管理系統管理員帳戶
ONTAP 9

NetApp
February 12, 2026

目錄

管理系統管理員帳戶

瞭解如何管理 ONTAP 系統管理員帳戶

視啟用帳戶存取的方式而定、您可能需要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、或設定AD、LDAP或NIS存取。您可以在啟用帳戶存取之前或之後執行所有這些工作。

將公開金鑰與 ONTAP 系統管理員帳戶建立關聯

若要進行SSH公開金鑰驗證、您必須先將公開金鑰與系統管理員帳戶建立關聯、帳戶才能存取SVM。您可以使用 `security login publickey create`命令將金鑰與系統管理員帳戶建立關聯。

關於這項工作

如果您同時使用密碼和SSH公開金鑰透過SSH驗證帳戶、則會先使用公開金鑰驗證帳戶。

開始之前

- 您必須已產生SSH金鑰。
- 您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 將公開金鑰與系統管理員帳戶建立關聯：

   ```
   security login publickey create -vserver SVM_name -username user_name -index
   index -publickey certificate -comment comment
   ```

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

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

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

範例

下列命令會將公開金鑰與 SVM 管理員帳戶建立關聯 `svmadmin1` 適用於 SVM `engData1`。公開金鑰已指派索引編號5。

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

管理 ONTAP 系統管理員的 SSH 公開金鑰和 X.509 憑證

為了提高使用系統管理員帳戶的 SSH 驗證安全性，您可以使用 `security login publickey` 一組命令來管理 SSH 公開金鑰及其與 X.509 憑證的關聯性。

將公開金鑰和 X.509 憑證與系統管理員帳戶建立關聯

從 ONTAP 9.13.1 開始、您可以將 X.509 憑證與您與系統管理員帳戶相關聯的公開金鑰建立關聯。這可讓您在登入該帳戶的 SSH 時、更安全地進行憑證過期或撤銷檢查。

關於這項工作

如果您透過 SSH 同時使用 SSH 公開金鑰和 X.509 憑證來驗證帳戶、 ONTAP 會在使用 SSH 公開金鑰進行驗證之前、先檢查 X.509 憑證的有效性。如果該憑證過期或撤銷、 SSH 登入將會被拒絕、而且會自動停用公開金鑰。

開始之前

- 您必須是叢集或SVM管理員、才能執行此工作。
- 您必須已產生SSH金鑰。
- 如果您只需要檢查 X.509 憑證是否過期、您可以使用自我簽署的憑證。
- 如果您需要檢查 X.509 憑證是否過期及撤銷：
  - 您必須已從憑證授權單位（ CA ）收到憑證。
  - 您必須使用命令來安裝憑證鏈結（中繼和根 CA 憑證） `security certificate install`。如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。
  - 您需要啟用 SSH 的 OCSP 。請參閱 "使用OCSP驗證數位憑證是否有效" 以取得相關指示。

步驟

1. 將公開金鑰和 X.509 憑證與系統管理員帳戶建立關聯：

   ```
   security login publickey create -vserver SVM_name -username user_name -index
   index -publickey certificate -x509-certificate install
   ```

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

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

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

範例

下列命令會將公開金鑰和 X.509 憑證與 SVM 系統管理員帳戶建立關聯 `svmadmin2` 適用於 SVM `engData2`。公開金鑰會被指派索引編號 6 。

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

從系統管理員帳戶的 SSH 公開金鑰中移除憑證關聯

您可以從帳戶的 SSH 公開金鑰中移除目前的憑證關聯、同時保留公開金鑰。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 從系統管理員帳戶移除 X.509 憑證關聯、並保留現有的 SSH 公開金鑰：

   ```
   security login publickey modify -vserver SVM_name -username user_name -index
   index -x509-certificate delete
   ```

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

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

範例

下列命令會從 SVM 系統管理員帳戶移除 X.509 憑證關聯 `svmadmin2` 適用於 SVM `engData2` 索引編號 6 。

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

從系統管理員帳戶移除公開金鑰和憑證關聯

您可以從帳戶移除目前的公開金鑰和憑證組態。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 從系統管理員帳戶移除公開金鑰和 X.509 憑證關聯：

   ```
   security login publickey delete -vserver SVM_name -username user_name -index
   index
   ```

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

2. 檢視公開金鑰以驗證變更：

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

範例

下列命令會從 SVM 系統管理員帳戶移除公開金鑰和 X.509 憑證 `svmadmin3` 適用於 SVM `engData3` 索引編號 7 。

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

相關資訊

- "安全登入公鑰"

