# 管理存取控制角色

ONTAP 9

NetApp
April 24, 2024

# 目錄

# 管理存取控制角色

## 管理存取控制角色總覽

指派給系統管理員的角色會決定系統管理員可以存取的命令。當您為系統管理員建立帳戶時、可以指派角色。您可以指派不同的角色、或視需要定義自訂角色。

## 修改指派給系統管理員的角色

您可以使用 `security login modify` 用於變更叢集或 SVM 系統管理員帳戶角色的命令。您可以指派預先定義或自訂的角色。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 變更叢集或SVM管理員的角色：

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   如需完整的命令語法、請參閱 "工作表"。

   "建立或修改登入帳戶"

   下列命令會變更 AD 叢集管理員帳戶的角色 `DOMAIN1\guest1` 至預先定義的 `readonly` 角色：

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   下列命令會變更 AD 群組帳戶中 SVM 管理員帳戶的角色 `DOMAIN1\adgroup` 自訂 `vol_role` 角色：

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

## 定義自訂角色

您可以使用 `security login role create` 定義自訂角色的命令。您可以視需要多次執行命令、以取得想要與角色建立關聯的確切功能組合。

關於這項工作

- 無論是預先定義或自訂的角色、都會授予或拒絕ONTAP 存取各種指令或命令目錄。

  命令目錄 (`volume`（例如）是一組相關命令和命令子目錄。除非如本程序所述、否則授與或拒絕存取命令目錄會授與或拒絕存取目錄及其子目錄中的每個命令。

- 特定命令存取或子目錄存取會覆寫父目錄存取。

  如果某個角色是以命令目錄定義、然後以不同的存取層級再次定義、以用於特定命令或父目錄的子目錄、則為該命令或子目錄指定的存取層級會覆寫父目錄的存取層級。

> 您無法為 SVM 管理員指派一個角色、讓其存取僅供使用的命令或命令目錄 `admin` 叢集管理員、例如 `security` 命令目錄。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 定義自訂角色：

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   如需完整的命令語法、請參閱 "工作表"。

   下列命令會授與 `vol_role` 角色完整存取中的命令 `volume` 命令目錄及中命令的唯讀存取權 `volume snapshot` 子目錄。

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   下列命令會授與 `SVM_storage` 角色對中命令的唯讀存取權 `storage` 命令目錄、無法存取中的命令 `storage encryption` 子目錄、以及對的完整存取權 `storage aggregate plex offline` 非固有命令。

   ```
   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage" -access readonly

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage encryption" -access none

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage aggregate plex offline" -access all
   ```

# 叢集管理員的預先定義角色

叢集管理員的預先定義角色應能滿足您大部分的需求。您可以視需要建立自訂角色。依預設、會指派預先定義的叢集管理員 `admin` 角色：

下表列出叢集管理員的預先定義角色：

| 此角色... | 具有此存取層級... | 至下列命令或命令目錄 |
|---|---|---|
| 管理 | 全部 | 所有命令目錄 (`DEFAULT`) |
| admin-no FSA（ONTAP 從功能性的9.12.1開始提供） | 讀取/寫入 | • 所有命令目錄 (`DEFAULT`)<br>• `security login rest-role`<br>• `security login role` |
| 唯讀 | • `security login rest-role create`<br>• `security login rest-role delete`<br>• `security login rest-role modify`<br>• `security login rest-role show`<br>• `security login role create`<br>• `security login role create`<br>• `security login role delete`<br>• `security login role modify`<br>• `security login role show`<br>• `volume activity-tracking`<br>• `volume analytics` | 無 |
| `volume file show-disk-usage` | AutoSupport | 全部 |

| | | |
|---|---|---|
| • set<br>• system node autosupport | 無 | 所有其他命令目錄 (DEFAULT) |
| 備份 | 全部 | vserver services ndmp |
| 唯讀 | volume | 無 |
| 所有其他命令目錄 (DEFAULT) | 唯讀 | 全部 |
| • security login password<br>僅用於管理自己的使用者帳戶本機密碼和金鑰資訊<br>• set | 無 | security |
| 唯讀 | 所有其他命令目錄 (DEFAULT) | 無 |

