



Konfigurieren der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC)

SnapCenter software

NetApp
January 09, 2026

Inhalt

- Konfigurieren der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC)..... 1
 - Erstellen Sie eine Rolle 1
 - Fügen Sie mithilfe von Sicherheits-Login-Befehlen eine RBAC-Rolle für NetApp ONTAP hinzu 1
 - Erstellen Sie SVM-Rollen mit minimalen Berechtigungen 3
 - ONTAP CLI-Befehle zum Erstellen von SVM-Rollen und Zuweisen von Berechtigungen..... 4
 - Erstellung von SVM-Rollen für ASA r2 Systeme 8
 - ONTAP CLI-Befehle zum Erstellen von SVM-Rollen und Zuweisen von Berechtigungen..... 9
 - Erstellen Sie ONTAP-Cluster-Rollen mit minimalen Berechtigungen 13
 - ONTAP CLI Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen 14
 - Erstellen von ONTAP Clusterrollen für ASA r2-Systeme 20
 - ONTAP CLI Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen 20
 - Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu..... 27

Konfigurieren der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC)

Erstellen Sie eine Rolle

Zusätzlich zur Nutzung vorhandener SnapCenter-Rollen können Sie eigene Rollen erstellen und die Berechtigungen anpassen.

Um eigene Rollen zu erstellen, ist eine Anmeldung mit der Rolle „SnapCenterAdmin“ erforderlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Rollen**.
3. Klicken Sie Auf .
4. Geben Sie einen Namen und eine Beschreibung für die neue Rolle an.



In Benutzernamen und Gruppennamen dürfen nur die folgenden Sonderzeichen verwendet werden: Leerzeichen (), Bindestrich (-), Unterstrich (_) und Doppelpunkt (:).

5. Wählen Sie **Alle Mitglieder dieser Rolle können Objekte anderer Mitglieder** sehen, damit andere Mitglieder der Rolle nach der Aktualisierung der Ressourcenliste Ressourcen wie Volumes und Hosts sehen können.

Sie sollten diese Option deaktivieren, wenn Sie nicht möchten, dass Mitglieder dieser Rolle Objekte sehen, denen andere Mitglieder zugewiesen sind.



Wenn diese Option aktiviert ist, ist es nicht erforderlich, Benutzern Zugriff auf Objekte oder Ressourcen zuzuweisen, wenn Benutzer derselben Rolle angehören wie der Benutzer, der die Objekte oder Ressourcen erstellt hat.

6. Wählen Sie auf der Seite Berechtigungen die Berechtigungen aus, die Sie der Rolle zuweisen möchten, oder klicken Sie auf **Alle auswählen**, um der Rolle alle Berechtigungen zu gewähren.
7. Klicken Sie Auf **Absenden**.

Fügen Sie mithilfe von Sicherheits-Login-Befehlen eine RBAC-Rolle für NetApp ONTAP hinzu

Sie können die Sicherheitskontinbefehle verwenden, um eine RBAC-Rolle für NetApp ONTAP hinzuzufügen, wenn auf Ihren Storage-Systemen Clustered ONTAP ausgeführt wird.

Bevor Sie beginnen

- Identifizieren Sie die Aufgabe (oder Aufgaben), die Sie ausführen möchten, und die Berechtigungen, die zum Ausführen dieser Aufgaben erforderlich sind.

- Gewähren Sie Berechtigungen für Befehle und/oder Befehlsverzeichnisse.

Für jedes Befehlsverzeichnis gibt es zwei Zugriffsebenen: All-Access und Read-Only.

Sie müssen immer zuerst die All-Access-Berechtigungen zuweisen.

- Rollen Benutzern zuweisen.
- Identifizieren Sie Ihre Konfiguration, je nachdem, ob Ihre SnapCenter-Plug-Ins mit der Cluster-Administrator-IP für den gesamten Cluster oder direkt mit einer SVM innerhalb des Clusters verbunden sind.

Über diese Aufgabe

Um die Konfiguration dieser Rollen auf Speichersystemen zu vereinfachen, können Sie das Tool „RBAC User Creator für NetApp ONTAP“ verwenden, das im NetApp Communities Forum veröffentlicht wird.

