ONTAP tools for VMware vSphere Dokumentation

ONTAP tools for VMware vSphere 10

NetApp
September 29, 2025

Inhalt

ONTAP tools for VMware vSphere Dokumentation

Versionshinweise

Versionshinweise

Informieren Sie sich über die neuen und verbesserten Funktionen der ONTAP tools for VMware vSphere 10.4.

Eine vollständige Liste der neuen Funktionen und Verbesserungen finden Sie unterWas ist neu in den ONTAP tools for VMware vSphere 10.4 .

Um mehr darüber zu erfahren, ob die Migration von ONTAP tools for VMware vSphere 9 auf ONTAP Tools 10.4 für Ihre Bereitstellung geeignet ist, lesen SieFunktionsvergleich von ONTAP tools for VMware vSphere 9 und ONTAP tools for VMware vSphere 10 . Die Migration von ONTAP tools for VMware vSphere 9.12-D und 9.13-D-Versionen zu ONTAP tools for VMware vSphere 10.4 wird unterstützt.

Weitere Informationen finden Sie im "ONTAP tools for VMware vSphere 10.4 – Versionshinweise" . Sie müssen sich mit Ihrem NetApp -Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zugreifen zu können.

Was ist neu in den ONTAP tools for VMware vSphere 10.4

Informieren Sie sich über die neuen Funktionen der ONTAP tools for VMware vSphere 10.4.

Aktualisieren	Beschreibung
"Unterstützung für ASA R2-System mit 12 Knoten pro Cluster"	ONTAP tools for VMware vSphere 10.4 unterstützen Workflows für ASA R2-Speichersysteme mit bis zu 12 Knoten pro Cluster und verbessern so die Effizienz und Skalierbarkeit des Datenmanagements. Es unterstützt vVols -Datenspeicher mit iSCSI- und FC-Protokoll sowie VMFS-Datenspeicher mit iSCSI-, FC- und NVMe-Protokoll und bietet flexible und erweiterte Speicheroptionen.
"Verbesserungen der Benutzeroberfläche des ONTAP Tools Manager"	Sie können jetzt den NTP-Server für eine präzise Zeitsynchronisierung in der gesamten Umgebung aktivieren und die Telemetrieeinstellungen konfigurieren, um die Systemleistung über die ONTAP Tools Manager-Schnittstelle zu überwachen und zu analysieren. Diese Einstellungen sind in der Wartungskonsole nicht mehr verfügbar.
Verbesserte Sicherheitsfunktionen	Sicherheitsfunktionen bieten jetzt verbesserten Schutz und Konformität mit Branchenstandards und sorgen für eine robuste und benutzerfreundliche Erfahrung, die Administratoren dabei hilft, VMware-Umgebungen effektiver zu verwalten.
"Erweiterte SRA-Disaster-Recovery-Funktionen"	ONTAP tools for VMware vSphere 10.4 unterstützen jetzt Disaster Recovery-Vorgänge mithilfe der Site Recovery Appliance (SRA) mit Snapshots mit benutzerdefinierten Namen zusätzlich zu den geplanten SnapMirror -Snapshot-Kopien.

Funktionsvergleich von ONTAP tools for VMware vSphere 9 und ONTAP tools for VMware vSphere 10

Erfahren Sie, ob die Migration von ONTAP tools for VMware vSphere 9 auf ONTAP tools for VMware vSphere 10.1 oder spätere Versionen das Richtige für Sie ist.

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

Funktion	ONTAP -Tools 9.13	ONTAP -Tools 10.1	ONTAP -Tools ab 10.2
Wichtigstes Wertversprechen	Optimieren und vereinfachen Sie den Betrieb von Tag 0 bis Tag 2 mit verbesserten Sicherheits-, Compliance- und Automatisierungsfunktionen	Weiterentwicklung der ONTAP Tools 10.x in Richtung 9.xx-Parität bei gleichzeitiger Erweiterung der Hochverfügbarkeit, Leistung und Skalierungsgrenzen	Erweiterte Unterstützung um FC für VMFS und vVols sowie NVMe-oF/FC, NVMe-oF/TCP nur für VMFS. Benutzerfreundlichkeit für NetApp SnapMirror, einfache Einrichtung für vSphere Metro Storage-Cluster und VMware Live Site Recovery-Unterstützung für drei Standorte
ONTAP Release-Qualifizierung	ONTAP 9.9.1 bis ONTAP 9.16.1	ONTAP 9.12.1 bis ONTAP 9.14.1	ONTAP 9.12.1 bis ONTAP 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 erforderlich, wenn ASA R2-Systeme verwendet werden.
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 VMware Site Recovery Manager (SRM) 8.7 bis VMware Live Site Recovery 9.0	vSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 bis VMware Live Site Recovery 9.0
Protokollunterstützung	NFS- und VMFS-Datenspeicher: NFS (v3 und v4.1), VMFS (iSCSI und FCP) vVols -Datenspeicher: iSCSI, FCP, NVMe/FC, NFS v3	NFS- und VMFS-Datenspeicher: NFS (v3 und v4.1), VMFS (iSCSI) vVols -Datenspeicher: iSCSI, NFS v3	NFS- und VMFS-Datenspeicher: NFS (v3 und v4.1), VMFS (iSCSI/FCP/NVMe-oF) vVols -Datenspeicher: iSCSI, FCP, NFS v3
Skalierbarkeit	Hosts und VMs: 300 Hosts, bis zu 10.000 VMs. Datenspeicher: 600 NFS, bis zu 50 VMFS, bis zu 250 vVols. vVols: Bis zu 14.000	Hosts und VMs: 600 Hosts vVols: Bis zu 140.000	Hosts und VMs: 600 Hosts vVols: Bis zu 140.000

Funktion	ONTAP -Tools 9.13	ONTAP -Tools 10.1	ONTAP -Tools ab 10.2
Beobachtbarkeit	Dashboards zu Leistung, Kapazität und Host-Compliance Dynamische VM- und Datenspeicherberichte	Aktualisierte Dashboards zu Leistung, Kapazität und Host-Compliance. Dynamische VM- und Datenspeicherberichte.	Aktualisierte Dashboards zu Leistung, Kapazität und Host-Compliance. Dynamische VM- und Datenspeicherberichte.
Datenschutz	SRA-Replikation für VMFS und NFS FlexVols-basierte Replikation für vVols SCV-Integration und interoperabel für Backup	SRA-Replikation für iSCSI-VMFS- und NFS v3-Datenspeicher	SRA-Replikation für iSCSI-VMFS- und NFS v3-Datenspeicher, Drei-Site-Schutz durch Kombination von SMAS und VMware Live Site Recovery.
VASA-Anbieterunterstützung	VASA 4,0	VASA 3,0	VASA 3,0

Konzepte

ONTAP tools for VMware vSphere – Übersicht

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

ONTAP tools for VMware vSphere bestehen aus Folgendem:

- Funktionen virtueller Maschinen wie Basisschutz und Notfallwiederherstellung
- VASA-Anbieter für granulares VM-Management
- Speicherrichtlinienbasierte Verwaltung
- Speicherreplikationsadapter (SRA)

Wichtige Konzepte und Begriffe

Der folgende Abschnitt beschreibt die wichtigsten Konzepte und Begriffe, die im Dokument verwendet werden.

ASA R2-Systeme

Die neuen NetApp ASA r2-Systeme bieten eine einheitliche Hardware- und Softwarelösung, die ein vereinfachtes Erlebnis bietet, das speziell auf die Anforderungen von reinen SAN-Kunden zugeschnitten ist. "Erfahren Sie mehr über ASA R2-Speichersysteme" .

Zertifizierungsstelle (CA)

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

Konsistenzgruppe (CG)

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

Doppelstapel

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

Hohe Verfügbarkeit (HA)

Clusterknoten werden für unterbrechungsfreie Vorgänge in HA-Paaren konfiguriert.

Logische Gerätenummer (LUN)

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

NVMe-Namespace und -Subsystem

Ein NVMe-Namespace ist eine Menge nichtflüchtigen Speichers, der in logische Blöcke formatiert werden kann. Namespaces entsprechen LUNs für FC- und iSCSI-Protokolle und ein NVMe-Subsystem entspricht einer igroup. Ein NVMe-Subsystem kann mit Initiatoren verknüpft werden, sodass die verknüpften Initiatoren auf Namespaces innerhalb des Subsystems zugreifen können.

ONTAP Tools Manager

ONTAP Tools Manager bietet ONTAP tools for VMware vSphere über die verwalteten vCenter Server-Instanzen und integrierten Speicher-Backends. Es hilft bei der Verwaltung von vCenter Server-Instanzen, Speicher-Backends, Zertifikaten, Passwörtern und Protokollpaket-Downloads.

Öffnen Sie die virtuelle Appliance (OVA).

OVA ist ein offener Standard zum Verpacken und Verteilen virtueller Appliances oder Software, die auf virtuellen Maschinen ausgeführt werden muss.

Wiederherstellungspunktziel (RPO)

RPO misst, wie häufig Sie Daten sichern oder replizieren. Es gibt den genauen Zeitpunkt an, zu dem Sie nach einem Ausfall die Daten wiederherstellen müssen, um den Geschäftsbetrieb wieder aufzunehmen. Wenn eine Organisation beispielsweise über ein RPO von 4 Stunden verfügt, kann sie im Katastrophenfall einen Datenverlust von bis zu 4 Stunden tolerieren.

SnapMirror aktive Synchronisierung

SnapMirror Active Sync ermöglicht die Weiterführung des Betriebs von Geschäftsdiensten auch bei einem vollständigen Site-Ausfall und unterstützt Anwendungen bei einem transparenten Failover mithilfe einer sekundären Kopie. Zum Auslösen eines Failovers mit SnapMirror Active Sync sind kein manuelles Eingreifen oder benutzerdefiniertes Skripting erforderlich. Erfahren Sie mehr über "SnapMirror aktive Synchronisierung" .

Speicher-Backends

Speicher-Backends sind die zugrunde liegende Speicherinfrastruktur, die der ESXi-Host zum Speichern von Dateien, Daten und anderen Ressourcen virtueller Maschinen verwendet. 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 (Speicher-Backend)

Globale Speicher-Backends, die nur mit ONTAP Cluster-Anmeldeinformationen verfügbar sind, werden über die ONTAP Tools Manager-Schnittstelle integriert. Sie können mit minimalen Berechtigungen hinzugefügt werden, um die Erkennung wesentlicher Clusterressourcen zu ermöglichen, die für die vVols Verwaltung

erforderlich sind. Globale Cluster eignen sich ideal für Multitenancy-Szenarien, in denen ein SVM-Benutzer lokal zur vVols Verwaltung hinzugefügt wird.

Lokales Speicher-Backend

Lokale Speicher-Backends mit Cluster- oder SVM-Anmeldeinformationen werden über die Benutzeroberfläche der ONTAP Tools hinzugefügt und sind auf ein 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 ONTAP -Tools SVM-Anmeldeinformationen, ohne dass ein globaler Cluster erforderlich ist.

Speicherreplikationsadapter (SRA)

SRA ist die speicheranbieterspezifische Software, die im VMware Live Site Recovery-Gerät installiert ist. Der Adapter ermöglicht die Kommunikation zwischen Site Recovery Manager und einem Speichercontroller auf der Ebene der Storage Virtual Machine (SVM) und der Konfiguration auf Clusterebene.

Virtuelle Speichermaschine (SVM)

SVM ist die Einheit der Multitenancy in ONTAP. Wie eine virtuelle Maschine, die auf einem Hypervisor ausgeführt wird, ist SVM eine logische Einheit, die physische Ressourcen abstrahiert. SVM enthält Datenvolumes und ein oder mehrere LIFs, über die sie den Clients Daten bereitstellen.

Einheitliche und uneinheitliche Konfiguration

- **Einheitlicher Hostzugriff** bedeutet, dass Hosts von zwei Standorten mit allen Pfaden zu Speicherclustern an beiden Standorten verbunden sind. Standortübergreifende Wege sind über weite Strecken gestreckt.
- **Nicht einheitlicher Hostzugriff** bedeutet, dass Hosts an jedem Standort nur mit dem Cluster am selben Standort verbunden sind. Standortübergreifende Pfade und gestreckte Pfade sind nicht verbunden.

> Einheitlicher Hostzugriff wird für jede SnapMirror Active Sync-Bereitstellung unterstützt; nicht einheitlicher Hostzugriff wird nur für symmetrische Active/Active-Bereitstellungen unterstützt. Erfahren Sie mehr über "SnapMirror Active Sync-Übersicht in ONTAP" .

Dateisystem der virtuellen Maschine (VMFS)

VMFS ist ein Cluster-Dateisystem zum Speichern von Dateien virtueller Maschinen in VMware vSphere-Umgebungen.

Virtuelle Volumes (vVols)

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

VM-Speicherrichtlinie

VM-Speicherrichtlinien werden im vCenter Server unter Richtlinien und Profile erstellt. Erstellen Sie für vVols einen Regelsatz mit Regeln vom NetApp vVols Speichertypanbieter.

VMware Live Site Recovery

VMware Live Site Recovery, früher bekannt als Site Recovery Manager (SRM), bietet Geschäftskontinuität, Notfallwiederherstellung, Site-Migration und unterbrechungsfreie Testfunktionen für virtuelle VMware-

Umgebungen.

VMware vSphere-APIs für Storage Awareness (VASA)

VASA ist ein Satz von APIs, die Speicher-Arrays zur Verwaltung und Administration mit vCenter Server 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 ein Satz von APIs, der die Kommunikation zwischen VMware vSphere ESXi-Hosts und den Speichergeräten ermöglicht. Die APIs umfassen eine Reihe primitiver Operationen, die von den Hosts verwendet werden, um Speicheroperationen auf das Array auszulagern. VAAI kann bei speicherintensiven Aufgaben erhebliche Leistungsverbesserungen bieten.

vSphere Metro Storage Cluster

vSphere Metro Storage Cluster (vMSC) ist eine Architektur, die vSphere in einer Stretched-Cluster-Bereitstellung ermöglicht und unterstützt. vMSC-Lösungen werden mit NetApp MetroCluster und SnapMirror Active Sync (früher SMBC) unterstützt. Diese Lösungen sorgen für eine verbesserte Geschäftskontinuität im Falle eines Domänenausfalls. Das Resilienzmodell basiert auf Ihren spezifischen Konfigurationsentscheidungen. Erfahren Sie mehr über "VMware vSphere Metro Storage Cluster" .

vVols -Datenspeicher

Der vVols Datenspeicher ist eine logische Datenspeicherdarstellung eines vVols Containers, der von einem VASA-Anbieter erstellt und verwaltet wird.

Null RPO

RPO steht für Recovery Point Objective und bezeichnet den Umfang des Datenverlusts, der innerhalb eines bestimmten Zeitraums als akzeptabel erachtet wird. Null RPO bedeutet, dass kein Datenverlust akzeptabel ist.

Rollenbasierte Zugriffskontrolle

Erfahren Sie mehr über ONTAP tools for VMware vSphere 10 RBAC

Die rollenbasierte Zugriffskontrolle (RBAC) ist ein Sicherheitsrahmen zur Kontrolle des Zugriffs auf Ressourcen innerhalb einer Organisation. RBAC vereinfacht die Verwaltung, indem es Rollen mit bestimmten Berechtigungsstufen zum Ausführen von Aktionen definiert, anstatt einzelnen Benutzern Berechtigungen zuzuweisen. Die definierten Rollen werden den Benutzern zugewiesen, wodurch das Fehlerrisiko verringert und die Verwaltung der Zugriffskontrolle in Ihrem Unternehmen vereinfacht wird.

Das RBAC-Standardmodell besteht aus mehreren Implementierungstechnologien oder Phasen zunehmender Komplexität. Das Ergebnis ist, dass die tatsächlichen RBAC-Bereitstellungen je nach den Anforderungen der Softwareanbieter und ihrer Kunden unterschiedlich sein und von relativ einfach bis sehr komplex reichen können.

RBAC-Komponenten

Auf hoher Ebene gibt es mehrere Komponenten, die im Allgemeinen in jeder RBAC-Implementierung enthalten

sind. Diese Komponenten werden im Rahmen der Definition der Autorisierungsprozesse auf unterschiedliche Weise miteinander verknüpft.

Privileges

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

Rollen

Eine *Rolle* ist ein Container, der ein oder mehrere Privilegien enthält. Rollen werden im Allgemeinen auf der Grundlage bestimmter Aufgaben oder Arbeitsfunktionen definiert. Wenn einem Benutzer eine Rolle zugewiesen wird, erhält der Benutzer alle in der Rolle enthaltenen Berechtigungen. Und wie bei den Berechtigungen umfassen Implementierungen vordefinierte Rollen und ermöglichen im Allgemeinen die Erstellung benutzerdefinierter Rollen.

Objekte

Ein *Objekt* stellt eine reale oder abstrakte Ressource dar, die innerhalb der RBAC-Umgebung identifiziert wird. Die durch die Berechtigungen definierten Aktionen werden an oder mit den zugehörigen Objekten ausgeführt. Je nach Implementierung können Berechtigungen einem Objekttyp oder einer bestimmten Objektinstanz erteilt werden.

Benutzer und Gruppen

Benutzern wird nach der Authentifizierung eine Rolle zugewiesen oder zugeordnet. Bei einigen RBAC-Implementierungen kann einem Benutzer nur eine Rolle zugewiesen werden, während bei anderen mehrere Rollen pro Benutzer zulässig sind, wobei möglicherweise immer nur eine Rolle aktiv ist. Durch die Zuweisung von Rollen zu *Gruppen* kann die Sicherheitsverwaltung weiter vereinfacht werden.

Berechtigungen

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

Zwei RBAC-Umgebungen

Es gibt zwei unterschiedliche RBAC-Umgebungen, die Sie bei der Arbeit mit ONTAP tools for VMware vSphere 10 berücksichtigen müssen.

VMware vCenter Server

Die RBAC-Implementierung in VMware vCenter Server wird verwendet, um den Zugriff auf Objekte einzuschränken, die über die Benutzeroberfläche des vSphere-Clients verfügbar gemacht werden. Im Rahmen der Installation von ONTAP tools for VMware vSphere 10 wird die RBAC-Umgebung um zusätzliche Objekte erweitert, die die Funktionen der ONTAP -Tools darstellen. Der Zugriff auf diese Objekte erfolgt über das Remote-Plugin. Siehe"vCenter Server RBAC-Umgebung" für weitere Informationen.

ONTAP -Cluster

ONTAP tools for VMware vSphere 10 stellen über die ONTAP REST API eine Verbindung zu einem ONTAP Cluster her, um speicherbezogene Vorgänge auszuführen. Der Zugriff auf die Speicherressourcen wird über eine ONTAP Rolle gesteuert, die dem bei der Authentifizierung angegebenen ONTAP -Benutzer zugeordnet ist. Sehen "ONTAP RBAC-Umgebung" für weitere Informationen.

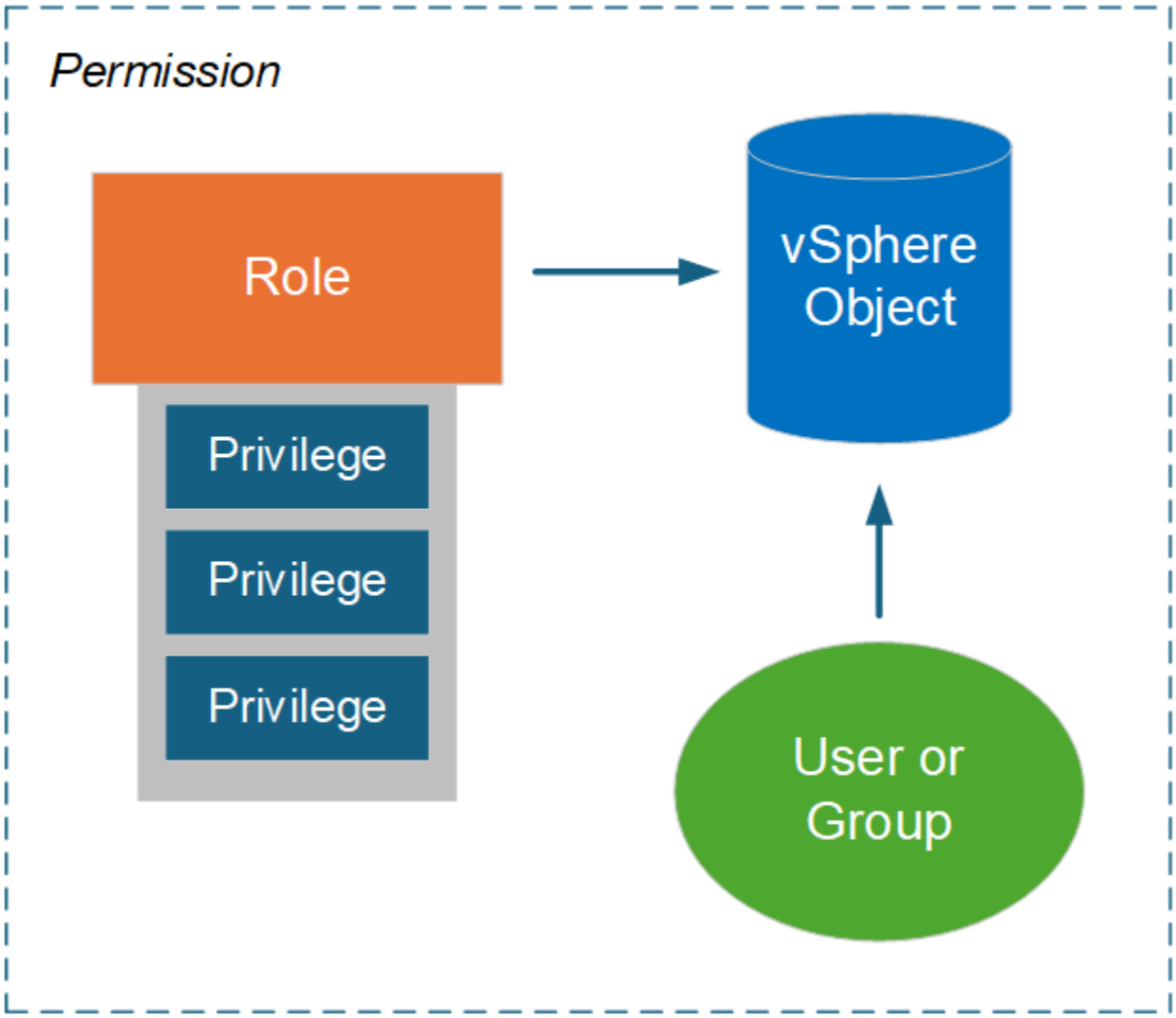
RBAC mit VMware vSphere

vCenter Server RBAC-Umgebung mit ONTAP tools for VMware vSphere 10

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

Abbildung einer vCenter Server-Berechtigung

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



Komponenten einer vCenter Server-Berechtigung

Eine vCenter Server-Berechtigung ist ein Paket aus mehreren Komponenten, die beim Erstellen der

Berechtigung miteinander verbunden werden.

vSphere-Objekte

Berechtigungen sind mit vSphere-Objekten verknüpft, beispielsweise mit dem vCenter Server, ESXi-Hosts, virtuellen Maschinen, Datenspeichern, Rechenzentren und Ordnern. Basierend auf den dem Objekt zugewiesenen Berechtigungen bestimmt vCenter Server, welche Aktionen oder Aufgaben von jedem Benutzer oder jeder Gruppe am Objekt ausgeführt werden können. Für die für ONTAP tools for VMware vSphere spezifischen Aufgaben werden alle Berechtigungen auf der Stamm- oder Stammordnerebene von vCenter Server zugewiesen und validiert. Sehen "Verwenden von RBAC mit vCenter-Server" für weitere Informationen.

Privileges und Rollen

Es gibt zwei Arten von vSphere-Berechtigungen, die mit ONTAP tools for VMware vSphere 10 verwendet werden. Um die Arbeit mit RBAC in dieser Umgebung zu vereinfachen, stellen ONTAP Tools Rollen bereit, die die erforderlichen nativen und benutzerdefinierten Berechtigungen enthalten. Zu den Privilegien gehören:

- Native vCenter Server-Berechtigungen

  Dies sind die von vCenter Server bereitgestellten Berechtigungen.

- ONTAP -Tool-spezifische Berechtigungen

  Dies sind benutzerdefinierte Berechtigungen, die nur für ONTAP tools for VMware vSphere gelten.

Benutzer und Gruppen

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

Verwenden Sie vCenter Server RBAC mit ONTAP tools for VMware vSphere 10

Es gibt mehrere Aspekte der ONTAP tools for VMware vSphere 10 RBAC-Implementierung mit vCenter Server, die Sie berücksichtigen sollten, bevor Sie sie in einer Produktionsumgebung verwenden.

vCenter-Rollen und das Administratorkonto

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

vSphere-Objekthierarchie

Das vSphere-Objektinventar ist hierarchisch organisiert. Sie können sich beispielsweise wie folgt in der Hierarchie nach unten bewegen:

`vCenter Server` ⟶ `Datacenter` ⟶ `Cluster` ⟶ `ESXi host` ⟶ `Virtual Machine`

Alle Berechtigungen werden in der vSphere-Objekthierarchie validiert, mit Ausnahme der VAAI-Plug-In-Vorgänge, die anhand des ESXi-Zielhosts validiert werden.

In den ONTAP tools for VMware vSphere 10 enthaltene Rollen

Um die Arbeit mit vCenter Server RBAC zu vereinfachen, bieten ONTAP tools for VMware vSphere vordefinierte Rollen, die auf verschiedene Verwaltungsaufgaben zugeschnitten sind.

> Sie können bei Bedarf neue benutzerdefinierte Rollen erstellen. In diesem Fall sollten Sie eine der vorhandenen ONTAP -Tool-Rollen klonen und nach Bedarf bearbeiten. Nach dem Vornehmen der Konfigurationsänderungen müssen sich die betroffenen vSphere-Client-Benutzer abmelden und erneut anmelden, um die Änderungen zu aktivieren.

Um die ONTAP tools for VMware vSphere -Rollen anzuzeigen, wählen Sie oben im vSphere-Client **Menü** und klicken Sie auf **Verwaltung** und dann links auf **Rollen**. Es gibt drei vordefinierte Rollen, die unten beschrieben werden.

NetApp ONTAP tools for VMware vSphere Administrator

Bietet alle nativen vCenter Server-Berechtigungen und ONTAP Tool-spezifischen Berechtigungen, die zum Ausführen zentraler ONTAP tools for VMware vSphere Administratoraufgaben erforderlich sind.

NetApp ONTAP tools for VMware vSphere Read Only

Bietet schreibgeschützten Zugriff auf ONTAP -Tools. Diese Benutzer können keine ONTAP tools for VMware vSphere Aktionen ausführen, für die der Zugriff kontrolliert wird.

NetApp ONTAP tools for VMware vSphere Provision

Bietet einige der nativen vCenter Server-Berechtigungen und ONTAP Tool-spezifischen Berechtigungen, die für die Speicherbereitstellung erforderlich sind. Sie können die folgenden Aufgaben ausführen:

- Erstellen neuer Datenspeicher
- Verwalten von Datenspeichern

vSphere-Objekte und ONTAP -Speicher-Backends

Die beiden RBAC-Umgebungen arbeiten zusammen. Beim Ausführen einer Aufgabe in der vSphere-Clientschnittstelle werden zuerst die für vCenter Server definierten ONTAP -Toolrollen überprüft. Wenn der Vorgang von vSphere zugelassen wird, werden die ONTAP Rollenberechtigungen geprüft. Dieser zweite Schritt wird basierend auf der ONTAP Rolle ausgeführt, die dem Benutzer beim Erstellen und Konfigurieren des Speicher-Backends zugewiesen wurde.

Arbeiten mit vCenter Server RBAC

Beim Arbeiten mit den Privilegien und Berechtigungen des vCenter Servers sind einige Dinge zu beachten.

Erforderliche Berechtigungen

Um auf die Benutzeroberfläche der ONTAP tools for VMware vSphere 10 zugreifen zu können, benötigen Sie das für ONTAP -Tools spezifische *Anzeige*-Privileg. 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. Wenn Sie dem Stammobjekt die Berechtigung „Anzeigen“ zuweisen, können Sie durch Klicken auf das NetApp -Symbol auf ONTAP tools for VMware vSphere zugreifen.

Sie können die Anzeigeberechtigung stattdessen einer anderen niedrigeren vSphere-Objektebene zuweisen. Dadurch werden jedoch die ONTAP tools for VMware vSphere -Menüs eingeschränkt, auf die Sie zugreifen und die Sie verwenden können.

Berechtigungen zuweisen

Sie müssen vCenter Server-Berechtigungen verwenden, wenn Sie den Zugriff auf die vSphere-Objekte und -Aufgaben beschränken möchten. Wo Sie in der vSphere-Objekthierarchie Berechtigungen zuweisen, bestimmt, welche ONTAP tools for VMware vSphere 10-Aufgaben Benutzer ausführen können.

Sofern Sie keinen restriktiveren Zugriff definieren müssen, empfiehlt es sich im Allgemeinen, Berechtigungen auf der Ebene des Stammobjekts oder des Stammordners zuzuweisen.

Die mit den ONTAP tools for VMware vSphere 10 verfügbaren Berechtigungen gelten für benutzerdefinierte Nicht-vSphere-Objekte, beispielsweise Speichersysteme. Wenn möglich, sollten Sie diese Berechtigungen den ONTAP tools for VMware vSphere Stammobjekt zuweisen, da es kein vSphere-Objekt gibt, dem Sie sie zuweisen können. Beispielsweise sollte jede Berechtigung, die ein ONTAP tools for VMware vSphere Privileg zum „Hinzufügen/Ändern/Entfernen von Speichersystemen“ umfasst, auf der Stammobjektebene zugewiesen werden.

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

Sie können eine Berechtigung jederzeit ändern. Wenn Sie Berechtigungen innerhalb einer Berechtigung ändern, müssen sich die mit der Berechtigung verknüpften Benutzer von vSphere abmelden und erneut anmelden, um die Änderung zu aktivieren.

RBAC mit ONTAP

ONTAP RBAC-Umgebung mit ONTAP tools for VMware vSphere 10

ONTAP bietet eine robuste und erweiterbare RBAC-Umgebung. Sie können die RBAC-Funktion verwenden, um den Zugriff auf die Speicher- und Systemvorgänge zu steuern, die über die REST-API und CLI bereitgestellt werden. Es ist hilfreich, sich mit der Umgebung vertraut zu machen, bevor Sie sie mit einem ONTAP tools for VMware vSphere 10 verwenden.

Übersicht der administrativen Möglichkeiten

Bei der Verwendung von ONTAP RBAC stehen Ihnen je nach Umgebung und Zielen mehrere Optionen zur Verfügung. Nachfolgend finden Sie eine Übersicht über die wichtigsten Verwaltungsentscheidungen. Siehe auch "ONTAP -Automatisierung: Übersicht über die RBAC-Sicherheit" für weitere Informationen.

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

Arten von Rollen und Berechtigungen

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

- AUSRUHEN

  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 Berechtigungen sind hinsichtlich des Zugriffs auf die ONTAP REST API-Endpunkte und die zugehörigen Aktionen definiert.

- Traditionell

  Dies sind die Legacy-Rollen, die vor ONTAP 9.6 enthalten waren. Sie sind weiterhin ein grundlegender Aspekt von RBAC. Die Berechtigungen werden in Bezug auf den Zugriff auf die ONTAP CLI-Befehle definiert.

Während die REST-Rollen erst vor kurzem eingeführt wurden, bieten die traditionellen Rollen einige Vorteile. Beispielsweise können optional zusätzliche Abfrageparameter eingefügt werden, sodass die Berechtigungen die Objekte, auf die sie angewendet werden, genauer definieren.

Umfang

ONTAP -Rollen können mit einem von zwei verschiedenen Bereichen 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. Sie können auch benutzerdefinierte Rollen definieren.

Arbeiten mit ONTAP REST-Rollen

Bei der Verwendung der in den ONTAP tools for VMware vSphere 10 enthaltenen ONTAP REST-Rollen sind mehrere Aspekte zu beachten.

Rollenzuordnung

Unabhängig davon, ob eine herkömmliche oder eine REST-Rolle verwendet wird, werden alle ONTAP Zugriffsentscheidungen auf Grundlage des zugrunde liegenden CLI-Befehls getroffen. Da die Berechtigungen in einer REST-Rolle jedoch in Bezug auf die REST-API-Endpunkte definiert sind, muss ONTAP für jede der REST-Rollen eine *zugeordnete* traditionelle Rolle erstellen. Daher wird jede REST-Rolle einer zugrunde liegenden traditionellen Rolle zugeordnet. Dadurch kann ONTAP unabhängig vom Rollentyp konsistente Entscheidungen zur Zugriffskontrolle treffen. Sie können die parallel zugeordneten Rollen nicht ändern.

Definieren einer REST-Rolle mit CLI-Berechtigungen

Da ONTAP immer die CLI-Befehle verwendet, um den Zugriff auf einer Basisebene zu bestimmen, ist es möglich, eine REST-Rolle mithilfe von CLI-Befehlsberechtigungen anstelle von REST-Endpunkten auszudrücken. Ein Vorteil dieses Ansatzes ist die zusätzliche Granularität, die mit den herkömmlichen Rollen verfügbar ist.

Verwaltungsschnittstelle beim Definieren von ONTAP Rollen

Sie können Benutzer und Rollen mit der ONTAP CLI und der REST API erstellen. Es ist jedoch bequemer, die System Manager-Schnittstelle zusammen mit der JSON-Datei zu verwenden, die über den ONTAP Tools Manager verfügbar ist. Sehen "Verwenden Sie ONTAP RBAC mit ONTAP tools for VMware vSphere 10" für weitere Informationen.

Verwenden Sie ONTAP RBAC mit ONTAP tools for VMware vSphere 10

Es gibt mehrere Aspekte der ONTAP tools for VMware vSphere 10 RBAC-Implementierung mit ONTAP , die Sie berücksichtigen sollten, bevor Sie sie in einer Produktionsumgebung verwenden.

Übersicht über den Konfigurationsprozess

ONTAP tools for VMware vSphere 10 unterstützen die Erstellung eines ONTAP Benutzers mit einer benutzerdefinierten Rolle. Die Definitionen sind in einer JSON-Datei verpackt, die Sie in den ONTAP Cluster hochladen können. Sie können den Benutzer erstellen und die Rolle an Ihre Umgebung und Sicherheitsanforderungen anpassen.

Die wichtigsten Konfigurationsschritte werden unten ausführlich beschrieben. Siehe"Konfigurieren Sie ONTAP Benutzerrollen und -Berechtigungen" für weitere Details.

1. Vorbereiten

Sie benötigen Administratoranmeldeinformationen sowohl für den ONTAP Tools Manager als auch für den ONTAP Cluster.

2. Laden Sie die JSON-Definitionsdatei herunter

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

3. Erstellen Sie einen ONTAP -Benutzer mit einer Rolle

Nachdem Sie sich beim System Manager angemeldet haben, können Sie den Benutzer und die Rolle erstellen:

1. Wählen Sie links **Cluster** und dann **Einstellungen**.
2. Scrollen Sie nach unten zu **Benutzer und Rollen** und klicken Sie auf −→ .
3. Wählen Sie unter **Benutzer Hinzufügen** und wählen Sie **Virtualisierungsprodukte**.
4. Wählen Sie die JSON-Datei auf Ihrer lokalen Workstation aus und laden Sie sie hoch.

4. Konfigurieren der Rolle

Im Rahmen der Rollendefinition müssen Sie mehrere administrative Entscheidungen treffen. SehenKonfigurieren der Rolle mit System Manager für weitere Details.

Konfigurieren der Rolle mit System Manager

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

Grundlegende Benutzer- und Rollenkonfiguration

Die RBAC-Definitionen sind als mehrere Produktfunktionen verpackt, darunter Kombinationen aus VSC, VASA Provider und SRA. Sie sollten die Umgebung(en) auswählen, in denen Sie RBAC-Unterstützung benötigen. Wenn Sie beispielsweise möchten, dass Rollen die Remote-Plug-In-Funktion unterstützen, wählen Sie VSC aus. Außerdem müssen Sie den Benutzernamen und das zugehörige Passwort wählen.

Privileges

Die Rollenberechtigungen sind in vier Gruppen unterteilt, basierend auf der erforderlichen Zugriffsebene auf den ONTAP Speicher. Zu den den Rollen zugrunde liegenden Berechtigungen gehören:

- Entdeckung

  Mit dieser Rolle können Sie Speichersysteme hinzufügen.

