Dokumentation zu ONTAP Tools für VMware vSphere

ONTAP tools for VMware vSphere 10.1

NetApp
March 17, 2025

This PDF was generated from https://docs.netapp.com/de-de/ontap-tools-vmware-vsphere-101/index.html on March 17, 2025. Always check docs.netapp.com for the latest.

Inhalt

Dokumentation zu ONTAP Tools für VMware vSphere

Versionshinweise

Versionshinweise

Erfahren Sie mehr über die neuen und erweiterten Funktionen, die in den ONTAP Tools für VMware vSphere 10.1 verfügbar sind.

Eine vollständige Liste der neuen Funktionen und Verbesserungen finden Sie unter Neuerungen bei ONTAP Tools für VMware vSphere 10.1.

Weitere Informationen darüber, ob die Migration von ONTAP-Tools für VMware vSphere 9 zu ONTAP-Tools 10.1 für Ihre Implementierung geeignet ist, finden Sie unter Vergleich der Funktionen der ONTAP Tools für VMware vSphere 9 und der ONTAP Tools für VMware vSphere 10. Die Migration wird von ONTAP-Tools für VMware vSphere 9.10D2, 9.11D4, 9.12 und 9.13 Versionen auf ONTAP-Tools 10.1 unterstützt.

Details zu bekannten Problemen und Einschränkungen in ONTAP-Tools für VMware vSphere 10.1 finden Sie in der "Versionshinweise zu ONTAP Tools für VMware vSphere 10.1". Sie müssen sich mit Ihrem NetApp Konto anmelden oder ein Konto erstellen, um auf die Versionshinweise zuzugreifen.

Neuerungen bei ONTAP Tools für VMware vSphere 10.1

Erfahren Sie mehr über die neuen Funktionen in den ONTAP Tools für VMware vSphere 10.1.

Aktualisieren	Beschreibung
Unterstützung von NFS- und VMFS-Datastore	Diese Version der ONTAP Tools für VMware vSphere unterstützt die VVols Datastore-Bereitstellung über VASA Provider sowie NFS v3- und VMFS-Datastores. Datastore-Operationen wie das Erstellen, Ändern der Größe, Mounten, Unmounten und Löschen werden unterstützt. Sie können VMFS-Datastores mithilfe des iSCSI-Protokolls bereitstellen. Als VMware Administrator können Sie iSCSI VMFS Datastores nahtlos von ONTAP Tools für VMware vSphere 9.xx Version auf Version 10.1 implementieren, aktualisieren und verschieben. Die Migration wird von ONTAP-Tools für VMware vSphere 9.10D2, 9.11D4, 9.12 und 9.13 Versionen bis 10.1 unterstützt.
Storage Replication Adapter (SRA) für NFS- und VMFS-Datastores	SRA implementiert die spezifikationsbasierte Disaster Recovery (DR) des VMware Site Recovery Manager (SRM). Bei NFS-Datastores werden ONTAP Volumes über NFS v3-Protokolle auf dem ESXi Host gemountet. Für VMFS-Datastores werden ONTAP-LUNS über das iSCSI-Protokoll auf einem ESXi Host gemountet. ONTAP SnapMirror Beziehungen replizieren Volumes und LUNs am Zielstandort. SRA implementiert testFailover-, Failover- und Reprotect-Befehle, die von VMware SRM aufgerufen werden. Im Rahmen der Implementierung stellt SRA sicher, dass alle Volumes und LUNs bei einer Recovery-Störung am Ziel mountbar sind, und dass die Volumes und LUNs am sekundären Standort gelesen werden, um Datenabweichungen zu vermeiden.

Aktualisieren	Beschreibung
Umfangreiche Unterstützung der Integration von vCenter User Interface (UI) für alle Workflows	ONTAP Tools für VMware vSphere 10.1 bieten eine grafische Benutzeroberfläche für Workflows, die Parität mit ONTAP Tools für VMware vSphere 9.xx Versionen ermöglichen. Das Remote-Plug-in unterstützt: • Beobachtbarkeit und Monitoring von NFS, VMFS und VVols Datastores • Storage Replication Adapter für NFS- und VMFS-Datastores • Registrierung und Abmeldung des VASA-Providers • VAAI-Plug-in-Installation • Download des Protokollpakets für das ausgewählte vCenter
Unterstützung für einfache Bereitstellungsvarianten	Sie können schnell die ONTAP Tools für VMware vSphere 10.1 integrieren und die Funktionen nutzen, indem Sie die einfache Implementierungsoption nutzen. Auch die Snapshot-basierte Recovery lässt sich problemlos implementieren.
ONTAP Tools Manager-Benutzeroberfläche für alle ONTAP-Tools – Admin-Workflows	Der ONTAP Tools Manager bietet Administratoren von ONTAP Tools eine bessere Kontrolle über die Instanzen von Managed vCenter und Onboard Storage Back-Ends. Der ONTAP Tools Manager unterstützt Sie bei folgenden Aufgaben: • VCenter Management – Hinzufügen und Managen von vCenter-Instanzen zu ONTAP-Tools für VMware vSphere • Storage-Back-End-Management: Fügen Sie ONTAP Storage-Cluster zu ONTAP Tools für VMware vSphere hinzu und managen Sie sie den global integrierten vCenter Instanzen. • Log Bundle Downloads - Sammeln Sie Log-Dateien für ONTAP-Tools für VMware vSphere. • Zertifikatverwaltung – Ändern Sie das selbstsignierte Zertifikat in ein benutzerdefiniertes CA-Zertifikat, und erneuern oder aktualisieren Sie alle Zertifikate. • Password Management - Zurücksetzen OVA-Anwendungs-Passwort für den Benutzer.
Zertifikatmanagement	Mit einer einzelnen Instanz der ONTAP Tools für VMware vSphere können mehrere vCenter Instanzen gemanagt werden. Wenn Sie ONTAP-Tools für VMware vSphere bereitstellen, wird standardmäßig allen vCenter-Instanzen ein selbstsigniertes Zertifikat zugewiesen. Wenn Sie mehrere vCenter Instanzen managen und VVols-Funktionen auf mehreren vCenter Instanzen aktivieren möchten, müssen Sie über die Schnittstelle des ONTAP Tools Managers das selbstsignierte Zertifikat in ein benutzerdefiniertes CA-Zertifikat ändern. Sie können die gleiche Oberfläche verwenden, um alle Zertifikate zu erneuern oder zu aktualisieren.

Aktualisieren	Beschreibung
Recovery Point Objective (RPO) ohne Recovery	Wenn Sie Ihre ONTAP Tools für die VMware vSphere Einrichtung verlieren, können Sie Ihre ONTAP Tools Setup mit der ONTAP Datenmanagement-Software ohne Datenverlust wiederherstellen. Die Recovery mit einem RPO von null wird für einfache Implementierungsoptionen nicht unterstützt.
Unterstützung des iSCSI-Protokolls für die Bereitstellung	Trident unterstützt NFS- und iSCSI-Protokolle für die Bereitstellung persistenter Volumes. Beim Implementieren der ONTAP Tools für VMware vSphere können Sie das iSCSI-Protokoll verwenden, um VASA Provider-Services-Daten in persistenten Volumes zu speichern.
IPv6-Adressunterstützung für Speicher und vCenter-Onboarding	Sie können Speicher-Back-Ends mit IPv4-Adressen, IPv6-Adressen oder vollständig qualifizierten Domänennamen (FQDNs) integrieren. Storage-Services und Storage Proxy-Services verwenden zum Kommunizieren mit der ONTAP-REST-API dieselben IPv4- oder IPv6-Adressen. Data Pathing wird mit IPv4-Adressen, IPv6-Adressen oder FQDN unter Verwendung von Regeln für Exportrichtlinien unterstützt.

Vergleich der Funktionen der ONTAP Tools für VMware vSphere 9 und der ONTAP Tools für VMware vSphere 10

Erfahren Sie, wie eine Migration von ONTAP-Tools für VMware vSphere 9 zu ONTAP-Tools für VMware vSphere 10.1 genau das Richtige für Sie ist. Die aktuellsten Informationen zur Kompatibilität finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

Funktion	ONTAP-Tools 9.13	ONTAP-Tools 10.1
Wichtiges Wertversprechen	Optimieren und vereinfachen Sie den täglichen Betrieb von 0 bis 2 durch verbesserte Sicherheits-, Compliance- und Automatisierungsfunktionen	Entwicklung der ONTAP Tools 10.x in Richtung 9.x-Parität mit erweiterter Hochverfügbarkeit, Performance und Skalierungslimits
ONTAP Release Qualification	ONTAP 9.9.1 bis ONTAP 9.15.1	ONTAP 9.12.1 bis ONTAP 9.14.1
VMware Versionsunterstützung	VSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.5 auf VMware Live Site Recovery 9.0	VSphere 7.x-8.x VMware Site Recovery Manager (SRM) 8.7 auf VMware Live Site Recovery 9.0
Protokollunterstützung	NFS- und VMFS-Datastores: NFS (v3 und v4.1), VMFS (iSCSI und FCP) VVols-Datastores: ISCSI, FCP, NVMe/FC, NFS v3	NFS- und VMFS-Datastores: NFS (v3 und v4.1), VMFS (iSCSI) VVols-Datastores: ISCSI, NFS v3
Skalierbarkeit	Hosts und VMs: 300 Hosts, bis zu 10.000 VMs Datastores: 600 NFS, bis zu 50 VMFS, bis zu 250 VVols: Bis zu 14.000	Hosts und VMs: 600 Hosts VVols: Bis zu 140.000
Beobachtbarkeit	Dashboards für Performance-, Kapazitäts- und Host-Compliance, dynamische VM- und Datastore-Berichte	Aktualisierte Dashboards für Performance, Kapazität und Host Compliance, dynamische VM- und Datastore-Berichte

Funktion	ONTAP-Tools 9.13	ONTAP-Tools 10.1
Datensicherung	SRA-Replizierung für VMFS und NFS FlexVols basierte Replizierung für VVols SCV-Integration und Interoperabilität für Backups	SRA-Replizierung für iSCSI VMFS und NFS v3 Datastores

Konzepte

Überblick über die ONTAP Tools für VMware vSphere

ONTAP Tools für VMware vSphere sind eine Sammlung von Tools für das Lifecycle Management von Virtual Machines. Sie lässt sich in das VMware Ecosystem integrieren, um die Bereitstellung von Datastores zu unterstützen und bietet grundlegende Sicherung für Virtual Machines. Mit den ONTAP Tools für VMware vSphere können Administratoren das Storage Lifecycle Management nahtlos managen

Die ONTAP Tools für die Version VMware vSphere 10.1 sind eine Sammlung horizontal skalierbarer, ereignisgesteuerter Microservices, die als offene virtuelle Appliance (OVA) implementiert werden. Diese Version verfügt über REST-API-Integration mit ONTAP.

ONTAP Tools für VMware vSphere umfassen:

- Funktionen von Virtual Machines wie grundlegende Sicherung und Disaster Recovery
- VASA Provider für granulares VM-Management
- Richtlinienbasiertes Storage-Management
- Storage Replication Adapter (SRA)

Schlüsselkonzepte und -Begriffe

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

Zertifizierungsstelle (CA)

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

Dual-Stack

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

Hochverfügbarkeit

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

Logical Unit Number (LUN)

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

ONTAP Tools Manager

Der ONTAP Tools Manager bietet ONTAP Tools für VMware vSphere Administratoren mehr Kontrolle über die gemanagten vCenter Server Instanzen und On-Board Storage Backends. ONTAP Tools Manager unterstützt

Sie beim Management von vCenter Server-Instanzen, Speicher-Back-Ends, Zertifikaten, Passwörtern und Log-Bundle-Downloads.

Offene virtuelle Appliance (OVA)

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

SnapMirror aktiv (SMAS)

SnapMirror Active Sync ermöglicht Business Services auch bei einem vollständigen Standortausfall den Betrieb weiter und unterstützt Applikationen bei einem transparenten Failover mithilfe einer sekundären Kopie. Um einen Failover mit SnapMirror Active Sync auszulösen, sind manuelle Eingriffe oder benutzerdefiniertes Scripting erforderlich.

Storage Replication Adapter (SRA)

SRA ist die Software des Storage-Anbieters, die innerhalb der SRM Appliance installiert wird. Der Adapter ermöglicht die Kommunikation zwischen Site Recovery Manager und einem Storage Controller auf Storage Virtual Machine (SVM)-Ebene und der Konfiguration auf Cluster-Ebene.

Storage Virtual Machine (SVM)

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

Virtual Machine File System (VMFS)

VMFS ist ein geclustertes Filesystem, das speziell zum Speichern von VM-Dateien in VMware vSphere Umgebungen entwickelt wurde.

Virtuelle Volumes (VVols)

VVols bieten eine Abstraktion auf Volume-Ebene für den von einer Virtual Machine verwendeten Storage. Sie bietet mehrere Vorteile und eine Alternative zur Verwendung einer herkömmlichen LUN. Ein vVol Datastore wird normalerweise mit einer einzelnen LUN verknüpft, die als Container für die VVols fungiert.

VM-Storage-Richtlinie

VM-Storage-Richtlinien werden in vCenter Server unter Richtlinien und Profile erstellt. Für VVols erstellen Sie mithilfe von Regeln des NetApp VVols Storage-Typ-Providers eine Regelsammlung.

VMware Site Recovery Manager (SRM)

SRM bietet Business Continuity, Disaster Recovery, Standortmigration und unterbrechungsfreie Testfunktionen für virtuelle VMware-Umgebungen.

VMware vSphere APIs für Storage Awareness (VASA)

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

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

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

VVols Datastore

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

Kein RPO

RPO steht für den Recovery Point Objective. Dieser Wert ist das Maß des Datenverlusts, das während eines bestimmten Zeitraums als akzeptabel erachtet wird. Ein RPO von null bedeutet, dass kein Datenverlust akzeptabel ist.

Rollenbasierte Zugriffssteuerung

Überblick über die rollenbasierte Zugriffssteuerung in ONTAP Tools für VMware vSphere

VCenter Server bietet rollenbasierte Zugriffssteuerung (RBAC), mit der Sie den Zugriff auf vSphere-Objekte steuern können. VCenter Server bietet zentralisierte Authentifizierungs- und Autorisierungsservices auf vielen verschiedenen Ebenen innerhalb des Bestands, wobei Benutzer- und Gruppenrechte mit Rollen und Privileges verwendet werden. VCenter Server verfügt über fünf Hauptkomponenten für das Management von RBAC:

Komponenten	Beschreibung
Berechtigungen	Eine Berechtigung aktiviert oder verweigert den Zugriff auf Aktionen in vSphere.
Rollen	Eine Rolle enthält mindestens eine Systemberechtigung, bei der jede Berechtigung ein Administratorrecht für ein bestimmtes Objekt oder einen Objekttyp im System definiert. Wenn Sie einem Benutzer eine Rolle zuweisen, erbt der Benutzer die Fähigkeiten der in dieser Rolle definierten Berechtigungen.
Benutzer und Gruppen	Benutzer und Gruppen werden in Berechtigungen verwendet, um Rollen aus Active Directory (AD) zuzuweisen. VCenter Server verfügt über eigene lokale Benutzer und Gruppen, die Sie verwenden können.

Berechtigungen	Mit Berechtigungen können Sie Privileges Benutzern oder Gruppen zuweisen, um bestimmte Aktionen durchzuführen und Änderungen an Objekten innerhalb von vCenter Server vorzunehmen. VCenter Server-Berechtigungen betreffen nur die Benutzer, die sich bei vCenter Server anmelden, und nicht die Benutzer, die sich direkt bei einem ESXi-Host anmelden.
Objekt	Eine Einheit, auf der Aktionen ausgeführt werden. VMware vCenter Objekte sind Datacenter, Ordner, Ressourcen-Pools, Cluster, Hosts, und VMs

Um eine Aufgabe erfolgreich abzuschließen, sollten Sie über die entsprechenden RBAC-Rollen für vCenter Server verfügen. Während einer Aufgabe prüft ONTAP Tools für VMware vSphere die vCenter Server-Rollen eines Benutzers, bevor die ONTAP-Berechtigungen des Benutzers überprüft werden.

Die vCenter Server-Rollen gelten für ONTAP-Tools für VMware vSphere vCenter-Benutzer und nicht für Administratoren. Standardmäßig haben Administratoren vollen Zugriff auf das Produkt und benötigen keine Rollen, die ihnen zugewiesen sind.

Die Benutzer und Gruppen erhalten Zugriff auf eine Rolle, indem sie Teil einer vCenter Server-Rolle sind.

Wichtige Punkte zum Zuweisen und Ändern von Rollen für vCenter Server

Sie müssen nur vCenter Server-Rollen einrichten, wenn Sie den Zugriff auf vSphere-Objekte und -Aufgaben einschränken möchten. Andernfalls können Sie sich als Administrator anmelden. Mit dieser Anmeldung können Sie automatisch auf alle vSphere Objekte zugreifen.

Bei der Zuweisung einer Rolle werden ONTAP-Tools für VMware vSphere-Aufgaben festgelegt, die ein Benutzer ausführen kann. Sie können eine Rolle jederzeit ändern. Wenn Sie die Berechtigungen innerhalb einer Rolle ändern, muss sich der Benutzer, der dieser Rolle zugeordnet ist, abmelden und sich dann wieder anmelden, um die aktualisierte Rolle zu aktivieren.

Standardrollen im Paket mit ONTAP-Tools für VMware vSphere

Zur Vereinfachung der Arbeit mit vCenter Server-Berechtigungen und RBAC bietet das ONTAP Tool für VMware vSphere standardmäßige ONTAP Tools für VMware vSphere Rollen, mit denen Sie wichtige ONTAP Tools für VMware vSphere Aufgaben ausführen können. Es gibt auch eine schreibgeschützte Rolle, mit der Sie die Informationen anzeigen, aber keine Aufgaben ausführen können.

Sie können ONTAP-Tools für VMware vSphere-Standardrollen anzeigen, indem Sie auf der vSphere-Client-Startseite auf **Rollen** klicken. Mithilfe der Rollen, die ONTAP Tools für VMware vSphere bieten, können Sie folgende Aufgaben ausführen:

* Rolle*	**Beschreibung**
NetApp ONTAP-Tools für VMware vSphere Administrator	Bietet alle nativen vCenter Server-Berechtigungen und ONTAP-Tools-spezifischen Berechtigungen, die für die Ausführung einiger ONTAP-Tools für VMware vSphere-Aufgaben erforderlich sind.

NetApp ONTAP-Tools für VMware vSphere schreibgeschützt	Bietet schreibgeschützten Zugriff auf ONTAP Tools. Diese Benutzer können keine ONTAP Tools für VMware vSphere Aktionen ausführen, die zugriffsgesteuert sind.
NetApp ONTAP Tools für VMware vSphere Bereitstellung	Bietet einige der nativen vCenter Server-Berechtigungen und ONTAP-Tools-spezifischen Berechtigungen, die für die Bereitstellung von Speicher erforderlich sind. Sie können die folgenden Aufgaben ausführen: • Erstellen neuer Datenspeicher • Managen von Datastores

Die Administratorrolle des ONTAP Tools Managers ist nicht bei vCenter Server registriert. Diese Rolle ist spezifisch für den ONTAP Tools Manager.

Wenn in Ihrem Unternehmen Rollen implementiert werden müssen, die restriktiver sind als die standardmäßigen ONTAP Tools für VMware vSphere Rollen, können Sie neue Rollen mit ONTAP Tools für VMware vSphere Rollen erstellen.

In diesem Fall klonen Sie die erforderlichen ONTAP Tools für VMware vSphere Rollen und bearbeiten dann die geklonte Rolle nur so, dass sie über die Berechtigungen verfügt, die Ihr Benutzer benötigt.

Berechtigungen für ONTAP Storage Back-Ends und vSphere Objekte

Wenn die Berechtigungen für vCenter Server ausreichend sind, prüfen ONTAP Tools für VMware vSphere die RBAC-Berechtigungen von ONTAP (Ihre ONTAP Rolle), die den Anmeldedaten für Storage-Back-Ends (Benutzername und Passwort) zugeordnet sind. um zu ermitteln, ob Sie über ausreichende Berechtigungen verfügen, um die Speichervorgänge auszuführen, die von diesen ONTAP-Tools für VMware vSphere auf diesem Speicher-Back-End erforderlich sind. Wenn Sie über die richtige ONTAP Privileges verfügen, können Sie auf die Storage-Back-Ends zugreifen und ONTAP Tools für VMware vSphere Aufgaben durchführen. Die ONTAP-Rollen bestimmen ONTAP Tools für VMware vSphere Aufgaben, die Sie auf dem Storage Back-End durchführen können.

Komponenten von vCenter Server-Berechtigungen

Der vCenter Server erkennt Berechtigungen und keine Berechtigungen. Jede vCenter Server-Berechtigung besteht aus drei Komponenten.

Der vCenter Server verfügt über die folgenden Komponenten:

- Mindestens eine Berechtigung (die Rolle)

  Die Berechtigungen definieren die Aufgaben, die ein Benutzer ausführen kann.

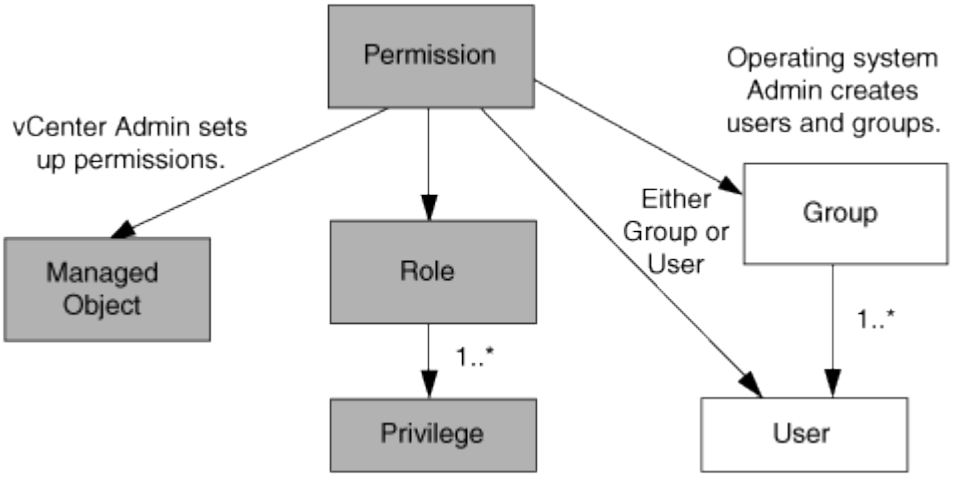
- VSphere Objekt

  Das Objekt ist das Ziel für die Aufgaben.

- Ein Benutzer oder eine Gruppe

  Der Benutzer oder die Gruppe definiert, wer die Aufgabe ausführen kann.

In diesem Diagramm zeigen die grauen Felder Komponenten im vCenter Server an, und die weißen Felder geben die Komponenten an, die im Betriebssystem vorhanden sind, auf dem vCenter Server ausgeführt wird.



Berechtigungen

ONTAP Tools für VMware vSphere beinhalten zwei Arten von Berechtigungen:

- Native vCenter Server-Berechtigungen

  Diese Berechtigungen werden mit dem vCenter Server geliefert.

- Spezifische Berechtigungen für ONTAP-Tools

  Diese Berechtigungen werden für bestimmte ONTAP-Tools für VMware vSphere-Tasks definiert. Sie sind einzigartig in den ONTAP Tools für VMware vSphere.

ONTAP-Tools für VMware vSphere-Tasks erfordern sowohl ONTAP-Tools-spezifische Berechtigungen als auch native vCenter Server-Berechtigungen. Diese Berechtigungen stellen die „`Rolle`“ für den Benutzer dar. Eine Berechtigung kann mehrere Berechtigungen haben. Diese Berechtigungen gelten für einen Benutzer, der beim vCenter Server angemeldet ist.

Zur Vereinfachung der Arbeit mit RBAC für vCenter Server bietet ONTAP Tools für VMware vSphere mehrere Standardrollen, die alle spezifischen und nativen Berechtigungen von ONTAP enthalten, die für die Ausführung von ONTAP Tools für VMware vSphere Aufgaben erforderlich sind.

Wenn Sie die Berechtigungen innerhalb einer Berechtigung ändern, sollte sich der Benutzer, der mit dieser Berechtigung verknüpft ist, ausloggen und sich dann anmelden, um die aktualisierte Berechtigung zu aktivieren.

VSphere Objekte

Berechtigungen werden mit vSphere Objekten verknüpft, z. B. vCenter Server, ESXi Hosts, Virtual Machines, Datastores, Datacenter, Und Ordner. Sie können jedem vSphere-Objekt Berechtigungen zuweisen. Auf Grundlage der Berechtigung, die einem vSphere-Objekt zugewiesen ist, bestimmt der vCenter Server, wer welche Aufgaben auf dem Objekt ausführen kann. Für ONTAP-Tools für VMware vSphere-spezifische Aufgaben werden Berechtigungen nur auf der Root-Ordnerebene (vCenter Server) und nicht auf einer anderen

Einheit zugewiesen und validiert. Mit Ausnahme des VAAI-Plug-in-Betriebs, wenn Berechtigungen für den betreffenden ESXi-Host validiert werden.

Benutzer und Gruppen

Sie können Active Directory (oder den lokalen vCenter Server-Rechner) verwenden, um Benutzer und Benutzergruppen einzurichten. Sie können dann vCenter Server-Berechtigungen verwenden, um diesen Benutzern oder Gruppen Zugriff zu gewähren, damit sie spezifische ONTAP-Tools für VMware vSphere-Aufgaben ausführen können.

Diese vCenter Server-Berechtigungen gelten für ONTAP-Tools für VMware vSphere vCenter-Benutzer, nicht für ONTAP-Tools für VMware vSphere-Administratoren. Standardmäßig haben ONTAP-Tools für VMware vSphere-Administratoren vollen Zugriff auf das Produkt und benötigen keine ihnen zugewiesenen Berechtigungen.

Benutzern und Gruppen sind ihnen keine Rollen zugewiesen. Sie erhalten Zugriff auf eine Rolle, indem sie Teil einer vCenter Server-Berechtigung sind.

Zuweisen und Ändern von Berechtigungen für vCenter Server

Bei der Arbeit mit vCenter Server-Berechtigungen gibt es einige wichtige Punkte, die Sie beachten sollten. Ob eine ONTAP-Tools für VMware vSphere-Aufgabe erfolgreich ist, hängt davon ab, wo Sie eine Berechtigung zugewiesen haben oder welche Aktionen ein Benutzer nach der Änderung einer Berechtigung ergriffen hat.

Berechtigungen werden zugewiesen

Sie müssen nur vCenter Server-Berechtigungen einrichten, wenn Sie den Zugriff auf vSphere-Objekte und -Aufgaben einschränken möchten. Andernfalls können Sie sich als Administrator anmelden. Mit dieser Anmeldung können Sie automatisch auf alle vSphere Objekte zugreifen.

Bei der Zuweisung von Berechtigungen werden ONTAP-Tools für VMware vSphere-Aufgaben bestimmt, die ein Benutzer ausführen kann.

Um die Fertigstellung einer Aufgabe zu gewährleisten, sollten Sie manchmal Berechtigungen auf einer höheren Ebene zuweisen, z. B. das Stammobjekt. Dies ist der Fall, wenn eine Aufgabe eine Berechtigung erfordert, die nicht auf ein bestimmtes vSphere-Objekt angewendet wird (z. B. Tracking the Task), oder wenn eine erforderliche Berechtigung auf ein nicht-vSphere-Objekt (z. B. ein Storage-System) angewendet wird.

In diesen Fällen können Sie eine Berechtigung so einrichten, dass sie von den untergeordneten Entitäten übernommen wird. Sie können den untergeordneten Entitäten auch andere Berechtigungen zuweisen. Die einer untergeordneten Entität zugewiesene Berechtigung überschreibt immer die Berechtigung, die von der übergeordneten Einheit übernommen wurde. Dies bedeutet, dass Sie einer untergeordneten Entität Berechtigungen erteilen können, um den Umfang einer Berechtigung einzuschränken, die einem Stammobjekt zugewiesen und von der untergeordneten Entität geerbt wurde.

