



Rollenbasierte Zugriffssteuerung

ONTAP tools for VMware vSphere 9.12

NetApp
December 19, 2023

Inhalt

- Rollenbasierte Zugriffssteuerung 1
 - Übersicht über die rollenbasierte Zugriffssteuerung in den ONTAP Tools 1
 - Komponenten von vCenter Server-Berechtigungen 1
 - Kernpunkte zum Zuweisen und Ändern von Berechtigungen für vCenter Server 3
 - Standardrollen in Paket mit ONTAP Tools 4
 - Erforderliche Berechtigungen für Aufgaben mit ONTAP-Tools 6
 - Berechtigungen für ONTAP Storage-Systeme und vSphere-Objekte 6
 - So konfigurieren Sie die rollenbasierte ONTAP-Zugriffssteuerung für ONTAP Tools für VMware vSphere .. 9

Rollenbasierte Zugriffssteuerung

Übersicht über die rollenbasierte Zugriffssteuerung in den ONTAP Tools

vCenter Server bietet rollenbasierte Zugriffssteuerung (RBAC), über die Sie den Zugriff auf vSphere Objekte kontrollieren können. In ONTAP® Tools für VMware vSphere arbeitet vCenter Server RBAC mit ONTAP RBAC zusammen, um zu bestimmen, welche ONTAP-Tools ein bestimmter Benutzer an Objekten auf einem bestimmten Speichersystem ausführen kann.

Zum erfolgreichen Abschluss einer Aufgabe müssen Sie über die entsprechenden Berechtigungen für die rollenbasierte Zugriffssteuerung von vCenter Server verfügen. Während einer Aufgabe prüfen ONTAP-Tools die vCenter Server-Berechtigungen eines Benutzers, bevor die ONTAP-Berechtigungen des Benutzers überprüft werden.

Sie können die vCenter Server-Berechtigungen auf dem Root-Objekt (auch als Stammordner bekannt) festlegen. Sie können dann die Sicherheit verbessern, indem Sie untergeordnete Entitäten, die diese Berechtigungen nicht benötigen, einschränken.

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.

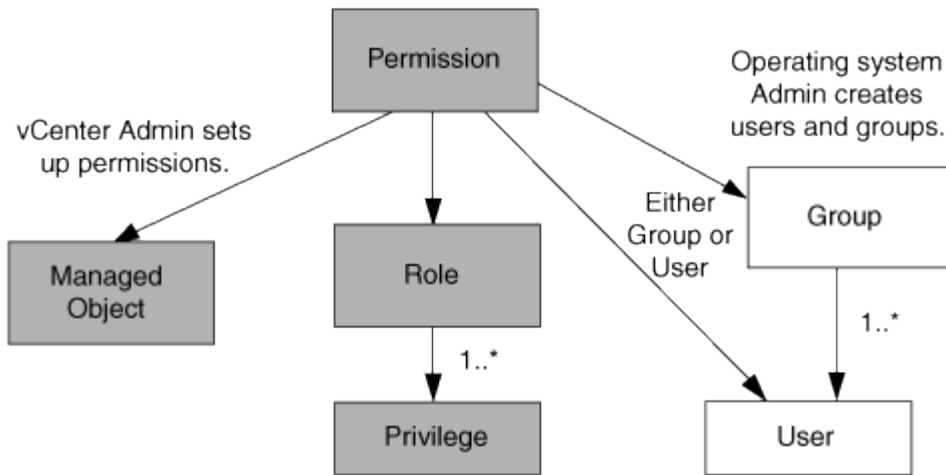
- Ein Benutzer oder eine Gruppe

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

Wie das folgende Diagramm veranschaulicht, müssen Sie alle drei Elemente haben, um eine Berechtigung zu erhalten.



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 Aufgaben mit ONTAP-Tools definiert. Sie sind einzigartig bei ONTAP Tools.

ONTAP-Tools-Aufgaben 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 mehrere Standardrollen, die alle ONTAP für das Ausführen von ONTAP-Tools erforderlichen spezifischen und nativen Berechtigungen enthalten.

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.

Privilege	Rollen	Aufgaben
NetApp ONTAP Tools Console > View	<ul style="list-style-type: none"> • VSC Administrator • VSC Provisionierung • VSC schreibgeschützt 	Für alle ONTAP-Tools und VASA Provider-spezifischen Aufgaben ist die Berechtigung zum Anzeigen erforderlich.