Dieses Tool verarbeitet automatisch die korrekte Einrichtung der ONTAP-Berechtigungen. Das Tool RBAC User Creator for NetApp ONTAP fügt beispielsweise die Privileges automatisch in der richtigen Reihenfolge hinzu, sodass die Privileges mit allen Zugriffsrechten zuerst angezeigt werden. Wenn Sie zuerst die schreibgeschützten Berechtigungen hinzufügen und dann die All-Access-Berechtigungen hinzufügen, markiert ONTAP die All-Access-Berechtigungen als Duplikate und ignoriert sie.



Wenn Sie später SnapCenter oder ONTAP aktualisieren, sollten Sie das RBAC-Benutzerersteller für NetApp ONTAP-Tool erneut ausführen, um die zuvor erstellten Benutzerrollen zu aktualisieren. Benutzerrollen, die für eine frühere Version von SnapCenter oder ONTAP erstellt wurden, funktionieren nicht ordnungsgemäß mit aktualisierten Versionen. Wenn Sie das Tool erneut ausführen, übernimmt es automatisch die Aktualisierung. Sie müssen die Rollen nicht neu erstellen.

Weitere Informationen zum Einrichten von ONTAP RBAC-Rollen finden Sie im ["ONTAP 9 Administratorauthentifizierung und RBAC-Energiehandbuch"](#).

Schritte

1. Erstellen Sie auf dem Storage-System eine neue Rolle, indem Sie den folgenden Befehl eingeben:

```
security login role create <role_name> -cmddirname "command" -access all
-vserver <svm_name>
```

- svm_Name ist der Name der SVM. Wenn Sie dieses Feld leer lassen, werden standardmäßig Cluster-Administratoren verwendet.
- Role_Name ist der Name, den Sie für die Rolle angeben.
- Befehl ist die ONTAP Funktion.



Sie müssen diesen Befehl für jede Berechtigung wiederholen. Beachten Sie, dass vor schreibgeschützten Befehlen All-Access-Befehle aufgelistet werden müssen.

Informationen zur Liste der Berechtigungen finden Sie unter ["ONTAP CLI-Befehle zum Erstellen von Rollen und Zuweisen von Berechtigungen"](#).

2. Erstellen Sie einen Benutzernamen durch Eingabe des folgenden Befehls:

```
security login create -username <user_name> -application ontapi -authmethod
<password> -role <name_of_role_in_step_1> -vserver <svm_name> -comment
```

"user_description"

- User_Name ist der Name des von Ihnen erstellten Benutzers.
- <password> ist Ihr Passwort. Wenn Sie kein Passwort angeben, werden Sie vom System aufgefordert, ein Passwort einzugeben.
- svm_Name ist der Name der SVM.

3. Weisen Sie dem Benutzer die Rolle durch Eingabe des folgenden Befehls zu:

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod <password\>
```

- <user_Name> ist der Name des Benutzers, den Sie in Schritt 2 erstellt haben. Mit diesem Befehl können Sie den Benutzer so ändern, dass er der Rolle zugeordnet wird.
- <svm_Name> ist der Name der SVM.
- <Role_Name> ist der Name der Rolle, die Sie in Schritt 1 erstellt haben.
- <password> ist Ihr Passwort. Wenn Sie kein Passwort angeben, werden Sie vom System aufgefordert, ein Passwort einzugeben.

4. Überprüfen Sie, ob der Benutzer ordnungsgemäß erstellt wurde, indem Sie den folgenden Befehl eingeben:

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

User_Name ist der Name des Benutzers, den Sie in Schritt 3 erstellt haben.

Erstellen Sie SVM-Rollen mit minimalen Berechtigungen

Beim Erstellen einer Rolle für einen neuen SVM-Benutzer in ONTAP müssen Sie verschiedene ONTAP-CLI-Befehle ausführen. Diese Rolle ist erforderlich, wenn Sie SVMs in ONTAP für die Verwendung mit SnapCenter konfigurieren und Sie nicht die vsadmin-Rolle verwenden möchten.

Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

```
security login role create -vserver <svm_name\> -role <SVM_Role_Name\>  
-cmddirname <permission\>
```



Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer, und weisen Sie die Rolle diesem Benutzer zu.