。 autosupport 角色會指派給預先定義的 autosupport 帳戶、由 AutoSupport OnDemand 使用。ONTAP 可防止您修改或刪除 autosupport 帳戶。ONTAP 也會防止您指派 autosupport 其他使用者帳戶的角色。

# SVM系統管理員的預先定義角色

SVM系統管理員的預先定義角色應能滿足您大部分的需求。您可以視需要建立自訂角色。根據預設、系統會指派預先定義的 SVM 管理員 vsadmin 角色：

下表列出SVM系統管理員的預先定義角色：

| 角色名稱 | 功能 |
|---|---|

| | |
|---|---|
| vsadmin | • 管理自己的使用者帳戶本機密碼和金鑰資訊<br>• 管理磁碟區、磁碟區移動除外<br>• 管理配額、qtree、Snapshot複本和檔案<br>• 管理LUN<br>• 執行SnapLock 不含權限刪除的功能<br>• 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP<br>• 設定服務：DNS、LDAP及NIS<br>• 監控工作<br>• 監控網路連線和網路介面<br>• 監控SVM的健全狀況 |
| vsadmin-volume | • 管理自己的使用者帳戶本機密碼和金鑰資訊<br>• 管理磁碟區、包括磁碟區移動<br>• 管理配額、qtree、Snapshot複本和檔案<br>• 管理LUN<br>• 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP<br>• 設定服務：DNS、LDAP及NIS<br>• 監控網路介面<br>• 監控SVM的健全狀況 |
| vsadmin-Protocol | • 管理自己的使用者帳戶本機密碼和金鑰資訊<br>• 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP<br>• 設定服務：DNS、LDAP及NIS<br>• 管理LUN<br>• 監控網路介面<br>• 監控SVM的健全狀況 |
| vsadmin-Backup | • 管理自己的使用者帳戶本機密碼和金鑰資訊<br>• 管理NDMP作業<br>• 使還原的Volume能夠讀取/寫入<br>• 管理SnapMirror關係和Snapshot複本<br>• 檢視磁碟區和網路資訊 |

| | |
|---|---|
| vsadmin-SnapLock | • 管理自己的使用者帳戶本機密碼和金鑰資訊<br>• 管理磁碟區、磁碟區移動除外<br>• 管理配額、qtree、Snapshot複本和檔案<br>• 執行SnapLock 包含特權刪除在內的功能<br>• 設定傳輸協定：NFS和SMB<br>• 設定服務：DNS、LDAP及NIS<br>• 監控工作<br>• 監控網路連線和網路介面 |
| vsadmin-readonly | • 管理自己的使用者帳戶本機密碼和金鑰資訊<br>• 監控SVM的健全狀況<br>• 監控網路介面<br>• 檢視磁碟區和LUN<br>• 檢視服務與傳輸協定 |

# 控制系統管理員存取權

指派給系統管理員的角色會決定系統管理員可以使用System Manager執行哪些功能。叢集管理員和儲存VM管理員的預先定義角色由System Manager提供。 您可以在建立系統管理員帳戶時指派角色、也可以稍後指派不同的角色。

視啟用帳戶存取的方式而定、您可能需要執行下列任一項：

- 將公開金鑰與本機帳戶建立關聯。
- 安裝CA簽署的伺服器數位憑證。
- 設定AD、LDAP或NIS存取。

您可以在啟用帳戶存取之前或之後執行這些工作。

## 指派角色給系統管理員

指派角色給系統管理員、如下所示：

步驟

1. 選擇*叢集>設定*。
2. 選取 → 緊鄰*使用者與角色*。
3. 選取 + Add 在*使用者*下。
4. 指定使用者名稱、然後在下拉式功能表中選取*角色*的角色。
5. 指定使用者的登入方法和密碼。

## 變更系統管理員的角色

變更系統管理員的角色、如下所示：

步驟

1. 按一下*叢集>設定*。
2. 選取您要變更其角色的使用者名稱、然後按一下 ⋮ 顯示在使用者名稱旁。
3. 按一下 * 編輯 * 。
4. 在下拉式功能表中選取*角色*的角色。