastores.

Ansicht des Speichers virtueller Maschinen in ONTAP tools

Die Speicheransicht zeigt die Liste der vVols, die von der virtuellen Maschine erstellt wurden.



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

Schritte

1. Im vSphere Client zur virtuellen Maschine gehen.
2. Im rechten Bereich die Registerkarte **Monitor** auswählen.
3. **NetApp ONTAP tools > Storage** auswählen. Die **Storage**-Details erscheinen im rechten Bereich. Die Liste der auf der VM vorhandenen vVols ist sichtbar.

Die Option „Spalten verwalten“ ermöglicht das Ein- oder Ausblenden verschiedener Spalten.

Speicherschwellenwerte in ONTAP tools verwalten

Sie können den Schwellenwert festlegen, um Benachrichtigungen im vCenter Server zu erhalten, wenn das Volumen und die Aggregatkapazität bestimmte Werte erreichen.

Schritte:

1. Melden Sie sich beim vSphere Client an.
2. Auf der Seite „Shortcuts“ im Abschnitt „Plug-ins“ ist **NetApp ONTAP tools** auszuwählen.
3. Im linken Bereich von ONTAP tools zu **Einstellungen > Schwellenwerteinstellungen > Bearbeiten** wechseln.
4. Im Fenster **Schwellenwert bearbeiten** die gewünschten Werte in den Feldern **Fast voll** und **Voll** eingeben und **Speichern** auswählen. Die Schwellenwerte können auf die empfohlenen Standardwerte zurückgesetzt werden: 80 für Fast voll und 90 für Voll.

Speicher-Backends in ONTAP tools verwalten

Storage Backends sind Systeme, die von den ESXi-Hosts zur Datenspeicherung verwendet werden.

Speicher entdecken

Die Erkennung eines Storage-Backends kann bei Bedarf durchgeführt werden, ohne auf eine geplante Erkennung warten zu müssen, um die Speicherdetails sofort zu aktualisieren. Für MetroCluster Konfigurationen sollte die ONTAP tools discovery nach einem Switchover manuell ausgeführt werden.

Führen Sie die folgenden Schritte aus, um die Storage-Backends zu ermitteln.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Auf der Seite „Shortcuts“ im Abschnitt „Plug-ins“ ist **NetApp ONTAP tools** auszuwählen.
3. Im linken Bereich der ONTAP tools zu **Storage Backends** wechseln und ein Storage Backend auswählen.
4. Das Menü mit den vertikalen Auslassungspunkten auswählen und anschließend **Discover storage** wählen.

Der Fortschritt kann im Bereich „Letzte Aufgaben“ verfolgt werden.

Storage-Backends ändern

Sie können die Zugangsdaten für das Storage-Backend oder den Portnamen ändern. Das Storage-Backend für globale ONTAP Cluster kann auch mit ONTAP tools Manager angepasst werden. Wenn das Zertifikat in 30 Tagen oder weniger abläuft, zeigt ONTAP tools eine Warnung an. Das Storage-Backend kann angepasst und das neue Zertifikat vom ONTAP Administrator hochgeladen werden.

Wenn das Speicher-Backend geändert wird, führt ONTAP tools for VMware vSphere eine Erkennung des Speicher-Backends durch, um die Speicherdetails zu aktualisieren.

In diesem Abschnitt werden die Schritte zum Modifizieren eines Storage-Backends beschrieben.

1. Melden Sie sich beim vSphere Client an.
2. Auf der Seite „Shortcuts“ im Abschnitt „Plug-ins“ ist **NetApp ONTAP tools** auszuwählen.
3. Im linken Bereich der ONTAP tools zu **Storage Backends** wechseln und ein Storage Backend auswählen.
4. Das vertikale Ellipsenmenü auswählen und **Ändern** wählen, um die Anmeldeinformationen oder den Portnamen zu ändern. Der Fortschritt kann im Bereich „Letzte Aufgaben“ nachverfolgt werden.

Globale ONTAP Cluster mit ONTAP tools Manager wie folgt anpassen.

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Speicher-Backends in der Seitenleiste auswählen.
4. Wählen Sie das Storage Backend aus, das Sie ändern möchten.
5. Das Menü mit den vertikalen Auslassungspunkten auswählen und **Ändern** wählen.
6. Sie können die Zugangsdaten oder den Port ändern. **Benutzername** und **Passwort** eingeben, um das Storage-Backend zu ändern.

Storage-Backends entfernen

Alle an das Storage-Backend angeschlossenen Datenspeicher müssen entfernt werden, bevor es entfernt wird. Die folgenden Schritte sind zu befolgen, um ein Storage-Backend zu entfernen.

1. Melden Sie sich beim vSphere Client an.
2. Auf der Seite „Shortcuts“ im Abschnitt „Plug-ins“ ist **NetApp ONTAP tools** auszuwählen.
3. Im linken Bereich der ONTAP tools zu **Storage Backends** wechseln und ein Storage Backend auswählen.
4. Wählen Sie im Menü mit den drei Punkten die Option **Entfernen**. Stellen Sie sicher, dass das Storage-Backend keine Datenspeicher enthält. Der Fortschritt kann im Bereich „Letzte Aufgaben“ verfolgt werden.

Sie können globale ONTAP-Cluster mit ONTAP tools Manager entfernen.

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. **Storage Backends** in der Seitenleiste auswählen.
4. Wählen Sie das Speicher-Backend aus, das entfernt werden soll.
5. Das Menü mit den vertikalen Auslassungspunkten auswählen und **Entfernen** wählen.

Detaillierte Ansicht des Storage-Backends

Die Seite „Storage Backend“ listet alle Storage Backends auf. Es sind Discover Storage-, Änderungs- und Entfernungsoperationen für die von Ihnen hinzugefügten Storage Backends möglich, jedoch nicht für die einzelnen untergeordneten SVMs im Cluster.

Wählen Sie den übergeordneten Cluster oder das untergeordnete Element aus, um die Komponentenübersicht anzuzeigen. Für den übergeordneten Cluster steht das Dropdown-Menü „Aktionen“ zur Verfügung, um den Storage zu erkennen, zu ändern oder das Storage-Backend zu entfernen.

Die Übersichtsseite enthält folgende Details:

- Status des Storage-Backends
- Kapazitätsinformationen
- Grundlegende Informationen zur VM

- Zertifikatsdetails wie der Zertifikatsstatus und das Ablaufdatum.
- Netzwerkinformationen wie die IP-Adresse und der Port des Netzwerks. Für die untergeordnete SVM sind die Informationen identisch mit denen des übergeordneten Storage-Backends.
- Privileges erlaubt und eingeschränkt für das Storage-Backend. Für das untergeordnete SVM sind die Informationen dieselben wie für das übergeordnete Storage-Backend. ONTAP tools zeigt Privileges nur bei clusterbasierten Storage-Backends an. Wenn Sie SVM als Storage-Backend hinzufügen, werden keine Privileges-Informationen 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 Kapazitäts-Portlet nicht angezeigt. Das Kapazitätsportal ist nur erforderlich, wenn die Eigenschaft „disaggregiert“ für die SVM oder den Cluster auf „true“ gesetzt ist.
- Bei ASA r2 SVM-Systemen wird im Abschnitt Basisinformationen der Plattformtyp angezeigt.

Die Registerkarte „Schnittstelle“ bietet detaillierte Informationen zur Schnittstelle.

Die Registerkarte „Lokale Ebenen“ bietet detaillierte Informationen zur Aggregatliste.

Verwaltung von vCenter Server-Instanzen in ONTAP tools

vCenter Server Instanzen sind zentrale Managementplattformen, die die Steuerung von Hosts, virtuellen Maschinen und Storage-Backends ermöglichen.

Speicher-Backends von der vCenter Server-Instanz trennen

Die vCenter Server-Übersichtsseite zeigt die Anzahl der zugehörigen Storage-Backends an. Jede vCenter Server-Instanz hat die Möglichkeit, einem Storage-Backend zugeordnet oder davon getrennt zu werden.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie die gewünschte vCenter Serverinstanz in der Seitenleiste aus.
4. Wählen Sie die vertikalen Auslassungspunkte neben dem vCenter Server aus, den Sie mit Storage-Backends verknüpfen oder von diesen trennen möchten.
5. **Speicher-Backend trennen** auswählen.

Eine vCenter Server-Instanz ändern

Führen Sie die folgenden Schritte aus, um eine vCenter Serverinstanz zu modifizieren.

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie die entsprechende vCenter Serverinstanz aus der Seitenleiste aus.
4. Wählen Sie die vertikalen Auslassungspunkte neben dem vCenter Server aus, den Sie ändern möchten,

und wählen Sie **Ändern**.

5. Im Fenster **Ändern vCenter** werden Benutzername, Passwort und Portdetails eingegeben.
6. Das Zertifikat wird hochgeladen und **Ändern** ausgewählt.

Eine vCenter Server-Instanz entfernen

Alle Storage-Backends müssen vom vCenter Server entfernt werden, bevor dieser entfernt wird.

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie die entsprechenden vCenter Serverinstanzen aus der Seitenleiste 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 diese nicht mehr von der Anwendung verwaltet.

Wenn vCenter Server-Instanzen in ONTAP tools entfernt werden, erfolgen die folgenden Aktionen automatisch:

- Das Plug-in ist nicht registriert.
- Plug-in-Berechtigungen und Plug-in-Rollen werden entfernt.

Zertifikat des vCenter Servers erneuern

ONTAP tools benachrichtigen Sie, wenn das vCenter-Zertifikat bald abläuft oder bereits abgelaufen ist. Nach der Erneuerung des vCenter-Zertifikats kann das neue Zertifikat mit den folgenden Schritten in ONTAP tools hochgeladen werden:

1. Melden Sie sich bei der ONTAP tools Remote Diagnose-Shell an.
2. Das erneuerte vCenter-Zertifikat kann aus der Diagnose-Shell bezogen werden:

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

3. Das Zertifikat muss im Base 64-ASCII-Format vorliegen und die Anfangs- sowie Endzeile enthalten, zum Beispiel:

ONTAP tools-Zertifikate verwalten

Für ONTAP tools und VASA Provider wird während der Bereitstellung standardmäßig ein selbstsigniertes Zertifikat generiert. Über die ONTAP tools Manager-Oberfläche kann dieses Zertifikat erneuert oder durch ein benutzerdefiniertes CA-Zertifikat ersetzt werden. In Multi-vCenter-Bereitstellungen ist die Verwendung benutzerdefinierter CA-Zertifikate erforderlich.

Bevor Sie beginnen

Folgendes sollte vor Beginn vorhanden sein:

- Der Domänenname, der der virtuellen IP-Adresse zugeordnet ist.
- Erfolgreicher nslookup des Domainnamens, Bestätigung, dass er zur korrekten IP-Adresse aufgelöst wird.
- Zertifikate, die mit dem Domännennamen und der ONTAP tools IP-Adresse erstellt wurden.



Eine ONTAP tools IP-Adresse sollte einem vollqualifizierte Domain (FQDN) zugeordnet sein. Zertifikate sollten denselben FQDN enthalten, der der ONTAP tools IP-Adresse im Subject oder Subject Alternative Names zugeordnet ist.



Ein Wechsel von einem CA-signierten Zertifikat zu einem selbstsignierten Zertifikat ist nicht möglich.

Upgrade ONTAP tools Zertifikat

ONTAP tools Tab zeigt Details wie Zertifikatstyp (selbstsigniert/CA-signiert) und Domainname. Während der Bereitstellung wird standardmäßig ein selbstsigniertes Zertifikat generiert. Das Zertifikat kann erneuert oder auf ein CA-Zertifikat aktualisiert werden.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **Zertifikate** > **ONTAP tools** > **Erneuern**, um die Zertifikate zu erneuern.

Sie können das Zertifikat erneuern, wenn es abgelaufen ist oder sich dem Ablaufdatum nähert. Die Option zum Erneuern ist verfügbar, wenn der Zertifikatstyp CA-signiert ist. Im Pop-up-Fenster sind die Details des Serverzertifikats, des privaten Schlüssels, der Root-CA und des Zwischenzertifikats anzugeben.



Das System bleibt offline, bis das Zertifikat erneuert ist, und Sie werden von der ONTAP tools Manager Oberfläche abgemeldet.

4. Um das selbstsignierte Zertifikat auf ein benutzerdefiniertes CA-Zertifikat zu aktualisieren, **Zertifikate** > **ONTAP tools** > **Upgrade to CA** auswählen.
 - a. Im Popup-Fenster werden die Serverzertifikatsdatei, der private Schlüssel des Serverzertifikats, das Root-CA-Zertifikat und die Zwischenzertifikatsdateien hochgeladen.
 - b. Geben Sie den FQDN der Load Balancer IP ein, für die Sie dieses Zertifikat generiert haben, und aktualisieren Sie das Zertifikat.