```
security login create -user <user_name\> -vserver <svm_name\> -application  
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. Entsperren Sie den Benutzer.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

ONTAP CLI-Befehle zum Erstellen von SVM-Rollen und Zuweisen von Berechtigungen

Es gibt verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um SVM-Rollen zu erstellen und Berechtigungen zuzuweisen.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"volume clone split start" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone split stop" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume destroy" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file clone create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file show-disk-usage" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume modify" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume offline" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot modify" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "volume snapshot modify-snaplock-expiry-time" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot rename" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot restore" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

```
"nvme subsystem create" -access all
```

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

Erstellung von SVM-Rollen für ASA r2 Systeme

Es gibt mehrere ONTAP CLI-Befehle, die Sie ausführen müssen, um eine Rolle für einen neuen SVM-Benutzer in ASA r2-Systemen zu erstellen. Diese Rolle ist erforderlich, wenn Sie SVMs in ASA r2-Systemen für die Verwendung mit SnapCenter konfigurieren und die Rolle „vsadmin“ nicht verwenden möchten.

Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```



Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer, und weisen Sie die Rolle diesem Benutzer zu.

```
security login create -user <user_name\> -vserver <svm_name\> -application
http -authmethod password -role <SVM_Role_Name\>
```

3. Entsperren Sie den Benutzer.

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

ONTAP CLI-Befehle zum Erstellen von SVM-Rollen und Zuweisen von Berechtigungen

Es gibt verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um SVM-Rollen zu erstellen und Berechtigungen zuzuweisen.

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"volume clone split start" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone split stop" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume destroy" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file clone create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file show-disk-usage" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume modify" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume offline" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot modify" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "volume snapshot modify-snaplock-expiry-time" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot rename" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot restore" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

```

"nvme subsystem create" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem delete" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem modify" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem host" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem controller" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem show" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme namespace create" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme namespace delete" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme namespace modify" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme namespace show" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "storage-unit show" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "consistency-group" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "snapmirror protect" -access all
• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "volume delete" -access all
• security login create -user-or-group-name user_name -application http
  -authentication-method password -role SVM_Role_Name -vserver SVM_Name
• security login create -user-or-group-name user_name -application ssh
  -authentication-method password -role SVM_Role_Name -vserver SVM_Name

```

Erstellen Sie ONTAP-Cluster-Rollen mit minimalen Berechtigungen

Sie sollten eine ONTAP-Cluster-Rolle mit minimalen Berechtigungen erstellen, damit Sie die ONTAP-Administratorrolle nicht verwenden müssen, um Vorgänge in SnapCenter auszuführen. Sie können mehrere ONTAP CLI-Befehle ausführen, um die ONTAP-Cluster-Rolle zu erstellen und minimale Berechtigungen zuzuweisen.

Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

```
security login role create -vserver <cluster_name\>- role <role_name\>  
-cmddirname <permission\>
```



Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer, und weisen Sie die Rolle diesem Benutzer zu.

```
security login create -user <user_name\> -vserver <cluster_name\> -application  
ontapi http -authmethod password -role <role_name\>
```

3. Entsperren Sie den Benutzer.

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

ONTAP CLI Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen

Es gibt verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um Cluster-Rollen zu erstellen und Berechtigungen zuzuweisen.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname`

```

"lun create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun igroup add" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun igroup create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun igroup delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun igroup modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun igroup rename" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun igroup show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun mapping add-reporting-nodes" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun mapping create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun mapping delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun mapping remove-reporting-nodes" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun mapping show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun move-in-volume" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun offline" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun online" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun persistent-reservation clear" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun resize" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun serial" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun show" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"snapmirror policy delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy modify-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy remove-rule" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror policy show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror show-history" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror update" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror update-ls-set" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "system license add" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "system license clean-up" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "system license delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "system license show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "system license status show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "system node modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "system node show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "system status show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "version" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone show" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"volume snapshot rename" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore-file" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show-delta" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume unmount" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule delete" -access all

```

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all`
- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

Erstellen von ONTAP Clusterrollen für ASA r2-Systeme

Sie sollten eine ONTAP-Cluster-Rolle mit minimalen Berechtigungen erstellen, damit Sie die ONTAP-Administratorrolle nicht verwenden müssen, um Vorgänge in SnapCenter auszuführen. Sie können mehrere ONTAP CLI-Befehle ausführen, um die ONTAP-Cluster-Rolle zu erstellen und minimale Berechtigungen zuzuweisen.