為 ONTAP SSH 登入設定 Cisco 雙核心 2FA

從 ONTAP 9.14.1 開始、您可以將 ONTAP 設定為在登入 SSH 期間使用 Cisco 雙核心進行雙重驗證（ 2FA ）。您可以在叢集層級設定雙核心、而且預設會套用至所有使用者帳戶。或者、您也可以在儲存 VM 層級（之前稱為 vserver ）設定雙核心、在這種情況下、它只適用於該儲存 VM 的使用者。如果您啟用和設定雙核心、它會作為額外的驗證方法、以補充所有使用者的現有方法。

如果您為 SSH 登入啟用雙核心驗證、使用者下次使用 SSH 登入時、將需要註冊裝置。如需報名資訊、請參閱 Cisco Duo "註冊文件"。

您可以使用 ONTAP 命令列介面來執行 Cisco 雙核心的下列工作：

- 設定 Cisco Duo
- 變更 Cisco Duo 組態
- 移除 Cisco Duo 組態
- 查看 Cisco Duo 組態
- 移除 " 雙核心 " 群組
- [檢視雙核心群組]
- [略過使用者的雙核心驗證]

設定 Cisco Duo

您可以使用命令為整個叢集或特定儲存 VM （在 ONTAP CLI 中稱為 Vserver ）建立 Cisco 雙核心組態 `security login duo create`。當您這麼做時、 Cisco Duo 會啟用此叢集或儲存 VM 的 SSH 登入。如"指令參考資料ONTAP"需詳細 `security login duo create`資訊，請參閱。

步驟

1. 登入 Cisco Duo 管理面板。

2. 前往 * 應用程式 > UNIX 應用程式 * 。
3. 記錄您的整合金鑰、秘密金鑰和 API 主機名稱。
4. 使用 SSH 登入您的 ONTAP 帳戶。
5. 啟用此儲存 VM 的 Cisco Duo 驗證、以環境中的資訊取代方括號中的值：

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

變更 Cisco Duo 組態

您可以變更 Cisco Duo 驗證使用者的方式（例如、提供多少驗證提示、或使用什麼 HTTP Proxy ）。如果您需要變更儲存 VM 的 Cisco 雙核心組態（在 ONTAP CLI 中稱為 vserver ），您可以使用 `security login duo modify`命令。如"指令參考資料ONTAP"需詳細 `security login duo modify`資訊，請參閱。

步驟

1. 登入 Cisco Duo 管理面板。
2. 前往 * 應用程式 > UNIX 應用程式 * 。
3. 記錄您的整合金鑰、秘密金鑰和 API 主機名稱。
4. 使用 SSH 登入您的 ONTAP 帳戶。
5. 變更此儲存 VM 的 Cisco Duo 組態、以您環境中的更新資訊取代方括號中的值：

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-max-prompts 1|2|3 \
-is-enabled true|false \
-fail-mode safe|secure
```

移除 Cisco Duo 組態

您可以移除 Cisco Duo 組態、這樣就不需要 SSH 使用者在登入時使用 DuoTM 進行驗證。若要移除儲存 VM 的 Cisco 雙核心組態（在 ONTAP CLI 中稱為 vserver ），您可以使用 `security login duo delete`命令。如"指令參考資料ONTAP"需詳細 `security login duo delete`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 移除此儲存 VM 的 Cisco Duo 組態、以您的儲存 VM 名稱取代 `<STORAGE_VM_NAME>`：

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

這會永久刪除此儲存 VM 的 Cisco Duo 組態。

查看 Cisco Duo 組態

您可以使用命令檢視儲存 VM （在 ONTAP CLI 中稱為 vserver ）的現有 Cisco 雙核心組態 `security login duo show`。如"指令參考資料ONTAP"需詳細 `security login duo show`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 顯示此儲存 VM 的 Cisco Duo 組態。您也可以選擇使用 `vserver` 用於指定儲存 VM 的參數、請將儲存 VM 名稱取代為 `<STORAGE_VM_NAME>`：