Sofern die Sicherheitsrichtlinien Ihres Unternehmens keine restriktiveren Berechtigungen erfordern, empfiehlt es sich, dem Root-Objekt (auch als Stammordner bezeichnet) Berechtigungen zuzuweisen.

Berechtigungen und nicht vSphere Objekte

Die von Ihnen erstellte Berechtigung wird auf ein nicht-vSphere-Objekt angewendet. Beispielsweise ist ein Storage-System kein vSphere-Objekt. Wenn sich eine Berechtigung auf ein Speichersystem bezieht, sollten Sie die Berechtigung, die diese Berechtigung enthält, ONTAP-Tools für das VMware vSphere-Stammobjekt zuweisen, da es kein vSphere-Objekt gibt, dem Sie es zuweisen können.

Beispielsweise sollten alle Berechtigungen, die eine Berechtigung wie ONTAP Tools für VMware vSphere-Berechtigung „Speichersysteme hinzufügen/ändern/überspringen“ enthalten, auf der Root-Objektebene zugewiesen werden.

Ändern von Berechtigungen

Sie können jederzeit eine Berechtigung ändern.

Wenn Sie die Berechtigungen innerhalb einer Berechtigung ändern, muss sich der mit dieser Berechtigung verknüpfte Benutzer abmelden und sich dann wieder anmelden, um die aktualisierte Berechtigung zu aktivieren.

Berechtigungen für ONTAP-Tools für VMware vSphere-Tasks erforderlich

Für verschiedene ONTAP-Tools für VMware vSphere-Tasks sind unterschiedliche Kombinationen von Berechtigungen für ONTAP-Tools für VMware vSphere sowie native vCenter Server-Berechtigungen erforderlich.

Um auf die ONTAP Tools für die GUI von VMware vSphere zuzugreifen, sollten Sie über die für ONTAP Tools spezifische Berechtigung zur Ansicht auf der korrekten vSphere Objektebene verfügen. Wenn Sie sich ohne diese Berechtigung anmelden, zeigt ONTAP Tools für VMware vSphere eine Fehlermeldung an, wenn Sie auf das NetApp-Symbol klicken und verhindert, dass Sie auf ONTAP-Tools zugreifen können.

Mit der Berechtigung **Ansicht** können Sie auf ONTAP-Tools für VMware vSphere zugreifen. Mit dieser Berechtigung können Sie keine Aufgaben in ONTAP Tools für VMware vSphere ausführen. Um alle ONTAP-Tools für VMware vSphere Aufgaben auszuführen, sollten Sie über die entsprechenden spezifischen und nativen Berechtigungen für ONTAP-Tools für diese Aufgaben verfügen.

Die Zuweisungsebene legt fest, welche Teile der Benutzeroberfläche angezeigt werden können. Wenn Sie dem Stammobjekt (Ordner) die Berechtigung Ansicht zuweisen, können Sie ONTAP-Tools für VMware vSphere aufrufen, indem Sie auf das Symbol NetApp klicken.

Sie können die View Berechtigung einer anderen vSphere Objektebene zuweisen. Dadurch sind jedoch die ONTAP Tools für die VMware vSphere Menüs beschränkt, die Sie sehen und verwenden können.

Das Root-Objekt ist der empfohlene Ort, um alle Berechtigungen zuzuweisen, die die View-Berechtigung enthalten.

Empfohlene ONTAP-Rollen für ONTAP Tools für VMware vSphere

Sie können mehrere empfohlene ONTAP-Rollen für die Arbeit mit ONTAP Tools für VMware vSphere und rollenbasierte Zugriffssteuerung einrichten. Diese Rollen enthalten die ONTAP-Berechtigungen, die zur Durchführung der Speichervorgänge erforderlich sind, die von ONTAP-Tools für VMware vSphere-Aufgaben ausgeführt werden.

Um neue Benutzerrollen zu erstellen, müssen Sie sich als Administrator der Speichersysteme, auf denen

ONTAP ausgeführt wird, einloggen. Sie können ONTAP Rollen mit ONTAP System Manager 9.8P1 oder höher erstellen.

Jeder ONTAP-Rolle ist ein Benutzername- und Passwort-Paar zugeordnet, das die Anmeldeinformationen der Rolle darstellt. Wenn Sie sich nicht mit diesen Anmeldedaten anmelden, können Sie nicht auf die Speichervorgänge zugreifen, die der Rolle zugeordnet sind.

Als Sicherheitsmaßnahme werden die ONTAP-Tools für VMware vSphere-spezifische ONTAP-Rollen hierarchisch geordnet. Dies bedeutet, dass die erste Rolle die restriktivste ist und nur über die Berechtigungen verfügt, die mit dem grundlegendsten Satz von ONTAP Tools für VMware vSphere Storage-Vorgänge verknüpft sind. Die nächste Rolle umfasst ihre eigenen Berechtigungen und alle Berechtigungen, die mit der vorherigen Rolle verknüpft sind. Jede weitere Rolle ist hinsichtlich der unterstützten Speichervorgänge weniger restriktiv.

Im Folgenden finden Sie einige der empfohlenen ONTAP RBAC-Rollen beim Einsatz von ONTAP Tools für VMware vSphere. Nachdem Sie diese Rollen erstellt haben, können Sie sie Benutzern zuweisen, die Aufgaben im Zusammenhang mit Speicher ausführen müssen, z. B. beim Bereitstellen von virtuellen Maschinen.

* Rolle*	**Privilegien**
Ermitteln	Diese Rolle ermöglicht es Ihnen, Storage-Systeme hinzuzufügen.
Speicher Erstellen	Mit dieser Rolle können Sie Speicher erstellen. Diese Rolle umfasst auch alle Berechtigungen, die mit der Ermittlungs-Rolle verknüpft sind.
Speicher Ändern	Mit dieser Rolle können Sie Speicher ändern. Diese Rolle umfasst auch alle Berechtigungen, die der Rolle Ermittlung und der Rolle Speicher erstellen zugeordnet sind.
Speicher Zerstören	Mit dieser Rolle können Sie Speicher zerstören. Diese Rolle umfasst auch alle Berechtigungen, die der Rolle Ermittlung, der Rolle Speicher erstellen und der Rolle Speicher ändern zugeordnet sind.

Wenn Sie ONTAP-Tools für VMware vSphere verwenden, sollten Sie auch eine Policy-Based Management (PBM)-Rolle einrichten. Diese Rolle ermöglicht Ihnen das Storage-Management mithilfe von Storage-Richtlinien. Diese Rolle erfordert, dass Sie auch die Rolle “Diskovery” einrichten.

Hochverfügbarkeit für ONTAP Tools für VMware vSphere

ONTAP Tools für VMware vSphere unterstützen eine HA-Konfiguration (High Availability), damit die ONTAP Tools für VMware vSphere bei einem Ausfall ohne Unterbrechungen funktionieren.

Die Hochverfügbarkeitslösung (HA) sorgt für ein schnelles Recovery nach Ausfällen, die auf folgende Komponenten zurückzuführen sind:

- Host-Ausfall

> Es wird nur der Ausfall eines einzelnen Nodes unterstützt.

- Netzwerkausfall
- Fehler bei Virtual Machine (Ausfall des Gastbetriebssystems)
- Absturz der Applikation (ONTAP-Tools)

Für ONTAP Tools für VMware vSphere ist keine zusätzliche Konfiguration erforderlich, um Hochverfügbarkeit zu gewährleisten.

ONTAP Tools für VMware vSphere unterstützen vCenter HA nicht.

AutoSupport

AutoSupport ist ein Mechanismus, der proaktiv den Zustand Ihres Systems überwacht und automatisch Meldungen an den technischen Support von NetApp, Ihre interne Support-Abteilung und einen Support-Partner sendet.

AutoSupport ist standardmäßig aktiviert, wenn Sie das Storage-System zum ersten Mal konfigurieren. AutoSupport beginnt 24 Stunden nach Aktivierung von AutoSupport mit dem Senden von Meldungen an den technischen Support.

Sie können AutoSupport nur zum Zeitpunkt der Bereitstellung aktivieren oder deaktivieren. Es wird empfohlen, die Funktion aktiviert zu lassen. Durch das Aktivieren von AutoSupport werden Probleme schneller erkannt und schneller gelöst. Das System erfasst AutoSupport-Informationen und speichert diese lokal, selbst wenn die AutoSupport deaktiviert ist. Der Bericht wird jedoch nicht an ein Netzwerk gesendet. Für eine erfolgreiche Übertragung müssen Sie 216.240.21.18 // support.netapp.com URL in Ihr Netzwerk einfügen.

Implementieren Sie ONTAP-Tools für VMware vSphere

Voraussetzungen für die Bereitstellung von ONTAP-Tools für VMware vSphere

Bevor Sie ONTAP Tools für VMware vSphere implementieren, sollten Sie mit den Speicherplatzanforderungen für das Implementierungspaket und einigen grundlegenden Host-Systemanforderungen vertraut sein.

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

- **Platzanforderungen für Installationspaket pro Knoten**
  - 10 GB bei Thin Provisioning-Installationen
  - 248 GB für Thick Provisioning-Installationen
- **Größenanforderungen für das Host-System pro Knoten** Empfohlener Speicher je nach Größe der Bereitstellung und pro Knoten ist wie in der folgenden Tabelle dargestellt:

Art der Bereitstellung	* CPUs*	**Speicher (GB)**
Klein (S)	8	16
Mittel (M)	12	24
Groß (L)	16	32

"Konfigurationsbeschränkungen für die Implementierung von ONTAP Tools für VMware vSphere"Weitere Informationen finden Sie unter.

Mindestanforderungen hinsichtlich Storage und Applikationen

Storage, Host und Applikationen	**Mindestversionsanforderungen**
ONTAP	Neueste Patch-Version von ONTAP 9.12.1, 9.13.1 oder 9.14.1
ESXi-Hosts	ESXi 7.0.3
VCenter Server	VCenter 7.0U3
VASA-Provider	3,0
OVA-Anwendung	10,1

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

"Interoperabilitäts-Matrix-Tool"

Weitere Implementierungsüberlegungen

Sie sollten bei der Anpassung der Implementierung von ONTAP Tools einige Anforderungen berücksichtigen.

Benutzerkennwort der Anwendung

Dies ist das dem Administratorkonto zugewiesene Kennwort. Aus Sicherheitsgründen wird empfohlen, dass das Passwort acht bis dreißig Zeichen lang ist und mindestens ein oberes, ein unteres, eine Ziffer und ein Sonderzeichen enthält.

Anmeldedaten für die Appliance-Wartungskonsole

Sie sollten über den Benutzernamen „`maint`“ auf die Wartungskonsole zugreifen. Sie können das Passwort für den Benutzer „`maint`“ während der Bereitstellung festlegen. Sie können die Option Gastbetriebssystem neu starten verwenden, die während des VM-Neustarts in vCenter Server verfügbar ist, um das Passwort zu ändern.

Netzwerkeigenschaften von Appliances

Geben Sie einen gültigen (nicht qualifizierten) DNS-Hostnamen sowie die statische IP-Adresse für ONTAP-Tools für VMware vSphere und die anderen Netzwerkparameter an. Die angegebenen IP-Adressen sollten über das VLAN-Netzwerk zugänglich sein, das Sie während der Bereitstellung auswählen. DHCP wird für die ONTAP-Tools der VMware vSphere 10.1-Version nicht unterstützt. Alle diese Parameter sind für eine ordnungsgemäße Installation und Betrieb erforderlich.

Laden Sie ONTAP Tools für VMware vSphere herunter

Sie können die `.zip` Datei, die Binärdateien (*.ova*) und signierte Zertifikate für ONTAP-Tools für VMware vSphere enthält, von der herunterladen "NetApp Support-Website".

Nach Abschluss der Implementierung werden die ONTAP Tools für VMware vSphere und VASA-Produkte in Ihrer Umgebung installiert. ONTAP Tools für VMware vSphere funktionieren standardmäßig, sobald Sie das Implementierungsmodell ausgewählt haben und anhand Ihrer Anforderungen auswählen, ob VASA Provider aktiviert werden soll. Weitere Informationen finden Sie unter "Registrieren Sie den VASA Provider mit einer vCenter Server-Instanz" .

Content Library

Eine Content-Bibliothek in VMware ist ein Container-Objekt, das VM-Vorlagen, vApp-Vorlagen und andere Dateitypen speichert. Die Bereitstellung mit Inhaltsbibliothek bietet Ihnen eine nahtlose Erfahrung, da sie nicht von der Netzwerkkonnektivität abhängt.

> Sie sollten die Inhaltsbibliothek auf einem freigegebenen Datastore speichern, sodass alle Hosts in einem Cluster darauf zugreifen können. Sie müssen eine Inhaltsbibliothek erstellen, um die OVA zu speichern, bevor Sie die OVA in der HA-Konfiguration bereitstellen. Erstellen Sie die Inhaltsbibliothek mithilfe der folgenden Schritte:

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Wählen Sie die horizontalen Ellipsen neben vSphere Client aus und wählen Sie **Content Library**.

3. Wählen Sie auf der rechten Seite die Option **Erstellen**.
4. Geben Sie einen Namen für die Bibliothek ein, und erstellen Sie die Inhaltsbibliothek.
5. Navigieren Sie zu der von Ihnen erstellten Inhaltsbibliothek.
6. Wählen Sie **actions** rechts auf der Seite aus und wählen Sie **Import item** und importieren Sie die OVA-Datei.

Konfigurationsbeschränkungen für die Implementierung von ONTAP Tools für VMware vSphere

Die folgende Tabelle bietet einen Leitfaden zur Konfiguration von ONTAP Tools für VMware vSphere.

* Bereitstellung*	**Typ**	**Anzahl der VVols**	**Anzahl der Hosts**	**Protokolltyp**
Einfache Implementierung	Klein (S)	~12.000	32	NFS, iSCSI
Einfache Implementierung	Mittel (M)	~24.000	64	NFS, iSCSI
Hochverfügbarkeit	Klein (S)	~24.000	64	NFS, iSCSI
Hochverfügbarkeit	Mittel (M)	~50.000	128	NFS, iSCSI
Hochverfügbarkeit	Groß (L)	100 ~	256 [ANMERKUNG] die Anzahl der Hosts in der Tabelle zeigt die Gesamtzahl der Hosts von mehreren vCenter.	NFS, iSCSI

Weitere Informationen zur Größenbestimmung des Host-Systems pro Knoten finden Sie unter "Voraussetzungen für die Bereitstellung von ONTAP-Tools für VMware vSphere".

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

Die folgende Tabelle zeigt die unterstützten Zahlen pro SRM-Instanz mit ONTAP Tools für VMware vSphere.

VCenter-Bereitstellungsgröße	**Klein**	**Mittel**
Gesamtzahl der virtuellen Maschinen, die für den Schutz mithilfe einer Array-basierten Replikation konfiguriert wurden	2000	5000
Gesamtzahl der Array-basierten Replikationsschutzgruppen	250	250
Gesamtzahl der Schutzgruppen pro Wiederherstellungsplan	50	50
Anzahl replizierter Datastores	255	255
Anzahl der VMs	4000	7000

In der folgenden Tabelle sind die SRM-Anzahl und die entsprechenden ONTAP Tools für die VMware vSphere Implementierungsgröße aufgeführt.

Anzahl der SRM-Instanzen	Größe der Bereitstellung von ONTAP-Tools
Bis Zu 4	Klein
4 bis 8	Mittel
Mehr als 8	Groß

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

Bereiten Sie die Implementierung von ONTAP Tools für VMware vSphere vor

Vor der Implementierung von ONTAP Tools für VMware vSphere sollten Sie sich der grundlegenden Storage-Backend-Anforderungen, Applikationsanforderungen und Lizenzanforderungen bewusst sein. Planen Sie Ihre Implementierung im Voraus und entscheiden Sie, wie Sie ONTAP Tools für VMware vSphere in Ihrer Umgebung konfigurieren möchten.

Bereitstellung wird vorbereitet

Im Folgenden finden Sie ONTAP Tools für VMware vSphere Anforderungen, bevor Sie mit der Implementierung fortfahren:

1. Konfigurieren und richten Sie Ihre vCenter Server-Umgebung ein.
2. Laden Sie die Datei *.ova* herunter.
3. (Optional) wird für Automatisierungsbenutzer verwendet - Sammeln Sie die Postman-Sammlungen JSON-Datei von NetApp zur Verfügung gestellt.
4. Anmeldedaten des übergeordneten vCenter-Servers für die Bereitstellung der OVA. Das Passwort für den übergeordneten vCenter Server darf diese Sonderzeichen nicht enthalten (€, ', ')
5. Stellen Sie sicher, dass der Host oder der Ressourcenpool, auf dem die OVA bereitgestellt wird"Voraussetzungen für die Bereitstellung von ONTAP-Tools für VMware vSphere", über die im Abschnitt angegebenen Mindestressourcen verfügt.
6. Die Anmeldeinformationen für Ihre vCenter Server-Instanz, mit der sich die ONTAP-Tools für VMware vSphere nach der Bereitstellung zur Registrierung verbinden.
7. Löschen Sie den Browser-Cache.
8. Für die Implementierung ohne HA benötigen Sie drei freie IP-Adressen: Eine freie IP-Adresse für den Load Balancer und eine freie IP-Adresse für die Kubernetes-Kontrollebene und eine IP-Adresse für den Node. Für HA-Implementierung benötigen Sie zusammen mit diesen drei IP-Adressen zwei weitere IP-Adressen für den zweiten und dritten Node. Hostnamen sollten vor der Zuweisung den freien IP-Adressen auf dem DNS zugeordnet werden. Alle fünf IP-Adressen sollten sich in demselben VLAN befinden, das für die Bereitstellung ausgewählt wurde.
9. Nach dem Hochladen sollte die Vorlage der Inhaltsbibliothek nach der Bereitstellung nicht gelöscht werden, da sie bei einem Neustart verwendet wird.
10. Ordnen Sie in einer Multi-vCenter-Bereitstellung, bei der benutzerdefinierte CA-Zertifikate erforderlich sind,

den Domänennamen, auf dem das Zertifikat ausgestellt wird, der virtuellen IP-Adresse zu. Führen Sie eine Prüfung des Domänennamens *nslookup* durch, um zu überprüfen, ob die Domäne auf die beabsichtigte IP-Adresse aufgelöst wird. Die Zertifikate sollten mit dem Domänennamen und der IP-Adresse der Load Balancer-IP-Adresse erstellt werden.

11. IPv4/IPv6-unterstütztes VLAN – Pure IPV6 wird nicht unterstützt. Der gemischte Modus wird unterstützt, wenn VLAN sowohl IPv6- als auch IPv4-Adressen enthält.
12. NTP-Server, der dem vCenter-Server für die Zeitsynchronisierung zur Verfügung gestellt wird.
13. Statische IP-Adresse Konfigurationsdetails für den Knoten oder die VM, auf dem die OVA bereitgestellt wird (obligatorisch), sowie weitere Details.
    a. Hostname des vCenter-Servers (vCenter, in dem die OVA bereitgestellt wird)
    b. VCenter Server-Benutzername (vCenter, in dem die OVA bereitgestellt wird)
    c. VCenter Server-Kennwort (vCenter, in dem die OVA bereitgestellt wird)
    d. Ressourcen-Pool
    e. Daten-LIF (IPv4/IPv6)
    f. Management-LIF
    g. ONTAP-Benutzername
    h. ONTAP-Passwort
    i. SVM-Name
    j. Protokoll
    k. Virtuelle IP-Adressen für die Kubernetes-Kontrollebene:
    l. Drop-down für HA/NICHT-HA
    m. Liste der Hostnamen
    n. IP-Adressen (Zeichenfolge)
    o. Name der Inhaltsbibliothek
    p. OVF-Vorlagenname
    q. IPv6-Gateway (optional)
14. Bevor Sie die ONTAP-Tools für VMware vSphere 10.1 in der nicht-HA-erweiterten und HA-Konfiguration installieren, lesen Sie den KB-Artikel: "Voraussetzungen für die nicht-HA Advanced- und HA-Konfiguration".

Implementierung einer Single Node-Konfiguration ohne Hochverfügbarkeit

Sie können eine Single Node-Konfiguration ohne HA in einer kleinen oder mittelgroßen Konfiguration implementieren.

- Die kleine Konfiguration ohne HA umfasst 8 CPUs und 16 GB RAM.
- Mittelgroße Konfiguration ohne HA enthält 12 CPUs und 24 GB RAM.

Bevor Sie beginnen

Stellen Sie sicher, dass die Netzwerkroute vorhanden ist. Auf das Storage-Datennetzwerk muss über das VM Management-Netzwerk zugegriffen werden können. Beispiel: C1_sti67-vsim-ucs154k_1679633108:> Network

Route create -vserver <SVM> -Destination 0.0.0.0/0 -Gateway <gateway_ip>

Schritte

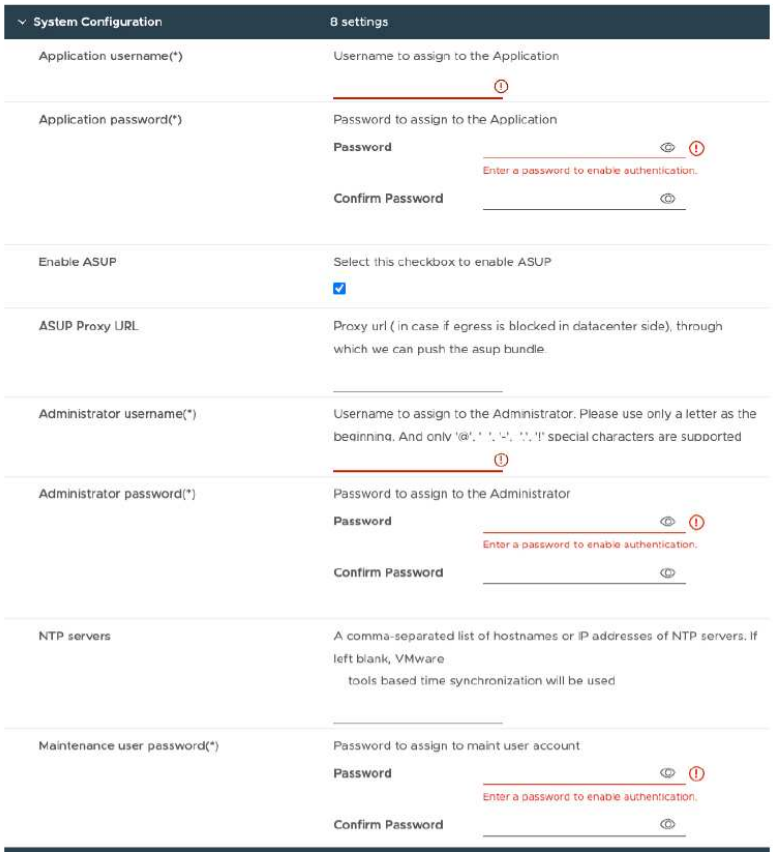
1. Melden Sie sich beim vSphere-Server an.
2. Navigieren Sie zu dem Ressourcenpool oder dem Cluster oder dem Host, auf dem Sie die OVA bereitstellen möchten.
3. Klicken Sie mit der rechten Maustaste auf den gewünschten Speicherort und wählen Sie **OVF-Vorlage bereitstellen…**.

   Stellen Sie keine ONTAP-Tools VMware vSphere Virtual Machine auf einem von ihm gemanagten VVols Datastore bereit.

4. Sie können entweder die URL für die *.ova*-Datei eingeben oder in den Ordner navigieren, in dem die *.ova* -Datei gespeichert ist, und dann **Weiter** auswählen.
5. Wählen Sie einen Namen und Ordner für die virtuelle Maschine aus und wählen Sie **Weiter**.
6. Wählen Sie den Host aus und wählen Sie **Weiter**
7. Überprüfen Sie die Zusammenfassung der Vorlage und wählen Sie **Weiter**.
8. Lesen und akzeptieren Sie die Lizenzvereinbarung und wählen Sie **Weiter**.
9. Wählen Sie im Fenster **Konfiguration** die Option **Einfache Bereitstellung(S)**, **Einfache Bereitstellung(M)** oder **Erweiterte Bereitstellung(S)** oder **erweiterte Bereitstellung(M)** aus.

   Bei den erweiterten Implementierungsoptionen kommt Trident zur dynamischen Storage-bereitstellung für ONTAP zum Erstellen von Volumes zum Einsatz. Bei der einfachen Implementierung werden lokale Storage-Ressourcen zur Erstellung von Volumes verwendet.

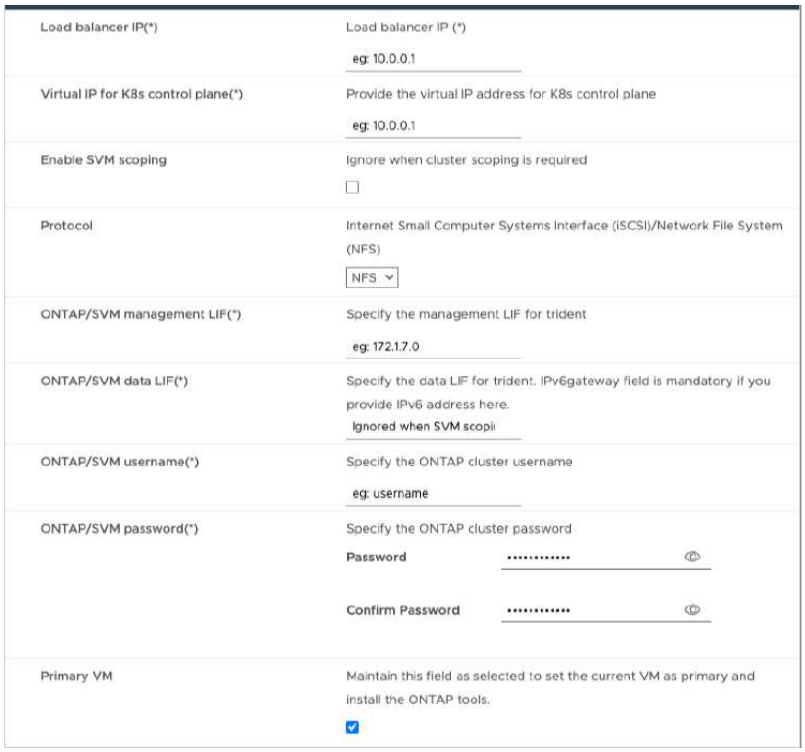
10. Wählen Sie den Datastore aus, an dem Sie die OVA bereitstellen möchten, und wählen Sie **Weiter**.
11. Wählen Sie das Quell- und Zielnetzwerk aus und wählen Sie **Weiter**.
12. Wählen Sie **Template anpassen** > **System Configuration**-Fenster.



Geben Sie die folgenden Details ein: .. Anwendungsbenutzername und Kennwort: Dieser Benutzername und dieses Kennwort werden für die Registrierung von VASA-Provider und SRA im vCenter Server verwendet. .. Das Kontrollkästchen **ASUP aktivieren** ist standardmäßig aktiviert.

AutoSupport kann nur während der Implementierung aktiviert oder deaktiviert werden. .. Geben Sie im Feld **ASUP Proxy URL** diese URL ein, um eine Blockierung der Firewall bei der Übertragung von AutoSupport-Daten zu vermeiden. .. Administratorbenutzername und Administratorkennwort: Dies ist das Passwort, das für die Anmeldung beim ONTAP-Tools-Manager verwendet wird. .. Geben Sie Ihre NTP-Server-Informationen in das Feld **NTP-Server** ein. .. Maintenance User password: Dies wird verwendet, um Zugriff auf 'IH Console Options' zu gewähren. . Geben Sie im Fenster **Vorlage anpassen** > **Bereitstellungskonfiguration** die folgenden Details ein:

+



1. Geben Sie eine verfügbare IP-Adresse in der virtuellen IP-Adresse für die Kubernetes-Kontrollebene ein. Sie benötigen dies für den Kubernetes-API-Server.
2. Wählen Sie die Option **SVM-Scoping aktivieren**, wenn Sie das direkt hinzugefügte SVM-Benutzerkonto verwenden möchten. Aktivieren Sie das Kontrollkästchen nicht, wenn Sie ONTAP Cluster verwenden möchten.