NetApp Virtual Storage Console > richtlinienbasiertes Management > Management oder privilege.nvpfVSC.VASAGroup.com.netapp.nvpf.label > Management	VSC Administrator	VSC und VASA Provider Aufgaben bezüglich Storage-Funktionsprofilen und Schwellenwerteinstellungen.
---	-------------------	--

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 spezifische Aufgaben von ONTAP-Tools werden Berechtigungen nur auf Root-Ordner Ebene (vCenter Server) und nicht auf einer anderen Einheit zugewiesen und validiert. Außer VAAI Plugin Betrieb, wo Berechtigungen gegen die betroffenen ESXi 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 bestimmte ONTAP-Tools-Aufgaben ausführen können.



Diese vCenter Server-Berechtigungen gelten für vCenter-Benutzer von ONTAP-Tools, nicht für Administratoren von ONTAP-Tools. Standardmäßig haben Administratoren von ONTAP-Tools 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.

Kernpunkte zum 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.

Wenn Sie eine Berechtigung zuweisen, bestimmt dies die Aufgaben der ONTAP-Tools, die ein Benutzer ausführen kann.

Um den Abschluss einer Aufgabe zu gewährleisten, müssen Sie die Berechtigung auf einer höheren Ebene zuweisen, z. B. dem Root-Objekt. 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 Berechtigungen für eine untergeordnete Einheit als Möglichkeit zur Einschränkung des Geltungsbereichs einer Berechtigung, die einem Root-Objekt zugewiesen und von der untergeordneten Einheit vererbt wurde, haben können.



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, müssen Sie die Berechtigung, die diese Berechtigung enthält, dem Stammobjekt ONTAP Tools zuweisen, da es kein vSphere-Objekt gibt, dem Sie es zuweisen können.

Beispielsweise müssen alle Berechtigungen, die eine Berechtigung wie die Berechtigung „Speichersysteme hinzufügen/ändern/überspringen“ für ONTAP-Tools 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.

Standardrollen in Paket mit ONTAP Tools

Um die Arbeit mit vCenter Server-Berechtigungen und rollenbasierter Zugriffssteuerung (Role Based Access Control, RBAC) zu vereinfachen, bieten die ONTAP Tools standardmäßige ONTAP-Tools, mit denen Sie wichtige ONTAP-Tools-Aufgaben ausführen können. Es gibt auch eine schreibgeschützte Rolle, mit der Sie die Informationen anzeigen, aber keine Aufgaben ausführen können.

Die Standard-ONTAP-Tool-Rollen verfügen sowohl über die erforderlichen spezifischen Berechtigungen für ONTAP-Tools als auch über die nativen vCenter Server-Berechtigungen, die Benutzer zum Ausführen von ONTAP-Tools-Aufgaben benötigen. Darüber hinaus werden die Rollen so eingerichtet, dass sie über die erforderlichen Berechtigungen für alle unterstützten Versionen des vCenter Servers verfügen.

Als Administrator können Sie diese Rollen bei Bedarf Benutzern zuweisen.



Wenn Sie ONTAP-Tools auf die neueste Version aktualisieren, werden die Standardrollen automatisch aktualisiert, um mit der neuen Version des Tools zu arbeiten.

Sie können die Standardrollen der ONTAP-Tools anzeigen, indem Sie auf der vSphere Client-Startseite auf **Rollen** klicken.

Mit den Rollen, die ONTAP-Tools zur Verfügung stellen, können Sie die folgenden Aufgaben ausführen:

* Rolle*	Beschreibung
VSC Administrator	Bietet alle nativen vCenter Server-Berechtigungen und ONTAP-Tools-spezifischen Berechtigungen, die für die Ausführung aller ONTAP-Tools-Aufgaben erforderlich sind.
VSC schreibgeschützt	Bietet schreibgeschützten Zugriff auf ONTAP Tools. Diese Benutzer können keine ONTAP-Tools-Aktionen ausführen, die über Zugriffskontrollmöglichkeiten verfügen.
VSC Provisionierung	Bietet alle nativen vCenter Server-Berechtigungen und ONTAP-Tools-spezifischen Berechtigungen, die für die Bereitstellung von Speicher erforderlich sind. Sie können die folgenden Aufgaben ausführen: <ul style="list-style-type: none"> • Erstellen neuer Datenspeicher • Datastores zerstören • Zeigt Informationen zu Storage-Funktionsprofilen an

Richtlinien zur Verwendung von Standardrollen in ONTAP-Tools

Wenn Sie mit standardmäßigen ONTAP-Tools für VMware vSphere-Rollen arbeiten, gibt es bestimmte Richtlinien, die Sie befolgen sollten.