```
security login duo show -vserver <STORAGE_VM_NAME>
```

您應該會看到類似下列的輸出：

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

建立雙核心群組

您可以指示 Cisco DuoTM 僅在特定 Active Directory 、 LDAP 或本機使用者群組中加入使用者、以進行 DuoTM 驗證程序。如果您建立雙核心群組、系統只會提示該群組中的使用者進行雙核心驗證。您可以使用命令建立雙核心群組 `security login duo group create`。建立群組時、您可以選擇性地將該群組中的特定使用者排除

在雙核心驗證程序之外。如"指令參考資料ONTAP"需詳細 `security login duo group create`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 建立 DuoTM 群組、以環境中的資訊取代方括號中的值。如果您省略 `-vserver` 參數、群組會在叢集層級建立：

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。您使用選用參數指定的使用者 `-excluded-users`將不會納入雙核心驗證程序。

檢視雙核心群組

您可以使用命令來檢視現有的 Cisco 雙核心群組項目 `security login duo group show`。如"指令參考資料ONTAP"需詳細 `security login duo group show`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 顯示 DUO 群組項目、以環境中的資訊取代方括號中的值。如果您省略 `-vserver` 參數、群組會顯示在叢集層級：

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。您使用選用參數指定的使用者 `-excluded-users`將不會顯示。

移除 " 雙核心 " 群組

您可以使用命令移除雙核心群組項目 `security login duo group delete`。如果您移除群組、該群組中的使用者將不再包含在雙核心驗證程序中。如"指令參考資料ONTAP"需詳細 `security login duo group delete`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 移除 DuoTM 群組項目、以環境中的資訊取代方括號中的值。如果您省略 `-vserver` 參數、群組會在叢集層級移除：

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。

略過使用者的雙核心驗證

您可以將所有使用者或特定使用者排除在雙核心 SSH 驗證程序之外。

排除所有雙核心使用者

您可以為所有使用者停用 Cisco 雙核心 SSH 驗證。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 停用 SSH 使用者的 Cisco Duo 驗證、以 vserver 名稱取代 `<STORAGE_VM_NAME>`：

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

不包括雙核心群組使用者

您可以從雙核心 SSH 驗證程序中排除屬於雙核心群組的特定使用者。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 針對群組中的特定使用者停用 Cisco Duo 驗證。以群組名稱和使用者清單取代方括號中的值：

```
security login duo group modify -group-name <GROUP_NAME> -excluded-users
<USER1, USER2>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。您使用參數指定的使用者 `-excluded-users`將不會包含在雙核心驗證程序中。

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

排除本機雙核心使用者

您可以使用 Cisco 雙核心管理面板、排除特定的本機使用者使用雙核心驗證。如需相關指示、請參閱 "Cisco Duo 文件"。

在 ONTAP 中產生並安裝 CA 簽署的伺服器憑證

在正式作業系統上、最佳做法是安裝CA簽署的數位憑證、以用於將叢集或SVM驗證為SSL伺服器。您可以使用命令來產生憑證簽署要求（ CSR ），並 `security certificate install`使用 `security certificate generate-csr`命令來安裝從憑證授權單位收到的憑證。深入瞭解 `security certificate generate-csr`及 `security`

`certificate install` "指令參考資料ONTAP"。

產生憑證簽署要求

您可以使用 `security certificate generate-csr` 產生憑證簽署要求（ CSR ）的命令。在處理您的要求之後、憑證授權單位（CA）會傳送簽署的數位憑證給您。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 產生CSR：

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

下列命令會建立 CSR ，其中包含由雜湊函數產生的 2048 位元私密金鑰 `SHA256`，供自訂一般名稱為的公司部門 `server1.companyname.com`中的群組 `IT`使用 `Software`，位於美國加州森尼維爾。SVM 連絡人管理員的電子郵件地址為 `web@example.com`。系統會在輸出中顯示CSR和私密金鑰。

建立 **CSR** 的範例

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. 從CSR輸出複製憑證要求、然後以電子形式（例如電子郵件）將其傳送至信任的協力廠商CA進行簽署。

在處理您的要求之後、CA會將簽署的數位憑證傳送給您。您應該保留一份私密金鑰和CA簽署的數位憑證複本。

安裝CA簽署的伺服器憑證

您可以使用 `security certificate install`命令在 SVM 上安裝 CA 簽署的伺服器憑證。系統會提示您輸入憑證授權單位（CA）根憑證和中繼憑證、以構成伺服器憑證的憑證鏈結。ONTAP如"指令參考資料ONTAP"需詳細`security certificate install`資訊，請參閱。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 安裝 CA 簽署的伺服器憑證：

```
security certificate install -vserver SVM_name -type certificate_type
```

> 系統會提示您輸入CA根憑證和中繼憑證、這些憑證構成伺服器憑證的憑證鏈結。ONTAP鏈結從發行伺服器憑證的CA憑證開始、範圍最多可達CA的根憑證。任何遺失的中繼憑證都會導致伺服器憑證安裝失敗。

以下命令可在 SVM 上安裝 CA 簽署的伺服器憑證和中繼憑證 `engData2`。

安裝 **CA** 簽署的伺服器憑證中繼憑證的範例

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

相關資訊

- "產生安全性憑證-CSR"