Das System bleibt offline, bis das Upgrade abgeschlossen ist, und Sie werden von der ONTAP tools Manager Oberfläche abgemeldet.

Upgrade des VASA Provider-Zertifikats

ONTAP tools for VMware vSphere werden mit einem selbstsignierten Zertifikat für VASA Provider bereitgestellt. Damit kann nur eine vCenter Serverinstanz für vVols Datenspeicher verwaltet werden. Wenn mehrere vCenter Serverinstanzen verwaltet werden und die vVols Funktionalität auf diesen aktiviert werden soll, ist das selbstsignierte Zertifikat durch ein benutzerdefiniertes CA-Zertifikat zu ersetzen.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP tools für VMware vSphere Administratoranmeldeinformationen an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **Zertifikate** > **VASA Provider** oder **ONTAP tools** > **Erneuern**, um die Zertifikate zu erneuern.
4. Wählen Sie **Zertifikate** > **VASA Provider** oder **ONTAP tools** > **Upgrade to CA**, um das selbstsignierte Zertifikat auf ein benutzerdefiniertes CA-Zertifikat zu aktualisieren.
 - a. Im Popup-Fenster werden die Serverzertifikatsdatei, der private Schlüssel des Serverzertifikats, das Root-CA-Zertifikat und die Zwischenzertifikatsdateien hochgeladen.

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



Das System bleibt offline, bis das Upgrade abgeschlossen ist, und Sie werden von der ONTAP tools Manager Oberfläche abgemeldet.

Zugriff auf ONTAP tools für 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. Administrator- und Wartungskennwörter lassen sich aktualisieren, Support-Bundles generieren, Protokollierungsstufen konfigurieren, TLS-Einstellungen verwalten und die Remote-Diagnose aktivieren.

Nach der Bereitstellung von ONTAP tools for VMware vSphere ist bei nicht erreichbarer Wartungskonsole die Installation der VMware tools vom vCenter Server erforderlich. Die Anmeldung erfolgt mit dem `maint` Benutzernamen und dem während der Bereitstellung festgelegten Passwort. **nano** steht zum Bearbeiten von Dateien in der Wartungs- oder Root-Anmeldekonsole zur Verfügung.



Für den `diag`-Benutzer sollte beim Aktivieren der Diagnose ein Passwort festgelegt werden.

Die Registerkarte **Zusammenfassung** der bereitgestellten ONTAP tools for VMware vSphere bietet Zugriff auf die Wartungskonsole. Bei Auswahl von  startet die Wartungskonsole.

Konsolenmenü	Optionen
Anwendungskonfiguration	1. Serverstatusübersicht 2. Protokollebene für ONTAP tools Dienste ändern 3. Zertifikatvalidierungs-Flag ändern
Systemkonfiguration	1. Virtuelle Maschine neu starten 2. Virtuelle Maschine herunterfahren 3. 'maint'-Benutzerpasswort ändern 4. Zeitzone ändern 5. Jail-Datenträgergröße (/jail) erhöhen 6. Upgrade 7. VMware Tools installieren

Netzwerkconfiguration	1. IP-Adresseinstellungen anzeigen 2. Einstellungen für die Domainnamensuche anzeigen 3. Einstellungen für die Domainnamensuche ändern 4. Statische Routen anzeigen 5. Statische Routen ändern 6. Änderungen übernehmen 7. Einen Host anpingen 8. Standardeinstellungen wiederherstellen
Support und Diagnose	1. Zugriff auf die Diagnose-Shell 2. Remote-Diagnosezugriff aktivieren 3. Anmeldeinformationen für vCenter zur Sicherung bereitstellen 4. Backup erstellen

Konfigurieren Sie den Ferndiagnosezugriff für ONTAP tools

Sie können ONTAP tools for VMware vSphere so konfigurieren, dass der SSH-Zugriff für den diag-Benutzer aktiviert wird.

Bevor Sie beginnen

Die VASA Provider Erweiterung für Ihre vCenter Serverinstanz aktivieren.

Über diese Aufgabe

Die Verwendung von SSH für den Zugriff auf das diag-Benutzerkonto hat folgende Einschränkungen:

- Pro SSH-Aktivierung ist nur ein Login-Konto zulässig.
- Der SSH-Zugriff auf das diag-Benutzerkonto ist deaktiviert, wenn eine der folgenden Bedingungen eintritt:
 - Die Zeit ist abgelaufen.

Die Anmeldesitzung läuft am nächsten Tag um Mitternacht ab.

- Sie melden sich erneut als diag-Benutzer per SSH an.

Schritte

1. Vom vCenter Server aus eine Konsole zum VASA Provider öffnen.
2. Melden Sie sich als Wartungsb Benutzer an.
3. Geben Sie 4 ein, um **Support und Diagnose** auszuwählen.
4. Drücken Sie 2, um **Remote-Diagnosezugriff aktivieren** auszuwählen.
5. Geben Sie y im Bestätigungsdia logfeld ein, um den Remote-Diagnosezugriff zu aktivieren.
6. Ein Passwort für den Ferndiagnosezugriff eingeben.

Starten Sie SSH auf anderen ONTAP tools-Knoten

SSH muss auf anderen Knoten gestartet werden, bevor das Upgrade erfolgt.

Bevor Sie beginnen

Die VASA Provider Erweiterung für Ihre vCenter Serverinstanz aktivieren.

Über diese Aufgabe

Dieser Vorgang ist auf jedem Knoten vor dem Upgrade zu wiederholen.

Schritte

1. Vom vCenter Server aus eine Konsole zum VASA Provider öffnen.
2. Melden Sie sich als Wartungsbenutzer an.
3. Geben Sie 4 ein, um Support und Diagnose auszuwählen.
4. Drücken Sie die Eingabetaste 1, um die Access Diagnostic Shell auszuwählen.
5. Geben Sie `y` ein, um fortzufahren.
6. Der Befehl `sudo systemctl restart ssh` wird ausgeführt.

Aktualisieren Sie die vCenter Server-Anmeldeinformationen in ONTAP tools

Sie können die Anmeldeinformationen der vCenter Serverinstanz über die Wartungskonsole aktualisieren.

Bevor Sie beginnen

Sie benötigen die Anmeldedaten für den Wartungsbenutzer.

Über diese Aufgabe

Wenn die vCenter Server-Zugangsdaten nach der Bereitstellung geändert wurden, können sie mit diesem Verfahren aktualisiert werden.

Schritte

1. Vom vCenter Server aus eine Konsole zum VASA Provider öffnen.
2. Melden Sie sich als Wartungsbenutzer an.
3. Geben Sie 2 ein, um das Menü Systemkonfiguration auszuwählen.
4. Geben Sie 8 ein, um die vCenter-Anmeldedaten zu ändern.

Ändern Sie das Zertifikatvalidierungsflag in ONTAP tools

Standardmäßig ist die Zertifikatsvalidierungs-Flag aktiviert (auf true gesetzt). Das ONTAP Speicher-Backend Zertifikatsvalidierungs-Flag kann auf false gesetzt werden, wenn eine Umgehung der SAN-Zertifikatsprüfung erforderlich ist. Diese Einstellung ist nicht anwendbar auf vCenter Server-Zertifikate.

Bevor Sie beginnen

Sie benötigen die Anmeldedaten für den Wartungsbenutzer.

Schritte

1. Vom vCenter Server aus eine Konsole zu ONTAP tools öffnen.
2. Melden Sie sich als Wartungsbenutzer an.
3. Geben Sie 1 ein, um das Menü **Application Configuration** auszuwählen.
4. Geben Sie 3 ein, 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 das Flag umzuschalten, oder 'n', um abubrechen.

Wenn die Zertifikatsvalidierungs-Flagge aktiviert ist (auf „true“ gesetzt), prüft ONTAP tools, ob alle Storage-Backends Zertifikate mit einem Subject Alternative Name (SAN) verwenden. Wenn ein Backend ein Zertifikat ohne SAN verwendet, kann die Zertifikatsvalidierung nicht aktiviert werden. Vor der Aktivierung dieser Flagge sollte überprüft werden, dass alle Storage-Backends SAN-basierte Zertifikate verwenden. Wenn die Zertifikatsvalidierungs-Flagge deaktiviert ist (auf „false“ gesetzt), überspringen ONTAP tools die Zertifikatsvalidierung für alle konfigurierten Storage-Backends.

SAN-basierte Zertifikate für Storage-Backends überprüfen

Um eine sichere Kommunikation und ordnungsgemäße Validierung zu gewährleisten, überprüfen Sie, ob alle Storage-Backends SAN-basierte Zertifikate verwenden:

1. Prüfen Sie, ob das ONTAP-Managementzertifikat einen Subject Alternative Name (SAN)-Eintrag enthält.
2. Bestätigen Sie, dass die SAN-Einträge mit der ONTAP-Management-IP-Adresse oder dem DNS-Namen oder beiden übereinstimmen.
3. Stellen Sie sicher, dass die für die Onboarding von ONTAP verwendeten Details mit der IP-Adresse oder dem DNS-Namen im SAN-Eintrag des Zertifikats übereinstimmen.

Durch die Befolgung dieser Schritte lassen sich Probleme bei der Zertifikatsvalidierung vermeiden und sicherstellen, dass das ONTAP-System sicher integriert ist.

Das folgende Beispielzertifikat zeigt die dekodierten Informationen:

```
HG8u6GK r2JJonWe/kjoKTUnkjwW7feDI747RUuFrthcvTDqhBNWL76jihNp1VX7
v0SDWMaVdecTeU1X/1X3qMxiL+tU4p9SbKVpQw6hjM/zi0LNC784EYIOSQ7qVob
6f21mfPOJHbqs5fLim9NFFUu2DQIDAQA8oQw0jBABgNVHREEEOT43hwShsSHdKXsgi9z
dGkyMjAtdnNpbS1zcjA1MWUtY2OuY2Rs LmdkbC5lbmdsYWJuZKThcPHauY29nt
BgkqhkiG9wQBAQsFAAOCCAQAEEagptz11RN7PLuJUo-SSQExBsF5/3JHr0+sSIMZDzm
4P24kxbxQZbfryy68itKGF4LeAid0hgyxc3y9iv4zKlx85fLNgiTnVqAe8'KYNoyD6
IEWppDUE0eVNZIZQjrz9QjUAAF9ifjq8+SKr'lphoXnYYUiM6utvobPMG8cR8Gca
jiLibiMM01K6rD7Ng+7+ydUCAwBQwMDDwdn8+7RIRdKgwx9QDLegcC5IL5WFLwbMc
2GBv8VM839m0KUAKXSDGwJBZ5nSHQdNi7MU3AES7Nzkv63kGEQJT/5Wr1DmOwlf
osl4qeeeMRigrAbFL6EHMsOMSP0521rtTrJrjBooB22r0tyDA--
-----END CERTIFICATE-----
```

Certificate Information:

- ✓ Common Name: **test.xyz.com**
- ✓ Subject Alternative Names: IP Address: **xxx.xx.xxx.xxx**, **test.xyz.com**
- ✓ Organization: Self-signed-certificate
- ✓ Organization Unit:
- ✓ Locality: N/A
- ✓ State: N/A
- ✓ Country: XX
- ✓ Valid From: March 8, 2026
- ✓ Valid To: March 7, 2028
- ✓ Issuer: **test.xyz.com**, Self-signed-certificate
- ✓ Serial Number: 640c2752bd2c972c5775180070cfdd2120809ee

ONTAP tools Berichte

ONTAP tools for VMware vSphere Plug-in stellt Berichte für virtuelle Maschinen und Datenspeicher bereit. Bei Auswahl des NetApp ONTAP tools for VMware vSphere Plug-in-Symbols im Schnellzugriffsbereich des vCenter Clients wird die Benutzeroberfläche auf die Übersichtsseite weitergeleitet. Im Tab „Berichte“ kann der Bericht für die virtuelle Maschine und die Datenspeicher eingesehen werden.

Der Bericht „Virtuelle Maschinen“ zeigt die Liste der erkannten virtuellen Maschinen (mit mindestens einer Festplatte aus ONTAP Storage-basierten Datastores) mit Leistungskennzahlen. Beim Erweitern des VM-Eintrags werden alle festplattenbezogenen Datastore-Informationen angezeigt.

Der Datenspeicherbericht listet von ONTAP tools for VMware vSphere erkannte oder identifizierte Datenspeicher auf, die beliebigen ONTAP Storage verwenden, mit Leistungskennzahlen.

Die Option „Spalten verwalten“ ermöglicht das Ein- oder Ausblenden verschiedener Spalten.

Virtuelle Maschinen verwalten

Überlegungen zur Migration und zum Klonen virtueller Maschinen für ONTAP tools

ONTAP tools für VMware vSphere unterstützen alle gängigen Arten der virtuellen Maschinenmigration, einschließlich reiner Compute- (vMotion), reiner Storage- (Storage vMotion) und kombinierter Compute- und Storage-Migration über alle Datenspeicher hinweg. In diesem Abschnitt werden wichtige Aspekte und Best Practices für eine erfolgreiche Migration und das Klonen von virtuellen Maschinen unabhängig vom zugrunde liegenden Datenspeichertyp erläutert.