> Wenn der SVM-Umfang aktiviert ist, sollten Sie bereits die SVM-Unterstützung mit der Management-IP-Adresse aktiviert haben.

3. Wählen Sie entweder NFS oder iSCSI im Feld **Protokoll** aus.
4. Geben Sie den ONTAP-Cluster oder die IP-Adresse des SVM-Managements in das Feld **ONTAP/SVM-Management-LIF** ein.
5. Geben Sie den ONTAP Cluster oder die SVM ONTAP/SVM-Daten-LIF ein. Die Daten-LIF sollte zum ausgewählten Protokoll gehören. Wenn beispielsweise das iSCSI-Protokoll ausgewählt ist, sollte eine iSCSI-Daten-LIF angegeben werden.
6. Bei Storage VM können Sie entweder die Standard-Storage-VM-Details Ihres ONTAP angeben oder eine neue Storage-VM erstellen. Geben Sie den Wert nicht in das Feld **Storage VM** ein, wenn die Option SVM-Scoping aktivieren ausgewählt ist, da dieses Feld ignoriert wird.
7. Geben Sie den ONTAP/SVM-Benutzernamen ein. Der Benutzername und das Passwort für ONTAP/SVM sind erforderlich, damit Trident Volumes für die Speicherung der Services-Daten im Falle einer erweiterten Implementierung oder HA-Implementierung erstellt und die Daten bei einem Node-Ausfall von Volumes wiederhergestellt werden können.
8. Geben Sie das ONTAP/SVM-Passwort ein.
9. Die primäre VM ist standardmäßig aktiviert. Ändern Sie diese Auswahl nicht.
    a. Geben Sie im Fenster **Template anpassen** > **Node Configuration** die Netzwerkeigenschaften des OVA ein.

Die hier angegebenen Informationen werden während des Installationsprozesses auf korrekte Muster überprüft. Im Falle einer Abweichung wird eine Fehlermeldung auf der Webkonsole angezeigt, und Sie werden aufgefordert, falsche Informationen zu korrigieren.

10. Geben Sie den Hostnamen ein. Hostnamen, die aus Groß- und Kleinbuchstaben (A-Z), Kleinbuchstaben (a-z), Ziffern (0-9) und dem Bindestrich (-) bestehen, werden nur unterstützt. Wenn Sie Dual-Stack konfigurieren möchten, geben Sie den Hostnamen an, der der IPv6-Adresse zugeordnet ist.
11. Geben Sie die dem Hostnamen zugeordnete IP-Adresse (IPV4) ein. Geben Sie im Fall eines Dual-Stacks alle verfügbaren IPv4-IP-Adressen an, die sich im gleichen VLAN wie die IPv6-Adresse befinden.
12. Geben Sie die IPV6-Adresse im bereitgestellten Netzwerk nur ein, wenn Sie Dual-Talk benötigen.
13. Geben Sie nur die Präfixlänge für IPV6 an.
14. Geben Sie im Feld Netzmaske (nur für IPV4) das Subnetz an, das im bereitgestellten Netzwerk verwendet werden soll.
15. Geben Sie das Gateway im bereitgestellten Netzwerk an.
16. Geben Sie die IP-Adresse des primären DNS-Servers an.
17. Geben Sie die IP-Adresse des sekundären DNS-Servers an.
18. Geben Sie den Suchdomänennamen an, der beim Auflösen des Hostnamens verwendet werden soll.
19. Geben Sie das IPV6-Gateway im bereitgestellten Netzwerk nur an, wenn Sie Dual-Stack benötigen.
    a. Überprüfen Sie die Details im Fenster **Ready to Complete**, wählen Sie **Finish**.

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

    b. Schalten Sie die VM nach Abschluss der Aufgabe ein.

       Die Installation beginnt. Sie können den Installationsfortschritt in der Web-Konsole der VM verfolgen. Im Rahmen der Installation werden Node-Konfigurationen validiert. Die Eingaben, die unter verschiedenen Abschnitten unter der Vorlage „Anpassen“ im OVF-Formular bereitgestellt werden, werden validiert. Bei Unstimmigkeiten werden Sie in einem Dialogfeld aufgefordert, Korrekturmaßnahmen zu ergreifen.

    c. Nehmen Sie die erforderlichen Änderungen in der Dialogaufforderung vor. Verwenden Sie die Tabulatortaste, um über das Bedienfeld zu navigieren, um Ihre Werte einzugeben, **OK** oder **Abbrechen**.
    d. Bei Auswahl von **OK** werden die angegebenen Werte erneut validiert. Mit den ONTAP-Tools für VMware können Sie drei Versuche durchführen, ungültige Werte zu korrigieren. Wenn Sie Probleme nach drei Versuchen nicht beheben können, wird die Produktinstallation angehalten, und Sie werden aufgefordert, die Installation auf einer neuen VM zu versuchen.
    e. Nach der erfolgreichen Installation zeigt die Webkonsole den Status der ONTAP Tools für VMware vSphere an.

Implementierung der HA-Konfiguration

Sie können HA für drei Nodes in kleinen, mittleren oder großen Konfigurationen konfigurieren. Für die HA-Implementierung werden die Servicedaten mithilfe von Trident gespeichert.

- Kleine HA, drei Nodes, enthalten 8 CPUs und 16 GB RAM pro Node.
- Mittlere HA, drei Nodes enthalten 12 CPUs und 24 GB RAM pro Node.
- Große HA, drei Nodes enthalten 16 CPUs und 32 GB RAM pro Node.

Bevor Sie beginnen

Diese Aufgabe enthält Anweisungen zum Installieren von HA Three Nodes in kleinen, mittleren oder hohen Konfigurationen.

> Das Erstellen der Content Library ist ein obligatorischer Schritt für die Bereitstellung der HA-Konfiguration mit drei Nodes. Weitere Informationen finden Sie unter "ONTAP Tools herunterladen" . Weitere Informationen "Erstellen und Verwenden der Inhaltsbibliothek".

Stellen Sie sicher, dass Sie Ihre OVA in Ihre Inhaltsbibliothek importiert haben. Halten Sie den Namen der Inhaltsbibliothek und den Namen des Bibliothekselements, den Sie für Ihr OVA-Element angegeben haben, griffbereit.

> Bevor Sie mit der Bereitstellung fortfahren, setzen Sie den Distributed Resource Scheduler (DRS) des Clusters im Inventar während der Installation von ONTAP-Tools auf „konservativ“. Dadurch wird sichergestellt, dass VMs während der Installation nicht migriert werden.

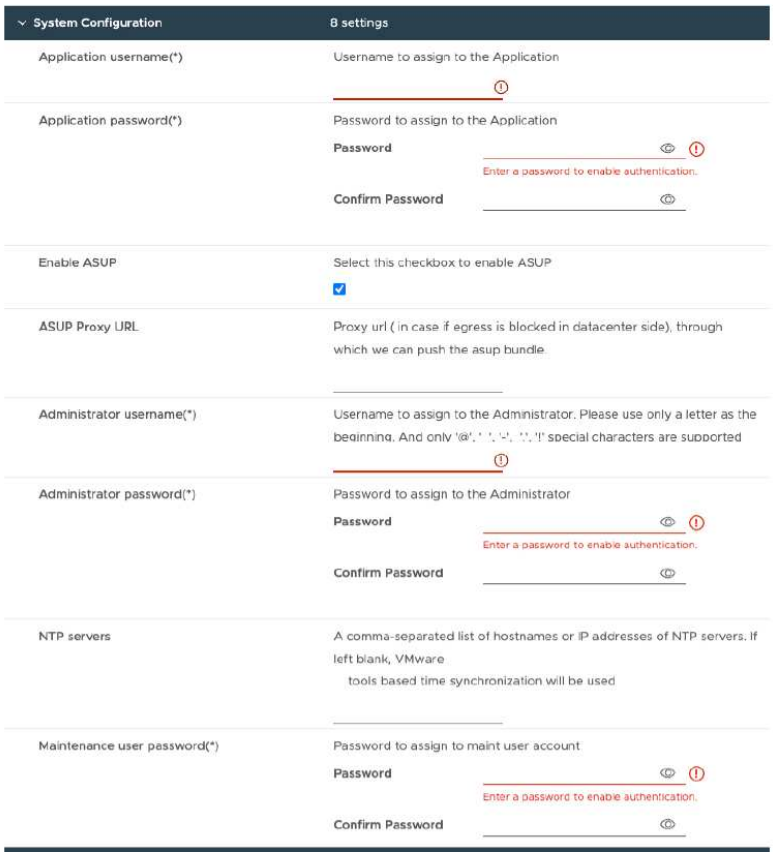
Schritte

1. So stellen Sie vom vSphere-Server bereit:
   a. Melden Sie sich beim vSphere-Server an.
   b. Navigieren Sie zum Ressourcenpool oder Host, auf dem Sie die OVA bereitstellen möchten, und klicken Sie mit der rechten Maustaste auf den gewünschten Speicherort, an dem die VM bereitgestellt werden soll, und wählen Sie **OVF-Vorlage bereitstellen…**

      > Stellen Sie keine ONTAP-Tools VMware vSphere Virtual Machine auf einem von ihm gemanagten VVols Datastore bereit.

   c. Sie können entweder die URL für die *.ova*-Datei eingeben oder in den Ordner navigieren, in dem die *.ova*-Datei gespeichert ist, und dann **Weiter** auswählen
2. So stellen Sie aus der Inhaltsbibliothek bereit:
   a. Öffnen Sie Ihre Inhaltsbibliothek, und klicken Sie auf das Bibliothekselement, das Sie bereitstellen möchten.
   b. Klicken Sie auf **actions** > **New VM from this Template**
3. Wählen Sie einen Namen und Ordner für die virtuelle Maschine aus und wählen Sie **Weiter**.
4. Wählen Sie den Host aus und wählen Sie **Weiter**
5. Überprüfen Sie die Zusammenfassung der Vorlage und wählen Sie **Weiter**.
6. Lesen und akzeptieren Sie die Lizenzvereinbarung und wählen Sie **Weiter**.
7. Wählen Sie im Fenster **Konfiguration** je nach Anforderung **Bereitstellung für hohe Verfügbarkeit**, **Bereitstellung für hohe Verfügbarkeit(M)** oder **Bereitstellung für hohe Verfügbarkeit(L)** aus.
8. Wählen Sie den Speicher für die Konfigurations- und Festplattendateien aus, und wählen Sie **Weiter**.
9. Wählen Sie für jedes Quellnetzwerk das Zielnetzwerk aus, und wählen Sie **Weiter**.

10. Wählen Sie **Template anpassen** > **System Configuration**-Fenster.



Geben Sie die folgenden Details ein:

a. Anwendungsbenutzername und Kennwort: Dieser Benutzername und dieses Kennwort werden für die Registrierung von VASA-Provider und SRA im vCenter Server verwendet.

b. Das Kontrollkästchen **Enable AutoSupport** ist standardmäßig aktiviert. AutoSupport kann nur während der Implementierung aktiviert oder deaktiviert werden.

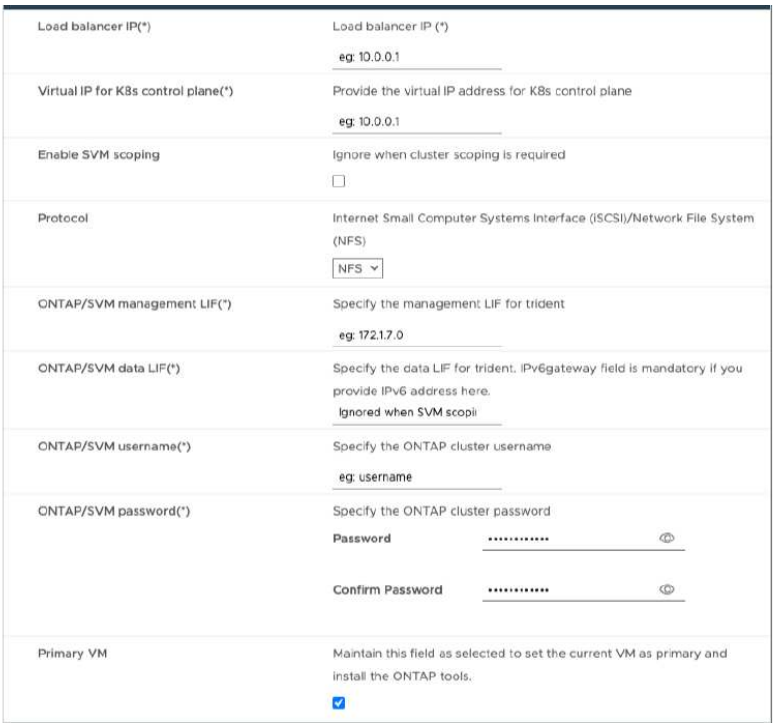
c. Geben Sie im Feld **ASUP Proxy URL** diese URL ein, um eine Blockierung der Firewall bei der Übertragung von AutoSupport-Daten zu vermeiden.

d. Administratorbenutzername und Administratorkennwort: Dies ist das Passwort, das zur Anmeldung beim ONTAP Tools Manager verwendet wird.

e. Geben Sie Ihre NTP-Server-Informationen in das Feld **NTP-Server** ein.

f. Maintenance User password: Dies wird verwendet, um Zugriff auf ‘IH Console Options’ zu gewähren.

11. Geben Sie im Fenster **Vorlage anpassen** > **Bereitstellungskonfiguration** die folgenden Details ein:



a. Geben Sie eine verfügbare IP-Adresse in der virtuellen IP-Adresse für die Kubernetes-Kontrollebene ein. Sie benötigen dies für den Kubernetes-API-Server.

b. Wählen Sie in der erweiterten Bereitstellungsoption **Enable SVM Scoping** aus, wenn Sie das direkt hinzugefügte SVM-Benutzerkonto verwenden möchten. Aktivieren Sie das Kontrollkästchen nicht, wenn Sie ONTAP Cluster verwenden möchten.

> Wenn der SVM-Bereich aktiviert ist, sollte die SVM-Unterstützung mit der Management-IP-Adresse bereits aktiviert sein.

c. Wählen Sie entweder NFS oder iSCSI im Feld **Protokoll** aus.

d. Geben Sie den ONTAP-Cluster oder die IP-Adresse des SVM-Managements in das Feld **ONTAP/SVM-Management-LIF** ein.

e. Geben Sie den ONTAP Cluster oder die SVM ONTAP/SVM-Daten-LIF ein. Die Daten-LIF sollte zum ausgewählten Protokoll gehören. Wenn beispielsweise das iSCSI-Protokoll ausgewählt ist, sollte eine iSCSI-Daten-LIF angegeben werden.

f. Bei Storage VM können Sie entweder die Standard-Storage-VM-Details Ihres ONTAP angeben oder eine neue Storage-VM erstellen. Geben Sie den Wert nicht in das Feld **Storage VM** ein, wenn die Option SVM-Scoping aktivieren ausgewählt ist, da dieses Feld ignoriert wird.

g. Geben Sie den ONTAP/SVM-Benutzernamen ein. Der Benutzername und das Passwort für ONTAP/SVM sind erforderlich, damit Trident Volumes für die Speicherung der Services-Daten im Falle einer erweiterten Implementierung oder HA-Implementierung erstellt und die Daten bei einem Node-Ausfall von Volumes wiederhergestellt werden können.

h. Geben Sie das ONTAP/SVM-Passwort ein.

i. Die primäre VM ist standardmäßig aktiviert. Ändern Sie diese Auswahl nicht.

12. Geben Sie im Fenster **Vorlage anpassen** > **Inhaltsbibliothek Details** den Namen der **Inhaltsbibliothek** und den Namen der **OVF-Vorlage** ein.

13. Geben Sie im Fenster **Vorlage anpassen** > **vCenter-Konfiguration** die Details des vCenter-Servers an, auf dem die Inhaltsbibliothek gehostet wird.

14. Geben Sie im Fenster **Vorlage anpassen** > **Knotenkonfiguration** die Netzwerkeigenschaften der OVA für alle drei Knoten ein.

> Die hier angegebenen Informationen werden während des Installationsprozesses auf korrekte Muster überprüft. Im Falle einer Abweichung wird eine Fehlermeldung auf der Webkonsole angezeigt, und Sie werden aufgefordert, falsche Informationen zu korrigieren.

    a. Geben Sie den Hostnamen ein. Hostnamen, die aus Groß- und Kleinbuchstaben (A-Z), Kleinbuchstaben (a-z), Ziffern (0-9) und dem Bindestrich (-) bestehen, werden nur unterstützt. Wenn Sie Dual-Stack konfigurieren möchten, geben Sie den Hostnamen an, der der IPv6-Adresse zugeordnet ist.
    b. Geben Sie die dem Hostnamen zugeordnete IP-Adresse (IPV4) ein. Geben Sie im Fall eines Dual-Stacks alle verfügbaren IPv4-IP-Adressen an, die sich im gleichen VLAN wie die IPv6-Adresse befinden.
    c. Geben Sie die IPV6-Adresse im bereitgestellten Netzwerk nur ein, wenn Sie Dual Stack benötigen.
    d. Geben Sie nur die Präfixlänge für IPV6 an.
    e. Geben Sie im Feld Netzmaske (nur für IPV4) das Subnetz an, das im bereitgestellten Netzwerk verwendet werden soll.
    f. Geben Sie das Gateway im bereitgestellten Netzwerk an.
    g. Geben Sie die IP-Adresse des primären DNS-Servers an.
    h. Geben Sie die IP-Adresse des sekundären DNS-Servers an.
    i. Geben Sie den Suchdomänennamen an, der beim Auflösen des Hostnamens verwendet werden soll.
    j. Geben Sie das IPV6-Gateway im bereitgestellten Netzwerk nur an, wenn Sie Dual-Stack benötigen.

15. Geben Sie im Fenster **Template anpassen** > **Node 2 Configuration** und **Node 3 Configuration** die folgenden Details ein:
    a. Hostname 2 und 3: Hostnamen, die aus Groß- und Kleinbuchstaben (A-Z), Kleinbuchstaben (a-z), Ziffern (0-9) und dem Bindestrich (-) bestehen, werden nur unterstützt. Wenn Sie Dual-Stack konfigurieren möchten, geben Sie den Hostnamen an, der der IPv6-Adresse zugeordnet ist.
    b. IP-Adresse
    c. IPV6-Adresse
16. Überprüfen Sie die Details im Fenster **Ready to Complete**, wählen Sie **Finish**.

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

17. Schalten Sie die VM nach Abschluss der Aufgabe ein.

    Die Installation beginnt. Sie können den Installationsfortschritt in der Web-Konsole der VM verfolgen. Im Rahmen der Installation werden Node-Konfigurationen validiert. Die Eingaben, die unter verschiedenen Abschnitten unter der Vorlage „Anpassen“ im OVF-Formular bereitgestellt werden, werden validiert. Bei Unstimmigkeiten werden Sie in einem Dialogfeld aufgefordert, Korrekturmaßnahmen zu ergreifen.

18. Nehmen Sie die erforderlichen Änderungen in der Dialogaufforderung vor. Verwenden Sie die Tabulatortaste, um über das Bedienfeld zu navigieren, um Ihre Werte einzugeben, **OK** oder **Abbrechen**.
19. Bei Auswahl von **OK** werden die angegebenen Werte erneut validiert. Mit den ONTAP-Tools für VMware können Sie drei Versuche durchführen, ungültige Werte zu korrigieren. Wenn Sie Probleme nach drei Versuchen nicht beheben können, wird die Produktinstallation angehalten, und Sie werden aufgefordert, die Installation auf einer neuen VM zu versuchen.

20. Nach der erfolgreichen Installation zeigt die Webkonsole den Status der ONTAP Tools für VMware vSphere an.

Stellen Sie Ihre ONTAP Tools für die Einrichtung von VMware vSphere wieder her

Wenn Sie Ihre ONTAP Tools für die VMware vSphere-Einrichtung verlieren, können Sie die ONTAP Tools für die VMware vSphere-Einrichtung unter Verwendung der in den ONTAP Volume-Daten verfügbaren Daten wiederherstellen. Wenn Sie das Setup verlieren, fahren Sie das Setup ordnungsgemäß herunter.

Sie können Ihre ONTAP Tools für die VMware vSphere-Einrichtung nicht wiederherstellen, wenn Probleme mit vCenter Server- oder ONTAP-Datenmanagement-Software auftreten.

Schritte

1. Melden Sie sich beim vSphere-Server an.
2. Navigieren Sie zum Ressourcen-Pool, zum Node-Cluster oder zum Host, auf dem Sie die OVA bereitstellen möchten.
3. Klicken Sie mit der rechten Maustaste auf den gewünschten Speicherort und wählen Sie **OVF-Vorlage bereitstellen**.
4. Sie können entweder die URL für die *.ova*-Datei eingeben oder in den Ordner navigieren, in dem die *.ova* -Datei gespeichert ist, und dann **Weiter** auswählen.

   Sie sollten denselben OVA-Build verwenden, den Sie für die Installation der Wiederherstellungseinrichtung verwendet haben.

5. Wählen Sie einen Namen und Ordner für die virtuelle Maschine aus und wählen Sie **Weiter**.
6. Wählen Sie den Host aus und wählen Sie **Weiter**.
7. Überprüfen Sie die Zusammenfassung der Vorlage und wählen Sie **Weiter**.
8. Lesen und akzeptieren Sie die Lizenzvereinbarung und wählen Sie **Weiter**.
9. Wählen Sie im Fenster **Konfiguration** die Option **Wiederherstellung**.
10. Wählen Sie im Fenster **Speicher auswählen** den Speicher für die Konfigurationen und Festplattendateien aus.
11. Wählen Sie im Fenster **Netzwerke auswählen** für jedes Quellnetzwerk ein Zielnetzwerk aus.

    Sie müssen die IP-Adresse des Load Balancer und die IP-Adresse des Kubernetes API Servers beibehalten. Sie können die Node-IP-Adresse ändern oder dieselbe IP-Adresse beibehalten.

12. Wählen Sie **Template anpassen** > **System Configuration**-Fenster. Geben Sie die folgenden Details ein:
    a. Anwendungsbenutzername und Kennwort: Dieser Benutzername und dieses Kennwort werden für die Registrierung von VASA-Provider und SRA im vCenter Server verwendet. Dies kann sich von dem Benutzernamen und Passwort unterscheiden, die bei der ersten Bereitstellung angegeben wurden.
    b. Das Kontrollkästchen **ASUP aktivieren** ist standardmäßig aktiviert.

AutoSupport kann nur während der Implementierung aktiviert oder deaktiviert werden. .. Geben Sie im Feld **ASUP Proxy URL** diese URL ein, um eine Blockierung der Firewall bei der Übertragung von AutoSupport-Daten zu vermeiden. .. Administratorbenutzername und Administratorkennwort: Dies ist das Passwort, das für die Anmeldung beim ONTAP-Tools-Manager verwendet wird. Dies kann sich von dem Benutzernamen und Passwort unterscheiden, die bei der ersten Bereitstellung angegeben wurden. .. Geben Sie Ihre NTP-Server-Informationen in das Feld **NTP-Server** ein. .. Maintenance user password: Dies wird verwendet, um Zugriff auf Wartungskonsolenoptionen zu gewähren. . Geben Sie im Fenster **Vorlage anpassen** > **Bereitstellungskonfiguration** die während der Bereitstellung angegebenen Details ein. Alle Werte in diesem Abschnitt sollten mit Ausnahme des Daten-LIF-Werts identisch sein, die während der ersten Implementierung angegeben wurden.

> Der Storage-SVM-Name sollte nicht geändert werden, da dort die Recovery-Daten gespeichert werden. Dies gilt auch für direkt hinzugefügte SVM-Benutzerkonten. . Im Fall der HA-Bereitstellung Wiederherstellung, geben Sie die folgenden Details: .. Details zur Content Library .. VCenter-Konfigurationsdetails. . Geben Sie im Fenster **Customize template** > **Node Configuration** die Details gemäß dem Setup ein, das Sie wiederherstellen möchten, nicht-HA oder HA-Setup. . Überprüfen Sie die Details im Fenster **Ready to Complete**, wählen Sie **Finish**.

+ während die Bereitstellungsaufgabe erstellt wird, wird der Fortschritt in der vSphere-Taskleiste angezeigt. . Schalten Sie die VM nach Abschluss der Aufgabe ein.

+ die Installation beginnt. Sie können den Installationsfortschritt in der Web-Konsole der VM verfolgen. Im Rahmen der Installation werden Node-Konfigurationen validiert. Die Eingaben, die unter verschiedenen Abschnitten unter der Vorlage „Anpassen“ im OVF-Formular bereitgestellt werden, werden validiert. Bei Unstimmigkeiten werden Sie in einem Dialogfeld aufgefordert, Korrekturmaßnahmen zu ergreifen. . Nehmen Sie die erforderlichen Änderungen in der Dialogaufforderung vor. Verwenden Sie die Tabulatortaste, um über das Bedienfeld zu navigieren, um Ihre Werte einzugeben, **OK** oder **Abbrechen**. . Bei der Auswahl von **OK** oder **Cancel** werden die angegebenen Werte erneut validiert. Mit den ONTAP-Tools für VMware können Sie drei Versuche durchführen, ungültige Werte zu korrigieren. Wenn Sie Probleme nach drei Versuchen nicht beheben können, wird die Produktinstallation angehalten, und Sie werden aufgefordert, die Installation auf einer neuen VM zu versuchen. . Nach der erfolgreichen Installation zeigt die Webkonsole den Status der ONTAP Tools für VMware vSphere an. Nach erfolgreicher Installation sollten Sie die Hardwareanforderungen gemäß den Richtlinien auf der Seite manuell bearbeiten "Voraussetzungen für die Bereitstellung von ONTAP-Tools für VMware vSphere" .

Fehlercodes für die Bereitstellung

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

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

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

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

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

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

Deployment-Fehlercode	Arbeitsablauf	* Auflösung*
050	Generierung des SSH-Schlüssels fehlgeschlagen	Starten Sie die primäre virtuelle Maschine (VM) neu.
051	Fehler beim Bereitstellen von sekundären VMs	* Wenn die zweite und dritte VM erstellt werden, dann stellen Sie sicher, dass genügend CPU/Speicher vorhanden sind, bevor Sie die sekundären VMs einschalten und die primäre VM neu starten. * Wenn die zweite und dritte VMs in Deploy ONTAP Tools for VMware vSphere Template Task sind, warten Sie, bis die Aufgabe abgeschlossen ist, schalten Sie die VMs ein und starten Sie die primäre VM neu. * Neuimplementierung.
052	Kopieren der SSH-Schlüssel fehlgeschlagen	Starten Sie die primäre VM neu.
053	RKE2 konnte nicht installiert werden	Führen Sie entweder Folgendes aus und starten Sie die primäre VM neu oder Neuimplementierung: Sudo rke2-killall.sh (alle VMs) sudo rke2-uninstall.sh (alle VMs).
054	Einstellung von kubeconfig fehlgeschlagen	Neuimplementierung
055	Fehler beim Bereitstellen der Registrierung	Wenn der Registrierungs-Pod vorhanden ist, warten Sie, bis der Pod bereit ist, starten Sie dann die primäre VM neu oder starten Sie es andernfalls neu.