使用系統管理員管理 ONTAP 憑證

從ONTAP 版本號《21：10.1》開始、您可以使用System Manager來管理信任的憑證授權單位、用戶端/伺服器憑證、以及本機（內建）憑證授權單位。

有了System Manager、您可以管理從其他應用程式接收到的憑證、以便驗證這些應用程式的通訊。 您也可以管理自己的憑證、以便將系統識別給其他應用程式。

檢視憑證資訊

使用System Manager、您可以檢視儲存在叢集上的信任憑證授權單位、用戶端/伺服器憑證和本機憑證授權單位。

步驟

1. 在System Manager中、選取*叢集>設定*。
2. 捲動至* Security（安全性）區域。
   在「*憑證」區段中、會顯示下列詳細資料：
   - 儲存的信任憑證授權單位數目。
   - 儲存的用戶端/伺服器憑證數目。
   - 儲存的本機憑證授權單位數目。
3. 選取任何數字以檢視有關某一類別憑證的詳細資料、或選取 → 以開啟包含所有類別資訊的 * 憑證 * 頁面。
   清單會顯示整個叢集的資訊。如果您只想顯示特定儲存VM的資訊、請執行下列步驟：
   a. 選取 * 儲存 > 儲存 VM* 。
   b. 選取儲存VM。
   c. 切換至 * 設定 * 索引標籤。
   d. 選取 * 憑證 * 區段中顯示的數字。

接下來該怎麼做

- 您可以從*憑證*頁面 [產生憑證簽署要求]。
- 憑證資訊分成三個索引標籤、每個類別各一個。 您可以從每個索引標籤執行下列工作：

在此索引標籤上…	您可以執行下列程序…
受信任的憑證授權單位	• [install-trusted-cert] • [刪除信任的憑證授權單位] • [續約信任的憑證授權單位]
用戶端/伺服器憑證	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]

當地證書管理機構	• [建立新的本機憑證授權單位] • [使用本機憑證授權單位簽署憑證] • [刪除本機憑證授權單位] • [更新本機憑證授權單位]

產生憑證簽署要求

您可以從「憑證」頁面的任何索引標籤、使用System Manager產生憑證簽署要求（CSR）。系統會產生私密金鑰和對應的CSR、您可以使用憑證授權單位來簽署以產生公開憑證。

步驟

1. 查看*憑證*頁面。 請參閱 [檢視憑證資訊]。
2. 選取 **+** 產生 **CSR** 。
3. 填寫主旨名稱的資訊：
   a. 輸入*通用名稱*。
   b. 選擇*國家/地區*。
   c. 輸入*組織*。
   d. 輸入*組織單位*。
4. 如果您要置換預設值、請選取*更多選項*並提供其他資訊。

安裝（新增）信任的憑證授權單位

您可以在System Manager中安裝其他信任的憑證授權單位。

步驟

1. 檢視*信任的憑證授權單位*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選擇。 + Add
3. 在「新增信任的憑證授權單位」面板上、執行下列步驟：
   - 輸入*名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。
   - 選擇*類型*。
   - 輸入或匯入*憑證詳細資料*。

刪除信任的憑證授權單位

使用System Manager、您可以刪除信任的憑證授權單位。

您無法刪除預先安裝 ONTAP 的信任憑證授權單位。

步驟

1. 檢視*信任的憑證授權單位*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取信任的憑證授權單位名稱。
3. 選取 ⋮ 名稱旁邊的，然後選取 * 刪除 * 。

續約信任的憑證授權單位

有了System Manager、您可以續約已過期或即將過期的信任憑證授權單位。

步驟

1. 檢視*信任的憑證授權單位*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取信任的憑證授權單位名稱。
3. 選取 ⋮ 憑證名稱旁邊的 * 更新 * 。

安裝（新增）用戶端/伺服器憑證

有了System Manager、您可以安裝其他用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選擇。 

3. 在「新增用戶端/伺服器憑證」面板上、執行下列步驟：
   - 輸入*憑證名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。
   - 選擇*類型*。
   - 輸入或匯入*憑證詳細資料*。
     您可以從文字檔寫入或複製及貼上憑證詳細資料、也可以按一下*匯入*從憑證檔案匯入文字。
   - 輸入 * 私密金鑰 * 。
     您可以從文字檔中寫入或複製及貼上私密金鑰、也可以按一下*匯入*從私密金鑰檔匯入文字。

