Für VSC Aufgaben erforderliche Berechtigungen

VSC, VASA Provider, and SRA 9.7

NetApp
March 21, 2024

Inhalt

Für VSC Aufgaben erforderliche Berechtigungen

Für verschiedene Aufgaben der Virtual Storage Console für VMware vSphere sind unterschiedliche Kombinationen von Berechtigungen erforderlich, die spezifisch für (VSC) und native vCenter Server-Berechtigungen gelten.

Informationen zu den für VSC Aufgaben erforderlichen Berechtigungen finden Sie im NetApp Knowledgebase Artikel 1032542.

"So konfigurieren Sie RBAC für die Virtual Storage Console"

Berechtigung auf Produktebene erforderlich von VSC für VMware vSphere

Um auf die Virtual Storage Console für VMware vSphere GUI zuzugreifen, müssen Sie über die VSC-spezifische View Berechtigung auf Produktebene, die auf der richtigen vSphere Objektebene zugewiesen ist, verfügen. Wenn Sie sich ohne diese Berechtigung anmelden, zeigt die VSC eine Fehlermeldung an, wenn Sie auf das NetApp Symbol klicken und verhindert, dass Sie auf die VSC zugreifen.

In den folgenden Informationen wird die VSC Berechtigung auf Produktebene View beschrieben:

Berechtigung	Beschreibung	Zuweisungsebene
Anzeigen	Sie können auf die VSC GUI zugreifen. Diese Berechtigung ermöglicht Ihnen nicht, Aufgaben in der VSC auszuführen. Zum Ausführen von VSC Aufgaben müssen Sie über die richtigen VSC-spezifischen und nativen vCenter Server-Berechtigungen für diese Aufgaben verfügen.	Die Zuweisungsebene legt fest, welche Teile der Benutzeroberfläche angezeigt werden können. Durch das Zuweisen der View-Berechtigung im Root-Objekt (Ordner) können Sie VSC durch Klicken auf das NetApp Symbol eingeben. Sie können die View-Berechtigung einer anderen vSphere Objektebene zuweisen. Dabei ist jedoch die VSC-Menüs, die Sie anzeigen und verwenden können, beschränkt. Das Root-Objekt ist der empfohlene Ort, um alle Berechtigungen zuzuweisen, die die View-Berechtigung enthalten.

Rollenbasierte Zugriffssteuerung von ONTAP für die virtuelle Appliance für VSC, VASA Provider und SRA

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 der Virtual Storage Console für VMware vSphere arbeitet die ONTAP RBAC mit der rollenbasierten Zugriffssteuerung von vCenter Server zusammen, um festzulegen, welche Aufgaben der Virtual Storage Console (VSC) ein bestimmter Benutzer auf den Objekten auf einem bestimmten Storage-System ausführen kann.

VSC verwendet die in VSC festgelegten Anmeldedaten (Benutzername und Passwort) zur Authentifizierung jedes Storage-Systems und zur Bestimmung der Storage-Vorgänge auf diesem Storage-System. VSC verwendet einen Satz Credentials für jedes Storage-System. Mit diesen Anmeldedaten wird festgelegt, welche VSC Aufgaben auf dem Storage-System ausgeführt werden können. Das heißt, die Anmeldedaten gelten für die VSC, nicht für einen individuellen VSC Benutzer.

ONTAP RBAC gilt nur für den Zugriff auf Storage-Systeme und die Durchführung von VSC-Aufgaben, die mit dem Storage zusammenhängen, beispielsweise für die 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 ONTAP RBAC zusammen mit den VSC-spezifischen Berechtigungen verwenden, um zu steuern, welche VSC Aufgaben 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

Durch den Einsatz der ONTAP RBAC mit den VSC-spezifischen Berechtigungen wird eine Storage-orientierte Sicherheitsebene bereitgestellt, die der Storage-Administrator managen kann. Somit verfügen Sie über eine feingranulare Zugriffssteuerung als nur die ONTAP RBAC oder die alleine vCenter Server RBAC unterstützt. Mit der RBAC für vCenter Server können Sie beispielsweise vCenterUserB die Bereitstellung eines Datenspeichers im Storage zulassen und gleichzeitig vCenterUserA daran hindern, Datenspeicher bereitzustellen. 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.