056	Anmeldung bei ISCSI fehlgeschlagen	Stellen Sie sicher, dass das iSCSI-Protokoll auf ONTAP aktiviert und ordnungsgemäß konfiguriert ist. Stellen Sie sicher, dass die angegebene iSCSI-Daten-LIF-IP-Adresse korrekt und online ist. Starten Sie die VM neu, wenn die vorherigen Punkte korrekt sind. Ansonsten Neuimplementierung.
057	Die Trident-Implementierung ist fehlgeschlagen	*Stellen Sie sicher, dass Management LIF und Data LIF IP Adressen von VM erreichbar sind. * Stellen Sie sicher, dass das NFS- oder iSCSI-Protokoll aktiviert und auf ONTAP richtig konfiguriert ist. *Stellen Sie sicher, dass die angegebene LIF-IP-Adresse für NFS/iSCSI-Daten korrekt und online ist. *Stellen Sie sicher, dass der Benutzername und das Passwort korrekt sind und der Benutzer über ausreichende Berechtigungen verfügt, um ein Volume zu erstellen. * Starten Sie neu, wenn alle oben genannten Punkte korrekt sind. Ansonsten Neuimplementierung.
058	Der Import von Trident ist fehlgeschlagen	*Stellen Sie sicher, dass der Benutzername und das Passwort korrekt sind und der Benutzer über ausreichende Berechtigungen zum Erstellen, Mounten, Klonen und Löschen von Volumes verfügt. *Stellen Sie sicher, dass das gleiche ONTAP-Setup verwendet wird, um das Setup wiederherzustellen und die Wiederherstellung zu wiederholen.
059	Die KubeVip-Bereitstellung ist fehlgeschlagen	Vergewissern Sie sich, dass die während der Implementierung angegebene virtuelle IP-Adresse für die Kubernetes-Kontrollebene und den Load Balancer im selben VLAN gehören und freie IP-Adressen sind. Neu starten, wenn alle vorherigen Punkte korrekt sind. Ansonsten Neuimplementierung.
060	Die Benutzerbereitstellung ist fehlgeschlagen	Neu Starten

061	Die Bereitstellung der Dienste ist fehlgeschlagen	Führen Sie einfache Kubernetes-Fehlerbehebungen wie get Pods, get rs, get svc usw. im ntv-System-Namespace durch, um weitere Details und Fehlerprotokolle unter /var/log/ansible-perl-errors.log und /var/log/ansible-run.log zu erhalten und Neuimplementierungen durchzuführen.
062	VASA-Provider- und SRA-Bereitstellung ist fehlgeschlagen	Weitere Informationen und Neuimplementierungen finden Sie in den Fehlerprotokollen unter /var/log/ansible-perl-errors.log.
064	version.xml Überprüfung fehlgeschlagen	Neuimplementierung
065	Die URL der Swagger-Seite ist nicht erreichbar	Neuimplementierung
066	Schritte nach der Bereitstellung sind fehlgeschlagen	-
088	Die Konfiguration der Protokollrotation für journald ist fehlgeschlagen	Starten Sie die primäre VM neu.
089	Ändern der Eigentumsrechte für die Konfigurationsdatei „Zusammenfassung Protokoll drehen“ ist fehlgeschlagen	Starten Sie die primäre VM neu.

Fehlercode für Neustart	**Arbeitsablauf**
067	Zeitüberschreitung beim Warten auf Rke2-Server
101	Fehler beim Zurücksetzen des Benutzerpassworts für Wartung/Konsole
102	Fehler beim Löschen der Kennwortdatei beim Zurücksetzen des Benutzerpassworts für Wartung/Konsole
103	Fehler beim Aktualisieren des neuen Benutzerpassworts für Wartung/Konsole im Tresor

Wiederherstellungsfehler-Code	**Arbeitsablauf**	* Auflösung*
104	Schritte nach der Wiederherstellung sind fehlgeschlagen.	-
105	Kopieren des Inhalts auf das Wiederherstellungsvolume ist fehlgeschlagen.	-

106	Recovery-Volume konnte nicht bereitgestellt werden.	* Stellen Sie sicher, dass die gleiche SVM verwendet wird und das Wiederherstellungsvolume in der SVM vorhanden ist. (Der Name des Recovery-Volumes beginnt mit otvng_Trident_Recovery) * Stellen Sie sicher, dass Management-LIF und Daten-LIF-IP-Adressen von VM erreichbar sind. * Stellen Sie sicher, dass das NFS/iSCSI-Protokoll auf ONTAP aktiviert und richtig konfiguriert ist. * Stellen Sie sicher, dass die angegebene NFS/iSCSI DAT LIF IP Adresse korrekt und online ist. * Stellen Sie sicher, dass der Benutzername, das Passwort und das Protokoll korrekt sind und der Benutzer über ausreichende Berechtigungen zum Erstellen, Mounten, Klonen, Löschen verfügt. * Wiederholen Sie die Wiederherstellung

Konfigurieren von ONTAP Tools

Benutzeroberfläche von ONTAP Tools Manager

ONTAP Tools für VMware vSphere sind ein mandantenfähiges System, das mehrere vCenter Server-Instanzen managen kann. Der ONTAP Tools Manager bietet eine bessere Kontrolle über die ONTAP Tools für den VMware vSphere Administrator über die Instanzen der gemanagten vCenter Server und On-Board Storage Backends.

Der ONTAP Tools Manager unterstützt Sie bei folgenden Aufgaben:

- VCenter Server Instance Management - Hinzufügen und verwalten vCenter Server Instanzen zu ONTAP Tools.
- Storage-Back-End-Management: Fügen Sie ONTAP Storage-Cluster zu ONTAP Tools für VMware vSphere hinzu und managen Sie sie den global integrierten vCenter Server Instanzen.
- Log Bundle Downloads - Sammeln Sie Log-Dateien für ONTAP-Tools für VMware vSphere.
- Zertifikatverwaltung - Ändern Sie das selbstsignierte Zertifikat in ein benutzerdefiniertes CA-Zertifikat und erneuern oder aktualisieren Sie alle Zertifikate.
- Password Management - Zurücksetzen OVA-Anwendungs-Passwort für den Benutzer.

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

Fügen Sie vCenter Server-Instanzen hinzu und verwalten Sie sie

VCenter Server stellt die zentrale Managementplattform bereit, mit der Sie Hosts, Virtual Machines (VMs) und Storage-Back-Ends steuern können.

Fügen Sie eine vCenter Server-Instanz hinzu

Über diese Aufgabe

Sie können mehrere vCenter Server-Instanzen mit einer Instanz von ONTAP-Tools für VMware vSphere hinzufügen und managen.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste **vCenters** aus.
4. Wählen Sie **Add** für die Instanzen des vCenter-Servers aus und geben Sie Ihre vCenter-IP-Adresse/den Hostnamen, den Benutzernamen, das Kennwort und die Portdetails an.

Wenn Sie ONTAP Tools eine vCenter Server-Instanz hinzufügen, werden die folgenden Aktionen automatisch ausgeführt:

- Das vCenter Client-Plug-in ist registriert
- Benutzerdefinierte Berechtigungen für die Plug-ins und APIs werden an die vCenter Server Instanz übertragen
- Zum Verwalten der Benutzer werden benutzerdefinierte Rollen erstellt.

Registrieren Sie ONTAP-Tools für das VMware vSphere Plug-in mit vCenter Server-Instanz

Wenn Sie eine vCenter Server-Instanz hinzufügen, werden ONTAP-Tools für VMware vSphere-Plug-in automatisch als Remote-Plug-in für vCenter Server registriert. Das Plug-in ist auf den vSphere-Benutzeroberflächen-Shortcuts sichtbar.

Das Plug-in wird mit einem Schlüssel *com.netapp.otv* für die vCenter Server Instanz registriert und ist im ExtensionManager der vCenter Server Instanz zu sehen.

Heben Sie die Registrierung von ONTAP Tools für das VMware vSphere Plug-in auf

Sie können die ONTAP-Tools für das VMware vSphere Plug-in mithilfe der folgenden Schritte von einer vCenter Server-Instanz abmelden.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste vCenter aus.
4. Klicken Sie auf die vertikalen Ellipsen gegenüber dem vCenter, das Sie entfernen möchten, und wählen Sie die Option **Entfernen** aus.

> Sie können eine vCenter Server-Instanz nicht entfernen, wenn eine Speicherzuweisung mit ihr verbunden ist. Sie müssen die Zuordnung entfernen, bevor Sie die vCenter Server-Instanz entfernen.

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

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

Registrieren Sie den VASA Provider mit einer vCenter Server-Instanz

Sie können den VASA-Provider mit einer vCenter Server-Instanz über die ONTAP-Tools für die Remote-Plug-in-Schnittstelle von VMware vSphere registrieren und abmelden. Im

Abschnitt „VASA Provider Settings“ wird der Registrierungsstatus des VASA Providers für den ausgewählten vCenter Server angezeigt.

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie auf der Shortcuts-Seite unter dem Plug-ins-Bereich auf **NetApp ONTAP Tools**.
3. Wählen Sie **Einstellungen** > **VASA Provider-Einstellungen**. Der Registrierungsstatus des VASA-Providers wird als nicht registriert angezeigt.
4. Klicken Sie auf die Schaltfläche **REGISTRIEREN**, um den VASA Provider zu registrieren.
5. Geben Sie einen Namen für den VASA-Provider ein, und stellen Sie ONTAP-Tools für die Anmeldedaten der VMware vSphere-Anwendung bereit. Klicken Sie anschließend auf **REGISTRIEREN**.
6. Bei erfolgreicher Registrierung und Seitenaktualisierung zeigt die Benutzeroberfläche den Status, den Namen und die Version des registrierten VASA-Providers an. Die Aktion zur Registrierung wird aktiviert.
7. Wenn Sie die Registrierung des VASA-Providers aufheben möchten, führen Sie die folgenden Schritte aus:
   a. Um die Registrierung des VASA-Providers aufzuheben, wählen Sie die Option **Registrierung aufheben** unten im Bildschirm.
   b. Auf der Seite **Registrierung des VASA-Providers aufheben** sehen Sie den Namen des VASA-Providers. Geben Sie auf dieser Seite die Anmeldeinformationen des Anwendungsbenutzers ein und klicken Sie auf **Registrierung aufheben**.

Überprüfen Sie den registrierten VASA-Anbieter

Vergewissern Sie sich, dass der Onboarding VASA-Provider in der vCenter Client-UI und über die Remote-Plug-in-UI unter VASA Provider aufgeführt ist.

Schritte

1. Gehen Sie wie folgt vor, um VASA Provider von der vCenter-Client-Benutzeroberfläche zu überprüfen:
   a. Navigieren Sie zu vCenter Server.
   b. Melden Sie sich mit den Administratoranmeldeinformationen an.
   c. Wählen Sie **Speicheranbieter** Aus.
   d. Wählen Sie **Konfigurieren**.
   e. Überprüfen Sie unter Storage Provider/Storage Back-Ends, ob der Onboarding VASA Provider korrekt aufgeführt ist.
2. Gehen Sie wie folgt vor, um VASA Provider von der Remote-Plug-in-Benutzeroberfläche zu überprüfen:
   a. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
   b. Klicken Sie auf der Shortcuts-Seite unter dem Plug-ins-Bereich auf **NetApp ONTAP Tools**.
   c. Sie können den registrierten VASA Provider auf der Übersichtsseite und auf der Seite **Einstellungen** > **VASA Provider Einstellungen** sehen.

Installieren Sie das NFS VAAI Plug-in

Sie können das NetApp NFS-Plug-in für VMware vStorage APIs für die Array-Integration

(VAAI) mit den ONTAP Tools für VMware vSphere installieren.

Was Sie brauchen

- Sie sollten das Installationspaket für das NFS-Plugin für VAAI (`.vib`von der NetApp-Support-Website heruntergeladen haben. "NetApp NFS Plug-in für VMware VAAI"
- Sie sollten den aktuellen ESXi-Host 7.0U3-Patch als Mindestversion und ONTAP 9.12.1Px (neueste P-Version) 9.13.1Px, 9.14.1Px oder höher installiert haben.
- Sie sollten den ESXi-Host eingeschaltet und einen NFS-Datastore gemountet haben.
- Sie sollten die Werte der `DataMover.HardwareAcceleratedMove` , `DataMover.HardwareAcceleratedInit` und `VMFS3.HardwareAcceleratedLocking` Host-Einstellungen auf „`1`“ gesetzt haben.

  Diese Werte werden automatisch auf dem ESXi-Host gesetzt, wenn das Dialogfeld Empfohlene Einstellungen aktualisiert wird.

- Sie sollten die vstorage-Option auf der Storage Virtual Machine (SVM) mit dem `vserver nfs modify -vserver vserver_name -vstorage enabled` Befehl aktiviert haben.
- Sie sollten ESXi 7.0U3 oder höher verwenden, wenn Sie das NetApp NFS VAAI Plug-in 2.0 verwenden.
- Sie sollten die neuesten vSphere 7.0U3-Patch-Versionen haben, da vSphere 6.5 veraltet ist.
- VSphere 8.x wird mit dem NetApp NFS VAAI Plug-in 2.0.1(Build 16) unterstützt.

Schritte

1. Klicken Sie auf der Startseite von ONTAP Tools für VMware vSphere auf **Einstellungen**.
2. Klicken Sie auf die Registerkarte * NFS VAAI Tools*.
3. Wenn das VAAI-Plug-in auf vCenter Server hochgeladen wird, wählen Sie im Bereich **existing Version Change** aus. Wenn kein VAAI-Plug-in auf den vCenter-Server hochgeladen wird, klicken Sie auf die Schaltfläche **Upload**.
4. Durchsuchen Sie die `.vib` Datei, wählen Sie sie aus, und klicken Sie dann auf **Hochladen**, um die Datei in ONTAP-Tools hochzuladen.
5. Klicken Sie auf **auf EXSI-Host installieren**, wählen Sie den ESXi-Host aus, auf dem Sie das NFS VAAI-Plug-in installieren möchten, und klicken Sie dann auf **Installieren**.

   Es werden nur die ESXi-Hosts angezeigt, die für die Plug-in-Installation geeignet sind. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Installation abzuschließen. Sie können den Installationsfortschritt im Abschnitt Letzte Aufgaben von vSphere Web Client überwachen.

6. Sie sollten den ESXi-Host nach Abschluss der Installation manuell neu starten.

   Wenn der VMware-Administrator den ESXi-Host neu startet, erkennen die ONTAP-Tools für VMware vSphere automatisch das NFS VAAI-Plug-in. Sie müssen keine weiteren Schritte zum Aktivieren des Plug-ins ausführen.

Aktualisieren Sie die Hostdaten

Sie können eine On-Demand-Erkennung auf dem ESXi-Host ausführen, um die neuesten Updates für die Storage-Daten zu erhalten.

Schritte

1. Klicken Sie auf der VMware vSphere Web Client-Startseite auf **Hosts und Cluster**.
2. Klicken Sie mit der rechten Maustaste auf einen Host und wählen Sie dann **NetApp ONTAP Tools** > **Host-Daten aktualisieren**.
3. Wählen Sie im Popup-Fenster **Update Host Data Yes** aus, um die Erkennung aller verbundenen Speichersysteme neu zu starten.

Konfigurieren Sie ESXi-Hosteinstellungen

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

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

Über diese Aufgabe

Dieser Prozess kann je nach Konfiguration und Systemlast sehr viel Zeit in Anspruch nehmen. Der Aufgabenfortschritt wird im Fenster Letzte Aufgaben angezeigt. Wenn die Aufgaben abgeschlossen sind, wird das Symbol für die Warnung des Host-Status durch das Symbol Normal oder das Symbol Ausstehender Neustart ersetzt.

Schritte

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

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

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

Legen Sie ESXi-Hostwerte fest

Mithilfe der ONTAP-Tools für VMware vSphere können Timeouts und andere Werte auf den ESXi-Hosts festgelegt werden, um beste Leistung und erfolgreiches Failover zu gewährleisten. Die Werte, die ONTAP Tools für VMware vSphere Set bieten, basieren auf internen NetApp-Tests.

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

HBA/CNA-Adaptereinstellungen

Legt die empfohlenen Einstellungen für das HBA-Zeitlimit für NetApp-Speichersysteme fest.

- **Disk.QFullSampleSize**

  Setzen Sie diesen Wert für alle Konfigurationen auf 32. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.

- **Disk.QFullThreshold**

  Setzen Sie diesen Wert für alle Konfigurationen auf 8. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.

- * Emulex FC HBA-Timeouts*

  Standardwert verwenden.

- **QLogic FC HBA Timeouts**

  Standardwert verwenden.

MPIO-Einstellungen

MPIO-Einstellungen definieren bevorzugte Pfade für NetApp-Speichersysteme. Die MPIO-Einstellungen legen fest, welche der verfügbaren Pfade optimiert sind (im Gegensatz zu nicht optimierten Pfaden, die das Verbindungskabel durchlaufen), und sie legen den bevorzugten Pfad zu einem dieser Pfade fest.

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

NFS-Einstellungen

- **Net.TcpipHeapSize**

  Setzen Sie diesen Wert auf 32.

- **Net.TcpipHeapMax**

  Setzen Sie diesen Wert auf 1024 MB.

- **NFS.MaxVolumes**

  Setzen Sie diesen Wert auf 256.

- **NFS41.MaxVolumes**

  Setzen Sie diesen Wert auf 256.

- **NFS.MaxQueueDepth**

  Setzen Sie diesen Wert auf 128 oder höher, um Engpässe in der Warteschlange zu vermeiden.

- **NFS.HeartbeatMaxFailures**

  Setzen Sie diesen Wert für alle NFS-Konfigurationen auf 10.

- **NFS.HeartbeatFrequency**

  Setzen Sie diesen Wert für alle NFS-Konfigurationen auf 12.

- **NFS.HeartbeatTimeout**

  Setzen Sie diesen Wert für alle NFS-Konfigurationen auf 5.

Erkennen von Storage-Systemen und Hosts

Wenn Sie ONTAP-Tools für VMware vSphere zum ersten Mal in einem vSphere Client ausführen, erkennt ONTAP-Tools die ESXi-Hosts, ihre LUNs und NFS-Exporte und die NetApp-Storage-Systeme, die Eigentümer dieser LUNs und Exporte sind.

Was Sie brauchen

- Alle ESXi-Hosts sollten eingeschaltet und verbunden sein.
- Alle zu ermittelenden Storage Virtual Machines (SVMs) sollten ausgeführt werden. Jeder Cluster-Node sollte mindestens eine Daten-LIF für das verwendete Storage-Protokoll (NFS oder iSCSI) konfiguriert haben.

Über diese Aufgabe

Sie können jederzeit neue Storage-Systeme ermitteln oder Informationen zu vorhandenen Storage-Systemen aktualisieren, um die aktuellsten Kapazitäts- und Konfigurationsinformationen zu erhalten. Sie können auch die Anmeldeinformationen ändern, die die ONTAP-Tools für VMware vSphere für die Anmeldung bei den Speichersystemen verwenden.

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

Schritte

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

   ONTAP Tools für VMware vSphere zeigt ein **Confirm**-Dialogfeld mit der folgenden Meldung an:

   „Diese Aktion startet die Erkennung aller verbundenen Speichersysteme neu und kann einige Minuten dauern. Möchten Sie fortfahren?“

3. Klicken Sie Auf **Ja**.
4. Wählen Sie die ermittelten Speicher-Controller aus `Authentication Failure`, die den Status haben, und klicken Sie dann auf **actions** > **Modify**.
5. Geben Sie die erforderlichen Informationen in das Dialogfeld * Speichersystem ändern* ein.
6. Wiederholen Sie die Schritte 4 und 5 für alle Speicher-Controller mit `Authentication Failure` Status.

Führen Sie nach Abschluss des Erkennungsvorgangs die folgenden Schritte aus:

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

Fügen Sie ein Storage-Back-End hinzu

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

Über diese Aufgabe

Diese Aufgabe unterstützt Sie beim Onboarding eines ONTAP-Clusters. Wenn Sie mit dem ONTAP Tools Manager ein Storage Back-End hinzufügen, wird das Storage Back-End dem globalen Cluster hinzugefügt. Ordnen Sie das globale Cluster einer vCenter Server-Instanz zu, um einen SVM-Benutzer für die Bereitstellung von VVols-Datastores zu aktivieren.

Wenn Sie mithilfe der vSphere Client-UI ein Storage-Back-End hinzufügen, unterstützt VVols Datastore das direkte Hinzufügen eines SVM-Benutzers nicht.

Fügen Sie mithilfe des ONTAP Tools Managers das Storage-Back-End hinzu

Ein Storage-Back-End ist global verfügbar, wenn sie über den ONTAP Tools Manager oder die ONTAP Tools APIs hinzugefügt wird. Ein Storage-Back-End ist lokal, wenn es über die vCenter Server-APIs hinzugefügt wird. So können Sie beispielsweise in einer mandantenfähigen Einrichtung ein globales Storage-Back-End (Cluster) und eine lokale SVM hinzufügen, um die SVM-Benutzeranmeldeinformationen zu verwenden.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste **Speicher-Backends** aus.
4. Wählen Sie **Hinzufügen**.
5. Geben Sie die IP-Adresse des Servers oder den FQDN, den Benutzernamen und das Kennwort ein, und wählen Sie **Hinzufügen**.

IPV4- und IPV6-Management-LIFs werden unterstützt. Auch die benutzerbasierten SVM-Anmeldedaten mit Management-LIFs werden unterstützt.

Storage-Back-End mithilfe der vSphere Client-UI hinzufügen:

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie auf der Shortcuts-Seite unter dem Plug-ins-Bereich auf **NetApp ONTAP Tools**.

3. Navigieren Sie im linken Bereich der ONTAP-Tools zu **Speicher-Backends** und wählen Sie **Hinzufügen**.
4. Geben Sie im Fenster **Add Storage Backend** die IP-Adresse, den Benutzernamen, das Passwort und die Port-Details des Servers an und klicken Sie auf **Add**.

> Sie können Cluster-basierte Anmeldedaten und IPV4- und IPV6-Management-LIFs hinzufügen oder SVM-basierte Anmeldedaten mit der Management-LIF der SVM bereitstellen, um einen SVM-Benutzer direkt hinzuzufügen.

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

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

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

Über diese Aufgabe

Mit dieser Aufgabe können Sie eine Zuordnung zwischen dem Storage-Back-End und der neu aufgenommenen vCenter Server-Instanz global erstellen.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Randleiste vCenter aus.
4. Klicken Sie auf die vertikalen Ellipsen gegenüber dem vCenter, das Sie mit Speicher-Back-Ends verknüpfen möchten.
5. Wählen Sie im Popup-Fenster aus der Dropdown-Liste das Storage-Back-End aus.
6. Wählen Sie die Option **Speicher-Backend zuordnen**, um vCenter Server-Instanz mit dem erforderlichen Speicher-Backend zu verknüpfen.

Konfigurieren Sie den Netzwerkzugriff

Wenn Sie mehrere ESXi-Host-IP-Adressen haben, werden standardmäßig alle vom Host ermittelten IP-Adressen zu einer Exportrichtlinie hinzugefügt. Wenn Sie nicht alle IP-Adressen zu einer Exportrichtlinie hinzufügen möchten, geben Sie eine Einstellung für das Zulassen bestimmter IP-Adressen in einer kommagetrennten Liste oder einem CIDR oder einer Kombination aller drei für jedes vCenter ein.

Sie können wählen, ob Sie einige bestimmte ESXi-Hostadressen für den Datastore-Mount-Vorgang zulassen möchten. Wenn die Einstellung nicht angegeben ist, fügt die Exportrichtlinie alle im Schritt Pre-Mount ermittelten IP-Adressen hinzu. Wenn die Einstellung angegeben ist, fügen ONTAP-Tools für VMware vSphere nur diejenigen hinzu, die in den aufgeführten IP-Adressen oder -Bereich fallen. Wenn keine der IP-Adressen

eines Hosts zu den aufgeführten IP-Adressen gehört, schlägt der Mount-Vorgang auf diesem Host fehl.

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie auf der Shortcuts-Seite unter dem Plug-ins-Bereich auf **NetApp ONTAP Tools**.
3. Navigieren Sie im linken Bereich der ONTAP-Tools zu **Einstellungen** > **Netzwerkzugang verwalten** > **Bearbeiten**.

   Verwenden Sie ein Komma (,), um die IP-Adressen zu trennen. Sie können eine bestimmte IP-Adresse oder einen Bereich von IP-Adressen oder IPv6-Adressen angeben.

4. Klicken Sie Auf **Speichern**.

Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen

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

Was Sie brauchen

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

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

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

Schritte

1. Extrahieren Sie die heruntergeladene Datei *https://<loadbalancerIP>:8443/Virtualization/user-Privileges/users_roles.zip*.
2. Sie können über die Cluster-Management-IP-Adresse des Clusters auf ONTAP System Manager zugreifen.
3. Melden Sie sich als Cluster- oder SVM-Benutzer an.
4. Wählen Sie **Cluster** > **Einstellungen** > **Benutzer und Rollen**.
5. Wählen Sie unter Benutzer * Hinzufügen *.
6. Wählen Sie im Dialogfeld * Benutzer hinzufügen* die Option **Virtualisierungsprodukte** aus.
7. **Browse**, um die JSON-Datei für ONTAP-Berechtigungen auszuwählen und hochzuladen.

   Das Produktfeld wird automatisch ausgefüllt.

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

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

9. Geben Sie den erforderlichen Benutzernamen und das erforderliche Passwort ein.
10. Wählen Sie die für den Benutzer erforderlichen Berechtigungen (Ermittlung, Speicher erstellen, Speicher ändern, Speicher zerstören, NAS/SAN-Rolle) aus, und klicken Sie dann auf **Hinzufügen**.

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

> Beim Deinstallationsvorgang werden die Rollen des ONTAP-Tools nicht entfernt, sondern die lokalisierten Namen der ONTAP-Tool-spezifischen Privileges entfernt und das Präfix an `XXX missing privilege` sie angehängt. Wenn Sie ONTAP-Tools für VMware vSphere neu installieren oder auf eine neuere Version aktualisieren, werden alle standardmäßigen ONTAP-Tools für VMware vSphere-Rollen und spezifischen Berechtigungen für ONTAP-Tools wiederhergestellt.

Anforderungen für die SVM-Aggregatzuordnung

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

REST-API:

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

ONTAP-CLI:

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

Erstellen Sie ONTAP-Benutzer und -Rolle manuell

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

1. Sie können über die Cluster-Management-IP-Adresse des Clusters auf ONTAP System Manager zugreifen.
2. Melden Sie sich als Cluster- oder SVM-Benutzer an.

