管理存取控制角色
ONTAP 9

NetApp
February 12, 2026

目錄

管理存取控制角色

瞭解如何管理 ONTAP 存取控制角色

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 ONTAP 管理員的角色

您可以使用 `security login modify`命令來變更叢集或 SVM 管理員帳戶的角色。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
   ```

   "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
   ```

   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

為 ONTAP 管理員定義自訂角色

您可以使用 `security login role create`命令來定義自訂角色。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
   ```

   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
   ```

   如"指令參考資料ONTAP"需詳細 `security login role create`資訊，請參閱。

相關資訊

- "建立安全登入角色"
- "離線儲存Aggregate叢"
- "儲存加密"

預先定義的 ONTAP 叢集管理員角色

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 （從 ONTAP 9.12.1 開始提供）	讀取/寫入	• 所有命令目錄 (`DEFAULT`) • `security login rest-role` • `security login role`

唯讀	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	無
volume file show-disk-usage	AutoSupport	全部
• set • 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 僅用於管理自己的使用者帳戶本機密碼和金鑰資訊 • set	• 從 ONTAP 9.8 開始，只讀 • ONTAP 9.8 之前，無	security

唯讀	所有其他命令目錄 (DEFAULT)	SnapLock
全部	• set • volume create • volume modify • volume move • volume show	無
• volume move governor • volume move recommend	無	所有其他命令目錄 (DEFAULT)
無	無	所有命令目錄 (DEFAULT)

。 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。

相關資訊

- "安全登入"
- "設定"
- "Volume"
- "Vserver 服務 NDMP"

預先定義的 ONTAP SVM 管理員角色

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 • 管理磁碟區、磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 管理LUN • 執行SnapLock 不含權限刪除的功能 • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務：DNS、LDAP及NIS • 監控工作 • 監控網路連線和網路介面 • 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 • 管理磁碟區、磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 管理LUN • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務：DNS、LDAP及NIS • 監控網路介面 • 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 • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務：DNS、LDAP及NIS • 管理LUN • 監控網路介面 • 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 • 管理NDMP作業 • 使還原的Volume能夠讀取/寫入 • 管理 SnapMirror 關係和快照 • 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 • 管理磁碟區、磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 執行SnapLock 包含特權刪除在內的功能 • 設定傳輸協定：NFS和SMB • 設定服務：DNS、LDAP及NIS • 監控工作 • 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 • 監控SVM的健全狀況 • 監控網路介面 • 檢視磁碟區和LUN • 檢視服務與傳輸協定

使用系統管理員管理 ONTAP 管理員存取

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 → * 使用者與角色 * 旁的。
3. 在 * 使用者 * 下選取 + Add 。
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 ⋮ 出現在使用者名稱旁的。
3. 按一下 * 編輯 * 。
4. 在下拉式功能表中選取*角色*的角色。

在ONTAP中存取 JIT 權限提升

從ONTAP 9.17.1 開始，叢集管理員可以"配置即時（JIT）權限提升"允許ONTAP使用者暫時提升其權限以執行某些任務。為使用者設定 JIT 後，使用者可以將其權限暫時提升到具有執行任務所需權限的角色。會話到期後，使用者將恢復其原始存取等級。

叢集管理員可以設定使用者存取 JIT 提升的時長。例如，叢集管理員可以將使用者存取 JIT 提升的權限配置為每次會話 30 分鐘（會話有效期），為期 30 天（JIT 有效期）。在 30 天的期限內，使用者可以根據需要多次提升權限，但每次會話的時長限制為 30 分鐘。

關於這項工作

- JIT 權限提升僅適用於使用 SSH 存取ONTAP的使用者。提升的權限僅在目前 SSH 會話中可用，但您可以根據需要在任意數量的並發 SSH 會話中提升權限。
- JIT 權限提升僅支援使用密碼、nsswitch 或網域驗證登入的使用者。 JIT 權限提升不支援多重身分驗證 (MFA)。
- 如果設定的會話或 JIT 有效期到期，或叢集管理員撤銷使用者的 JIT 存取權限，則使用者的 JIT 會話將會終止。

開始之前

- 若要存取 JIT 權限提升，叢集管理員必須為您的帳戶設定 JIT 存取權限。叢集管理員將確定您可以提升權限的角色，以及您可以存取提升權限的時間長度。

步驟

1. 暫時將您的權限提升至配置的角色：

   ```
   security jit-privilege elevate
   ```

   輸入此指令後，系統會提示您輸入登入密碼。如果您的帳戶配置了 JIT 存取權限，您將在配置的會話時間長度內獲得提升的存取權限。會話時長到期後，您將恢復到原始存取等級。您可以在設定的 JIT 有效期內根據需要多次提升權限。