Geschützte virtuelle Maschinen migrieren

Sie können geschützte virtuelle Maschinen migrieren zu:

- Derselbe Datenspeicher auf einem anderen ESXi-Host
- Ein anderer kompatibler Datenspeicher auf demselben ESXi-Host
- Ein anderer kompatibler Datenspeicher auf einem anderen ESXi-Host

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

Informationen zur Migration virtueller Maschinen finden Sie in der Broadcom-Dokumentation: ["vSphere Migration virtueller Maschinen"](#)

Geschützte virtuelle Maschinen klonen

Geschützte virtuelle Maschinen können in die folgenden Verzeichnisse geklont werden:

- Derselbe Container desselben FlexVol volume unter Verwendung einer Replikationsgruppe

Die Metadatendatei desselben FlexVol volumes wird mit den Details der geklonten virtuellen Maschine aktualisiert.

- Derselbe Container eines anderen FlexVol volume unter Verwendung einer Replikationsgruppe

Im FlexVol volume, in dem die geklonte virtuelle Maschine abgelegt ist, wird die Metadatendatei mit den Details der geklonten virtuellen Maschine aktualisiert.

- Ein anderer Container oder vVols Datenspeicher

Im FlexVol volume, in dem die geklonte virtuelle Maschine platziert ist, wird die Metadatendatei mit den Details der virtuellen Maschine aktualisiert.

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

Das Klonen eines Klonen einer geschützten virtuellen Maschine wird unterstützt.

Weitere Einzelheiten finden Sie in der Broadcom-Dokumentation: ["Erstellen einer virtuellen Maschine zum Klonen"](#).

Snapshots virtueller Maschinen

ONTAP tools unterstützt Snapshots virtueller Maschinen über standardmäßige VMware-Workflows. Snapshots sind kurzfristige Wiederherstellungspunkte, die für Anwendungsfälle wie Tests und Patch-Vorbereitung vorgesehen sind. Sie sind kein Ersatz für Backup oder replikationsbasierte Datensicherung. Der Betrieb einer virtuellen Maschine auf einem Snapshot über längere Zeiträume kann zu Instabilität und Datenverlust führen.

Sie können absturzkonsistente Snapshots (Snapshots ohne Speicherzustand, mit denen die virtuelle Maschine in einen konsistenten Zustand neu gestartet werden kann) auf allen unterstützten Datenspeichertypen erstellen. Auch quiesced Snapshots, die VMware Tools verwenden, um die Daten im Arbeitsspeicher vor der Erfassung auf die Festplatte zu schreiben, werden unterstützt. Eine Übersicht über Snapshot-Typen und deren Verhalten finden Sie unter ["Übersicht über Snapshots virtueller Maschinen in vSphere"](#).



Speicher-Snapshots erfassen den aktuellen Speicherzustand und führen zu einer temporären Unterbrechung der virtuellen Maschine. Sie werden in ONTAP tools Workflows nicht unterstützt. Wenn eine virtuelle Maschine über einen Speicher-Snapshot verfügt, muss dieser gelöscht werden, bevor die virtuelle Maschine in eine Konsistenzgruppe oder eine Host-Cluster-Beziehung aufgenommen werden kann, die von ONTAP tools verwaltet wird.

Auf ASA r2-Speichersystemen unterscheidet sich das Verhalten von VM-Snapshots von anderen Speichertypen. Snapshots sind schreibgeschützt. Beim Einschalten der virtuellen Maschine erstellt der VASA Provider eine LUN aus dem schreibgeschützten Snapshot und aktiviert IOPS. Beim Ausschalten der virtuellen Maschine löscht der VASA Provider die LUN und deaktiviert IOPS.

Informationen zur Verwaltung von Snapshots virtueller Maschinen finden Sie in der Broadcom-Dokumentation ["Virtuelle Maschinen mit Snapshots verwalten"](#).

Migrieren Sie virtuelle Maschinen zu vVols-Datenspeichern in ONTAP tools

Virtuelle Maschinen lassen sich von NFS- und VMFS-Datenspeichern auf Virtual Volumes (vVols)-Datenspeicher migrieren, sodass die Vorteile der richtlinienbasierten VM-Verwaltung und weiterer vVols-Funktionen genutzt werden können. vVols-Datenspeicher ermöglichen die Erfüllung gesteigerter Workload-Anforderungen.

Bevor Sie beginnen

Stellen Sie sicher, dass der VASA Provider auf keiner der virtuellen Maschinen ausgeführt wird, die Sie migrieren möchten. Wenn eine virtuelle Maschine, auf der der VASA Provider ausgeführt wird, auf einen vVols Datenspeicher migriert wird, sind keine Verwaltungsoperationen möglich, einschließlich des Einschaltens der virtuellen Maschinen, die sich auf vVols Datenspeichern befinden.

Über diese Aufgabe

Bei der Migration von einem NFS- und VMFS-Datenspeicher zu einem vVols-Datenspeicher verwendet der vCenter Server vStorage APIs für Array Integration (VAAI) Offloads beim Verschieben von Daten aus VMFS-Datenspeichern, jedoch nicht aus einer NFS-VMDK-Datei. VAAI Offloads reduzieren normalerweise die Last auf dem Host.

Schritte

1. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, die migriert werden soll, und wählen Sie **Migrieren**.
2. **Nur Speicher ändern** auswählen und dann **Weiter** wählen.
3. Wählen Sie ein virtuelles Festplattenformat, eine VM-Speicherrichtlinie und einen vVol Datenspeicher, der den Funktionen des zu migrierenden Datenspeichers entspricht.

4. Die Einstellungen werden überprüft und **Fertigstellen** wird ausgewählt.

Bereinigen Sie die VASA-Konfigurationen in ONTAP tools

Um den VASA Bereinigungsprozess abzuschließen, sind die folgenden Schritte erforderlich.



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

Schritte

1. Das Plug-in kann abgemeldet werden, indem zu https://OTV_IP:8143/Register.html gewechselt wird.
2. Es wird überprüft, ob das Plug-in auf dem vCenter Server nicht mehr verfügbar ist.
3. ONTAP tools für VMware vSphere VM herunterfahren.
4. ONTAP tools für VMware vSphere VM löschen.

Eine Datenfestplatte an eine VM in ONTAP tools anhängen oder trennen

Führen Sie die folgenden Schritte aus, um Datenträger an virtuelle Maschinen in vSphere anzuhängen oder von ihnen zu trennen und deren Speicherressourcen zu verwalten.

Einer virtuellen Maschine eine Datenfestplatte hinzufügen

Eine Datenfestplatte kann an eine virtuelle Maschine angehängt werden, um zusätzlichen Speicherplatz bereitzustellen.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Mit der rechten Maustaste auf eine virtuelle Maschine im Inventar klicken und **Einstellungen bearbeiten** auswählen.
3. Auf der Registerkarte **Virtuelle Hardware** wird **Vorhandene Festplatte** ausgewählt.
4. Wählen Sie die virtuelle Maschine aus, in der sich die Festplatte befindet.
5. Wählen Sie die Festplatte aus, die Sie anhängen möchten, und wählen Sie die Schaltfläche **OK** aus.

Ergebnis

Die Festplatte wird in der Liste der virtuellen Hardwaregeräte angezeigt.

Eine Datenfestplatte von der virtuellen Maschine trennen

Eine Datenfestplatte kann von einer virtuellen Maschine getrennt werden, wenn sie nicht mehr benötigt wird. Die Festplatte wird nicht gelöscht, sondern verbleibt im ONTAP Storage-System.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Mit der rechten Maustaste auf eine virtuelle Maschine im Inventar klicken und **Einstellungen bearbeiten** auswählen.
3. Bewegen Sie den Mauszeiger über die Festplatte und wählen Sie **Entfernen**.



Die Festplatte wird aus der virtuellen Maschine entfernt. Wenn andere virtuelle Maschinen die Festplatte gemeinsam nutzen, werden die Festplattendateien nicht gelöscht.

Verwandte Informationen

["Einer virtuellen Maschine eine neue Festplatte hinzufügen"](#)

["Hinzufügen einer vorhandenen Festplatte zu einer virtuellen Maschine"](#)

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, deren zugehörige LUNs und NFS-Exporte sowie die NetApp Speichersysteme erkannt, denen diese Ressourcen zugeordnet sind.

Bevor Sie beginnen

- Alle ESXi Hosts müssen eingeschaltet und verbunden sein.
- Es muss sichergestellt sein, dass alle zu erkennenden Storage Virtual Machines (SVMs) in Betrieb sind und dass auf jedem Cluster-Knoten 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. Es besteht außerdem die Möglichkeit, ONTAP tools for VMware vSphere Anmeldedaten für den Zugriff auf das Speichersystem zu ändern.

Während der Erkennung der Speichersysteme sammelt ONTAP tools for VMware vSphere Informationen von den ESXi-Hosts, die von der vCenter Serverinstanz verwaltet werden.

Schritte

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

Im Dialogfeld **Bestätigen** wird die Auswahl bestätigt.

3. Wählen Sie die erkannten Speichercontroller aus, die den Status `Authentication Failure` haben, und wählen Sie **Aktionen > Ändern**.
4. Geben Sie die erforderlichen Informationen im Dialogfeld **Speichersystem ändern** ein.
5. Wiederholen Sie die Schritte 4 und 5 für alle Speichercontroller mit `Authentication Failure` Status.

Nach Abschluss des Ermittlungsprozesses sind die folgenden Aktionen auszuführen:

- Mit ONTAP tools for VMware vSphere lassen sich ESXi-Hosteinstellungen für Hosts konfigurieren, die das Warnsymbol in der Spalte Adaptereinstellungen, der Spalte MPIO-Einstellungen oder der Spalte NFS-Einstellungen anzeigen.
- Geben Sie die Zugangsdaten für das Speichersystem an.

ESXi-Hosteinstellungen mit ONTAP tools ändern

Das ONTAP tools Dashboard in VMware vSphere bietet die Möglichkeit, Konfigurationsprobleme zu identifizieren, ESXi Hosts auszuwählen, von NetApp empfohlene Einstellungen zu überprüfen und diese anzuwenden.

Bevor Sie beginnen

Das Portlet „ESXi-Hostsysteme“ zeigt Probleme mit den ESXi-Hosteinstellungen an. Ein Problem kann ausgewählt werden, um den Hostnamen oder die IP-Adresse anzuzeigen.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Auf der Seite „Shortcuts“ im Abschnitt „Plug-ins“ ist **NetApp ONTAP tools** auszuwählen.
3. Zum Portlet **ESXi Host compliance** im Überblick (Dashboard) des ONTAP tools for VMware vSphere Plug-in wechseln.
4. Den Link **Empfohlene Einstellungen anwenden** auswählen.
5. Im Fenster **Empfohlene Hosteinstellungen anwenden** die Hosts auswählen, für die NetApp empfohlene Hosteinstellungen verwendet werden sollen, und **Weiter** auswählen.



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

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

Verwandte Informationen

["ESXi Host-Einstellungen konfigurieren"](#)

Passwörter verwalten

ONTAP tools Manager-Passwort ändern

Das Administratorpasswort lässt sich mit ONTAP tools Manager ändern.

Schritte

1. ONTAP tools Manager aus einem Webbrowser starten:
`https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit Ihren Administrator-Anmeldedaten für ONTAP tools for VMware vSphere an.
3. Das **Administrator**-Symbol in der oberen rechten Ecke des Bildschirms auswählen und **Passwort ändern** auswählen.
4. Im Pop-up-Fenster zum Ändern des Passworts werden das alte und das neue Passwort eingegeben. Auf dem Bildschirm der Benutzeroberfläche werden die Passwortanforderungen angezeigt.
5. **Ändern** auswählen, um die Änderungen anzuwenden.

ONTAP tools Manager-Passwort zurücksetzen

Wenn das ONTAP tools Manager-Passwort vergessen wurde, lässt sich der Administratorzugriff mithilfe eines Reset-Tokens wiederherstellen, das von der ONTAP tools for VMware vSphere Wartungskonsole generiert wurde.

Schritte

1. Einen Webbrowser öffnen und zu <https://<ONTAPtoolsIP>:8443/virtualization/ui/> navigieren, um auf ONTAP tools Manager zuzugreifen.
2. Auf der Anmeldeseite die Option **Passwort zurücksetzen** auswählen.
3. Ein Token zum Zurücksetzen des Kennworts wird mithilfe der ONTAP tools for VMware vSphere Wartungskonsole generiert:
 - a. Melden Sie sich am vCenter Server an und öffnen Sie die Wartungskonsole.
 - b. Geben Sie 2 ein, um **System Configuration** auszuwählen.
 - c. Drücken Sie die Eingabetaste 3, um **Passwort des 'maint'-Benutzers ändern** auszuwählen.
4. Im Dialogfeld zum Zurücksetzen des Passworts das Reset-Token, den Benutzernamen und das neue Passwort eingeben.
5. **Zurücksetzen** auswählen, um die Anmeldeinformationen zu aktualisieren.
6. Melden Sie sich mit dem neuen Passwort beim ONTAP tools Manager an.

