Konzepte

ONTAP tools for VMware vSphere 10

NetApp
February 11, 2026

Inhalt

Konzepte

Erfahren Sie mehr über ONTAP tools

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

ONTAP tools for VMware vSphere unterstützen:

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

Hohe Verfügbarkeit für ONTAP -Tools für VMware

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

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

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

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

ONTAP tools for VMware vSphere unterstützen vCenter HA nicht.

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

Schlüsselkonzepte und Begriffe in ONTAP tools

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

Zertifizierungsstelle (CA)

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

Konsistenzgruppe

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

Dual-Stack

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

Hochverfügbarkeit

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

Logical Unit Number (LUN)

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

NVMe-Namespace und -Subsystem

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

ONTAP Tools Manager

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

Offene virtuelle Appliance (OVA)

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

Recovery-Zeitpunkt (RPO)

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

SnapMirror Active Sync

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

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

Storage-Back-Ends

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

Globaler Cluster (Storage Back-End)

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

Lokales Storage-Back-End

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

Storage Replication Adapter (SRA)

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

Storage Virtual Machine (SVM)

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

Einheitliche und uneinheitliche Konfiguration

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

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

Virtual Machine File System (VMFS)

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

Virtuelle Volumes (VVols)

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

VM-Storage-Richtlinie

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

VMware Live Site Recovery

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

VMware vSphere APIs für Storage Awareness (VASA)

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

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

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

VSphere Metro Storage-Cluster

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

VVols Datastore

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

Kein RPO

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

Rollenbasierte Zugriffskontrolle (RBAC)