2. 查看 JIT 會話中的剩餘時間：

   ```
   security jit-privilege show-remaining-time
   ```

如果您目前處於 JIT 會話中，此命令將顯示剩餘時間。

3. 如果需要，請提前結束 JIT 會話：

```
security jit-privilege reset
```

如果您目前處於 JIT 會話中，此命令將結束 JIT 會話並恢復您的原始存取等級。

在ONTAP中設定 JIT 權限提升

從ONTAP 9.17.1 開始，叢集管理員可以設定即時 (JIT) 權限提升，以允許ONTAP使用者暫時提升其權限以執行某些任務。為使用者配置 JIT 後，他們可以臨時"提升他們的特權"賦予具有執行任務所需權限的角色。會話持續時間到期後，使用者將恢復其原始存取等級。

叢集管理員可以設定使用者存取 JIT 提升的時長。例如，您可以設定使用者存取 JIT 提升的時長，在 30 天的時間內（即「JIT 有效期」），每次會話的時長限制為 30 分鐘（即「會話有效期限」）。在這 30 天的時間段內，使用者可以根據需要多次提升權限，但每次會話的時間限制為 30 分鐘。

JIT 權限提升支援最小權限原則，讓使用者執行需要提升權限的任務，而無需永久授予這些權限。這有助於降低未經授權的存取或意外更改系統的風險。以下範例描述了 JIT 權限提升的一些常見用例：

- 允許臨時訪問 `security login create`和 `security login delete`命令來啟用使用者的入職和離職。
- 允許臨時訪問 `system node image update`和 `system node upgrade-revert`在更新視窗期間。更新完成後，命令存取權限將被撤銷。
- 允許臨時訪問 `cluster add-node`， `cluster remove-node`， 和 `cluster modify`以啟用叢集擴充或重新配置。叢集變更完成後，命令存取權限將被撤銷。
- 允許臨時訪問 `volume snapshot restore`啟用還原作業和備份目標管理。還原或設定完成後，命令存取權限將被撤銷。
- 允許臨時訪問 `security audit log show`在合規性檢查期間啟用稽核日誌審查和匯出。

如需查看更詳細的常見 JIT 用例列表，請參閱常見的 JIT 用例 。

叢集管理員可以為ONTAP使用者設定 JIT 存取權限，並在整個叢集範圍內或為特定 SVM 配置預設 JIT 有效期。

關於這項工作

- JIT 權限提升僅適用於使用 SSH 存取ONTAP的使用者。提升的權限僅在使用者目前的 SSH 會話中可用，但使用者可以根據需要在任意數量的並發 SSH 會話中提升權限。
- JIT 權限提升僅支援使用密碼、nsswitch 或網域驗證登入的使用者。 JIT 權限提升不支援多重身分驗證 (MFA)。

開始之前

- 您必須是ONTAP叢集管理員 `admin`權限等級來執行下列任務。

修改全域 JIT 設定

您可以修改ONTAP叢集全域或特定 SVM 的預設 JIT 設定。這些設定決定了已配置 JIT 存取的使用者的預設會話有效期和最大 JIT 有效期。

關於這項工作

- 預設 `default-session-validity-period`值為一小時。此設定決定使用者在 JIT 會話中可以存取提升權限的時間，之後需要重新提升權限。
- 預設 `max-jit-validity-period`值為 90 天。此設定決定了使用者在配置的開始日期之後可以存取 JIT 提升權限的最長期限。您可以為單一使用者設定 JIT 有效期，但不能超過最長 JIT 有效期。

步驟

1. 檢查目前 JIT 設定：

```
security jit-privilege show -vserver <svm_name>
```

`-vserver`是可選的。如果您未指定 SVM，則命令將顯示全域 JIT 設定。

2. 全域或針對 SVM 修改 JIT 設定：

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

如果您未指定 SVM，則命令將修改全域 JIT 設定。以下範例將 SVM 的預設 JIT 會話時長設定為 45 分鐘，最大 JIT 長度設定為 30 天 `svm1` ：+
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