- Speicher erstellen

  Mit dieser Rolle können Sie Speicher erstellen. Es umfasst auch alle mit der Discovery-Rolle verbundenen Berechtigungen.

- Speicher ändern

  Mit dieser Rolle können Sie den Speicher ändern. Es umfasst auch alle Berechtigungen, die mit den Rollen „Erkennen“ und „Speicher erstellen“ verbunden sind.

- Speicher zerstören

  Mit dieser Rolle können Sie Speicher zerstören. Es umfasst außerdem alle Berechtigungen, die mit der Erkennung, Speichererstellung und Speicheränderungsrollen verbunden sind.

Generieren Sie den Benutzer mit einer Rolle

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

- Konstanter Präfixwert, der in der JSON-Datei definiert ist (z. B. „OTV_10“)
- Die von Ihnen 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.

Hohe Verfügbarkeit für ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere unterstützen eine Hochverfügbarkeitskonfiguration (HA), um bei einem Ausfall die unterbrechungsfreie Funktionalität der ONTAP tools for VMware vSphere zu gewährleisten.

Die Hochverfügbarkeitslösung (HA) ermöglicht eine schnelle Wiederherstellung nach Ausfällen, die durch Folgendes verursacht werden:

- Hostfehler

  Es wird nur der Ausfall eines einzelnen Knotens unterstützt.

- Netzwerkfehler
- Ausfall der virtuellen Maschine (Ausfall des Gastbetriebssystems)
- Anwendungsabsturz (ONTAP -Tools)

Für ONTAP tools for VMware vSphere ist keine zusätzliche Konfiguration erforderlich, um Hochverfügbarkeit (HA) bereitzustellen.

ONTAP tools for VMware vSphere unterstützen vCenter HA nicht.

Um die HA-Funktion zu aktivieren, sollten CPU Hot Add und Memory Hot Plug während der Bereitstellung oder später in den ONTAP tools for VMware vSphere VM-Einstellungen aktiviert werden.

ONTAP Tools Manager-Benutzeroberfläche

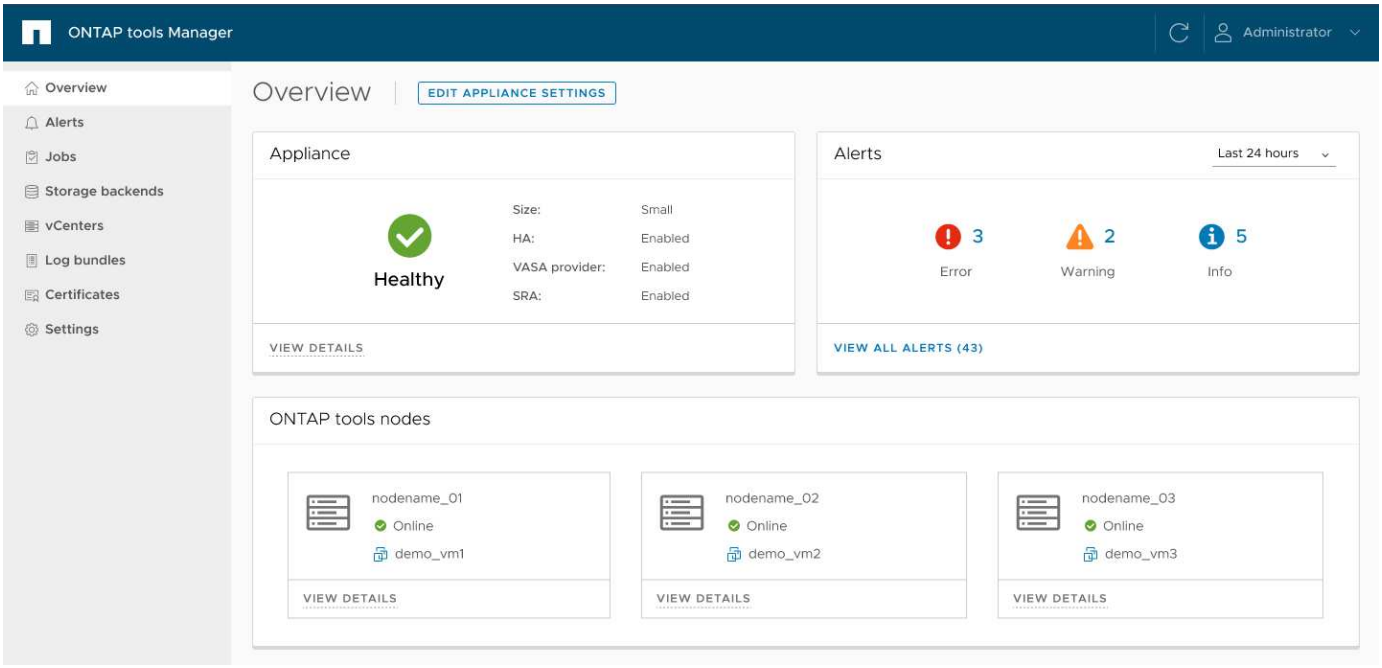
ONTAP tools for VMware vSphere sind ein Multi-Tenant-System, das mehrere vCenter Server-Instanzen verwalten kann. ONTAP Tools Manager bietet den ONTAP tools for VMware vSphere Administrator mehr Kontrolle über die verwalteten vCenter Server-Instanzen und integrierten Speicher-Backends.

ONTAP Tools Manager hilft bei:

- vCenter Server-Instanzverwaltung – Fügen Sie vCenter Server-Instanzen zu ONTAP Tools hinzu und verwalten Sie sie.
- Speicher-Backend-Verwaltung – Fügen Sie ONTAP Speichercluster zu ONTAP tools for VMware vSphere hinzu, verwalten Sie sie und ordnen Sie sie global integrierten vCenter Server-Instanzen zu.
- Downloads von Protokollpaketen – Sammeln Sie Protokolldateien für ONTAP tools for VMware vSphere.
- Zertifikatsverwaltung – Ändern Sie das selbstsignierte Zertifikat in ein benutzerdefiniertes CA-Zertifikat und erneuern oder aktualisieren Sie alle Zertifikate des VASA-Anbieters und der ONTAP Tools.
- Kennwortverwaltung – Setzen Sie das Kennwort des Benutzers für die OVA-Anwendung zurück.

Um auf den ONTAP Tools Manager zuzugreifen, starten Sie `https://<ONTAPtoolsIP>:8443/virtualization/ui/` vom Browser aus und melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.

Der Abschnitt „Übersicht“ des ONTAP Tools Managers hilft bei der Verwaltung der Appliance-Konfiguration, beispielsweise bei der Dienstverwaltung, der Skalierung der Knotengröße und der Aktivierung von Hochverfügbarkeit (HA). Sie können auch die allgemeinen Informationen der ONTAP -Tools im Zusammenhang mit den Knoten überwachen, z. B. Integrität, Netzwerkdetails und Warnungen.



Karte	Beschreibung
Gerätekarte	Die Appliance-Karte zeigt den Gesamtstatus der ONTAP Tools-Appliance an. Es zeigt die Konfigurationsdetails des Geräts und den Status der aktivierten Dienste. Weitere Informationen zur ONTAP Tools-Appliance erhalten Sie, wenn Sie auf den Link **Details anzeigen** klicken. Wenn ein Aktionsauftrag zum Bearbeiten von Geräteeinstellungen ausgeführt wird, zeigt das Geräte-Portlet den Status und die Details des Auftrags an.
Warnungskarte	Auf der Karte „Warnungen“ werden die Warnungen der ONTAP -Tools nach Typ aufgelistet, einschließlich der Warnungen auf HA-Knotenebene. Sie können die Liste der Warnungen anzeigen, indem Sie auf den Zähltext (Hyperlink) klicken. Über den Link gelangen Sie zur Seite mit der nach dem ausgewählten Typ gefilterten Warnmeldungsansicht.
vCenter	Die vCenter-Karte zeigt den Integritätsstatus der vCenter im System.
Speicher-Backends	Die Karte „Storage-Backends“ zeigt den Integritätsstatus der Storage-Backends im System.
ONTAP -Tools-Knotenkarte	Die Knotenkarte des ONTAP -Tools zeigt die Liste der Knoten mit Knotennamen, Knoten-VM-Namen, Status und allen netzwerkbezogenen Daten. Sie können **Details anzeigen** auswählen, um die zusätzlichen Details zum ausgewählten Knoten anzuzeigen. [HINWEIS] In einem Nicht-HA-Setup wird nur ein Knoten angezeigt. Im HA-Setup werden drei Knoten angezeigt.

Bereitstellen von ONTAP tools for VMware vSphere

Schnellstart für ONTAP tools for VMware vSphere

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

Zunächst stellen Sie ONTAP tools for VMware vSphere als kleine Einzelknotenkonfiguration bereit, die Kerndienste zur Unterstützung von NFS- und VMFS-Datenspeichern bereitstellt. Wenn Sie Ihre Konfiguration erweitern müssen, um vVols Datenspeicher und Hochverfügbarkeit (HA) zu verwenden, tun Sie dies, nachdem Sie diesen Workflow abgeschlossen haben. Weitere Informationen finden Sie im "Workflow für die HA-Bereitstellung" .

Planen Ihrer Bereitstellung

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

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

- "Interoperabilitätsmatrix-Tool"
- "ONTAP tools for VMware vSphere – Anforderungen und Konfigurationsgrenzen"
- "Bevor Sie beginnen"

Bereitstellen von ONTAP tools for VMware vSphere

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

- "Bereitstellen von ONTAP tools for VMware vSphere"

vCenter Server-Instanzen hinzufügen

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

- "vCenter Server-Instanzen hinzufügen"

Konfigurieren Sie ONTAP Benutzerrollen und -Berechtigungen

Konfigurieren Sie neue Benutzerrollen und Berechtigungen für die Verwaltung von Speicher-Backends mithilfe der JSON-Datei, die mit den ONTAP tools for VMware vSphere bereitgestellt wird.

- "Konfigurieren Sie ONTAP Benutzerrollen und -Berechtigungen"

5 Konfigurieren der Speicher-Backends

Fügen Sie einem ONTAP -Cluster ein Speicher-Backend hinzu. Verwenden Sie für Multitenancy-Setups, bei denen vCenter als Mandant mit einem zugehörigen SVM fungiert, den ONTAP Tools Manager, um den Cluster hinzuzufügen. Verknüpfen Sie das Speicher-Backend mit dem vCenter Server, um es global der integrierten vCenter Server-Instanz zuzuordnen.

Fügen Sie die lokalen Speicher-Backends mit Cluster- oder SVM-Anmeldeinformationen über die Benutzeroberfläche der ONTAP Tools hinzu. Diese Speicher-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 ONTAP -Tools SVM-Anmeldeinformationen, ohne dass ein globaler Cluster erforderlich ist.

- "Hinzufügen eines Speicher-Backends"
- "Verknüpfen Sie das Speicher-Backend mit einer vCenter Server-Instanz"

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

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

- "Zertifikate verwalten"

7 (Optional) Konfigurieren des SRA-Schutzes

Aktivieren Sie die SRA-Funktion, um die Notfallwiederherstellung zu konfigurieren und NFS- oder VMFS-Datenspeicher zu schützen.

- "Aktivieren Sie ONTAP tools for VMware vSphere -Dienste"
- "Konfigurieren von SRA auf der VMware Live Site Recovery-Appliance"

8 (Optional) Aktivieren Sie den SnapMirror Active Sync-Schutz

Konfigurieren Sie ONTAP tools for VMware vSphere, um den Hostclusterschutz für SnapMirror Active Sync zu verwalten. Führen Sie das ONTAP Cluster- und SVM-Peering in ONTAP Systemen durch, um SnapMirror Active Sync zu verwenden. Dies gilt nur für VMFS-Datenspeicher.

- "Schützen Sie sich mit dem Hostclusterschutz"

9 Einrichten von Backup und Recovery für Ihre ONTAP tools for VMware vSphere Bereitstellung

Planen Sie Backups Ihrer ONTAP tools for VMware vSphere -Setup, mit denen Sie das Setup im Fehlerfall wiederherstellen können.

- "Erstellen Sie ein Backup und stellen Sie das ONTAP -Tools-Setup wieder her"

Workflow für die Bereitstellung hoher Verfügbarkeit (HA)

Wenn Sie vVols Datenspeicher verwenden, müssen Sie die anfängliche Bereitstellung der ONTAP Tools auf eine Hochverfügbarkeitskonfiguration (HA) erweitern und die VASA-Provider-Dienste aktivieren.

1 **Skalieren Sie die Bereitstellung**

Sie können die ONTAP tools for VMware vSphere -Konfiguration skalieren, um die Anzahl der Knoten in der Bereitstellung zu erhöhen und die Konfiguration in ein HA-Setup zu ändern.

- "Ändern Sie die ONTAP tools for VMware vSphere Konfiguration"

2 **Dienste aktivieren**

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

Aktivieren Sie die SRA-Dienste, um die ONTAP -Tools Storage Replication Adapter (SRA) für VMware Site Recovery Manager (SRM) oder VMware Live Site Recovery (VLSR) zu verwenden.

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

3 **Aktualisieren Sie die Zertifikate**

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

- "Zertifikate verwalten"

ONTAP tools for VMware vSphere – Anforderungen und Konfigurationsgrenzen

Bevor Sie die ONTAP tools for VMware vSphere bereitstellen, sollten Sie mit den Speicherplatzanforderungen für das Bereitstellungspaket und einigen grundlegenden Hostsystemanforderungen vertraut sein.

Sie können ONTAP tools for VMware vSphere mit VMware vCenter Server Virtual Appliance (vCSA) verwenden. Sie sollten ONTAP tools for VMware vSphere auf einem unterstützten vSphere-Client bereitstellen, der ein ESXi-System enthält.

Systemanforderungen

- **Speicherplatzbedarf des Installationspakets pro Knoten**
  - 15 GB für Thin Provisioning-Installationen
  - 348 GB für Thick Provisioning-Installationen

- **Größenanforderungen des Hostsystems** Der empfohlene Speicher entsprechend der Bereitstellungsgröße ist in der folgenden Tabelle aufgeführt. Um Hochverfügbarkeit (HA) bereitzustellen, benötigen Sie die dreifache Appliance-Größe, die in der Tabelle angegeben ist.

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

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

Mindestanforderungen an Speicher und Anwendung

Speicher, Host und Anwendungen	Versionsanforderungen
ONTAP	9.14.1, 9.15.1, 9.16.0, 9.16.1 und 9.16.1P3 FAS, ASA A-Serie, ASA C-Serie, AFF A-Serie, AFF C-Serie und ASA r2.
Von ONTAP -Tools unterstützte ESXi-Hosts	Ab 7.0.3
ONTAP -Tools unterstützten vCenter Server	Ab 7.0U3
VASA-Anbieter	3,0
OVA-Anwendung	10,4
ESXi-Host zum Bereitstellen der virtuellen Maschine mit ONTAP -Tools	7.0U3 und 8.0U3
vCenter Server zum Bereitstellen der virtuellen Maschine mit ONTAP -Tools	7.0 und 8.0

Beginnend mit 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 neuesten Informationen zu den unterstützten Versionen von ONTAP, vCenter Server, ESXi-Hosts und Plug-in-Anwendungen.

"Interoperabilitätsmatrix-Tool"

Portanforderungen

Die folgende Tabelle zeigt die von NetApp verwendeten Netzwerkports und deren Zweck. Stellen Sie sicher, dass diese Ports offen und zugänglich sind, um einen ordnungsgemäßen Betrieb und die Kommunikation innerhalb des Systems zu gewährleisten. Stellen Sie sicher, dass die erforderlichen Netzwerkkonfigurationen

vorhanden sind, um den Datenverkehr über diese Ports zu ermöglichen, damit die zugehörigen Dienste ordnungsgemäß funktionieren. Abhängig von Ihren Sicherheitsrichtlinien müssen Sie möglicherweise Firewalls oder andere Sicherheitsanwendungen konfigurieren, um diesen Datenverkehr innerhalb Ihres Netzwerks zuzulassen.

Hafen	Protokoll	Beschreibung
8143	TCP	HTTP/HTTPS-Verbindungen für ONTAP -Tools.
8043	TCP	HTTP/HTTPS-Verbindungen für ONTAP -Tools.
9060	TCP	HTTP/HTTPS-Verbindungen für ONTAP -Tools.
22	TCP	Ansible verwendet diesen SSH-Port für die Kommunikation während der Clusterbereitstellung. Dieser Port wird für Funktionen wie das Ändern des Wartungsbenutzerkennworts, Statusmeldungen und zum Aktualisieren von Werten auf allen drei Knoten im Falle einer HA-Konfiguration benötigt.
443	TCP	Dies ist der Durchgangsport für die eingehende Kommunikation für den VASA-Provider-Dienst. Auf diesem Port werden das selbstsignierte Zertifikat des VASA-Anbieters und das benutzerdefinierte CA-Zertifikat gehostet.
8443	TCP	Dieser Port hostet die API-Dokumentation über Swagger und die Manager-Benutzeroberflächenanwendung.
2379	TCP	Dies ist der Standardport für Clientanforderungen wie „Get“, „Put“, „Delete“ oder „Watch“ für Schlüssel im etcd-Schlüsselwertspeicher.
2380	TCP	Dies ist der Standardport für die Server-zu-Server-Kommunikation für den etcd-Cluster, der für den Raft-Konsensalgorithmus verwendet wird, auf den etcd für die Datenreplikation und -konsistenz angewiesen ist.
7472	TCP/UDP	Dies ist der Prometheus Metrics Service-Port.

7946	TCP/UDP	Dieser Port wird für die Container-Netzwerkerkennung von Docker verwendet.
9083	TCP	Dieser Port ist ein intern verwendeter Service-Port für den VASA-Provider-Dienst.
1162	UDP	Dies ist der Port für SNMP-Trap-Pakete.
6443	TCP	Quelle: RKE2-Agentenknoten. Ziel: REK2-Serverknoten. Beschreibung: Kubernetes-API
9345	TCP	Quelle: RKE2-Agentenknoten. Ziel: REK2-Serverknoten. Beschreibung: REK2 Supervisor-API
8472	TCP+UDP	Alle Knoten müssen in der Lage sein, andere Knoten über den UDP-Port 8472 zu erreichen, wenn Flannel VXLAN verwendet wird. Quelle: alle RKE2-Knoten. Ziel: alle REK2-Knoten. Beschreibung: Canal CNI mit VXLAN
10250	TCP	Quelle: alle RKE2-Knoten. Ziel: alle REK2-Knoten. Beschreibung: Kubelet-Metriken
30000-32767	TCP	Quelle: alle RKE2-Knoten. Ziel: alle REK2-Knoten. Beschreibung: NodePort-Portbereich
123	TCP	Ntpd verwendet diesen Port, um die Validierung des NTP-Servers durchzuführen.
137-139	TCP/UDP	SMB/Windows-Freigabepakete.
6789	TCP	Ceph-Monitor (MON)
3300	TCP	Ceph-Monitor (MON)
6800-7300	TCP	Ceph-Manager, OSDs und Dateisystem (MDS).
80	TCP	Ceph RADOS Gateway (RGW)
9080	TCP	VP HTTP/HTTPS-Verbindungen (nur ab 127.0.0.0/8 für IPv4 oder ::1/128 für IPv6).

Konfigurationslimits für die Bereitstellung von ONTAP tools for VMware vSphere

Sie können die folgende Tabelle als Leitfaden zum Konfigurieren von ONTAP tools for VMware vSphere verwenden.

Einsatz	Typ	Anzahl der vVols	Anzahl der Hosts
Nicht-HA	Klein (S)	~12K	32
Nicht-HA	Mittel (M)	~24K	64
Hohe Verfügbarkeit	Klein (S)	~24K	64
Hohe Verfügbarkeit	Mittel (M)	~50k	128
Hohe Verfügbarkeit	Groß (L)	~100k	256 [HINWEIS] Die Anzahl der Hosts in der Tabelle zeigt die Gesamtzahl der Hosts aus mehreren vCentern.

ONTAP tools for VMware vSphere – Storage Replication Adapter (SRA)

Die folgende Tabelle zeigt die pro VMware Live Site Recovery-Instanz unterstützten Zahlen mit ONTAP tools for VMware vSphere.

vCenter-Bereitstellungsgröße	Klein	Medium
Gesamtzahl der virtuellen Maschinen, die für den Schutz mithilfe arraybasierter Replikation konfiguriert sind	2000	5000
Gesamtzahl der Array-basierten Replikationsschutzgruppen	250	250
Gesamtzahl der Schutzgruppen pro Wiederherstellungsplan	50	50
Anzahl replizierter Datenspeicher	255	255
Anzahl der VMs	4000	7000

Die folgende Tabelle zeigt die Anzahl von VMware Live Site Recovery und die entsprechenden ONTAP tools for VMware vSphere .

Anzahl der VMware Live Site Recovery-Instanzen	* Größe der ONTAP -Toolbereitstellung*
Bis zu 4	Klein
4 bis 8	Medium
Mehr als 8	Groß

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

Bevor Sie beginnen…

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

Anforderungen	Ihr Status
Die vSphere-Version, die ONTAP Version und die ESXi-Host-Version sind mit der ONTP-Tool-Version kompatibel.	□ Ja □ Nein
vCenter Server-Umgebung ist eingerichtet und konfiguriert	□ Ja □ Nein
Browser-Cache wird gelöscht	□ Ja □ Nein
Sie verfügen über die Anmeldeinformationen für den übergeordneten vCenter Server	□ Ja □ Nein
Sie verfügen über die Anmeldeinformationen für die vCenter Server-Instanz, mit der sich die ONTAP tools for VMware vSphere nach der Bereitstellung zur Registrierung verbinden.	□ Ja □ Nein
Der Domänenname, für den das Zertifikat ausgestellt wird, wird der virtuellen IP-Adresse in einer Multi-vCenter-Bereitstellung zugeordnet, in der benutzerdefinierte CA-Zertifikate obligatorisch sind.	□ Ja □ Nein
Sie haben die nslookup-Prüfung für den Domänennamen ausgeführt, um zu überprüfen, ob die Domäne in die gewünschte IP-Adresse aufgelöst wird.	□ Ja □ Nein
Das Zertifikat wird mit dem Domänennamen und der IP-Adresse der ONTAP Tools erstellt.	□ Ja □ Nein
Die Anwendung und die internen Dienste der ONTAP -Tools sind vom vCenter Server aus erreichbar.	□ Ja □ Nein
Wenn Sie Multi-Tenant-SVMs verwenden, verfügen Sie auf jedem SVM über ein SVM-Verwaltungs-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 zu sammeln:

Erfordernis	Ihr Wert
IP-Adresse für die ONTAP -Tools-Anwendung. Dies ist die IP-Adresse für den Zugriff auf die Weboberfläche der ONTAP -Tools	
Virtuelle IP-Adresse der ONTAP -Tools für die interne Kommunikation. Diese IP-Adresse wird für die interne Kommunikation in einem Setup mit mehreren ONTAP -Tools-Instanzen verwendet. Diese IP-Adresse darf nicht mit der IP-Adresse für die ONTAP -Tools -Anwendung identisch sein.	
DNS-Hostname für den ersten Knoten	

Erfordernis	Ihr Wert
Primärer DNS-Server	
Sekundärer DNS-Server	
DNS-Suchdomäne	
IPv4-Adresse für den ersten Knoten. Es handelt sich um eine eindeutige IPv4-Adresse für die Knotenverwaltungsschnittstelle im Verwaltungsnetzwerk.	
Subnetzmaske für die IPv4-Adresse	
Standard-Gateway für die IPv4-Adresse	
IPv6-Adresse (optional)	
IPv6-Präfixlänge (optional)	
Gateway für die IPv6-Adresse (optional)	

Erstellen Sie DNS-Einträge für alle oben genannten IP-Adressen. Ordnen Sie Hostnamen vor der Zuweisung den freien IP-Adressen im DNS zu. Alle IP-Adressen sollten sich im selben VLAN befinden, das für die Bereitstellung ausgewählt wurde.

Für die Bereitstellung mit hoher Verfügbarkeit (HA)

Zusätzlich zu den Anforderungen für die Bereitstellung eines einzelnen Knotens benötigen Sie für die HA-Bereitstellung die folgenden Informationen:

Erfordernis	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

Öffnen Sie die erforderlichen Ports für die IP-Adressen in Ihrer Netzwerk-Firewall. ONTAP -Tools müssen dieses LIF über Port 443 erreichen können. Siehe"Portanforderungen" für die neuesten Updates.

ONTAP -Speichereinstellungen

Um eine nahtlose Integration des ONTAP Speichers mit ONTAP tools for VMware vSphere sicherzustellen, sollten Sie die folgenden Einstellungen berücksichtigen:

- Wenn Sie Fibre Channel (FC) für die Speicherkonnektivität verwenden, konfigurieren Sie die Zoning auf

Ihren FC-Switches, um die ESXi-Hosts mit den FC-LIFs der SVM zu verbinden. "Erfahren Sie mehr über FC- und FCoE-Zoning mit ONTAP -Systemen"

- Um die von ONTAP -Tools verwaltete SnapMirror -Replikation zu verwenden, sollte der ONTAP Speicheradministrator "ONTAP Cluster-Peer-Beziehungen" Und "ONTAP Intercluster SVM Peer-Beziehungen" in ONTAP , bevor Sie SnapMirror verwenden.

Bereitstellen von ONTAP tools for VMware vSphere

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

Bevor Sie beginnen

Eine Inhaltsbibliothek in VMware ist ein Containerobjekt, das VM-Vorlagen, vApp-Vorlagen und andere Dateitypen speichert. Die Bereitstellung mit Inhaltsbibliothek bietet Ihnen ein nahtloses Erlebnis, da sie nicht von der Netzwerkkonnektivität abhängig ist.

Sie sollten die Inhaltsbibliothek auf einem gemeinsam genutzten Datenspeicher speichern, damit alle Hosts innerhalb eines Clusters darauf zugreifen können. Erstellen Sie eine Inhaltsbibliothek zum Speichern der OVA, bevor Sie das Gerät auf HA-Konfiguration konfigurieren. Löschen Sie die Inhaltsbibliotheksvorlage nach der Bereitstellung nicht.

Um die HA-Bereitstellung später zu aktivieren, stellen Sie die virtuelle Maschine, auf der die ONTAP Tools gehostet werden, nicht direkt auf einem ESXi-Host bereit. Stellen Sie es stattdessen auf einem Cluster oder Ressourcenpool bereit.

Wenn Sie keine Inhaltsbibliothek haben, führen Sie die folgenden Schritte aus, um eine zu erstellen:

Inhaltsbibliothek erstellen Wenn Sie nur eine kleine Bereitstellung mit einem einzelnen Knoten verwenden möchten, ist das Erstellen einer Inhaltsbibliothek nicht erforderlich.

1. Laden Sie die Datei mit den Binärdateien (*.ova*) und signierten Zertifikaten für ONTAP tools for VMware vSphere von der "NetApp Support Site" .
2. Melden Sie sich beim vSphere-Client an
3. Wählen Sie das vSphere-Clientmenü und wählen Sie **Inhaltsbibliotheken**.
4. Wählen Sie rechts auf der Seite **Erstellen** aus.
5. Geben Sie der Bibliothek einen Namen und erstellen Sie die Inhaltsbibliothek.
6. Navigieren Sie zu der von Ihnen erstellten Inhaltsbibliothek.
7. Wählen Sie rechts auf der Seite **Aktionen** und wählen Sie **Element importieren** und importieren Sie die OVA-Datei.

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

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

Die ONTAP tools for VMware vSphere werden zunächst als Nicht-HA-Setup bereitgestellt. Um auf die HA-

Bereitstellung zu skalieren, müssen Sie das CPU-Hot-Plug-in und das Memory-Hot-Plug-in aktivieren. Sie können diesen Schritt als Teil des Bereitstellungsprozesses ausführen oder die VM-Einstellungen nach der Bereitstellung bearbeiten.

Schritte

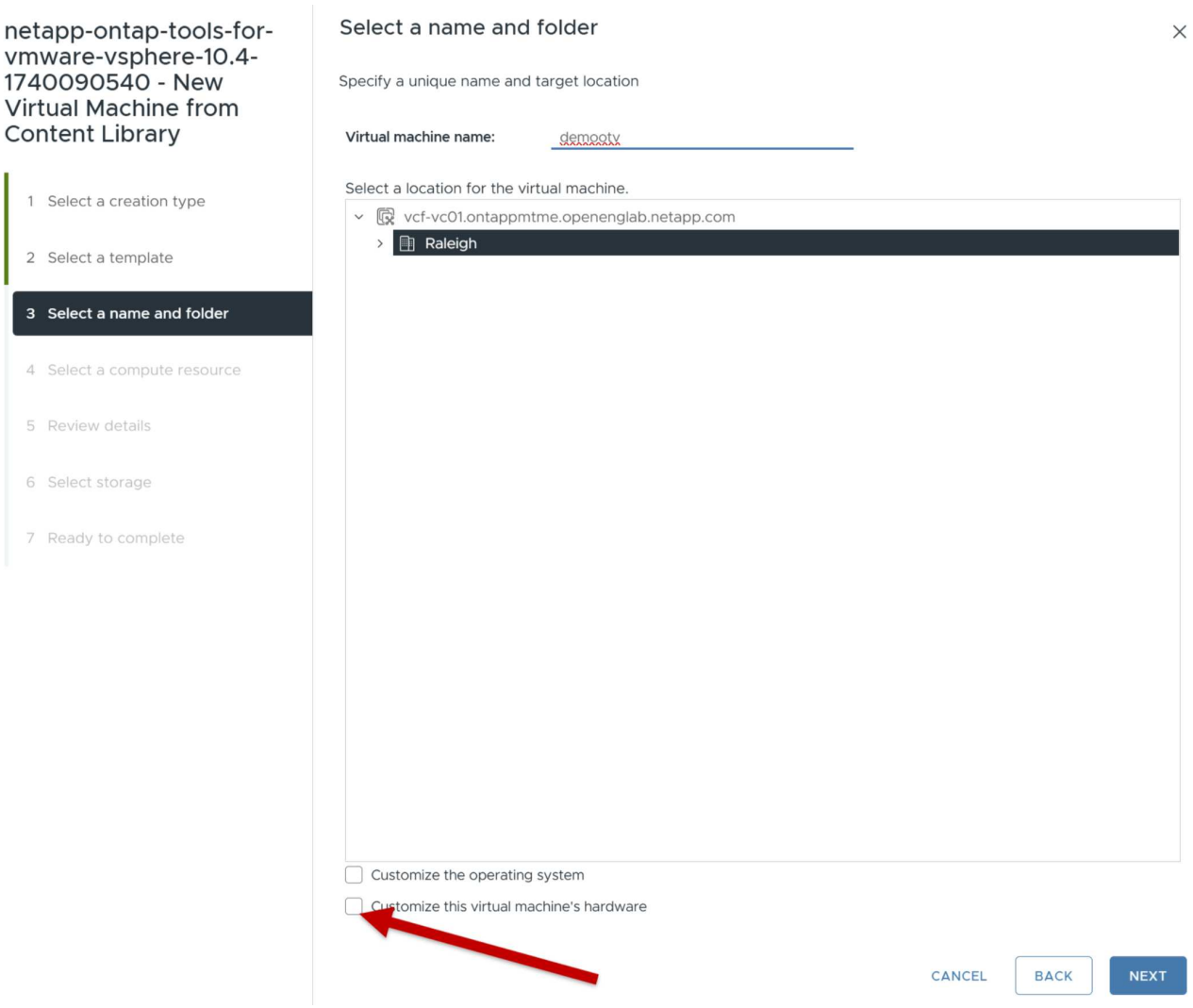
1. Laden Sie die Datei herunter, die die Binärdateien (*.ova*) und signierten Zertifikate für die ONTAP tools for VMware vSphere enthält "NetApp Support Site". Wenn Sie die OVA in die Inhaltsbibliothek importiert haben, können Sie diesen Schritt überspringen und mit dem nächsten Schritt fortfahren
2.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

   Speichern Sie ONTAP tools for VMware vSphere Maschinen niemals auf den von ihnen verwalteten vVols -Datenspeichern.

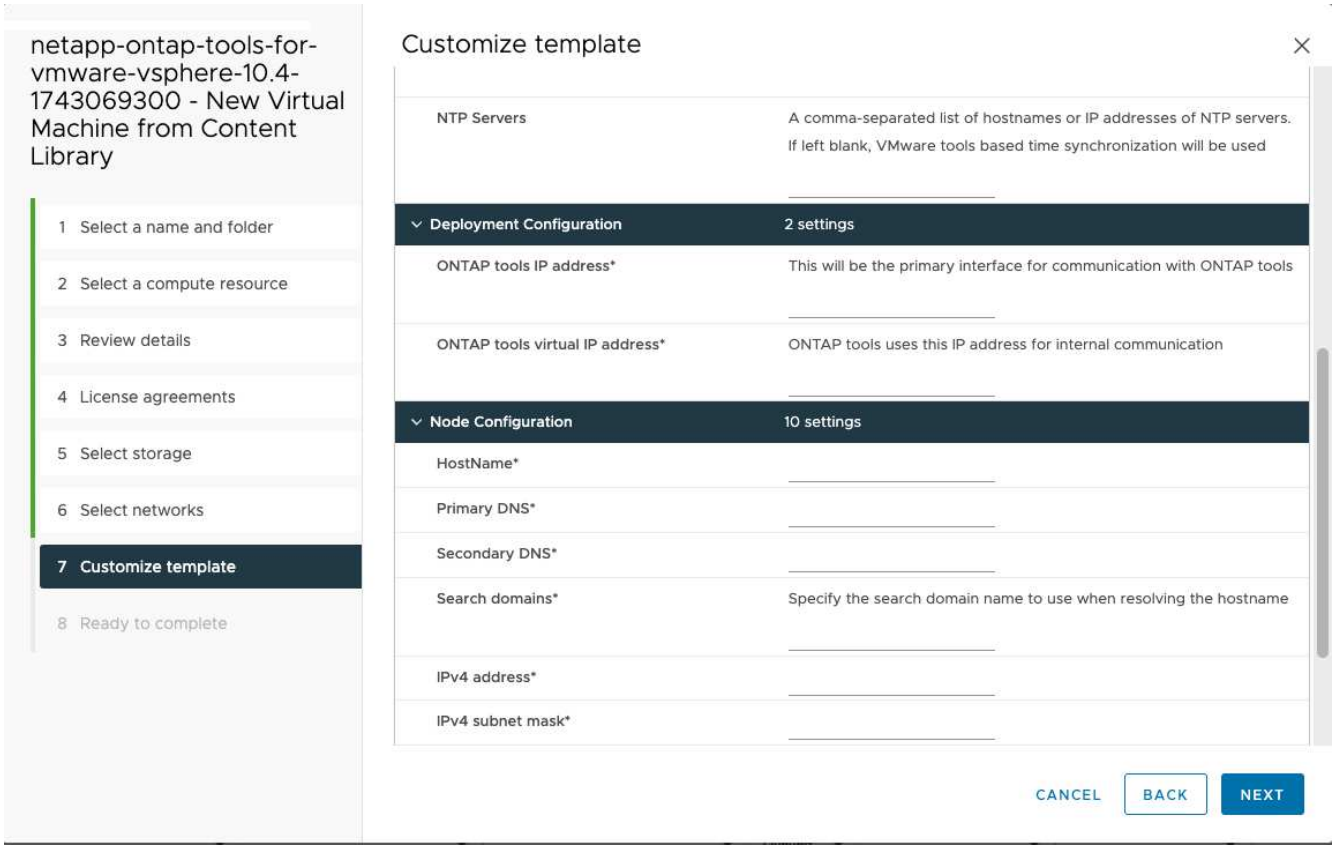
4. Sie können die OVA aus der Inhaltsbibliothek oder vom lokalen System bereitstellen.

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

5. Geben Sie im Feld **Namen und Ordner auswählen** den Namen der virtuellen Maschine ein und wählen Sie ihren Speicherort aus.
   - Wenn Sie die Version 8.0.3 von vCenter Server verwenden, wählen Sie die Option **Hardware dieser virtuellen Maschine anpassen**. Dadurch wird ein zusätzlicher Schritt namens **Hardware anpassen** aktiviert, bevor Sie mit dem Fenster **Bereit zum Abschließen** fortfahren.
   - Wenn Sie die Version 7.0.3 von vCenter Server verwenden, befolgen Sie die Schritte im Abschnitt **Was kommt als Nächstes?** am Ende der Bereitstellung.