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

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

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

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

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

Verwenden von APIs:

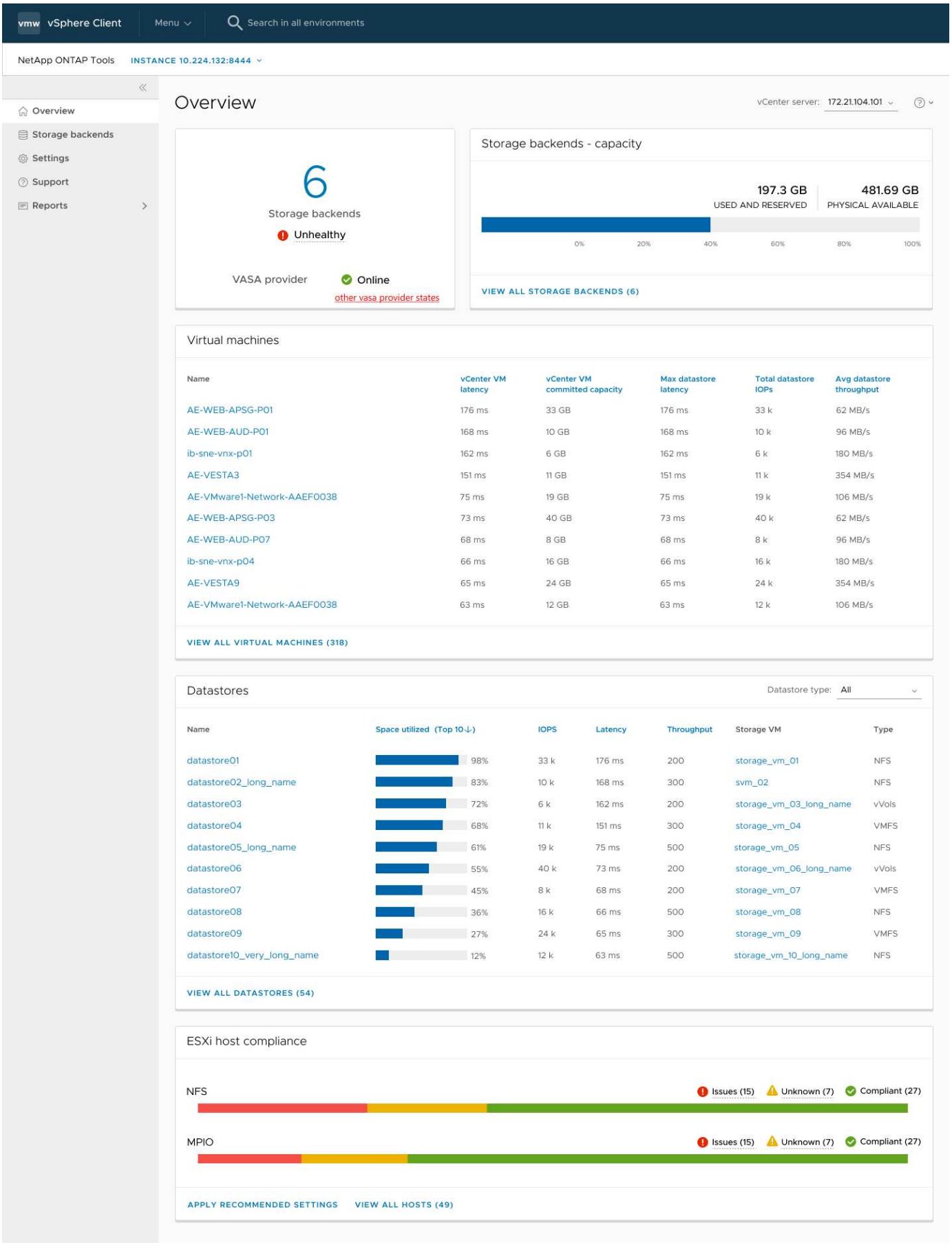
API	Zugangsstufe	Verwendet für
/API/Cluster	Schreibgeschützt	Erkennung Der Clusterkonfiguration
/API/Cluster/Lizenzierung/Lizenzen	Schreibgeschützt	Lizenzprüfung für protokollspezifische Lizenzen
/API/Cluster/Nodes	Schreibgeschützt	Erkennung des Plattformtyps
/API/Storage/Aggregate	Schreibgeschützt	Speicherplatzüberprüfung von Aggregaten während der Bereitstellung von Datastores/Volumes
/API/Storage/Cluster	Schreibgeschützt	Um Speicherplatz auf Cluster-Ebene und Effizienzdaten zu erhalten
/API/Storage/Festplatten	Schreibgeschützt	Um die in einem Aggregat zugeordneten Festplatten zu erhalten

/API/Storage/qos/Richtlinien	Lesen/Erstellen/Ändern	QoS- und VM-Richtlinienmanagement
/API/svm/svms	Schreibgeschützt	Um die SVM-Konfiguration für den Fall zu erhalten, dass das Cluster lokal hinzugefügt wird.
/API/Netzwerk/ip/Schnittstellen	Schreibgeschützt	Storage Back-end hinzufügen: Zur Identifizierung des Management-LIF-Umfangs ist Cluster/SVM
/API	Schreibgeschützt	Cluster-Benutzer sollten über diese Berechtigung verfügen, um den korrekten Speicher-Back-End-Status zu erhalten. Andernfalls zeigt der ONTAP Tools Manager „unbekannten“ Speicher-Backend-Status an.

Dashboard der NetApp ONTAP Tools für VMware vSphere Plug-in – Übersicht

Wenn Sie im Abschnitt Verknüpfungen des vCenter-Clients das Symbol NetApp ONTAP-Tools für VMware vSphere Plug-in auswählen, wechselt die Benutzeroberfläche zur Übersichtsseite. Diese Seite ähnelt dem Dashboard mit einer Zusammenfassung der ONTAP Tools für VMware vSphere Plug-in.

Im Fall von Enhanced Linked Mode Setup (ELM) wird das Drop-down-Menü vCenter Server SELECT angezeigt, und Sie können einen gewünschten vCenter Server auswählen, um die für ihn relevanten Daten anzuzeigen. Diese Dropdown-Liste ist für alle anderen Listenansichten des Plugins verfügbar. VCenter Server-Auswahl auf einer Seite besteht über die Registerkarten des Plug-ins.



Das Dashboard verfügt über mehrere Karten, die verschiedene Elemente des Systems anzeigen. Die folgende

Tabelle zeigt die verschiedenen Karten und was sie darstellen.

Kartenname	Beschreibung
Status	Die Statuskarte zeigt die Anzahl der hinzugefügten Speicher-Back-Ends sowie den allgemeinen Integritätsstatus von Speicher-Back-Ends und VASA Provider-Status eines vCenter an. Der Status von Storage Back-Ends wird als „funktionstüchtiger“ angezeigt, wenn der Status aller Storage Back-Ends „Normal“ lautet. Der Status „Speicher-Back-Ends“ wird als „fehlerhaft“ angezeigt, wenn eines der Speicher-Back-Ends ein Problem aufweist (Unbekannt/Unerreichbar/herabgesetzt). Wenn Sie auf den Status „fehlerhaft“ klicken, wird eine QuickInfo mit dem Status der Speicher-Back-Ends geöffnet. Sie können auf ein beliebiges Storage-Back-End klicken, um mehr Details zu erhalten. Der Link „Other VASA Provider (VP) States“ zeigt den aktuellen Status des VP an, der auf dem vCenter Server registriert ist.
Storage Back-Ends – Kapazität	Diese Karte zeigt die aggregierte genutzte und verfügbare Kapazität aller Speicher-Back-Ends für die ausgewählte vCenter Server-Instanz an.
Virtual Machines	Diese Karte zeigt die 10 wichtigsten VMs nach Performance-Metrik. Sie können auf die Kopfzeile klicken, um die 10 wichtigsten VMs für die ausgewählte Metrik nach aufsteigender oder absteigender Reihenfolge zu erhalten. Die auf der Karte vorgenommenen Änderungen beim Sortieren und Filtern bleiben bestehen, bis Sie den Browser-Cache ändern oder löschen.
Datenspeicher	Diese Karte zeigt die 10 besten Datastores, sortiert nach einer Performance-Metrik. Sie können auf die Kopfzeile klicken, um die 10 wichtigsten Datastores für die ausgewählte Metrik nach aufsteigender oder absteigender Reihenfolge zu erhalten. Die auf der Karte vorgenommenen Änderungen beim Sortieren und Filtern bleiben bestehen, bis Sie den Browser-Cache ändern oder löschen. Zum Auswählen des Typs der Datastores – NFS, VMFS oder VVols – existiert ein Dropdown-Menü zum Datenspeichertyp.
ESXi-Host-Compliance-Karte	Diese Karte zeigt den allgemeinen Compliance-Status aller ESXi-Hosts (für das ausgewählte vCenter)-Einstellungen in Bezug auf die empfohlenen NetApp-Host-Einstellungen nach Einstellungsgruppe/Kategorie an. Sie können auf den Link Empfohlene Einstellungen anwenden klicken, um die empfohlenen Einstellungen anzuwenden. Klicken Sie auf Probleme/unbekannt, um die Liste der Hosts anzuzeigen.

Erstellen eines Datenspeichers

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

Der Assistent „Datastore erstellen“ unterstützt die Erstellung von NFS-, VMFS- und VVols-Datenspeichern.

Erstellen Sie einen VVols-Datastore

Sie können einen VVols-Datastore entweder mit neuen Volumes oder mit vorhandenen Volumes erstellen. Sie können keinen VVols-Datastore mit einer Kombination aus vorhandenen und neuen Volumes erstellen.

Überprüfen Sie, ob die Root-Aggregate nicht der SVM zugeordnet sind.

Bevor Sie beginnen

Stellen Sie sicher, dass der VASA-Anbieter beim ausgewählten vCenter registriert ist.

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem oder einen Hostcluster oder ein Rechenzentrum, und wählen Sie dann **NetApp ONTAP Tools** > **Datastore erstellen** aus.
3. Wählen Sie im Bereich **Typ** unter **Datastore Type** die Option VVols aus.
4. Geben Sie im Bereich **Name und Protokoll** die Informationen **Datastore Name** und **Protocol** an.
5. Wählen Sie im Bereich **Storage Platform** und **Storage VM** aus. Wählen Sie im Abschnitt **Erweiterte Optionen** die Option Benutzerdefinierte Exportrichtlinie (für NFS-Protokoll) oder benutzerdefinierten Initiatorgruppennamen (für iSCSI-Protokoll) aus.
   - Mit Plattform- und asymmetrischen Optionen können Sie die Dropdown-Optionen für SVMs herausfiltern. Sie sollten die SVM auswählen, die erstellt werden soll, oder die Volumes für die Datastore-Erstellung verwenden.
   - Die Umschalttaste **Asymmetric** ist nur sichtbar, wenn iSCSI im vorherigen Schritt ausgewählt wurde und Leistung oder Kapazität im Dropdown-Menü Plattform ausgewählt ist.
   - Wählen Sie die Schaltfläche **Asymmetric** für die AFF-Plattform und deaktivieren Sie sie für die ASA-Plattform.
6. Im Bereich **Speicherattribute** können Sie entweder neue Volumes erstellen oder die vorhandenen Volumes verwenden. Beim Erstellen eines neuen Volumes können Sie die QoS auf dem Datastore aktivieren.
7. Überprüfen Sie Ihre Auswahl im Fenster **Zusammenfassung** und klicken Sie auf **Fertig stellen**. Der VVols Datastore wird auf allen Hosts erstellt und gemountet.

Erstellen Sie einen NFS-Datastore

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

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem oder einen Hostcluster oder ein Rechenzentrum, und wählen Sie dann **NetApp ONTAP Tools** > **Datastore erstellen** aus.
3. Wählen Sie im Bereich **Typ** NFS unter **Datastore Type** aus.
4. Geben Sie im Bereich **Name und Protokoll** den Namen, die Größe und die Protokollinformationen des Datastore ein. Wählen Sie in den erweiterten Optionen **Datastore Cluster** und **Kerberos Authentication** aus.

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

5. Wählen Sie im Bereich **Storage Platform** und **Storage VM** aus. Sie können **Custom Export Policy** im Abschnitt **Advanced Option** auswählen.
   - **Asymmetric** Umschalttaste ist nur sichtbar, wenn Leistung oder Kapazität im Dropdown-Menü Plattform ausgewählt ist.
   - **Any** Option in der Plattform-Dropdown ermöglicht es Ihnen, alle SVMs zu sehen, die Teil des vCenter sind, unabhängig von der Plattform oder asymmetrischen Flagge.
6. Wählen Sie im Bereich **Speicherattribute** das Aggregat für die Erstellung des Volumes aus. Wählen Sie in den erweiterten Optionen **Space Reserve** und **Enable QoS** je nach Bedarf.
7. Überprüfen Sie die Auswahl im Fenster **Zusammenfassung** und klicken Sie auf **Fertig stellen**.

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

Erstellen Sie einen VMFS-Datastore

Virtual Machine File System (VMFS) ist ein geclustertes Filesystem, das speziell zum Speichern von VM-Dateien in VMware vSphere Umgebungen entwickelt wurde. Sie ermöglicht es mehreren ESXi-Hosts, gleichzeitig auf dieselben VM-Dateien zuzugreifen, was Funktionen wie vMotion und Hochverfügbarkeit ermöglicht.

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem oder einen Hostcluster oder einen Datastore, und wählen Sie dann **NetApp ONTAP Tools** > **Datastore erstellen** aus.
3. Wählen Sie im Bereich **Typ** VMFS unter **Datastore Type** aus.
4. Geben Sie im Bereich **Name und Protokoll** den Namen, die Größe und die Protokollinformationen des Datastore ein. Wählen Sie im Abschnitt **Erweiterte Optionen** des Teilfensters den Datastore-Cluster aus, dem Sie diesen Datastore hinzufügen möchten.
5. Wählen Sie im Fensterbereich Storage die Option Platform and Storage VM aus. Wählen Sie die Schaltfläche Asymmetric Toggle. Geben Sie den **Custom Initiator Group Name** im Abschnitt **Advanced options** des Fensters ein (optional). Sie können entweder eine vorhandene Initiatorgruppe für den Datastore auswählen oder eine neue Initiatorgruppe mit einem benutzerdefinierten Namen erstellen.

   Wenn Sie die Option **any** in der Dropdown-Liste der Plattform wählen, sehen Sie alle SVMs, die Teil des vCenter sind, unabhängig von der Plattform oder dem asymmetrischen Flag.

6. Wählen Sie im Bereich Speicherattribute aus dem Dropdown-Menü die Option **Aggregat** aus. Wählen Sie im Abschnitt **Erweiterte Optionen** die Optionen **Platzreserve**, **vorhandenes Volume verwenden** und **QoS** aktivieren aus und geben Sie die erforderlichen Details an.

7. Überprüfen Sie die Datastore-Details im Bereich **Summary** und klicken Sie auf **Finish**. Der VMFS Datastore wird auf allen Hosts erstellt und gemountet.

Sicherung von Data Stores und Virtual Machines

Aktivieren Sie SRA, um Datastores zu sichern

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

Was Sie brauchen

- Sie sollten Ihre vCenter Server-Instanz eingerichtet und den ESXi-Host konfiguriert haben.
- Sie hätten ONTAP Tools bereitstellen sollen.
- Sie sollten die SRA Adapter- `.tar.gz`Datei von der heruntergeladen haben "NetApp Support-Website".

Schritte

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

Konfiguration des Storage-Systems für Disaster Recovery

Konfiguration von SRA für SAN- und NAS-Umgebungen

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

Konfiguration von SRA für SAN-Umgebungen

Was Sie brauchen

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

- SRM

  Dokumentation zur Installation von SRM befindet sich auf der VMware Site.

  "VMware Site Recovery Manager - Dokumentation"

- SRA

  Der Adapter ist auf SRM installiert.

Schritte

1. Vergewissern Sie sich, dass die primären ESXi-Hosts mit den LUNs im primären Speichersystem am geschützten Standort verbunden sind.
2. Überprüfen Sie, ob die LUNS in Initiatorgruppen sind, für die die `ostype` Option auf dem primären Storage-System auf „*VMware*“ gesetzt ist.
3. Überprüfen Sie, ob die ESXi-Hosts am Wiederherstellungsstandort über eine geeignete iSCSI-Verbindung zur Storage Virtual Machine (SVM) verfügen. Die ESXi-Hosts am sekundären Standort sollten Zugriff auf den sekundären Standortspeicher haben, und die ESXi-Hosts am primären Standort sollten Zugriff auf den primären Standortspeicher haben.

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

Konfiguration von SRA für NAS-Umgebungen

Was Sie brauchen

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

- SRM

  Dokumentation zur Installation von SRM finden Sie auf der VMware-Website.

  "VMware Site Recovery Manager - Dokumentation"

- SRA

  Der Adapter wird auf SRM und dem SRA Server installiert.

Schritte

1. Überprüfen Sie, ob die Datenspeicher am geschützten Standort virtuelle Maschinen enthalten, die bei vCenter Server registriert sind.
2. Überprüfen Sie, ob die ESXi-Hosts am geschützten Standort die NFS-Exporte-Volumes von der Storage Virtual Machine (SVM) gemountet haben.
3. Überprüfen Sie, ob gültige Adressen wie die IP-Adresse, der Hostname oder der FQDN, auf denen die NFS-Exporte vorhanden sind, im Feld **NFS-Adressen** angegeben sind, wenn Sie den Array Manager-Assistenten zum Hinzufügen von Arrays zu SRM verwenden.
4. `ping`Überprüfen Sie mit dem Befehl auf jedem ESXi Host am Recovery-Standort, ob der Host über einen VMkernel Port verfügt, der auf die IP-Adressen zugreifen kann, die für NFS-Exporte der SVM verwendet werden.

Konfiguration von SRA für hochskalierte Umgebungen

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

Einstellungen für Speicheranbieter

Sie sollten für eine skalierte Umgebung die folgenden Zeitüberschreitungswerte für SRM einstellen:

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

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

Weitere Informationen zum Ändern der Einstellungen für Storage Provider finden Sie in der VMware-Dokumentation.

"Dokumentation zu VMware vSphere: Ändern der Storage Provider-Einstellungen"

Speichereinstellungen

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

> Das angegebene Zeitüberschreitungsintervall ist der Höchstwert. Sie müssen nicht warten, bis die maximale Zeitüberschreitung erreicht ist. Die meisten Befehle sind innerhalb des festgelegten maximalen Timeout-Intervalls abgeschlossen.

Weitere Informationen finden Sie in der VMware-Dokumentation zum Ändern der SAN-Provider-Einstellungen.

"Dokumentation zum VMware Site Recovery Manager: Storage-Einstellungen ändern"

Konfigurieren Sie SRA auf der SRM-Appliance

Nachdem Sie die SRM-Appliance bereitgestellt haben, sollten Sie SRA auf der SRM-Appliance konfigurieren. Durch die erfolgreiche Konfiguration von SRA kann die SRM-Appliance zur Disaster-Recovery-Verwaltung mit SRA kommunizieren. Sie sollten ONTAP Tools für VMware vSphere Credentials (IP-Adresse) in der SRM-Appliance speichern, um die Kommunikation zwischen der SRM-Appliance und SRA zu ermöglichen.

Was Sie brauchen

Sie sollten die Datei *tar.gz* von heruntergeladen haben "NetApp Support-Website".

Über diese Aufgabe

Die Konfiguration von SRA auf einer SRM-Appliance speichert die SRA-Anmeldedaten in der SRM-Appliance.

Schritte

1. Klicken Sie auf dem Bildschirm der SRM-Appliance auf **Storage Replication Adapter** > **New Adapter**.
2. Laden Sie die Datei *.tar.gz* in SRM hoch.
3. Melden Sie sich mit einem Administratorkonto bei der SRM-Appliance mit Putty 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 zu erhalten: `docker ps -l`
7. Um sich bei der Container-ID anzumelden, geben Sie den Befehl ein: `docker exec -it -u srm <container id> sh`
8. Konfigurieren Sie SRM mit den ONTAP Tools für VMware vSphere IP-Adresse und Passwort mit dem folgenden Befehl: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>'`

   Sie müssen den Kennwortwert in einfachen Anführungszeichen angeben, um sicherzustellen, dass das Perl-Skript die Sonderzeichen im Passwort nicht als Trennzeichen der Eingabe liest.

9. Überprüfen Sie die Adapter erneut, um sicherzustellen, dass die Details auf der Seite SRM Storage Replication Adapters aktualisiert werden.

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

SRA-Anmeldedaten aktualisieren

Damit SRM mit SRA kommunizieren kann, sollten Sie die SRA-Anmeldedaten auf dem SRM-Server aktualisieren, wenn Sie die Anmeldedaten geändert haben.

Was Sie brauchen

Sie sollten die im Thema genannten Schritte ausgeführt haben "Konfigurieren von SRA auf der SRM-Appliance".

Schritte

1. Führen Sie die folgenden Befehle aus, um das Kennwort für den im Cache gespeicherten ONTAP-Werkzeugordner des SRM-Computers zu löschen:
   a. `sudo su <enter root password>`
   b. `docker ps`
   c. `docker exec -it <container_id> sh`
   d. `cd /conf`

e. `rm -rf *`

2. Führen Sie den Perl-Befehl aus, um SRA mit den neuen Anmeldeinformationen zu konfigurieren:

   a. `cd ..`

   b. `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>` Sie benötigen ein einziges Angebot um den Passwortwert herum.

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

Geschützte Standorte und Recovery-Standorte konfigurieren

Konfigurieren Sie Schutzgruppen

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

Was Sie brauchen

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

- Dieselbe Version von SRM wurde installiert
- Virtual Machines
- Gepaarte geschützte Standorte und Recovery-Standorte
- Quell- und Ziel-Datastores sollten auf den jeweiligen Sites gemountet werden

Schritte

1. Melden Sie sich bei vCenter Server an und klicken Sie dann auf **Site Recovery** > **Protection Groups**.
2. Klicken Sie im Fensterbereich **Schutzgruppen** auf **Neu**.
3. Geben Sie einen Namen und eine Beschreibung für die Schutzgruppe, Richtung, und klicken Sie dann auf **Weiter**.
4. Wählen Sie im Feld **Typ** die Option **Typ Feld…** als Datastore-Gruppen (Array-basierte Replikation) für NFS- und VMFS-Datastore aus. Die Fehlerdomäne ist nichts anderes als SVMs mit aktivierter Replizierung. Es werden die SVMs angezeigt, für die lediglich Peering implementiert ist und keine Probleme vorhanden sind.
5. Wählen Sie auf der Registerkarte Replikationsgruppen entweder das aktivierte Array-Paar oder die Replikationsgruppen aus, für die die virtuelle Maschine konfiguriert ist, und klicken Sie dann auf **Weiter**.

   Alle virtuellen Maschinen auf der Replikationsgruppe werden der Schutzgruppe hinzugefügt.

6. Wählen Sie entweder den vorhandenen Wiederherstellungsplan aus oder erstellen Sie einen neuen Plan, indem Sie auf **zu neuem Wiederherstellungsplan hinzufügen** klicken.
7. Überprüfen Sie auf der Registerkarte bereit zum Abschließen die Details der von Ihnen erstellten Schutzgruppe, und klicken Sie dann auf **Fertig stellen**.

Kombinieren Sie geschützte Standorte und Recovery-Standorte

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

> Storage Replication Adapter (SRA) unterstützt keine Fan-out-SnapMirror-Konfigurationen. Bei SnapMirror Fan-out-Konfigurationen wird ein Quell-Volume auf zwei unterschiedliche Ziele repliziert. Diese stellen ein Problem während der Wiederherstellung dar, wenn SRM die Virtual Machine vom Ziel wiederherstellen muss.

Was Sie brauchen

- Sie sollten Site Recovery Manager (SRM) auf den geschützten und Recovery-Standorten installieren lassen.
- SRA sollte auf den geschützten und den Recovery-Standorten installiert sein.

Schritte

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

Ergebnis

Sowohl die geschützten als auch die Wiederherstellungsstandorte werden im Dialogfeld Objekte angezeigt.

Konfigurieren Sie geschützte Ressourcen und Recovery-Standortressourcen

Konfigurieren Sie die Netzwerkzuordnungen

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

Sie sollten die folgenden Ressourcenkonfigurationen abschließen:

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

Was Sie brauchen

Sie sollten die geschützten und Recovery-Standorte verbunden haben.

Schritte

1. Melden Sie sich am vCenter Server an und klicken Sie auf **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Seite aus, und klicken Sie dann auf **Verwalten**.
3. Wählen Sie auf der Registerkarte Verwalten die Option **Netzwerkzuordnungen** aus.
4. Klicken Sie auf **Neu**, um ein neues Netzwerk-Mapping zu erstellen.

   Der Assistent „Netzwerkzuordnung erstellen“ wird angezeigt.

5. Führen Sie im Assistenten „Netzwerkzuordnung erstellen“ folgende Schritte aus:
   a. Wählen Sie **Zuordnungen für Netzwerke mit übereinstimmenden Namen automatisch vorbereiten** aus und klicken Sie auf **Weiter**.
   b. Wählen Sie die gewünschten Rechenzentrumsobjekte für die geschützten und Recovery-Standorte aus und klicken Sie auf **Zuordnungen hinzufügen**.
   c. Klicken Sie auf **Weiter**, nachdem Zuordnungen erfolgreich erstellt wurden.
   d. Wählen Sie das zuvor verwendete Objekt aus, um eine umgekehrte Zuordnung zu erstellen, und klicken Sie dann auf **Fertig stellen**.

Ergebnis

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

Konfigurieren von Ordnerzuordnungen

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

Was Sie brauchen

Sie sollten die geschützten und Recovery-Standorte verbunden haben.

Schritte

1. Melden Sie sich am vCenter Server an und klicken Sie auf **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Seite aus, und klicken Sie dann auf **Verwalten**.
3. Wählen Sie auf der Registerkarte Verwalten die Option **Ordnerzuordnungen** aus.
4. Wählen Sie das Symbol **Ordner**, um eine neue Ordnerzuordnung zu erstellen.

   Der Assistent zum Erstellen der Ordnerzuordnung wird angezeigt.

5. Führen Sie im Assistenten zum Erstellen der Ordnerzuordnung folgende Schritte aus:
   a. Wählen Sie **automatisch Zuordnungen für Ordner mit übereinstimmenden Namen vorbereiten**

aus und klicken Sie auf **Weiter**.

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

c. Klicken Sie auf **Weiter**, nachdem Zuordnungen erfolgreich erstellt wurden.

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

Ergebnis

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

Konfigurieren von Ressourcenzuordnungen

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

Was Sie brauchen

Sie sollten die geschützten und Recovery-Standorte verbunden haben.

Im Site Recovery Manager (SRM) können Ressourcen in Ressourcen-Pools, ESXi Hosts oder vSphere Clustern zusammengefasst werden.

Schritte

1. Melden Sie sich am vCenter Server an und klicken Sie auf **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Seite aus, und klicken Sie dann auf **Verwalten**.
3. Wählen Sie auf der Registerkarte Verwalten die Option **Ressourcenzuordnungen** aus.
4. Klicken Sie auf **Neu**, um eine neue Ressourcenzuordnung zu erstellen.

   Der Assistent „Ressourcenzuordnung erstellen“ wird angezeigt.

5. Führen Sie im Assistenten „Ressourcenzuordnung erstellen“ folgende Schritte aus:
   a. Wählen Sie **Zuordnungen für Ressource mit übereinstimmenden Namen automatisch vorbereiten** aus und klicken Sie auf **Weiter**.
   b. Wählen Sie die gewünschten Rechenzentrumsobjekte für die geschützten und Recovery-Standorte aus und klicken Sie auf **Zuordnungen hinzufügen**.
   c. Klicken Sie auf **Weiter**, nachdem Zuordnungen erfolgreich erstellt wurden.
   d. Wählen Sie das zuvor verwendete Objekt aus, um eine umgekehrte Zuordnung zu erstellen, und klicken Sie dann auf **Fertig stellen**.

Ergebnis

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

Platzhalter-Datastores konfigurieren

Sie sollten einen Platzhalterdatenspeicher konfigurieren, um einen Platz im vCenter Inventory am Recovery-Standort für die geschützte Virtual Machine (VM) zu halten. Der Platzhalter-Datenspeicher muss nicht groß sein, da die Platzhalter-VMs klein sind und nur einige Hundert Kilobyte verwenden.

Was Sie brauchen

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

Schritte

1. Melden Sie sich am vCenter Server an und klicken Sie auf **Site Recovery** > **Sites**.
2. Wählen Sie Ihre geschützte Seite aus, und klicken Sie dann auf **Verwalten**.
3. Wählen Sie auf der Registerkarte Verwalten die Option **Platzhalter-Datenspeicher** aus.
4. Klicken Sie auf **New**, um einen neuen Platzhalterdatenspeicher zu erstellen.
5. Wählen Sie den entsprechenden Datenspeicher aus, und klicken Sie dann auf **OK**.

   Als Platzhalter-Datenspeicher können lokale oder Remote-Standorte verwendet werden und sollten nicht repliziert werden.

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

Konfigurieren Sie SRA mit Array Manager

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

Was Sie brauchen

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

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

Schritte

1. Klicken Sie in SRM auf **Array Manager** und dann auf **Array Manager hinzufügen**.
2. Geben Sie die folgenden Informationen ein, um das Array in SRM zu beschreiben:

a. Geben Sie einen Namen ein, um den Array-Manager im Feld **Anzeigename** zu identifizieren.
b. Wählen Sie im Feld **SRA Typ NetApp Storage Replication Adapter für ONTAP** aus.
c. Geben Sie die Informationen ein, die für eine Verbindung zum Cluster oder zur SVM benötigen:
   - Wenn Sie eine Verbindung zu einem Cluster herstellen, sollten Sie die Cluster-Management-LIF eingeben.
   - Wenn Sie eine direkte Verbindung zu einer SVM herstellen, sollten Sie die IP-Adresse der SVM Management LIF eingeben.

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

d. Wenn Sie eine Verbindung zu einem Cluster herstellen, geben Sie den Namen der SVM in das Feld **SVM Name** ein.

   Sie können dieses Feld auch leer lassen.

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

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

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

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

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

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

3. Klicken Sie Auf **Weiter**.
4. Überprüfen Sie, ob das Array erkannt und unten im Fenster Array-Manager hinzufügen angezeigt wird, und klicken Sie auf **Fertig stellen**.

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

Überprüfung replizierter Storage-Systeme

Sie sollten überprüfen, ob der geschützte Standort und der Recovery-Standort nach der Konfiguration des Storage Replication Adapter (SRA) erfolgreich gepaart wurden. Das

replizierte Storage-System sollte sowohl vom geschützten Standort als auch vom Wiederherstellungsstandort erkannt werden können.