在此範例中，使用者將能夠一次存取 45 分鐘的 JIT 提升，並且可以在配置的開始日期之後最多 30 天內啟動 JIT 工作階段。

為使用者配置 JIT 權限提升存取權限

您可以為ONTAP使用者指派 JIT 權限提升存取權限。

步驟

1. 檢查使用者目前的 JIT 存取權限：

```
security jit-privilege user show -username <username>
```

`-username`是可選的。如果您未指定使用者名，該命令將顯示所有使用者的 JIT 存取權限。

2. 為使用者指派新的 JIT 存取權限：

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- 如果 `-vserver`未指定，則在叢集層級分配 JIT 存取。
- `-role`是使用者將被提升到的 RBAC 角色。如果未指定， `-role`預設為 `admin`。
- `-session-validity-period`是使用者在需要啟動新的 JIT 會話之前可以存取提升角色的時間長度。如果未指定，則全域或 SVM `default-session-validity-period`被使用。
- `-jit-validity-period`是使用者在配置的開始日期之後可以發起 JIT 會話的最長持續時間。如果未指定，則 `session-validity-period`被使用。此參數不能超過全域或 SVM `max-jit-validity-period`。
- `-start-time`是使用者可以啟動 JIT 會話的日期和時間。如果未指定，則使用目前日期和時間。

  下面的例子將允許 `ontap_user`訪問 `admin`角色運行 1 小時後才需要開始新的 JIT 會話。`ontap_user`將能夠從 2025 年 7 月 1 日下午 1 點開始啟動為期 60 天的 JIT 會話：+
  `security jit-privilege user create -username ontap_user -role admin -session-validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. 如果需要，撤銷使用者的 JIT 存取權限：

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

此命令將撤銷使用者的 JIT 存取權限，即使其存取權限尚未過期。如果 `-vserver`如果未指定，則 JIT 存取權限將在叢集層級撤銷。如果使用者處於活動的 JIT 會話中，則該會話將被終止。

常見的 JIT 用例

下表包含 JIT 權限提升的常見用例。對於每個用例，都需要配置一個 RBAC 角色來提供對相關命令的存取權限。每個命令都連結到ONTAP命令參考，其中包含有關該命令及其參數的更多資訊。

使用案例	命令	細節
使用者和角色管理	• `security login create` • `security login delete`	在入職或離職期間暫時提升新增/刪除使用者或變更角色的權限。
證書管理	• `security certificate create` • `security certificate install`	授予證書安裝或更新的短期存取權限。

使用案例	命令	細節
SSH/CLI 存取控制	• `security login create -application ssh`	暫時授予 SSH 存取權限以進行故障排除或供應商支援。
授權管理	• `system license add` • `system license delete`	授予在功能啟動或停用期間新增或刪除許可證的權限。
系統升級和修補	• `system node image update` • `system node upgrade-revert`	提升升級窗口，然後撤銷。
網路安全設定	• `security login role create` • `security login role modify`	允許對網路相關的安全角色進行臨時更改。
叢集管理	• `cluster add-node` • `cluster remove-node` • `cluster modify`	提升叢集擴充或重新配置。
SVM 管理	• `vserver create` • `vserver delete` • `vserver modify`	暫時授予 SVM 管理員權限以進行設定或停用。
磁碟區管理	• `volume create` • `volume delete` • `volume modify`	提升磁碟區配置、調整大小或刪除的權限。
快照管理	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	提升快照刪除或在復原期間復原的權限。
網路組態	• `network interface create` • `network port vlan create`	授予在維護時段內進行網路變更的權利。

使用案例	命令	細節
磁碟/聚合管理	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	提升新增或刪除磁碟或管理聚合的能力。
資料保護	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	暫時提升以配置或恢復SnapMirror關係。
效能調優	• `qos policy-group create` • `qos policy-group modify`	提升性能故障排除或調整。
審計日誌訪問	• `security audit log show`	在合規性檢查期間暫時提升稽核日誌審查或匯出權限。
事件和警報管理	• `event notification create` • `event notification modify`	提升設定或測試事件通知或 SNMP 陷阱的權限。
合規性驅動的數據訪問	• `volume show` • `security audit log show`	授予審計員臨時唯讀存取權限以審查敏感資料或日誌。
特權訪問審查	• `security login show` • `security login role show`	暫時提升權限以審查和報告特權存取權限。在限定時間內授予唯讀權限。

相關資訊

- "叢集"
- "事件通知"
- "網路"
- "QoS策略組"
- "安全性"
- "SnapMirror"
- "貯存"
- "系統"
- "Volume"

- "Vserver"

版權資訊

商標資訊