6. Wählen Sie eine Computerressource aus und klicken Sie auf **Weiter**. Aktivieren Sie optional das Kontrollkästchen „Bereitgestellte VM automatisch einschalten“.
7. Überprüfen Sie die Details der Vorlage und wählen Sie **Weiter**.
8. Lesen und akzeptieren Sie die Lizenzvereinbarung und wählen Sie **Weiter**.
9. Wählen Sie den Speicher für die Konfiguration und das Datenträgerformat aus und wählen Sie **Weiter**.
10. Wählen Sie für jedes Quellnetzwerk das Zielnetzwerk aus und wählen Sie **Weiter**.
11. Füllen Sie im Fenster **Vorlage anpassen** die erforderlichen Felder aus und wählen Sie **Weiter**
.

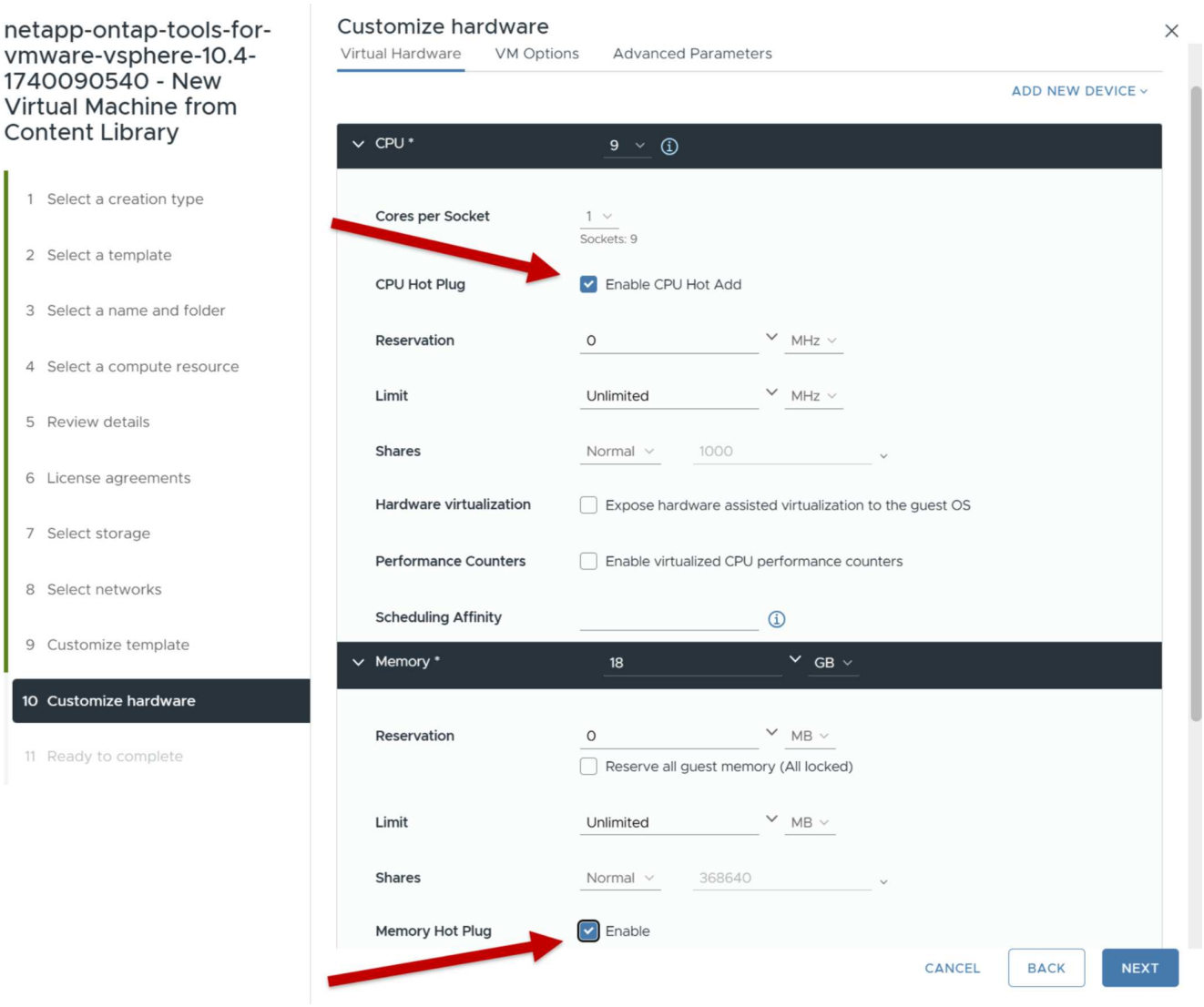


- Die Informationen werden während der Installation validiert. Bei Abweichungen erscheint eine Fehlermeldung auf der Webkonsole und Sie werden aufgefordert, diese zu korrigieren.
- Hostnamen müssen Buchstaben (AZ, az), Ziffern (0-9) und Bindestriche (-) enthalten. Um Dual Stack zu konfigurieren, geben Sie den Hostnamen an, der der IPv6-Adresse zugeordnet ist.

> Reines IPv6 wird nicht unterstützt. Der gemischte Modus wird mit VLAN unterstützt, das 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 verwendet werden kann, um zu Debugging- und Wartungszwecken den Diagnose-Shell- und SSH-Zugriff auf den Knoten zu ermöglichen.

12. Wenn Sie die Version 8.0.3 von vCenter Server verwenden, aktivieren Sie im Fenster **Hardware anpassen** die Optionen **CPU Hot Add** und **Memory Hot Plug**, um die HA-Funktionalität zu ermöglichen.



13. Überprüfen Sie die Details im Fenster **Bereit zum Abschließen** und wählen Sie **Fertig**.

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

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

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

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

Wie geht es weiter?

Wenn Sie über ONTAP tools for VMware vSphere mit vCenter Server 7.0.3 verfügen, führen Sie nach der Bereitstellung die folgenden Schritte aus.

1. Melden Sie sich beim vCenter-Client an
2. Fahren Sie den ONTAP Tools-Knoten herunter.

3. Navigieren Sie zu den ONTAP tools for VMware vSphere Maschine unter **Inventar** und wählen Sie die Option **Einstellungen bearbeiten**.
4. Aktivieren Sie unter den **CPU**-Optionen das Kontrollkästchen **CPU-Hot-Add aktivieren**
5. Aktivieren Sie unter den **Speicher**-Optionen das Kontrollkästchen **Aktivieren** neben **Speicher-Hotplug**.

Bereitstellungsfehlercodes

Bei der Bereitstellung, dem Neustart und der Wiederherstellung von ONTAP tools for VMware vSphere können Fehlercodes auftreten. Die Fehlercodes bestehen aus fünf Ziffern, wobei die ersten beiden Ziffern das Skript darstellen, bei dem das Problem aufgetreten ist, und die letzten drei Ziffern den spezifischen Arbeitsablauf innerhalb dieses Skripts darstellen.

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

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

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

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

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

Bereitstellungsfehlercode	Arbeitsablauf	Auflösung
049	Für Netzwerk und Validierung wird das Perl-Skript sie in Kürze ebenfalls zuweisen.	-
050	SSH-Schlüsselgenerierung fehlgeschlagen	Starten Sie die primäre virtuelle Maschine (VM) neu.

053	Fehler bei der Installation von RKE2	Führen Sie entweder Folgendes aus und starten Sie die primäre VM neu oder führen Sie eine erneute Bereitstellung durch: sudo rke2-killall.sh (alle VMs) sudo rke2-uninstall.sh (alle VMs).
054	Fehler beim Festlegen von „kubeconfig“	Erneut bereitstellen
055	Fehler beim Bereitstellen der Registrierung	Wenn der Registrierungs-Pod vorhanden ist, warten Sie, bis der Pod bereit ist, und starten Sie dann die primäre VM neu oder führen Sie eine erneute Bereitstellung durch.
059	Die KubeVip-Bereitstellung ist fehlgeschlagen	Stellen Sie sicher, dass die während der Bereitstellung bereitgestellte virtuelle IP-Adresse für die Kubernetes-Steuerebene und die IP-Adresse der ONTAP -Tools zum selben VLAN gehört und freie IP-Adressen sind. Starten Sie neu, wenn alle vorherigen Punkte korrekt sind. Andernfalls erneut bereitstellen.
060	Die Bereitstellung des Operators ist fehlgeschlagen	Neustart
061	Die Bereitstellung der Dienste ist fehlgeschlagen	Führen Sie grundlegende Kubernetes-Debugging-Vorgänge wie „Get Pods“, „Get RS“, „Get SVC“ usw. im NTV-System-Namespace durch, um weitere Details und Fehlerprotokolle unter /var/log/ansible-perl-errors.log und /var/log/ansible-run.log zu erhalten, und führen Sie die Bereitstellung erneut durch.
062	Die Bereitstellung der ONTAP -Tools-Dienste ist fehlgeschlagen	Weitere Einzelheiten und eine erneute Bereitstellung finden Sie in den Fehlerprotokollen unter /var/log/ansible-perl-errors.log.
065	Die URL der Swagger-Seite ist nicht erreichbar	Erneut bereitstellen

066	Die Schritte nach der Bereitstellung für das Gateway-Zertifikat sind fehlgeschlagen	Gehen Sie wie folgt vor, um das Upgrade wiederherzustellen/abzuschließen: * Aktivieren Sie die Diagnose-Shell. * Führen Sie den Befehl „sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postDeploy“ aus. * Überprüfen Sie die Protokolle unter /var/log/post-deploy-upgrade.log.
088	Das Konfigurieren der Protokollrotation für Journald ist fehlgeschlagen	Überprüfen Sie die VM-Netzwerkeinstellungen, die mit dem Host kompatibel sind, auf dem die VM gehostet wird. Sie können versuchen, auf einen anderen Host zu migrieren und die VM neu zu starten.
089	Das Ändern des Eigentümers der Rotationskonfigurationsdatei des Zusammenfassungsprotokolls ist fehlgeschlagen	Starten Sie die primäre VM neu.
096	Installieren Sie den Dynamic Storage Provisioner	-
108	Seeding-Skript fehlgeschlagen	-

Fehlercode beim Neustart	**Arbeitsablauf**	**Auflösung**
067	Beim Warten auf den RKE2-Server ist eine Zeitüberschreitung aufgetreten.	-
101	Das Zurücksetzen des Wartungs-/Konsolenbenutzerkennworts ist fehlgeschlagen.	-
102	Beim Zurücksetzen des Wartungs-/Konsolenbenutzerkennworts konnte die Kennwortdatei nicht gelöscht werden.	-
103	Das neue Wartungs-/Konsolenbenutzerkennwort konnte im Tresor nicht aktualisiert werden.	-
088	Die Konfiguration der Protokollrotation für Journald ist fehlgeschlagen.	Überprüfen Sie die VM-Netzwerkeinstellungen, die mit dem Host kompatibel sind, auf dem die VM gehostet wird. Sie können versuchen, auf einen anderen Host zu migrieren und die VM neu zu starten.

089	Das Ändern des Eigentümers der Rotationskonfigurationsdatei des Zusammenfassungsprotokolls ist fehlgeschlagen.	Starten Sie die VM neu.

Konfigurieren Sie ONTAP tools for VMware vSphere

vCenter Server-Instanzen hinzufügen

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. Wenn Sie mehrere vCenter Server-Instanzen hinzufügen, sind für die sichere Kommunikation zwischen ONTAP Tools und jedem vCenter Server benutzerdefinierte CA-Zertifikate erforderlich.

Über diese Aufgabe

Durch die Integration mit vCenter können Sie mit ONTAP -Tools Speicheraufgaben wie Bereitstellung, Snapshots und Datenschutz direkt vom vSphere-Client aus durchführen, sodass Sie nicht mehr auf separate Speicherverwaltungskonsolen umsteigen müssen.

Schritte

1. Öffnen Sie einen Webbrowser und navigieren Sie zur URL: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **vCenters** > **Hinzufügen**, um die vCenter Server-Instanzen zu integrieren. Geben Sie Ihre vCenter-IP-Adresse oder Ihren Hostnamen, Ihren Benutzernamen, Ihr Kennwort und Ihre Portdetails an.

> Sie benötigen kein Administratorkonto, um vCenter-Instanzen zu ONTAP -Tools hinzuzufügen. Sie können eine benutzerdefinierte Rolle ohne Administratorkonto mit eingeschränkten Berechtigungen erstellen. Siehe"Verwenden Sie vCenter Server RBAC mit ONTAP tools for VMware vSphere 10" für Details.

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

- Das vCenter-Client-Plug-In ist als Remote-Plug-In registriert.
- Benutzerdefinierte Berechtigungen für die Plug-Ins und APIs werden auf die vCenter Server-Instanz angewendet.
- Zur Verwaltung der Benutzer werden benutzerdefinierte Rollen erstellt.
- Das Plug-In wird als Verknüpfung auf der vSphere-Benutzeroberfläche angezeigt.

Registrieren Sie den VASA-Anbieter bei einer vCenter Server-Instanz

Sie können den VASA-Anbieter mithilfe von ONTAP tools for VMware vSphere bei einer vCenter Server-Instanz registrieren. Im Abschnitt „VASA-Provider-Einstellungen“ wird der Registrierungsstatus des VASA-Providers für den ausgewählten vCenter Server angezeigt. Stellen Sie bei einer Bereitstellung mit mehreren vCentern sicher, dass Sie für

jede vCenter Server-Instanz über benutzerdefinierte CA-Zertifikate verfügen.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie im Abschnitt „Plug-ins“ **Verknüpfungen** > * NetApp ONTAP Tools*.
3. Wählen Sie **Einstellungen** > **VASA-Anbietereinstellungen**. Der Registrierungsstatus des VASA-Anbieters wird als „Nicht registriert“ angezeigt.
4. Wählen Sie die Schaltfläche **Registrieren**, um den VASA-Anbieter zu registrieren.
5. Geben Sie einen Namen und Anmeldeinformationen für den VASA-Anbieter ein. Der Benutzername darf nur Buchstaben, Zahlen und Unterstriche enthalten. Die Passwortlänge sollte zwischen 8 und 256 Zeichen liegen.
6. Wählen Sie **Registrieren**.
7. Nach einer erfolgreichen Registrierung und Seitenaktualisierung werden Status, Name und Version des registrierten VASA-Anbieters angezeigt. Nach der Registrierung wird die Aktion „Abmelden“ aktiviert.

Was kommt als nächstes

Überprüfen Sie, ob der integrierte VASA-Anbieter unter „VASA-Anbieter“ im vCenter-Client aufgeführt ist:

Schritte

1. Navigieren Sie zur vCenter Server-Instanz.
2. Melden Sie sich mit den Administratoranmeldeinformationen an.
3. Wählen Sie **Speicheranbieter** > **Konfigurieren**. Überprüfen Sie, ob der integrierte VASA-Anbieter korrekt aufgeführt ist.

Installieren Sie das NFS VAAI-Plug-In

Das Plug-In NFS vStorage API for Array Integration (NFS VAAI) ist eine Softwarekomponente, die VMware vSphere und NFS-Speicher-Arrays integriert. Installieren Sie das NFS VAAI-Plug-in mithilfe von ONTAP tools for VMware vSphere , um die erweiterten Funktionen Ihres NFS-Speicherarrays zu nutzen und bestimmte speicherbezogene Vorgänge von den ESXi-Hosts auf das Speicherarray selbst auszulagern.

Bevor Sie beginnen

- Laden Sie die "NetApp NFS Plug-in für VMware VAAI" Installationspaket.
- Stellen Sie sicher, dass Sie über den ESXi-Host und den neuesten Patch für vSphere 7.0U3 oder spätere Versionen sowie ONTAP 9.14.1 oder spätere Versionen verfügen.
- Mounten Sie einen NFS-Datenspeicher.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie im Abschnitt „Plug-ins“ **Verknüpfungen** > * NetApp ONTAP Tools*.
3. Wählen Sie **Einstellungen** > **NFS VAAI Tools**.
4. Wenn das VAAI-Plug-In auf vCenter Server hochgeladen ist, wählen Sie im Abschnitt **Vorhandene Version Ändern** aus. Wenn kein VAAI-Plug-In auf den vCenter Server hochgeladen wird, wählen Sie die

Schaltfläche **Hochladen**.

5. Durchsuchen und wählen Sie die `.vib` Datei und wählen Sie **Hochladen**, um die Datei in die 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**.

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

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

   Wenn der VMware-Administrator den ESXi-Host neu startet, erkennen und aktivieren die ONTAP tools for VMware vSphere das NFS-VAAI-Plug-In automatisch.

Wie geht es weiter?

Nachdem Sie das NFS-VAAI-Plug-In installiert und Ihren ESXi-Host neu gestartet haben, müssen Sie die richtigen NFS-Exportrichtlinien für die VAAI-Kopierauslagerung konfigurieren. Wenn Sie VAAI in einer NFS-Umgebung konfigurieren, konfigurieren Sie die Exportrichtlinienregeln unter Berücksichtigung der folgenden Anforderungen:

- Das entsprechende ONTAP Volume muss NFSv4-Aufrufe zulassen.
- Der Root-Benutzer sollte Root bleiben und NFSv4 sollte in allen übergeordneten Junction-Volumes zulässig sein.
- Die Option für die VAAI-Unterstützung muss auf dem entsprechenden NFS-Server eingestellt werden.

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

Ähnliche Informationen

"Unterstützung für VMware vStorage über NFS"

"Aktivieren oder Deaktivieren von NFSv4.0"

"ONTAP -Unterstützung für NFSv4.2"

Konfigurieren der ESXi-Hosteinstellungen

Durch die Konfiguration der Multipfad- und Timeout-Einstellungen des ESXi-Servers wird eine hohe Verfügbarkeit und Datenintegrität gewährleistet, indem bei einem Ausfall eines primären Pfads nahtlos auf einen Sicherungsspeicherpfad umgeschaltet werden kann.

Konfigurieren der Multipath- und Timeout-Einstellungen des ESXi-Servers

ONTAP tools for VMware vSphere prüfen und legen die Multipath-Einstellungen des ESXi-Hosts und die HBA-Timeout-Einstellungen fest, die am besten mit NetApp -Speichersystemen funktionieren.

Über diese Aufgabe

Abhängig von Ihrer Konfiguration und Systemauslastung kann dieser Vorgang lange dauern. Der Aufgabenfortschritt wird im Bereich „Letzte Aufgaben“ angezeigt.

Schritte

1. Wählen Sie auf der Homepage des VMware vSphere-Webclients **Hosts und Cluster** aus.
2. Klicken Sie mit der rechten Maustaste auf einen Host und wählen Sie * NetApp ONTAP -Tools* > **Hostdaten aktualisieren**.
3. Wählen Sie auf der Verknüpfungsseite des VMware vSphere-Webclients im Abschnitt „Plug-ins“ die Option „NetApp ONTAP -Tools“ aus.
4. Gehen Sie in der Übersicht (Dashboard) der ONTAP tools for VMware vSphere Plug-In zur Karte **ESXi-Host-Compliance**.
5. Wählen Sie den Link **Empfohlene Einstellungen anwenden**.
6. Wählen Sie im Fenster **Empfohlene Hosteinstellungen anwenden** die Hosts aus, die Sie aktualisieren möchten, um den empfohlenen NetApp -Einstellungen zu entsprechen, und wählen Sie **Weiter**.

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

7. Wählen Sie auf der Einstellungsseite nach Bedarf die empfohlenen Werte aus.
8. Überprüfen Sie im Übersichtsbereich die Werte und wählen Sie **Fertig**. Sie können den Fortschritt im Bereich „Letzte Aufgaben“ verfolgen.

Festlegen von ESXi-Hostwerten

Mithilfe von ONTAP tools for VMware vSphere können Sie Timeouts und andere Werte auf den ESXi-Hosts festlegen, um die beste Leistung und ein erfolgreiches Failover sicherzustellen. Die von den ONTAP tools for VMware vSphere festgelegten Werte basieren auf internen NetApp Tests.

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

HBA/CNA-Adaptereinstellungen

Setzt die folgenden Parameter auf Standardwerte:

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

MPIO-Einstellungen

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

In Hochleistungsumgebungen oder beim Testen der Leistung mit einem einzelnen LUN-Datenspeicher sollten Sie die Lastausgleichseinstellung der Round-Robin-Pfadauswahlrichtlinie (VMW_PSP_RR) von der IOPS-Standardeinstellung von 1000 auf den Wert 1 ändern.

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

NFS-Einstellungen

Parameter	Setzen Sie diesen Wert auf …
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

Sie können neue Benutzerrollen und Berechtigungen für die Verwaltung von Speicher-Backends mithilfe der JSON-Datei konfigurieren, die mit den ONTAP tools for VMware vSphere und ONTAP System Manager bereitgestellt wird.

Bevor Sie beginnen

- Sie sollten die ONTAP -Berechtigungsdatei von den ONTAP tools for VMware vSphere mit *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip* heruntergeladen haben.
- Sie sollten die ONTAP Privileges Datei von ONTAP Tools heruntergeladen haben mit `https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip`.

> Sie können Benutzer auf Cluster- oder direkt auf der Ebene der virtuellen Speichermaschinen (SVMs) erstellen. Sie können Benutzer auch ohne Verwendung der Datei user_roles.json erstellen. In diesem Fall benötigen Sie einen Mindestsatz an Berechtigungen auf SVM-Ebene.

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

Schritte

1. Extrahieren Sie die heruntergeladene Datei *https://<ONTAPtoolsIP>:8443/virtualization/user-privileges/users_roles.zip*.
2. Greifen Sie über die Clusterverwaltungs-IP-Adresse des Clusters auf den ONTAP System Manager zu.
3. Melden Sie sich mit Administratorrechten beim Cluster an. Um einen Benutzer zu konfigurieren, führen Sie die folgenden Schritte aus:
   a. Um den Cluster ONTAP -Tools-Benutzer zu konfigurieren, wählen Sie den Bereich **Cluster** > **Einstellungen** > **Benutzer und Rollen**.
   b. Um den SVM ONTAP Tools-Benutzer zu konfigurieren, wählen Sie den Bereich **Storage SVM** > **Einstellungen** > **Benutzer und Rollen**.
   c. Wählen Sie unter „Benutzer“ die Option „Hinzufügen“ aus.

d. Wählen Sie im Dialogfeld **Benutzer hinzufügen** die Option **Virtualisierungsprodukte** aus.

e. **Durchsuchen**, um die JSON-Datei mit den ONTAP Privileges auszuwählen und hochzuladen.

   Das Produktfeld wird automatisch ausgefüllt.

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

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

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

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

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

Anforderungen für die SVM-Aggregatzuordnung

Um SVM-Benutzeranmeldeinformationen für die Bereitstellung von Datenspeichern zu verwenden, erstellen ONTAP tools for VMware vSphere intern Volumes auf dem in der POST-API der Datenspeicher angegebenen Aggregat. ONTAP erlaubt nicht die Erstellung von Volumes auf nicht zugeordneten Aggregaten auf einer SVM unter Verwendung von SVM-Benutzeranmeldeinformationen. Um dies zu beheben, müssen Sie die SVMs mithilfe der ONTAP REST API oder CLI wie hier beschrieben den Aggregaten zuordnen.

REST-API:

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

ONTAP CLI:

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

ONTAP Benutzer und -Rolle manuell erstellen

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

1. Greifen Sie über die Clusterverwaltungs-IP-Adresse des Clusters auf den ONTAP System Manager zu.
2. Melden Sie sich mit Administratorrechten beim Cluster an.
   a. Um die Rollen der Cluster ONTAP Tools zu konfigurieren, wählen Sie den Bereich **Cluster** > **Einstellungen** > **Benutzer und Rollen**.
   b. Um die Rollen der Cluster-SVM ONTAP -Tools zu konfigurieren, wählen Sie **Storage SVM** > **Einstellungen** > **Benutzer und Rollen**

3. Rollen erstellen:
   a. Wählen Sie unter der Tabelle **Rollen Hinzufügen** aus.
   b. Geben Sie den **Rollennamen** und die **Rollenattribute** ein.

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

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

Liste der erforderlichen Mindestberechtigungen für Clusterbenutzer mit globalem Geltungsbereich ohne Administratorrechte

In diesem Abschnitt sind die Mindestberechtigungen für Clusterbenutzer mit globalem Gültigkeitsbereich ohne Administratorrechte aufgeführt, die ohne Verwendung der JSON-Datei erstellt wurden. Wenn ein Cluster im lokalen Gültigkeitsbereich hinzugefügt wird, wird empfohlen, die JSON-Datei zum Erstellen der Benutzer zu verwenden, da ONTAP tools for VMware vSphere für die Bereitstellung auf ONTAP mehr als nur Leseberechtigungen erfordern.

Verwenden von APIs:

API	Zugriffsebene	Verwendet für
/api/cluster	Schreibgeschützt	Cluster-Konfigurationserkennung
/api/cluster/licensing/licenses	Schreibgeschützt	Lizenzprüfung für protokollspezifische Lizenzen
/api/cluster/nodes	Schreibgeschützt	Plattformtyperkennung
/api/security/accounts	Schreibgeschützt	Berechtigungsermittlung
/api/sicherheit/rollen	Schreibgeschützt	Berechtigungsermittlung
/api/storage/aggregates	Schreibgeschützt	Überprüfung des Gesamtspeicherplatzes während der Bereitstellung von Datenspeichern/Volumes
/api/storage/cluster	Schreibgeschützt	So erhalten Sie Platz- und Effizienzdaten auf Clusterebene
/API/Speicher/Festplatten	Schreibgeschützt	So erhalten Sie die in einem Aggregat verknüpften Datenträger
/api/storage/qos/policies	Lesen/Erstellen/Ändern	QoS- und VM-Richtlinienverwaltung

/api/svm/svms	Schreibgeschützt	Um die SVM-Konfiguration zu erhalten, falls der Cluster lokal hinzugefügt wird.
/api/netzwerk/ip/schnittstellen	Schreibgeschützt	Speicher-Backend hinzufügen – Um zu identifizieren, dass der Verwaltungs-LIF-Bereich Cluster/SVM ist
/api/storage/availability-zones	Schreibgeschützt	SAZ-Entdeckung. Gilt für ONTAP Versionen ab 9.16.1 und ASA r2-Systeme.

Erstellen Sie ONTAP tools for VMware vSphere ONTAP API-basierte Cluster-Benutzer

Sie benötigen Privileges zum Erkennen, Erstellen, Ändern und Löschen, um PATCH-Vorgänge und automatische Rollbacks im Falle eines Fehlers in den Datenspeichern durchzuführen. Das Fehlen all dieser Berechtigungen führt zu Arbeitsablaufstörungen und Bereinigungsproblemen.

Durch das Erstellen von ONTAP tools for VMware vSphere ONTAP API-basierte Benutzer mit den Berechtigungen „Erkennung“, „Speicher erstellen“, „Speicher ändern“ und „Speicher löschen“ können Erkennungen initiiert und ONTAP Tool-Workflows verwaltet werden.

Um einen Cluster-Benutzer mit allen oben genannten Berechtigungen zu erstellen, führen Sie die folgenden Befehle aus:

```
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
```

Führen Sie für ONTAP Versionen ab 9.16.0 zusätzlich den folgenden Befehl aus:

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

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

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

Erstellen Sie ONTAP tools for VMware vSphere ONTAP API-basierte SVM-Benutzer

Um einen SVM-Benutzer mit allen Berechtigungen zu erstellen, führen Sie die folgenden Befehle aus:

```
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 ab 9.16.0 zusätzlich den folgenden Befehl aus:

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

Um einen neuen API-basierten Benutzer mit den oben erstellten API-basierten Rollen zu erstellen, führen Sie den folgenden Befehl aus:

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

Beispiel:

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

Um das Konto zu entsperren und den Zugriff auf die Verwaltungsschnittstelle zu ermöglichen, führen Sie den folgenden Befehl aus:

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

Beispiel:

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

Upgrade der ONTAP tools for VMware vSphere 10.1-Benutzer auf 10.3-Benutzer

Verwenden Sie für Benutzer von ONTAP tools for VMware vSphere 10.1 mit einem clusterbezogenen Benutzer, der mithilfe der JSON-Datei erstellt wurde, die folgenden ONTAP CLI-Befehle mit Benutzeradministratorrechten, um ein Upgrade auf die Version 10.3 durchzuführen.

Für Produktfunktionen:

- VSC
- VSC- und VASA-Anbieter
- VSC und SRA
- VSC, VASA-Anbieter und SRA.

Cluster-Berechtigungen:

security login role create -role <vorhandener Rollenname> -cmddirname "vserver nvme namespace show" -access all

security login role create -role <vorhandener Rollenname> -cmddirname "vserver nvme subsystem show" -access all

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

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

security login role create -role <vorhandener Rollenname> -cmddirname "vserver nvme show-interface" -access read

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

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

security login role create -role <vorhandener Rollenname> -cmddirname "vserver nvme namespace delete" -access all

security login role create -role <vorhandener Rollenname> -cmddirname "vserver nvme subsystem delete" -access all

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

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

Verwenden Sie für ONTAP tools for VMware vSphere 10.1-Benutzer mit einem SVM-Bereichsbenutzer, der mithilfe der JSON-Datei erstellt wurde, die ONTAP CLI-Befehle mit Administratorrechten, um ein Upgrade auf die Version 10.3 durchzuführen.

SVM-Berechtigungen:

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

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

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

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

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

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

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

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

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

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

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

Durch Hinzufügen der Befehle *vserver nvme namespace show* und *vserver nvme subsystem show* zur vorhandenen Rolle werden die folgenden Befehle hinzugefügt.