Beim Starten einer VSC Aufgabe überprüft die VSC zunächst, ob Sie über die richtige vCenter Server-Berechtigung für diese Aufgabe verfügen. Wenn die Berechtigung des vCenter Servers nicht ausreicht, um eine Aufgabe ausführen zu können, muss die VSC die ONTAP-Berechtigungen für dieses Speichersystem nicht überprüfen, da Sie die erste Sicherheitsüberprüfung des vCenter Servers nicht bestanden haben. So kann nicht auf das Storage-System zugegriffen werden.

Falls die Berechtigung zum vCenter Server ausreichend ist, prüft VSC die ONTAP RBAC-Berechtigungen (Ihre ONTAP Rolle), die mit den Anmeldedaten des Storage-Systems verknüpft sind (Benutzername und Passwort). Um zu ermitteln, ob Sie über ausreichende Berechtigungen zur Durchführung der Storage-Operationen verfügen, die von dieser VSC Aufgabe auf diesem Storage-System benötigt werden. Wenn Sie die richtigen ONTAP-Rechte haben, können Sie auf das Storage-System zugreifen und die VSC-Aufgabe ausführen. Die ONTAP-Rollen bestimmen die VSC-Aufgaben, 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 bietet VSC ein Audit-Trail im Storage-System, anhand dessen Sie Ereignisse zurück an den vCenter Server Benutzer verfolgen können, der die Storage-Änderungen durchgeführt hat.

- Benutzerfreundlichkeit

  Sie können alle Controller-Anmeldedaten an einer Stelle beibehalten.

Empfohlene ONTAP Rollen bei der Verwendung von VSC für VMware vSphere

Sie können mehrere empfohlene ONTAP-Rollen für die Arbeit mit der Virtual Storage Console für VMware vSphere und der rollenbasierten Zugriffssteuerung einrichten. Diese Rollen enthalten die ONTAP-Berechtigungen, die erforderlich sind, um die erforderlichen Storage-Vorgänge auszuführen, die von den VSC-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 einer der folgenden Elemente erstellen:

- 9.7 oder höher

  "Konfigurieren von Benutzerrollen und -Berechtigungen"

- RBAC Benutzer Creator für ONTAP Tool (bei Verwendung von ONTAP 9.6 oder früher)

  "RBAC Benutzer Creator Tool für VSC, VASA Provider und Storage Replication Adapter 7.0 für VMware vSphere"

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.

Die VSC-spezifischen ONTAP-Rollen werden in hierarchischen Anordnung angeordnet. Das bedeutet, dass die erste Rolle die restriktivsten Rollen ist und nur die Berechtigungen besitzt, die mit dem Basissatz von VSC-Storage-Vorgängen 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.

Nachstehend finden Sie einige der empfohlenen ONTAP RBAC-Rollen beim Einsatz von VSC. 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 “Diskovery” einrichten.

So konfigurieren Sie die rollenbasierte Zugriffssteuerung für ONTAP für VMware vSphere

Sie müssen die rollenbasierte Zugriffssteuerung (RBAC) der ONTAP auf dem Storage-System konfigurieren, wenn Sie die rollenbasierte Zugriffssteuerung über die Virtual Storage Console für VMware vSphere (VSC) nutzen möchten. Über die ONTAP Funktion zur rollenbasierten Zugriffssteuerung können Sie ein oder mehrere benutzerdefinierte Benutzerkonten mit begrenzten Zugriffsberechtigungen erstellen.

VSC und SRA können auf Storage-Systeme entweder auf Cluster-Ebene oder auf Cluster-Ebene 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 direkte Hinzufügung von 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 benötigt wird, muss das Storage-System der VSC auf Cluster-Ebene hinzugefügt werden, selbst wenn Sie VSC oder SRA verwenden.