Was Sie brauchen

- Sie sollten Ihr Storage-System konfiguriert haben.
- Sie sollten den geschützten Standort und den Recovery-Standort mit dem SRM Array Manager gekoppelt haben.
- Bevor Sie den Test-Failover und den Failover-Vorgang für SRA durchführen, sollten Sie die FlexClone Lizenz und die SnapMirror Lizenz aktiviert haben.

Schritte

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

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

Management von ONTAP-Tools

Managen von Datastores

Mounten von NFS- und VMFS-Datastores

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

> Einige der Rechtsklick-Aktionen sind abhängig von den vSphere-Client-Versionen und dem ausgewählten Datastore-Typ deaktiviert oder nicht verfügbar. Wenn Sie vSphere Client 8.0 oder höher verwenden, sind einige der Optionen mit der rechten Maustaste ausgeblendet. Von vSphere 7.0U3 bis vSphere 8.0, obwohl die Optionen angezeigt werden, wird die Aktion deaktiviert.

Schritte

1. Klicken Sie auf der vSphere Client-Startseite auf **Hosts und Cluster**.
2. Wählen Sie im Navigationsbereich das Rechenzentrum aus, das den Host enthält.
3. Wiederholen Sie Schritt 2 für weitere Hosts.
4. Um NFS/VMFS-Datastores auf dem Host oder Host-Cluster zu mounten, klicken Sie mit der rechten Maustaste darauf, und wählen Sie dann **NetApp ONTAP Tools** > **Mount Datastores** aus.
5. Wählen Sie die Datenspeicher aus, die Sie mounten möchten, und klicken Sie dann auf **Mount**.

Sie können den Fortschritt im Fenster Letzte Aufgabe verfolgen.

Mounten Sie einen VVols Datastore

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

Schritte

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

Sie können den Fortschritt im Fenster Letzte Aufgabe verfolgen.

Redimensionierung von NFS- und VMFS-Datenspeichern

Durch die Größenänderung eines Datenspeichers können Sie den Speicher für die

Dateien Ihrer virtuellen Maschine erhöhen. Sie können die Größe eines Datastores ändern, wenn sich Ihre Infrastrukturanforderungen ändern.

Über diese Aufgabe

Sie können nur die Größe von NFS- und VMFS-Datastores erhöhen. Ein FlexVol Volume, das Teil eines NFS- und VMFS-Datastores ist, kann nicht unter die vorhandene Größe verkleinert, aber um maximal 120 % vergrößert werden.

Schritte

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

Erweitern Sie VVols Datastores

Wenn Sie in der vCenter-Objektansicht mit der rechten Maustaste auf das Datastore-Objekt klicken, werden im Abschnitt „Plug-in“ ONTAP-Tools für von VMware vSphere unterstützte Aktionen angezeigt. Bestimmte Aktionen werden abhängig vom Typ des Datenspeichers und den aktuellen Benutzerberechtigungen aktiviert.

Schritte

1. Klicken Sie auf der vSphere Client-Startseite auf **Hosts und Cluster**.
2. Wählen Sie im Navigationsbereich das Rechenzentrum aus, das den Datastore enthält.
3. Klicken Sie mit der rechten Maustaste auf den Datastore und wählen Sie **NetApp ONTAP Tools** > **Speicher zum Datastore hinzufügen**.
4. Im Fenster **create oder Select Volumes** können Sie entweder neue Volumes erstellen oder aus den vorhandenen Volumes auswählen. Die Benutzeroberfläche ist selbsterklärend. Befolgen Sie die Anweisungen gemäß Ihrer Wahl.
5. Überprüfen Sie im Fenster **Summary** die Auswahl und klicken Sie auf **Expand**. Sie können den Fortschritt im Fenster Letzte Aufgaben verfolgen.

VVols Datastores werden verkleinert

Mit der Aktion „Datastore löschen“ wird der Datastore gelöscht, wenn sich keine VVols auf dem ausgewählten Datastore befinden.

Schritte

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

Mit dieser Option können Sie das Volume auswählen, auf dem sich die VVols befinden, wird deaktiviert.

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

Löschen Sie Datastores

Die Aktion „Storage aus Datastore entfernen“ wird von allen ONTAP-Tools für VMware vSphere unterstützt, die VVols-Datastores im vCenter Server erkannt oder gemanagt haben. Durch diese Aktion können Volumes aus dem VVols Datastore entfernt werden.

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

Löschen des Datastore Task aus den ONTAP-Tools für VMware vSphere im vCenter-Server führt Folgendes aus:

- Unmountet den vVol Container.
- Bereinigt igroup. Wenn Initiatorgruppe nicht verwendet wird, entfernt iqn von der Initiatorgruppe.
- Löscht den Vvol-Container.
- Belässt die Flex-Volumes auf dem Storage Array.

Gehen Sie wie folgt vor, um NFS-, VMFS- oder vVOL-Datastore aus ONTAP-Tools aus vCenter Server zu löschen:

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie mit der rechten Maustaste auf ein Hostsystem oder einen Hostcluster oder einen Datastore, und wählen Sie dann **NetApp ONTAP Tools** > **Datastore löschen** aus.

   Sie können die Datastores nicht löschen, wenn es virtuelle Maschinen gibt, die diesen Datastore verwenden. Sie müssen die virtuellen Maschinen in einen anderen Datenspeicher verschieben, bevor Sie den Datastore löschen.

   a. Im Falle eines NFS- oder VMFS-Datenspeichers wird ein Dialogfeld mit der Liste der VMs angezeigt, die den Datenspeicher verwenden.

   b. Im Fall eines VVols Datastore wird der Datastore durch die Aktion „Datastore löschen“ nur gelöscht, wenn keine VVols damit verbunden sind. Das Dialogfeld Datastore löschen bietet eine Option zum Löschen von Volumes aus dem ONTAP-Cluster.
3. Um die Backing Volumes auf dem ONTAP-Speicher zu löschen, wählen Sie **Delete Volumes on ONTAP Cluster** aus.

ONTAP-Speicheransichten für Datastores

Die Ansicht „ONTAP Storage“ unter „Configure“ der ONTAP-Tools für VMware vSphere liefert Daten zu den Datastores und ihrem Volume. Diese Ansicht bietet die Storage-

Ansicht des Datastore.

ONTAP-Speicheransichten für NFS-Datastores

Schritte

1. Navigieren Sie vom vSphere Client zum NFS-Datastore.
2. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Configure**.
3. Wählen Sie **NetApp ONTAP-Tools** > **ONTAP-Speicher**. Die **Speicherdetails** und **NFS Details** werden im rechten Fensterbereich angezeigt.
   - Die Seite mit den Storage-Details enthält Informationen zu Storage-Back-Ends, Aggregaten und Volumes.
   - Die Seite mit den NFS-Details enthält Daten zum NFS-Datastore.

ONTAP-Speicheransichten für VMFS-Datastores

Schritte

1. Navigieren Sie vom vSphere Client zum VMFS-Datastore.
2. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Configure**.
3. Wählen Sie **NetApp ONTAP-Tools** > **ONTAP-Speicher**. Die **Speicherdetails** und **LUN Details** werden im rechten Fensterbereich angezeigt.
   - Die Seite mit den Storage-Details enthält Informationen zu Storage-Back-Ends, Aggregaten und Volumes.
   - Die Seite mit den LUN-Details enthält Daten zur LUN.

ONTAP Storage-Ansichten für VVols Datastores

Schritte

1. Navigieren Sie vom vSphere Client zum VVols Datastore.
2. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Configure**.
3. Wählen Sie **NetApp ONTAP-Tools** > **ONTAP-Speicher**.
4. In der Ansicht ONTAP Storage werden alle Volumes aufgelistet. Sie können Speicher im ONTAP-Speicherbereich erweitern oder entfernen.

   Befolgen Sie die Anweisungen im "Erweitern Sie VVols Datastores" Abschnitt zum Hinzufügen "VVols Datastores werden verkleinert"eines VVols-Datastores und im Abschnitt zum Löschen des Datastores.

Storage-Ansicht der virtuellen Maschine

In der Ansicht Storage wird die Liste der VVols angezeigt, die von der virtuellen Maschine erstellt werden.

Diese Ansicht gilt für die VM, auf der mindestens ein ONTAP-Tool für durch VMware vSphere gemanagte VVols-Datastore-bezogene Festplatte gemountet ist.

Schritte

1. Navigieren Sie vom vSphere Client zur virtuellen Maschine.

2. Klicken Sie im rechten Fensterbereich auf die Registerkarte **Monitor**.
3. Wählen Sie **NetApp ONTAP Tools** > **Speicher**. Die **Speicher**-Details werden im rechten Fensterbereich angezeigt. Sie können die Liste der VVols anzeigen, die auf der VM vorhanden sind.

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

Managen von Storage-Schwellenwerten

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

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie auf der Shortcuts-Seite unter dem Plug-ins-Bereich auf **NetApp ONTAP Tools**.
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 **nahezu voll** und **voll** ein und klicken Sie auf Speichern. Sie können die Zahlen auf die empfohlenen Werte zurücksetzen: 80 für fast voll und 90 für voll.

Managen von Storage-Back-Ends

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

Storage erkennen

Sie können die Erkennung eines Storage-Back-End nach Bedarf ausführen, ohne auf eine geplante Erkennung warten zu müssen, um die Speicherdetails zu aktualisieren.

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

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie auf der Shortcuts-Seite unter dem Plug-ins-Bereich auf **NetApp ONTAP Tools**.
3. Navigieren Sie im linken Bereich der ONTAP-Tools zu **Speicher-Backends** und wählen Sie ein Speicher-Backend aus.
4. Klicken Sie auf das vertikale Ellipsenmenü und wählen Sie **Speicher entdecken**

Sie können den Fortschritt im Fenster Letzte Aufgaben verfolgen.

Speicherbackends ändern

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

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`

2. Klicken Sie auf der Shortcuts-Seite unter dem Plug-ins-Bereich auf **NetApp ONTAP Tools**.
3. Navigieren Sie im linken Bereich der ONTAP-Tools zu **Speicher-Backends** und wählen Sie ein Speicher-Backend aus.
4. Klicken Sie auf das vertikale Ellipsenmenü und wählen Sie **Ändern**, um die Zugangsdaten oder den Portnamen zu ändern. Sie können den Fortschritt im Fenster Letzte Aufgaben verfolgen.

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

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste Speicher-Back-Ends aus.
4. Wählen Sie das zu ändernde Speicher-Back-End aus.
5. Klicken Sie auf das vertikale Ellipsenmenü und wählen Sie **Ändern**.
6. Sie können die Anmeldeinformationen oder den Port ändern. Geben Sie den **Username** und das **Passwort** ein, um das Speicher-Backend zu ändern.

Entfernen Sie die Speicher-Back-Ends

Sie müssen alle mit dem Speicher-Back-End verbundenen Datenspeicher löschen, bevor Sie das Speicher-Back-End entfernen. Gehen Sie wie folgt vor, um ein Speicher-Back-End zu entfernen.

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie auf der Shortcuts-Seite unter dem Plug-ins-Bereich auf **NetApp ONTAP Tools**.
3. Navigieren Sie im linken Bereich der ONTAP-Tools zu **Speicher-Backends** und wählen Sie ein Speicher-Backend aus.
4. Klicken Sie auf das vertikale Ellipsenmenü und wählen Sie **Entfernen**. Stellen Sie sicher, dass das Speicher-Back-End keine Datastores enthält. Sie können den Fortschritt im Fenster Letzte Aufgaben verfolgen.

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

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste **Speicher-Backends** aus.
4. Wählen Sie das Storage-Backend aus, das Sie entfernen möchten
5. Klicken Sie auf das vertikale Ellipsenmenü und wählen Sie **Entfernen**.

Drilldown-Ansicht des Storage-Back-End

Auf der Storage-Back-End-Seite werden alle Storage-Back-Ends aufgeführt. Sie können Vorgänge für die Speicher-Back-Ends, die Sie hinzugefügt haben, und nicht für die einzelnen untergeordneten Elemente des Clusters ausführen.

Wenn Sie entweder auf das übergeordnete Cluster oder auf das untergeordnete Cluster unter dem Speicher-Back-End klicken, wird die Gesamtzusammenfassung der Komponente angezeigt. Wenn Sie auf das übergeordnete Cluster klicken, haben Sie die Dropdown-Liste Aktionen, aus der Sie die Vorgänge Speicher erkennen, ändern und entfernen können. Diese Option fehlt, wenn Sie auf die untergeordnete SVM klicken.

Die Übersichtsseite enthält folgende Details:

- Status des Storage-Backends
- Kapazitätsinformationen
- Grundlegende Informationen zur VM
- Netzwerkinformationen wie IP-Adresse und Port des Netzwerks. Für die untergeordnete SVM werden die Informationen mit dem übergeordneten Speicher-Back-End identisch sein.
- Berechtigungen sind für das Speicher-Back-End zulässig und eingeschränkt. Für die untergeordnete SVM werden die Informationen mit dem übergeordneten Speicher-Back-End identisch sein. Berechtigungen werden nur auf den Cluster-basierten Speicher-Back-Ends angezeigt. Wenn Sie SVM als Speicher-Backend hinzufügen, werden die Informationen zu Berechtigungen nicht angezeigt.

Auf der Registerkarte Schnittstelle finden Sie detaillierte Informationen zur Schnittstelle.

Auf der Registerkarte Lokale Tiers finden Sie detaillierte Informationen zur Aggregationsliste.

Verwalten der vCenter Server-Instanz

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

Verknüpfen oder trennen Sie Storage-Back-Ends mit vCenter Server-Instanz

Auf der Listingseite des vCenter-Servers wird die zugehörige Anzahl von Speicher-Back-Ends angezeigt. Jede vCenter Server-Instanz hat die Möglichkeit, ein Storage-Back-End zuzuordnen oder zu deaktivieren. Diese Aufgabe hilft Ihnen, eine Zuordnung zwischen dem Storage-Backend und der eingebetgenen vCenter Server-Instanz global zu erstellen.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste vCenter Server Instanzen aus.
4. Klicken Sie auf die vertikalen Ellipsen gegenüber dem vCenter Server, den Sie mit Speicher-Back-Ends verknüpfen oder trennen möchten.
5. Wählen Sie **Speicher-Backend verknüpfen oder trennen**, je nachdem, welche Aktion Sie durchführen möchten.

VCenter Server-Instanz ändern

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

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste vCenter Server Instanzen aus
4. Klicken Sie auf die vertikalen Ellipsen gegenüber dem vCenter Server, den Sie ändern möchten, und wählen Sie **Ändern**.
5. Ändern Sie die Details der vCenter Server-Instanz, und wählen Sie **Ändern** aus.

Entfernen Sie die vCenter Server-Instanz

Sie müssen alle Speicher-Back-Ends entfernen, die mit dem vCenter Server verbunden sind, bevor Sie ihn entfernen.

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste vCenter Server Instanzen aus
4. Klicken Sie auf die vertikalen Ellipsen gegenüber dem vCenter Server, den Sie entfernen möchten, und wählen Sie **Entfernen** aus.

> Sobald Sie die vCenter Server-Instanzen entfernt haben, wird sie nicht mehr von der Anwendung verwaltet.

Verwalten von Zertifikaten

Mit einer einzigen Instanz der ONTAP Tools für VMware vSphere können mehrere vCenter Server-Instanzen gemanagt werden. ONTAP Tools für VMware vSphere werden mit einem selbstsignierten Zertifikat für VASA Provider implementiert. Dadurch kann nur eine vCenter Server-Instanz für VVols-Datastores gemanagt werden. Wenn Sie mehrere vCenter Server-Instanzen managen und die VVols-Funktion auf mehreren vCenter Server-Instanzen aktivieren möchten, müssen Sie das selbstsignierte Zertifikat über die Benutzeroberfläche von ONTAP Tools Manager in ein benutzerdefiniertes CA-Zertifikat ändern. Sie können die gleiche Oberfläche verwenden, um alle Zertifikate zu erneuern oder zu aktualisieren.

> Eine andere Load Balancer-IP-Adresse, die verschiedenen Domänen zugeordnet ist, wird nicht unterstützt, wenn Sie ein selbstsigniertes Upgrade auf eine benutzerdefinierte CA durchführen.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.

3. Wählen Sie **Certificates** > **VASA Provider** > **Renew**, um die Zertifikate zu erneuern.

   Das System ist offline, bis das Zertifikat erneuert wird.

4. Um das selbstsignierte Zertifikat auf ein benutzerdefiniertes CA-Zertifikat zu aktualisieren, wählen Sie **Certificates** > **VASA Provider** > **Upgrade auf CA**.
   a. Laden Sie im Popup-Fenster **Upgrade Certificate to Custom CA** das Serverzertifikat, den privaten Schlüssel des Serverzertifikats, das Stammzertifizierungszertifikat und die Zwischenzertifikatdateien hoch. Der QuickInfo enthält eine Beschreibung der Zertifikate.
   b. Geben Sie den Domänennamen ein, für den Sie dieses Zertifikat erstellt haben.
   c. Klicken Sie Auf **Upgrade**.

      Das System ist offline, bis das Upgrade abgeschlossen ist.

Verwalten von Initiatorgruppen und Exportrichtlinien

In ONTAP werden Exportrichtlinien verwendet, um Hosts einen Datenzugriff auf Volume-Pfaden zu ermöglichen und Initiatorgruppen werden verwendet, um ESXi Hosts den Datenzugriff auf dem Datenpfad mit der logischen Einheitennummer (LUN) zu ermöglichen. Die ONTAP Tools für VMware vSphere erleichtern die igroup-Erstellung und bieten umfassende, intuitive Workflows. Um Konsistenz zu gewährleisten, wird die direkte iGroup-Erstellung auf Speicherplattformen nicht unterstützt.

Wenn Datastores für virtuelle Volumes erstellt oder auf Hosts in vCenter Server gemountet werden, müssen die Hosts abhängig vom Protokolltyp des Datastore Zugriff auf Volumes (NFS) oder LUNs (iSCSI) erhalten.

Die Exportpolitik ist dynamisch und die neue Exportpolitik wird mit dem Namensformat Dreizack-UUID erstellt. Gehen Sie auf Ihrem ONTAP System Manager zu **Speicher** > **Speicher-VMs** > **[Name der Speicher-VM]** > **Einstellungen** > **Exportrichtlinien**, um die Exportrichtlinie anzuzeigen.

Die Initiatorgruppen und Exportrichtlinien in den ONTAP Tools für VMware vSphere werden effizient gemanagt und bieten folgende Vorteile:

- Unterstützt migrierte Exportrichtlinien und Initiatorgruppen.
- Keine Unterbrechung der ein- und Ausgabevorgänge der virtuellen Maschine.
- Unterstützt das Mounten auf zusätzlichen Hosts ohne manuelles Eingreifen.
- Minimiert den Bedarf zum Managen der Anzahl von Initiatorgruppen und Exportrichtlinien.
- Ein Garbage Collector löscht automatisch alle nicht verwendeten verwalteten Initiatorgruppen und exportiert Richtlinien in regelmäßigen Abständen.
- Wenn ein Datastore auf Host-Cluster-Ebene bereitgestellt wird, wird die Initiatorgruppe mit allen Host-Initiatoren unter dem Host-Cluster erstellt, die der Initiatorgruppe hinzugefügt werden.

Zugriff auf ONTAP Tools für die VMware vSphere Wartungskonsole

Überblick über die ONTAP Tools für die VMware vSphere Wartungskonsole

Sie können Ihre Applikations-, System- und Netzwerkkonfigurationen mithilfe der Wartungskonsole der ONTAP Tools managen. Sie können Ihr Administratorkennwort und Ihr Wartungskennwort ändern. Außerdem können Sie Supportpakete generieren, verschiedene Protokollebenen festlegen, TLS-Konfigurationen anzeigen und verwalten und die Remote-Diagnose starten.

Sie sollten VMware Tools nach der Bereitstellung von ONTAP Tools für VMware vSphere installieren lassen, um auf die Wartungskonsole zuzugreifen. Sie sollten `maint` als Benutzernamen und Passwort verwenden, 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-Login-Konsole verwenden.

Sie sollten ein Kennwort für den `diag` Benutzer festlegen, während Sie die Ferndiagnose aktivieren.

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

Konsolenmenü	Optionen
Anwendungskonfiguration	1. Zeigt eine Zusammenfassung des Serverstatus an 2. Ändern der PROTOKOLLEBENE für VASA Provider Services und SRA Services 3. Deaktivieren Sie AutoSupport
Systemkonfiguration	1. Starten Sie die virtuelle Maschine neu 2. Virtuelle Maschine herunterfahren 3. Erstellen Sie ein Token, um das Passwort der Manager-Benutzeroberfläche zurückzusetzen 4. Zeitzone ändern 5. Fügen Sie den neuen NTP-Server hinzu 6. Erhöhen der Größe der Jail-Festplatte (/jail) 7. Upgrade 8. Installation der VMware Tools

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

Konfigurieren Sie den Zugriff auf die Remote-Diagnose

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

Was Sie brauchen

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 weist folgende Einschränkungen auf:

- Sie haben nur ein Anmeldekonto pro Aktivierung von SSH.
- SSH-Zugriff auf das Diagnose-Benutzerkonto ist 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 Diagnose-Benutzer mit SSH an.

Schritte

1. Öffnen Sie vom vCenter Server aus eine Konsole zu VASA Provider.
2. Melden Sie sich als Wartungbenutzer an.
3. Geben Sie ein `4`, um Support und Diagnose auszuwählen.
4. Geben Sie ein `3`, um den Zugriff auf die Ferndiagnose aktivieren auszuwählen.
5. Geben Sie `y` in das Dialogfeld Bestätigung ein, um den Remote-Diagnosemodus zu aktivieren.
6. Geben Sie ein Kennwort für den Remote-Diagnosezugriff ein.

Starten Sie SSH auf anderen Nodes

Sie müssen SSH auf anderen Nodes vor dem Upgrade starten.

Was Sie brauchen

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

Über diese Aufgabe

Führen Sie dieses Verfahren vor dem Upgrade für jeden der Nodes durch.

Schritte

1. Öffnen Sie vom vCenter Server aus eine Konsole zu VASA Provider.
2. Melden Sie sich als Wartungbenutzer an.
3. Geben Sie ein `4`, um Support und Diagnose auszuwählen.
4. Geben Sie ein `1`, um Access Diagnostic Shell auszuwählen.
5. Geben Sie ein, `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 über die Wartungskonsole aktualisieren.

Was Sie brauchen

Sie müssen über Anmeldedaten für Wartungsbenutzer verfügen.

Über diese Aufgabe

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

Schritte

1. Öffnen Sie vom vCenter Server aus eine Konsole zu VASA Provider.
2. Melden Sie sich als Wartungbenutzer an.
3. Geben Sie ein `2` , um das Menü Systemkonfiguration auszuwählen.
4. Geben Sie ein, `9` um die ONTAP-Anmeldedaten zu ändern.
5. Geben Sie ein, `10` um die vCenter-Anmeldedaten zu ändern.

Berichte zum ONTAP-Tool

ONTAP Tools für das VMware vSphere Plug-in bieten Berichte für Virtual Machines und Datastores. Wenn Sie im Abschnitt „Verknüpfungen“ des vCenter-Clients das Symbol „NetApp ONTAP-Tools für VMware vSphere“ auswählen, wechselt die

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

Der Bericht „Virtual Machines“ enthält die Liste der erkannten virtuellen Maschinen (mindestens eine Festplatte aus ONTAP-Storage-basierten Datastores) mit Leistungskennzahlen. Wenn Sie den VM-Datensatz erweitern, werden alle Informationen zum festplattenbezogenen Datenspeicher angezeigt.

Der Datastores-Bericht zeigt die Liste erkannter oder anerkannter ONTAP Tools für von VMware vSphere gemanagte Datastores, die über das ONTAP Storage Back-End aller Arten mit Performance-Kennzahlen bereitgestellt werden.

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

Sammeln Sie die Protokolldateien

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

Die Generierung von Protokollen über den ONTAP-Tools-Manager umfasst alle Protokolle für alle vCenter-Serverinstanzen. Das Generieren von Protokollen aus der vCenter Client-Benutzeroberfläche wird für den ausgewählten vCenter Server berücksichtigt.

Schritte

1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Wählen Sie in der Seitenleiste **Log Bundles** aus.

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

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

Gehen Sie wie folgt vor, um Protokollbündel über die vCenter-Client-Benutzeroberfläche zu generieren:

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Gehen Sie auf der vSphere Client-Homepage zu **Support** > **Log Bundle** > **Generate**.
3. Geben Sie das Protokollbündel-Label an, und generieren Sie das Protokollbündel. Sie können die Download-Option sehen, wenn die Dateien generiert werden. Das Herunterladen kann einige Zeit in Anspruch nehmen.

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

Management von Virtual Machines

Überlegungen zum Migrieren oder Klonen von Virtual Machines

Beachten Sie einige Überlegungen bei der Migration vorhandener Virtual Machines in Ihrem Datacenter.

Migrieren Sie geschützte Virtual Machines

Sie können die geschützten virtuellen Maschinen migrieren in:

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

Wenn die Virtual Machine in ein anderes FlexVol Volume migriert wird, wird auch die entsprechende Metadatendatei mit den Informationen der Virtual Machine aktualisiert. Wenn eine virtuelle Maschine zu einem anderen ESXi-Host, aber demselben Storage migriert wird, wird die zugrunde liegende FlexVol-Volume-Metadatendatei nicht geändert.

Klonen geschützter Virtual Machines

Sie können geschützte Virtual Machines folgendermaßen klonen:

- Derselbe Container desselben FlexVol Volumes mithilfe der Replizierungsgruppe

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

- Derselbe Container eines anderen FlexVol Volumes unter Verwendung der Replizierungsgruppe

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

- Unterschiedlicher Container oder VVols Datastore

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

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

Der Klon einer geschützten Virtual Machine wird unterstützt.

Snapshots Von Virtual Machines

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

Sie können auch nicht geschützte virtuelle Maschinen mit einem Speicher-Snapshot schützen. Für diesen Release sollten Sie den Speicher-Snapshot löschen, bevor Sie den Schutz für die virtuelle Maschine

aktivieren.

Migrieren Sie Virtual Machines mit NFS- und VMFS-Datastores zu VVols Datastores

Sie können Virtual Machines von NFS- und VMFS-Datastores auf Virtual Volumes (VVols) Datastores migrieren, um von richtlinienbasiertem VM Management und anderen VVols Funktionen zu profitieren. Mit VVols Datastores können Sie höhere Workload-Anforderungen erfüllen.

Was Sie brauchen

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

Über diese Aufgabe

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

Schritte

1. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine, die Sie migrieren möchten, und klicken Sie dann auf **Migrieren**.
2. Wählen Sie **nur Speicher ändern** und klicken Sie dann auf **Weiter**.
3. Wählen Sie ein virtuelles Festplattenformat, eine VM-Speicherrichtlinie und einen vVol-Datastore aus, der den Funktionen des zu migrierenden Datastore entspricht. Klicken Sie Auf **Weiter**.
4. Überprüfen Sie die Einstellungen und klicken Sie dann auf **Fertig stellen**.

VASA-Bereinigung

Verwenden Sie die Schritte in diesem Abschnitt, um die VASA-Bereinigung durchzuführen.

Es wird empfohlen, alle VVols-Datastores zu entfernen, bevor Sie die VASA-Bereinigung durchführen.

Schritte

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

Ändern Sie ESXi Hosteinstellungen mithilfe von ONTAP Tools

Über das Dashboard der ONTAP Tools für VMware vSphere können Sie Ihre ESXi Host-Einstellungen bearbeiten.

Was Sie brauchen

Wenn ein Problem mit den ESXi-Hosteinstellungen auftritt, wird das Problem im Portlet „ESXi-Hostsysteme“ des Dashboards angezeigt. Sie können auf das Problem klicken, um den Hostnamen oder die IP-Adresse des ESXi-Hosts anzuzeigen, der das Problem hat.

