



Konzepte

ONTAP tools for VMware vSphere 10

NetApp

November 17, 2025

This PDF was generated from <https://docs.netapp.com/de-de/ontap-tools-vmware-vsphere-103/concepts/ontap-tools-overview.html> on November 17, 2025. Always check docs.netapp.com for the latest.

Inhalt

Konzepte	1
Überblick über die ONTAP Tools für VMware vSphere	1
Schlüsselkonzepte und -Begriffe	1
Rollenbasierte Zugriffssteuerung	4
Erfahren Sie mehr über ONTAP Tools für die rollenbasierte Zugriffssteuerung von VMware vSphere	
10	4
RBAC mit VMware vSphere	5
RBAC mit ONTAP	9
Hochverfügbarkeit für ONTAP Tools für VMware vSphere	12
AutoSupport	13
Benutzeroberfläche von ONTAP Tools Manager	13

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.

Die ONTAP Tools für VMware vSphere sind eine Sammlung horizontal skalierbarer, ereignisgesteuerter Microservices, die als Open Virtual 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)
- SnapMirror aktiv/synchron (SMAS)

Schlüsselkonzepte und -Begriffe

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

ASA r2-Systeme

Die neuen NetApp ASA r2 Systeme bieten eine einheitliche Hardware- und Softwarelösung, mit der eine vereinfachte Benutzererfahrung speziell für die Anforderungen von reinen SAN-Kunden erzielt wird. ["Erfahren Sie mehr über ASA r2 Storage-Systeme".](#)

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 gemanagt werden. In ONTAP sorgen Konsistenzgruppen für ein einfaches Management und eine Garantie für die Sicherung eines Applikations-Workloads, der sich über mehrere Volumes erstreckt. Erfahren Sie mehr über ["Konsistenzgruppe"](#).

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, sodass 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 Backends. ONTAP Tools Manager unterstützt Sie beim Management von vCenter Server-Instanzen, Speicher-Back-Ends, Zertifikaten, Passwörtern und Download 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 ist ein Maß für die Häufigkeit von Daten-Backups bzw. -Replikation. Er gibt den Zeitpunkt an, zu dem Daten nach einem Ausfall wiederhergestellt werden 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 aktiv/synchron (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. Lear 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. Über das Storage-Backend kann der ESXi Host auf persistente Daten zugreifen und diese managen. Die erforderliche Storage-Kapazität und Performance für virtualisierte Umgebungen wird bereitgestellt.

Storage Replication Adapter (SRA)

SRA ist die spezifische Storage-Software eines Anbieters, die innerhalb der VMware Live Site Recovery 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.

Einheitliche und uneinheitliche Konfiguration

- **Einheitlicher Hostzugriff** bedeutet, dass Hosts von beiden Standorten mit allen Pfaden zu Speicherclustern an beiden Standorten verbunden sind. Standortübergreifende Wege sind über die Distanz gestreckt.
- **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.

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 Live Site Recovery

VMware Live Site Recovery 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.

VSphere Metro Storage-Cluster

VSphere Metro Storage Cluster (vMSC) ist eine Technologie, 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 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

Erfahren Sie mehr über ONTAP Tools für die rollenbasierte Zugriffssteuerung von VMware vSphere 10

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 *Privilege* ist eine Aktion oder Fähigkeit, die erlaubt oder verweigert werden kann. Es könnte etwas einfaches sein, wie die Fähigkeit, eine Datei zu lesen, oder es könnte eine abstraktere Operation spezifisch für ein bestimmtes Softwaresystem sein. Privileges kann auch definiert werden, um den Zugriff auf REST-API-Endpunkte und CLI-Befehle einzuschränken. Jede RBAC-Implementierung umfasst vordefinierte Privileges und kann Administratoren auch die Erstellung benutzerdefinierter Privileges ermöglichen.

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

Beim Einsatz von ONTAP Tools für VMware vSphere 10 müssen Sie zwei unterschiedliche RBAC-Umgebungen berücksichtigen.