```
vserver nvme namespace create

vserver nvme namespace modify

vserver nvme subsystem create

vserver nvme subsystem modify
```

Upgrade der ONTAP tools for VMware vSphere 10.3-Benutzer auf 10.4-Benutzer

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

Verwenden Sie für ONTAP tools for VMware vSphere 10.3-Benutzer mit einem Cluster-Benutzer, der mithilfe der JSON-Datei und ONTAP Version 9.16.1 oder höher erstellt wurde, den ONTAP CLI-Befehl mit Administratorrechten, um ein Upgrade auf die Version 10.4 durchzuführen.

Für Produktfunktionen:

- VSC
- VSC- und VASA-Anbieter
- VSC und SRA
- VSC, VASA-Anbieter und SRA.

Cluster-Berechtigungen:

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

Hinzufügen eines Speicher-Backends

Durch Hinzufügen eines Speicher-Backends können Sie einen ONTAP Cluster integrieren.

Über diese Aufgabe

Verwenden Sie bei Multitenancy-Setups, bei denen vCenter als Mandant mit einem zugehörigen SVM fungiert, den ONTAP Tools Manager, um den Cluster hinzuzufügen. Verknüpfen Sie das Speicher-Backend mit dem vCenter Server, um es global der integrierten vCenter Server-Instanz zuzuordnen. Der vCenter-Mandant muss die gewünschten Storage Virtual Machines (SVMs) an Bord nehmen. Dies ermöglicht einem SVM-Benutzer die Bereitstellung von vVols Datenspeichern. Sie können mithilfe der SVM Speicher in vCenter hinzufügen.

Fügen Sie die lokalen Speicher-Backends mit Cluster- oder SVM-Anmeldeinformationen über die Benutzeroberfläche der ONTAP Tools hinzu. Diese Speicher-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 ONTAP -Tools SVM-Anmeldeinformationen, ohne dass ein globaler Cluster erforderlich ist.

Verwenden des ONTAP Tools Managers

In einer Multi-Tenant-Konfiguration können Sie global einen Storage-Backend-Cluster und lokal SVM hinzufügen, um SVM-Benutzeranmeldeinformationen zu verwenden.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **Storage Backends** aus der Seitenleiste.
4. Fügen Sie das Speicher-Backend hinzu und geben Sie die Server-IP-Adresse oder den FQDN, den Benutzernamen und das Kennwort an.

   LIFs zur Adressverwaltung von IPv4 und IPv6 werden unterstützt.

Verwenden der vSphere-Client-Benutzeroberfläche

Beim Konfigurieren eines Speicher-Backends über die Benutzeroberfläche des vSphere-Clients ist zu beachten, dass die vVols Datenspeicher das direkte Hinzufügen eines SVM-Benutzers nicht unterstützen.

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie auf der Verknüpfungsseite im Abschnitt „Plug-ins“ die Option „NetApp ONTAP Tools“ aus.
3. Wählen Sie **Storage Backends** aus der Seitenleiste.
4. Fügen Sie das Speicher-Backend hinzu und geben Sie die Server-IP-Adresse, den Benutzernamen, das Kennwort und die Portdetails an.

   Um einen SVM-Benutzer direkt hinzuzufügen, können Sie clusterbasierte Anmeldeinformationen und LIFs zur IPv4- und IPv6-Adressverwaltung hinzufügen oder SVM-basierte Anmeldeinformationen mit einem SVM-Verwaltungs-LIF bereitstellen.

Wie geht es weiter?

Die Liste wird aktualisiert und Sie können das neu hinzugefügte Speicher-Backend in der Liste sehen.

Zuordnen eines Speicher-Backends zu einer vCenter Server-Instanz

Ordnen Sie dem vCenter Server ein Speicher-Backend zu, um eine globale Zuordnung zwischen dem Speicher-Backend und der integrierten vCenter Server-Instanz zu erstellen.

Schritte

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

2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie vCenter in der Seitenleiste aus.
4. Wählen Sie die vertikalen Auslassungspunkte neben der vCenter Server-Instanz aus, die Sie mit den Speicher-Backends verknüpfen möchten.
5. Wählen Sie das Speicher-Backend aus der Dropdown-Liste aus, um die vCenter Server-Instanz mit dem erforderlichen Speicher-Backend zu verknüpfen.

Konfigurieren des Netzwerkzugriffs

Wenn Sie den Netzwerkzugriff nicht konfiguriert haben, werden alle erkannten IP-Adressen des ESXi-Hosts standardmäßig zur Exportrichtlinie hinzugefügt. Sie können es so konfigurieren, dass der Exportrichtlinie einige bestimmte IP-Adressen hinzugefügt und der Rest ausgeschlossen wird. Wenn Sie jedoch einen Mountvorgang auf den ausgeschlossenen ESXi-Hosts durchführen, schlägt der Vorgang fehl.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie auf der Verknüpfungsseite im Abschnitt „Plug-Ins“ * NetApp ONTAP -Tools* aus.
3. Navigieren Sie im linken Bereich der ONTAP -Tools zu **Einstellungen** > **Netzwerkzugriff verwalten** > **Bearbeiten**.

   Um mehrere IP-Adressen hinzuzufügen, trennen Sie die Liste durch Kommas, Bereiche, Classless Inter-Domain Routing (CIDR) oder eine Kombination aus allen dreien.

4. Wählen Sie **Speichern**.

Erstellen eines Datenspeichers

Wenn Sie einen Datenspeicher auf Hostclusterebene erstellen, wird der Datenspeicher erstellt und auf allen Hosts des Ziels bereitgestellt. Die Aktion wird nur aktiviert, wenn der aktuelle Benutzer über die entsprechende Berechtigung zur Ausführung verfügt.

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

ONTAP tools for VMware vSphere 10 erstellen verschachtelte igroups für Datenspeicher, wobei übergeordnete igroups spezifisch für Datenspeicher und untergeordnete igroups den Hosts zugeordnet sind. Sie können flache igroups vom ONTAP -Systemmanager aus erstellen und diese zum Erstellen von VMFS-Datenspeichern verwenden, ohne ONTAP Tools zu verwenden. Siehe "Verwalten von SAN-Initiatoren und igroups" für weitere Informationen.

Wenn der Speicher in ONTAP -Tools integriert und die Datenspeichererkennung ausgeführt wird, werden flache igroups und VMFS-Datenspeicher von ONTAP -Tools verwaltet und in verschachtelte igroups konvertiert. Sie können die früheren flachen igroups nicht zum Erstellen neuer Datenspeicher verwenden. Sie müssen die Benutzeroberfläche der ONTAP Tools oder die REST-API verwenden, um die verschachtelten igroups wiederzuverwenden.

Erstellen eines vVols -Datenspeichers

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

Bevor Sie beginnen

- Stellen Sie sicher, dass Root-Aggregate nicht auf SVM abgebildet werden.
- Stellen Sie sicher, dass der VASA-Anbieter beim ausgewählten vCenter registriert ist.
- Im ASA R2-Speichersystem sollte SVM dem Aggregat für den SVM-Benutzer zugeordnet werden.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem, einen Hostcluster oder ein Rechenzentrum und wählen Sie * NetApp ONTAP Tools* > **Datastore erstellen**.
3. Wählen Sie vVols **Datenspeichertyp** aus.
4. Geben Sie den **Datenspeichernamen** und die **Protokoll**-Informationen ein.

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

5. Wählen Sie die Speicher-VM aus, auf der Sie den Datenspeicher erstellen möchten.
6. Unter erweiterten Optionen:
   - Wenn Sie die **Benutzerdefinierte Exportrichtlinie** auswählen, stellen Sie sicher, dass Sie die Erkennung in vCenter für alle Objekte ausführen. Es wird empfohlen, diese Option nicht zu verwenden.
   - Sie können den Namen **Benutzerdefinierte Initiatorgruppe** für die iSCSI- und FC-Protokolle auswählen.

     Im ASA R2-Speichersystemtyp SVM werden keine Speichereinheiten (LUN/Namespace) erstellt, da der Datenspeicher nur ein logischer Container ist.

7. Im Bereich **Speicherattribute** können Sie neue Volumes erstellen oder die vorhandenen Volumes verwenden. Sie können diese beiden Volumetypen jedoch nicht kombinieren, um einen vVols Datenspeicher zu erstellen.

   Beim Erstellen eines neuen Volumes können Sie QoS im Datenspeicher aktivieren. Standardmäßig wird für jede LUN-Erstellungsanforderung ein Volume erstellt. Dieser Schritt ist nicht anwendbar für vVols -Datenspeicher, die die ASA r2-Speichersysteme verwenden.

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

Erstellen eines NFS-Datenspeichers

Ein VMware Network File System (NFS)-Datenspeicher verwendet das NFS-Protokoll, um ESXi-Hosts über ein Netzwerk mit einem gemeinsam genutzten Speichergerät zu verbinden. NFS-Datenspeicher werden häufig in VMware vSphere-Umgebungen verwendet und bieten mehrere Vorteile, wie beispielsweise Einfachheit und Flexibilität.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem, einen Hostcluster oder ein Rechenzentrum und wählen Sie * NetApp ONTAP Tools* > **Datenspeicher erstellen**.
3. Wählen Sie NFS im Feld **Datenspeichertyp** aus.
4. Geben Sie im Bereich **Name und Protokoll** den Namen, die Größe und die Protokollinformationen des Datenspeichers ein. Wählen Sie in den erweiterten Optionen **Datastore-Cluster** und **Kerberos-Authentifizierung** aus.

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

5. Wählen Sie im Bereich **Speicher Plattform** und **Speicher-VM** aus.
6. Wenn Sie unter den erweiterten Optionen **Benutzerdefinierte Exportrichtlinie** auswählen, führen Sie die Erkennung in vCenter für alle Objekte aus. Es wird empfohlen, diese Option nicht zu verwenden.

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

   - In den erweiterten Optionen ist die Umschalttaste **Asymmetrisch** nur sichtbar, wenn im Plattform-Dropdownmenü „Leistung“ oder „Kapazität“ ausgewählt ist.
   - Wenn Sie im Plattform-Dropdown-Menü die Option **Beliebig** auswählen, können Sie die SVMs sehen, die Teil des vCenters sind, unabhängig von der Plattform oder dem asymmetrischen Flag.
7. Wählen Sie im Bereich **Speicherattribute** das Aggregat für die Volumeerstellung aus. Wählen Sie in den erweiterten Optionen je nach Bedarf **Speicherplatz reservieren** und **QoS aktivieren**.
8. Überprüfen Sie die Auswahl im Bereich **Zusammenfassung** und wählen Sie **Fertig**.

Der NFS-Datenspeicher wird erstellt und auf allen Hosts gemountet.

Erstellen eines VMFS-Datenspeichers

Virtual Machine File System (VMFS) ist ein Cluster-Dateisystem, das Dateien virtueller Maschinen in VMware vSphere-Umgebungen speichert. VMFS ermöglicht mehreren ESXi-Hosts den gleichzeitigen Zugriff auf dieselben virtuellen Maschinendateien und ermöglicht so Funktionen wie vMotion und Hochverfügbarkeit.

Auf einem geschützten Cluster:

- Sie können nur VMFS-Datenspeicher erstellen. Wenn Sie einem geschützten Cluster einen VMFS-Datenspeicher hinzufügen, wird der Datenspeicher automatisch geschützt.
- Sie können keinen Datenspeicher in einem Rechenzentrum mit einem oder mehreren geschützten Hostclustern erstellen.
- Sie können auf dem ESXi-Host keinen Datenspeicher erstellen, wenn der übergeordnete Hostcluster mit einer Beziehung vom Typ „Automatisierte Failover-Duplex-Richtlinie“ (einheitliche/nicht einheitliche Konfiguration) geschützt ist.
- Sie können einen VMFS-Datenspeicher nur auf einem ESXi-Host erstellen, der durch eine asynchrone Beziehung geschützt ist. Sie können keinen Datenspeicher auf einem ESXi-Host erstellen und mounten, der Teil eines Hostclusters ist, der durch die Richtlinie „Automated Failover Duplex“ geschützt ist.

Bevor Sie beginnen

- Aktivieren Sie Dienste und LIFs für jedes Protokoll auf der ONTAP Speicherseite.
- Ordnen Sie SVM dem Aggregat für SVM-Benutzer im ASA R2-Speichersystem zu.
- Konfigurieren Sie den ESXi-Host, wenn Sie das NVMe/TCP-Protokoll verwenden:
  a. Überprüfen Sie die "VMware-Kompatibilitätshandbuch"

  > 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. Überprüfen Sie, ob der Anbieter der Netzwerkschnittstellenkarte (NIC) ESXi NIC mit dem NVMe/TCP-Protokoll unterstützt.
  c. Konfigurieren Sie die ESXi-NIC für NVMe/TCP gemäß den Spezifikationen des NIC-Anbieters.
  d. Wenn Sie VMware vSphere 7 verwenden, folgen Sie den Anweisungen auf der VMware-Site "Konfigurieren der VMkernel-Bindung für den NVMe over TCP-Adapter" um die NVMe/TCP-Portbindung zu konfigurieren. Wenn Sie VMware vSphere 8 verwenden, folgen Sie "Konfigurieren von NVMe über TCP auf ESXi" , um die NVMe/TCP-Portbindung zu konfigurieren.
  e. Für VMware vSphere 7 folgen Sie den Anweisungen auf Seite "Aktivieren Sie NVMe über RDMA oder NVMe über TCP-Softwareadapter" zum Konfigurieren von NVMe/TCP-Softwareadaptern. Für die VMware vSphere 8-Version folgen Sie "Fügen Sie Software-NVMe über RDMA oder NVMe über TCP-Adapter hinzu" um die NVMe/TCP-Softwareadapter zu konfigurieren.
  f. Laufen"Entdecken Sie Speichersysteme und Hosts" Aktion auf dem ESXi-Host. Weitere Informationen finden Sie unter "So konfigurieren Sie NVMe/TCP mit vSphere 8.0 Update 1 und ONTAP 9.13.1 für VMFS-Datenspeicher" .
- Wenn Sie das NVME/FC-Protokoll verwenden, führen Sie die folgenden Schritte aus, um den ESXi-Host zu konfigurieren:
  a. Aktivieren Sie NVMe over Fabrics (NVMe-oF) auf Ihrem/Ihren ESXi-Host(s), falls dies noch nicht geschehen ist.
  b. Vollständige SCSI-Zonierung.
  c. Stellen Sie sicher, dass ESXi-Hosts und das ONTAP System auf einer physischen und logischen Ebene verbunden sind.

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

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-Konfigurationshandbuch" Und "TR-4684" .

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem, einen Hostcluster oder ein Rechenzentrum und wählen Sie * NetApp ONTAP Tools* > **Datastore erstellen**.
3. Wählen Sie den VMFS-Datenspeichertyp aus.
4. Geben Sie im Bereich „Name und Protokoll“ den Namen, die Größe und die Protokollinformationen

des Datenspeichers ein. Wenn Sie den neuen Datenspeicher zu einem vorhandenen VMFS-Datenspeichercluster hinzufügen möchten, wählen Sie unter „Erweiterte Optionen“ die Datenspeicherclusterauswahl aus.

5. Wählen Sie im Bereich **Speicher** die Speicher-VM aus. Geben Sie bei Bedarf den **Namen der benutzerdefinierten Initiatorgruppe** im Abschnitt **Erweiterte Optionen** an. Sie können eine vorhandene Igroup für den Datenspeicher auswählen oder eine neue Igroup mit einem benutzerdefinierten Namen erstellen.

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

6. Aus dem Bereich **Speicherattribute**:

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

      Bei ASA R2-Speichersystemen wird die Option „Aggregat“ nicht angezeigt, da es sich beim ASA R2-Speicher um einen disaggregierten Speicher handelt. Wenn Sie einen ASA R2-Speichersystemtyp „SVM“ auswählen, werden auf der Seite mit den Speicherattributen die Optionen zum Aktivieren von QoS angezeigt.

   b. Gemäß dem ausgewählten Protokoll wird eine Speichereinheit (LUN/Namespace) mit einer Speicherplatzreserve vom Typ „Thin“ erstellt.

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

   c. Wählen Sie das **Leistungsservicelevel** für ASA R2-Speichersysteme mit 12 SVM-Knoten, bei denen es sich um einen heterogenen Cluster handelt. Diese Option ist nicht verfügbar, wenn es sich bei der ausgewählten SVM um einen homogenen Cluster handelt oder sie einen SVM-Benutzer verwendet.

      „Beliebig“ ist der Standardwert für das Performance Service Level (PSL). Diese Einstellung erstellt die Speichereinheit mithilfe des ausgeglichenen Platzierungsalgorithmus von ONTAP . Sie können jedoch je nach Bedarf die Option „Performance“ oder „Extrem“ auswählen.

   d. Wählen Sie nach Bedarf die Optionen **Vorhandenes Volume verwenden**, **QoS aktivieren** und geben Sie die Details ein.

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

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

7. Überprüfen Sie die Datenspeicherdetails im Bereich **Zusammenfassung** und wählen Sie **Fertig**.

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

Ergebnis

Der VMFS-Datenspeicher wird erstellt und auf allen Hosts gemountet.

Schützen Sie Datenspeicher und virtuelle Maschinen

Schützen Sie sich mit dem Hostclusterschutz

ONTAP tools for VMware vSphere verwalten den Schutz von Host-Clustern. Unter einem Hostcluster werden alle Datenspeicher geschützt, die zur ausgewählten SVM gehören und auf einem oder mehreren Hosts des Clusters gemountet sind.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der Hostcluster verfügt nur über Datenspeicher von einer SVM.
- Auf dem Hostcluster gemountete Datenspeicher sollten nicht auf einem Host außerhalb des Clusters gemountet werden.
- Alle auf dem Hostcluster bereitgestellten Datenspeicher müssen VMFS-Datenspeicher mit iSCSI/FC-Protokoll sein. vVols, NFS- oder VMFS-Datenspeicher mit NVMe/FC- und NVMe/TCP-Protokollen werden nicht unterstützt.
- Auf dem Hostcluster gemountete FlexVol/LUN-bildende Datenspeicher sollten nicht Teil einer vorhandenen Konsistenzgruppe (CG) sein.
- Auf dem Hostcluster bereitgestellte FlexVol/LUN-bildende Datenspeicher sollten nicht Teil einer bestehenden SnapMirror -Beziehung sein.
- Der Hostcluster sollte mindestens einen Datenspeicher haben.

Schritte

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

   Der Richtlinientyp kann „Asynchron“ oder „AutomatedFailOverDuplex“ sein.

   Wenn Sie die SnapMirror -Beziehung als Richtlinie vom Typ „AutomatedFailOverDuplex“ hinzufügen, müssen Sie die Zielspeicher-VM als Speicher-Backend zum selben vCenter hinzufügen, in dem ONTAP tools for VMware vSphere bereitgestellt werden.

   Beim Richtlinientyp „AutomatedFailOverDuplex“ gibt es einheitliche und nicht einheitliche Hostkonfigurationen. Wenn Sie die Umschalttaste **einheitliche Hostkonfiguration** auswählen, wird die Konfiguration der Hostinitiatorgruppe implizit auf der Zielsite repliziert. Weitere Einzelheiten finden Sie unter"Wichtige Konzepte und Begriffe" .

7. Wenn Sie sich für eine nicht einheitliche Hostkonfiguration entscheiden, wählen Sie den Hostzugriff (Quelle/Ziel) für jeden Host innerhalb dieses Clusters aus.
8. Wählen Sie **Hinzufügen**.
9. Im Fenster **Cluster schützen** können Sie den geschützten Cluster während des Erstellungsvorgangs nicht bearbeiten. Sie können den Schutz löschen und erneut hinzufügen. Während des Vorgangs „Hostclusterschutz ändern“ ist die Bearbeitungsoption verfügbar. Sie können die Beziehungen mithilfe der Auslassungspunkte-Menüoptionen bearbeiten oder löschen.
10. Wählen Sie die Schaltfläche **Schützen**.

    Eine vCenter-Aufgabe wird mit Job-ID-Details erstellt und ihr Fortschritt wird im Bereich „Letzte Aufgaben“ angezeigt. Dies ist eine asynchrone Aufgabe. Die Benutzeroberfläche zeigt nur den Status der Anforderungsübermittlung an und wartet nicht auf die Fertigstellung der Aufgabe.

11. Um die geschützten Host-Cluster anzuzeigen, navigieren Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**.

Schützen Sie sich mit SRA-Schutz

Konfigurieren Sie SRA zum Schutz von Datenspeichern

ONTAP tools for VMware vSphere bieten die Möglichkeit, die SRA-Funktion zur Konfiguration der Notfallwiederherstellung zu aktivieren.

Bevor Sie beginnen

- Sie sollten Ihre vCenter Server-Instanz eingerichtet und den ESXi-Host konfiguriert haben.
- Sie sollten ONTAP tools for VMware vSphere bereitgestellt haben.
- Sie sollten den SRA-Adapter heruntergeladen haben `.tar.gz` Datei aus dem "NetApp Support Site" .
- Für Quell- und Ziel- ONTAP Cluster müssen vor der Ausführung der SRA-Workflows dieselben benutzerdefinierten SnapMirror -Zeitpläne erstellt werden.
- "Aktivieren Sie ONTAP tools for VMware vSphere -Dienste" um die SRA-Funktion zu aktivieren.

Schritte

1. Melden Sie sich mit der folgenden URL bei der Verwaltungsschnittstelle der VMware Live Site Recovery-Appliance an: `https://:<srm_ip>:5480` und gehen Sie dann zu Storage Replication Adapters in der Verwaltungsschnittstelle der VMware VMware Live Site Recovery-Appliance.
2. Wählen Sie **Neuer Adapter**.
3. Laden Sie das *.tar.gz*-Installationsprogramm für das SRA-Plug-In auf VMware Live Site Recovery hoch.
4. Scannen Sie die Adapter erneut, um zu überprüfen, ob die Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ aktualisiert sind.

Konfigurieren von SRA für SAN- und NAS-Umgebungen

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

Konfigurieren von SRA für SAN-Umgebungen

Bevor Sie beginnen

Sie sollten die folgenden Programme auf der geschützten Site und der Wiederherstellungssite installiert haben:

- VMware Live Site Recovery

  Dokumentation zur Installation von VMware Live Site Recovery finden Sie auf der VMware-Site.

  "Informationen zu VMware Live Site Recovery"

- SRA

  Der Adapter ist auf VMware Live Site Recovery installiert.

Schritte

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

   Sie können dies tun, indem Sie entweder überprüfen, ob die ESXi-Hosts lokale LUNs auf der SVM verbunden haben oder die `iscsi show initiators` Befehl auf den SVMs. Überprüfen Sie den LUN-Zugriff für die zugeordneten LUNs im ESXi-Host, um die iSCSI-Konnektivität zu überprüfen.

Konfigurieren von SRA für NAS-Umgebungen

Bevor Sie beginnen

Sie sollten die folgenden Programme auf der geschützten Site und der Wiederherstellungssite installiert haben:

- VMware Live Site Recovery

  Dokumentation zur Installation von VMware Live Site Recovery finden Sie auf der VMware-Site.

  "Informationen zu VMware Live Site Recovery"

- SRA

  Der Adapter wird auf VMware Live Site Recovery und dem SRA-Server installiert.

Schritte

1. Stellen Sie sicher, dass die Datenspeicher am geschützten Standort virtuelle Maschinen enthalten, die bei vCenter Server registriert sind.
2. Stellen Sie sicher, dass die ESXi-Hosts am geschützten Standort die NFS-Exportvolumes von der Storage Virtual Machine (SVM) gemountet haben.
3. Stellen Sie sicher, dass gültige Adressen wie die IP-Adresse oder der FQDN, unter dem die NFS-Exporte vorliegen, im Feld **NFS-Adressen** angegeben sind, wenn Sie den Array Manager-Assistenten zum

Hinzufügen von Arrays zu VMware Live Site Recovery verwenden. Verwenden Sie im Feld **NFS-Adressen** nicht den NFS-Hostnamen.

4. Verwenden Sie die `ping` auf jedem ESXi-Host am Wiederherstellungsstandort, um zu überprüfen, ob der Host über einen VMkernel-Port verfügt, der auf die IP-Adressen zugreifen kann, die zum Ausführen von NFS-Exporten vom SVM verwendet werden.

Konfigurieren von SRA für hochskalierte Umgebungen

Sie sollten die Speicher-Timeout-Intervalle gemäß den empfohlenen Einstellungen für den Storage Replication Adapter (SRA) konfigurieren, um in stark skalierten Umgebungen eine optimale Leistung zu erzielen.

Speicheranbietereinstellungen

Sie sollten die folgenden Timeout-Werte für VMware Live Site Recovery für eine skalierte Umgebung festlegen:

Erweiterte Einstellungen	Timeout-Werte
`StorageProvider.resignatureTimeout`	Erhöhen Sie den Wert der Einstellung von 900 Sekunden auf 12.000 Sekunden.
`storageProvider.hostRescanDelaySec`	60
`storageProvider.hostRescanRepeatCnt`	20
`storageProvider.hostRescanTimeoutSec`	Stellen Sie einen hohen Wert ein (Beispiel: 99999)

Aktivieren Sie außerdem die `StorageProvider.autoResignatureMode` Option.

Siehe "Speicheranbietereinstellungen ändern" Weitere Informationen zum Ändern der Speicheranbietereinstellungen.

Speichereinstellungen

Wenn Sie ein Timeout erreichen, erhöhen Sie die Werte von `storage.commandTimeout` Und `storage.maxConcurrentCommandCnt` auf einen höheren Wert.

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

Siehe "Speichereinstellungen ändern" zum Ändern der SAN-Provider-Einstellungen.

Konfigurieren von SRA auf der VMware Live Site Recovery-Appliance

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

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

Bevor Sie beginnen

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

Schritte

1. Wählen Sie auf dem Bildschirm der VMware Live Site Recovery-Appliance **Storage Replication Adapter** > **New Adapter**.
2. Laden Sie die Datei *.tar.gz* in VMware Live Site Recovery hoch.
3. Melden Sie sich mit einem Administratorkonto über einen SSH-Client wie PuTTY bei der VMware Live Site Recovery-Appliance an.
4. Wechseln Sie mit dem folgenden Befehl zum Root-Benutzer: `su root`
5. Führen Sie den Befehl aus `cd /var/log/vmware/srm` , um zum Protokollverzeichnis zu navigieren.
6. Geben Sie am Protokollspeicherort den Befehl ein, um die von SRA verwendete Docker-ID abzurufen: `docker ps -l`
7. Um sich bei der Container-ID anzumelden, geben Sie den folgenden Befehl ein: `docker exec -it -u srm <container id> sh`
8. Konfigurieren Sie VMware Live Site Recovery mit ONTAP tools for VMware vSphere IP-Adresse und das Kennwort mithilfe des folgenden Befehls: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv -username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
   - Geben Sie das Kennwort in einfachen Anführungszeichen ein, damit das Perl-Skript Sonderzeichen als Teil des Kennworts und nicht als Trennzeichen behandelt.
   - Sie können den Benutzernamen und das Kennwort der Anwendung (VASA Provider/SRA) im ONTAP Tools Manager festlegen, wenn Sie diese Dienste zum ersten Mal aktivieren. Verwenden Sie diese Anmeldeinformationen, um SRA bei VMware Live Site Recovery zu registrieren.
   - Um die vCenter-GUID zu finden, gehen Sie nach dem Hinzufügen Ihrer vCenter-Instanz zur vCenter-Server-Seite im ONTAP Tools Manager. Siehe"vCenter-Server hinzufügen" Abschnitt.
9. Scannen Sie die Adapter erneut, um zu bestätigen, dass die aktualisierten Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ angezeigt werden.

Ergebnisse

Eine Bestätigungsmeldung zeigt an, dass die Speicheranmeldeinformationen gespeichert wurden. SRA kann nun über die angegebene IP-Adresse, den Port und die Anmeldeinformationen mit dem SRA-Server kommunizieren.

SRA-Anmeldeinformationen aktualisieren

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

Bevor Sie beginnen

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

Schritte

1. Führen Sie die folgenden Befehle aus, um den im Ordner „VMware Live Site Recovery“ zwischengespeicherten Benutzernamen und das Kennwort für die ONTAP -Tools 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>`Der Kennwortwert muss in einfache Anführungszeichen gesetzt werden.

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

Konfigurieren von geschützten Sites und Wiederherstellungssites

Sie sollten Schutzgruppen erstellen, um eine Gruppe virtueller Maschinen auf der geschützten Site zu schützen.

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

Koppeln Sie geschützte Sites und Wiederherstellungssites

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

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

Bevor Sie beginnen

- Sie sollten VMware Live Site Recovery auf den geschützten Sites und Wiederherstellungssites installiert haben.
- Sie sollten SRA auf den geschützten Sites und Wiederherstellungssites installiert haben.

Schritte

1. Doppelklicken Sie auf der Startseite des vSphere-Clients auf **Site Recovery** und wählen Sie **Sites** aus.
2. Wählen Sie **Objekte** > **Aktionen** > **Sites koppeln**.
3. Geben Sie im Dialogfeld **Site Recovery Manager-Server koppeln** die Adresse des Platform Services Controllers der geschützten Site ein und wählen Sie dann **Weiter**.
4. Führen Sie im Abschnitt „vCenter Server auswählen“ die folgenden Schritte aus:
   a. Überprüfen Sie, 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 dann **Fertig**.
5. Wählen Sie bei der entsprechenden Aufforderung **Ja** aus, um die Sicherheitszertifikate zu akzeptieren.

Ergebnis

Sowohl die geschützten als auch die Wiederherstellungssites werden im Dialogfeld „Objekte“ angezeigt.

Konfigurieren von Schutzgruppen

Bevor Sie beginnen

Sie sollten sicherstellen, dass sowohl die Quell- als auch die Zielsites für Folgendes konfiguriert sind:

- Dieselbe Version von VMware Live Site Recovery installiert
- Virtuelle Maschinen
- Gepaarte geschützte Sites und Wiederherstellungssites
- Quell- und Zieldatenspeicher sollten auf den jeweiligen Sites gemountet werden

Schritte

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

Alle virtuellen Maschinen in der Replikationsgruppe werden der Schutzgruppe hinzugefügt.

6. Sie können entweder den vorhandenen Wiederherstellungsplan auswählen oder einen neuen erstellen, indem Sie **Zum neuen Wiederherstellungsplan hinzufügen** auswählen.
7. Überprüfen Sie auf der Registerkarte „Bereit zum Abschließen“ die Details der von Ihnen erstellten Schutzgruppe und wählen Sie dann **Fertig stellen** aus.

Konfigurieren von geschützten Site- und Wiederherstellungs-Site-Ressourcen

Konfigurieren von Netzwerkzuordnungen

Sie sollten Ihre Ressourcenzuordnungen wie VM-Netzwerke, ESXi-Hosts und Ordner auf beiden Sites konfigurieren, um die Zuordnung jeder Ressource von der geschützten Site zur entsprechenden Ressource auf der Wiederherstellungssite zu ermöglichen.

Sie sollten die folgenden Ressourcenkonfigurationen durchführen:

- Netzwerkzuordnungen
- Ordnerzuordnungen
- Ressourcenzuordnungen
- Platzhalter-Datenspeicher

Bevor Sie beginnen

Sie sollten die geschützten und Wiederherstellungssites verbunden haben.

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie auf der Registerkarte „Verwalten“ **Netzwerkzuordnungen** > **Neu**, um eine neue Netzwerkzuordnung zu erstellen.
4. Führen Sie im Assistenten „Netzwerkzuordnung erstellen“ die folgenden Schritte aus:
   a. Wählen Sie **Zuordnungen für Netzwerke mit übereinstimmenden Namen automatisch vorbereiten** und wählen Sie **Weiter**.
   b. Wählen Sie die erforderlichen Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
   c. Wählen Sie **Weiter**, nachdem die Zuordnungen erfolgreich erstellt wurden.
   d. Wählen Sie das zuvor zum Erstellen der Rückwärtszuordnung verwendete Objekt aus und wählen Sie dann **Fertig**.

Ergebnis

Auf der Seite „Netzwerkzuordnungen“ werden die Ressourcen der geschützten Site und der Wiederherstellungssite angezeigt. Sie können dieselben Schritte für andere Netzwerke in Ihrer Umgebung ausführen.

Konfigurieren von Ordnerzuordnungen

Sie sollten Ihre Ordner auf der geschützten Site und der Wiederherstellungssite zuordnen, um die Kommunikation zwischen ihnen zu ermöglichen.

Bevor Sie beginnen

Sie sollten die geschützten und Wiederherstellungssites verbunden haben.

Schritte

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

Ergebnis

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

Konfigurieren von Ressourcenzuordnungen

Sie sollten Ihre Ressourcen auf der geschützten Site und der Wiederherstellungssite so zuordnen, dass virtuelle Maschinen für ein Failover in die eine oder andere Hostgruppe konfiguriert sind.

Bevor Sie beginnen

Sie sollten die geschützten und Wiederherstellungssites verbunden haben.

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

Schritte

1. Melden Sie sich bei vCenter Server an und wählen Sie **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Site aus und wählen Sie **Verwalten**.
3. Wählen Sie auf der Registerkarte „Verwalten“ **Ressourcenzuordnungen** > **Neu** aus, um eine neue Ressourcenzuordnung zu erstellen.
4. Führen Sie im Assistenten „Ressourcenzuordnung erstellen“ die folgenden Schritte aus:
   a. Wählen Sie **Zuordnungen für Ressourcen mit übereinstimmenden Namen automatisch vorbereiten** und klicken Sie auf **Weiter**.
   b. Wählen Sie die erforderlichen Rechenzentrumsobjekte für die geschützten und Wiederherstellungsstandorte aus und wählen Sie **Zuordnungen hinzufügen**.
   c. Wählen Sie **Weiter**, nachdem die Zuordnungen erfolgreich erstellt wurden.

d. Wählen Sie das zuvor zum Erstellen der Rückwärtszuordnung verwendete Objekt aus und wählen Sie dann **Fertig**.

Ergebnis

Auf der Seite „Ressourcenzuordnungen“ werden die Ressourcen der geschützten Site und der Wiederherstellungssite angezeigt. Sie können dieselben Schritte für andere Netzwerke in Ihrer Umgebung ausführen.

Platzhalter-Datenspeicher konfigurieren

Sie sollten einen Platzhalterdatenspeicher konfigurieren, der im vCenter-Inventar am Wiederherstellungsstandort Platz für die geschützte virtuelle Maschine (VM) reserviert. Der Platzhalterdatenspeicher muss nicht groß sein, da die Platzhalter-VMs klein sind und nur wenige hundert Kilobyte oder weniger belegen.

Bevor Sie beginnen

- Sie sollten die geschützten und Wiederherstellungssites verbunden haben.
- Sie sollten Ihre Ressourcenzuordnungen konfiguriert haben.

Schritte

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

   Platzhalter-Datenspeicher können lokal oder remote sein und sollten nicht repliziert werden.

5. Wiederholen Sie die Schritte 3 bis 5, um einen Platzhalterdatenspeicher für die Wiederherstellungssite zu konfigurieren.

Konfigurieren Sie SRA mit dem Array-Manager

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

Bevor Sie beginnen

- Sie sollten die geschützten Sites und Wiederherstellungssites in VMware Live Site Recovery gekoppelt haben.
- Sie sollten Ihren integrierten Speicher konfiguriert haben, bevor Sie den Array-Manager konfigurieren.
- Sie sollten die SnapMirror -Beziehungen zwischen den geschützten Sites und den Wiederherstellungssites konfiguriert und repliziert haben.
- Sie sollten die SVM-Verwaltungs-LIFs aktiviert haben, um Multitenancy zu ermöglichen.

SRA unterstützt die Verwaltung auf Cluster- und SVM-Ebene. Wenn Sie Speicher auf Clusterebene hinzufügen, können Sie alle SVMs im Cluster erkennen und Vorgänge darauf ausführen. Wenn Sie Speicher auf SVM-Ebene hinzufügen, können Sie nur dieses bestimmte SVM verwalten.

Schritte

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

   a. Geben Sie im Feld **Anzeigename** einen Namen zur Identifizierung des Array-Managers ein.

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

   c. Geben Sie die Informationen zum Herstellen einer Verbindung mit dem Cluster oder der SVM ein:

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

      Beim Konfigurieren des Array-Managers sollten Sie für das Speichersystem dieselbe Verbindung (IP-Adresse) verwenden, die zum Onboarding des Speichersystems in den ONTAP tools for VMware vSphere verwendet wurde. Wenn die Array-Manager-Konfiguration beispielsweise auf SVM beschränkt ist, sollte der Speicher unter ONTAP tools for VMware vSphere auf SVM-Ebene hinzugefügt werden.

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

   e. Geben Sie die zu ermittelnden Volumes in das Feld **Volume-Einschlussliste** ein.

      Sie können das Quellvolume am geschützten Standort und das replizierte Zielvolume am Wiederherstellungsstandort eingeben.

      Wenn Sie beispielsweise das Volume src_vol1 ermitteln möchten, das in einer SnapMirror -Beziehung mit dem Volume dst_vol1 steht, sollten Sie src_vol1 im Feld „geschützte Site“ und dst_vol1 im Feld „Wiederherstellungssite“ angeben.

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

      Sie können das Quellvolume am geschützten Standort und das replizierte Zielvolume am Wiederherstellungsstandort eingeben.

   Wenn Sie beispielsweise das Volume *src_vol1* ausschließen möchten, das in einer SnapMirror -Beziehung mit dem Volume *dst_vol1* steht, sollten Sie *src_vol1* im Feld „Geschützter Standort“ und *dst_vol1* im Feld „Wiederherstellungsstandort“ angeben.

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

Sie können dieselben Schritte für die Wiederherstellungssite ausführen, indem Sie die entsprechenden SVM-Verwaltungs-IP-Adressen und Anmeldeinformationen verwenden. Überprüfen Sie auf dem Bildschirm „Array-Paare aktivieren“ des Assistenten „Array-Manager hinzufügen“, ob das richtige Array-Paar ausgewählt ist und als zur Aktivierung bereit angezeigt wird.

Überprüfen replizierter Speichersysteme

Sie sollten überprüfen, ob die geschützte Site und die Wiederherstellungssite nach der Konfiguration des Storage Replication Adapter (SRA) erfolgreich gekoppelt wurden. Das replizierte Speichersystem sollte sowohl vom geschützten Standort als auch vom Wiederherstellungsstandort erkennbar sein.

Bevor Sie beginnen

- Sie sollten Ihr Speichersystem konfiguriert haben.
- Sie sollten die geschützte Site und die Wiederherstellungssite mithilfe des VMware Live Site Recovery-Array-Managers gekoppelt haben.
- Sie sollten die FlexClone -Lizenz und die SnapMirror -Lizenz aktiviert haben, bevor Sie den Test-Failover-Vorgang und den Failover-Vorgang für SRA durchführen.
- Sie sollten auf Quell- und Zielsites dieselben SnapMirror -Richtlinien und -Zeitpläne haben.

Schritte

1. Melden Sie sich bei Ihrem vCenter Server an.
2. Navigieren Sie zu **Site Recovery** > **Array-basierte Replikation**.
3. Wählen Sie das gewünschte Array-Paar aus und überprüfen Sie die entsprechenden Angaben.

   Die Speichersysteme sollten am geschützten Standort und am Wiederherstellungsstandort mit dem Status „Aktiviert“ erkannt werden.

Fan-Out-Schutz

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

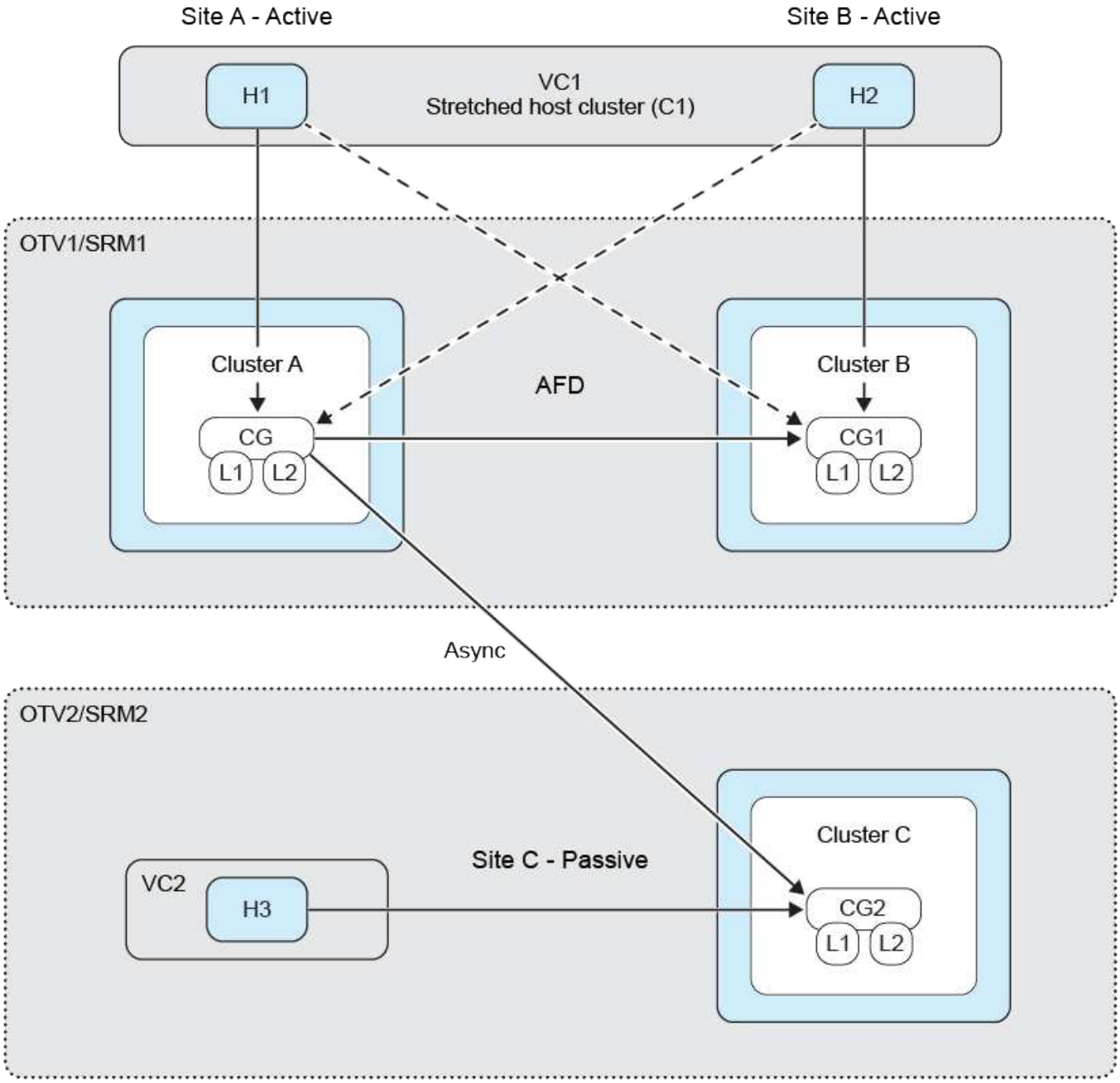
Um einen Fan-Out-Schutz einzurichten, müssen Sie drei Site-Cluster und SVMs miteinander verbinden.

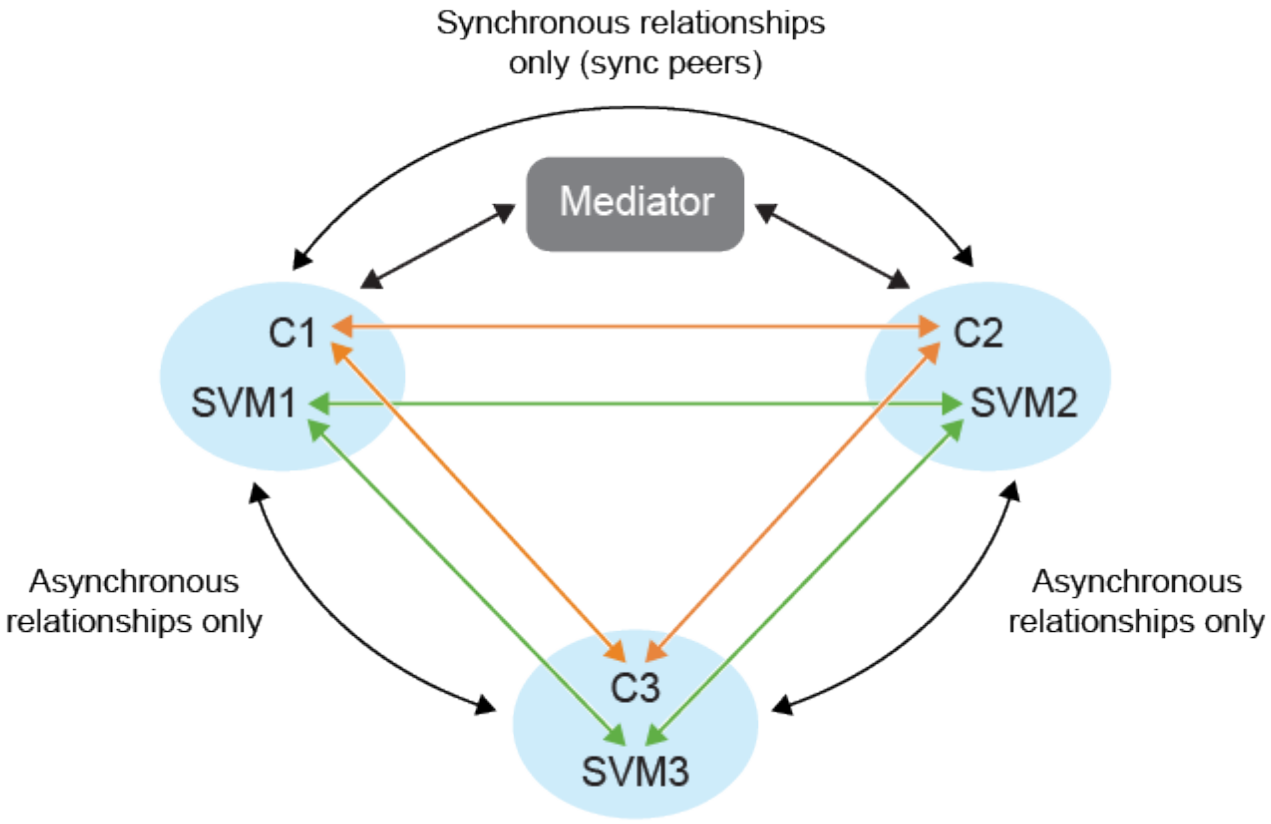
Beispiel:

Wenn	Dann

• Die Quellkonsistenzgruppe befindet sich auf Cluster c1 und SVM svm1 • Die erste Zielkonsistenzgruppe befindet sich auf Cluster c2 und SVM svm2 und • Die zweite Zielkonsistenzgruppe 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 wird (C2, C1) und (C2, C3) sein und • Das Cluster-Peering auf dem zweiten Ziel ONTAP Cluster wird (C3, C1) und (C3, C2) sein. • SVM-Peering auf Quell-SVM wird (svm1, svm2) und (svm1, svm3) sein. • SVM-Peering auf dem ersten Ziel-SVM wird (svm2, svm1) und (svm2, svm3) sein und • Das SVM-Peering auf dem zweiten Ziel-SVM erfolgt (svm3, svm1) und (svm3, svm2).

Das folgende Diagramm zeigt die Fan-Out-Schutzkonfiguration:


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



Schritte

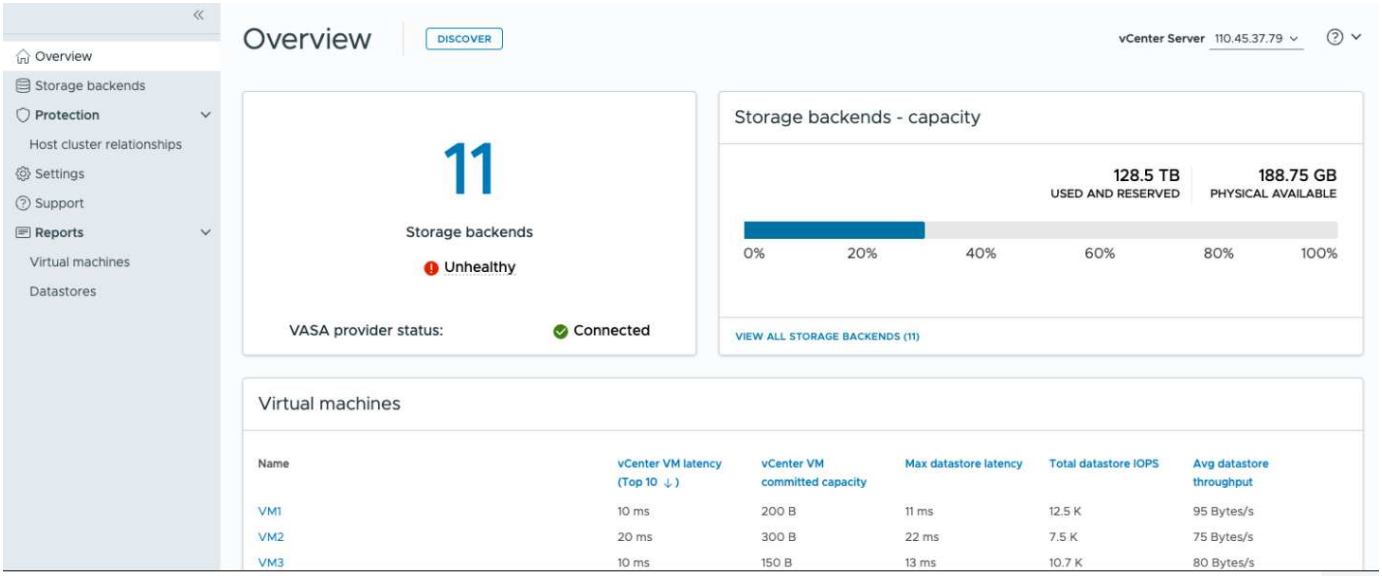
1. Erstellen Sie einen neuen Platzhalter-Datenspeicher. Verweisen "Wählen Sie einen Platzhalter-Datenspeicher aus"
2. Fügen Sie dem Hostclusterschutz einen Datenspeicher hinzu"Geschützten Hostcluster ändern" . Sie müssen sowohl asynchrone als auch synchrone Richtlinientypen hinzufügen.

Verwalten Sie ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere – Dashboard-Übersicht

Wenn Sie im Abschnitt „Verknüpfungen“ des vCenter-Clients das Plug-In-Symbol „ONTAP tools for VMware vSphere“ auswählen, navigiert die Benutzeroberfläche zur Übersichtsseite. Diese Seite fungiert als Dashboard und bietet Ihnen eine Übersicht über die ONTAP tools for VMware vSphere Plug-in.

Bei der Einrichtung im Enhanced Linked Mode (ELM) wird das Dropdown-Menü zur Auswahl des vCenter-Servers angezeigt und Sie können einen gewünschten vCenter-Server auswählen, um die entsprechenden Daten anzuzeigen. Dieses Dropdown-Menü ist für alle anderen Listenansichten des Plug-Ins verfügbar. Die auf einer Seite getroffene vCenter Server-Auswahl bleibt auf allen Registerkarten des Plug-Ins erhalten.



Von der Übersichtsseite aus können Sie die Aktion **Discovery** ausführen. Die Erkennungsaktion führt die Erkennung auf vCenter-Ebene aus, um alle neu hinzugefügten oder aktualisierten Speicher-Backends, Hosts, Datenspeicher und Schutzstatus/-beziehungen zu erkennen. Sie können eine On-Demand-Erkennung von Entitäten ausführen, ohne auf die geplante Erkennung warten zu müssen.

Die Aktionsschaltfläche wird nur aktiviert, wenn Sie über die Berechtigung zum Ausführen der Erkennungsaktion verfügen.

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

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

Karte	Beschreibung

Status	Die Statuskarte zeigt die Anzahl der Speicher-Backends und den allgemeinen Integritätsstatus der Speicher-Backends und des VASA-Anbieters. Der Status der Speicher-Backends wird „**Healthy**“ angezeigt, wenn der Status aller Speicher-Backends normal ist, und „Unhealthy*“, wenn bei einem der Speicher-Backends ein Problem vorliegt (Status „Unbekannt/Nicht erreichbar/Beeinträchtigt“). Wählen Sie den Tooltip aus, um die Statusdetails der Speicher-Backends zu öffnen. Sie können ein beliebiges Speicher-Backend auswählen, um weitere Details zu erhalten. Der Link **Andere VASA-Provider-Status** zeigt den aktuellen Status des VASA-Providers, der im vCenter Server registriert ist.