Sie sollten die Standardrollen nicht direkt ändern. Wenn Sie dies tun, überschreiben ONTAP-Tools Ihre Änderungen bei jedem Upgrade. Das Installationsprogramm aktualisiert die Standardrollendefinitionen jedes Mal, wenn Sie ONTAP-Tools aktualisieren. Dadurch wird sichergestellt, dass die Rollen für Ihre Version von ONTAP-Tools sowie für alle unterstützten Versionen von vCenter Server aktuell sind.

Sie können jedoch die Standardrollen verwenden, um Rollen zu erstellen, die auf Ihre Umgebung zugeschnitten sind. Dazu sollten Sie die Standardrolle „ONTAP Tools“ kopieren und dann die kopierte Rolle bearbeiten. Wenn Sie eine neue Rolle erstellen, können Sie diese Rolle auch dann beibehalten, wenn Sie den Windows-Dienst für ONTAP-Tools neu starten oder aktualisieren.

Folgende Standardrollen für ONTAP-Tools können u. a. verwendet werden:

- Verwenden Sie die Standardrollen der ONTAP-Tools für alle Aufgaben mit ONTAP-Tools.

In diesem Szenario bieten die Standardrollen alle Berechtigungen, die ein Benutzer zur Ausführung der Aufgaben der ONTAP-Tools benötigt.

- Kombinieren Sie Rollen, um die Aufgaben zu erweitern, die ein Benutzer ausführen kann.

Wenn die Standard-ONTAP-Tools-Rollen zu viel Granularität für Ihre Umgebung bieten, können Sie die Rollen erweitern, indem Sie Gruppen auf höherer Ebene erstellen, die mehrere Rollen enthalten.

Wenn ein Benutzer andere Aufgaben, die nicht zu ONTAP gehören, ausführen muss, für die zusätzliche native vCenter Server-Berechtigungen erforderlich sind, können Sie eine Rolle erstellen, die diese Berechtigungen bereitstellt, und diese auch der Gruppe hinzufügen.

- Erstellung feingranularer Rollen

Wenn in Ihrem Unternehmen Rollen implementiert werden müssen, die restriktiver sind als die Standardrollen für ONTAP-Tools, können Sie mithilfe der Rollen im Bereich ONTAP-Tools neue Rollen erstellen.

In diesem Fall klonen Sie die erforderlichen Rollen der ONTAP-Tools und bearbeiten dann die geklonte Rolle, sodass nur die Berechtigungen zum Benutzer gehören.

Erforderliche Berechtigungen für Aufgaben mit ONTAP-Tools

Verschiedene ONTAP-Tools für VMware vSphere-Aufgaben erfordern unterschiedliche Kombinationen von Berechtigungen für ONTAP-Tools und native vCenter Server-Berechtigungen.

Informationen zu den für Aufgaben mit ONTAP-Tools erforderlichen Berechtigungen finden Sie im NetApp Knowledge Base Artikel 1032542.

["So konfigurieren Sie RBAC für die Virtual Storage Console"](#)

Product-Level-Berechtigung erforderlich, die von ONTAP Tools für VMware vSphere benötigt wird

Um auf die ONTAP Tools für die VMware vSphere GUI zuzugreifen, müssen Sie über die für ONTAP Tools spezifische Produktberechtigung auf der richtigen vSphere Objektebene verfügen. Wenn Sie sich ohne diese Berechtigung anmelden, zeigt ONTAP Tools beim Klicken auf das Symbol NetApp eine Fehlermeldung an und verhindert, dass Sie auf ONTAP-Tools zugreifen können.

Mit der Berechtigung **Ansicht** können Sie auf die Benutzeroberfläche der ONTAP-Tools zugreifen. Mit dieser Berechtigung können Sie keine Aufgaben in ONTAP-Tools ausführen. Um ONTAP-Tools-Aufgaben auszuführen, müssen 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. Durch Zuweisen der Berechtigung Ansicht im Stammobjekt (Ordner) können Sie ONTAP-Tools aufrufen, indem Sie auf das Symbol NetApp klicken.