產生（新增）自我簽署的用戶端/伺服器憑證

有了System Manager、您可以產生額外的自我簽署用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選取 *+ 產生自我簽署的憑證 * 。
3. 在「產生自我簽署的憑證」面板上、執行下列步驟：
   - 輸入*憑證名稱*。
   - 對於*範圍*、請選取儲存VM。

- 輸入*通用名稱*。
- 選擇*類型*。
- 選取*雜湊函數*。
- 選取*金鑰大小*。
- 選擇*儲存VM*。

刪除用戶端/伺服器憑證

使用System Manager、您可以刪除用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取用戶端 / 伺服器憑證的名稱。
3. 選取 ⋮ 名稱旁邊的，然後按一下 * 刪除 * 。

續約用戶端/伺服器憑證

有了System Manager、您可以續約已過期或即將過期的用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選取用戶端 / 伺服器憑證的名稱。
3. 選取 ⋮ 名稱旁邊的、然後按一下 * 更新 * 。

建立新的本機憑證授權單位

有了System Manager、您就能建立新的本機憑證授權單位。

步驟

1. 查看*本地證書頒發機構*選項卡。 請參閱 [檢視憑證資訊]。
2. 選擇。 

3. 在「新增本機憑證授權單位」面板上、執行下列步驟：
   - 輸入*名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。
4. 如果您要置換預設值、請選取*更多選項*並提供其他資訊。

使用本機憑證授權單位簽署憑證

在System Manager中、您可以使用本機憑證授權單位來簽署憑證。

步驟

1. 查看*本地證書頒發機構*選項卡。 請參閱 [檢視憑證資訊]。
2. 選取本機憑證授權單位的名稱。
3. 選擇 ⋮ 名稱旁邊的，然後 * 簽署證書 * 。
4. 填寫*簽署憑證簽署要求*表單。
   - 您可以貼上憑證簽署內容、或按一下*匯入*以匯入憑證簽署要求檔案。
   - 指定憑證有效的天數。

刪除本機憑證授權單位

使用System Manager、您可以刪除本機憑證授權單位。

步驟

1. 檢視*本機憑證授權單位*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選取本機憑證授權單位的名稱。
3. 選擇 ⋮ 名稱旁邊的 * 刪除 * 。

更新本機憑證授權單位

有了System Manager、您可以續約已過期或即將過期的本機憑證授權單位。

步驟

1. 檢視*本機憑證授權單位*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取本機憑證授權單位的名稱。
3. 選取 ⋮ 名稱旁邊的、然後按一下 * 更新 * 。

在 ONTAP 中設定 Active Directory 網域控制站存取

您必須先設定AD網域控制器存取叢集或SVM、AD帳戶才能存取SVM。如果您已為資料SVM設定SMB伺服器、則可將SVM設定為閘道、或將_tunnel_設定為用於AD存取叢集的閘道。如果您尚未設定SMB伺服器、可以在AD網域上建立SVM的電腦帳戶。

支援下列網域控制器驗證服務：ONTAP

- Kerberos
- LDAP
- Netlogon
- 本機安全性授權（LSA）

支援下列工作階段金鑰演算法以確保Netlogon連線安全：ONTAP

工作階段金鑰演算法	可從 … 開始使用。

HMA-SHA256、以進階加密標準（AES）為基礎 如果您的叢集執行的是 ONTAP 9.9.1 或更早版本、而且您的網域控制器會強制執行 AES 來提供安全的 Netlogon 服務、則連線會失敗。在這種情況下、您需要重新設定網域控制器、改為接受與 ONTAP 的強大金鑰連線。	零點9.10.1 ONTAP
DE和HMC-MD5（設定強式金鑰時）	所有ONTAP 的版本

如果您想要在 Netlogon 安全通道建立期間使用 AES 工作階段金鑰、則需要驗證 SVM 上是否已啟用 AES 。

- 從 ONTAP 9.14.1 開始、在建立 SVM 時、預設會啟用 AES 、而且您不需要修改 SVM 的安全設定、即可在 Netlogon 安全通道建立期間使用 AES 工作階段金鑰。
- 在 ONTAP 9.10.1 至 9.13.1 中、建立 SVM 時、預設會停用 AES 。您需要使用下列命令來啟用 AES ：

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

當您升級至 ONTAP 9.14.1 或更新版本時、以舊版 ONTAP 建立的現有 SVM 的 AES 設定將不會自動變更。您仍需要更新此設定的值、才能在這些 SVM 上啟用 AES 。

設定驗證通道

如果您已為資料 SVM 設定 SMB 伺服器、則可以使用 `security login domain-tunnel create` 命令將 SVM 設定為閘道或 *tunnel* 、以便 AD 存取叢集。