Anwendungsbutzerpasswort in ONTAP tools zurücksetzen

Die folgenden Schritte setzen das für die SRA- und VASA-Provider-Registrierung beim vCenter Server benötigte Anwendungsbutzerkennwort mithilfe von ONTAP tools for VMware vSphere zurück.

Schritte

1. Einen Webbrowser öffnen und zu folgendem navigieren:
<https://<ONTAPtoolsIP>:8443/virtualization/ui/>
2. Melden Sie sich mit den Administratoranmeldeinformationen an, die während der Bereitstellung der ONTAP tools konfiguriert wurden.
3. In der Seitenleiste **Einstellungen** auswählen.
4. Auf der Seite **VASA/SRA credentials** die Option **Passwort zurücksetzen** auswählen.
5. Das neue Passwort eingeben und bestätigen.
6. **Zurücksetzen** auswählen, um das neue Passwort anzuwenden.

Passwort der ONTAP tools for VMware vSphere Wartungskonsole zurücksetzen

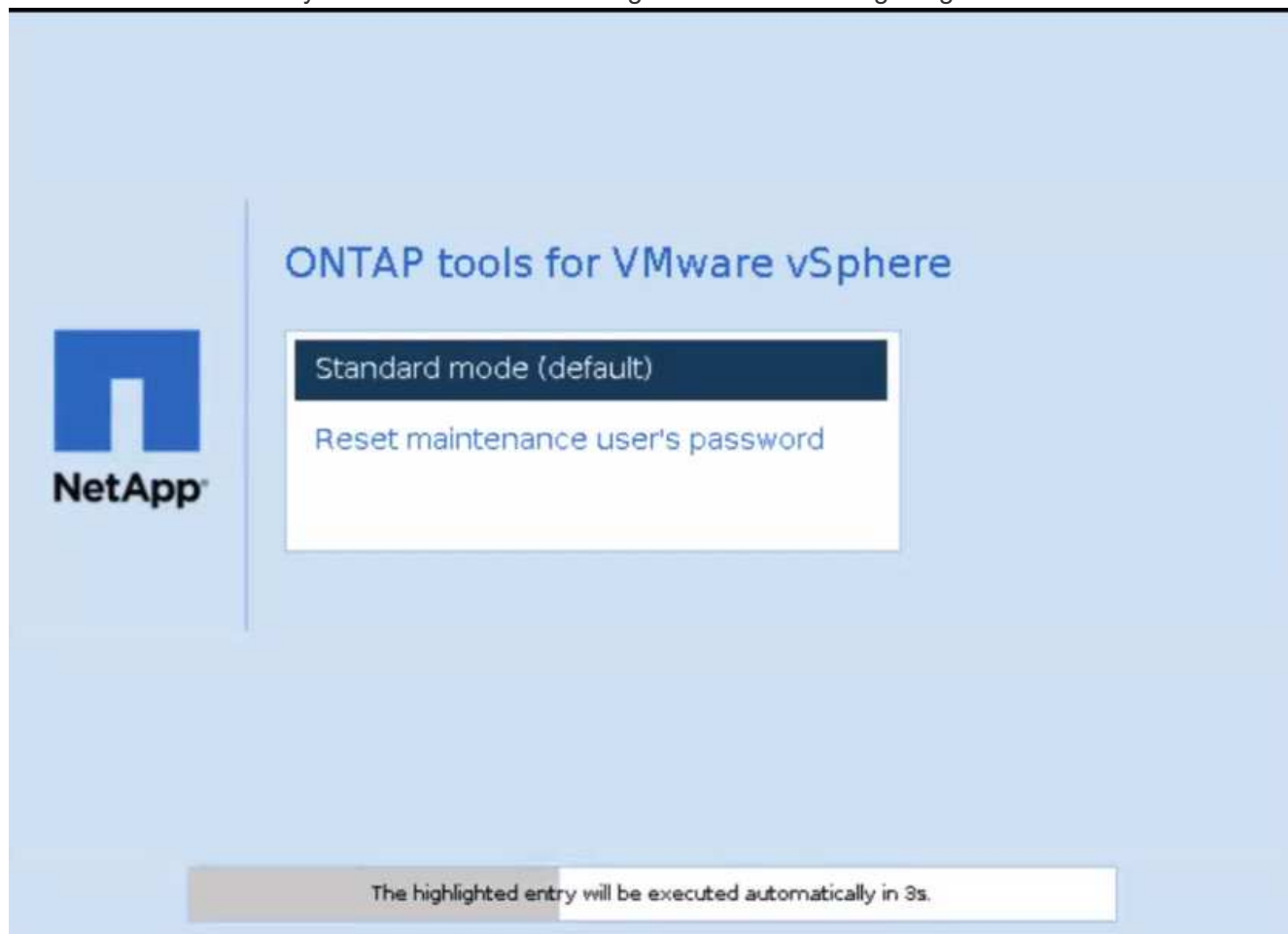
Beim Neustart des Gastbetriebssystems bietet das GRUB-Menü die Option, das Passwort des Wartungskonsolenbenutzers zurückzusetzen. Verwenden Sie diese Option, um das Passwort des Wartungskonsolenbenutzers auf der VM zu aktualisieren. Nach dem Zurücksetzen des Passworts wird die VM neu gestartet, um das neue Passwort festzulegen. In einer HA-Bereitstellung wird das Passwort nach dem Neustart der VM automatisch auf den beiden anderen VMs aktualisiert.



Für die HA-Bereitstellung von ONTAP tools for VMware vSphere sollte das Benutzerkennwort der Wartungskonsole auf dem ONTAP tools Management-Knoten, also node1, geändert werden.

Schritte

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



Sie haben 5 Sekunden Zeit, um Ihre Option auszuwählen. Durch das Drücken einer beliebigen Taste wird der Fortschritt gestoppt und das GRUB-Menü eingefroren.

3. Die Option **Passwort des Wartungsbenedutzers zurücksetzen** auswählen. Die Wartungskonsole öffnet sich.
4. In der Konsole das neue Passwort eingeben und bestätigen. Es stehen drei Versuche zur Verfügung. Das System startet nach erfolgreicher Eingabe des neuen Passworts neu.
5. Drücken Sie die **Eingabetaste**, um fortzufahren. Das System aktualisiert das Passwort auf der VM.



Beim Einschalten der virtuellen Maschine erscheint dasselbe GRUB-Menü. Die Option zum Zurücksetzen des Passworts sollte jedoch nur in Verbindung mit der Option **Restart Guest OS** verwendet werden.

Host-Cluster-Schutz verwalten

Ändern eines geschützten Hostclusters in ONTAP tools

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

- Neue Datenspeicher oder Hosts zum geschützten Cluster hinzufügen.
- Neue SnapMirror Beziehungen zu den Schutzeinstellungen hinzufügen.
- Bestehende SnapMirror Beziehungen aus den Schutzeinstellungen löschen.
- Eine bestehende SnapMirror Beziehung ändern.



Nach dem Erstellen, Bearbeiten oder Löschen des Schutzes für einen Hostcluster ist eine Speichererkennung erforderlich, damit die Änderungen übernommen werden. Wenn keine Speichererkennung durchgeführt wird, werden die Änderungen übernommen, nachdem die periodische Speichererkennung ausgelöst wurde.

Überwachung des Host-Cluster-Schutzes

Der Schutzstatus, die SnapMirror Beziehungen, die Datenspeicher und der SnapMirror Status für jeden geschützten Hostcluster werden überwacht.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Zu **NetApp ONTAP tools > Protection > Host cluster relationships** navigieren.

In der Spalte „Schutz“ wird ein Symbol angezeigt, das den Schutzstatus anzeigt.

3. Fahren Sie mit dem Mauszeiger über das Symbol, um weitere Details zu sehen.

Neue Datenspeicher oder Hosts hinzufügen

Hosts können hinzugefügt oder Datenspeicher auf dem geschützten Cluster mithilfe der vCenter Benutzeroberfläche erstellt werden.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Um die Eigenschaften eines geschützten Clusters zu bearbeiten, können Sie entweder
 - a. Zu **NetApp ONTAP tools > Protection > Host cluster relationships** navigieren, das Menü mit den drei Punkten neben dem Cluster auswählen und **Bearbeiten** oder
 - b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie **NetApp ONTAP tools > Protect Cluster**.
3. Wenn ein Datenspeicher in der vCenter Benutzeroberfläche erstellt wird, erscheint er als ungeschützt. Alle Datenspeicher im Cluster und deren Schutzstatus sind in einem Dialogfeld sichtbar. Mit der Schaltfläche **Schützen** lässt sich der Schutz aktivieren.



Nach dem Erstellen eines Datenspeichers in der vCenter Server-Benutzeroberfläche erscheint der Datenspeicher nach Auswahl von **Erkennen** auf der Übersichtsseite als Kandidat für den Schutz im Host-Cluster. Der Schutzstatus wird nach der nächsten periodischen Schutzerkennung auf „Geschützt“ aktualisiert.

4. Wenn ein neuer ESXi-Host hinzugefügt wird, wird der Schutzstatus als teilweise geschützt angezeigt. Im Menü unter den SnapMirror Einstellungen kann über die Auswahl von **Bearbeiten** die Nähe des neu hinzugefügten ESXi-Hosts festgelegt werden.



Für asynchrone Beziehungen wird die Bearbeitung in ONTAP tools nicht unterstützt, da die Ziel-SVM für einen Tertiär-Standort nicht zur gleichen Instanz hinzugefügt werden kann. Zur Änderung der Beziehungskonfiguration kann der System Manager oder die CLI auf der Ziel-SVM verwendet werden.

5. Nach dem Vornehmen von Änderungen **Speichern** auswählen.
6. Die Änderungen sind im Fenster **Cluster schützen** sichtbar.

ONTAP tools erstellt eine vCenter-Aufgabe, und der Fortschritt kann im Bereich **Letzte Aufgaben** verfolgt werden.

Eine neue SnapMirror Beziehung hinzufügen

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Um die Eigenschaften eines geschützten Clusters zu bearbeiten, können Sie entweder
 - a. Zu **NetApp ONTAP tools > Protection > Host cluster relationships** wechseln, das Auslassungszeichen-Menü beim Cluster auswählen und **Edit** auswählen oder
 - b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie **NetApp ONTAP tools > Protect Cluster**.
3. **Beziehung hinzufügen** auswählen.
4. Eine neue Beziehung kann entweder als **Asynchron** oder als **AutomatedFailOverDuplex** Richtlinientyp hinzugefügt werden.
5. **Schutz** auswählen.

Die Änderungen sind im Fenster **Cluster schützen** sichtbar.

ONTAP tools erstellt eine vCenter-Aufgabe, und der Fortschritt kann im Bereich **Letzte Aufgaben** verfolgt werden.

Eine bestehende SnapMirror Beziehung löschen

Zum Löschen einer asynchronen SnapMirror Beziehung muss die sekundäre SVM oder der Cluster als Storage-Backend in ONTAP tools for VMware vSphere hinzugefügt sein. Es ist nicht möglich, alle SnapMirror Beziehungen gleichzeitig zu löschen. Beim Löschen einer Beziehung wird die entsprechende Beziehung auch aus dem ONTAP Cluster entfernt. Beim Löschen einer Automated Failover Duplex SnapMirror Beziehung hebt das System die Zuordnung der Zieldatenspeicher auf und entfernt die Konsistenzgruppe, LUNs, Volumes und Initiatorgruppen aus dem Ziel-ONTAP Cluster.

Wenn die Beziehung gelöscht wird, 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 entweder
 - a. Zu **NetApp ONTAP tools > Protection > Host cluster relationships** wechseln, das Auslassungszeichen-Menü beim Cluster auswählen und **Edit** auswählen oder
 - b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie **NetApp ONTAP tools > Protect Cluster**.
3. Wählen Sie das Auslassungszeichen-Menü unter den SnapMirror Einstellungen aus und wählen Sie **Löschen**.
 - Wenn eine asynchron richtlinienbasierte SnapMirror Beziehung eines geschützten Hostclusters gelöscht wird, müssen die Speicherelemente manuell aus dem Tertiär-Storage-Cluster entfernt werden. Zu den Speicherelementen gehören Konsistenzgruppen, Volumes (für ONTAP Systeme), Speichereinheiten (LUNs/Namespaces) und Snapshots.
 - Wenn eine auf einer Automated Failover Duplex (AFD) Richtlinie basierende Beziehung eines geschützten Hostclusters gelöscht wird, besteht die Möglichkeit, die zugehörigen Speicherelemente auf dem sekundären Storage direkt über die Schnittstelle zu entfernen.
 - Wenn eine Automated Failover Duplex (AFD) Richtlinien-basierte Beziehung gelöscht wird und die Konsistenzgruppe für Backups auf Anwendungsebene nun hierarchisch ist, erscheint eine Warnung bezüglich der Auswirkungen auf das Backup. Eine Bestätigung ist erforderlich, um fortzufahren. Nach der Bestätigung werden die zugehörigen Speicherelemente auf dem sekundären Storage gelöscht. Werden sie nicht entfernt, verbleiben sie am sekundären Standort.