Sie können die Berechtigung Ansicht einer anderen vSphere Objektebene zuweisen. Dadurch sind jedoch die Menüs der ONTAP Tools eingeschränkt, die Sie sehen und verwenden können.

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

Berechtigungen für ONTAP Storage-Systeme und vSphere-Objekte

Mit der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) von ONTAP können Sie den Zugriff auf bestimmte Storage-Systeme steuern und die Aktionen steuern, die ein Benutzer auf diesen Storage-Systemen durchführen kann. In ONTAP®

Tools für VMware vSphere arbeitet ONTAP RBAC mit vCenter Server RBAC zusammen, um zu bestimmen, welche ONTAP-Tools ein bestimmter Benutzer an den Objekten eines bestimmten Speichersystems ausführen kann.

ONTAP Tools verwenden die innerhalb der ONTAP Tools festgelegten Anmeldedaten (Benutzername und Passwort), um jedes Storage-System zu authentifizieren und um zu ermitteln, welche Storage-Vorgänge auf diesem Storage-System ausgeführt werden können. Die ONTAP Tools verwenden für jedes Storage-System einen Satz an Zugangsdaten. Diese Referenzen legen fest, welche Aufgaben der ONTAP Tools auf diesem Storage-System ausgeführt werden können. Anders ausgedrückt: Die Zugangsdaten gelten für ONTAP Tools und nicht für einzelne Benutzer von ONTAP Tools.

Die rollenbasierte Zugriffssteuerung von ONTAP gilt nur für den Zugriff auf Storage-Systeme und die Durchführung von Aufgaben mit ONTAP-Tools, die im Zusammenhang mit Storage stehen, beispielsweise zur Bereitstellung von Virtual Machines. Wenn Sie nicht über die entsprechenden ONTAP RBAC-Berechtigungen für ein bestimmtes Storage-System verfügen, können Sie auf einem vSphere Objekt, das auf diesem Storage-System gehostet wird, keine Aufgaben ausführen. Sie können die rollenbasierte Zugriffssteuerung von ONTAP in Verbindung mit spezifischen Berechtigungen der ONTAP-Tools verwenden, um zu steuern, welche Aufgaben für ONTAP-Tools ein Benutzer ausführen kann:

- Überwachung und Konfiguration von Storage- oder vCenter Server-Objekten in einem Storage-System
- Bereitstellung von vSphere Objekten in einem Storage-System

Die Nutzung der rollenspezifischen Berechtigungen für ONTAP mit den ONTAP Tools verschafft dem Storage-Administrator eine Storage-orientierte Sicherheitsebene, die er managen kann. Somit verfügen Sie über eine feingranulare Zugriffssteuerung als nur die ONTAP RBAC oder die alleine vCenter Server RBAC unterstützt. So können Sie mit vCenter Server RBAC z. B. vCenterUserB die Bereitstellung eines Datenspeichers auf NetApp Storage zulassen und zugleich verhindern, dass vCenterUserA Datenspeicher bereitstellt. Wenn die Anmeldeinformationen des Speichersystems für ein bestimmtes Speichersystem die Erstellung von Speicher nicht unterstützen, können weder vCenterUserB noch vCenterUserA einen Datenspeicher auf diesem Speichersystem bereitstellen.

Wenn Sie eine ONTAP-Tool-Aufgabe starten, überprüft ONTAP-Tools zunächst, ob Sie die richtige vCenter-Server-Berechtigung für diese Aufgabe haben. Wenn die vCenter Server-Berechtigung nicht ausreicht, um die Ausführung der Aufgabe zu ermöglichen, müssen ONTAP-Tools die ONTAP-Berechtigungen für dieses Speichersystem nicht überprüfen, da Sie die erste vCenter Server-Sicherheitsprüfung nicht bestanden haben. So kann nicht auf das Storage-System zugegriffen werden.

Wenn die Berechtigungen für vCenter Server ausreichend sind, prüfen ONTAP-Tools dann die RBAC-Berechtigungen von ONTAP (Ihre ONTAP-Rolle), die mit den Anmeldedaten des Storage-Systems (Benutzername und Passwort) verknüpft sind. Um zu ermitteln, ob Sie über ausreichende Berechtigungen verfügen, um die Speichervorgänge auszuführen, die für die Aufgabe „ONTAP-Tools“ auf diesem Speichersystem erforderlich sind. Wenn Sie über die richtigen ONTAP-Berechtigungen verfügen, können Sie auf das Speichersystem zugreifen und die Aufgabe „ONTAP-Tools“ ausführen. Die ONTAP-Rollen bestimmen die Aufgaben der ONTAP-Tools, die Sie auf dem Storage-System durchführen können.