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

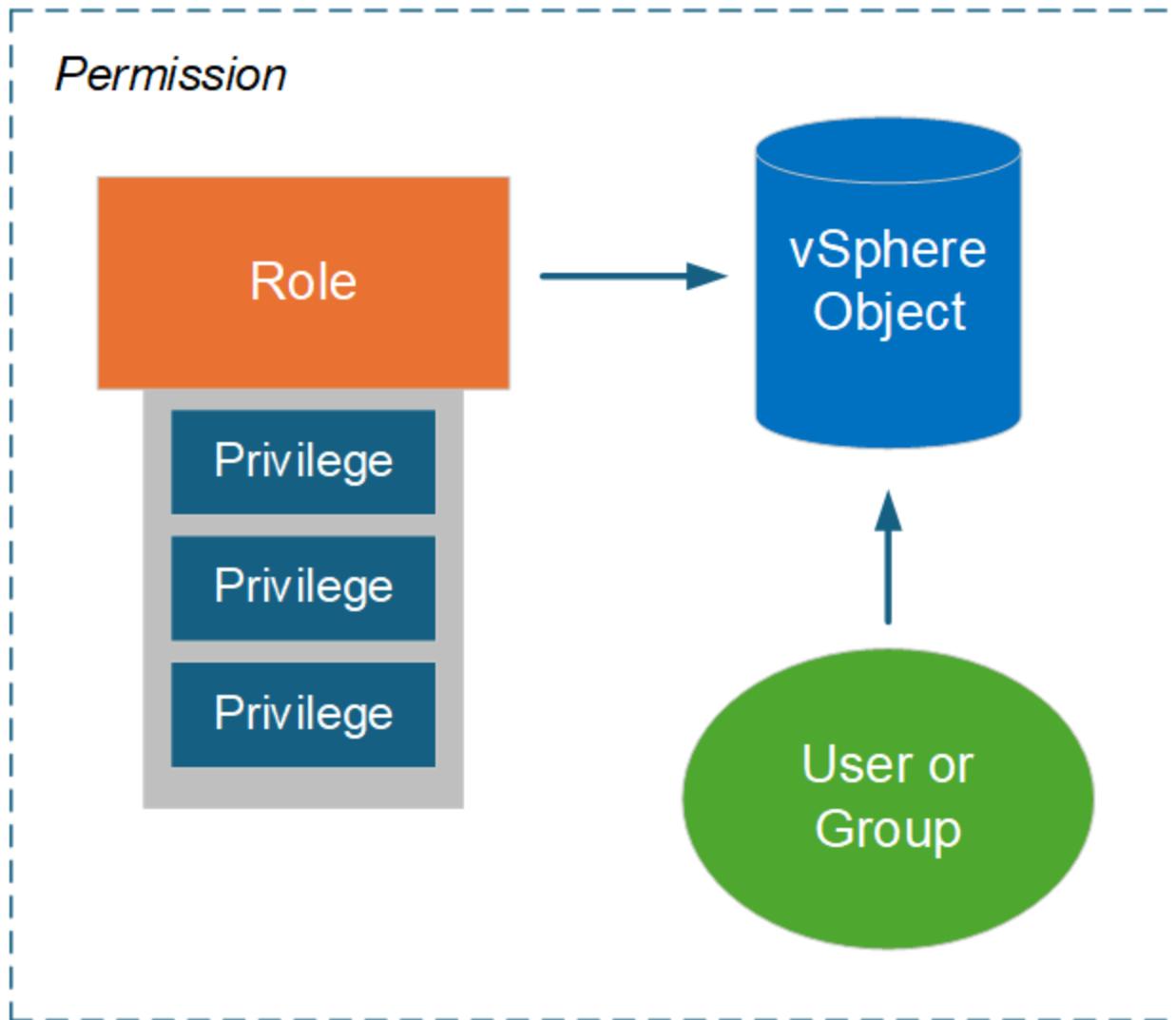
RBAC-Umgebung für vCenter Server mit ONTAP Tools für VMware vSphere 10

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 mithilfe von Active Directory oder der lokalen 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 auf Basis der Privileges in der zugehörigen Rolle. Beachten Sie, dass Rollen nicht isoliert direkt Benutzern zugewiesen werden. Stattdessen erhalten Benutzer und Gruppen über die Rolle Privileges als Teil der größeren vCenter Server-Berechtigung Zugriff auf ein Objekt.

Nutzen Sie die RBAC für vCenter Server mit ONTAP Tools für VMware vSphere 10

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 für VMware vSphere-Rollen anzuzeigen, wählen Sie oben im vSphere-Client **Menü** aus und klicken Sie auf **Administration** und dann auf **Rollen** auf der linken Seite. Es gibt drei vordefinierte Rollen, wie unten beschrieben.

