設定角色型存取控制（RBAC）

SnapCenter Software 4.8

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/zh-tw/snapcenter-48/install/task_add_a_user_or_group_and_assign_role_and_assets.html on September 26, 2025. Always check docs.netapp.com for the latest.

目錄

設定角色型存取控制（RBAC） . . . 1
- 新增使用者或群組、並指派角色和資產 . . . 1
- 建立角色 . . . 3
- 使用ONTAP 安全登入命令新增一個RBAC角色 . . . 4
- 以最低權限建立SVM角色 . . . 6
  - 用於建立SVM角色和指派權限的CLI命令ONTAP . . . 6
- 以ONTAP 最低權限建立叢集角色 . . . 10
  - 用於建立叢集角色和指派權限的CLI命令ONTAP . . . 10
- 設定「IIS應用程式集區」以啟用Active Directory讀取權限 . . . 16

設定角色型存取控制（RBAC）

新增使用者或群組、並指派角色和資產

若要設定SnapCenter 適用於哪些使用者的角色型存取控制、您可以新增使用者或群組並指派角色。角色決定SnapCenter 了使用者可以存取的選項。

您需要的是什麼

- 您必須以「SnapCenterAdmin」角色登入。
- 您必須在作業系統或資料庫的Active Directory中建立使用者或群組帳戶。您無法使用SnapCenter 不禁用功能來建立這些帳戶。

> 從S32 4.5開始SnapCenter 、您只能在使用者名稱和群組名稱中包含下列特殊字元：空格（ ）、連字號（-）、底線（_）和分號（：）。 如果您想要使用在SnapCenter 舊版的下列特殊字元中建立的角色、可以在SnapCenter 安裝了Web.config檔案中、將「isableSQLInjectionValidation」參數的值變更為true、以停用角色名稱驗證。修改值之後、您不需要重新啟動服務。

- 包含數個預先定義的角色。SnapCenter

  您可以將這些角色指派給使用者、或是建立新角色。

- 新增至SnapCenter RBAC的AD使用者和AD群組必須擁有Active Directory中「使用者容器」和「電腦容器」的讀取權限。
- 將角色指派給包含適當權限的使用者或群組之後、您必須指派使用者存取SnapCenter 諸如主機和儲存連線等各種資源。

  如此一來、使用者就能對指派給他們的資產執行其擁有權限的動作。

- 您應該在某個時間點指派角色給使用者或群組、以充分利用RBAC權限和效率。
- 您可以指派主機、資源群組、原則、儲存連線、外掛程式、 並在建立使用者或群組時向使用者提供認證。
- 您應指派使用者執行特定作業的最低資產如下：

營運	資產指派
保護資源	主機、原則
備份	主機、資源群組、原則
還原	主機、資源群組
複製	主機、資源群組、原則
複製生命週期	主機

營運	資產指派
建立資源群組	主機

- 當新節點新增至Windows叢集或DAG（Exchange Server資料庫可用度群組）資產、且此新節點已指派給使用者時、您必須將資產重新指派給使用者或群組、以便將新節點納入使用者或群組。

  您應該將RBAC使用者或群組重新指派給叢集或DAG、以便將新節點納入RBAC使用者或群組。例如、您有一個雙節點叢集、而且已將RBAC使用者或群組指派給叢集。當您將另一個節點新增至叢集時、應將RBAC使用者或群組重新指派至叢集、以納入RBAC使用者或群組的新節點。

- 如果您打算複寫Snapshot複本、則必須將來源和目的地Volume的儲存連線指派給執行作業的使用者。

  您應該先新增資產、再將存取權指派給使用者。

如果您使用SnapCenter VMware vSphere的VMware vSphere功能的VMware vCenter外掛程式來保護VM、VMDK或資料存放區、則應使用VMware vSphere GUI將vCenter使用者新增至SnapCenter VMware vSphere的「VMware vSphere的VMware vSphere插件」角色。如需VMware vSphere角色的相關資訊、請參閱 "VMware SnapCenter vSphere隨附於VMware vSphere的VMware vCenter外掛程式的預先定義角色"。

步驟

1. 在左側導覽窗格中、按一下*設定*。
2. 在「設定」頁面中、按一下「使用者與存取>*」 *。
3. 在「從Active Directory或工作群組新增使用者/群組」頁面中：