Jedem Speichersystem ist ein Satz von ONTAP-Berechtigungen zugeordnet.

Die Nutzung der ONTAP RBAC und der vCenter Server RBAC bietet folgende Vorteile:

- Sicherheit

Der Administrator kann steuern, welche Benutzer welche Aufgaben auf feingranularen vCenter Server-Objektebene und auf Ebene des Storage-Systems ausführen können.

- Audit-Informationen

In vielen Fällen bieten ONTAP Tools ein Prüfprotokoll auf dem Storage-System, mit dem Sie Ereignisse an den vCenter Server-Benutzer zurückverfolgen können, der die Storage-Änderungen durchgeführt hat.

- Benutzerfreundlichkeit

Sie können alle Controller-Anmeldedaten an einer Stelle beibehalten.

Empfohlene ONTAP-Rollen bei der Verwendung von ONTAP Tools für VMware vSphere

Sie können mehrere empfohlene ONTAP-Rollen für die Arbeit mit ONTAP®-Tools für VMware vSphere und rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) einrichten. Diese Rollen verfügen über die ONTAP-Berechtigungen, die zur Durchführung der erforderlichen Storage-Vorgänge erforderlich sind, die von den ONTAP-Tools-Aufgaben ausgeführt werden.

Um neue Benutzerrollen zu erstellen, müssen Sie sich als Administrator auf Storage-Systemen, auf denen ONTAP ausgeführt wird, einloggen. Sie können ONTAP Rollen mit ONTAP System Manager 9.8P1 oder höher erstellen. Siehe "[Konfigurieren von Benutzerrollen und -Berechtigungen](#)" Finden Sie weitere Informationen.

Jeder ONTAP-Rolle ist ein zugehöriger Benutzername und ein Passwort zugeordnet, was 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-spezifischen ONTAP-Rollen hierarchisch geordnet. Dies bedeutet, dass die erste Rolle die restriktivste Rolle ist und nur über die Berechtigungen verfügt, die mit dem grundlegendsten Satz von ONTAP-Tools-Speichervorgängen verknüpft sind. Die nächste Rolle umfasst sowohl eigene Berechtigungen als auch alle Berechtigungen, die mit der vorherigen Rolle verknüpft sind. Jede zusätzliche Rolle ist hinsichtlich des unterstützten Storage-Betriebs weniger restriktiv.

Im Folgenden finden Sie einige der empfohlenen ONTAP RBAC-Rollen bei der Verwendung von ONTAP Tools. Nachdem Sie diese Rollen erstellt haben, können Sie sie Benutzern zuweisen, die Storage-Aufgaben ausführen müssen, z. B. Virtual Machines bereitstellen.

1. Ermitteln

Diese Rolle ermöglicht es Ihnen, Storage-Systeme hinzuzufügen.

2. Speicher Erstellen

Mit dieser Rolle können Sie Speicher erstellen. Diese Rolle umfasst außerdem alle Berechtigungen, die mit der Ermittlungsrolle verknüpft sind.

3. Speicher Ändern

Mit dieser Rolle können Sie Speicher ändern. Diese Rolle umfasst außerdem alle Berechtigungen, die der Bestandsernahmerrolle und der Rolle „Speicher erstellen“ zugeordnet sind.

4. Speicher Zerstören

Mit dieser Rolle können Sie Speicher zerstören. Diese Rolle umfasst außerdem alle Berechtigungen, die der Bestandsernahmerrolle, der Rolle „Speicher erstellen“ und der Rolle „Speicher ändern“ zugeordnet sind.

Wenn Sie VASA Provider für ONTAP nutzen, sollten Sie auch eine richtlinienbasierte Managementrolle (PBM, richtlinienbasiertes Management) einrichten. Diese Rolle ermöglicht Ihnen das Storage-Management mithilfe von Storage-Richtlinien. Diese Rolle erfordert, dass Sie auch die Rolle "Discovery" einrichten.