Speicher-Backends – Kapazität	Diese Karte zeigt die aggregierte genutzte und verfügbare Kapazität aller Speicher-Backends für die ausgewählte vCenter Server-Instanz. Bei ASA R2-Speichersystemen werden die Kapazitätsdaten nicht angezeigt, da es sich um ein disaggregiertes System handelt.
Virtuelle Maschinen	Diese Karte zeigt die Top 10 VMs, sortiert nach Leistungsmetrik. Sie können die Kopfzeile auswählen, um die Top 10 VMs für die ausgewählte Metrik in aufsteigender oder absteigender Reihenfolge sortiert zu erhalten. Die auf der Karte vorgenommenen Sortier- und Filteränderungen bleiben bestehen, bis Sie den Browser-Cache ändern oder leeren.
Datenspeicher	Diese Karte zeigt die Top 10 Datenspeicher, sortiert nach Leistungskennzahlen. Sie können die Kopfzeile auswählen, um die Top 10 Datenspeicher für die ausgewählte Metrik in aufsteigender oder absteigender Reihenfolge sortiert zu erhalten. Die auf der Karte vorgenommenen Sortier- und Filteränderungen bleiben bestehen, bis Sie den Browser-Cache ändern oder leeren. Es gibt ein Dropdown-Menü „Datenspeichertyp“, in dem Sie den Typ der Datenspeicher auswählen können – NFS, VMFS oder vVols.
ESXi-Host-Compliance-Karte	Diese Karte zeigt den Gesamtkonformitätsstatus aller ESXi-Hosteinstellungen (für das ausgewählte vCenter) in Bezug auf die empfohlenen NetApp -Hosteinstellungen nach Einstellungsgruppe/Kategorie. Sie können den Link **Empfohlene Einstellungen anwenden** auswählen, um die empfohlenen Einstellungen anzuwenden. Sie können den Konformitätsstatus der Hosts auswählen, um die Liste der Hosts anzuzeigen.

ONTAP Tools Manager-Benutzeroberfläche

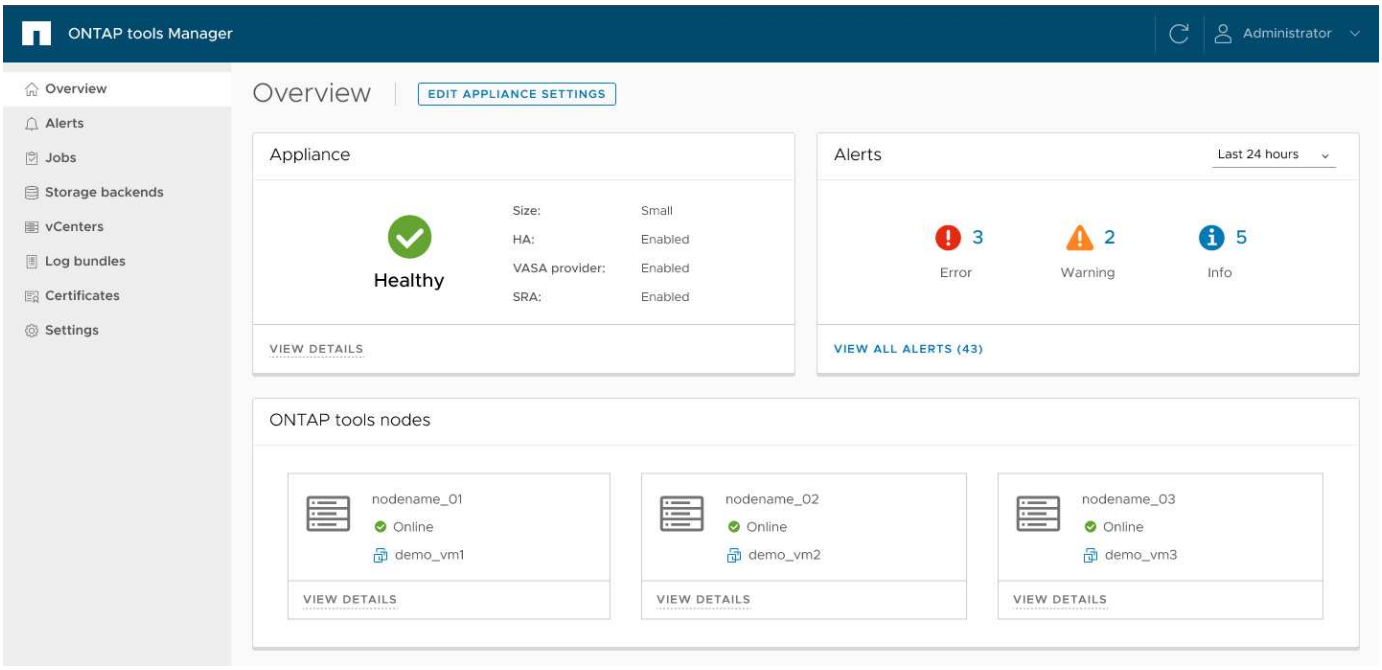
ONTAP tools for VMware vSphere sind ein Multi-Tenant-System, das mehrere vCenter Server-Instanzen verwalten kann. ONTAP Tools Manager bietet den ONTAP tools for VMware vSphere Administrator mehr Kontrolle über die verwalteten vCenter Server-Instanzen und integrierten Speicher-Backends.

ONTAP Tools Manager hilft bei:

- vCenter Server-Instanzverwaltung – Fügen Sie vCenter Server-Instanzen zu ONTAP Tools hinzu und verwalten Sie sie.
- Speicher-Backend-Verwaltung – Fügen Sie ONTAP Speichercluster zu ONTAP tools for VMware vSphere hinzu, verwalten Sie sie und ordnen Sie sie global integrierten vCenter Server-Instanzen zu.
- Downloads von Protokollpaketen – Sammeln Sie Protokolldateien für ONTAP tools for VMware vSphere.
- Zertifikatsverwaltung – Ändern Sie das selbstsignierte Zertifikat in ein benutzerdefiniertes CA-Zertifikat und erneuern oder aktualisieren Sie alle Zertifikate des VASA-Anbieters und der ONTAP Tools.
- Kennwortverwaltung – Setzen Sie das Kennwort des Benutzers für die OVA-Anwendung zurück.

Um auf den ONTAP Tools Manager zuzugreifen, starten Sie `https://<ONTAPtoolsIP>:8443/virtualization/ui/` vom Browser aus und melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.

Der Abschnitt „Übersicht“ des ONTAP Tools Managers hilft bei der Verwaltung der Appliance-Konfiguration, beispielsweise bei der Dienstverwaltung, der Skalierung der Knotengröße und der Aktivierung von Hochverfügbarkeit (HA). Sie können auch die allgemeinen Informationen der ONTAP -Tools im Zusammenhang mit den Knoten überwachen, z. B. Integrität, Netzwerkdetails und Warnungen.



Karte	Beschreibung
Gerätekarte	Die Appliance-Karte zeigt den Gesamtstatus der ONTAP Tools-Appliance an. Es zeigt die Konfigurationsdetails des Geräts und den Status der aktivierten Dienste. Weitere Informationen zur ONTAP Tools-Appliance erhalten Sie, wenn Sie auf den Link **Details anzeigen** klicken. Wenn ein Aktionsauftrag zum Bearbeiten von Geräteeinstellungen ausgeführt wird, zeigt das Geräte-Portlet den Status und die Details des Auftrags an.
Warnungskarte	Auf der Karte „Warnungen“ werden die Warnungen der ONTAP -Tools nach Typ aufgelistet, einschließlich der Warnungen auf HA-Knotenebene. Sie können die Liste der Warnungen anzeigen, indem Sie auf den Zähltext (Hyperlink) klicken. Über den Link gelangen Sie zur Seite mit der nach dem ausgewählten Typ gefilterten Warnmeldungsansicht.
vCenter	Die vCenter-Karte zeigt den Integritätsstatus der vCenter im System.
Speicher-Backends	Die Karte „Storage-Backends“ zeigt den Integritätsstatus der Storage-Backends im System.
ONTAP -Tools-Knotenkarte	Die Knotenkarte des ONTAP -Tools zeigt die Liste der Knoten mit Knotennamen, Knoten-VM-Namen, Status und allen netzwerkbezogenen Daten. Sie können **Details anzeigen** auswählen, um die zusätzlichen Details zum ausgewählten Knoten anzuzeigen. [HINWEIS] In einem Nicht-HA-Setup wird nur ein Knoten angezeigt. Im HA-Setup werden drei Knoten angezeigt.

Verstehen Sie igroups und Exportrichtlinien in ONTAP tools for VMware vSphere

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

In ONTAP tools for VMware vSphere 9.x wurden igroups in einer flachen Struktur erstellt und verwaltet, wobei jeder Datenspeicher in vCenter einer einzelnen igroup zugeordnet war. Dieses Modell schränkte die Flexibilität und Wiederverwendung von igroups über mehrere Datenspeicher hinweg ein. ONTAP tools for VMware vSphere 10.x führen verschachtelte igroups ein, bei denen jeder Datenspeicher in vCenter einer übergeordneten igroup zugeordnet ist, während jeder Host mit einer untergeordneten igroup unter dieser übergeordneten igroup verknüpft ist. Sie können benutzerdefinierte übergeordnete igroups mit benutzerdefinierten Namen zur Wiederverwendung in mehreren Datenspeichern definieren und so eine flexiblere und vernetztere Verwaltung von igroups ermöglichen. Das Verständnis des igroup-Workflows ist für die effektive Verwaltung von LUNs und Datenspeichern in ONTAP tools for VMware vSphere von entscheidender Bedeutung. Verschiedene Workflows erzeugen unterschiedliche igroup-Konfigurationen, wie in den folgenden Beispielen gezeigt:

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

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

Beispiel 1:

Erstellen Sie einen Datenspeicher auf einem einzelnen Host mit einem Initiator

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

Ergebnis:

- DS1I-Gruppe:
  - host1Igroup → (iqn1: lun1)

Auf den ONTAP Systemen für DS1 wird eine übergeordnete Igroup DS1Igroup erstellt, wobei eine untergeordnete Igroup host1Igroup auf lun1 abgebildet wird. LUNs werden immer untergeordneten igroups zugeordnet.

Beispiel 2:

Mounten Sie den vorhandenen Datenspeicher auf einem zusätzlichen Host

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

Ergebnis:

- DS1I-Gruppe:
  - host1Igroup → (iqn1: lun1)
  - host2Igroup → (iqn2: lun1)

Eine untergeordnete Igroup „host2Igroup“ wird erstellt und der vorhandenen übergeordneten Igroup „DS1Igroup“ hinzugefügt.

Beispiel 3:

Unmounten eines Datenspeichers von einem Host

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

Ergebnis:

- DS1I-Gruppe:
  - host2Igroup → (iqn2: lun1)

Die Host1I-Gruppe wird aus der Hierarchie entfernt. Untergeordnete igroups werden nicht explizit gelöscht. Die Löschung erfolgt unter diesen beiden Bedingungen:

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

Beispiel 4:

Datenspeicher löschen

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

Ergebnis:

- DS1I-Gruppe:
  - host2Igroup → (iqn2: lun1)

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

Beispiel 5:

Erstellen Sie mehrere Datenspeicher unter einer benutzerdefinierten übergeordneten igroup

Arbeitsablauf:

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

Ergebnis:

- Benutzerdefinierte Gruppe1:
  - host1Igroup → (iqn1: lun2, lun3)
  - host2Igroup → (iqn2: lun2)
  - host3Igroup → (iqn3: lun3)

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

Beispiel 6:

Löschen Sie einen Datenspeicher unter einer benutzerdefinierten übergeordneten Igroup.

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

Ergebnis:

- Benutzerdefinierte Gruppe1:
  - host1Igroup → (iqn1: lun3)
  - host3Igroup → (iqn3: lun3)
- Obwohl CustomIgroup1 nicht wiederverwendet wird, wird es nicht gelöscht.
- Wenn keine LUNs zugeordnet sind, löscht das ONTAP -System host2Igroup.
- Die Host1-Igroup wird nicht gelöscht, da sie der Lun3 von DS3 zugeordnet ist. Benutzerdefinierte Igroups werden unabhängig vom Wiederverwendungsstatus nie gelöscht.

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

Arbeitsablauf:

Vor der Erweiterung:

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

- DS4Igroup: host4Igroup → (iqn4: lun4)

Nach der Erweiterung:

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

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

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

Beispiel 8:
vVols -Datenspeicher verkleinern (Volume entfernen)

Arbeitsablauf:

Vor dem Schrumpfen:

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

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

Nach dem Schrumpfen:

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

- DS4Igroup: host4Igroup → (iqn4: lun4)

Die angegebene LUN (lun5) wird von der untergeordneten igroup getrennt. Die igroup bleibt aktiv, solange sie mindestens eine zugeordnete LUN hat.

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

Arbeitsablauf

ONTAP -Tools für VMware vSPhere 9.x-Versionen unterstützen keine hierarchischen igroups. Während der

Migration auf Version 10.3 oder höher müssen igroups in die hierarchische Struktur normalisiert werden.

Vor der Migration:

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

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

Nach der Migration:

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

Während der Migration:

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

Dadurch wird die Einhaltung des hierarchischen Modells sichergestellt.

Verwandte Themen

"Über igroups"

Exportrichtlinien

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

Wenn Sie in den ONTAP tools for VMware vSphere einen NFS-Datenspeicher erstellen, können Sie eine vorhandene Exportrichtlinie auswählen oder eine neue erstellen. Die Exportrichtlinie wird dann auf den Datenspeicher angewendet, um sicherzustellen, dass nur autorisierte Clients darauf zugreifen können.

Wenn Sie einen NFS-Datenspeicher auf einem neuen ESXi-Host mounten, fügen ONTAP tools for VMware vSphere die IP-Adresse des Hosts der vorhandenen Exportrichtlinie hinzu, die mit dem Datenspeicher verknüpft ist. Dadurch kann der neue Host auf den Datenspeicher zugreifen, ohne eine neue Exportrichtlinie erstellen zu müssen.

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

Die Zuweisung der Exportrichtlinie unterscheidet sich, wenn sie in verschiedenen Datenspeichern wiederverwendet wird. Bei der Wiederverwendung der Exportrichtlinie können Sie die neue Host-IP-Adresse anhängen. Beim Löschen oder Unmounten eines Datenspeichers mit einer freigegebenen Exportrichtlinie wird die Richtlinie nicht gelöscht. Sie bleibt unverändert, und die Host-IP-Adresse wird nicht entfernt, da sie mit den

anderen Datenspeichern gemeinsam genutzt wird. Die Wiederverwendung von Exportrichtlinien wird nicht empfohlen, da dies zu Zugriffs- und Latenzproblemen führen kann.

Verwandte Themen

"Erstellen einer Exportrichtlinie"

Verstehen Sie die von ONTAP -Tools verwalteten igroups

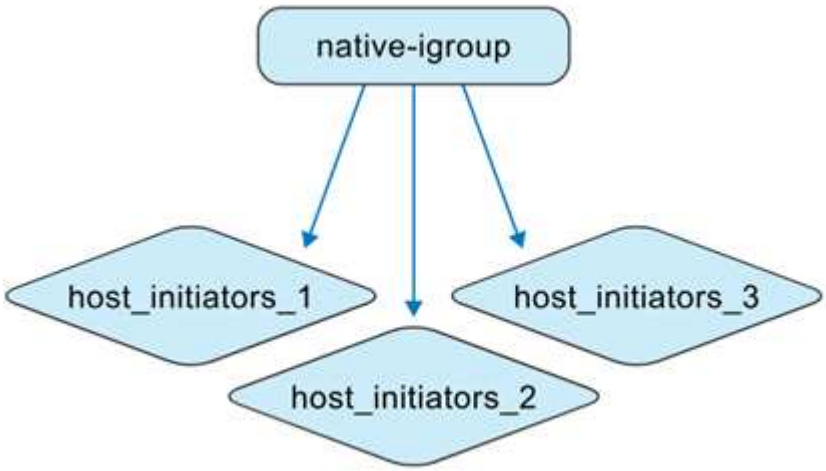
Beim Verwalten von ONTAP -Tool-VMs und ONTAP Speichersystemen ist es wichtig, das Verhalten von igroups zu verstehen, insbesondere beim Migrieren von Datenspeichern aus Umgebungen ohne ONTAP Tools zur Verwaltung von ONTAP Tools. In diesem Abschnitt wird beschrieben, wie igroups während dieses Übergangs aktualisiert werden.

ONTAP tools for VMware vSphere 10.4 vereinfachen die Datenspeicherverwaltung durch Automatisierung der Erstellung und Wartung von ONTAP und vCenter-Objekten in VMware-Rechenzentrumsumgebungen.

ONTAP tools for VMware vSphere 10.4 interpretieren igroups in zwei verschiedenen Kontexten:

Von Nicht- ONTAP -Tools verwaltete igroups

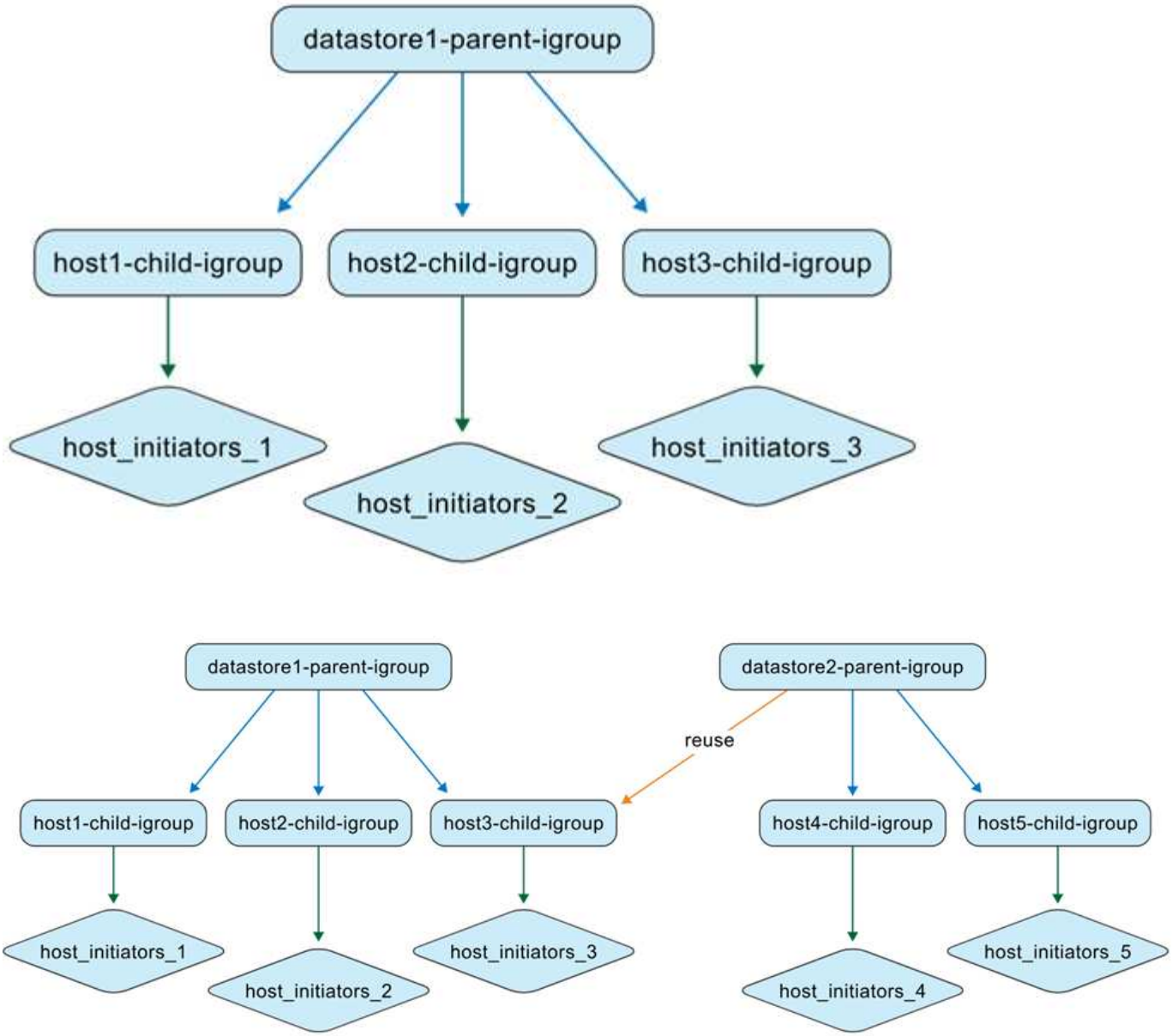
Als Speicheradministrator können Sie igroups auf dem ONTAP -System als flache oder verschachtelte Strukturen erstellen. Die Abbildung zeigt eine flache igroup, die im ONTAP -System erstellt wurde.



Von ONTAP -Tools verwaltete igroups

Wenn Sie Datenspeicher erstellen, erstellen ONTAP tools for VMware vSphere 10.4 automatisch igroups mithilfe einer verschachtelten Struktur für eine einfachere LUN-Zuordnung.

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



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

Wenn Sie einen Datenspeicher mit Standard-Igroup-Einstellungen erstellen

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

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

Wenn Sie einen Datenspeicher mit einem benutzerdefinierten igroup-Namen erstellen

Während der Datenspeichererstellung in ONTAP -Tools können Sie einen benutzerdefinierten Igroup-Namen

eingeben, anstatt ihn aus der Dropdown-Liste auszuwählen. Anschließend erstellen die ONTAP -Tools eine übergeordnete igroup auf Datenspeicherebene mit dem von Ihnen angegebenen Namen. Wenn derselbe Host für mehrere Datenspeicher verwendet wird, wird die vorhandene (untergeordnete) igroup auf Hostebene wiederverwendet. Infolgedessen wird die LUN für den neuen Datenspeicher dieser vorhandenen untergeordneten Igroup zugeordnet, die jetzt möglicherweise mit mehreren übergeordneten Igroups verknüpft ist (eine für jeden Datenspeicher). Die Datenspeicherliste der vCenter Server-Benutzeroberfläche bestätigt die erfolgreiche Erstellung des neuen Datenspeichers mit dem benutzerdefinierten igroup-Namen.

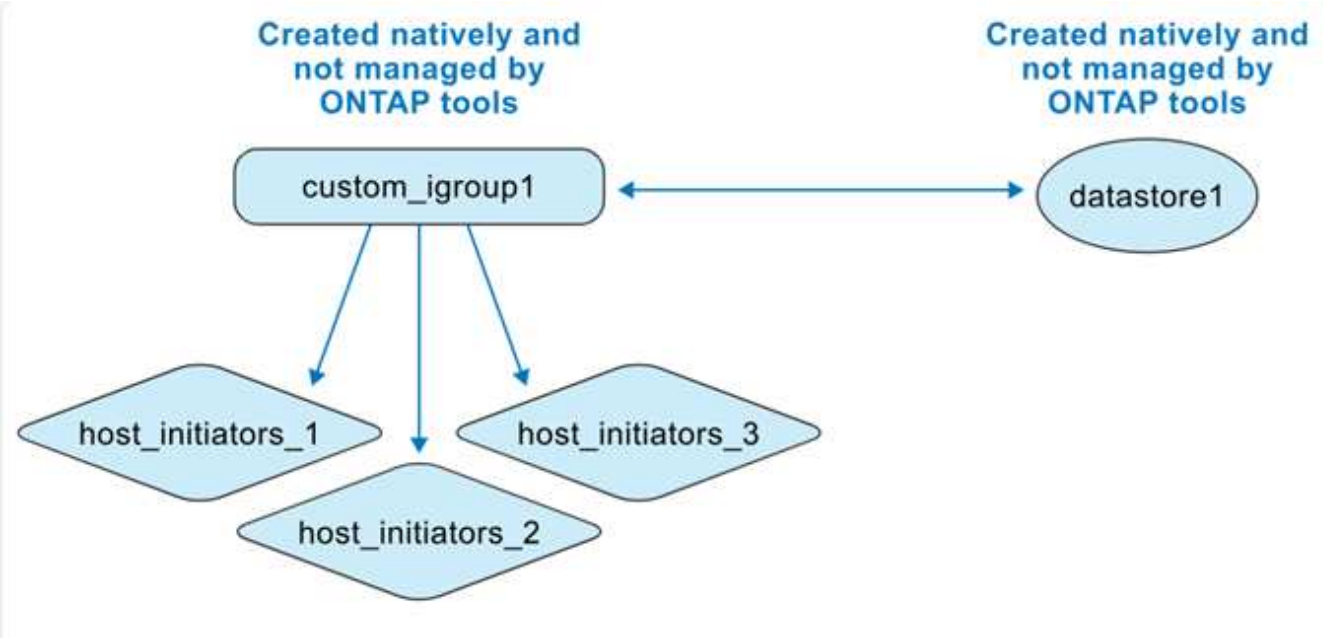
Wenn Sie den Igroup-Namen während der Datenspeichererstellung wiederverwenden

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

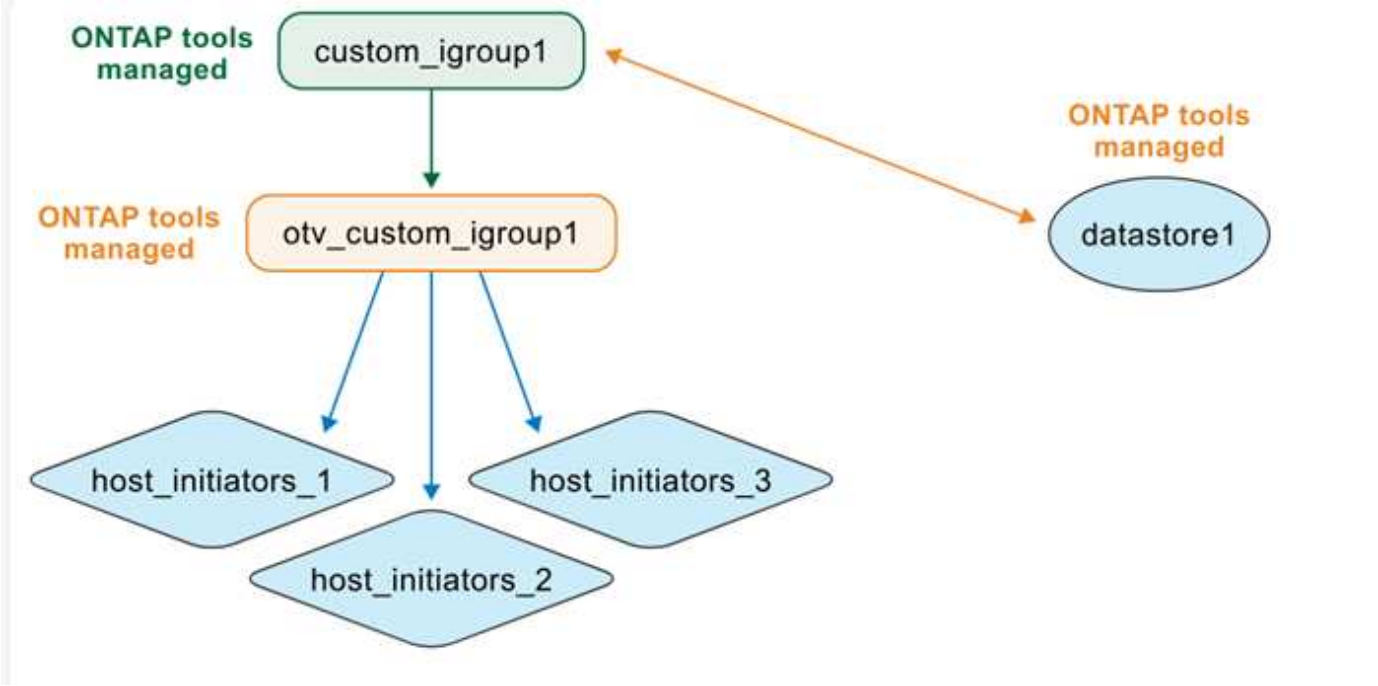
Dieser Vorgang kann auch mithilfe der API durchgeführt werden. Um eine vorhandene Igroup während der Datenspeichererstellung wiederzuverwenden, geben Sie die Igroup-UUID in der Nutzlast der API-Anforderung an.

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

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



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



Sie können einen Datenspeicher direkt im vCenter Server erstellen und ihn später unter die Verwaltung der ONTAP -Tools stellen. Erstellen Sie zunächst eine flache igroup in ONTAP -Systemen und ordnen Sie ihr eine LUN zu. Nach dem Ausführen der Datenspeichererkennung in ONTAP -Tools wird die flache Igroup in eine verschachtelte Struktur konvertiert. ONTAP -Tools verwalten dann die igroup und benennen sie mit dem Präfix „otv_“ um. Die LUN bleibt während des gesamten Vorgangs derselben Igroup zugeordnet.

Wie ONTAP -Tools nativ erstellte igroups wiederverwenden

Sie können einen Datenspeicher in ONTAP -Tools mithilfe einer ursprünglich in ONTAP Systemen erstellten Igroup bereitstellen, nachdem diese von ONTAP -Tools verwaltet wurde. Diese Igroups werden in der Dropdown-Liste mit den benutzerdefinierten Initiatorgruppennamen angezeigt. Die neue LUN für den Datenspeicher wird dann der entsprechenden normalisierten untergeordneten Igroup zugeordnet, beispielsweise „otv_NativeIgroup1“.

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

Aktivieren Sie ONTAP tools for VMware vSphere -Dienste

Sie können das Administratorkennwort mit dem ONTAP Tools Manager ändern, um Dienste wie den VASA Provider, den Import der vVols Konfiguration und die Notfallwiederherstellung (SRA) mit dem ONTAP Tools Manager zu aktivieren.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie im Übersichtsbereich **Geräteeinstellungen bearbeiten**.
4. Im Abschnitt **Dienste** können Sie optionale Dienste wie VASA Provider, Import der vVols Konfiguration und Disaster Recovery (SRA) je nach Bedarf aktivieren.

Wenn Sie die Dienste zum ersten Mal aktivieren, müssen Sie die VASA-Provider- und SRA-Anmeldeinformationen erstellen. Diese werden verwendet, um den VASA-Provider und die SRA-Dienste auf dem vCenter Server zu registrieren oder zu aktivieren. Der Benutzername darf nur Buchstaben, Zahlen und Unterstriche enthalten. Die Passwortlänge sollte zwischen 8 und 256 Zeichen liegen.

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

Die Option **Import der vVols -Konfiguration zulassen** wird nur angezeigt, wenn der VASA-Provider-Dienst aktiviert ist. Diese Option ermöglicht die vVols Datenmigration von ONTAP Tools 9.xx zu ONTAP Tools 10.4.

Ändern Sie die ONTAP tools for VMware vSphere Konfiguration

Skalieren Sie mithilfe des ONTAP Tools Manager die ONTAP tools for VMware vSphere -Konfiguration, um die Anzahl der Knoten in der Bereitstellung zu erhöhen oder die Konfiguration auf High Availability (HA)-Setup zu ändern. Die ONTAP tools for VMware vSphere Appliance werden zunächst in einer Einzelknoten-Konfiguration ohne Hochverfügbarkeit bereitgestellt.

Um zu HA zu migrieren, wenn die Nicht-HA-Sicherung aktiviert ist, deaktivieren Sie zuerst die Sicherung und aktivieren Sie sie nach der Migration erneut.

Bevor Sie beginnen

- Stellen Sie sicher, dass Ihre OVA-Vorlage dieselbe OVA-Version wie Knoten 1 hat. Knoten 1 ist der Standardknoten, auf dem die ONTAP tools for VMware vSphere OVA zunächst bereitgestellt werden.
- Stellen Sie sicher, dass CPU-Hot-Add und Speicher-Hot-Plug aktiviert sind.
- Legen Sie im vCenter Server die Automatisierungsebene des Disaster Recovery Service (DRS) auf „teilweise automatisiert“ fest. Stellen Sie nach der Bereitstellung von HA die vollständige Automatisierung wieder her.
- Knoten-Hostnamen im HA-Setup sollten in Kleinbuchstaben geschrieben sein.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie im Übersichtsbereich **Geräteeinstellungen bearbeiten**.
4. Im Abschnitt **Konfiguration** können Sie die Knotengröße erhöhen und die HA-Konfiguration entsprechend Ihren Anforderungen aktivieren. Sie benötigen die vCenter Server-Anmeldeinformationen, um Änderungen vorzunehmen.

   Wenn sich die ONTAP Tools in der HA-Konfiguration befinden, können Sie die Details der Inhaltsbibliothek ändern. Für die neue Bearbeitungsübermittlung sollten Sie das Passwort erneut eingeben.

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

5. Verwenden Sie die HA-Umschalttaste, um die HA-Konfiguration zu aktivieren. Stellen Sie auf der Seite **HA-Einstellungen** Folgendes sicher:
   - Die Inhaltsbibliothek gehört zum selben vCenter Server, auf dem die Knoten-VMs der ONTAP Tools ausgeführt werden. Die vCenter Server-Anmeldeinformationen werden zum Validieren und Herunterladen der OVA-Vorlage für Appliance-Änderungen verwendet.
   - Die virtuelle Maschine, auf der die ONTAP Tools gehostet werden, wird nicht direkt auf einem ESXi-Host bereitgestellt. Die VM sollte auf einem Cluster oder einem Ressourcenpool bereitgestellt werden.

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

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

   Zur Vereinfachung des Arbeitsablaufs sind die meisten Eingabeoptionen bereits mit Netzwerkdetails zu Knoten 1 ausgefüllt. Sie können die Eingabedaten jedoch bearbeiten, bevor Sie zur letzten Seite des Assistenten navigieren. Sie können IPv6-Adressdetails für die anderen beiden Knoten nur eingeben, wenn die IPv6-Adresse auf dem ersten Knoten aktiviert ist.

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

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

Wie geht es weiter?

Auf der Seite **Übersicht** wird der Status der Bereitstellung angezeigt. Mithilfe der Job-ID können Sie den Status des Jobs zum Bearbeiten der Geräteeinstellungen auch in der Jobansicht verfolgen.

Wenn die HA-Bereitstellung fehlschlägt und der Status des neuen Knotens als „Neu“ angezeigt wird, löschen Sie die neue VM im vCenter, bevor Sie den Vorgang zum Aktivieren von HA erneut versuchen.

Auf der Registerkarte **Warnungen** im linken Bereich werden Warnungen für ONTAP tools for VMware vSphere aufgelistet.

Verwalten von Datenspeichern

Mounten Sie NFS- und VMFS-Datenspeicher

Durch das Mounten eines Datenspeichers wird Speicherzugriff auf zusätzliche Hosts bereitgestellt. Sie können den Datenspeicher auf den zusätzlichen Hosts mounten, nachdem Sie die Hosts zu Ihrer VMware-Umgebung hinzugefügt haben.

Informationen zu diesem Vorgang

- Einige Rechtsklickaktionen sind je nach vSphere-Clientversion und ausgewähltem Datenspeichertyp

deaktiviert oder nicht verfügbar.

  - Wenn Sie vSphere Client 8.0 oder eine spätere Version verwenden, sind einige der Rechtsklickoptionen ausgeblendet.
  - Von vSphere 7.0U3 bis vSphere 8.0 wird die Aktion deaktiviert, obwohl die Optionen angezeigt werden.

- Die Option zum Einbinden des Datenspeichers ist deaktiviert, wenn der Hostcluster mit einheitlichen Konfigurationen geschützt ist.

Schritte

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

Wie geht es weiter?

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

NFS- und VMFS-Datenspeicher aushängen

Mit der Aktion „Datenspeicher aushängen“ wird die Bereitstellung eines NFS- oder VMFS-Datenspeichers von ESXi-Hosts aufgehoben. Die Aktion „Datenspeicher aushängen“ ist für NFS- und VMFS-Datenspeicher aktiviert, die von den 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**.

   Ein Dialogfeld wird geöffnet und listet die ESXi-Hosts auf, auf denen der Datenspeicher gemountet ist. Wenn der Vorgang auf einem geschützten Datenspeicher ausgeführt wird, wird eine Warnmeldung auf dem Bildschirm angezeigt.

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

   Sie können den Datenspeicher nicht von allen Hosts aushängen. Die Benutzeroberfläche schlägt vor, dass Sie stattdessen den Vorgang zum Löschen des Datenspeichers verwenden.

4. Wählen Sie die Schaltfläche **Aushängen**.

   Wenn der Datenspeicher Teil eines geschützten Hostclusters ist, wird eine Warnmeldung angezeigt.

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

Wie geht es weiter?

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

Mounten Sie einen vVols Datenspeicher

Sie können einen VMware Virtual Volumes (vVols)-Datenspeicher auf einem oder mehreren zusätzlichen Hosts bereitstellen, um zusätzlichen Hosts Speicherzugriff zu gewähren. Sie können den vVols Datenspeicher nur über die APIs aushängen.

Schritte

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

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

Größe des NFS- und VMFS-Datenspeichers ändern

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

Über diese Aufgabe

Sie können nur die Größe eines NFS- und VMFS-Datenspeichers erhöhen. Ein FlexVol volume , das Teil eines NFS- und VMFS-Datenspeichers ist, kann nicht unter die vorhandene Größe schrumpfen, kann aber um maximal 120 % wachsen.

Schritte

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

Erweitern Sie vVols Datenspeicher

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

Der Vorgang „vVols Datenspeicher erweitern“ ist für vVols -Datenspeicher auf Basis des ASA R2-Systems nicht anwendbar.

Schritte

1. Wählen Sie auf der Startseite des vSphere-Clients **Hosts und Cluster** aus.

2. Wählen Sie im Navigationsbereich das Rechenzentrum aus, das den Datenspeicher enthält.
3. Klicken Sie mit der rechten Maustaste auf den Datenspeicher und wählen Sie * NetApp ONTAP -Tools* > **Speicher zum Datenspeicher hinzufügen**.
4. Im Fenster „Volumes erstellen oder auswählen“ können Sie entweder neue Volumes erstellen oder aus den vorhandenen Volumes auswählen. Die Benutzeroberfläche ist selbsterklärend. Befolgen Sie die Anweisungen Ihrer Wahl.
5. Überprüfen Sie im Fenster **Zusammenfassung** die Auswahl und wählen Sie **Erweitern**. Sie können den Fortschritt im Bereich „Letzte Aufgaben“ verfolgen.

Verkleinern Sie den vVols Datenspeicher

Die Aktion „Datenspeicher löschen“ löscht den Datenspeicher, wenn sich auf dem ausgewählten Datenspeicher keine vVols befinden.

Der Vorgang zum Verkleinern des vVols Datenspeichers wird für den auf dem ASA R2-System basierenden vVols Datenspeicher nicht unterstützt.

Schritte

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

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

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

Datenspeicher löschen

Die Aktion „Speicher aus Datenspeicher entfernen“ wird auf allen ONTAP tools for VMware vSphere erkannte oder verwaltete vVols -Datenspeicher im vCenter Server unterstützt. Diese Aktion ermöglicht das Entfernen von Volumes aus den vVols Datenspeichern.

Die Option zum Entfernen ist deaktiviert, wenn sich auf einem bestimmten Volume vVols befinden. Zusätzlich zum Entfernen von Volumes aus dem Datenspeicher können Sie das ausgewählte Volume im ONTAP -Speicher löschen.

Die Aufgabe „Datastore löschen“ aus den ONTAP tools for VMware vSphere im vCenter Server führt Folgendes aus:

- Hängt den vVol-Container ab.
- Bereinigt igroup. Wenn igroup nicht verwendet wird, wird iqn aus igroup entfernt.
- Löscht den Vvol-Container.

- Belässt die Flex-Volumes auf dem Speicherarray.

Führen Sie die folgenden Schritte aus, um NFS-, VMFS- oder vVOL-Datenspeicher aus ONTAP -Tools vom vCenter Server zu löschen:

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem, einen Hostcluster oder ein Rechenzentrum und wählen Sie * NetApp ONTAP Tools* > **Datenspeicher löschen**.

   Sie können die Datenspeicher nicht löschen, wenn dieser Datenspeicher von virtuellen Maschinen verwendet wird. Sie müssen die virtuellen Maschinen in einen anderen Datenspeicher verschieben, bevor Sie den Datenspeicher löschen. Sie können das Kontrollkästchen „Volume löschen“ nicht aktivieren, wenn der Datenspeicher zu einem geschützten Hostcluster gehört.

   a. Bei NFS- oder VMFS-Datenspeichern wird ein Dialogfeld mit der Liste der VMs angezeigt, die den Datenspeicher verwenden.
   b. Wenn der VMFS-Datenspeicher auf ASA R2-Systemen erstellt wird und Teil des Schutzes ist, müssen Sie den Schutz des Datenspeichers aufheben, bevor Sie ihn löschen.
   c. Bei vVols -Datenspeichern löscht die Aktion „Datenspeicher löschen“ den Datenspeicher nur, wenn ihm keine vVols zugeordnet sind. Das Dialogfeld „Datenspeicher löschen“ bietet eine Option zum Löschen von Volumes aus dem ONTAP Cluster.
   d. Bei vVols -Datenspeichern auf Basis von ASA R2-Systemen ist das Kontrollkästchen zum Löschen der Sicherungsvolumes nicht anwendbar.
3. Um die Sicherungsvolumes auf dem ONTAP Speicher zu löschen, wählen Sie **Volumes auf dem ONTAP Cluster löschen**.

   Sie können das Volume auf dem ONTAP Cluster für einen VMFS-Datenspeicher, der Teil des geschützten Hostclusters ist, nicht löschen.

ONTAP Speicheransichten für Datenspeicher

ONTAP tools for VMware vSphere zeigen die ONTAP Speicherseitenansicht der Datenspeicher und ihrer Volumes auf der Registerkarte „Konfigurieren“.

Schritte

1. Navigieren Sie vom vSphere-Client zum Datenspeicher.
2. Wählen Sie im rechten Bereich die Registerkarte **Konfigurieren**.
3. Wählen Sie * NetApp ONTAP -Tools* > * ONTAP Speicher*. Je nach Datenspeichertyp ändert sich die Ansicht. Weitere Informationen finden Sie in der folgenden Tabelle:

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 Details zum Speicher-Backend, Aggregat, Volume und zur Speicherverfügbarkeitszone (SAZ). Die Seite **Lagereinheitendetails** enthält Details zur Lagereinheit.
vVols -Datenspeicher	Listet alle Bände auf. Sie können Speicher im ONTAP Speicherbereich erweitern oder entfernen. Diese Ansicht wird für den auf dem ASA R2-System basierenden vVols Datenspeicher nicht unterstützt.

Speicheransicht der virtuellen Maschine

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

Diese Ansicht ist für die VM anwendbar, auf der mindestens eine mit ONTAP tools for VMware vSphere verwaltete vVols Datenspeicher verbundene Festplatte gemountet ist.

Schritte

1. Navigieren Sie vom vSphere-Client zur virtuellen Maschine.
2. Wählen Sie im rechten Bereich die Registerkarte **Monitor**.
3. Wählen Sie * NetApp ONTAP -Tools* > **Speicher**. Die **Speicher**-Details werden im rechten Bereich angezeigt. Sie können die Liste der auf der VM vorhandenen vVols sehen.

   Mit der Option „Spalten verwalten“ können Sie verschiedene Spalten ausblenden oder anzeigen.

Verwalten von Speicherschwellenwerten

Sie können den Schwellenwert festlegen, um Benachrichtigungen in vCenter Server zu erhalten, wenn das Volume und die Gesamtkapazität bestimmte Werte erreichen.

Schritte:

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie auf der Verknüpfungsseite im Abschnitt „Plug-ins“ die Option „NetApp ONTAP Tools“ aus.
3. Navigieren Sie im linken Bereich der ONTAP -Tools zu **Einstellungen** > **Schwellenwerteinstellungen** > **Bearbeiten**.
4. Geben Sie im Fenster **Schwellenwert bearbeiten** die gewünschten Werte in die Felder **Fast voll** und **Voll** ein und wählen Sie **Speichern**. Sie können die Zahlen auf die empfohlenen Werte zurücksetzen, nämlich 80 für „Fast voll“ und 90 für „voll“.

Verwalten von Speicher-Backends

Speicher-Backends sind Systeme, die die ESXi-Hosts zur Datenspeicherung verwenden.

Entdecken Sie Speicher

Sie können die Erkennung eines Speicher-Backends bei Bedarf ausführen, ohne auf eine geplante Erkennung zur Aktualisierung der Speicherdetails warten zu müssen.

Befolgen Sie die folgenden Schritte, um die Speicher-Backends zu ermitteln.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie auf der Verknüpfungsseite im Abschnitt „Plug-ins“ die Option „NetApp ONTAP Tools“ aus.
3. Navigieren Sie im linken Bereich der ONTAP -Tools zu **Storage Backends** und wählen Sie ein Storage Backend aus.
4. Wählen Sie das vertikale Auslassungsmenü und wählen Sie **Speicher entdecken**

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

Speicher-Backends ändern

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

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie auf der Verknüpfungsseite im Abschnitt „Plug-ins“ die Option „NetApp ONTAP Tools“ aus.
3. Navigieren Sie im linken Bereich der ONTAP -Tools zu **Storage Backends** und wählen Sie ein Storage Backend aus.
4. Wählen Sie das vertikale Auslassungsmenü und wählen Sie **Ändern**, um die Anmeldeinformationen oder den Portnamen zu ändern. Sie können den Fortschritt im Bereich „Letzte Aufgaben“ verfolgen.

Sie können den Änderungsvorgang für globale ONTAP Cluster mithilfe des ONTAP Tools Manager mit den folgenden Schritten durchführen.

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie Speicher-Backends aus der Seitenleiste aus.
4. Wählen Sie das Speicher-Backend aus, das Sie ändern möchten.
5. Wählen Sie das vertikale Auslassungsmenü und wählen Sie **Ändern**.
6. Sie können die Anmeldeinformationen oder den Port ändern. Geben Sie den **Benutzernamen** und das **Passwort** ein, um das Speicher-Backend zu ändern.

Entfernen von Speicher-Backends

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

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie auf der Verknüpfungsseite im Abschnitt „Plug-ins“ die Option „NetApp ONTAP Tools“ aus.
3. Navigieren Sie im linken Bereich der ONTAP -Tools zu **Storage Backends** und wählen Sie ein Storage

Backend aus.

4. Wählen Sie das vertikale Auslassungsmenü und wählen Sie **Entfernen**. Stellen Sie sicher, dass das Speicher-Backend keine Datenspeicher enthält. Sie können den Fortschritt im Bereich „Letzte Aufgaben“ verfolgen.

Sie können den Entfernungsvorgang für globale ONTAP Cluster mit dem ONTAP Tools Manager durchführen.

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **Storage Backends** aus der Seitenleiste.
4. Wählen Sie das Speicher-Backend aus, das Sie entfernen möchten
5. Wählen Sie das vertikale Auslassungsmenü und wählen Sie **Entfernen**.

Drilldown-Ansicht des Speicher-Backends

Auf der Speicher-Backend-Seite sind alle Speicher-Backends aufgelistet. Sie können Speichererkennungs-, Änderungs- und Entfernungsvorgänge auf den von Ihnen hinzugefügten Speicher-Backends durchführen und nicht auf den einzelnen untergeordneten SVMs unter dem Cluster.

Wenn Sie unter dem Speicher-Backend entweder den übergeordneten Cluster oder den untergeordneten Cluster auswählen, können Sie die Gesamtübersicht der Komponente sehen. Wenn Sie den übergeordneten Cluster auswählen, wird Ihnen das Dropdown-Menü „Aktionen“ angezeigt, in dem Sie die Vorgänge zum Erkennen, Ändern und Entfernen von Speicher ausführen können.

Die Übersichtsseite enthält die folgenden Details:

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

Die Registerkarte „Schnittstelle“ bietet detaillierte Informationen zur Schnittstelle.

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

Verwalten von vCenter Server-Instanzen

vCenter Server-Instanzen sind zentrale Verwaltungsplattformen, mit denen Sie Hosts, virtuelle Maschinen und Speicher-Backends steuern können.

Trennen Sie Speicher-Backends von der vCenter Server-Instanz

Auf der vCenter Server-Listenseite wird die zugehörige Anzahl von Speicher-Backends angezeigt. Jede vCenter Server-Instanz verfügt über die Möglichkeit, die Verbindung zu einem Speicher-Backend herzustellen oder die Verbindung zu trennen.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie die erforderliche vCenter Server-Instanz aus der Seitenleiste aus.
4. Wählen Sie die vertikalen Auslassungspunkte neben dem vCenter Server aus, den Sie mit Speicher-Backends verknüpfen oder von dem Sie die Verknüpfung aufheben möchten.
5. Wählen Sie **Speicher-Backend trennen**.

Ändern einer vCenter Server-Instanz

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

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie die entsprechende vCenter Server-Instanz aus der Seitenleiste aus
4. Wählen Sie die vertikalen Auslassungspunkte neben dem vCenter Server aus, den Sie ändern möchten, und wählen Sie **Ändern**.
5. Ändern Sie die Details der vCenter Server-Instanz und wählen Sie **Ändern**.

Entfernen einer vCenter Server-Instanz

Sie müssen alle an den vCenter Server angeschlossenen Speicher-Backends entfernen, bevor Sie ihn entfernen.

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie die entsprechenden vCenter Server-Instanzen 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 sie nicht mehr von der Anwendung verwaltet.

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

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

Zertifikate verwalten

Während der Bereitstellung wird standardmäßig ein selbstsigniertes Zertifikat für ONTAP -Tools und VASA Provider generiert. Über die ONTAP Tools Manager-Schnittstelle können Sie das Zertifikat erneuern oder auf eine benutzerdefinierte Zertifizierungsstelle aktualisieren. Benutzerdefinierte CA-Zertifikate sind in einer Multi-vCenter-Bereitstellung obligatorisch.

Bevor Sie beginnen

- Der Domänenname, auf den das Zertifikat ausgestellt ist, sollte der virtuellen IP-Adresse zugeordnet werden.
- Führen Sie die nslookup-Prüfung für den Domänennamen aus, um zu überprüfen, ob die Domäne in die gewünschte IP-Adresse aufgelöst wird.
- Die Zertifikate sollten mit dem Domänennamen und der IP-Adresse des ONTAP Tools erstellt werden.

Die IP-Adresse eines ONTAP -Tools sollte einem vollqualifizierten Domänennamen (FQDN) zugeordnet sein. Zertifikate sollten im Betreff oder in alternativen Betreffnamen denselben FQDN enthalten, der der IP-Adresse der ONTAP Tools zugeordnet ist.

Sie können nicht von einem CA-signierten zu einem selbstsignierten Zertifikat wechseln.

Aktualisieren Sie das ONTAP Tools-Zertifikat

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

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere 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 „Erneuern“ ist verfügbar, wenn der Zertifikatstyp CA-signiert ist. Geben Sie im Popup-Fenster die Details zum Serverzertifikat, privaten Schlüssel, Stammzertifizierungsstelle und Zwischenzertifikat ein.

   Das System ist offline, bis das Zertifikat erneuert wird, und Sie werden von der ONTAP Tools Manager-Schnittstelle abgemeldet.

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

      Das System ist offline, bis das Upgrade abgeschlossen ist, und Sie werden von der ONTAP Tools Manager-Schnittstelle 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 Server-Instanz für vVols -Datenspeicher verwaltet werden. Wenn Sie mehrere vCenter Server-Instanzen verwalten und die vVols Funktion auf ihnen aktivieren möchten, müssen Sie das selbstsignierte Zertifikat in ein benutzerdefiniertes CA-Zertifikat ändern.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **Zertifikate** > **VASA-Anbieter** oder * ONTAP Tools* > **Erneuern**, um die Zertifikate zu erneuern.
4. Wählen Sie **Zertifikate** > **VASA-Anbieter** oder * ONTAP Tools* > **Upgrade auf CA**, um das selbstsignierte Zertifikat auf ein benutzerdefiniertes CA-Zertifikat zu aktualisieren.
   a. Laden Sie im Popup-Fenster das Serverzertifikat, den privaten Schlüssel des Serverzertifikats, das Stamm-CA-Zertifikat und die Zwischenzertifikatdateien hoch.

b. Geben Sie den Domänennamen ein, für den Sie dieses Zertifikat generiert haben, und aktualisieren Sie das Zertifikat.

Das System ist offline, bis das Upgrade abgeschlossen ist, und Sie werden von der ONTAP Tools Manager-Schnittstelle abgemeldet.

Zugriff auf ONTAP tools for VMware vSphere Wartungskonsole

Übersicht über ONTAP tools for VMware vSphere Wartungskonsole

Sie können Ihre Anwendungs-, System- und Netzwerkkonfigurationen mithilfe der Wartungskonsole der ONTAP Tools verwalten. Sie können Ihr Administratorkennwort und Ihr Wartungskennwort ändern. Sie können außerdem Support-Pakete erstellen, verschiedene Protokollebenen festlegen, TLS-Konfigurationen anzeigen und verwalten sowie Remote-Diagnosen starten.

Sie sollten VMware-Tools installiert haben, nachdem Sie die ONTAP tools for VMware vSphere bereitgestellt haben, um auf die Wartungskonsole zuzugreifen. Sie sollten verwenden `maint` als Benutzername und Kennwort, das Sie während der Bereitstellung konfiguriert haben, um sich bei der Wartungskonsole der ONTAP Tools anzumelden. Sie sollten **nano** zum Bearbeiten der Dateien in der Wartungs- oder Root-Anmeldekonsole verwenden.

Sie sollten ein Passwort festlegen für `diag` Benutzer beim Aktivieren der Ferndiagnose.

Sie sollten die Registerkarte **Zusammenfassung** Ihrer bereitgestellten ONTAP tools for VMware vSphere verwenden, um auf die Wartungskonsole zuzugreifen. Wenn Sie  , die Wartungskonsole wird gestartet.

Konsolenmenü	Optionen
Anwendungskonfiguration	1. Serverstatusübersicht anzeigen 2. LOG-Level für VASA-Provider-Dienste und SRA-Dienste ändern
Systemkonfiguration	1. Starten Sie die virtuelle Maschine neu 2. Virtuelle Maschine herunterfahren 3. Ändern Sie das Benutzerkennwort „maint“. 4. Zeitzone ändern 5. Größe der Jail-Festplatte erhöhen (/jail) 6. Upgrade 7. Installieren Sie VMware Tools

Netzwerkkonfiguration	1. IP-Adresseinstellungen anzeigen 2. Sucheinstellungen für Domänennamen anzeigen 3. Sucheinstellungen für Domänennamen ändern 4. Statische Routen anzeigen 5. Statische Routen ändern 6. Änderungen festschreiben 7. Pingen Sie einen Host an 8. Standardeinstellungen wiederherstellen
Support und Diagnose	1. Zugriff auf die Diagnose-Shell 2. Aktivieren Sie den Ferndiagnosezugriff 3. Geben Sie die vCenter-Anmeldeinformationen für die Sicherung an 4. Backup erstellen

Konfigurieren des Remotediagnosezugriffs