Um einen neuen Benutzer zu erstellen und ein Cluster oder eine Verbindung zu VSC, VASA Provider und SRA herzustellen, sollten Sie Folgendes durchführen:

- Erstellen eines Cluster-Administrators oder einer Administratorrolle

Sie können eine der folgenden Funktionen verwenden, um diese Rollen zu erstellen:

- ONTAP System Manager 9.7 oder höher

"Konfigurieren von Benutzerrollen und -Berechtigungen"

- RBAC Benutzer Creator für ONTAP Tool (bei Verwendung von ONTAP 9.6 oder früher)

"RBAC Benutzer Creator Tool für VSC, VASA Provider und Storage Replication Adapter 7.0 für VMware vSphere"

- Erstellen Sie Benutzer mit der zugewiesenen Rolle und dem entsprechenden Anwendungssatz mithilfe von ONTAP

  Sie benötigen diese Storage-System-Anmeldedaten, um die Storage-Systeme für VSC zu konfigurieren. Sie können Storage-Systeme für VSC konfigurieren, indem Sie die Anmeldedaten in der VSC eingeben. Jedes Mal, wenn Sie sich mit diesen Anmeldedaten in einem Storage-System anmelden, erhalten Sie Berechtigungen für die VSC Funktionen, die Sie bei der Erstellung der Anmeldedaten in ONTAP eingerichtet hatten.

- Fügen Sie das Storage-System zur VSC hinzu und stellen Sie die Zugangsdaten des gerade erstellten Benutzers bereit

VSC Rollen

Die VSC klassifiziert die ONTAP Berechtigungen in folgende VSC-Rollen:

- 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 auf der Ebene. So können Benutzer SRM-Vorgänge ausführen.

Wenn Sie Rollen und Berechtigungen mithilfe von ONTAP-Befehlen manuell konfigurieren möchten, müssen Sie sich in den Knowledge Base-Artikeln informieren.

- "VSC, VASA und SRA 7.0 ONTAP RBAC-Konfiguration"
- "Führen Sie alle Befehle auf VSC- und SRA-Ebene auf SVM-Ebene durch"

VSC führt eine erste Berechtigungsvalidierung der ONTAP RBAC-Rollen durch, wenn Sie das Cluster der VSC hinzufügen. Wenn Sie eine direkte Storage-IP hinzugefügt haben, führt VSC die erste Validierung nicht durch. VSC überprüft und erzwingt die Berechtigungen später im Task-Workflow.

Konfigurieren von Benutzerrollen und -Berechtigungen

Neue Benutzerrollen zum Management von Storage-Systemen können mit der JSON-Datei konfiguriert werden, die mit der virtuellen Appliance für VSC, VASA Provider, SRA und ONTAP System Manager bereitgestellt wird.

Bevor Sie beginnen

- Sie sollten die Datei ONTAP-Berechtigungen mithilfe von von von von der virtuellen Appliance für VSC, VASA Provider und SRA heruntergeladen haben `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip`.
- Sie sollten ONTAP 9.7 System Manager konfiguriert haben.
- Sie sollten sich mit Administratorrechten für das Speichersystem angemeldet haben.

Schritte

1. Entpacken Sie die heruntergeladene Datei `https://{virtual_appliance_IP}:9083/vsc/config/VSC_ONTAP_User_Privileges.zip` Datei:
2. Greifen Sie auf ONTAP System Manager zu.
3. Klicken Sie auf Menü:CLUSTER[Einstellungen > Benutzer und Rollen].
4. Klicken Sie Auf **Benutzer Hinzufügen**.
5. Wählen Sie im Dialogfeld * Benutzer hinzufügen* die Option **Virtualisierungsprodukte** aus.
6. Klicken Sie auf **Durchsuchen**, um die JSON-Datei der ONTAP-Berechtigungen auszuwählen und hochzuladen.

   DAS PRODUKTFELD wird automatisch ausgefüllt.

7. Wählen Sie die gewünschte Funktion aus dem Dropdown-Menü * PRODUCT CAPABILITY* aus.

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

8. Geben Sie den erforderlichen Benutzernamen und das erforderliche Passwort ein.
9. Wählen Sie die für den Benutzer erforderlichen Berechtigungen (Discovery, Create Storage, Modify Storage, Destroy Storage) aus, und klicken Sie dann auf **Add**.

Ergebnisse

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