Schritte

1. Melden Sie sich mit beim vSphere-Client an `https://vcenterip/ui`
2. Klicken Sie auf der Shortcuts-Seite unter dem Plug-ins-Bereich auf **NetApp ONTAP Tools**.
3. Gehen Sie in der Übersicht (Dashboard) des ONTAP Tools für VMware vSphere Plug-ins zum Portlet **ESXi Host Compliance**.
4. Wählen Sie den Link **Empfohlene Einstellungen anwenden**.
5. Wählen Sie im Fenster **empfohlene Hosteinstellungen anwenden** die Hosts aus, die Sie den von NetApp empfohlenen Hosteinstellungen entsprechen möchten, und klicken Sie auf **Weiter**.

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

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

Passwörter verwalten

Ändern Sie das Kennwort des ONTAP Tools Managers

Sie können das Administratorkennwort mit dem ONTAP Tools Manager ändern.

Schritte

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

Kennwort des ONTAP Tools Managers zurücksetzen

Falls Sie das Passwort des ONTAP Tools Managers vergessen haben, können Sie die Administratoranmeldedaten mithilfe des Tokens zurücksetzen, das von den ONTAP Tools für die VMware vSphere Wartungskonsole generiert wurde.

Schritte

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

   Zum Zurücksetzen des Manager-Passworts müssen Sie das Reset-Token mithilfe der ONTAP-Tools für die VMware vSphere-Wartungskonsole generieren. .. Öffnen Sie vom vCenter Server aus die Wartungskonsole .. Geben Sie „2“ ein, um die Option „Systemkonfiguration“ auszuwählen. Geben Sie „3“ ein, um das Token zum Zurücksetzen des Manager-Kennworts zu generieren
3. Geben Sie im Popup-Fenster Passwort ändern den Token zum Zurücksetzen des Passworts, den Benutzernamen und die neuen Kennwortdetails ein.
4. Klicken Sie auf **Reset**, um die Änderungen zu implementieren. Nach erfolgreichem Zurücksetzen des Passworts können Sie sich mit dem neuen Passwort anmelden.

Benutzerkennwort der Anwendung zurücksetzen

Das Benutzerkennwort der Anwendung wird für die Registrierung des SRA- und VASA-Providers bei vCenter Server verwendet.

Schritte

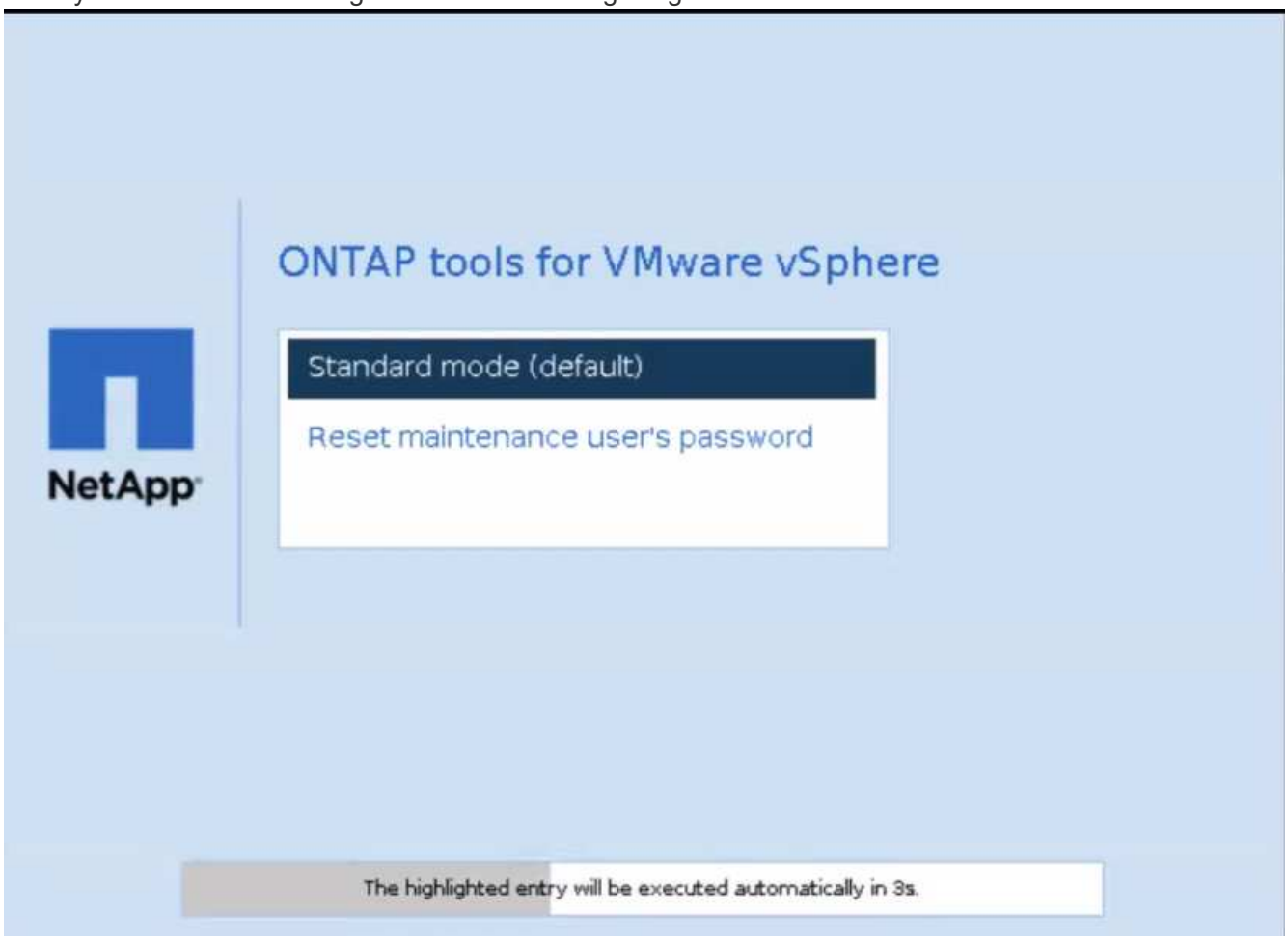
1. Starten Sie den ONTAP Tools Manager über einen Webbrowser: `https://loadBalanceIP:8443/virtualization/ui/`
2. Melden Sie sich mit den ONTAP Tools für VMware vSphere Administrator-Anmeldeinformationen an, die Sie während der Implementierung angegeben haben.
3. Klicken Sie in der Seitenleiste auf **Einstellungen**.
4. Wählen Sie im Fenster **Application user credentials** die Option **Passwort zurücksetzen** aus.
5. Geben Sie den Benutzernamen und das neue Passwort ein, und bestätigen Sie die Eingabe des neuen Passworts.
6. Klicken Sie auf **Reset**, um die Änderungen zu implementieren.

Setzt das Benutzerpasswort der Wartungskonsole zurück

Während des Neustarts des Gastbetriebssystems wird im Menü grub eine Option zum Zurücksetzen des Benutzerpassworts der Wartungskonsole angezeigt. Diese Option wird verwendet, um das Benutzerpasswort der Wartungskonsole auf der entsprechenden VM zu aktualisieren. Sobald das Kennwort zum Zurücksetzen abgeschlossen ist, wird die VM neu gestartet, um das neue Kennwort festzulegen. In einem Szenario mit HA-Bereitstellung wird nach dem Neustart der VM automatisch das Passwort auf den anderen beiden VMs aktualisiert.

Schritte

1. Melden Sie sich bei Ihrem vCenter-Server an
2. Klicken Sie mit der rechten Maustaste auf die VM und wählen Sie **Power** > **Restart Guest OS** während des Systemneustarts wird folgender Bildschirm angezeigt:



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

3. Wählen Sie die Option **Passwort des Wartungsbenutzers zurücksetzen**. Die Wartungskonsole wird geöffnet.
4. Geben Sie in der Konsole die Details zum neuen Passwort ein. Das neue Passwort und die neuen Passwortdetails müssen übereinstimmen, um das Passwort erfolgreich zurückzusetzen. Sie haben drei Chancen, das richtige Passwort einzugeben. Das System wird nach erfolgreicher Eingabe des neuen Passworts neu gestartet.
5. Drücken Sie die Eingabetaste, um fortzufahren. Das Passwort wird auf der VM aktualisiert.

> Das gleiche grub-Menü erscheint auch beim Einschalten der VM. Sie sollten jedoch die Option zum Zurücksetzen des Passworts nur mit der Option **Gast-OS neu starten** verwenden.

Volumes bereinigen

Nachdem Sie ONTAP Tools für die VMware vSphere Implementierung gelöscht haben, sollten Sie die während der Implementierung erstellten FlexVol Volumes bereinigen.

Wenn Sie einen dedizierten ONTAP Cluster für Implementierungen verwendet haben, sollten Sie die FlexVols bereinigen, da die Implementierung viele FlexVols erstellt, die ungenutzt bleiben, was die Performance senkt.

Verwenden Sie die folgenden Richtlinien, um die FlexVols nach der Entfernung von ONTAP Tools zur Implementierung von VMware vSphere zu bereinigen.

Schritte

1. Führen Sie in der VM des primären Node in ONTAP Tools für VMware vSphere den folgenden Befehl aus, um den Bereitstellungstyp zu ermitteln.

   CAT /opt/netapp/meta/ansible_vars.yaml grep -i Protocol

   Handelt es sich um eine iSCSI-Bereitstellung, müssen auch Initiatorgruppen gelöscht werden.

2. Rufen Sie die Liste der in ONTAP während der Implementierung erstellten FlexVols mit dem folgenden Befehl ab.

   Kubectl Beschreiben Sie dauerhafte Volumina.Name AWK -F'=' '{Print 2}'

3. Löschen Sie VMs von vCenter Server, siehe "Entfernen Sie VMs oder VM-Vorlagen aus vCenter Server oder aus dem Datastore"
4. Löschen von Volumes aus ONTAP System Manager, siehe "Löschen Sie ein FlexVol Volume". Geben Sie den genauen Namen des FlexVolume im cli-Befehl ein, um das Volume zu löschen.
5. Löschen Sie im Fall der iSCSI-Bereitstellung SAN-Initiatorgruppen aus ONTAP, siehe "Zeigen Sie SAN-Initiatoren und -Initiatorgruppen an und verwalten Sie sie".

   Bei der HA-Bereitstellung werden vier Initiatorgruppen erstellt und in der nicht-HA-Bereitstellung werden zwei Initiatorgruppen erstellt. Führen Sie den folgenden Befehl aus, um den ersten Initiatorgruppennamen zu finden:

   Kubectl -n dreident get tbc dreident-Backend -o yaml{grep igroupName: '} Print 2'

   Die anderen Initiatorgruppennamen beginnen mit dem Hostnamen der VM.

Upgrade von ONTAP-Tools

Upgraden auf die aktuelle Version von ONTAP-Tools

Beim Upgrade von ONTAP Tools für VMware vSphere 10.0 und 10.1 auf 10.1 wird ein Recovery-Volume erstellt und alle erforderlichen Details in das Recovery-Volume übernommen. Das Recovery Volume kann verwendet werden, um die ONTAP Tools für die Einrichtung von VMware vSphere wiederherzustellen, wenn Sie Ihre Konfiguration wiederherstellen müssen. Wenn Sie ein Upgrade der ONTAP Tools auf Patch-Ebene für VMware vSphere 10.1 durchführen, wird dasselbe Recovery-Volume verwendet und die Details aktualisiert. Upgrade wird sowohl für HA-Implementierungen als auch für Implementierungen ohne HA unterstützt.

Bevor Sie beginnen

Sie müssen die folgenden Schritte ausführen, bevor Sie mit der Upgrade-Aufgabe fortfahren:

Diagnose Aktivieren

1. Öffnen Sie im vCenter Server eine Konsole für ONTAP Tools.
2. Melden Sie sich als Wartungbenutzer an.
3. Geben Sie **4** ein, um Support und Diagnose auszuwählen.
4. Geben Sie **2** ein, um den Zugriff auf die Ferndiagnose zu aktivieren.
5. Geben Sie **y** ein, um das Passwort Ihrer Wahl festzulegen.
6. Melden Sie sich an der VM-IP-Adresse vom Terminal/Putty mit dem Benutzer als 'diag' und dem Passwort an, das im vorherigen Schritt festgelegt wurde.

Backup von MongoDB

Führen Sie die folgenden Befehle aus, um ein Backup von MongoDB zu erstellen:

- Kn exec -it ntv-mongodb-0 sh - kn ist ein Alias von kubectl -n ntv-System.
- dev_grep MONGODB_ROOT_PASSWORD - Führen Sie diesen Befehl im Pod aus.
- „EXIT“ – Führen Sie diesen Befehl aus, um aus dem POD zu kommen.
- Kn exec ntv-mongodb-0 --mongodump -U ROOT -p MONGODB_ROOT_PASSWORD --Archive=/tmp/mongodb-backup.gz --gzip - Führen Sie diesen Befehl aus, um MONGO_ROOT_PASSWORD set aus dem obigen Befehl zu ersetzen.
- Kn CP ntv-mongodb-0:/tmp/mongodb-backup.gz ./mongodb-backup.gz - Führen Sie diesen Befehl aus, um das mit dem obigen Befehl erstellte mongodb Backup von Pod zu Host zu kopieren.

Nehmen Sie den Snapshot von allen Volumen

- Führen Sie den Befehl 'kn get pvc' aus und speichern Sie die Ausgabe des Befehls.
- Erstellen Sie Snapshots aller Volumes nacheinander mit einer der folgenden Methoden:
  - Führen Sie in der CLI den Befehl *Volume Snapshot create -vserver <vserver_name> -Volume <volume_name> -Snapshot <snapshot_name>* aus

◦ Über die Benutzeroberfläche des ONTAP-Systemmanagers können Sie das Volume in der Suchleiste anhand des Namens durchsuchen und dann das Volume durch Klicken auf den Namen öffnen. Wechseln Sie zu Snapshot und fügen Sie den Snapshot dieses Volumes hinzu.

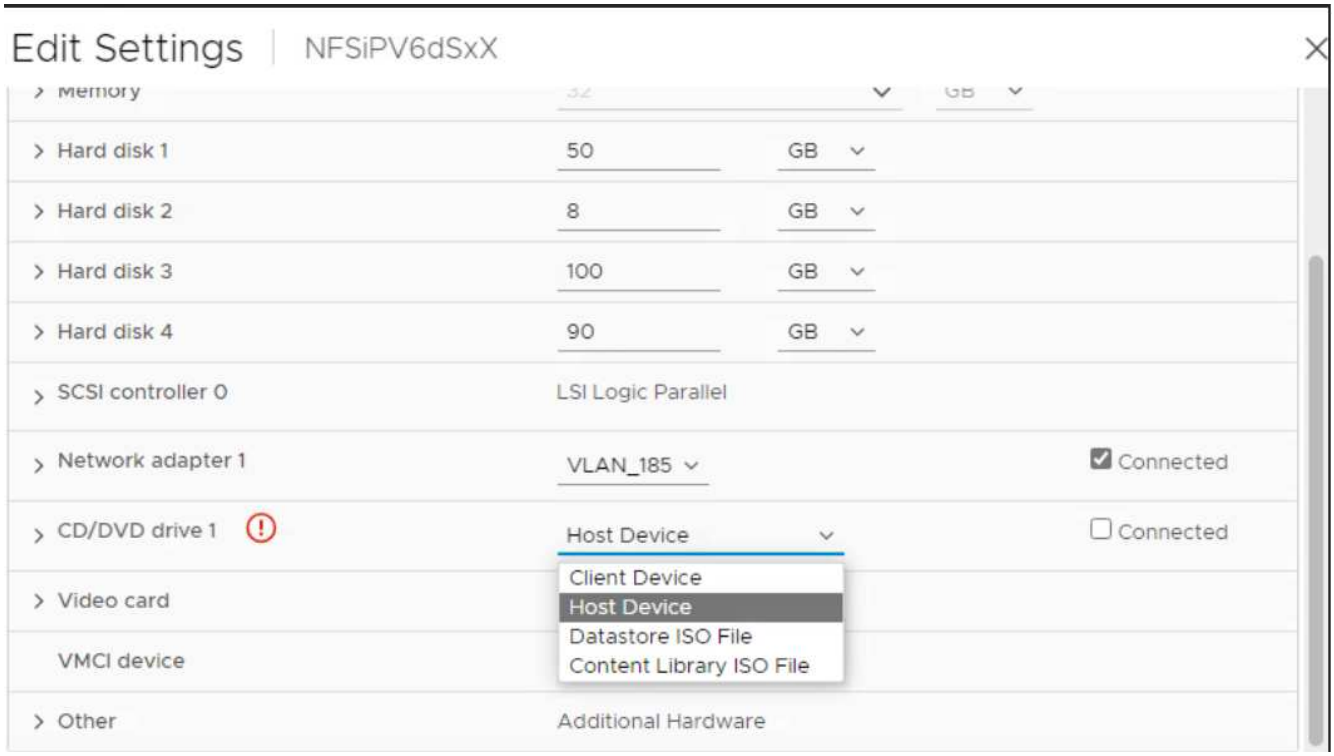
Nehmen Sie die Momentaufnahme von ONTAP-Tools für VMware vSphere VMs in vCenter (3VMs im Fall der HA-Bereitstellung, 1 VM im Falle einer nicht-HA-Bereitstellung)

- Wählen Sie in der vSphere-Client-Benutzeroberfläche die VM aus.
- Gehen Sie zur Registerkarte Snapshots und klicken Sie auf die Schaltfläche **Snapshot erstellen**.

Löschen Sie aus dem Protokoll-Bundle die fertig gestellten Pods mit dem Präfix „Generate-Support-Bundle-Job“, bevor Sie das Upgrade durchführen. Wenn derzeit das Support-Bundle generiert wird, warten Sie, bis der Vorgang abgeschlossen ist, und löschen Sie den Pod.

Schritte

1. Laden Sie ONTAP-Tools für VMware vSphere hoch, aktualisieren Sie ISO in die Content Library.
2. Wählen Sie auf der primären VM-Seite **actions** > **Edit Settings** aus
3. Wählen Sie im Fenster Einstellungen bearbeiten unter dem Feld **CD/DVD-Laufwerk** die ISO-Datei der Inhaltsbibliothek aus.
4. Wählen Sie die ISO-Datei aus und klicken Sie auf **OK**. Aktivieren Sie das Kontrollkästchen Verbunden im Feld **CD/DVD-Laufwerk**.



5. Öffnen Sie im vCenter Server eine Konsole für ONTAP Tools.
6. Melden Sie sich als Wartungbenutzer an.
7. Geben Sie **3** ein, um das Menü Systemkonfiguration auszuwählen.
8. Geben Sie **7** ein, um die Upgrade-Option auszuwählen.
9. Wenn Sie ein Upgrade durchführen, werden die folgenden Aktionen automatisch ausgeführt:
   a. Zertifikataktualisierung

b. Remote-Plug-in-Upgrade

Upgrade-Fehlercodes

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

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

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

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

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

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

Upgrade-Fehlercode	**Arbeitsablauf**	* Auflösung*
063	Kopieren des Inhalts auf das Wiederherstellungsvolume ist fehlgeschlagen	Snapshot-basierte Recovery
068	Das Rollback von Debian-Paketen ist fehlgeschlagen	Snapshot-basierte Recovery
069	Wiederherstellung der Dateien fehlgeschlagen	Snapshot-basierte Recovery
070	Backup konnte nicht gelöscht werden	Snapshot-basierte Recovery
071	Das Kubernetes-Cluster war in keinem ordnungsgemäßen Zustand	Snapshot-basierte Recovery

072	Die CR-Datei ist nicht auf der Jail-Disk vorhanden	Snapshot-basierte Recovery
073	Beim Anwenden des CR ist ein Fehler aufgetreten, während das Flag für die Abstimmung erzwingen auf FALSE gesetzt wurde	Snapshot-basierte Recovery
074	Mount-ISO ist fehlgeschlagen	Wiederholen Sie die Aktualisierung.
075	Die Vorabprüfungen für die Aktualisierung sind fehlgeschlagen	Wiederholen Sie die Aktualisierung.
076	Aktualisierung der Registrierung fehlgeschlagen	Snapshot-basierte Recovery
077	Fehler beim Zurücksetzen der Registrierung	Snapshot-basierte Recovery
078	Upgrade des Bedieners fehlgeschlagen	Snapshot-basierte Recovery
079	Rollback des Benutzers fehlgeschlagen	Snapshot-basierte Recovery
080	Aktualisierung der Dienste ist fehlgeschlagen	Snapshot-basierte Recovery
081	Rollback der Dienste ist fehlgeschlagen	Snapshot-basierte Recovery
082	Löschen alter Bilder aus Container fehlgeschlagen	Snapshot-basierte Recovery
083	Löschen des Backups ist fehlgeschlagen	Snapshot-basierte Recovery
084	JobManager konnte nicht wieder in die Produktion geändert werden	Snapshot-basierte Recovery
085	Erstellen von CA-Zertifikatgeheimnissen fehlgeschlagen	Snapshot-basierte Recovery
086	Fehler beim Erstellen von Zertifikatsgeheimnissen für Server/privaten Schlüssel	Snapshot-basierte Recovery
087	Fehler! Führen Sie die Schritte für die Aktualisierung nach 10.0 bis 10.1 durch	Schritte nach dem Upgrade fehlgeschlagen.
088	Die Konfiguration der Protokollrotation für journald ist fehlgeschlagen	Wiederholen Sie die Aktualisierung.

Weitere Informationen zu "So stellen Sie ONTAP-Tools für VMware vSphere wieder her, wenn das Upgrade von Version 10.0 auf 10.1 fehlschlägt"

Migration der ONTAP-Tools

Migrieren Sie zur neuesten Version der ONTAP-Tools

Bei der Migration von Storage-Daten werden Storage-Back-Ends manuell über REST-APIs integriert. Bei der Migration von VASA Provider-Daten werden die Daten aus der bestehenden Derby-Datenbank exportiert und in die MongoDB-Datenbank importiert.

Es wird empfohlen, die ONTAP-Tools für das Setup von VMware vSphere 9.xx nur zu migrieren, wenn das Setup die Funktion des VASA-Providers alleine bedient. Bei NVMe-Datastores und vVol-Replizierung wird die Migration des Setups zu ONTAP-Tools für VMware vSphere 10.1 nicht empfohlen.

Über diese Aufgabe

Die Migration wird von ONTAP-Tools für VMware vSphere 9.10D2, 9.11D4, 9.12 und 9.13 Versionen bis 10.1 unterstützt.

Als bestehender Benutzer müssen Sie das OVA-Backup von Ihrer aktuellen Version durchführen, bevor Sie ein Upgrade auf die Patch-Versionen durchführen.

Allgemeine Migrationsschritte

1. Implementieren Sie OVA für ONTAP Tools für VMware vSphere 10.1.
2. Fügen Sie die vCenter Server-Instanz hinzu, die Sie zu ONTAP-Tools für die Version VMware vSphere 10.1 migrieren möchten. Siehe "Fügen Sie vCenter Server-Instanzen hinzu und verwalten Sie sie"
3. Lokales Storage-Back-End aus den ONTAP Tools für VMware vSphere Plug-in vCenter APIs integrieren Fügen Sie Storage als lokal im Umfang enthaltenen Storage für die Migration hinzu.
4. Die NFS- und VMFS-Datenspeicher, die aus den ONTAP-Tools für VMware vSphere 9.xx migriert wurden, sind in den ONTAP-Tools für VMware vSphere 10.1 erst sichtbar, nachdem der Datastore-Erkennungsvorgang ausgelöst wurde. Das Auslösen kann bis zu 30 Minuten dauern. Überprüfen Sie, ob die Datastores auf der Seite „Übersicht“ der UI-Seite „ONTAP Tools for VMware vSphere Plugin“ angezeigt werden.

SRA-Migrationsschritte

Bevor Sie beginnen

Stellen Sie vor der Migration sicher, dass sich einer der Standorte in einem geschützten Zustand befindet und sich der andere im Wiederherstellungsstatus befindet.

Führen Sie keine Migration durch, wenn das Failover gerade abgeschlossen ist und der erneute Schutz aussteht. Führen Sie die erneute Sicherung durch, und führen Sie die Migration durch. Das gilt auch für das Testen des Wiederherstellungsplans. Sobald das Testen des Wiederherstellungsplans abgeschlossen ist, bereinigen Sie die Test-Recovery und starten Sie dann die Migration.

1. Führen Sie die folgenden Schritte aus, um ONTAP-Tools für den SRA-Release-Adapter VMware vSphere 9.xx in der SRM-Benutzeroberfläche zu löschen:

a. Rufen Sie die Seite SRM Configuration Management auf
b. Gehen Sie zum Abschnitt Storage Replication Adapter
c. Klicken Sie auf das Kebab-Menü und dann auf **Konfiguration zurücksetzen**
d. Klicken Sie auf das Kebab-Menü und wählen Sie **Löschen**

   Führen Sie diese Schritte sowohl an Sicherungs- als auch an Recovery-Standorten aus.

2. Installieren Sie ONTAP-Tools für den VMware vSphere 10.1 SRA-Adapter anhand der Schritte in auf Schutz- und Recovery-Seiten "Konfigurieren Sie SRA auf der SRM-Appliance"
3. Führen Sie auf der SRM-UI-Seite die Vorgänge **Arrays ermitteln** und **Geräte ermitteln** aus, und überprüfen Sie, ob die Geräte vor der Migration so angezeigt werden, wie es war.

Migrationsschritte für VASA-Provider

1. Aktivieren Sie Derby-PORT 1527 auf den vorhandenen ONTAP-Tools für VMware vSphere. Um den Port zu aktivieren, melden Sie sich bei CLI mit root user an und führen Sie den folgenden Befehl aus:

```
iptables -I INPUT 1 -p tcp --dport 1527 -j ACCEPT
```

2. Implementieren Sie OVA für ONTAP Tools für VMware vSphere 10.1.
3. Fügen Sie die vCenter Server-Instanz hinzu, die Sie zu ONTAP-Tools für die Version VMware vSphere 10.1 migrieren möchten. Siehe "Fügen Sie eine vCenter Server-Instanz hinzu".
4. Lokales Storage-Back-End aus den Remote Plug-in vCenter APIs integrieren Hinzufügen von Storage als lokalen Umfang für die Migration
5. Geben Sie den folgenden API-Aufruf zur Migration aus:

HTTP-Methode und Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
POST	/API/v1

Verarbeitungsart

Asynchron

Beispiel für Curl

/API/v1/vcenters/{vcguid}/Migration-Jobs

JSON-Eingabebeispiel Request Body für Migration von 9.12 und 9.13:

{ "otv_ip": "10.12.13.45", "vasa_Provider_credentials": { "Username": "Vasauser", "password": **"" } "Database_password": ""** }

Request Body für andere Release-Migration:

{ „otv_ip“: „10.12.13.45“, „vasa_Provider_credentials“: { „Username“: „Vasauser“, „password“: „*“ } }

JSON-Ausgabebeispiel

Ein Jobobjekt wird zurückgegeben. Sie sollten die Jobkennung speichern, um sie im nächsten Schritt zu verwenden.

{ „id“: 123, „Migration_id“: „D50073ce-35b4-4c51-9d2e-4ce66f802c35“, „Status“: „Läuft“ }

6. Verwenden Sie den folgenden URI, um den Status zu überprüfen:

```
https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?includeSubJobsAndTasks=true
```

   Sobald der Job abgeschlossen ist, validieren Sie den Migrationsbericht. Sie können den Bericht aus der Jobantwort als Teil der JobData sehen.

7. Fügen Sie dem vCenter-Server ONTAP-Tools für VMware vSphere Storage Provider hinzu und "Registrieren Sie VASA Provider auf vCenter Server".
8. Stoppen Sie ONTAP Tools für VMware vSphere Storage Provider 9.10/9.11/9.12/9.13 VASA Provider Service von der Wartungskonsole aus.

   Löschen Sie den VASA-Anbieter nicht.

   Sobald der alte VASA-Provider angehalten wurde, erfolgt ein Failover von vCenter Server zu ONTAP-Tools für VMware vSphere. Der Zugriff auf alle Datenspeicher und VMs erfolgt über ONTAP Tools für VMware vSphere.