Schritte

1. Erstellen Sie auf dem Speichersystem eine Rolle und weisen Sie der Rolle alle Berechtigungen zu.

```
security login role create -vserver <cluster_name>- role <role_name>-
-cmddirname <permission>
```



Sie sollten diesen Befehl für jede Berechtigung wiederholen.

2. Erstellen Sie einen Benutzer, und weisen Sie die Rolle diesem Benutzer zu.

```
security login create -user <user_name> -vserver <cluster_name> -application
http -authmethod password -role <role_name>
```

3. Entsperren Sie den Benutzer.

```
security login unlock -user <user_name> -vserver <cluster_name>
```

ONTAP CLI Befehle zum Erstellen von Clusterrollen und Zuweisen von Berechtigungen

Es gibt verschiedene ONTAP CLI Befehle, die Sie ausführen sollten, um Cluster-Rollen zu erstellen und Berechtigungen zuzuweisen.

- `security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly`
- `security login role create -vserver Cluster_name or cluster_name -role`

```

Role_Name -cmddirname "cluster identity modify" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```
"nvme subsystem show" -access all
```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"volume qtree create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot promote" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot rename" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore-file" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show-delta" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume unmount" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver cifs share modify" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "storage-unit show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "consistency-group" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror protect" show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume delete" show" -access all

Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu

Um die rollenbasierte Zugriffssteuerung für SnapCenter-Benutzer zu konfigurieren, können Sie Benutzer oder Gruppen hinzufügen und Rollen zuweisen. Die Rolle legt die Optionen fest, auf die SnapCenter-Benutzer zugreifen können.

Bevor Sie beginnen

- Sie müssen sich als „SnapCenterAdmin“-Rolle angemeldet haben.
- Sie müssen die Benutzer- oder Gruppenkonten in Active Directory im Betriebssystem oder in der Datenbank erstellt haben. Sie können SnapCenter nicht zum Erstellen dieser Konten verwenden.



In Benutzernamen und Gruppennamen können nur die folgenden Sonderzeichen eingefügt werden: Leerzeichen (), Bindestrich (-), Unterstrich (_) und Doppelpunkt (:).

- SnapCenter umfasst mehrere vordefinierte Rollen.

Sie können diese Rollen entweder dem Benutzer zuweisen oder neue Rollen erstellen.

- AD-Benutzer und AD-Gruppen, die SnapCenter RBAC hinzugefügt werden, müssen über DIE LESEBERECHTIGUNG auf dem Benutzer-Container und dem Computer-Container im Active Directory verfügen.
- Nachdem Sie einem Benutzer oder einer Gruppe eine Rolle zugewiesen haben, die die entsprechenden Berechtigungen enthält, müssen Sie den Benutzerzugriff auf SnapCenter-Ressourcen wie Hosts und Speicherverbindungen zuweisen.

Auf diese Weise können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

- Sie sollten dem Benutzer oder der Gruppe irgendwann eine Rolle zuweisen, um die RBAC-Berechtigungen und Effizienzfunktionen zu nutzen.
- Sie können Assets wie Host, Ressourcengruppen, Richtlinien, Storage-Verbindungen, Plug-in, Und Anmeldeinformationen für den Benutzer beim Erstellen des Benutzers oder der Gruppe.
- Die Mindestwerte, die Sie einem Benutzer zur Durchführung bestimmter Vorgänge zuweisen sollten, sind:

Betrieb	Zuweisung von Assets
Ressourcen schützen	Host, Richtlinie
Backup	Host, Ressourcengruppe und Richtlinie
Wiederherstellen	Host, Ressourcengruppe
Klon	Host, Ressourcengruppe und Richtlinie
Lebenszyklus von Klonen	Host
Erstellen Sie eine Ressourcengruppe	Host

- Wenn ein neuer Knoten zu einem Windows Cluster oder einer DAG (Exchange Server Database Availability Group)-Ressource hinzugefügt wird und wenn dieser neue Knoten einem Benutzer zugewiesen ist, müssen Sie das Element dem Benutzer oder der Gruppe neu zuweisen, um den neuen Knoten dem Benutzer oder der Gruppe hinzuzufügen.