Erfahren Sie mehr über ONTAP tools RBAC

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

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

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

RBAC-Komponenten

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

Berechtigungen

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

Rollen

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

Objekte

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

Benutzer und Gruppen

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

Berechtigungen

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

Zwei RBAC-Umgebungen

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

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

VMware vCenter Server

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

ONTAP-Cluster

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

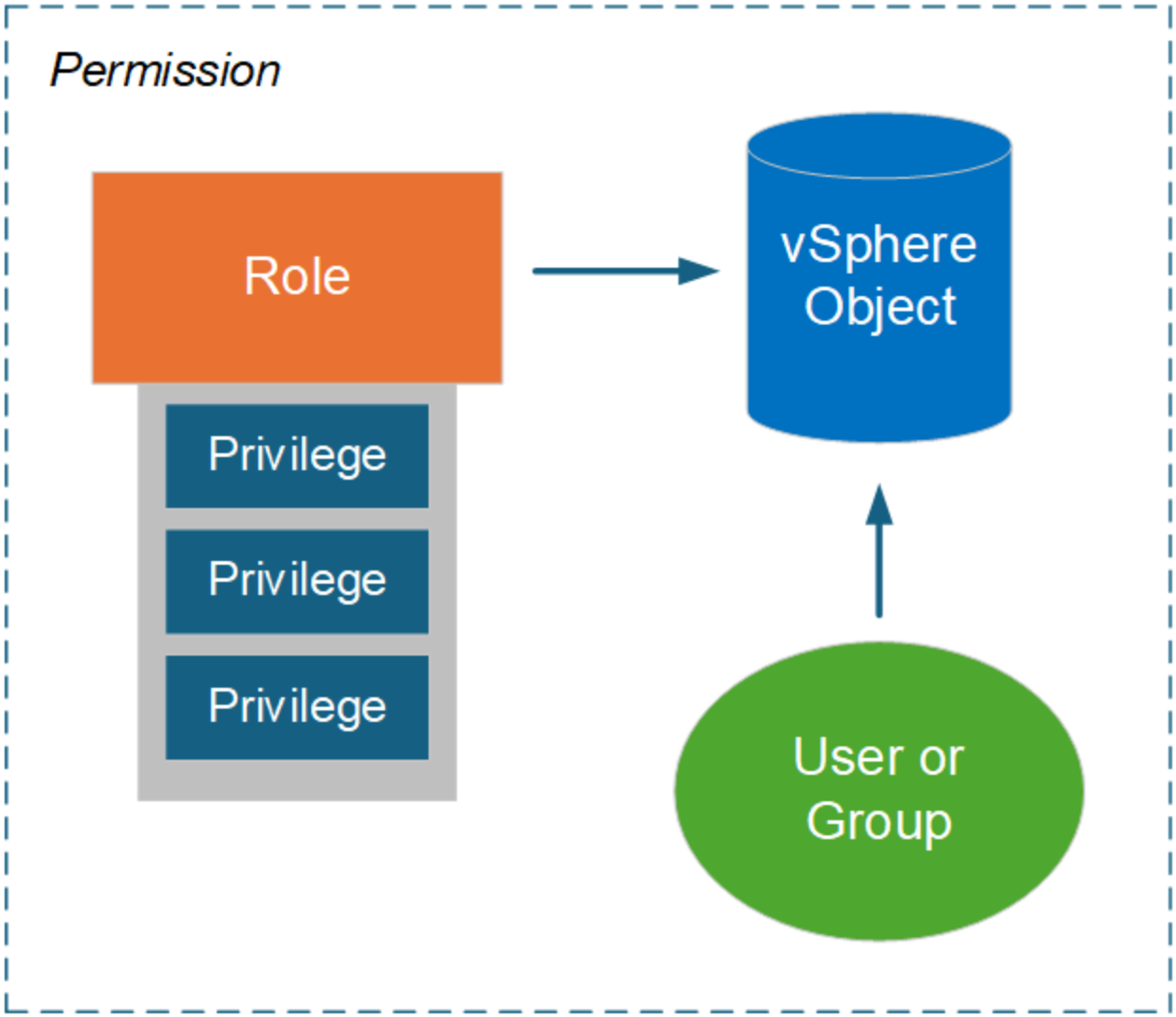
RBAC mit VMware vSphere

Wie vCenter Server-RBAC mit ONTAP tools funktioniert

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

Abbildung einer vCenter Server-Berechtigung

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



Komponenten einer vCenter Server-Berechtigung

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

VSphere Objekte

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

Privileges und Rollen

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

- Native vCenter Server-Berechtigungen

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

- Spezifische Berechtigungen für ONTAP-Tools

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

Benutzer und Gruppen

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

vCenter Server-RBAC-Überlegungen für ONTAP tools

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

VCenter-Rollen und das Administratorkonto

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

VSphere Objekthierarchie

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

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

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

In ONTAP Tools für VMware vSphere 10 enthaltene Rollen

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

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

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

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

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

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

Es gibt drei vordefinierte Rollen, die unten beschrieben werden.

NetApp ONTAP-Tools für VMware vSphere Administrator

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

NetApp ONTAP-Tools für VMware vSphere schreibgeschützt

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

NetApp ONTAP Tools für VMware vSphere Bereitstellung

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

- Erstellen neuer Datenspeicher
- Managen von Datastores

VSphere Objekte und ONTAP Storage Back-Ends

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

Arbeiten mit vCenter Server RBAC

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

Erforderliche Berechtigungen

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

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

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

Berechtigungen werden zugewiesen

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

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

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

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

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

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

RBAC mit ONTAP

Wie ONTAP RBAC mit ONTAP tools funktioniert

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

Überblick über die administrativen Optionen

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

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

Rollen- und Privileges-Typen

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

- RUHE

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

- Traditionell

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

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

Objekte genauer definieren, auf die sie angewendet werden.

Umfang

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

Rollendefinitionen

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

Arbeiten mit ONTAP-REST-Rollen

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

Rollenzuordnung

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

Definieren einer REST-Rolle mithilfe von CLI-Privileges

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

Administratorschnittstelle beim Definieren von ONTAP-Rollen

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

ONTAP RBAC-Überlegungen für ONTAP tools

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

Überblick über den Konfigurationsprozess

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

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

1. Vorbereiten

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

ONTAP Cluster verfügen.

2. Laden Sie die JSON-Definitionsdatei herunter

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

3. Erstellen Sie einen ONTAP-Benutzer mit einer Rolle

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

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

4. Konfigurieren Sie die Rolle

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

Konfigurieren Sie die Rolle mit System Manager

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

Konfiguration von Kernbenutzern und -Rollen

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

Berechtigungen

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

- Ermitteln

  Diese Rolle ermöglicht es Ihnen, Storage-Systeme hinzuzufügen.

- Storage erstellen

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

- Speicher ändern

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

- Zerstören Sie den Speicher

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

Benutzer mit einer Rolle generieren

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

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

Beispiel

```
OTV_10_VSC_Discovery_Create
```

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