針對此欄位...	執行此動作...
存取類型	選取網域或工作群組 對於網域驗證類型、您應該指定要將使用者新增至角色的使用者或群組網域名稱。 依預設、系統會預先填入登入的網域名稱。 您必須在「設定>*全域設定*>*網域設定*」頁面中註冊不受信任的網域。
類型	選取使用者或群組 支援僅安全群組、不支援通訊群組。SnapCenter

針對此欄位...	執行此動作...
使用者名稱	a. 輸入部分使用者名稱、然後按一下「新增」。 使用者名稱區分大小寫。 b. 從搜尋清單中選取使用者名稱。 當您新增來自不同網域或不受信任網域的使用者時、應該完整輸入使用者名稱、因為沒有跨網域使用者的搜尋清單。 重複此步驟、將其他使用者或群組新增至選取的角色。
角色	選取您要新增使用者的角色。

4. 按一下「指派」、然後在「指派資產」頁面中：
   a. 從*資產*下拉式清單中選取資產類型。
   b. 在「資產」表格中、選取資產。

      只有在使用者將資產新增SnapCenter 至下列項目時、才會列出這些資產。

   c. 針對所有必要資產重複此程序。
   d. 按一下「 * 儲存 * 」。
5. 按一下*提交*。

新增使用者或群組並指派角色之後、請重新整理資源清單。

建立角色

除了使用現有SnapCenter 的功能、您還可以建立自己的角色、並自訂權限。

您應該以「SnapCenterAdmin」角色登入。

步驟

1. 在左側導覽窗格中、按一下*設定*。
2. 在「設定」頁面中、按一下「角色」。
3. 按一下 ＋。
4. 在「新增角色」頁面中、指定新角色的名稱和說明。

從S32 4.5開始SnapCenter 、您只能在使用者名稱和群組名稱中包含下列特殊字元：空格（ ）、連字號（-）、底線（_）和分號（：）。 如果您想要使用在SnapCenter 舊版的下列特殊字元中建立的角色、可以在SnapCenter 安裝了Web.config檔案中、將「isableSQLInjectionValidation」參數的值變更為true、以停用角色名稱驗證。修改值之後、您不需要重新啟動服務。

5. 選取*此角色的所有成員都可以看到其他成員的物件*、以便其他角色成員在重新整理資源清單之後、能夠查看資源、例如磁碟區和主機。

   如果不希望此角色的成員看到指派給其他成員的物件、則應取消選取此選項。

   啟用此選項時、如果使用者與建立物件或資源的使用者具有相同角色、則不需要指派使用者存取物件或資源的權限。

6. 在「權限」頁面中、選取您要指派給該角色的權限、或按一下*全選*、將所有權限授予該角色。
7. 按一下*提交*。

使用ONTAP 安全登入命令新增一個RBAC角色

當儲存系統執行叢集式的動作時、您可以使用安全登入命令來新增ONTAP 一個無法使用的RBAC角色ONTAP 。

您需要的是什麼

- 在您為ONTAP 執行叢集ONTAP 式功能的儲存系統建立一套不必要的RBAC角色之前、您必須先識別下列項目：
  - 您要執行的工作
  - 執行這些工作所需的權限
- 若要設定RBAC角色、您必須執行下列動作：
  - 授予命令和（或）命令目錄的權限。

    每個命令/命令目錄都有兩種存取層級：All存取和唯讀。

  您必須一律先指派所有存取權限。

  - 指派角色給使用者。
  - 根據SnapCenter 您的不確定插件是連接至整個叢集的叢集管理員IP、還是直接連接至叢集內的SVM、而有所不同。

關於此工作

為了簡化儲存系統上的角色設定、您可以使用Data ONTAP NetApp社群論壇上發佈的RBAC User Creator for Soliding工具。

此工具會自動ONTAP 正確處理設定功能不正確的功能。例如、RBAC User Creator for Data ONTAP BIOS工具會自動以正確順序新增權限、以便先顯示所有存取權限。如果您先新增唯讀權限、然後新增全存取權限、ONTAP 則將全存取權限標示為重複、並予以忽略。