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 restiktiveren 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

ONTAP RBAC-Umgebung mit ONTAP Tools für VMware vSphere 10

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](#)".



RBAC von ONTAP ist auf eine Storage-Umgebung zugeschnitten und ist einfacher als die RBAC-Implementierung, die über vCenter Server zur Verfügung steht. Mit ONTAP weisen Sie dem Benutzer direkt eine Rolle zu. Die Konfiguration expliziter Berechtigungen, wie sie beispielsweise mit vCenter Server verwendet werden, ist für die 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"](#)" .

Nutzen Sie die rollenbasierte Zugriffssteuerung von ONTAP mit ONTAP-Tools für VMware vSphere 10

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

Die ONTAP Tools für VMware vSphere 10 unterstützen das Erstellen eines ONTAP-Benutzers mit einer benutzerdefinierten Rolle. Die Definitionen sind in eine JSON-Datei verpackt, die Sie in das 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 unter [Konfigurieren 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.

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



Nur Ausfall eines einzelnen Nodes wird 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.

Um die HA-Funktion zu aktivieren, sollten der Hot Plug für CPU und Arbeitsspeicher während der Implementierung oder später in den ONTAP Tools für VMware vSphere VM-Einstellungen aktiviert werden.

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 über die Wartungskonsolenoption **Anwendungskonfiguration > AutoSupport deaktivieren** 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. Sie müssen die Proxy-url über die Wartungskonsole der ersten VM bereitstellen. Verwenden Sie die Option **Anwendungskonfiguration > AutoSupport-Proxy-URL aktualisieren**, um die Proxy-URL einzugeben.

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 von VASA Provider und ONTAP Tools.
- Passwortverwaltung - Zurücksetzen des OVA-Anwendungskennworts des Benutzers.

Um auf den ONTAP Tools Manager zuzugreifen, starten Sie

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

Im Abschnitt mit der Übersicht über den ONTAP Tools Manager wird die Appliance-Konfiguration gemanagt, z. B. Services-Management, Upscaling der Node-Größe und Unterstützung für Hochverfügbarkeit. Sie können auch die allgemeinen Informationen von ONTAP-Tools zu den Knoten überwachen, wie z. B. Systemzustand,

Netzwerkdetails und Warnmeldungen.

The screenshot shows the ONTAP tools Manager interface with the following details:

- Appliance Status:** Healthy
- Alerts:** Last 24 hours
 - Error: 3
 - Warning: 2
 - Info: 5
- ONTAP tools nodes:**
 - nodename_01: Online, demo_vm1
 - nodename_02: Online, demo_vm2
 - nodename_03: Online, demo_vm3

Karte	Beschreibung
Gerätekarte	Die Appliance-Karte zeigt den Gesamtstatus der ONTAP Tools Appliance an. Es zeigt die Details der Appliance-Konfiguration und den Status der aktivierten Dienste an. Weitere Informationen zur ONTAP Tools Appliance erhalten Sie über den Link Details anzeigen . Wenn ein Aktionsjob zum Bearbeiten der Appliance-Einstellungen ausgeführt wird, werden im Portlet der Appliance der Status und die Details des Jobs angezeigt.
Warnkarte	Auf der Warnkarte werden die Warnmeldungen der ONTAP-Tools nach Typ aufgeführt, einschließlich der Warnmeldungen auf HA-Node-Ebene. Sie können die Liste der Warnmeldungen anzeigen, indem Sie auf den Zähltextr (Hyperlink) klicken. Über den Link gelangen Sie zur Seite mit der Warn-Ansicht, die nach dem ausgewählten Typ gefiltert ist.
Karte der ONTAP-Tools-Knoten	Die Knotenkarte „ONTAP Tools“ zeigt die Liste der Knoten mit Knotennamen, Node-VM-Namen, Status und allen netzwerkbezogenen Daten an. Sie können auf Details anzeigen auswählen, um die zusätzlichen Details zu dem ausgewählten Knoten anzuzeigen. [HINWEIS] in einem nicht-HA-Setup wird nur ein Node angezeigt. Im HA-Setup werden drei Nodes angezeigt.

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 BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 VERTRÄGLICH 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.