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

Bevor Sie beginnen

Die VASA Provider-Erweiterung sollte für Ihre vCenter Server-Instanz aktiviert sein.

Über diese Aufgabe

Die Verwendung von SSH für den Zugriff auf das Diagnose-Benutzerkonto unterliegt den folgenden Einschränkungen:

- Pro Aktivierung von SSH ist nur ein Anmeldekonto zulässig.
- Der SSH-Zugriff auf das Diagnose-Benutzerkonto wird deaktiviert, wenn eines der folgenden Ereignisse eintritt:
  - Die Zeit läuft ab.

    Die Anmeldesitzung bleibt nur bis Mitternacht des nächsten Tages gültig.
  - Sie melden sich erneut als Diag-Benutzer per SSH an.

Schritte

1. Öffnen Sie vom vCenter Server aus eine Konsole für den VASA-Anbieter.
2. Melden Sie sich als Wartungsbenutzer an.
3. Eingeben `4` , um Support und Diagnose auszuwählen.
4. Eingeben `2` , um Remote-Diagnosezugriff aktivieren auszuwählen.
5. Eingeben `y` im Dialogfeld „Bestätigung“, um den Ferndiagnosezugriff zu aktivieren.

6. Geben Sie ein Passwort für den Ferndiagnosezugriff ein.

Starten Sie SSH auf anderen Knoten

Sie müssen SSH auf anderen Knoten starten, bevor Sie ein Upgrade durchführen.

Bevor Sie beginnen

Die VASA Provider-Erweiterung sollte für Ihre vCenter Server-Instanz aktiviert sein.

Über diese Aufgabe

Führen Sie dieses Verfahren vor dem Upgrade auf jedem Knoten durch.

Schritte

1. Öffnen Sie vom vCenter Server aus eine Konsole für den VASA-Anbieter.
2. Melden Sie sich als Wartungsbenutzer an.
3. Eingeben `4` , um Support und Diagnose auszuwählen.
4. Eingeben `1` , um „Zugriff auf die Diagnose-Shell“ auszuwählen.
5. Eingeben `y` um fortzufahren.
6. Führen Sie den Befehl *sudo systemctl restart ssh* aus.

Aktualisieren Sie die vCenter Server- und ONTAP -Anmeldeinformationen

Sie können die vCenter Server-Instanz und die ONTAP Anmeldeinformationen mithilfe der Wartungskonsole aktualisieren.

Bevor Sie beginnen

Sie benötigen die Anmeldedaten eines Wartungsbenutzers.

Über diese Aufgabe

Wenn Sie die Anmeldeinformationen für vCenter Server, ONTAP oder Data LIF nach der Bereitstellung geändert haben, müssen Sie die Anmeldeinformationen mit diesem Verfahren aktualisieren.

Schritte

1. Öffnen Sie vom vCenter Server aus eine Konsole für den VASA-Anbieter.
2. Melden Sie sich als Wartungsbenutzer an.
3. Eingeben `2` , um das Systemkonfigurationsmenü auszuwählen.
4. Eingeben `9` um die ONTAP Anmeldeinformationen zu ändern.
5. Eingeben `10` um die vCenter-Anmeldeinformationen zu ändern.

ONTAP -Tools-Berichte

ONTAP tools for VMware vSphere Plug-in bieten Berichte für virtuelle Maschinen und Datenspeicher. Wenn Sie im Abschnitt „Verknüpfungen“ des vCenter-Clients das Plug-In-Symbol „NetApp ONTAP tools for VMware vSphere“ auswählen, navigiert die

Benutzeroberfläche zur Seite „Übersicht“. Wählen Sie die Registerkarte „Berichte“ aus, um den Bericht zur virtuellen Maschine und den Datenspeichern anzuzeigen.

Der Bericht „Virtuelle Maschinen“ zeigt die Liste der erkannten virtuellen Maschinen (sollte mindestens eine Festplatte aus ONTAP Speicher-basierten Datenspeichern haben) mit Leistungsmetriken. Wenn Sie den VM-Datensatz erweitern, werden alle datenträgerbezogenen Datenspeicherinformationen angezeigt.

Der Datastores-Bericht zeigt die Liste der erkannten oder erkannten ONTAP tools for VMware vSphere verwaltete Datastores, die vom ONTAP -Speicher-Backend aller Typen mit Leistungsmetriken bereitgestellt werden.

Mit der Option „Spalten verwalten“ können Sie verschiedene Spalten ausblenden oder anzeigen.

Erfassen der Protokolldateien

Sie können Protokolldateien für ONTAP tools for VMware vSphere über die in der Benutzeroberfläche des ONTAP Tools-Managers verfügbaren Optionen sammeln. Der technische Support bittet Sie möglicherweise, die Protokolldateien zu sammeln, um bei der Behebung eines Problems zu helfen.

Das Generieren von Protokollen aus dem ONTAP Tools Manager umfasst alle Protokolle für alle vCenter Server-Instanzen. Das Generieren von Protokollen über die Benutzeroberfläche des vCenter-Clients ist auf den ausgewählten vCenter-Server beschränkt.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **Protokollpakete** aus der Seitenleiste.

   Dieser Vorgang kann mehrere Minuten dauern.

4. Wählen Sie **Generieren**, um die Protokolldateien zu generieren.
5. Geben Sie die Bezeichnung für das Protokollpaket ein und wählen Sie **Generieren**.

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

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

Schritte

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

Das generierte Protokollpaket ersetzt das Protokollpaket, das innerhalb der letzten 3 Tage oder 72 Stunden generiert wurde.

Verwalten virtueller Maschinen

Überlegungen zum Migrieren oder Klonen virtueller Maschinen

Bei der Migration vorhandener virtueller Maschinen in Ihrem Rechenzentrum sollten Sie sich einiger Überlegungen bewusst sein.

Migrieren geschützter virtueller Maschinen

Sie können die geschützten virtuellen Maschinen migrieren nach:

- Gleicher vVols Datenspeicher auf einem anderen ESXi-Host
- Unterschiedlicher kompatibler vVols Datenspeicher im selben ESXi-Host
- Anderer kompatibler vVols Datenspeicher in einem anderen ESXi-Host

Wenn die virtuelle Maschine auf ein anderes FlexVol volume migriert wird, wird auch die entsprechende Metadatendatei mit den Informationen zur virtuellen Maschine aktualisiert. Wenn eine virtuelle Maschine auf einen anderen ESXi-Host, aber denselben Speicher migriert wird, wird die zugrunde liegende Metadatendatei des FlexVol volume nicht geändert.

Klonen Sie geschützte virtuelle Maschinen

Sie können geschützte virtuelle Maschinen wie folgt klonen:

- Gleicher Container desselben FlexVol volume unter Verwendung einer Replikationsgruppe

  Die Metadatendatei desselben FlexVol Volumes wird mit den Details der geklonten virtuellen Maschine aktualisiert.

- Gleicher Container eines anderen FlexVol volume mit Replikationsgruppe

  Das FlexVol volume , auf dem die geklonte virtuelle Maschine platziert wird, die Metadatendatei wird mit den Details der geklonten virtuellen Maschine aktualisiert.

- Anderer Container oder vVols -Datenspeicher

  Das FlexVol volume , auf dem die geklonte virtuelle Maschine platziert ist, die Metadatendatei erhält aktualisierte Details der virtuellen Maschine.

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

Clone-of-Clone einer geschützten virtuellen Maschine wird unterstützt.

Siehe "Erstellen einer virtuellen Maschine zum Klonen" für weitere Details.

Snapshots virtueller Maschinen

Derzeit werden nur Snapshots virtueller Maschinen ohne Speicher unterstützt. Wenn die virtuelle Maschine über einen Snapshot mit Speicher verfügt, wird die virtuelle Maschine für den Schutz nicht berücksichtigt.

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

Wenn Sie bei einer Windows-VM mit dem Speichertyp ASA R2 einen Snapshot der virtuellen Maschine erstellen, handelt es sich um einen schreibgeschützten Snapshot. Wenn für die VM Strom angefordert wird, erstellt der VASA-Anbieter mithilfe des schreibgeschützten Snapshots eine LUN und aktiviert sie dann für IOPS. Während der Ausschaltanforderung löscht der VASA-Anbieter die erstellte LUN und deaktiviert dann die IOPS.

Migrieren Sie virtuelle Maschinen mit NFS- und VMFS-Datenspeichern zu vVols -Datenspeichern

Sie können virtuelle Maschinen von NFS- und VMFS-Datenspeichern in Virtual Volumes (vVols)-Datenspeicher migrieren, um die Vorteile der richtlinienbasierten VM-Verwaltung und anderer vVols Funktionen zu nutzen. Mit vVols Datenspeichern können Sie erhöhte Arbeitslastanforderungen erfüllen.

Bevor Sie beginnen

Stellen Sie sicher, dass VASA Provider auf keiner der virtuellen Maschinen ausgeführt wird, die Sie migrieren möchten. Wenn Sie eine virtuelle Maschine, auf der VASA Provider ausgeführt wird, zu einem vVols Datenspeicher migrieren, können Sie keine Verwaltungsvorgänge durchführen, einschließlich des Einschaltens der virtuellen Maschinen, die sich auf vVols Datenspeichern befinden.

Über diese Aufgabe

Wenn Sie von einem NFS- und VMFS-Datenspeicher zu einem vVols -Datenspeicher migrieren, verwendet der vCenter Server beim Verschieben von Daten aus VMFS-Datenspeichern vStorage APIs for Array Integration (VAAI)-Offloads, jedoch nicht aus einer NFS-VMDK-Datei. VAAI-Offloads reduzieren normalerweise die Belastung des Hosts.

Schritte

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

VASA-Bereinigung

Führen Sie die VASA-Bereinigung mit den Schritten in diesem Abschnitt durch.

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

Schritte

1. Heben Sie die Registrierung des Plug-Ins auf, indem Sie in https://OTV_IP:8143/Register.html gehen.
2. Stellen Sie sicher, dass das Plug-In auf dem vCenter Server nicht mehr verfügbar ist.
3. Fahren Sie die ONTAP tools for VMware vSphere VM herunter.
4. Löschen Sie ONTAP tools for VMware vSphere VM.

Anfügen oder Trennen eines Datenträgers an eine virtuelle Maschine

Anfügen eines Datenträgers an eine virtuelle Maschine

Schließen Sie eine Datenfestplatte an eine virtuelle Maschine an, um die Speicherkapazität zu erweitern.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Klicken Sie mit der rechten Maustaste auf eine virtuelle Maschine im Inventar und wählen Sie **Einstellungen bearbeiten**.
3. Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **Vorhandene Festplatte** aus.
4. Wählen Sie die virtuelle Maschine aus, auf der sich die Festplatte befindet.
5. Wählen Sie die Festplatte aus, die Sie anschließen möchten, und wählen Sie **OK**

Ergebnis

Die Festplatte wird in der Liste der virtuellen Hardwaregeräte angezeigt.

Trennen Sie einen Datenträger von der virtuellen Maschine

Sie können eine an eine virtuelle Maschine angeschlossene Datenfestplatte trennen, wenn sie nicht mehr benötigt wird. Wenn Sie die Festplatte von der virtuellen Maschine trennen, wird sie nicht automatisch gelöscht; sie verbleibt auf dem ONTAP Speichersystem.

Schritte

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

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

Ähnliche Informationen

"Hinzufügen einer neuen Festplatte zu einer virtuellen Maschine"

"Hinzufügen einer vorhandenen Festplatte zu einer virtuellen Maschine"

Entdecken Sie Speichersysteme und Hosts

Wenn Sie ONTAP tools for VMware vSphere zum ersten Mal in einem vSphere-Client ausführen, erkennen ONTAP -Tools die ESXi-Hosts, ihre LUNs und NFS-Exporte sowie die NetApp -Speichersysteme, denen diese LUNs und Exporte gehören.

Bevor Sie beginnen

- Alle ESXi-Hosts sollten eingeschaltet und verbunden sein.
- Alle zu erkennenden virtuellen Speichermaschinen (SVMs) sollten ausgeführt werden und für jeden Clusterknoten sollte mindestens ein Daten-LIF für das verwendete Speicherprotokoll (NFS oder iSCSI) konfiguriert sein.

Über diese Aufgabe

Sie können neue Speichersysteme entdecken oder Informationen zu vorhandenen Speichersystemen aktualisieren, um jederzeit die neuesten Kapazitäts- und Konfigurationsinformationen zu erhalten. Sie können auch die Anmeldeinformationen ändern, die ONTAP tools for VMware vSphere zum Anmelden bei den Speichersystemen verwenden.

Beim Erkennen der Speichersysteme erfassen ONTAP tools for VMware vSphere Informationen von den ESXi-Hosts, die von der vCenter Server-Instanz verwaltet werden.

Schritte

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

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

3. Wählen Sie die erkannten Speichercontroller mit dem Status `Authentication Failure` und wählen Sie **Aktionen** > **Ändern**.
4. Geben Sie die erforderlichen Informationen in das Dialogfeld **Speichersystem ändern** ein.
5. Wiederholen Sie die Schritte 4 und 5 für alle Speichercontroller mit `Authentication Failure` Status.

Führen Sie nach Abschluss des Erkennungsprozesses die folgenden Aktionen aus:

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

Ändern Sie die ESXi-Hosteinstellungen mit ONTAP -Tools

Sie können das Dashboard der ONTAP tools for VMware vSphere verwenden, um Ihre ESXi-Hosteinstellungen zu bearbeiten.

Bevor Sie beginnen

Wenn ein Problem mit Ihren ESXi-Hosteinstellungen vorliegt, wird das Problem im ESXi-Hostsystem-Portlet des Dashboards angezeigt. Sie können das Problem auswählen, um den Hostnamen oder die IP-Adresse des ESXi-Hosts anzuzeigen, bei dem das Problem auftritt.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Wählen Sie auf der Verknüpfungsseite im Abschnitt „Plug-ins“ die Option „NetApp ONTAP Tools“ aus.
3. Gehen Sie zum Portlet **ESXi Host Compliance** in der Übersicht (Dashboard) der ONTAP tools for VMware vSphere Plug-In.
4. Wählen Sie den Link **Empfohlene Einstellungen anwenden**.
5. Wählen Sie im Fenster **Empfohlene Hosteinstellungen anwenden** die Hosts aus, die den von NetApp empfohlenen Hosteinstellungen entsprechen sollen, und wählen Sie **Weiter**.

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

6. Wählen Sie auf der Einstellungsseite nach Bedarf die empfohlenen Werte aus.
7. Überprüfen Sie im Übersichtsbereich die Werte und wählen Sie **Fertig**. Sie können den Fortschritt im Bereich „Letzte Aufgaben“ verfolgen.

Ähnliche Informationen

"Konfigurieren der ESXi-Hosteinstellungen"

Passwörter verwalten

Kennwort für den ONTAP Tools Manager ändern

Sie können das Administratorkennwort mit dem ONTAP Tools Manager ändern.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie das **Administrator**-Symbol in der oberen rechten Ecke des Bildschirms und wählen Sie **Passwort ändern**.
4. Geben Sie im Popup-Fenster zum Ändern des Passworts das alte Passwort und die neuen Passwortdetails ein. Die Einschränkung zum Ändern des Passworts wird auf dem Bildschirm der Benutzeroberfläche angezeigt.
5. Wählen Sie **Ändern**, um die Änderungen zu implementieren.

Kennwort für den ONTAP Tools Manager zurücksetzen

Wenn Sie das Kennwort für den ONTAP Tools Manager vergessen haben, können Sie die Administratoranmeldeinformationen mithilfe des von den ONTAP tools for VMware vSphere Wartungskonsole generierten Tokens zurücksetzen.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Wählen Sie auf dem Anmeldebildschirm die Option **Passwort zurücksetzen**.

   Um das Managerkennwort zurückzusetzen, müssen Sie das Reset-Token mithilfe der ONTAP tools for VMware vSphere Wartungskonsole generieren.

   a. Öffnen Sie vom vCenter Server aus die Wartungskonsole
   b. Geben Sie „2“ ein, um die Option „Systemkonfiguration“ auszuwählen
   c. Geben Sie „3“ ein, um das Benutzerkennwort „maint“ zu ändern.
3. Geben Sie im Popup-Fenster zum Ändern des Kennworts das Token zum Zurücksetzen des Kennworts, den Benutzernamen und die neuen Kennwortdetails ein.
4. Wählen Sie **Zurücksetzen**, um die Änderungen zu übernehmen. Nach erfolgreicher Kennwortzurücksetzung können Sie sich mit dem neuen Kennwort anmelden.

Anwendungsbenutzerkennwort zurücksetzen

Das Anwendungsbenutzerkennwort wird für die SRA- und VASA-Provider-Registrierung bei vCenter Server verwendet.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **Einstellungen** in der Seitenleiste.
4. Wählen Sie im Bildschirm **VASA/SRA-Anmeldeinformationen** die Option **Passwort zurücksetzen**.
5. Geben Sie ein neues Passwort ein und bestätigen Sie die Eingabe des neuen Passworts.
6. Wählen Sie **Zurücksetzen**, um die Änderungen zu übernehmen.

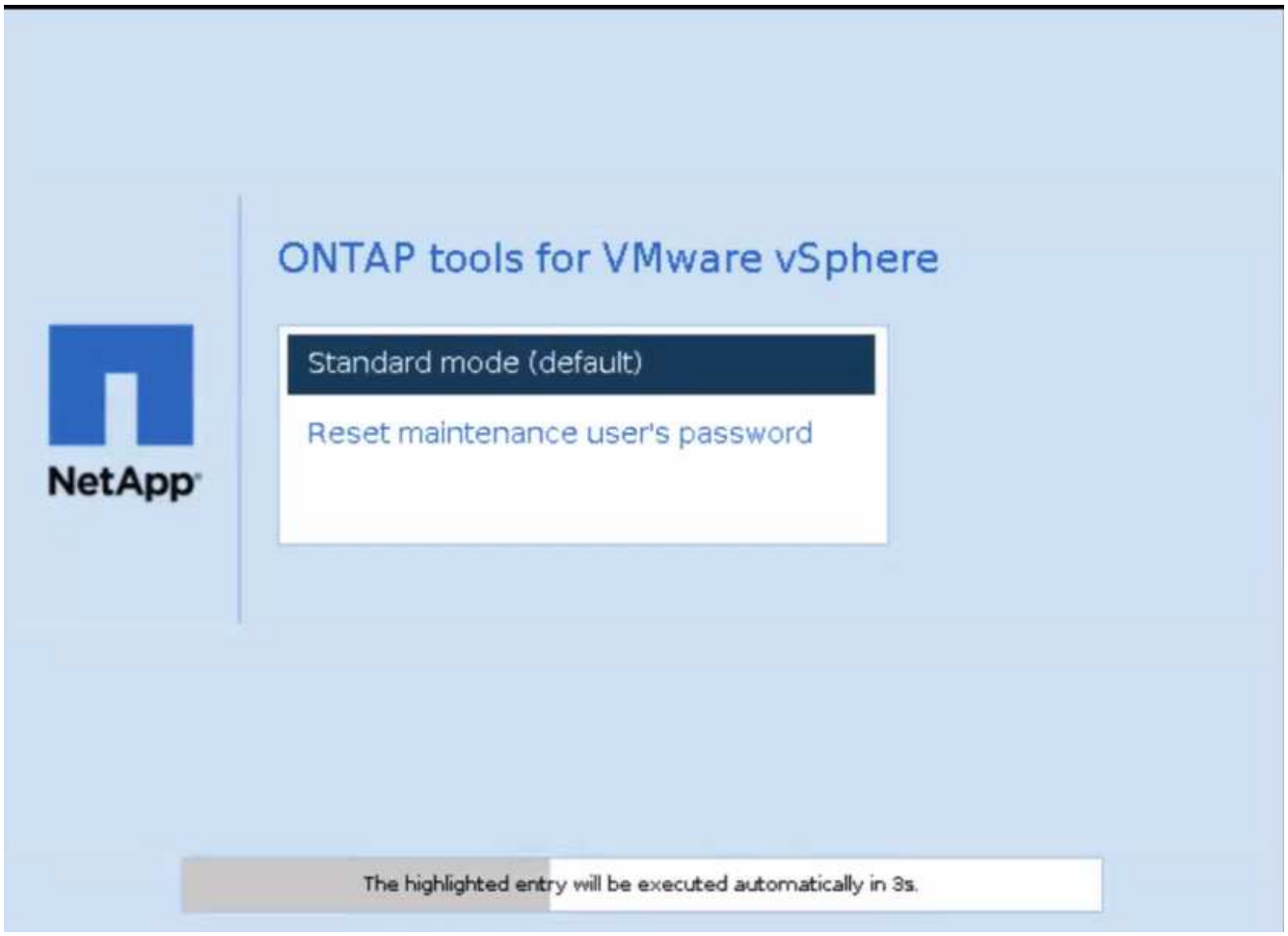
Benutzerkennwort der Wartungskonsole zurücksetzen

Während des Neustarts des Gastbetriebssystems wird im Grub-Menü eine Option zum Zurücksetzen des Benutzerkennworts der Wartungskonsole angezeigt. Mit dieser Option wird das Benutzerkennwort der Wartungskonsole auf der entsprechenden VM aktualisiert. Nach dem Zurücksetzen des Kennworts wird die VM neu gestartet, um das neue Kennwort festzulegen. Im HA-Bereitstellungsszenario wird das Kennwort nach dem Neustart der VM automatisch auf den beiden anderen VMs aktualisiert.

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

Schritte

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



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

3. Wählen Sie die Option **Passwort des Wartungsbenutzers zurücksetzen**. Die Wartungskonsole wird geöffnet.
4. Geben Sie in der Konsole die neuen Kennwortdetails ein. Um das Passwort erfolgreich zurücksetzen zu können, müssen die Angaben für das neue Passwort und die erneute Eingabe des neuen Passworts übereinstimmen. Sie haben drei Versuche, das richtige Passwort einzugeben. Nach erfolgreicher Eingabe des neuen Passworts wird das System neu gestartet.
5. Drücken Sie die Eingabetaste, um fortzufahren. Das Passwort wird auf der VM aktualisiert.

Das gleiche GRUB-Menü wird auch beim Einschalten der VM angezeigt. Sie sollten die Option zum Zurücksetzen des Kennworts jedoch nur mit der Option **Gastbetriebssystem neu starten** verwenden.

Verwalten des Hostclusterschutzes

Geschützten Hostcluster ändern

Im Rahmen des Änderungsschutzes können Sie folgende Aufgaben durchführen. Sie können alle Änderungen im selben Workflow durchführen.

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

Überwachen des Hostclusterschutzes

Verwenden Sie dieses Verfahren, um den Status des Hostclusterschutzes zu überwachen. Sie können jeden geschützten Hostcluster zusammen mit seinem Schutzstatus, den SnapMirror -Beziehungen, Datenspeichern und dem entsprechenden SnapMirror Status überwachen.

Schritte

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

   Das Symbol unter der Schutzspalte zeigt den Status des Schutzes an

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

Neue Datenspeicher oder Hosts hinzufügen

Verwenden Sie dieses Verfahren, um die neu hinzugefügten Datenspeicher oder Hosts zu schützen. Sie können dem geschützten Cluster neue Hosts hinzufügen oder mithilfe der nativen vCenter-Benutzeroberfläche neue Datenspeicher auf dem Hostcluster erstellen.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Um die Eigenschaften eines geschützten Clusters zu bearbeiten, können Sie entweder
   a. Navigieren Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**, wählen Sie das Auslassungsmenü neben dem Cluster und wählen Sie **Bearbeiten** oder
   b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie * NetApp ONTAP -Tools* > **Cluster schützen**.
3. Wenn Sie einen Datenspeicher in der nativen Benutzeroberfläche von vCenter erstellt haben, wird dieser Datenspeicher als ungeschützt angezeigt. Die Benutzeroberfläche zeigt alle Datenspeicher im Cluster und ihren Schutzstatus in einem Dialogfeld an. Wählen Sie die Schaltfläche **Schützen**, um den vollständigen Schutz zu aktivieren.
4. Wenn Sie einen neuen ESXi-Host hinzugefügt haben, wird der Schutzstatus als teilweise geschützt angezeigt. Wählen Sie das Auslassungsmenü unter den SnapMirror -Einstellungen und wählen Sie **Bearbeiten**, um die Nähe des neu hinzugefügten ESXi-Hosts festzulegen.

   Bei asynchronen Beziehungen wird die Bearbeitungsaktion nicht unterstützt, da Sie die Ziel-SVM für den tertiären Standort nicht derselben ONTAP -Tools-Instanz hinzufügen können. Sie können jedoch den Systemmanager oder die CLI der Ziel-SVM verwenden, um die Beziehungskonfiguration zu ändern.

5. Wählen Sie **Speichern**, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
6. Sie können die Änderungen im Fenster **Cluster schützen** sehen.

Eine vCenter-Aufgabe wird erstellt und Sie können den Fortschritt im Bereich **Letzte Aufgabe** verfolgen.

Fügen Sie eine neue SnapMirror -Beziehung hinzu

Schritte

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

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

Eine vCenter-Aufgabe wird erstellt und Sie können den Fortschritt im Bereich **Letzte Aufgabe** verfolgen.

Löschen einer bestehenden SnapMirror Beziehung

Um eine asynchrone SnapMirror -Beziehung zu löschen, muss ein sekundärer Site-SVM oder Cluster als Speicher-Backend auf ONTAP tools for VMware vSphere hinzugefügt werden. Sie können nicht alle SnapMirror -Beziehungen löschen. Wenn Sie eine Beziehung löschen, wird auch die entsprechende Beziehung im ONTAP Cluster entfernt. Wenn Sie eine AutomatedFailOverDuplex SnapMirror -Beziehung löschen, wird die Zuordnung der Datenspeicher auf dem Ziel aufgehoben und Konsistenzgruppe, LUNs, Volumes und igroups werden aus dem ONTAP Zielcluster entfernt.

Das Löschen der Beziehung löst einen erneuten Scan auf der sekundären Site aus, 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. Navigieren Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**, wählen Sie das Auslassungsmenü neben dem Cluster und wählen Sie **Bearbeiten** oder
   b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie * NetApp ONTAP -Tools* > **Cluster schützen**.
3. Wählen Sie das Auslassungsmenü unter den SnapMirror -Einstellungen und wählen Sie **Löschen**.

Eine vCenter-Aufgabe wird erstellt und Sie können den Fortschritt im Bereich **Letzte Aufgabe** verfolgen.

Ändern einer vorhandenen SnapMirror -Beziehung

Um eine asynchrone SnapMirror Beziehung zu ändern, sollte ein sekundärer Site-SVM oder Cluster als Speicher-Backend auf ONTAP tools for VMware vSphere hinzugefügt werden. Wenn es sich um eine AutomatedFailOverDuplex SnapMirror -Beziehung handelt, können Sie die Host-Nähe bei einheitlicher Konfiguration und den Host-Zugriff bei nicht einheitlicher Konfiguration ändern. Sie können die Richtlinientypen „Asynchronous“ und „AutomatedFailOverDuplex“ nicht austauschen. Sie können die Nähe oder den Zugriff für die neu erkannten Hosts im Cluster festlegen.

Sie können eine vorhandene asynchrone SnapMirror Beziehung nicht bearbeiten.

Schritte

1. Melden Sie sich beim vSphere-Client an.
2. Um die Eigenschaften eines geschützten Clusters zu bearbeiten, können Sie entweder
   a. Navigieren Sie zu * NetApp ONTAP Tools* > **Schutz** > **Host-Cluster-Beziehungen**, wählen Sie das Auslassungsmenü neben dem Cluster und wählen Sie **Bearbeiten** oder
   b. Klicken Sie mit der rechten Maustaste auf einen Hostcluster und wählen Sie * NetApp ONTAP -Tools* > **Cluster schützen**.
3. Wenn der Richtlinientyp „AutomatedFailOverDuplex“ ausgewählt ist, fügen Sie Details zur Hostnähe oder zum Hostzugriff hinzu.
4. Wählen Sie die Schaltfläche **Schützen**.

Eine vCenter-Aufgabe wird erstellt und Sie können den Fortschritt im Bereich **Letzte Aufgabe** verfolgen.

Entfernen des Hostclusterschutzes

Wenn Sie den Hostclusterschutz entfernen, sind die Datenspeicher nicht mehr geschützt.

Schritte

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

   Auf dieser Seite können Sie die geschützten Hostcluster zusammen mit ihrem Schutzstatus, der SnapMirror -Beziehung und dem entsprechenden SnapMirror Status überwachen.

2. Wählen Sie im Fenster **Hostclusterschutz** das Auslassungsmenü neben dem Cluster aus und wählen Sie dann **Schutz entfernen**.

AutoSupport deaktivieren

Wenn Sie Ihr Speichersystem zum ersten Mal konfigurieren, ist AutoSupport standardmäßig aktiviert. Es sendet 24 Stunden nach der Aktivierung Nachrichten an den technischen Support. Wenn Sie AutoSupport deaktivieren, erhalten Sie keinen proaktiven Support und keine Überwachung mehr.

Es wird empfohlen, AutoSupport aktiviert zu lassen. Es trägt dazu bei, die Problemerkennung und -lösung zu beschleunigen. Das System sammelt AutoSupport -Informationen und speichert sie lokal, auch wenn es deaktiviert ist. Der Bericht wird jedoch nicht an ein Netzwerk gesendet.

Schritte

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

Aktualisieren Sie die AutoSupport Proxy-URL

Aktualisieren Sie die AutoSupport -Proxy-URL, um die ordnungsgemäße Funktion der AutoSupport -Funktion in Szenarien sicherzustellen, in denen ein Proxyserver für die Netzwerkzugriffskontrolle oder Sicherheitsmaßnahmen verwendet wird. Es ermöglicht die Weiterleitung der AutoSupport -Daten über den entsprechenden Proxy und sorgt so für eine sichere Übertragung und Einhaltung der Vorschriften.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie **Einstellungen** in der Seitenleiste.
4. Wählen Sie die Option **Einstellungen** > **Telemetrie** > **Bearbeiten**.
5. Geben Sie eine gültige **Proxy-URL** ein und speichern Sie die Änderungen.

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

NTP-Server hinzufügen

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

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser:
   `https://<ONTAPtoolsIP>:8443/virtualization/ui/`
2. Melden Sie sich mit den Administratoranmeldeinformationen für ONTAP tools for VMware vSphere an, die Sie während der Bereitstellung angegeben haben.
3. Wählen Sie die Option **Einstellungen** > **NTP-Server** > **Bearbeiten**.
4. Geben Sie den durch Kommas getrennten vollqualifizierten Domänennamen (FQDN), die IPv4- oder IPv6-Adresse ein.

   Aktualisieren Sie den Bildschirm, um die aktualisierten Werte anzuzeigen.

Erstellen Sie ein Backup und stellen Sie das ONTAP -Tools -Setup wieder her

Ab ONTAP tools for VMware vSphere 10.3 verwendet das Gerät einen dynamischen Speicherbereitsteller. Sie können kein Zero-RPO erreichen. Sie können jedoch einen RPO nahe Null erreichen. Um einen RPO-Wert nahe Null zu erreichen, müssen Sie eine Sicherungskopie des Setups erstellen und diese auf einer neuen virtuellen Maschine wiederherstellen.

Um zu HA zu migrieren, wenn die Nicht-HA-Sicherung aktiviert ist, deaktivieren Sie zuerst die Sicherung und aktivieren Sie sie nach der Migration erneut.

Backup erstellen und Backup-Datei herunterladen

Schritte

1. Öffnen Sie vom vCenter Server aus die Wartungskonsole.
2. Melden Sie sich als Wartungsbenutzer an.
3. Eingeben `4` um **Support und Diagnose** auszuwählen.
4. Eingeben `3` um die Option **Systemsicherung aktivieren** auszuwählen.
5. Geben Sie im Falle von Nicht-HA die vCenter-Anmeldeinformationen ein, wo die virtuelle Maschine der ONTAP -Tools bereitgestellt wird.
6. Geben Sie einen Wert zwischen 5 und 60 Minuten für die Sicherungshäufigkeit ein.
7. Drücken Sie **Enter**

   Dadurch wird das Backup erstellt und in regelmäßigen Abständen in den Datenspeicher der virtuellen Maschine übertragen.

8. Um auf das Backup zuzugreifen, navigieren Sie zum Speicherbereich und wählen Sie den Datenspeicher der virtuellen Maschine aus
9. Wählen Sie den Abschnitt **Dateien** aus.

   Im Dateibereich können Sie das Verzeichnis sehen. Der Name des Verzeichnisses ist die IP-Adresse des ONTAP -Tools, wobei die Punkte (.) durch Unterstriche ersetzt werden und das Suffix *backup* angehängt wird.

10. Weitere Sicherungsinformationen erhalten Sie, wenn Sie die Datei backup_info.txt unter **Dateien** > **Download** herunterladen.

Genesen

Um das Setup wiederherzustellen, schalten Sie die vorhandene virtuelle Maschine aus und stellen Sie eine neue virtuelle Maschine mithilfe der OVA bereit, die bei der ersten Bereitstellung verwendet wurde.

Sie müssen für die neue virtuelle Maschine dieselbe IP-Adresse der ONTAP -Tools verwenden und die Systemkonfiguration, z. B. aktivierte Dienste, Knotengröße und HA-Modus, muss mit der ursprünglichen Bereitstellung identisch sein.

Führen Sie die folgenden Schritte aus, um das Setup aus der Sicherungsdatei wiederherzustellen.

1. Öffnen Sie vom vCenter Server aus die Wartungskonsole.
2. Melden Sie sich als Wartungsbenutzer an.
3. Eingeben `4` um **Support und Diagnose** auszuwählen.
4. Eingeben `2` um die Option **Ferndiagnosezugriff aktivieren** auszuwählen und ein neues Passwort für den Diagnosezugriff zu erstellen.
5. Wählen Sie ein beliebiges Backup aus dem heruntergeladenen Verzeichnis aus. Der Name der letzten Sicherungsdatei wird in der Datei *backup_info.txt* aufgezeichnet.

6. Führen Sie den folgenden Befehl aus, um die Sicherung auf die neue virtuelle Maschine zu kopieren, und geben Sie das Diagnosekennwort ein, wenn Sie dazu aufgefordert werden.

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

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

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

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

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

8. Nach erfolgreicher Wiederherstellung werden Dienste und vCenter-Objekte wiederhergestellt.

Deinstallieren Sie die ONTAP tools for VMware vSphere

Durch die Deinstallation der ONTAP tools for VMware vSphere werden alle Daten in den Tools gelöscht.

Schritte

1. Entfernen oder verschieben Sie alle virtuellen Maschinen aus den ONTAP tools for VMware vSphere verwaltete Datenspeicher.
   - Informationen zum Entfernen der virtuellen Maschinen finden Sie unter "Entfernen und erneutes Registrieren von VMs und VM-Vorlagen"
   - Informationen zum Verschieben in einen nicht verwalteten Datenspeicher finden Sie unter "So migrieren Sie Ihre virtuelle Maschine mit Storage vMotion"
2. "Datenspeicher löschen"erstellt auf ONTAP tools for VMware vSphere.
3. Wenn Sie den VASA-Anbieter aktiviert haben, wählen Sie in den ONTAP Tools **Einstellungen** > **VASA-Anbietereinstellungen** > **Registrierung aufheben**, um die Registrierung der VASA-Anbieter von allen vCenter-Servern aufzuheben.
4. Trennen Sie alle Speicher-Backends von der vCenter Server-Instanz. Weitere Informationen finden Sie unter "Trennen Sie Speicher-Backends von der vCenter Server-Instanz" .
5. Löschen Sie alle Speicher-Backends. Weitere Informationen finden Sie unter "Verwalten von Speicher-Backends" .
6. Entfernen Sie den SRA-Adapter aus VMware Live Site Recovery:
   a. Melden Sie sich als Administrator über Port 5480 bei der Verwaltungsschnittstelle der VMware Live Site Recovery-Appliance an.
   b. Wählen Sie **Speicherreplikationsadapter** aus.
   c. Wählen Sie die entsprechende SRA-Karte aus und wählen Sie im Dropdown-Menü **Löschen**.
   d. Bestätigen Sie, dass Sie die Ergebnisse des Löschens des Adapters kennen, und wählen Sie **Löschen**.

7. Löschen Sie die in ONTAP tools for VMware vSphere integrierten vCenter-Serverinstanzen. Weitere Informationen finden Sie unter "Verwalten von vCenter Server-Instanzen" .
8. Schalten Sie die ONTAP tools for VMware vSphere VMs vom vCenter Server aus und löschen Sie die VMs.

Wie geht es weiter?

"FlexVol -Volumes entfernen"

FlexVol -Volumes entfernen

Wenn Sie einen dedizierten ONTAP Cluster für ONTAP Tools für die VMware-Bereitstellung verwenden, werden viele ungenutzte FlexVol Volumes erstellt. Nachdem Sie ONTAP tools for VMware vSphere entfernt haben, sollten Sie die FlexVol Volumes entfernen, um mögliche Leistungseinbußen zu vermeiden.

Schritte

1. Bestimmen Sie die ONTAP tools for VMware vSphere Bereitstellungstyp aus der ersten Knoten-VM.

   cat /opt/netapp/meta/ansible_vars.yaml | grep -i Protokoll

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

2. Rufen Sie die Liste der FlexVol -Volumes ab.

   kubectl beschreibe persistente Volumes | grep internalName | awk -F=' '{print $2}'

3. Entfernen Sie die VMs vom vCenter Server. Siehe "Entfernen und erneutes Registrieren von VMs und VM-Vorlagen" .
4. Löschen Sie FlexVol -Volumes. Siehe "Löschen eines FlexVol volume" . Geben Sie im CLI-Befehl zum Löschen eines Volumes den genauen Namen des FlexVol -Volumes an.
5. Löschen Sie im Falle einer iSCSI-Bereitstellung SAN-igroups aus dem ONTAP -Speichersystem. Siehe "Anzeigen und Verwalten von SAN-Initiatoren und igroups" .

Aktualisieren Sie ONTAP tools for VMware vSphere

Upgrade von ONTAP tools for VMware vSphere 10.x auf 10.4

Sie können von ONTAP tools for VMware vSphere 10.2 oder 10.3 auf 10.4 aktualisieren. Ein direktes Upgrade von ONTAP Tools 10.0 oder 10.1 auf 10.4 wird jedoch nicht unterstützt.

NOTIZ:

- In ASA r2-Systemen sollten Sie auf ONTAP tools for VMware vSphere 10.4 mit ONTAP 9.16.1 aktualisieren, bevor Sie weitere Storage Availability Zones (SAZs) hinzufügen.
- Wenn das Upgrade von ONTAP tools for VMware vSphere 10.2 oder 10.3 auf die Version 10.4 fehlschlägt, wird ein Rollback nicht unterstützt. Um das Setup wiederherzustellen, verwenden Sie RPO für ONTAP tools for VMware vSphere 10.2 und Near-Zero-RPO oder Snapshot-Wiederherstellung für ONTAP tools for VMware vSphere 10.3.

Bevor Sie beginnen

Schalten Sie bei einem Nicht-HA-Upgrade die ONTAP -Tools-VM aus und schalten Sie bei einem HA-Upgrade den ersten Knoten aus, bevor Sie die folgenden Änderungen an den Einstellungen der virtuellen Maschine (VM) vornehmen.

Wenn Sie von ONTAP tools for VMware vSphere 10.2 oder 10.3 aktualisieren, müssen Sie vor dem Upgrade folgende Schritte ausführen: * Fügen Sie jedem Knoten eine zusätzliche 100-GB-Festplatte hinzu, da die Servicedaten lokal auf der VM gespeichert sind. * Passen Sie CPU und Speicher für die ausgeschaltete VM entsprechend Ihrer Implementierung an. Aktivieren Sie das Hot-Plugin für CPU und RAM.

+

Bereitstellungstyp	CPU (Kern) pro Knoten	Speicher (GB) pro Knoten	Festplattenspeicher (GB) pro Knoten	CPU gesamt (Kern)	Speicher (GB)	Gesamter Festplattenspeicher (GB)
Nicht-HA Klein	9	18	350	9	18	350
Nicht-HA-Medium	13	26	350	13	26	350
HA Klein	9	18	350	27	54	1050
HA Mittel	13	26	350	39	78	1050
HA Groß	17	34	350	51	102	1050

- Schalten Sie die VM ein, nachdem die Änderungen vorgenommen wurden, und warten Sie, bis die Dienste in den laufenden Zustand versetzt werden.
- Nehmen Sie im Falle einer HA-Bereitstellung die Ressourcenänderungen vor, aktivieren Sie das Hot-Plugin für CPU und RAM und fügen Sie auch für den zweiten und dritten Knoten 100-GB-Festplatten hinzu. Ein Neustart dieser Knoten ist nicht erforderlich.
- Wenn die Appliance mit ONTAP Tools 10.2 als lokaler Pfad (einfache Bereitstellung) bereitgestellt wurde, müssen Sie vor dem Upgrade einen Quiesce-Snapshot erstellen.

Wenn Sie ein Upgrade von ONTAP tools for VMware vSphere 10.0 auf 10.1 durchführen, müssen Sie die folgenden Schritte ausführen, bevor Sie mit der Upgrade-Aufgabe fortfahren: **Diagnose aktivieren**

1. Öffnen Sie vom vCenter Server aus eine Konsole für die ONTAP Tools.
2. Melden Sie sich als Wartungsbenutzer an.
3. Geben Sie **4** ein, um **Support und Diagnose** auszuwählen.
4. Geben Sie **2** ein, um **Remotediagnosezugriff aktivieren** auszuwählen.
5. Geben Sie **y** ein, um das Passwort Ihrer Wahl festzulegen.
6. Melden Sie sich vom Terminal/Putty aus mit dem Benutzer „diag“ und dem im vorherigen Schritt festgelegten Kennwort bei der VM-IP-Adresse an.

Erstellen Sie ein Backup von MongoDB

Führen Sie die folgenden Befehle aus, um eine Sicherung von MongoDB zu erstellen:

- kn exec -it ntv-mongodb-0 sh - kn ist ein Alias von kubectl -n ntv-system.
- Führen Sie den Befehl *env | grep MONGODB_ROOT_PASSWORD* im Pod aus.
- Führen Sie den Befehl *exit* aus, um den Pod zu verlassen.
- Führen Sie den Befehl *kn exec ntv-mongodb-0 --mongodump -u root -p MONGODB_ROOT_PASSWORD --archive=/tmp/mongodb-backup.gz --gzip* aus, um das im obigen Befehl festgelegte MONGO_ROOT_PASSWORD zu ersetzen.
- Führen Sie den Befehl *kn cp ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz* aus, um das mit dem obigen Befehl erstellte MongoDB-Backup vom Pod auf den Host zu kopieren.

Machen Sie den Quasi-Schnappschuss aller Bände

- Führen Sie den Befehl „kn get pvc“ aus und speichern Sie die Befehlsausgabe.
- Erstellen Sie mit einer der folgenden Methoden nacheinander Snapshots aller Volumes:
  - Führen Sie in der CLI den Befehl *volume snapshot create -vserver <vserver_name> -volume <volume_name> -snapshot <snapshot_name>* aus.
  - Suchen Sie in der Benutzeroberfläche des ONTAP System Managers nach dem Volume anhand seines Namens in der Suchleiste und öffnen Sie das Volume dann, indem Sie auf den Namen klicken. Gehen Sie zum Snapshot und fügen Sie den Snapshot dieses Volumes hinzu.

Erstellen Sie den Snapshot der ONTAP tools for VMware vSphere VMs in vCenter (3 VMs im Fall einer HA-Bereitstellung, 1 VM im Fall einer Nicht-HA-Bereitstellung)

- Wählen Sie in der Benutzeroberfläche des vSphere-Clients die VM aus.
- Gehen Sie zur Registerkarte „Schnappschüsse“ und wählen Sie die Schaltfläche „Schnappschuss machen“ aus. Erstellen Sie einen Ruhe-Snapshot der VM. Siehe "Erstellen Sie einen Snapshot einer virtuellen Maschine" für Details.

Löschen Sie vor dem Upgrade die abgeschlossenen Pods aus dem Protokollpaket mit dem Präfix „generate-support-bundle-job“. Wenn die Generierung des Support-Pakets läuft, warten Sie, bis sie abgeschlossen ist, und löschen Sie dann den Pod.

Für jede Art von Upgrade müssen Sie ein zusätzliches 100-GB-Festplattenlaufwerk (HDD) hinzufügen. Um eine Festplatte hinzuzufügen, führen Sie die folgende Aufgabe aus.

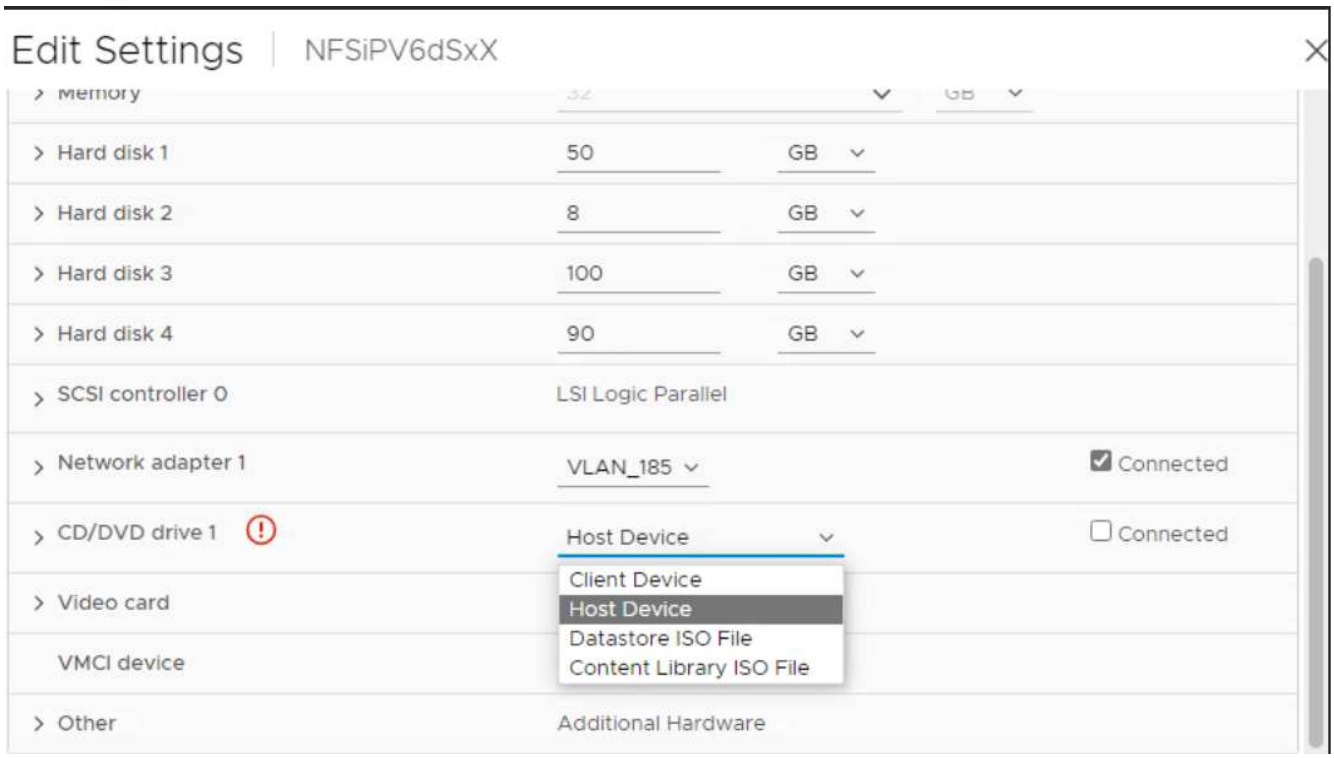
1. Wählen Sie die VM in der Einzelknotenkonfiguration oder alle drei VMs in der HA-Konfiguration aus.
2. Klicken Sie mit der rechten Maustaste auf die VM(s) und wählen Sie **Neues Gerät hinzufügen** > **Festplatte**
3. Fügen Sie im Feld **Neue Festplatte** eine 100-GB-Festplatte hinzu.
4. Wählen Sie **Übernehmen**

Aktualisieren Sie nach dem Hinzufügen der Festplatte die Ressourcen der VM für die jeweiligen Konfigurationen und starten Sie die primäre VM neu.

Es wird eine neue Festplatte erstellt. Der Dynamic Storage Provisioner verwendet diese Festplatte zum Generieren oder Replizieren der Volumes.

Schritte

1. Laden Sie ONTAP tools for VMware vSphere -Upgrade-ISO in die Inhaltsbibliothek hoch.
2. Wählen Sie auf der primären VM-Seite **Aktionen** > **Einstellungen bearbeiten**
3. Wählen Sie die ISO-Datei der Inhaltsbibliothek im Fenster „Einstellungen bearbeiten“ unter dem Feld „CD/DVD-Laufwerk“ aus.
4. Wählen Sie die ISO-Datei aus und klicken Sie auf **OK**. Aktivieren Sie das Kontrollkästchen neben dem Feld **CD/DVD-Laufwerk**
   .



5. Öffnen Sie vom vCenter Server aus eine Konsole für die ONTAP Tools.
6. Melden Sie sich als Wartungsbenutzer an.
7. Geben Sie **3** ein, um das Menü „Systemkonfiguration“ auszuwählen.
8. Geben Sie **7** ein, um die Upgrade-Option auszuwählen.
9. Beim Upgrade werden die folgenden Aktionen automatisch ausgeführt:
   a. Zertifikatsupgrade

b. Remote-Plugin-Upgrade

Nach dem Upgrade auf ONTAP tools for VMware vSphere 10.4 können Sie:

- Deaktivieren Sie die Dienste über die Manager-Benutzeroberfläche
- Wechseln Sie von einem Nicht-HA-Setup zu einem HA-Setup
- Skalieren Sie eine kleine Konfiguration ohne HA auf eine mittlere Konfiguration ohne HA oder auf eine mittlere oder große Konfiguration mit HA.
- Starten Sie im Falle eines Nicht-HA-Upgrades die ONTAP -Tools-VM neu, um die Änderungen zu übernehmen. Starten Sie im Falle eines HA-Upgrades den ersten Knoten neu, um die Änderungen auf dem Knoten zu übernehmen.

Was kommt als nächstes

Nachdem Sie von früheren Versionen der ONTAP tools for VMware vSphere auf 10.4 aktualisiert haben, scannen Sie die SRA-Adapter erneut, um zu überprüfen, ob die Details auf der Seite „VMware Live Site Recovery Storage Replication Adapters“ aktualisiert wurden.

Nachdem Sie das Upgrade erfolgreich durchgeführt haben, löschen Sie die Trident -Volumes manuell von ONTAP , indem Sie das folgende Verfahren verwenden:

Diese Schritte sind nicht erforderlich, wenn sich die ONTAP tools for VMware vSphere 10.1 oder 10.2 in kleinen oder mittleren (lokalen Pfad-)Konfigurationen ohne HA befanden.

1. Öffnen Sie vom vCenter Server aus eine Konsole für die ONTAP Tools.
2. Melden Sie sich als Wartungsbenutzer an.
3. Geben Sie **4** ein, um das Menü **Support und Diagnose** auszuwählen.
4. Geben Sie **1** ein, um die Option **Auf Diagnose-Shell zugreifen** auszuwählen.
5. Führen Sie den folgenden Befehl aus