Sie sollten den RBAC-Benutzer oder die Gruppe dem Cluster oder der DAG neu zuweisen, um den neuen Node auch dem RBAC-Benutzer oder der Gruppe einzuschließen. Sie verfügen beispielsweise über ein Cluster mit zwei Nodes und haben dem Cluster einen RBAC-Benutzer oder eine Gruppe zugewiesen. Wenn Sie dem Cluster einen weiteren Node hinzufügen, sollten Sie den RBAC-Benutzer oder die Gruppe dem Cluster neu zuweisen, um den neuen Node für den Benutzer oder die Gruppe der RBAC einzubeziehen.

- Wenn Sie planen, Snapshots zu replizieren, müssen Sie dem Benutzer, der den Vorgang durchführt, die Speicherverbindung für das Quell- und das Ziel-Volume zuweisen.

Sie sollten Assets hinzufügen, bevor Sie den Benutzern Zugriff zuweisen.



Wenn Sie zum Schutz von VMs, VMDKs oder Datastores das SnapCenter Plug-in für VMware vSphere verwenden, sollten Sie ein vCenter Benutzer zu einem SnapCenter Plug-in für VMware vSphere hinzufügen. Weitere Informationen zu VMware vSphere-Rollen finden Sie unter ["Vordefinierte Rollen in Paketen mit SnapCenter Plug-in für VMware vSphere"](#).

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Benutzer und Zugriff** > .
3. Auf der Seite Benutzer/Gruppen aus Active Directory oder Workgroup hinzufügen:

Für dieses Feld...	Tun Sie das...
Zugriffstyp	Wählen Sie entweder Domäne oder Arbeitsgruppe aus Für den Authentifizierungstyp Domäne müssen Sie den Domänennamen des Benutzers oder der Gruppe angeben, dem Sie den Benutzer zu einer Rolle hinzufügen möchten. Standardmäßig wird er mit dem angemeldeten Domänennamen ausgefüllt.  Sie müssen die nicht vertrauenswürdige Domäne auf der Seite Einstellungen > Globale Einstellungen > Domain-Einstellungen registrieren.

Für dieses Feld...	Tun Sie das...
Typ	Wählen Sie entweder Benutzer oder Gruppe aus  SnapCenter unterstützt nur Sicherheitsgruppen, nicht die Vertriebsgruppe.
Benutzername	a. Geben Sie den teilweisen Benutzernamen ein, und klicken Sie dann auf Hinzufügen.  Bei Benutzername wird die Groß-/Kleinschreibung berücksichtigt. b. Wählen Sie den Benutzernamen aus der Suchliste aus.  Wenn Sie Benutzer aus einer anderen Domäne oder einer nicht vertrauenswürdigen Domäne hinzufügen, sollten Sie den Benutzernamen vollständig eingeben, da keine Suchliste für domänenübergreifende Benutzer vorhanden ist. Wiederholen Sie diesen Schritt, um der ausgewählten Rolle weitere Benutzer oder Gruppen hinzuzufügen.
Rollen	Wählen Sie die Rolle aus, der Sie den Benutzer hinzufügen möchten.

4. Klicken Sie auf **Zuweisen** und dann auf der Seite „Assets zuweisen“ auf:

- Wählen Sie den Typ des Assets aus der Dropdown-Liste **Asset** aus.
- Wählen Sie in der Asset-Tabelle das Asset aus.

Die Assets werden nur aufgeführt, wenn der Benutzer die Assets zu SnapCenter hinzugefügt hat.

- Wiederholen Sie diesen Vorgang für alle erforderlichen Assets.
- Klicken Sie Auf **Speichern**.

5. Klicken Sie Auf **Absenden**.

Nachdem Sie Benutzer oder Gruppen hinzugefügt und Rollen zugewiesen haben, aktualisieren Sie die Ressourcenliste.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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