ONTAP tools erstellt eine vCenter-Aufgabe, und der Fortschritt kann im Bereich **Letzte Aufgaben** verfolgt werden.

Eine bestehende SnapMirror Beziehung ändern

Um eine SnapMirror asynchron Beziehung zu ändern, muss sichergestellt sein, dass die sekundäre SVM oder der Cluster als Storage-Backend in ONTAP tools for VMware vSphere hinzugefügt ist. Für Automated Failover Duplex SnapMirror Beziehungen kann die Host-Nähe für uniforme Konfigurationen oder der Host-Zugriff für nicht-uniforme Konfigurationen aktualisiert werden. Ein Wechsel zwischen asynchronen und Automated Failover Duplex Richtlinientypen wird nicht unterstützt. Proximitäts- oder Zugriffseinstellungen für neu entdeckte Hosts im Cluster können konfiguriert werden.



Eine bestehende SnapMirror asynchrone Beziehung kann nicht bearbeitet werden.

Schritte

1. Melden Sie sich beim vSphere Client an.
2. Um die Eigenschaften eines geschützten Clusters zu bearbeiten, können Sie entweder
 - a. Zu **NetApp ONTAP tools > Protection > Host cluster relationships** wechseln, das Auslassungszeichen-Menü beim Cluster auswählen und **Edit** auswählen oder
 - b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie **NetApp ONTAP tools > Protect Cluster**.
3. Wenn der AutomatedFailOverDuplex Richtlinientyp ausgewählt ist, sind Host-Nähe oder Host-Zugriffsdetails hinzuzufügen.
4. Die Schaltfläche **Schützen** auswählen.

ONTAP tools erstellen eine vCenter-Aufgabe. Der Fortschritt kann im Bereich **Letzte Aufgaben** verfolgt werden.

werden.

Hostclusterschutz in ONTAP tools entfernen

Wenn der Hostclusterschutz entfernt wird, sind die Datenspeicher ungeschützt.

Schritte

1. Die Liste der geschützten Hostcluster ist unter **NetApp ONTAP tools > Protection > Host cluster relationships** zu finden.

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

2. Im Fenster **Hostclusterschutz** das Menü mit den Auslassungspunkten neben dem Cluster auswählen und **Schutz entfernen** wählen.
 - Wenn der Schutz eines Hostclusters entfernt wird, bei dem nur eine SnapMirror asynchron Beziehung besteht, müssen die Speicherelemente manuell gelöscht werden. Zu den Speicherelementen gehören Konsistenzgruppen, Volumes (für ONTAP System), Speichereinheiten (LUNs) und Snapshots.
 - Wenn der Schutz von einem Hostcluster entfernt wird, das nur über eine automatisierte, duplexbasierte Failover SnapMirror-Richtlinienbeziehung und eine nicht-hierarchische Konsistenzgruppe verfügt, können die zugehörigen Speicherelemente auf dem sekundären Speicher direkt vom selben Bildschirm gelöscht werden.
 - Wenn der Schutz eines Hostclusters mit SnapMirror-Richtlinien und einer hierarchischen Konsistenzgruppe für Backups entfernt wird, erscheint eine Warnung zu den Auswirkungen auf die Backups. Eine Bestätigung ist erforderlich, um fortzufahren. Nach der Bestätigung werden die zugehörigen Speicherelemente auf dem sekundären Speicher gelöscht. Ohne Bereinigung verbleiben die Speicherelemente am sekundären Standort.

Wiederherstellung der ONTAP tools Konfiguration

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

Der Datenspeicher, in dem ONTAP tools for VMware vSphere virtuelle Maschinen bereitgestellt werden, speichert die Sicherungsdateien. Ein Ordner, der nach der ONTAP tools IP-Adresse benannt ist (Punkte werden durch Unterstriche ersetzt und mit *OTV_backup* als Suffix versehen), enthält die beiden aktuellsten Sicherungsdateien (*OTV_backup_1.tar.enc* und *OTV_backup_2.tar.enc*) sowie eine Info-Datei (*OTV_backup_info.txt*), die den Namen der letzten Sicherung enthält.

Es ist sicherzustellen, dass die neue virtuelle Maschine dieselbe ONTAP tools IP-Adresse verwendet und mit der ursprünglichen Systemkonfiguration übereinstimmt, einschließlich aktivierter Dienste, Knotengröße und HA-Modus.

Schritte

1. Die Sicherungsdateien sind vom Datenspeicher der ursprünglichen virtuellen Maschine auf das lokale System herunterzuladen.
 - a. Zum Speicherbereich wechseln und den Datenspeicher auswählen, der die Sicherungsdateien für die virtuelle Maschine enthält.
 - b. Den Abschnitt **Dateien** auswählen.

- c. Das benötigte Sicherungsverzeichnis herunterladen.
2. Die bestehende virtuelle Maschine wird ausgeschaltet. Anschließend wird eine neue virtuelle Maschine mit derselben OVA-Datei wie bei der ursprünglichen Bereitstellung bereitgestellt.
3. Öffnen Sie auf dem vCenter Server die Wartungskonsole.
4. Melden Sie sich als Wartungsbenutzer an.
5. Geben Sie 4 ein, um **Support und Diagnose** auszuwählen.
6. Geben Sie 2 ein, um die Option **Ferndiagnosezugriff aktivieren** auszuwählen und ein neues Passwort für den Diagnosezugriff zu erstellen.
7. Wählen Sie eine Sicherungsdatei aus dem heruntergeladenen Verzeichnis aus. In der Datei *OTV_backup_info.txt* lässt sich die neueste Sicherung identifizieren.
8. Verwenden Sie den folgenden Befehl, um die Sicherungsdatei auf die neue virtuelle Maschine zu übertragen. Wenn Sie dazu aufgefordert werden, ist das Diagnosekennwort einzugeben.

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



Der im Befehl angegebene Zielpfad und Dateiname (/home/diag/system_recovery.tar.enc) sollte nicht geändert werden.

9. Nachdem die Sicherungsdatei übertragen wurde, im Diagnose-Shell anmelden und den folgenden Befehl ausführen:

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

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

Nach Abschluss der Wiederherstellung stellt ONTAP tools die Dienste und vCenter-Objekte wieder her.

ONTAP tools deinstallieren

Die Deinstallation der ONTAP tools für VMware vSphere löscht alle Daten in den Tools.

Schritte

1. Alle virtuellen Maschinen aus den von ONTAP tools for VMware vSphere verwalteten Datenspeichern entfernen oder verschieben.
 - Informationen zum Entfernen der virtuellen Maschinen finden Sie unter ["VMs und VM-Vorlagen entfernen und erneut registrieren"](#)
 - Informationen zum Verschieben in einen nicht verwalteten Datenspeicher finden Sie unter ["Migration Ihrer virtuellen Maschine mit Storage vMotion"](#)
2. ["Datenspeicher löschen"](#) erstellt auf ONTAP tools for VMware vSphere.
3. Wenn Sie den VASA Provider aktiviert haben, in ONTAP tools **Einstellungen > VASA Provider settings > Unregister** auswählen, um die VASA Provider von allen vCenter Servern abzumelden.
4. Alle Storage-Backends von der vCenter Server-Instanz disassoziiieren. Siehe ["Speicher-Backends von der"](#)

[vCenter Server-Instanz trennen](#)".

5. Alle Storage-Backends löschen. Siehe ["Storage-Backends verwalten"](#).
6. Den SRA-Adapter aus VMware Live Site Recovery entfernen:
 - a. Melden Sie sich als admin an der VMware Live Site Recovery Appliance Managementoberfläche über Port 5480 an.
 - b. **Storage Replication Adapters** auswählen.
 - c. Die entsprechende SRA-Karte auswählen und im Dropdown-Menü **Löschen** auswählen.
 - d. Bestätigen Sie, dass Ihnen die Ergebnisse des Löschens des Adapters bekannt sind, und wählen Sie **Löschen** aus.
7. Löschen der vCenter Serverinstanzen, die in ONTAP tools for VMware vSphere integriert sind. Siehe ["vCenter Server-Instanzen verwalten"](#).
8. Die ONTAP tools for VMware vSphere VMs werden über den vCenter Server ausgeschaltet und die VMs gelöscht.

Was kommt als Nächstes?

["FlexVol Volumes entfernen"](#)

Entfernen Sie FlexVol-Volumes nach der Deinstallation von ONTAP tools

Wenn ein dedizierter ONTAP Cluster für die Bereitstellung von ONTAP tools for VMware verwendet wird, entstehen zahlreiche ungenutzte FlexVol volumes. Nach dem Entfernen von ONTAP tools for VMware vSphere sollten die FlexVol volumes entfernt werden, um mögliche Leistungseinbußen zu vermeiden.

Schritte

1. Der Bereitstellungstyp der ONTAP tools for VMware vSphere kann über die ONTAP tools Management-Node-VM ermittelt werden. Mit folgendem Befehl lässt sich der Bereitstellungstyp prüfen: `cat /opt/netapp/meta/ansible_vars.yaml | grep -i protocol`

Handelt es sich um eine iSCSI-Bereitstellung, sollten die igroups ebenfalls gelöscht werden.
2. Die Liste der FlexVol Volumes abrufen. `kubectl describe persistentvolumes | grep internalName | awk -F='{' '{print $2}'`
3. Entfernen Sie die VMs vom vCenter Server. Siehe ["VMs und VM-Vorlagen entfernen und erneut registrieren"](#).
4. Löschen Sie FlexVol Volumes. Siehe ["Ein FlexVol Volume löschen"](#). Der genaue FlexVol Volume-Name ist im CLI-Befehl zum Löschen eines Volumes einzugeben.
5. Löschen Sie die SAN-iGroups aus dem ONTAP-Speichersystem im Falle einer iSCSI-Bereitstellung. Siehe ["SAN-Initiatoren und Initiatorgruppen anzeigen und verwalten"](#).

Upgrade ONTAP tools für VMware vSphere

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

Ein Upgrade von ONTAP tools for VMware vSphere 10.3 oder 10.4 auf 10.5 ist möglich. Für ein Upgrade von ONTAP tools 10.0, 10.1 oder 10.2 auf 10.5 ist zunächst ein Upgrade auf 10.3 oder 10.4 erforderlich, bevor auf 10.5 gewechselt werden kann.



- Bei ASA r2-Systemen müssen Sie ONTAP tools for VMware vSphere auf Version 10.5 und ONTAP auf Version 9.16.1 aktualisieren, 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. Zur Wiederherstellung der Konfiguration kann eine Wiederherstellung mit niedrigem RPO oder per Snapshot erfolgen. Für ONTAP tools for VMware vSphere 10.2 und frühere Versionen kann eine Wiederherstellung mit Zero-RPO erfolgen.

Bevor Sie beginnen

- Alle Knoten müssen aktiv sein.
- Es ist sicherzustellen, dass das ONTAP Systemzertifikat und die eingebundenen vCenter Zertifikate mindestens 5 Tage gültig sind. Sollten die Zertifikate früher ablaufen, schlägt das Upgrade fehl.
- Stellen Sie sicher, dass auf allen Knoten eine fünfte Festplatte mit einer Kapazität von 100 GB vorhanden ist.
- Es sollte sichergestellt sein, dass die Knotenkonfiguration den Spezifikationen in der folgenden Tabelle entspricht.

Bereitstellungstyp	CPU (Kern) pro Knoten	Speicher (GB) pro Knoten	Speicherplatz (GB) pro Knoten	Gesamt-CPU (Core)	Arbeitsspeicher (GB)	Gesamtspeicherplatz (GB)
Nicht-HA Small	9	18	350	9	18	350
Nicht-HA Medium	13	26	350	13	26	350
HA Small	9	18	350	27	54	1050
HA Medium	13	26	350	39	78	1050
HA Large	17	34	350	51	102	1050

- Sichergestellt ist, dass Hot-Plug-in für CPU und RAM aktiviert ist.
- Eine Sicherung mit niedrigem RPO aktivieren und sicherstellen, dass eine Sicherung in der vCenter Client-Oberfläche sichtbar ist. Der Sicherungsordner sollte vor dem Upgrade heruntergeladen werden.
- Ein Backup mit niedrigem RPO wird empfohlen. In einer Bereitstellung ohne Hochverfügbarkeit (HA) kann vor dem Upgrade ein konsistenter Snapshot der virtuellen Maschine der ONTAP tools erstellt werden.