如果您稍後升級SnapCenter 了版本的功能、ONTAP 應該重新執行RBAC User Creator for Data ONTAP BIOS工具、以更新您先前建立的使用者角色。為SnapCenter 舊版的版本的使用者角色無法ONTAP 在升級版本中正常運作。當您重新執行此工具時、它會自動處理升級作業。您不需要重新建立角色。

如需設定ONTAP RBAC角色的詳細資訊、請參閱 "《Administrator驗證與RBAC電源指南》（英文）ONTAP"。

為了保持一致性、SnapCenter 本文檔將角色稱為使用權限。這個「系統管理員GUI」OnCommand 使用術語_attributes_而非_privation_。在設定ONTAP 支援RBAC角色時、這兩個詞彙代表相同的意義。

步驟

1. 在儲存系統上、輸入下列命令以建立新角色：

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

   - SVM_name是SVM的名稱。如果您將此欄位保留空白、則預設為叢集管理員。
   - role名稱是您為角色指定的名稱。
   - Command ONTAP 是功能不一的功能。

     您必須針對每個權限重複此命令。請記住、All Access命令必須在唯讀命令之前列出。

   如需權限清單的相關資訊，請參閱 "用於建立角色和指派權限的CLI命令ONTAP"。

2. 輸入下列命令來建立使用者名稱：

```
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是您要建立的使用者名稱。
   - 是您的密碼。如果您未指定密碼、系統會提示您輸入密碼。
   - SVM_name是SVM的名稱。

3. 輸入下列命令、將角色指派給使用者：

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

   - 是您在步驟2中建立的使用者名稱。此命令可讓您修改使用者、使其與角色建立關聯。
   - SVM_name>是SVM的名稱。
   - <role名稱>是您在步驟1中建立的角色名稱。
   - 是您的密碼。如果您未指定密碼、系統會提示您輸入密碼。

4. 輸入下列命令、確認使用者已正確建立：

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

user_name是您在步驟3中建立的使用者名稱。

以最低權限建立SVM角色

在這個功能中為新的SVM使用者建立角色時、您必須執行幾ONTAP 個SfCLI命令ONTAP 。如果您將SVM設定ONTAP 為搭配SnapCenter 使用、但不想使用vsadmin角色、則需要此角色。

步驟

1. 在儲存系統上、建立角色並將所有權限指派給該角色。

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

   您應該針對每個權限重複此命令。

2. 建立使用者並將角色指派給該使用者。

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

3. 解除鎖定使用者。

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

用於建立SVM角色和指派權限的CLI命令ONTAP

您應該執行幾ONTAP 個SVM命令來建立SVM角色並指派權限。

- `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 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 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 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

以ONTAP 最低權限建立叢集角色

您應該建立ONTAP 具有最低權限的支援功能、以便不必使用ONTAP 這個功能來SnapCenter 執行動作。您可以執行數ONTAP 個CLI命令來建立ONTAP 一個不含指令集的叢集角色、並指派最低權限。

步驟

1. 在儲存系統上、建立角色並將所有權限指派給該角色。

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

   您應該針對每個權限重複此命令。

2. 建立使用者並將角色指派給該使用者。

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

3. 解除鎖定使用者。

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

用於建立叢集角色和指派權限的CLI命令ONTAP

您應該執行幾ONTAP 個CLI命令來建立叢集角色並指派權限。

- 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 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 "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 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 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`

設定「IIS應用程式集區」以啟用Active Directory讀取權限

您可以在Windows伺服器上設定Internet Information Services（IIS）、以便在需要啟用Active Directory的SnapCenter 讀取權限以供使用時建立自訂的應用程式集區帳戶。

步驟

1. 在SnapCenter 安裝了Windows*的Windows Server上開啟「IIS管理員」。
2. 在左導覽窗格中、按一下*應用程式集區*。
3. 在SnapCenter 「應用程式集區」清單中選取「功能」、然後按一下「動作」窗格中的「進階設定」。
4. 選取「Identity」、然後按一下「...」以編輯SnapCenter 該應用程式集區的身分識別。
5. 在「自訂帳戶」欄位中、輸入具有Active Directory讀取權限的網域使用者或網域管理員帳戶名稱。
6. 按一下「確定」。

   自訂帳戶會取代SnapCenter 適用於整個應用程式集區的內建ApplicationPoolIdentity帳戶。

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。