```
sudo python3 /home/maint/scripts/ontap_cleanup.py
```

6. Geben Sie den ONTAP -Benutzernamen und das Kennwort ein

Dadurch werden alle Trident -Volumes in ONTAP gelöscht, die in ONTAP tools for VMware vSphere 10.1/10.2 verwendet werden.

Ähnliche Informationen

"Migrieren Sie von ONTAP tools for VMware vSphere 9.xx auf 10.4"

Upgrade-Fehlercodes

Während des Upgradevorgangs der ONTAP tools for VMware vSphere können Fehlercodes auftreten. Die Fehlercodes bestehen aus fünf Ziffern, wobei die ersten beiden Ziffern das Skript darstellen, bei dem das Problem aufgetreten ist, und die letzten drei Ziffern den spezifischen Arbeitsablauf innerhalb dieses Skripts darstellen.

Alle Fehlerprotokolle werden in der Datei ansible-perl-errors.log aufgezeichnet, um die einfache Verfolgung

und Lösung von Problemen zu ermöglichen. Diese Protokolldatei enthält den Fehlercode und die fehlgeschlagene Ansible-Aufgabe.

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

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

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

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

Upgrade-Fehlercode	Arbeitsablauf	Auflösung
052	Die ISO-Datei kann mit der aktuellen Version identisch sein oder zwei Versionen über der aktuellen Version liegen.	Verwenden Sie eine kompatible ISO-Version, um ein Upgrade von Ihrer aktuellen Version durchzuführen.
068	Das Rollback der Debian-Pakete ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
069	Wiederherstellung der Dateien fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
070	Löschen der Sicherung fehlgeschlagen	-
071	Der Kubernetes-Cluster war nicht fehlerfrei	-
074	Das Einbinden von ISO ist fehlgeschlagen	Überprüfen Sie /var/log/upgrade-run.log und versuchen Sie das Upgrade erneut.

Upgrade-Fehlercode	Arbeitsablauf	Auflösung
075	Upgrade-Vorprüfungen sind fehlgeschlagen	Versuchen Sie das Upgrade erneut.
076	Das Upgrade der Registrierung ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
077	Das Rollback der Registrierung ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
078	Das Operator-Upgrade ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
079	Das Rollback des Operators ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
080	Das Upgrade der Dienste ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
081	Das Rollback der Dienste ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
082	Das Löschen alter Bilder aus dem Container ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
083	Das Löschen der Sicherung ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
084	Das Zurücksetzen von JobManager auf Produktion ist fehlgeschlagen	Befolgen Sie die folgenden Schritte, um das Upgrade wiederherzustellen/abzuschließen. 1. Aktivieren Sie Diagnostic Shell 2. Führen Sie den Befehl aus: *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* 3. Überprüfen Sie die Protokolle unter /var/log/post-deploy-upgrade.log

Upgrade-Fehlercode	Arbeitsablauf	Auflösung
087	Die Schritte nach dem Upgrade sind fehlgeschlagen.	Führen Sie die folgenden Schritte aus, um das Upgrade wiederherzustellen/abzuschließen. 1. Aktivieren Sie Diagnostic Shell 2. Führen Sie den Befehl *sudo perl /home/maint/scripts/post-deploy-upgrade.pl --postupgrade* aus. 3. Überprüfen Sie die Protokolle unter /var/log/post-deploy-upgrade.log
088	Das Konfigurieren der Protokollrotation für Journald ist fehlgeschlagen	Überprüfen Sie, ob die VM-Netzwerkeinstellungen 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	Das Ändern des Eigentümers der Rotationskonfigurationsdatei des Zusammenfassungsprotokolls ist fehlgeschlagen	Versuchen Sie das Upgrade erneut.
095	Betriebssystem-Upgrade fehlgeschlagen	Keine Wiederherstellung für Betriebssystem-Upgrade. Die ONTAP -Tool-Dienste werden aktualisiert und neue Pods werden ausgeführt.
096	Installieren Sie den Dynamic Storage Provisioner	Überprüfen Sie die Upgrade-Protokolle und versuchen Sie das Upgrade erneut.
097	Die Deinstallation der Dienste für das Upgrade ist fehlgeschlagen	Verwenden Sie eine Wiederherstellung auf Basis von Null-RPO oder Snapshots und versuchen Sie das Upgrade erneut.
098	Das Kopieren des Dockercred-Geheimnisses vom NTV-System in den Namespace des dynamischen Speicherbereitstellers ist fehlgeschlagen	Überprüfen Sie die Upgrade-Protokolle und versuchen Sie das Upgrade erneut.
099	Die Validierung der neuen HDD-Erweiterung ist fehlgeschlagen.	Fügen Sie die neue Festplatte im Falle einer HA allen Knoten und im Falle einer Nicht-HA-Bereitstellung einem Knoten hinzu.
108	Seeding-Skript fehlgeschlagen	-
109	Das Sichern persistenter Volumedaten ist fehlgeschlagen	Überprüfen Sie die Upgrade-Protokolle und versuchen Sie das Upgrade erneut.

Upgrade-Fehlercode	Arbeitsablauf	Auflösung
110	Das Wiederherstellen persistenter Volumedaten ist fehlgeschlagen	Verwenden Sie Zero-RPO oder eine Snapshot-basierte Wiederherstellung und versuchen Sie das Upgrade erneut.
111	Das Aktualisieren der etcd-Timeout-Parameter für RKE2 ist fehlgeschlagen	Überprüfen Sie die Upgrade-Protokolle und versuchen Sie das Upgrade erneut.
112	Die Deinstallation des Dynamic Storage Provisioner ist fehlgeschlagen	-
113	Das Aktualisieren der Ressourcen auf sekundären Knoten ist fehlgeschlagen	Überprüfen Sie die Upgrade-Protokolle und versuchen Sie das Upgrade erneut.
104	Der Neustart des sekundären Knotens ist fehlgeschlagen	Starten Sie die Knoten manuell einzeln neu
100	Kernel-Rollback ist fehlgeschlagen	-
051	Das Upgrade des dynamischen Speicherbereitstellers ist fehlgeschlagen	Überprüfen Sie die Upgrade-Protokolle und versuchen Sie das Upgrade erneut.
056	Das Löschen der Migrationssicherung ist fehlgeschlagen	N / A

Ab ONTAP tools for VMware vSphere 10.3 wird Zero RPO nicht mehr unterstützt.

Erfahren Sie mehr über "So stellen Sie ONTAP tools for VMware vSphere wieder her, wenn das Upgrade von Version 10.0 auf 10.1 fehlschlägt"

Migrieren Sie ONTAP tools for VMware vSphere 9.xx auf 10.4

Migrieren Sie von ONTAP tools for VMware vSphere 9.xx auf 10.4

Das Verschieben der NetApp ONTAP tools for VMware vSphere -Setup von Version 9.xx auf 10.x erfordert aufgrund der erheblichen Produktaktualisierungen und -verbesserungen in den Versionen einen Migrationsprozess.

Sie können von den ONTAP tools for VMware vSphere 9.12D1, 9.13D2 und 9.13P2 auf die ONTAP tools for VMware vSphere 10.4 migrieren.

Wenn Sie in Ihrem Setup NFS- und VMFS-Datenspeicher und keine vVols Datenspeicher haben, deinstallieren Sie einfach ONTAP Tools 9.xx und stellen Sie ONTAP Tools 10.x bereit. Wenn Ihr Setup jedoch vVols Datenspeicher enthält, müssen Sie den VASA-Provider und den SRA migrieren.

Die folgende Tabelle skizziert den Migrationsprozess in diesen beiden unterschiedlichen Szenarien.

Wenn das Setup über vVols -Datenspeicher verfügt	Wenn das Setup nur NFS- und VMFS-Datenspeicher enthält
Schritte: 1. "Migrieren des VASA-Anbieters" 2. "Erstellen von VM-Speicherrichtlinien"	Schritte: 1. Entfernen Sie ONTAP Tools 9.xx aus Ihrer Umgebung. Siehe "So entfernen Sie OTV 9.xx aus Ihrer Umgebung" NetApp Knowledge Base-Artikel. 2. "Bereitstellen und Konfigurieren von ONTAP tools for VMware vSphere 10.4" 3. "Aktualisieren Sie die SRA" 4. "Erstellen von VM-Speicherrichtlinien"

Nach der Migration von ONTAP tools for VMware vSphere 9.xx auf 10.4 sind vVols Datenspeicher, die das NVMe/FC-Protokoll verwenden, nicht mehr betriebsbereit, da ONTAP Tools 10.4 das NVMe-oF-Protokoll nur mit VMFS-Datenspeichern unterstützt.

Migrieren Sie den VASA-Anbieter und aktualisieren Sie die SRA

Schritte zur Migration des VASA-Anbieters

1. Um Derby PORT 1527 auf den vorhandenen ONTAP tools for VMware vSphere zu aktivieren, aktivieren Sie den Root-Benutzer und melden Sie sich über SSH bei der CLI an. Führen Sie dann den folgenden Befehl aus:

   ```
   iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
   ```

2. Stellen Sie OVA für ONTAP tools for VMware vSphere 10.4 bereit.
3. Fügen Sie die vCenter Server-Instanz hinzu, die Sie zu ONTAP tools for VMware vSphere 10.4 Release migrieren möchten. Weitere Informationen finden Sie unter "Hinzufügen einer vCenter Server-Instanz" für

weitere Informationen.

4. Integrieren Sie das Speicher-Backend lokal von den vCenter-Server-APIs für das ONTAP Tools-Plug-In.
5. Führen Sie zur Migration die folgende API von Swagger oder in Postman aus.

   curl -X POST `https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/{vcguid}/migration-jobs`

   Sie können über diese URL auf Swagger zugreifen: `https://$FQDN_IP_PORT/', for example: `\https://10.67.25.33:8443 .`

   HTTP-Methode und Endpunkt

   Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Weg
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": "" }'

   Anforderungstext für die Migration zu anderen Releases:

   { "otv_ip": "xx.xx.xx.xx", "vasa_provider_credentials": { "Benutzername": "xxxxx", "Passwort": "*" } }

   JSON-Ausgabebeispiel

   Es wird ein Jobobjekt zurückgegeben. Sie sollten die Jobkennung speichern, um sie im nächsten Schritt zu verwenden.

   { "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "läuft" }

6. Verwenden Sie die folgende URI in Swagger, um den Status zu überprüfen:

   ```
   curl `\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?includeSubJobsAndTasks=true`
   ```

   Überprüfen Sie nach Abschluss des Auftrags den Migrationsbericht. Dieser Bericht ist in den Auftragsdaten enthalten und kann über die Auftragsantwort aufgerufen werden.

7. Fügen Sie die ONTAP tools for VMware vSphere Speicheranbieter zum vCenter Server hinzu und"Registrieren des VASA-Anbieters" mit ONTAP tools for VMware vSphere.
8. "VASA-Anbieter aktivieren"Dienst auf ONTAP tools for VMware vSphere 10.4.
9. Stoppen Sie den VASA Provider-Dienst von ONTAP tools for VMware vSphere Storage Provider 9.10/9.11/9.12/9.13 über die Wartungskonsole.

   Löschen Sie den VASA-Anbieter nicht.

   Nachdem der alte VASA-Provider gestoppt wurde, führt der vCenter Server ein Failover auf ONTAP tools for VMware vSphere durch. Alle Datenspeicher und VMs sind nun über ONTAP tools for VMware vSphere zugänglich und werden von diesen bedient.

10. Die aus den ONTAP tools for VMware vSphere 9.xxx migrierten NFS- und VMFS-Datenspeicher sind in den ONTAP tools for VMware vSphere 10.4 erst sichtbar, nachdem der Datenspeichererkennungsjob ausgelöst wurde. Dies kann bis zu 30 Minuten dauern. Stellen Sie sicher, dass die Datenspeicher auf der Übersichtsseite der ONTAP -Tools für die Benutzeroberflächenseite des VMware vSphere-Plugins sichtbar sind.
11. Führen Sie die Patchmigration mithilfe der folgenden API in Swagger oder Postman durch:

HTTP-Methode und Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Weg
PATCH	/api/v1

Verarbeitungsart

Asynchron

Curl-Beispiel

curl -X PATCH
`https://xx.xx.xx.xx:8443/virtualization/api/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/migration-jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43`

JSON-Ausgabebeispiel

Es wird ein Jobobjekt zurückgegeben. Sie sollten die Jobkennung speichern, um sie im nächsten Schritt zu verwenden.

{ "id": 123, "migration_id": "d50073ce-35b4-4c51-9d2e-4ce66f802c35", "status": "läuft" }

Der Anforderungstext ist für den Patchvorgang leer.

UUID ist die Migrations-UUID, die als Antwort auf die Post-Migrations-API zurückgegeben wird.

Nach dem Ausführen der Patch-Migrations-API entsprechen alle VMs der Speicherrichtlinie.

Was kommt als nächstes

Nachdem Sie die Migration abgeschlossen und ONTAP Tools 10.4 beim vCenter Server registriert haben, führen Sie die folgenden Schritte aus:

- Warten Sie, bis die **Erkennung** abgeschlossen ist. Die Zertifikate werden auf allen Hosts automatisch aktualisiert.
- Warten Sie ausreichend, bevor Sie Datenspeicher- und virtuelle Maschinenvorgänge starten. Die erforderliche Wartezeit hängt von der Anzahl der Hosts, Datenspeicher und virtuellen Maschinen in der Konfiguration ab. Andernfalls kann es zu zeitweiligen Betriebsausfällen kommen.

Wenn der Konformitätsstatus der virtuellen Maschine nach dem Upgrade veraltet ist, wenden Sie die Speicherrichtlinie mit den folgenden Schritten erneut an:

1. Navigieren Sie zum Datenspeicher und wählen Sie **Zusammenfassung** > **VM-Speicherrichtlinien**.

   Der Konformitätsstatus unter **VM-Speicherrichtlinienkonformität** wird als **Veraltet** angezeigt.

2. Wählen Sie die Storage VM-Richtlinie und die entsprechende VM aus
3. Wählen Sie **Übernehmen**

   Der Compliance-Status unter **VM-Speicherrichtlinien-Compliance** wird jetzt als konform angezeigt.

Ähnliche Informationen

- "Erfahren Sie mehr über ONTAP tools for VMware vSphere 10 RBAC"
- "Upgrade von ONTAP tools for VMware vSphere 10.x auf 10.4"

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 SRM-Oberfläche zeigt den Status des Wiederherstellungsplans mit Details zu den geschützten und den Wiederherstellungsstandorten an. Im Wiederherstellungsplan sind die Schaltflächen **CleanupP** und **Reprotect** deaktiviert, während die Schaltflächen TEST und RUN aktiviert bleiben. Dies zeigt an, dass der Standort für die Datenwiederherstellung vorbereitet ist. Stellen Sie vor der Migration des SRA sicher, dass sich ein Standort im geschützten Zustand und der andere im Wiederherstellungszustand befindet.

> Beginnen Sie nicht mit der Migration, wenn das Failover abgeschlossen ist, der erneute Schutz jedoch noch aussteht. Stellen Sie sicher, dass der erneute Schutzvorgang abgeschlossen ist, bevor Sie mit der Migration fortfahren. Wenn ein Test-Failover läuft, bereinigen Sie das Test-Failover und starten Sie die Migration.

1. Führen Sie die folgenden Schritte aus, um den SRA-Adapter der ONTAP -Tools für VMware vSphere 9.xx in VMware Site Recovery zu löschen:
   a. Gehen Sie zur Konfigurationsverwaltungsseite von VMware Live Site Recovery
   b. Gehen Sie zum Abschnitt **Storage Replication Adapter**.
   c. Wählen Sie im Auslassungsmenü **Konfiguration zurücksetzen**.
   d. Wählen Sie im Auslassungsmenü **Löschen** aus.
2. Führen Sie diese Schritte sowohl auf Schutz- als auch auf Wiederherstellungssites aus.

a. "Aktivieren Sie ONTAP tools for VMware vSphere -Dienste"

b. Installieren Sie ONTAP tools for VMware vSphere 10.4 SRA-Adapter mit den Schritten in"Konfigurieren von SRA auf der VMware Live Site Recovery-Appliance" .

c. Führen Sie auf der Benutzeroberflächenseite von VMware Live Site Recovery die Vorgänge **Arrays erkennen** und **Geräte erkennen** aus und vergewissern Sie sich, dass die Geräte wie vor der Migration angezeigt werden.

Automatisieren Sie mit der REST-API

Erfahren Sie mehr über die ONTAP tools for VMware vSphere 10 REST API

ONTAP tools for VMware vSphere 10 sind ein Satz von Tools für das Lebenszyklusmanagement virtueller Maschinen. Es enthält eine robuste REST-API, die Sie als Teil Ihrer Automatisierungsprozesse verwenden können.

REST-Webdienstgrundlagen

Representational State Transfer (REST) ist ein Stil zum Erstellen verteilter Webanwendungen, einschließlich des Designs von Webdienst-APIs. Es etabliert eine Reihe von Technologien zum Offenlegen serverbasierter Ressourcen und zum Verwalten ihrer Zustände.

Ressourcen und staatliche Vertretung

Ressourcen sind die grundlegenden Komponenten einer REST-Webdienstanwendung. Beim Entwerfen einer REST-API gibt es zunächst zwei wichtige Aufgaben:

- Identifizieren Sie die system- oder serverbasierten Ressourcen
- Definieren Sie die Ressourcenzustände und die zugehörigen Zustandsübergangsvorgänge

Clientanwendungen können die Ressourcenzustände durch klar definierte Nachrichtenflüsse anzeigen und ändern.

HTTP-Nachrichten

Hypertext Transfer Protocol (HTTP) ist das Protokoll, das vom Client und Server der Webdienste 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 Anforderungs- und Antwortheader sowie Antwortstatuscodes.

JSON-Datenformatierung

Obwohl mehrere Nachrichtenformate verfügbar sind, ist JavaScript Object Notation (JSON) die beliebteste Option. JSON ist ein Industriestandard zur Darstellung einfacher Datenstrukturen im Klartext und wird zur Übertragung von Statusinformationen verwendet, die die Ressourcen und gewünschten Aktionen beschreiben.

Sicherheit

Sicherheit ist ein wichtiger Aspekt einer REST-API. Zusätzlich zum Transport Layer Security (TLS)-Protokoll, das zum Schutz des HTTP-Verkehrs über das Netzwerk verwendet wird, verwenden die ONTAP tools for VMware vSphere 10 REST API auch Zugriffstoken zur Authentifizierung. Sie müssen ein Zugriffstoken erwerben und es bei nachfolgenden API-Aufrufen verwenden.

Unterstützung für asynchrone Anfragen

Die ONTAP tools for VMware vSphere 10 REST API führen die meisten Anfragen synchron aus und geben einen Statuscode zurück, wenn der Vorgang abgeschlossen ist. Es unterstützt auch die asynchrone Verarbeitung von Aufgaben, deren Ausführung mehr Zeit in Anspruch nimmt.

ONTAP Tools Manager-Umgebung

Es gibt mehrere Aspekte der ONTAP Tools Manager-Umgebung, die Sie berücksichtigen sollten.

Virtuelle Maschine

ONTAP tools for VMware vSphere 10 werden mithilfe der vSphere-Remote-Plugin-Architektur bereitgestellt. Die Software, einschließlich der Unterstützung für die REST-API, wird in einer separaten virtuellen Maschine ausgeführt.

IP-Adresse der ONTAP -Tools

ONTAP tools for VMware vSphere 10 stellen eine einzelne IP-Adresse bereit, die ein Gateway zu den Funktionen der virtuellen Maschine bereitstellt. Sie müssen die Adresse während der Erstkonfiguration angeben und sie wird einer internen Lastenausgleichskomponente zugewiesen. Die Adresse wird von der Benutzeroberfläche des ONTAP Tools Managers sowie für den direkten Zugriff auf die Swagger-Dokumentationsseite und die REST-API verwendet.

Zwei REST-APIs

Zusätzlich zu den 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, sich vor Augen zu halten, dass diese beiden APIs getrennt und unterschiedlich sind. Weitere Informationen finden Sie unter "ONTAP Automatisierung" .

Implementierungsdetails für die ONTAP tools for VMware vSphere 10 REST API

Während REST einen gemeinsamen Satz an Technologien und Best Practices etabliert, kann die genaue Implementierung jeder API je nach Designentscheidung variieren. Sie sollten mit der Konzeption der ONTAP tools for VMware vSphere 10 REST API vertraut sein, bevor Sie sie verwenden.

Die REST-API umfasst mehrere Ressourcenkategorien wie vCenter und Aggregate. Überprüfen Sie die"API-Referenz" für weitere Informationen.

So greifen Sie auf die REST-API zu

Sie können über die IP-Adresse und den Port der ONTAP -Tools auf die ONTAP tools for VMware vSphere 10 REST API zugreifen. Die vollständige URL besteht aus mehreren Teilen, darunter:

- IP-Adresse und Port der ONTAP -Tools
- API-Version
- Ressourcenkategorie
- Spezifische Ressource

Sie müssen die IP-Adresse während der Ersteinrichtung konfigurieren, während der Port fest auf 8443 bleibt. Der erste Teil der URL ist für jede ONTAP tools for VMware vSphere 10-Instanz konsistent; nur die Ressourcenkategorie und die spezifische Ressource ändern sich zwischen den Endpunkten.

Die IP-Adress- und Portwerte in den folgenden Beispielen dienen nur zu Illustrationszwecken. Sie müssen diese Werte für Ihre Umgebung ändern.

Beispiel für den Zugriff auf Authentifizierungsdienste