Weitere Informationen zu Backup und Recovery finden Sie unter ["Backup-Einstellungen bearbeiten"](#) und ["Wiederherstellung der ONTAP tools Konfiguration"](#).

Schritte

1. ONTAP tools für VMware vSphere Upgrade-ISO in die Inhaltsbibliothek hochladen.
2. Auf der primären VM-Seite **Aktionen > Einstellungen bearbeiten** auswählen. Zur Identifizierung des Namens der primären VM:
 - a. Die Diagnose-Shell auf einem beliebigen Knoten aktivieren
 - b. Führen Sie folgenden Befehl aus:

```
grep sourceHost /opt/netapp/meta/ansible_vars.yaml
```
3. Im Bearbeitungsfenster unter dem Feld **CD/DVD-Laufwerk** die **content library ISO-Datei** auswählen.
4. Die ISO-Datei auswählen, das Kontrollkästchen **Verbunden** für das Feld **CD/DVD-Laufwerk** aktivieren und auf **OK** klicken.
5. Vom vCenter Server aus eine Konsole zu ONTAP tools öffnen.
6. Melden Sie sich als Wartungsbenutzer an.
7. Geben Sie **2** ein, um das Menü **System Configuration** auszuwählen.
8. **6** eingeben, um die Option **Upgrade** auszuwählen.
9. Geben Sie die vCenter-Anmeldeinformationen ein, wenn Sie dazu aufgefordert werden. Dies ist die vCenter-Instanz, auf der die ONTAP tools gehostet werden.

Wenn Sie ONTAP tools in einer Zwei-vCenter-Server-Topologie verwenden – wobei die Appliance auf 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 die für die OVF-Vorlagenbereitstellung erforderlichen Berechtigungen besitzt. Weitere Informationen finden Sie in der Liste der Rollen "[Mit ONTAP tools for VMware vSphere 10 enthaltene Rollen](#)".

Für die vCenter Instanz, die von ONTAP tools verwaltet wird, muss das vCenter Benutzerkonto über Administratorrechte verfügen.

Während des Upgrades erhalten Sie eine Benachrichtigung, falls bei integrierten Storage-Backend-Zertifikaten Einträge für Subject Alternative Name (SAN) fehlen. Wenn Sie sich entscheiden, ohne Validierung des SAN fortzufahren, wird das Upgrade fortgesetzt, was jedoch aufgrund potenzieller Sicherheitsrisiken nicht empfohlen wird.

10. Beim Upgrade werden die folgenden Aktionen automatisch ausgeführt:
 - a. Das Gateway-Zertifikat wird mit einer Gültigkeitsdauer von einem Jahr erneuert. Beim Entfernen des vorherigen SRA-Adapters und Hochladen des neuen 10.5-Adapters ändert sich die Gültigkeitsdauer des SRA-Zertifikats von 10 Jahren auf 1 Jahr.
 - b. Das Remote Plug-in ist aktualisiert.
 - c. ONTAP und vCenter Server-Zertifikate werden validiert und zu ONTAP tools hinzugefügt
 - d. Backup ist aktiviert.

Was kommt als Nächstes

Nach dem Upgrade auf ONTAP tools für VMware vSphere 10.5:

- Systemwarnungen werden überwacht und es empfiehlt sich, die Erneuerung des Gateway-Zertifikats vor Ablauf der einjährigen Gültigkeitsdauer einzuplanen.
- Den ONTAP tools 10.4 oder 10.3 SRA Adapter entfernen und die 10.5 SRA Adapter tar-Datei hochladen.

- Nach dem Hochladen des SRA-Adapter-Tar-Archivs wird der Installationsbefehl ausgeführt. Anschließend erfolgt ein erneuter Scan der SRA-Adapter, wodurch die Seite „VMware Site Recovery Storage Replication Adapters“ aktualisiert wird.

Nach dem Upgrade können Sie:

- Die Dienste können über die Manager-Benutzeroberfläche deaktiviert werden.
- Wechsel von einer Non-HA-Konfiguration zu einer HA-Konfiguration
- Eine nicht-HA-Kleinkonfiguration kann auf eine nicht-HA-Mittlere oder auf eine HA-Mittlere oder HA-Großkonfiguration skaliert werden.

Verwandte Informationen

["Migration von ONTAP tools für VMware vSphere 9.xx auf 10.5"](#)

ONTAP tools-Upgrade-Fehlercodes

Während des Upgrades der ONTAP tools for VMware vSphere können Fehlercodes auftreten. Die Fehlercodes sind fünfstellig, wobei die ersten beiden Ziffern das Skript kennzeichnen, bei dem das Problem aufgetreten ist, und die letzten drei Ziffern den spezifischen Workflow innerhalb dieses Skripts darstellen.

Alle Fehlerprotokolle werden in der Datei `ansible-perl-errors.log` gespeichert, um die Nachverfolgung und Behebung von Problemen zu vereinfachen. 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, falls der Fehler weiterhin besteht oder keine Lösung genannt wird.

Die folgende Tabelle listet die Fehlercodes und die zugehörigen Dateinamen auf.

Fehlercode	Skriptname
00	firstboot-network-config.pl, Modus Deploy
01	firstboot-network-config.pl, Modus Upgrade
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, reboot
06	firstboot-deploy-otv-ng.pl, Upgrade, HA
07	firstboot-deploy-otv-ng.pl, Upgrade, non-HA
08	firstboot-otv-recovery.pl
09	post-deploy-upgrade.pl

Die letzten drei Ziffern des Fehlercodes geben den spezifischen Workflow-Fehler innerhalb des Skripts an:

Upgrade Fehlercode	Arbeitsablauf	Auflösung
052	Die ISO könnte mit der aktuellen Version identisch sein oder zwei Versionen über der aktuellen Version liegen.	Eine mit Ihrer aktuellen Version kompatible ISO-Version ermöglicht ein Upgrade.
068	Das Rollback der Debian Pakete ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
069	Fehler beim Wiederherstellen der Dateien	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
070	Fehler beim Löschen der Sicherung	-
071	Kubernetes Cluster war nicht fehlerfrei.	-
074	ISO-Einbindung ist fehlgeschlagen	Die Datei /var/log/upgrade-run.log prüfen und das Upgrade erneut versuchen.
075	Die Vorabprüfungen für das Upgrade sind fehlgeschlagen	Das Upgrade kann erneut versucht werden.
076	Das Registry Upgrade ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
077	Die Registry-Wiederherstellung ist fehlgeschlagen	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
078	Das Upgrade des Operators ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
079	Das Zurücksetzen des Operators ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
080	Das Upgrade der Services ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
081	Das Zurücksetzen der Dienste ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.

Upgrade Fehlercode	Arbeitsablauf	Auflösung
082	Das Löschen alter Images aus dem Container ist fehlgeschlagen.	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
083	Das Löschen der Sicherung ist fehlgeschlagen	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
084	Die Rückumstellung von JobManager auf Produktion ist fehlgeschlagen	Führen Sie die folgenden Schritte aus, um das Upgrade wiederherzustellen/abzuschließen. 1. Diagnose-Shell aktivieren 2. Den Befehl ausführen: <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> 3. Überprüfen Sie die Protokolle unter <i>/var/log/post-deploy-upgrade.log</i>
087	Die Schritte nach dem Upgrade sind fehlgeschlagen.	Führen Sie die folgenden Schritte aus, um das Upgrade wiederherzustellen/abzuschließen. 1. Diagnose-Shell aktivieren 2. Den Befehl <i>sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade</i> ausführen 3. Überprüfen Sie die Protokolle unter <i>/var/log/post-deploy-upgrade.log</i>
088	Die Konfiguration der Protokollrotation für journald ist fehlgeschlagen.	Prüfen Sie, ob die Netzwerkeinstellungen der VM 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	Die Änderung der Besitzverhältnisse der Konfigurationsdatei für die Rotation des Zusammenfassungsprotokolls ist fehlgeschlagen.	Das Upgrade kann erneut versucht werden.
095	Betriebssystem-Upgrade fehlgeschlagen	Keine Wiederherstellung für OS-Upgrade. ONTAP tools Dienste werden aktualisiert und neue Pods werden ausgeführt.
096	Dynamischen Speicherbereitsteller installieren	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.

Upgrade Fehlercode	Arbeitsablauf	Auflösung
097	Die Deinstallation der Dienste für das Upgrade ist fehlgeschlagen	Zero RPO oder snapshotbasierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
098	Das Kopieren des dockercréd-Secrets vom ntv-system in den Namespace des dynamischen Storage Provisioners ist fehlgeschlagen.	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.
099	Die Validierung der neuen HDD-Erweiterung ist fehlgeschlagen.	Die neue Festplatte wird im Fall einer HA-Bereitstellung allen Knoten und im Fall einer Nicht-HA-Bereitstellung nur einem Knoten hinzugefügt.
109	Die Sicherung der persistenten Volume-Daten ist fehlgeschlagen.	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.
110	Die Wiederherstellung der persistenten Volumendaten ist fehlgeschlagen	Zero-RPO oder Snapshot-basierte Wiederherstellung und erneuter Upgrade-Versuch können genutzt werden.
111	Die Aktualisierung der etcd Zeitüberschreitung Parameter für RKE2 ist fehlgeschlagen.	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.
112	Die Deinstallation des dynamischen Speicherbereitstellungsdienstes ist fehlgeschlagen.	-
113	Die Aktualisierung der Ressourcen auf den sekundären Knoten ist fehlgeschlagen	Die Upgrade-Protokolle prüfen und das Upgrade erneut versuchen.
104	Der Neustart des sekundären Knotens ist fehlgeschlagen	Starten Sie die Knoten manuell neu, einen nach dem anderen.
100	Kernel-Rollback ist fehlgeschlagen	-
051	Das Upgrade des dynamischen Speicherbereitstellungsdienstes ist fehlgeschlagen.	Upgrade-Protokolle prüfen und Upgrade erneut versuchen.
056	Das Löschen der Migrationssicherung ist fehlgeschlagen	NA
090	Zertifikatsvalidierung für Storage Backends und vCenter fehlgeschlagen	Upgrade-Protokolle und die Protokolldatei unter /var/log/cert_validation_error.log können geprüft und das Upgrade erneut versucht werden.

Upgrade Fehlercode	Arbeitsablauf	Auflösung
114	Interne Zertifikatsaktualisierung in der MongoDB-Collection fehlgeschlagen	Falls das Upgrade mit dem Fehlercode 114 fehlschlägt, führen Sie die folgenden Schritte aus: 1. Stellen Sie eine Verbindung zum Upgrade-ISO auf dem primären Knoten her und aktivieren Sie die Diagnose-Shell. 2. Mounten Sie die ISO-Datei über die SSH-Sitzung auf dem primären Knoten: <pre> sudo mount /dev/cdrom sudo mount -o loop,ro /dev/cdrom/APPLIANCE_UPGRADE.bin /upgrade </pre> 3. Debian-Pakete installieren: <pre> sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vplatform.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vpupgrader.deb sudo dpkg -iE /upgrade/dists/squeeze/main/binary-amd64/vmware-tools.deb </pre> 4. Kopieren Sie die Build-Informationsdatei: <pre> sudo cp /upgrade/APPLIANCE_BUILD / </pre>
138		Fügen Sie der Sammlung Zertifikate hinzu, indem Sie die



Ab ONTAP tools for VMware vSphere 10.3 wird Zero RPO nicht ⁵ unterstützt.

Erfahren Sie mehr über ["Wie ONTAP tools for VMware vSphere nach einem fehlgeschlagenen Upgrade von Version 10.0 auf 10.1 wiederhergestellt werden können"](#)

Diagnose-Shell aktivieren und folgenden Befehl ausführen:

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

Überprüfen Sie die Protokolle unter

/var/log/otvng/post-deploy-upgrade.log.

6. Starten Sie die Knoten neu:

```
sudo bash
/home/maint/scripts
/vault_decrypt.sh
cd
/home/maint/rke2-pb
sudo ansible-
playbook site.yaml
--tags
restart_nodes
--skip-tags
debian_upgrade,kern
el_upgrade,rescan_s
csi_bus,source_iso,
eject_upgrade,mount
Iso,upgradeNodes,re
gistryUpg,deleteOld
Images,wait,checkRe
achability,delete_o
tv_cr,uninstall_tri
dent,del_trident_im
ages,refresh_resour
ces,ntp_configure,n
tpd_uninstall
```

7. Führen Sie die Schritte nach dem Upgrade durch:

Migration von ONTAP tools für VMware vSphere 9.xx auf 10.5

Migration von ONTAP tools für VMware vSphere 9.xx auf 10.5

Die Umstellung der NetApp ONTAP tools for VMware vSphere Setups von Version 9.xx auf 10.5 erfordert einen Migrationsprozess aufgrund der signifikanten Produktaktualisierungen und -verbesserungen zwischen den Versionen.