9. Führen Sie die Patch-Migration mithilfe der folgenden API durch:

HTTP-Methode und Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
PATCH	/API/v1

Verarbeitungsart

Asynchron

Beispiel für Curl

PATCH „/API/v1/vcenters/56d373bd-4163-44f9-a872-9adabb008ca9/Migration-Jobs/84dr73bd-9173-65r7-w345-8ufdbb887d43

JSON-Eingabebeispiel

{ „id“: 123, „Migration_id“: „D50073ce-35b4-4c51-9d2e-4ce66f802c35“, „Status“: „Läuft“ }

JSON-Ausgabebeispiel

Ein Jobobjekt wird zurückgegeben. Sie sollten die Jobkennung speichern, um sie im nächsten Schritt zu verwenden.

{ „id“: 123, „Migration_id“: „D50073ce-35b4-4c51-9d2e-4ce66f802c35“, „Status“: „Läuft“ }

Anforderungskörper ist für Patchvorgang leer.

uuid ist die Migrations-uuid, die in der Antwort der API nach der Migration zurückgegeben wird.

Sobald die API für die Patch-Migration erfolgreich war, entsprechen alle VMs der Storage-Richtlinie.

10. Die delete-API für die Migration ist:

HTTP-Methode	Pfad
Löschen	/API/v1

Verarbeitungsart

Asynchron

Beispiel für Curl

/API/v1/vcenters/{vcguid}/Migration-Jobs/{Migration_id}

Diese API löscht die Migration nach Migrations-ID und löscht die Migration auf dem angegebenen vCenter Server.

Gehen Sie nach der erfolgreichen Migration und nach der Registrierung der ONTAP-Tools 10.1 im vCenter Server wie folgt vor:

- Aktualisieren Sie das Zertifikat auf allen Hosts.
- Warten Sie einige Zeit, bevor Sie Vorgänge in Datenspeicher (DS) und Virtual Machine (VM) ausführen. Die Wartezeit hängt von der Anzahl der Hosts, DS und VMs ab, die im Setup vorhanden sind. Wenn Sie nicht warten, können die Vorgänge zeitweise ausfallen.

Automatisierung mit REST-APIs

Übersicht ÜBER REST-APIs

REST-APIs können zur Ausführung mehrerer ONTAP Tools für Managementvorgänge von VMware vSphere verwendet werden. REST-APIs sind über die Swagger Webseite zugänglich.

Sie können die Swagger-Webseite unter *https://loadbalancerIP:8443/* aufrufen, um die REST-API-Dokumentation anzuzeigen und einen API-Aufruf manuell auszustellen.

> Alle APIs haben Anforderungskörper und Beispiele, die auf der Seite „swagger“ erwähnt werden. Die in diesem Abschnitt aufgeführten Workflows und Beispiele dienen lediglich als Referenz.

Zugriff auf ONTAP Tools für VMware vSphere REST-API

Sie können auf die ONTAP REST API auf unterschiedliche Weise zugreifen.

Netzwerküberlegungen

Sie können über folgende Schnittstellen eine Verbindung zur REST API herstellen:

- Cluster-Management-LIF
- Node Management-LIF
- SVM-Management-LIF

Die von Ihnen ausgewählte LIF sollte zur Unterstützung des HTTPS-Managementprotokolls konfiguriert sein. Außerdem sollte die Firewall-Konfiguration in Ihrem Netzwerk den HTTPS-Datenverkehr zulassen.

> Sie sollten immer eine Cluster-Management-LIF verwenden. Dadurch werden die API-Anforderungen über alle Nodes verteilt und Knoten, die offline sind oder Konnektivitätsprobleme haben, werden vermieden. Wenn Sie mehrere Cluster-Management-LIFs konfiguriert haben, entsprechen diese alle dem Zugriff auf die REST-API.

ONTAP Tools für VMware vSphere API – Online-Dokumentation

Der Zugriff auf Swagger erfolgt über den Hyperlink auf der Support-Seite des Plug-ins „NetApp ONTAP Tools for VMware vSphere“.

Das Format der URL, die zum Zugriff auf die Dokumentationsseite der neuesten Version der API verwendet wird, lautet:

`https://<loadbalancer_ip_address>/docs/API`

Benutzerdefinierte Software und Tools

Auf die ONTAP Tools für die VMware vSphere API können Sie über eine Reihe verschiedener Programmiersprachen und Tools zugreifen. Beliebte Optionen sind Python, Java, Curl und PowerShell. Ein

Programm, Skript oder Tool, das die API verwendet, fungiert als REST-Web-Services-Client. Die Verwendung einer Programmiersprache vermittelt ein tieferes Verständnis der API und bietet die Möglichkeit, ONTAP Tools für die VMware vSphere Administration zu automatisieren.

Das Format der Basis-URL, die für den direkten Zugriff auf die neueste Version der API verwendet wird, lautet:

`https://<loadbalancer_ip_address>/API`

Um auf eine bestimmte API-Version zuzugreifen, in der mehrere Versionen unterstützt werden, lautet das Format der URL:

`https://<loadbalancer_ip_address>/API/v1`

Eingabevariablen, die eine API-Anforderung steuern

Sie können steuern, wie ein API-Aufruf über Parameter und Variablen verarbeitet wird, die in der HTTP-Anforderung festgelegt sind.

HTTP-Methoden

Die folgende Tabelle zeigt die von ONTAP-Tools für die VMware vSphere REST API unterstützten HTTP-Methoden.

Nicht alle HTTP-Methoden sind an jedem REST-Endpunkt verfügbar.

HTTP-Methode	Beschreibung
GET	Ruft Objekteigenschaften auf einer Ressourceninstanz oder -Sammlung ab.
POST	Erstellt eine neue Ressourceninstanz basierend auf der angegebenen Eingabe.
Löschen	Löscht eine vorhandene Ressourceninstanz.
PUT	Ändert eine vorhandene Ressourceninstanz.

Anfragekopfzeilen

Sie sollten mehrere Header in die HTTP-Anfrage aufnehmen.

Inhaltstyp

Wenn der Anforderungsinstanz JSON enthält, sollte dieser Header auf *Application/json* gesetzt werden.

Akzeptieren

Dieser Header sollte auf *Application/json* gesetzt werden.

Autorisierung

Die grundlegende Authentifizierung sollte mit dem Benutzernamen und dem Passwort als base64-String codiert werden.

Text anfordern

Der Inhalt der Anfraentext variiert je nach Anruf. Der HTTP-Request-Text besteht aus einem der folgenden Elemente:

- JSON-Objekt mit Eingabevariablen
- Leer

Objekte filtern

Wenn Sie einen API-Aufruf ausgeben, der GET verwendet, können Sie die zurückgegebenen Objekte anhand eines beliebigen Attributs einschränken oder filtern. Sie können beispielsweise einen genauen Wert angeben, der übereinstimmt:

```
<field>=<query value>
```

Neben einer genauen Übereinstimmung stehen auch andere Operatoren zur Verfügung, um einen Satz von Objekten über einen Wertebereich zurückzugeben. Die ONTAP Tools für DIE REST-API von VMware vSphere unterstützen die in der folgenden Tabelle aufgeführten Filteroperatoren.

Operator	Beschreibung
=	Gleich
<	Kleiner als
>	Größer als
≪=	Kleiner oder gleich
>=	Größer oder gleich
AKTUALISIERUNG	Oder
!	Nicht gleich
*	Gierige Wildcard

Sie können auch eine Sammlung von Objekten zurückgeben, basierend darauf, ob ein bestimmtes Feld gesetzt wird oder nicht, indem Sie das Schlüsselwort **Null** oder dessen Negation **!null** als Teil der Abfrage verwenden.

Nicht festgelegte Felder werden in der Regel von übereinstimmenden Abfragen ausgeschlossen.

Es werden bestimmte Objektfelder angefordert

Standardmäßig gibt die Ausgabe eines API-Aufrufs mithilfe VON GET nur die Attribute zurück, die das Objekt oder die Objekte eindeutig identifizieren. Dieser minimale Feldsatz dient als Schlüssel für jedes Objekt und variiert je nach Objekttyp. Sie können mithilfe des Abfrageparameters weitere Objekteigenschaften wie folgt auswählen `fields` :

Allgemeine oder Standardfelder

Geben Sie **Fields=*** an, um die am häufigsten verwendeten Objektfelder abzurufen. Diese Felder werden normalerweise im lokalen Serverspeicher verwaltet oder erfordern nur wenig Verarbeitung für den Zugriff. Dies

sind die gleichen Eigenschaften, die für ein Objekt zurückgegeben werden, nachdem GET mit einem URL-Pfadschlüssel (UUID) verwendet wurde.

Alle Felder

Geben Sie **fields=**** an, um alle Objektfelder abzurufen, einschließlich derer, die für den Zugriff auf zusätzliche Serververarbeitung erforderlich sind.

Benutzerdefinierte Feldauswahl

Geben Sie mit **fields=<field_Name>** das genaue Feld ein. Wenn Sie mehrere Felder anfordern, sollten die Werte durch Kommas ohne Leerzeichen getrennt werden.

> Als Best Practice sollten Sie immer die gewünschten Felder identifizieren. Sie sollten nur die gemeinsamen Felder oder alle Felder abrufen, wenn Sie dies benötigen. Welche Felder sind als „Common“ klassifiziert und mit *fields=** zurückgegeben werden, wird durch NetApp aufgrund der internen Performance-Analyse bestimmt. Die Klassifizierung eines Felds kann sich in zukünftigen Releases ändern.

Sortieren von Objekten im Ausgabungsset

Die Datensätze in einer Ressourcensammlung werden in der vom Objekt definierten Standardreihenfolge zurückgegeben. Sie können die Reihenfolge mit dem Abfrageparameter mit dem Feldnamen und der Sortierrichtung wie folgt ändern `order_by` :

```
order_by=<field name> asc|desc
```

Sie können beispielsweise das Typfeld in absteigender Reihenfolge, gefolgt von id in aufsteigender Reihenfolge sortieren:

```
order_by=type desc, id asc
```

- Wenn Sie ein Sortierfeld angeben, aber keine Richtung angeben, werden die Werte in aufsteigender Reihenfolge sortiert.
- Wenn Sie mehrere Parameter eingeben, sollten Sie die Felder durch ein Komma trennen.

Paginierung beim Abrufen von Objekten in einer Sammlung

Wenn Sie einen API-Aufruf über GET für den Zugriff auf eine Sammlung von Objekten desselben Typs ausgeben, versucht ONTAP Tools für VMware vSphere anhand von zwei Einschränkungen so viele Objekte wie möglich zurückzugeben. Mit zusätzlichen Abfrageparametern auf der Anforderung können Sie jede dieser Einschränkungen steuern. Die erste Bedingung, die für eine bestimmte GET-Anforderung erreicht wurde, beendet die Anforderung und begrenzt damit die Anzahl der zurückgegebenen Datensätze.

> Wenn eine Anfrage endet, bevor sie alle Objekte anführt, enthält die Antwort den Link, der zum Abrufen des nächsten Stapels von Datensätzen benötigt wird.

Die Anzahl der Objekte wird begrenzt

Standardmäßig gibt ONTAP-Tools für VMware vSphere maximal 10,000 Objekte für eine GET-Anforderung zurück. Sie können diese Grenze mit dem Abfrageparameter *max_Records* ändern. Beispiel:

```
max_records=20
```

Die Anzahl der zurückgegebenen Objekte kann unter dem maximal wirkenden Wert liegen, basierend auf der zugehörigen Zeitbeschränkung sowie der Gesamtanzahl der Objekte im System.

Begrenzung der Zeit, die zum Abrufen der Objekte verwendet wird

Standardmäßig gibt ONTAP-Tools für VMware vSphere so viele Objekte wie möglich innerhalb der für die GET-Anforderung zulässigen Zeit zurück. Die Standard-Zeitüberschreitung beträgt 15 Sekunden. Sie können diese Grenze mit dem Abfrageparameter *return_timeout* ändern. Beispiel:

```
return_timeout=5
```

Die Anzahl der zurückgegebenen Objekte kann aufgrund der zugehörigen Einschränkung für die Anzahl der Objekte sowie der Gesamtanzahl der Objekte im System geringer sein als die maximal wirkende Anzahl.

Verengung des Ergebnisset

Bei Bedarf können Sie diese beiden Parameter mit zusätzlichen Abfrageparametern kombinieren, um den Ergebnissatz einzugrenzen. Im Folgenden werden z. B. bis zu 10 EMS-Ereignisse zurückgegeben, die nach der angegebenen Zeit generiert wurden:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

Sie können mehrere Anfragen zur Seite durch die Objekte ausgeben. Jeder nachfolgende API-Aufruf sollte einen neuen Zeitwert verwenden, der auf dem letzten Ereignis des letzten Ergebnisset basiert.

Größeneigenschaften

Die bei einigen API-Aufrufen verwendeten Eingabewerte sowie bestimmte Abfrageparameter sind numerisch. Anstatt eine ganze Zahl in Byte bereitzustellen, können Sie optional ein Suffix wie in der folgenden Tabelle aufgeführt verwenden.

Suffix	Beschreibung
KB	KB-Kilobyte (1024 Byte) oder Kibibyte
MB	MB Megabyte (KB x 1024 Byte) oder Mebibyte
GB	GB Gigabyte (MB x 1024 Byte) oder Gibibyte
TB	TB Terabyte (GB x 1024 byes) oder Tebibyte
PB	PB (TB x 1024 byes) oder Pebibyte

Zugriff auf die Referenzdokumentation zu ONTAP Tools für die VMware vSphere API über die Swagger-Benutzeroberfläche

Sie können über die Swagger-Benutzeroberfläche Ihres lokalen ONTAP-Systems auf die ONTAP-REST-API-Dokumentation zugreifen.

Bevor Sie beginnen

Sie sollten Folgendes haben:

- IP-Adresse oder Host-Name der ONTAP Cluster-Management-LIF
- Benutzername und Passwort für ein Konto, das über eine Berechtigung zum Zugriff auf die ONTAP-REST-API VERFÜGT

Schritte

1. Geben Sie die URL in Ihren Browser ein und drücken Sie **Enter**: *https://<ip_address>/docs/API*
2. Melden Sie sich mit dem ONTAP-Konto an

   Die Dokumentationsseite für die ONTAP-API wird angezeigt, auf der die API-Aufrufe unten in den Hauptressourcenkategorien organisiert sind.

3. Scrollen Sie als Beispiel für einen einzelnen API-Aufruf in die Kategorie **Cluster** und klicken Sie auf **GET /Cluster**.

Legen Sie los mit DER REST API

Sie können schnell damit beginnen, die ONTAP Tools für VMware vSphere REST API zu verwenden. Der Zugriff auf die API bietet eine gewisse Perspektive, bevor Sie mit den komplexeren Workflow-Prozessen bei Live-Einrichtung beginnen.

Hallo Welt

Sie können einen einfachen Befehl auf Ihrem System ausführen, um zu beginnen, die ONTAP-Tools für die REST-API von VMware vSphere zu verwenden und die Verfügbarkeit zu bestätigen.

Bevor Sie beginnen

- Stellen Sie sicher, dass das Curl-Dienstprogramm auf Ihrem System verfügbar ist.
- IP-Adresse oder Hostname der ONTAP-Tools für VMware vSphere Server
- Benutzername und Passwort für ein Konto mit Zugriffsberechtigung auf ONTAP Tools für VMware vSphere REST API.

> Wenn Ihre Anmeldeinformationen Sonderzeichen enthalten, müssen Sie diese auf der Grundlage der verwendeten Shell so formatieren, dass sie für Curl akzeptabel sind. Sie können beispielsweise vor jedem Sonderzeichen einen umgekehrten Schrägstrich einfügen oder die gesamte Zeichenfolge in einfache Anführungszeichen umbrechen `username:password` .

Schritt

Führen Sie bei der Befehlszeilenschnittstelle Folgendes aus, um die Plug-in-Informationen abzurufen:

```
curl -X GET -u username:password -k
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

Beispiel:

```
curl -X GET -u admin:password -k
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

Workflows

Speichererkennung

Das Erkennungsintervall kann als Teil der Konfigurationskarte konfiguriert werden. Die geplante Erkennung läuft alle 60 Minuten. Die hier angegebene API dient zum Ausführen der Ermittlung nach Bedarf für ein bestimmtes Speicher-Back-End, das dem lokalen Umfang hinzugefügt wird.

Verwenden Sie die folgende API, um die Erkennung auszuführen:

```
POST
/virtualization/api/v1/vcenters/{vcguid}/storage-backends/{id}/discovery-
jobs
```

Erfahren Sie im integrierten Storage-Backend-Workflow (SVM oder Cluster) und erhalten Sie ID aus der Antwort der Post-Storage-Back-End-API.

Die Erkennung über diesen API-Endpunkt wird nur für Storage-Back-Ends mit lokalem Umfang und nicht für Storage-Back-Ends mit globalem Umfang unterstützt. Wenn der Speicher-Backend-Typ Cluster ist, wird die Ermittlung implizit für die untergeordneten SVMs ausgeführt. Wenn der Storage-Back-End-Typ SVM ist, wird die Erkennung nur für die ausgewählte SVM ausgeführt.

Beispiel:

So führen Sie die Ermittlung auf einem durch ID angegebenen Speicher-Back-End aus

```
POST
/api/v1/vcenters/3fa85f64-5717-4562-b3fc-2c963f66afa6/storage-
backends/74e85f64-5717-4562-b3fc-2c963f669dde/discovery-jobs
```

Sie müssen x-auth für die API übergeben. Sie können diese X-Auth aus der neuen API generieren, die unter Auth in Swagger hinzugefügt wurde.

```
/virtualization/api/v1/auth/vcenter-login
```

Anforderungen für die SVM-Aggregatzuordnung

Um SVM-Benutzeranmeldeinformationen für die Bereitstellung von Datastores zu verwenden, erstellt ONTAP Tools für VMware vSphere Volumes im Aggregat, DAS in der POST-API für Datastores angegeben ist. In ONTAP ist es nicht möglich, Volumes auf Aggregaten ohne Zuordnung auf einer SVM mithilfe der SVM-Benutzeranmeldedaten zu erstellen. Zur Lösung dieses Problems ordnen Sie die SVMs wie hier beschrieben mit den Aggregaten zu. Verwenden Sie dazu die ONTAP REST-API oder CLI.

ONTAP-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
```

Onboard Storage Back-End (SVM oder Cluster) mit einer vCenter Server-Instanz

Verwenden Sie die folgende API, um die Storage-Back-Ends zu integrieren und die SVM lokal vCenter zuzuordnen. "Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen"Informationen zum Benutzer-Privileges für ONTAP SVM finden Sie im Abschnitt.

```
POST /virtualization/api/v1/vcenters/<vcguid>/storage-backends

{
     "hostname_or_ip": "172.21.103.107",
     "username": "svm11",
     "password": "xxxxxx"
   }
```

Die ID aus der obigen API-Antwort wird bei der Erkennung verwendet.

Sie müssen x-auth für die API übergeben. Sie können diese X-Auth aus der neuen API generieren, die unter Auth in Swagger hinzugefügt wurde.

```
/virtualization/api/v1/auth/vcenter-login
```

Erstellung eines VVols Datastore

Sie können einen VVols-Datastore mit neuen Volumes oder mit vorhandenen Volumes erstellen. Zudem ist es möglich, einen VVols-Datastore mit einer Kombination aus vorhandenen Volumes und neuen Volumes zu erstellen.

Überprüfen Sie, ob die Root-Aggregate nicht der SVM zugeordnet sind.

Generieren Sie ein JWT-Token, bevor Sie Datastores erstellen, oder erhöhen Sie den Ablauf des SAML-Tokens, indem Sie „Maximum Bearer Token Lifetime“ auf 60 m in vCenter festlegen.

Sie müssen x-auth für die API übergeben. Sie können diese X-Auth aus der neuen API generieren, die unter Auth in Swagger hinzugefügt wurde.

/Virtualization/API/v1/auth/vcenter-Login

1. Erstellung eines VVols-Datastore mit neuem Volume

Abrufen der Aggregat-id, Storage_id(SVM-UUID) mit der ONTAP REST-API POST /Virtualization/API/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-691250bfe2df/vvols/Datastores

Verwenden Sie den folgenden URI, um den Status zu überprüfen:

+

```
`\https://xx.xx.xx.xxx:8443/virtualization/api/jobmanager/v2/jobs/<JobID>?
includeSubJobsAndTasks=true`
```

+ Request Body für NFS Datastore

{ „Name“:„nfsds1“, „Protokoll“:„nfs“, „Platform_type“:„AFF“, „Moref“:„Domain-c8“, „Volumes{“:[{ „is_existing }“:false } }, „Name“:{„vol_nfs_pvt“, „size_in_mb“:2048000 200, „space_efficiency“:„Thin“, „Aggregate“,{ c677-460a_3827 5000 iops-9273 } }

Anfragekörper für iSCSI Datenspeicher: { "Name" : "iscsi_Custom", "Protocol" : "iscsi", "Platform_type": "AFF", "moref" : "Domain-c8", "Volumes {" : [{ "is_existing } }" : false, "Name {" : "iscsi_Custom 1960", "size_in_mb 9506" : 8034, "space_efficiency" : "Thin", "Aggregate } }" VVols-Datastore mit vorhandenen Volumes erstellen

Erhalten Sie „Aggregate_id“ und „Volume_id“ mit der ONTAP-REST-API.

```
 POST /virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores
Text Anfordern
```

```
 {
"name" : "nfsds2",
"protocol" : "nfs",
"platform_type": "aff",
"moref" : "domain-c8",
"volumes" : [
    {
          "is_existing": true,
          "id": "e632a632-1412-11ee-8a8c-00a09860a3ff"
        }
],
"storage_backend": {
                     "storage_id": "33a8b6b3-10cd-11ee-8a8c-00a09860a3ff"
}
```

}

Mounten und unmounten Sie einen VVols Datastore

Sie können einen VMware Virtual Volumes (VVols)-Datastore auf einen oder mehrere zusätzliche Hosts mounten, um zusätzlichen Hosts den Storage-Zugriff zu ermöglichen. Sie können VVols-Datastore mithilfe von APIs abmounten.

Verwenden Sie die folgende API, um einen VVols Datastore zu mounten oder abzuhängen. Sie müssen x-auth für die API übergeben. Sie können diese X-Auth aus der neuen API generieren, die unter Auth in Swagger hinzugefügt wurde.

```
/virtualization/api/v1/auth/vcenter-login
```

```
PATCH
/virtualization/api/v1/vcenters/{vcguid}/vvols/datastores/{moref}/hosts
```

Erhalten Sie den vVol Datastore moref von vCenter.

Text Anfordern

```
{
  "operation": "mount",
  "morefs": [
    "host-7044"
  ],
}
```

Beispiele: * Montage auf zusätzlichem Host

Verwenden Sie die folgende API, um auf zusätzlichen Host zu mounten:

```
/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/hosts

     Request Body
     {
      "operation": "mount",
      "morefs": ["host-13"],
     }
```

- Unmounten auf zusätzlichem Host

Verwenden Sie die folgende API, um die Bereitstellung auf einem zusätzlichen Host aufzuheben:

```
/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/hosts

     Request Body
     {
      "operation": "unmount",
      "morefs": ["host-13"],
     }
```

Erweitern oder verkleinern Sie Storage von vVol Datastore

Es gibt APIs zum Erhöhen oder verringern des verfügbaren Speichers.

Schritte

Erweitern oder verkleinern Sie den VVols Datastore mit der folgenden API:

```
PATCH
/virtualization/api/v1/vcenters/{vcguid}/vvols/datastores/{moref}/volumes
```

Beispiele

- VVols Datastore zum Hinzufügen eines neuen Volumes ändern

```
  PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/volumes

    Request Body
   {
    "operation": "grow",
    "volumes": [{
        "is_existing": false,
        "name": "exp3",
        "size_in_mb": 51200,
        "space_efficiency": "thin",
        "aggregate": {
            "id": "1466e4bf-c6d6-411a-91d5-c4f56210e1ab"
        },
        "storage_backend": {
            "storage_id": "13d86e4f-1fb1-11ee-9509-005056a75778"
        },
        "qos": {
            "max_iops": 5000
        }
    }]
}
```

- VVols Datastore zum Hinzufügen eines vorhandenen Volumes ändern

```
  PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/volumes

    Request Body
    {
      "operation": "grow",
      "volumes": [{
        "is_existing": true,
        "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
      }]
    }
```

- Ändern Sie den VVols-Datastore zur Entfernung von Volumes und löschen Sie das Volume aus dem Storage

```
  PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/volumes?delete_volumes=true

    Request Body
    {
      "operation": "shrink",
      "volumes": [{
        "is_existing": true,
        "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
      }]
    }
```

- VVols Datastore für die Entfernung von Volumes ändern und Volume nicht aus dem Storage löschen

```
  PATCH virtualization/api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-24/volumes?delete_volumes=false

    Request Body
    {
      "operation": "shrink",
      "volumes": [{
        "is_existing": true,
        "id": "vfded9ad-6bsd-4c9e-b44g-691250bfe2sd"
      }]
    }
```

VVols Datastore löschen

Ein VVols-Datastore existiert, solange mindestens ein FlexVol-Volume auf dem Datastore verfügbar ist. Wenn Sie einen VVols-Datastore in einem HA-Cluster löschen möchten, müssen Sie den Datastore zunächst von allen Hosts im HA-Cluster abmounten und anschließend den Ordner *.vsphere-HA* manuell über die vCenter-Server-Benutzeroberfläche löschen.

Schritte

Löschen Sie den VVols Datastore über die folgende API.

```
DELETE
/virtualization/api/v1/vcenters/{vcguid}/vvols/datastores/{moref}
```

Beispiele

- VVols Datastore löschen und Volumes aus dem Storage löschen

```
  DELETE /api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-28?delete_volumes=true
```

Durch Löschen des VVols Datastore Workflows werden Datastore-Volumes gelöscht, wenn Sie die Markierung delete_Volume als wahr übergeben haben, unabhängig davon, ob das Datastore-Volume gemanagt oder nicht gemanagt wird.

- Löschen Sie den VVols-Datastore und löschen Sie keine Volumes aus dem Storage

```
  DELETE /api/v1/vcenters/cdded9ad-6bsd-4c9e-b44g-
691250bfe2df/vvols/datastores/datastore-28?delete_volumes=false
```

Antwort:

```
{

    "id": "1889"

}
```

Speicherschwellenwert verwalten

Verwenden Sie die folgende get Threshold API, um die konfigurierten Storage-Grenzwerte für Volume und Aggregat abzurufen.

```
GET/virtualization/api/v1/vcenters/{vcguid}/storage-thresholds
```

Beispiele: Rufen Sie die Storage-Schwellenwerte pro vCenter Server-Instanz von vCenter GUID ab

```
GET "/api/v1/vcenters/beded9ad-6bbb-4c9e-b4c6-691250bfe2da/storage-
thresholds"
```

Verwenden Sie den folgenden PATCH-Konfigurationsalarm für Lautstärke und Aggregat, um eine Benachrichtigung zu generieren, wenn konfigurierte Grenzwerte erreicht werden.

```
PATCH/virtualization/api/v1/vcenters/{vcguid}/storage-thresholds
```

Beispiele: Aktualisieren Sie die Storage Thresholds per vCenter by vCenter GUID. Die Standardgrenzwerte sind 80 % für nahezu voll und 90 % für voll. Ändern aller Schwellenwerteinstellungen

```
{{{}PATCH "/api/v1/vcenters/beded9ad-6bbb-4c9e-b4c6-691250bfe2da/storage-
thresholds"
Request Body
{
"volume":

{ "nearly_full_percent": 80, "full_percent": 90 }
,
"aggregate": {
"nearly_full_percent": 80,
"full_percent": 90
}
}{}}}{}
```

Managen des Netzwerkzugriffs

Verwenden Sie die folgende API, um IP-Adressen für die Whitelisting hinzuzufügen:

```
patch /api/v1/vcenters/{vcguid}/settings/ip-whitelist

{
    value: string
}

GET /api/v1/vcenters/{vcguid}/settings/ip-whitelist

{
    value: string
}
```

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweis zu ONTAP-Tools für VMware vSphere 10.1"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.