在 ONTAP 9.16.1 之前，您必須使用驗證通道來管理具有 AD 的叢集管理員帳戶。

開始之前

- 您必須為資料SVM設定SMB伺服器。
- 您必須啟用AD網域使用者帳戶、才能存取叢集的管理SVM。
- 您必須是叢集管理員才能執行此工作。

從ONTAP 《S209.10.1》開始、如果您有SVM閘道（網域通道）可供AD存取、則如果您在AD網域中停用了NTLM、就可以使用Kerberos進行系統管理驗證。在舊版中、不支援Kerberos搭配SVM閘道的管理驗證。此功能預設為可用、不需設定。

一律會先嘗試Kerberos驗證。一旦失敗、就會嘗試執行NTLM驗證。

步驟

1. 將啟用SMB的資料SVM設定為驗證通道、以便AD網域控制器存取叢集：

```
security login domain-tunnel create -vserver <svm_name>
```

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

SVM必須執行、使用者才能通過驗證。

下列命令會將啟用 SMB 的資料 SVM 設定 `engData`為驗證通道。

```
cluster1::>security login domain-tunnel create -vserver engData
```

在網域上建立SVM電腦帳戶

如果您尚未設定資料 SVM 的 SMB 伺服器、則可以使用 `vserver active-directory create` 命令、為網域上的 SVM 建立電腦帳戶。

關於這項工作

輸入之後 `vserver active-directory create` 命令時、系統會提示您提供 AD 使用者帳戶的認證、並提供足夠的權限、以便將電腦新增至網域中指定的組織單位。帳戶密碼不可空白。

從 ONTAP 9.16.1 開始，您可以使用此程序來管理具有 AD 的叢集管理員帳戶。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 在AD網域上建立SVM的電腦帳戶：

```
vserver active-directory create -vserver <SVM_name> -account-name
<NetBIOS_account_name> -domain <domain> -ou <organizational_unit>
```

從 ONTAP 9.16.1 開始，此 `-vserver`參數會接受管理 SVM 。如"指令參考資料ONTAP"需詳細 `vserver active-directory create`資訊，請參閱。

以下命令將在 SVM 的域上 `example.com`創建一個名爲的 `engData`計算機帳戶 `ADSERVER1`。輸入命令後、系統會提示您輸入AD使用者帳戶認證。

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

在 ONTAP 中設定 LDAP 或 NIS 伺服器存取

您必須先設定LDAP或NIS伺服器存取SVM、LDAP或NIS帳戶才能存取SVM。交換器功能可讓您使用LDAP或NIS做為替代名稱服務來源。

設定LDAP伺服器存取

您必須先設定LDAP伺服器存取SVM、LDAP帳戶才能存取SVM。您可以使用 `vserver services name-service ldap client create` 在 SVM 上建立 LDAP 用戶端組態的命令。然後您就可以使用 `vserver services name-service ldap create` 用於將 LDAP 用戶端組態與 SVM 建立關聯的命令。

關於這項工作

大多數LDAP伺服器都可以使用ONTAP 由下列功能提供的預設架構：

- ms-AD-BIS（大多數Windows 2012及更新版本AD伺服器的偏好架構）
- AD-IDMU （ Windows 2008 、 Windows 2016 及更新版本的 AD 伺服器）
- AD-SFU（Windows 2003和舊版AD伺服器）
- RFC-2307（UNIX LDAP伺服器）

除非有其他需求、否則最好使用預設架構。如果是、您可以複製預設架構並修改複本、以建立自己的架構。如需詳細資訊、請參閱：

- "NFS 組態"
- "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"

開始之前

- 您必須已在 SVM 上安裝"CA簽署的伺服器數位憑證"。
- 您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 在 SVM 上建立 LDAP 用戶端組態：

   ```
   vserver services name-service ldap client create -vserver <SVM_name> -client
   -config <client_configuration> -servers <LDAP_server_IPs> -schema <schema>
   -use-start-tls <true|false>
   ```

   只有資料SVM存取才支援Start TLS。不支援存取管理SVM。

   如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client create`資訊，請參閱。

   以下命令用於創建名爲 SVM `engData` 的 LDAP 客戶端配置 `corp`。用戶端會匿名連結至 IP 位址為 172.0.0.100 和 172.16.0.101 的 LDAP 伺服器。用戶端使用 RFC-2307 架構進行 LDAP 查詢。用戶端與伺服器之間的通訊會使用Start TLS加密。