Eine Migration von ONTAP tools for VMware vSphere 9.12D1, 9.13D2 und 9.13P2 auf ONTAP tools for VMware vSphere 10.5 ist möglich.

Wenn Sie NFS- und VMFS-Datenspeicher haben und keine vVols-Datenspeicher in Ihrer Konfiguration vorhanden sind, deinstallieren Sie einfach ONTAP tools 9.xx und implementieren Sie ONTAP tools 10.5. Wenn Ihre Konfiguration jedoch vVols-Datenspeicher enthält, müssen Sie einen Prozess zur Migration des VASA Provider und der SRA durchlaufen.

Die folgende Tabelle beschreibt den Migrationsprozess in diesen beiden unterschiedlichen Szenarien.

Falls die Konfiguration vVols Datenspeicher enthält	Wenn die Konfiguration nur NFS und VMFS Datenspeicher enthält
Schritte: 1. "Den VASA Provider migrieren" 2. "VM-Speicherrichtlinien erstellen"	Schritte: 1. ONTAP tools 9.xx aus Ihrer Umgebung entfernen. Siehe "Entfernen von OTV 9.xx aus Ihrer Umgebung" NetApp Knowledge Base Artikel. 2. "ONTAP tools für VMware vSphere 10.5 bereitstellen und konfigurieren" 3. "SRA aktualisieren" 4. "VM-Speicherrichtlinien erstellen"



Nach der Migration von ONTAP tools for VMware vSphere 9.xx auf 10.5 werden vVols Datenspeicher, die das NVMe/FC-Protokoll verwenden, nicht mehr funktionsfähig, 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

In diesem Abschnitt werden die Schritte beschrieben, 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 Provider

1. Um Derby PORT 1527 auf den vorhandenen ONTAP tools for VMware vSphere zu aktivieren, muss der Root-Benutzer aktiviert und über SSH an der CLI angemeldet werden. Anschließend ist folgender Befehl auszuführen:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. OVA für ONTAP tools für VMware vSphere 10.5 bereitstellen.
3. Fügen Sie die vCenter Server-Instanz hinzu, die auf ONTAP tools for VMware vSphere 10.5 migriert werden soll. Weitere Informationen sind unter ["Eine vCenter Server-Instanz hinzufügen"](#) verfügbar.
4. ["VASA Provider aktivieren"](#) Service auf ONTAP tools for VMware vSphere 10.5.
5. Das Storage-Backend wird lokal über die vCenter Server-APIs für das ONTAP tools Plug-in eingebunden. Weitere Informationen sind unter ["Ein Storage-Backend über die vSphere Client-Oberfläche hinzufügen"](#) verfügbar.
6. Ein Zugriffstoken zur Authentifizierung von REST-API-Anfragen wird benötigt. Im folgenden Beispiel sind die Variablen durch die für Ihre Umgebung spezifischen Werte zu ersetzen.

```
sudo perl
/home/maint/scripts
/postdeploy
postupgrade
```

8. Überprüfen Sie den erfolgreichen Abschluss, indem Sie die Protokolle einsehen:

```
curl --request POST \
  --location "https://$FQDN_IP_PORT/virtualization/api/v1/auth/vcenter-
login" \
  --header "Content-Type: application/json" \
  --header "Accept: */*" \
  -d '{"username": "$MYUSER", "password": "$MYPASSWORD", "vcenter
hostname": "$MYVCENTER"}'
```

9. ISO auswerfen:

Das in der Antwort zurückgegebene Zugriffstoken kopieren und speichern.

7. Führen Sie die folgende API von Swagger oder Postman aus, um die Migration durchzuführen.

```
curl -X POST
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migra
tion-jobs`
```

Sie können Swagger über diese URL aufrufen: [https://\\$FQDN_IP_PORT/](https://$FQDN_IP_PORT/), zum Beispiel: <https://10.67.25.33:8443/>.

10. Starten Sie den primären Knoten neu:

```
sudo reboot -f
```

HTTP-Methode und Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/api/v1

Verarbeitungsart

asynchron

Curl-Beispiel

```
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": "*****"
}'
```

Anfragetext für andere Release-Migration:

```
{
  "otv_ip": "xx.xx.xx.xx",
  "vasa_provider_credentials": {
    "username": "xxxxx",
    "password": "*****"
  }
}
```

Beispiel für eine JSON-Ausgabe

Das System gibt ein Jobobjekt zurück. Die Job-ID wird gespeichert, um sie im nächsten Schritt zu verwenden.

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```

8. Die folgende URI in Swagger gibt den Status aus:

```
curl
`https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobId
>?includeSubJobsAndTasks=true`
```

Verwenden Sie den im vorherigen Schritt vom Migrationsauftrag zurückgegebenen Wert 'id'. Überprüfen Sie nach Abschluss des Auftrags den Migrationsbericht in der Auftragsantwort.

9. Den VASA Provider bei ONTAP tools for VMware vSphere registrieren. Anweisungen finden sich unter ["VASA Provider registrieren"](#).
10. Überprüfen Sie die VASA Provider-Registrierung:
 - a. Im vSphere Client navigieren Sie zum vCenter Server.
 - b. Wählen Sie **Configure > Storage Providers**.
 - c. Bestätigen Sie, dass der im vorherigen Schritt registrierte VASA Provider online erscheint.
11. ONTAP tools for VMware vSphere Storage Provider 9.10/9.11/9.12/9.13 VASA Provider-Dienst kann mit diesen Schritten gestoppt werden:
 - a. In ONTAP tools 9.x die Webkonsole öffnen.
 - b. Auf die Wartungskonsole zugreifen.
 - c. Geben Sie 1 ein, um das Menü **Application Configuration** auszuwählen.
 - d. Geben Sie 5 ein, um die VASA Provider und SRA Dienste zu beenden.
 - e. Im vSphere Client navigieren Sie zum vCenter Server und wählen Sie **Konfigurieren > Speicheranbieter**.
 - f. Wählen Sie den Offline VASA Provider für ONTAP tools 9.x aus und wählen Sie **Entfernen**.

Nachdem der alte VASA Provider gestoppt wurde, wechselt der vCenter Server auf ONTAP tools for VMware vSphere. Alle Datenspeicher und VMs sind zugänglich und werden von ONTAP tools for VMware vSphere bereitgestellt.
12. Migrierte NFS und VMFS Datenspeicher erscheinen in ONTAP tools for VMware vSphere 10.5 nach dem Datenspeicher-Erkennungsauftrag, was bis zu 30 Minuten dauern kann. Die Sichtbarkeit dieser Datenspeicher ist auf der Übersichtsseite ersichtlich.
13. Die Patch-Migration erfolgt mithilfe der folgenden API in Swagger oder in Postman:

HTTP-Methode und Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
PATCH	/api/v1

Verarbeitungsart

asynchron

Die folgende URI wird in Swagger verwendet:

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

HTTP-Methode und Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
PATCH	/api/v1

Verarbeitungsart

asynchron

Die folgende URI wird in Swagger verwendet:

```
curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/<vcenter_id>/migration-jobs/<migration_id>`
```

Curl-Beispiel

```
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`
```

Beispiel für eine JSON-Ausgabe

```
{
  "id": 123,
  "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35",
  "status": "running"
}
```



Verwenden Sie den in Schritt 7 zurückgegebenen Wert 'migration_id' als <migration_id> im PATCH-API-Aufruf. Der Anfragetext ist für die Patch-Operation leer.



UUID ist die Migrations-UUID, die als Antwort auf die post-migrate API zurückgegeben wird.

Nach Ausführung der Patch-Migrations-API entsprechen alle VMs der Speicherrichtlinie.

Was kommt als Nächstes

Nach Abschluss der Migration und Registrierung von ONTAP tools 10.5 beim vCenter Server sind die folgenden Schritte zu beachten:

- Warten, bis die **Erkennung** abgeschlossen ist, und das System aktualisiert die Zertifikate automatisch auf allen Hosts.
- Vor dem Start von Datenspeicher- und virtuellen Maschinen-Operationen ist zu warten. Die Wartezeit hängt von der Anzahl der Hosts, Datenspeicher und virtuellen Maschinen ab. Ohne diese Wartezeit können gelegentlich Fehler auftreten.

Nach dem Upgrade, falls der Konformitätsstatus der virtuellen Maschine veraltet ist, kann die Speicherrichtlinie mit den folgenden Schritten erneut angewendet werden:

1. Gehen Sie zum Datenspeicher und wählen Sie **Zusammenfassung > VM Storage policies**.
2. Das System zeigt den Compliance-Status unter **VM storage policy compliance** als **Out-of-date** an.
3. Die Storage-VM-Richtlinie und die entsprechende VM auswählen.
4. **Anwenden** auswählen.
5. Der Compliance-Status unter **VM-Speicherrichtlinienkonformität** wird als konform angezeigt.

Verwandte Informationen

- ["Informationen zu ONTAP tools für VMware vSphere 10 RBAC"](#)
- ["Upgrade von ONTAP tools für VMware vSphere 10.x auf 10.5"](#)

Schritte zum Aktualisieren des Speicherreplikationsadapters (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 Benutzeroberfläche der VMware Live Site Recovery Appliance zeigt den Status des Wiederherstellungsplans mit Details zum geschützten und zum Wiederherstellungsstandort an. Im Wiederherstellungsplan sind die Schaltflächen CLEANUP und REPROTECT deaktiviert, während die Schaltflächen TEST und RUN weiterhin aktiviert bleiben. Dies zeigt an, dass der Standort für die Datenwiederherstellung vorbereitet ist. Vor der Migration der SRA sollte überprüft werden, dass sich ein Standort im geschützten Status und der andere im

Wiederherstellungsstatus befindet.



Beginnen Sie die Migration nicht, wenn das Failover abgeschlossen ist, die Re-Protect-Funktion aber noch aussteht. Stellen Sie sicher, dass der Re-Protect-Vorgang abgeschlossen ist, bevor Sie mit der Migration fortfahren. Wenn ein Test-Failover läuft, bereinigen Sie das Test-Failover und starten Sie die Migration.

1. Die folgenden Schritte sind erforderlich, um den ONTAP tools SRA Adapter für VMware vSphere 9.xx in VMware Site Recovery zu löschen:
2. Wechseln Sie zur Konfigurationsverwaltungsseite von VMware Live Site Recovery.
 - a. Zum Abschnitt **Storage Replication Adapter** wechseln.
 - b. Im Menü mit den Auslassungspunkten die Option **Konfiguration zurücksetzen** auswählen.
 - c. Im Menü mit den Auslassungspunkten die Option **Löschen** auswählen.
3. Diese Schritte sind sowohl an der Schutz- als auch an der Wiederherstellungsseite durchzuführen.
 - a. ["ONTAP tools für VMware vSphere Dienste aktivieren"](#)
 - b. ONTAP tools für VMware vSphere 10.5 SRA Adapter werden mithilfe der Schritte in ["SRA auf der VMware Live Site Recovery Appliance konfigurieren"](#) konfiguriert.
 - c. In der VMware Live Site Recovery Oberfläche **Arrays ermitteln** und **Geräte ermitteln** ausführen. Bestätigen, dass die Geräte wie vor der Migration angezeigt werden.

Automatisierung mithilfe 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 Lebenszyklusmanagement virtueller Maschinen. Enthalten ist eine leistungsstarke REST-API, die als Teil von Automatisierungsprozessen genutzt werden kann.

Grundlagen der REST-Webdienste

Representational State Transfer (REST) ist ein Stil zur Erstellung verteilter Webanwendungen, einschließlich des Designs von Web-Service-APIs. Es definiert eine Reihe von Technologien zur Bereitstellung serverbasierter Ressourcen und zur Verwaltung ihrer Zustände.

Ressourcen und Statusdarstellung

Ressourcen sind die grundlegenden Komponenten einer REST-Webservices-Anwendung. Beim Entwurf einer REST-API gibt es zwei wichtige erste Aufgaben:

- System- oder serverbasierte Ressourcen identifizieren
- Definieren der Ressourcenzustände und der zugehörigen Zustandsübergangsoperationen

Clientanwendungen können die Ressourcenzustände über klar definierte Nachrichtenflüsse anzeigen und ändern.

HTTP-Nachrichten

HTTP (Hypertext Transfer Protocol) ist das Protokoll, das von Webdienst-Client und -Server zum Austausch von Nachrichten über die Ressourcen verwendet wird. Es folgt dem CRUD-Modell basierend auf den generischen Operationen Erstellen, Lesen, Aktualisieren und Löschen. Das HTTP-Protokoll umfasst Anfrage- und Antwortheader sowie Antwortstatuscodes.

JSON-Datenformatierung

Obwohl verschiedene Nachrichtenformate zur Verfügung stehen, ist die JavaScript Object Notation (JSON) die gängigste Option. JSON ist ein Industriestandard zur Darstellung einfacher Datenstrukturen in Klartext und wird verwendet, um Zustandsinformationen zu übertragen, die die Ressourcen und gewünschten Aktionen beschreiben.