So konfigurieren Sie die rollenbasierte ONTAP-Zugriffssteuerung für ONTAP Tools für VMware vSphere

Sie müssen die rollenbasierte Zugriffssteuerung (RBAC) von ONTAP auf dem Storage-System konfigurieren, wenn Sie eine rollenbasierte Zugriffssteuerung mit ONTAP Tools für VMware vSphere verwenden möchten. Über die ONTAP Funktion zur rollenbasierten Zugriffssteuerung können Sie ein oder mehrere benutzerdefinierte Benutzerkonten mit begrenzten Zugriffsberechtigungen erstellen.

ONTAP Tools und SRA können auf Storage-Systeme entweder auf Cluster-Ebene oder auf SVM-Ebene (Storage Virtual Machine) zugreifen. Wenn Sie Storage-Systeme auf Cluster-Ebene hinzufügen, müssen Sie die Anmeldedaten des Admin-Benutzers angeben, um alle erforderlichen Funktionen bereitzustellen. Wenn Sie Storage-Systeme durch direktes Hinzufügen von SVM-Details hinzufügen, müssen Sie beachten, dass der Benutzer „vsadmin“ nicht über alle erforderlichen Rollen und Funktionen zum Ausführen bestimmter Aufgaben verfügt.

VASA Provider kann nur auf Cluster-Ebene auf Storage-Systeme zugreifen. Wenn VASA Provider für einen bestimmten Storage-Controller erforderlich ist, muss das Storage-System zu ONTAP Tools auf Cluster-Ebene hinzugefügt werden, selbst wenn Sie ONTAP Tools oder SRA verwenden.

Um einen neuen Benutzer zu erstellen und ein Cluster oder eine SVM mit ONTAP-Tools zu verbinden, sollten Sie Folgendes durchführen:

- Erstellen Sie einen Cluster-Administrator oder eine SVM-Administratorrolle mit ONTAP System Manager 9.8P1 oder höher. Siehe "[Konfigurieren von Benutzerrollen und -Berechtigungen](#)" Finden Sie weitere Informationen.
- Erstellen Sie Benutzer mit der zugewiesenen Rolle und dem entsprechenden Anwendungssatz mithilfe von ONTAP

Sie benötigen diese Anmeldedaten für das Storage-System, um die Storage-Systeme für ONTAP Tools zu konfigurieren. Sie können Storage-Systeme für ONTAP Tools konfigurieren, indem Sie die Zugangsdaten in die ONTAP Tools eingeben. Jedes Mal, wenn Sie sich mit diesen Zugangsdaten bei einem Storage-System anmelden, haben Sie Berechtigungen für die ONTAP-Tools-Funktionen, die Sie in ONTAP eingerichtet hatten, während Sie die Anmeldedaten erstellen.

- Fügen Sie das Storage-System zu den ONTAP Tools hinzu und geben Sie die Anmeldeinformationen des soeben erstellten Benutzers an

Rollen in ONTAP Tools

ONTAP-Tools klassifiziert die ONTAP-Berechtigungen in die folgenden Rollen von ONTAP-Tools:

- Ermitteln
Ermöglicht die Erkennung aller verbundenen Storage Controller
- Speicher Erstellen

Ermöglicht die Erstellung von Volumes und LUNs (Logical Unit Number)

- Speicher Ändern

Ermöglicht die Anpassung und Deduplizierung von Storage-Systemen

- Speicher Zerstören

Aktiviert die Zerstörung von Volumes und LUNs

VASA Provider-Rollen

Sie können nur richtlinienbasiertes Management auf Cluster-Ebene erstellen. Diese Rolle ermöglicht ein richtlinienbasiertes Storage Management mithilfe von Storage-funktionsprofilen.

SRA-Rollen

SRA klassifiziert die ONTAP-Berechtigungen als SAN- oder NAS-Rolle auf Cluster-Ebene oder SVM-Ebene. So können Benutzer SRM-Vorgänge ausführen.

ONTAP-Tools führen eine Erstvalidierung von Berechtigungen für RBAC-Rollen von ONTAP durch, wenn Sie den Cluster zu ONTAP Tools hinzufügen. Wenn Sie eine direkte SVM-Storage-IP hinzugefügt haben, führen die ONTAP-Tools die erste Validierung nicht durch. ONTAP-Tools prüfen und erzwingt die Berechtigungen später im Task-Workflow.

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

Markeninformationen

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