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

這 `-ldap-servers`字段替換 `-servers`字段。您可以使用 `-ldap-servers`欄位指定 LDAP 伺服器的主機名稱或 IP 位址。

2. 將 LDAP 用戶端組態與 SVM 建立關聯： `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client-enabled <true|false>`

   如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap create`資訊，請參閱。

   下列命令會關聯 LDAP 用戶端組態 `corp` 使用 SVM `engData`，並在 SVM 上啟用 LDAP 用戶端。

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```

這 `vserver services name-service ldap create`如果ONTAP無法聯繫名稱伺服器，則該命令將執行自動設定驗證並報告錯誤訊息。

3. 使用vserver services name-service LDAP檢查命令來驗證名稱伺服器的狀態。

   下列命令會驗證SVM vs0上的LDAP伺服器。

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                  |
| Client Configuration Name: c1                                 |
| LDAP Status: up                                               |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                |
```

   您可以使用 `name service check``命令來驗證名稱伺服器的狀態。

設定 NIS 伺服器存取

您必須先設定NIS伺服器對SVM的存取權、NIS帳戶才能存取SVM。您可以使用 `vserver services name-service nis-domain create` 在 SVM 上建立 NIS 網域組態的命令。

開始之前

- 在SVM上設定NIS網域之前、所有已設定的伺服器都必須可供使用和存取。
- 您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 在 SVM 上建立 NIS 網域組態：

   ```
   vserver services name-service nis-domain create -vserver <SVM_name> -domain
   <client_configuration> -nis-servers <NIS_server_IPs>
   ```

   如"指令參考資料ONTAP"需詳細 `vserver services name-service nis-domain create`資訊，請參閱。

   > 這 `-nis-servers`字段替換 `-servers`字段。您可以使用 `-nis-servers`欄位指定 NIS 伺服器的主機名稱或 IP 位址。

   以下命令在 SVM 上創建 NIS 域配置 `engData`。NIS 網域 `nisdomain`會與 `IP` 位址為的 `NIS` 伺服器進行通訊 `192.0.2.180`。

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -nis-servers 192.0.2.180
   ```

建立名稱服務交換器

名稱服務交換器功能可讓您使用LDAP或NIS做為替代名稱服務來源。您可以使用 `vserver services name-service ns-switch modify` 命令以指定名稱服務來源的查詢順序。

開始之前

- 您必須已設定LDAP和NIS伺服器存取。
- 您必須是叢集管理員或SVM管理員、才能執行此工作。

步驟

1. 指定名稱服務來源的查詢順序：

   ```
   vserver services name-service ns-switch modify -vserver <SVM_name> -database
   <name_service_switch_database> -sources <name_service_source_order>
   ```

   如"指令參考資料ONTAP"需詳細 `vserver services name-service ns-switch modify`資訊，請參閱。

   以下命令指定 SVM 上資料庫 `engData`的 `LDAP` 和 `NIS` 名稱服務來源的查詢順序 `passwd`。

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

變更 ONTAP 管理員密碼

首次登入系統後、您應該立即變更初始密碼。如果您是 SVM 管理員、可以使用 `security login password` 命令以變更您自己的密碼。如果您是叢集管理員、可以使用 `security login password` 命令以變更任何系統管理員的密碼。

關於這項工作

新密碼必須遵守下列規則：

- 它不能包含使用者名稱
- 長度必須至少八個字元
- 它必須包含至少一個字母和一個數字
- 不能與最後六個密碼相同

您可以使用 `security login role config modify`命令來修改與指定角色相關聯之帳戶的密碼規則。

開始之前

- 您必須是叢集或SVM管理員、才能變更自己的密碼。
- 您必須是叢集管理員、才能變更其他管理員的密碼。

步驟

1. 變更管理員密碼： `security login password -vserver svm_name -username user_name`

   下列命令會變更系統管理員的密碼 `admin1` 適用於 SVM`vs1.example.com`。系統會提示您輸入目前密碼、然後輸入並重新輸入新密碼。

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

相關資訊

- "安全登入角色組態修改"
- "安全登入密碼"

鎖定及解除鎖定 ONTAP 系統管理員帳戶

您可以使用 `security login lock` 用於鎖定系統管理員帳戶的命令、以及 `security login unlock` 解除鎖定帳戶的命令。

開始之前

您必須是叢集管理員才能執行這些工作。

步驟

1. 鎖定系統管理員帳戶：

```
security login lock -vserver SVM_name -username user_name
```

下列命令會鎖定系統管理員帳戶 `admin1` 適用於 SVM `vs1.example.com`：

```
cluster1::>security login lock -vserver engData -username admin1
```