Sicherheit

Sicherheit ist ein wichtiger Aspekt einer REST API. Zusätzlich zu dem Transport Layer Security (TLS) Protokoll, das den HTTP-Datenverkehr im Netzwerk schützt, verwenden die ONTAP tools for VMware vSphere 10 REST API außerdem Zugriffstoken zur Authentifizierung. Für nachfolgende API-Aufrufe ist ein Zugriffstoken erforderlich.

Unterstützung für asynchrone Anfragen

Die ONTAP tools for VMware vSphere 10 REST API führt die meisten Anfragen synchron aus und gibt einen Statuscode zurück, wenn der Vorgang abgeschlossen ist. Es wird außerdem asynchrone Verarbeitung für Aufgaben unterstützt, die mehr Zeit zur Ausführung benötigen.

ONTAP tools Manager Umgebung

Es gibt mehrere Aspekte der ONTAP tools Manager Umgebung, die berücksichtigt werden sollten.

Virtuelle Maschine

ONTAP tools for VMware vSphere 10 wird mithilfe der vSphere Remote Plug-in-Architektur bereitgestellt. Die Software, einschließlich Unterstützung für die REST API, läuft in einer separaten virtuellen Maschine.

ONTAP tools IP-Adresse

ONTAP tools for VMware vSphere 10 stellt eine einzelne IP-Adresse bereit, die als Gateway zu den Funktionen der virtuellen Maschine dient. Die Adresse ist während der Erstkonfiguration anzugeben und wird einer internen Load-Balancer-Komponente zugewiesen. Die Adresse wird sowohl von der ONTAP tools Manager-Benutzeroberfläche als auch für den direkten Zugriff auf die Swagger-Dokumentationsseite und die REST API verwendet.

Zwei REST APIs

Zusätzlich zur ONTAP tools for VMware vSphere 10 REST API verfügt der ONTAP Cluster über eine eigene REST API. ONTAP tools Manager verwendet die ONTAP REST API als Client, um speicherbezogene Aufgaben auszuführen. Es ist wichtig zu beachten, dass diese beiden APIs getrennt und unterschiedlich sind. Weitere Informationen finden sich unter ["ONTAP Automatisierung"](#).

Details zur Implementierung der ONTAP tools REST API

REST etabliert zwar einen gemeinsamen Satz an Technologien und Best Practices, die genaue Implementierung jeder API kann jedoch je nach Designentscheidungen variieren. Es empfiehlt sich, sich mit dem Design der ONTAP tools for VMware vSphere 10 REST API vertraut zu machen, bevor diese verwendet wird.

Die REST-API umfasst verschiedene Ressourcenkategorien wie vCenters und Aggregate. Weitere Informationen enthält die ["API-Referenz"](#).

Zugriff auf die REST API

Auf die ONTAP tools for VMware vSphere 10 REST API kann über die IP-Adresse der ONTAP tools zusammen mit dem Port zugegriffen werden. Die vollständige URL besteht aus mehreren Teilen, darunter:

- ONTAP tools IP-Adresse und Port
- API Version
- Ressourcenkategorie
- Spezifische Ressource

Die IP-Adresse muss während der Ersteinrichtung konfiguriert werden, während der Port fest auf 8443 bleibt. Der erste Teil der URL ist für jede ONTAP tools for VMware vSphere 10 Instanz gleich; nur die Ressourcenkategorie und die spezifische Ressource unterscheiden sich zwischen den Endpunkten.



Die in den folgenden Beispielen angegebenen IP-Adressen und Portwerte dienen lediglich der Veranschaulichung. Diese Werte sind für Ihre Umgebung anzupassen.

Beispiel für den Zugriff auf Authentifizierungsdienste

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Diese URL kann verwendet werden, um mit der POST-Methode ein Zugriffstoken anzufordern.

Beispiel zum Auflisten der vCenter Server

`https://10.61.25.34:8443/virtualization/api/v1/vcenters`

Diese URL kann verwendet werden, um mit der GET-Methode eine Liste der definierten vCenter Serverinstanzen anzufordern.

HTTP-Details

Die ONTAP tools for VMware vSphere 10 REST API verwendet HTTP (Hypertext Transfer Protocol) und zugehörige Parameter, um auf die Ressourceninstanzen und Sammlungen zuzugreifen. Details der HTTP (Hypertext Transfer Protocol)-Implementierung sind nachfolgend dargestellt.

HTTP-Methoden

Die von der REST API unterstützten HTTP-Methoden bzw. Verben sind in der folgenden Tabelle aufgeführt.

Verfahren	CRUD	Beschreibung
GET	Lesen	Ruft Objekteigenschaften einer Ressourceninstanz oder -sammlung ab. Bei Verwendung mit einer Sammlung handelt es sich um eine Listenoperation.
POST	Erstellen	Erstellt eine neue Ressourceninstanz basierend auf den Eingabeparametern.
PUT	Aktualisieren	Aktualisiert eine gesamte Ressourceninstanz mit dem bereitgestellten JSON-Anfragetext. Schlüsselwerte, die nicht vom Benutzer geändert werden können, bleiben erhalten.
PATCH	Aktualisieren	Fordert die Anwendung einer Reihe ausgewählter Änderungen in der Anfrage auf die Ressourceninstanz an.
LÖSCHEN	Löschen	Löscht eine bestehende Ressourceninstanz.

Anfrage- und Antwortheader

Die folgende Tabelle fasst die wichtigsten HTTP-Header zusammen, die mit der REST API verwendet werden.

Kopfzeile	Typ	Nutzungshinweise
Akzeptieren	Anfrage	Dies ist der Inhaltstyp, den die Clientanwendung akzeptieren kann. Gültige Werte sind <code>*/*</code> oder <code>application/json</code> .
x-auth	Anfrage	Enthält ein Zugriffstoken, das den Benutzer identifiziert, der die Anfrage über die Client-Anwendung ausstellt.
Content-Type	Antwort	Wird vom Server basierend auf dem <code>Accept request</code> header zurückgegeben.

HTTP-Statuscodes

Die von der REST API verwendeten HTTP-Statuscodes sind nachfolgend beschrieben.

Code	Bedeutung	Beschreibung
200	OK	Zeigt Erfolg für Aufrufe an, die keine neue Ressourceninstanz erstellen.

Code	Bedeutung	Beschreibung
201	Erstellt	Ein Objekt wurde erfolgreich mit einer eindeutigen Kennung für die Ressourceninstanz erstellt.
202	Akzeptiert	Die Anfrage wurde angenommen und ein Hintergrundjob zur Ausführung der Anfrage erstellt.
204	Kein Inhalt	Die Anfrage war erfolgreich, obwohl kein Inhalt zurückgegeben wurde.
400	Ungültige Anforderung	Die Eingabe der Anfrage wird nicht erkannt oder ist ungeeignet.
401	Nicht autorisiert	Der Benutzer ist nicht autorisiert und muss sich authentifizieren.
403	Verboten	Der Zugriff wurde aufgrund eines Autorisierungsfehlers verweigert.
404	Nicht gefunden	Die in der Anfrage referenzierte Ressource existiert nicht.
409	Konflikt	Der Versuch, ein Objekt zu erstellen, ist fehlgeschlagen, da das Objekt bereits existiert.
500	Interner Fehler	Auf dem Server ist ein allgemeiner interner Fehler aufgetreten.

Authentifizierung

Die Authentifizierung eines Clients an der REST API erfolgt mittels eines Zugriffstokens. Zu den relevanten Merkmalen des Tokens und des Authentifizierungsprozesses gehören:

- Der Client muss ein Token mit den Administratoranmeldeinformationen (Benutzername und Passwort) des ONTAP tools Manager anfordern.
- Tokens sind im JSON Web Token (JWT)-Format formatiert.
- Jeder Token läuft nach 60 Minuten ab.
- API-Anfragen von einem Client müssen das Token im `x-auth` Anfrageheader enthalten.

Ein Beispiel für die Anforderung und Verwendung eines Zugriffstokens findet sich unter ["Ihr erster REST-API-Aufruf"](#).

Synchrone und asynchrone Anfragen

Die meisten REST API-Aufrufe werden schnell abgeschlossen und daher synchron ausgeführt. Das heißt, sie geben nach Abschluss der Anfrage einen Statuscode (wie 200) zurück. Anfragen, die länger dauern, werden asynchron mithilfe eines Hintergrundjobs ausgeführt.

Nach einem asynchron ausgeführten API-Aufruf gibt der Server den HTTP-Statuscode 202 zurück. Dies zeigt an, dass die Anfrage angenommen, aber noch nicht abgeschlossen wurde. Der Status des Hintergrundjobs kann abgefragt werden, um Erfolg oder Fehler zu ermitteln.

Die asynchrone Verarbeitung wird für verschiedene Arten von langlaufenden Operationen verwendet, darunter Datenspeicher- und vVol-Operationen. Weitere Informationen bietet die Kategorie „Jobmanager“ der REST API auf der Swagger-Seite.

Führen Sie Ihren ersten ONTAP tools REST API-Aufruf durch

Ein API-Aufruf mit curl ermöglicht den Einstieg in die ONTAP tools for VMware vSphere 10 REST API.

Bevor Sie beginnen

Die erforderlichen Informationen und Parameter, die in den curl-Beispielen benötigt werden, sollten überprüft werden.

Erforderliche Informationen

Sie benötigen Folgendes:

- ONTAP tools for VMware vSphere 10 IP-Adresse oder FQDN sowie den Port
- Anmeldeinformationen für den ONTAP tools Manager Admin (Benutzername und Passwort)

Parameter und Variablen

Die unten aufgeführten curl-Beispiele verwenden Variablen im Bash-Stil. Diese Variablen können in der Bash-Umgebung festgelegt oder vor der Ausführung der Befehle manuell aktualisiert werden. Wenn die Variablen festgelegt sind, ersetzt die Shell die Werte in jedem Befehl, bevor dieser ausgeführt wird. Die Variablen werden in der folgenden Tabelle beschrieben.

Variable	Beschreibung
\$FQDN_IP_PORT	Der vollqualifizierte Domainname oder die IP-Adresse des ONTAP tools Managers zusammen mit der Portnummer.
\$MYUSER	Benutzername für das ONTAP tools Manager Konto.
\$MYPASSWORD	Passwort, das mit dem Benutzernamen des ONTAP tools Manager verknüpft ist.
\$ACCESS_TOKEN	Das vom ONTAP tools Manager ausgestellte Zugriffstoken.

Die folgenden Befehle und Ausgaben an der Linux-Befehlszeile veranschaulichen, wie eine Variable gesetzt und angezeigt werden kann:

```
FQDN_IP_PORT=172.14.31.224:8443
echo $FQDN_IP
172.14.31.224:8443
```

Schritt 1: Zugriffstoken abrufen

Um die REST API nutzen zu können, benötigen Sie ein Zugriffstoken. Ein Beispiel für die Anforderung eines Zugriffstokens wird unten dargestellt. Dabei sind die entsprechenden Werte für Ihre Umgebung einzusetzen.

```
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 enthaltene Zugriffstoken.

Schritt 2: Den REST API-Aufruf ausführen

Nachdem Sie ein Zugriffstoken erhalten haben, kann curl verwendet werden, um einen REST-API-Aufruf durchzuführen. Das im ersten Schritt erworbene Zugriffstoken ist einzufügen.

Curl Beispiel

```
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 sind.

ONTAP tools REST API-Referenz

Die ONTAP tools for VMware vSphere 10 REST API-Referenz enthält Details zu allen API-Aufrufen. Diese Referenz ist hilfreich bei der Entwicklung von Automatisierungsanwendungen.

Die ONTAP tools for VMware vSphere 10 REST API-Dokumentation ist online über die Swagger-Benutzeroberfläche verfügbar. Die IP-Adresse oder der vollqualifizierte Domainname (FQDN) des ONTAP tools for VMware vSphere 10 Gateway-Dienstes sowie der Port werden benötigt.

Schritte

1. Geben Sie die folgende URL in Ihren Browser ein, ersetzen Sie dabei die Variable durch die entsprechende IP-Adresse und Portkombination und drücken Sie **Enter**.

```
https://$FQDN_IP_PORT/
```

Beispiel

```
https://10.61.25.33:8443/
```

2. Als Beispiel für einen einzelnen API-Aufruf nach unten zur Kategorie **vCenters** scrollen und **GET** neben dem Endpunkt auswählen `/virtualization/api/v1/vcenters`

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtsvermerke, Marken, Patente und mehr.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp Trademarks-Seite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patente

Eine aktuelle Liste der NetApp owned patents finden Sie unter:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Datenschutzrichtlinie

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open Source

Hinweisdateien enthalten Informationen über Urheberrechte und Lizenzen Dritter, die in NetApp Software verwendet werden.

["Hinweis zu ONTAP tools für VMware vSphere 10.5"](#)

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.