```
https://10.61.25.34:8443/virtualization/api/v1/auth/login
```

Über diese URL kann mit der POST-Methode ein Zugriffstoken angefordert werden.

Beispiel zum Auflisten der vCenter-Server

```
https://10.61.25.34:8443/virtualization/api/v1/vcenters
```

Über diese URL kann mit der GET-Methode eine Liste der definierten vCenter-Serverinstanzen angefordert werden.

HTTP-Details

Die ONTAP tools for VMware vSphere 10 REST-API verwenden HTTP und zugehörige Parameter, um auf die Ressourceninstanzen und -sammlungen einzuwirken. Details zur HTTP-Implementierung werden unten dargestellt.

HTTP-Methoden

Die von der REST-API unterstützten HTTP-Methoden oder Verben sind in der folgenden Tabelle aufgeführt.

Verfahren	CRUD	Beschreibung
ERHALTEN	Lesen	Ruft Objekteigenschaften für eine Ressourceninstanz oder -sammlung ab. Dies wird als Listenvorgang betrachtet, wenn es mit einer Sammlung verwendet wird.
POST	Erstellen	Erstellt eine neue Ressourceninstanz basierend auf den Eingabeparametern.
SETZEN	Aktualisieren	Aktualisiert eine gesamte Ressourceninstanz mit dem bereitgestellten JSON-Anforderungstext. Nicht vom Benutzer änderbare Schlüsselwerte bleiben erhalten.
PATCH	Aktualisieren	Fordert an, dass eine Reihe ausgewählter Änderungen in der Anforderung auf die Ressourceninstanz angewendet werden.
LÖSCHEN	Löschen	Löscht eine vorhandene Ressourceninstanz.

Anforderungs- und Antwortheader

Die folgende Tabelle fasst die wichtigsten mit der REST-API verwendeten HTTP-Header zusammen.

Kopfzeile	Typ	Verwendungshinweise
Akzeptieren	Anfrage	Dies ist der Inhaltstyp, den die Clientanwendung akzeptieren kann. Gültige Werte sind beispielsweise „*/*“ oder `application/json` .
x-auth	Anfrage	Enthält ein Zugriffstoken, das den Benutzer identifiziert, der die Anforderung über die Clientanwendung stellt.
Inhaltstyp	Antwort	Vom Server zurückgegeben basierend auf `Accept` Anforderungsheader.

HTTP-Statuscodes

Die von der REST-API verwendeten HTTP-Statuscodes werden unten beschrieben.

Code	Bedeutung	Beschreibung
200	OK	Zeigt den Erfolg von Aufrufen an, die keine neue Ressourceninstanz erstellen.
201	Erstellt	Ein Objekt mit einer eindeutigen Kennung für die Ressourceninstanz wurde erfolgreich 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 Anfrageeingabe wird nicht erkannt oder ist unpassend.
401	Nicht autorisiert	Der Benutzer ist nicht autorisiert und muss sich authentifizieren.
403	Verboten	Der Zugriff wird aufgrund eines Autorisierungsfehlers verweigert.
404	Nicht gefunden	Die in der Anfrage genannte Ressource existiert nicht.
409	Konflikt	Der Versuch, ein Objekt zu erstellen, ist fehlgeschlagen, da das Objekt bereits vorhanden ist.
500	Interner Fehler	Auf dem Server ist ein allgemeiner interner Fehler aufgetreten.

Authentifizierung

Die Authentifizierung eines Clients gegenüber der REST-API erfolgt mithilfe eines Zugriffstokens. Zu den relevanten Merkmalen des Tokens und des Authentifizierungsprozesses gehören:

- Der Client muss mit den Administratoranmeldeinformationen (Benutzername und Kennwort) des ONTAP Tools Manager ein Token anfordern.
- Token werden als JSON Web Token (JWT) formatiert.
- Jedes Token verfällt nach 60 Minuten.
- API-Anfragen von einem Client müssen das Token in der `x-auth` Anforderungsheader.

Siehe"Ihr erster REST-API-Aufruf" für ein Beispiel zum Anfordern und Verwenden eines Zugriffstokens.

Synchrone und asynchrone Anfragen

Die meisten REST-API-Aufrufe werden schnell abgeschlossen und laufen daher synchron. Das heißt, sie geben einen Statuscode (z. B. 200) zurück, nachdem eine Anfrage abgeschlossen wurde. Anfragen, deren Abschluss länger dauert, werden asynchron mithilfe eines Hintergrundjobs ausgeführt.

Nach der Ausgabe eines asynchron ausgeführten API-Aufrufs gibt der Server einen HTTP-Statuscode 202 zurück. Dies zeigt an, dass die Anfrage akzeptiert, aber noch nicht abgeschlossen wurde. Sie können den Hintergrundjob abfragen, um seinen Status zu ermitteln, einschließlich Erfolg oder Misserfolg.

Die asynchrone Verarbeitung wird für verschiedene Arten lang andauernder Vorgänge verwendet, darunter Datenspeicher- und vVol-Vorgänge. Weitere Informationen finden Sie in der Kategorie „Job-Manager“ der REST-API auf der Swagger-Seite.

Ihre ersten ONTAP tools for VMware vSphere 10 REST-API-Aufruf

Sie können einen API-Aufruf mit curl ausgeben, um mit den ONTAP tools for VMware vSphere 10 REST-API zu beginnen.

Bevor Sie beginnen

Sie sollten die erforderlichen Informationen und Parameter in den Curl-Beispielen überprüfen.

Erforderliche Informationen

Sie benötigen Folgendes:

- ONTAP tools for VMware vSphere 10 IP-Adresse oder FQDN sowie den Port
- Anmeldeinformationen für den ONTAP Tools Manager-Administrator (Benutzername und Passwort)

Parameter und Variablen

Die unten dargestellten Curl-Beispiele enthalten Variablen im Bash-Stil. Sie können diese Variablen in der Bash-Umgebung festlegen oder sie vor der Ausführung der Befehle manuell aktualisieren. Wenn Sie die Variablen festlegen, 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 Domänenname oder die IP-Adresse des ONTAP Tools Manager zusammen mit der Portnummer.
$MEINBENUTZER	Benutzername für das ONTAP Tools Manager-Konto.
$MEINPASSWORT	Mit dem Benutzernamen des ONTAP Tools Manager verknüpftes Kennwort.
$ACCESS_TOKEN	Das vom ONTAP Tools Manager ausgestellte Zugriffstoken.

Die folgenden Befehle und Ausgaben der Linux-CLI 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: Abrufen eines Zugriffstokens

Sie müssen ein Zugriffstoken erwerben, um die REST-API zu verwenden. Nachfolgend wird ein Beispiel für die Anforderung eines Zugriffstokens dargestellt. Sie sollten die entsprechenden Werte für Ihre Umgebung einsetzen.

```
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 bereitgestellte Zugriffstoken.

Schritt 2: Ausführen des REST-API-Aufrufs

Nachdem Sie über ein Zugriffstoken verfügen, können Sie mit curl einen REST-API-Aufruf tätigen. Fügen Sie das im ersten Schritt erworbene Zugriffstoken ein.

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 für den ONTAP Tools Manager konfigurierten VMware vCenter-Instanzen.

API-Referenz für die ONTAP tools for VMware vSphere 10 REST API

Die ONTAP tools for VMware vSphere 10 REST-API-Referenz enthalten Details zu allen API-Aufrufen. Diese Referenz ist bei der Entwicklung von Automatisierungsanwendungen hilfreich.

Sie können online über die Swagger-Benutzeroberfläche auf die ONTAP tools for VMware vSphere 10 REST-API-Dokumentation zugreifen. Sie benötigen die IP-Adresse oder den FQDN des ONTAP tools for VMware vSphere 10-Gateway-Dienst sowie den Port.

Schritte

1. Geben Sie die folgende URL in Ihren Browser ein, ersetzen Sie die Variable durch die entsprechende Kombination aus IP-Adresse und Port und drücken Sie die **Eingabetaste**.

   `https://$FQDN_IP_PORT/`

   Beispiel

   `https://10.61.25.33:8443/`

2. Als Beispiel für einen einzelnen API-Aufruf scrollen Sie nach unten zur Kategorie **vCenters** und wählen Sie **GET** neben dem Endpunkt `/virtualization/api/v1/vcenters`

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

"Hinweis zu ONTAP tools for VMware vSphere 10.4"