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

2. 解除鎖定系統管理員帳戶：

   `security login unlock -vserver SVM_name -username user_name`

   下列命令會解除鎖定系統管理員帳戶 `admin1` 適用於 SVM `vs1.example.com`：

   ```
   cluster1::>security login unlock -vserver engData -username admin1
   ```

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

相關資訊

- "安全登入"

在 ONTAP 中管理失敗的登入嘗試

重複失敗的登入嘗試有時表示入侵者正在嘗試存取儲存系統。您可以採取許多步驟來確保不會發生入侵。

如何得知登入嘗試失敗

事件管理系統（EMS）每小時都會通知您登入失敗的嘗試。您可以在中找到登入嘗試失敗的記錄 `audit.log` 檔案：

重複登入嘗試失敗時該怎麼辦

從短期來看、您可以採取許多步驟來預防入侵：

- 密碼必須由最少的大寫字元、小寫字元、特殊字元和/或數字組成
- 在登入嘗試失敗後強制延遲
- 限制允許的失敗登入嘗試次數、並在指定的失敗嘗試次數後鎖定使用者
- 過期並封鎖在指定天數內處於非使用中狀態的帳戶

您可以使用 `security login role config modify`命令來執行這些工作。如"指令參考資料ONTAP"需詳細 `security login role config modify`資訊，請參閱。

長期而言、您可以採取下列額外步驟：

- 使用 `security ssh modify`命令可限制所有新建立的 SVM 失敗登入嘗試次數。如"指令參考資料ONTAP"需詳細 `security ssh modify`資訊，請參閱。

- 要求使用者變更密碼、將現有的MD5-演算 法帳戶移轉至更安全的SHA-512演算法。

對 ONTAP 系統管理員帳戶密碼強制執行 SHA-2

在升級之後、ONTAP 在更新之前建立的管理員帳戶會繼續使用md5密碼、直到手動變更密碼為止。與SHA-2相比、MD5的安全性較低。因此、在升級之後、您應該提示使用者將密碼變更為使用預設的SHA-512雜湊功能。

關於這項工作

密碼雜湊功能可讓您執行下列動作：

- 顯示符合指定雜湊功能的使用者帳戶。
- 使使用指定雜湊功能的帳戶過期（例如、md5）、強制使用者在下次登入時變更密碼。
- 鎖定密碼使用指定雜湊功能的帳戶。
- 還原至ONTAP 版本早於發揮作用9的版本時、請重設叢集管理員自己的密碼、使其與舊版支援的雜湊功能（md5）相容。

ONTAP 只接受預先散列的 SHA-2 密碼、只能使用 NetApp Manageability SDK (`security-login-create` 和 `security-login-modify-password`) 。

步驟

1. 將md5系統管理員帳戶移轉至SHA-512密碼雜湊功能：
   a. 使所有 MD5 系統管理員帳戶過期： `security login expire-password -vserver * -username * -hash-function md5`

      如此一來、會強制md5帳戶使用者在下次登入時變更密碼。

   b. 要求具有MD5帳戶的使用者透過主控台或SSH工作階段登入。

      系統偵測到帳戶已過期、並提示使用者變更密碼。SHA-512預設用於變更的密碼。

2. 若使用者未在一段時間內登入以變更密碼的MD5帳戶、請強制進行帳戶移轉：
   a. 鎖定仍使用 MD5 雜湊功能的帳戶（進階權限層級）： `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

      在指定的天數之後 `-lock-after`、使用者無法存取其 MD5 帳戶。

   b. 當使用者準備好變更密碼時、請解除鎖定帳戶： `security login unlock -vserver` *`svm_name`* `-username` *`user_name`*
   c. 請使用者透過主控台或SSH工作階段登入帳戶、並在系統提示使用者時變更密碼。

相關資訊

- "安全登入過期密碼"
- "安全登入解除鎖定"

使用系統管理員診斷並修正 ONTAP 檔案存取問題

從功能不全的9.8開始ONTAP 、您可以追蹤及檢視檔案存取問題。

步驟

1. 在System Manager中、選取* Storage > Storage VM*。
2. 選取您要在其中執行追蹤的儲存VM。
3. 按一下 * 更多 * 。
4. 按一下*追蹤檔案存取*。
5. 提供使用者名稱和用戶端IP位址、然後按一下*開始追蹤*。

   追蹤結果會顯示在表格中。 「理由」欄提供無法存取檔案的原因。
6. 按一下 結果表左欄、即可檢視檔案存取權限。