使用CLI存取叢集（僅限叢集管理員）

ONTAP 9

NetApp
February 12, 2026

目錄

使用CLI存取叢集（僅限叢集管理員）

使用節點序列連接埠存取 ONTAP 叢集

您可以直接從連接至節點序列連接埠的主控台存取叢集。

步驟

1. 在主控台按Enter。

   系統會以登入提示回應。

2. 在登入提示下、執行下列其中一項：

若要存取叢集：	輸入下列帳戶名稱...
預設叢集帳戶	**admin**
另一個管理使用者帳戶	*username*

   系統會以密碼提示回應。

3. 輸入admin或管理使用者帳戶的密碼、然後按Enter。

使用 SSH 要求存取 ONTAP 叢集

您可以向 ONTAP 叢集發出 SSH 要求、以執行管理工作。SSH 預設為啟用。

開始之前

- 您必須擁有設定為使用的使用者帳戶 `ssh` 作為存取方法。

  `-application`命令參數 `security login`
  會指定使用者帳戶的存取方法。如link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html#description["指令參考資料ONTAP"^]需詳細`security login`資訊，請參閱。

- 如果您使用 Active Directory （ AD ）網域使用者帳戶來存取叢集、則必須透過啟用 CIFS 的儲存 VM 來設定叢集的驗證通道、而且您的 AD 網域使用者帳戶也必須新增至具有的叢集 `ssh` 作為存取方法和 `domain` 作為驗證方法。

關於這項工作

- 您必須使用OpenSSH 5.7或更新版本的用戶端。
- 僅支援SSH v2傳輸協定；不支援SSH v1。
- 支援每個節點最多64個並行SSH工作階段。ONTAP

如果叢集管理LIF位於節點上、則會與節點管理LIF共用此限制。

如果傳入連線速度高於每秒10次、服務會暫時停用60秒。

- 支援SSH的AES和3DES加密演算法（也稱為_ciphers_）ONTAP 。

  AES支援128、192和256位元金鑰長度。3DES的金鑰長度為56位元、與原始的DES相同、但會重複三次。

- 當FIPS模式開啟時、SSH用戶端應與省略曲線數位簽章演算法（ECDSA）公開金鑰演算法協商、以使連線成功。
- 如果您想ONTAP 要從Windows主機存取此功能、可以使用第三方公用程式、例如Putty。
- 如果您使用Windows AD使用者名稱登入ONTAP 到功能表、則應該使用在ONTAP 功能表中建立AD使用者名稱和網域名稱時所用的大小寫字母。

  AD使用者名稱和網域名稱不區分大小寫。不過ONTAP 、不區分使用者名稱大小寫。使用者名稱ONTAP 若不相符、而使用者名稱與在AD中建立的使用者名稱不相符、將導致登入失敗。

SSH 驗證選項

- 從 ONTAP 9.3 開始、您可以 "啟用 SSH 多因素驗證" 適用於本機系統管理員帳戶。

  啟用SSH多因素驗證時、使用者會使用公開金鑰和密碼進行驗證。

- 從 ONTAP 9.4 開始、您可以 "啟用 SSH 多因素驗證" 適用於 LDAP 和 NIS 遠端使用者。
- 從 ONTAP 9.13.1 開始、您可以選擇性地將憑證驗證新增至 SSH 驗證程序、以增強登入安全性。若要這麼做、 "將 X.509 憑證與公開金鑰建立關聯" 帳戶使用的。如果您同時使用 SSH 公開金鑰和 X.509 憑證登入、ONTAP 會先檢查 X.509 憑證的有效性、然後再使用 SSH 公開金鑰進行驗證。如果該憑證已過期或撤銷、SSH 公開金鑰會自動停用、則 SSH 登入會遭到拒絕。
- 從 ONTAP 9.14.1 開始、 ONTAP 系統管理員就可以 "將 Cisco 雙核心雙因素驗證新增至 SSH 驗證程序" 以增強登入安全性。啟用 Cisco 雙核心驗證之後、首次登入時、使用者必須註冊裝置、以作為 SSH 工作階段的驗證者。
- 從 ONTAP 9.15.1 開始、系統管理員就可以 "設定動態授權" 根據使用者的信任分數、為 SSH 使用者提供額外的自適應驗證。

步驟

1. 從可存取 ONTAP 叢集網路的主機、輸入 `ssh` 命令的格式如下：

   - **`ssh username@hostname_or_IP [command]`**
   - **`ssh -l username hostname_or_IP [command]`**

如果您使用的是 AD 網域使用者帳戶、則必須指定 *`username`* 的格式 *`domainname\\AD_accountname`* （在網域名稱後面加上雙反斜線）或 "*`domainname\AD_accountname`*" （以雙引號括住、並在網域名稱之後加上單一反斜線）。

`hostname_or_IP` 是叢集管理 LIF 或節點管理 LIF 的主機名稱或 IP 位址。建議使用叢集管理LIF。您可以使用IPv4或IPv6位址。

`command` 不需要 SSH 互動式工作階段。

SSH要求範例

下列範例顯示名為「'joe'」的使用者帳戶如何發出SSH要求、以存取叢集管理LIF為10.72.137.28的叢集：

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

下列範例顯示、名為「DOMAIN1」之網域中的「'John」使用者帳戶如何發出SSH要求、以存取叢集管理LIF為10.72.137.28的叢集：

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

下列範例顯示名為「'joe'」的使用者帳戶如何發出SSH MFA要求、以存取叢集管理LIF為10.72.137.32的叢集：

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

相關資訊

"系統管理員驗證與RBAC"

ONTAP SSH 登入安全性

從功能表9.5開始ONTAP 、您可以檢視上次成功登入後、先前登入、登入失敗、以及權限變更等資訊。

當您以SSH管理員使用者身分成功登入時、會顯示安全性相關資訊。您會收到下列情況的警示：

- 您的帳戶名稱上次登入的時間。
- 自上次成功登入以來、嘗試登入失敗的次數。
- 角色自上次登入後是否有所變更（例如、如果管理員帳戶的角色從「admin」變更為「備份」）。
- 自上次登入後、是否已修改角色的新增、修改或刪除功能。

如果顯示的任何資訊可疑、請立即聯絡您的安全部門。

若要在登入時取得此資訊、必須符合下列先決條件：

- 您的SSH使用者帳戶必須以ONTAP 功能不均的形式配置。
- 您必須建立SSH安全登入。
- 您的登入嘗試必須成功。

SSH登入安全性的限制和其他考量

下列限制與考量事項適用於SSH登入安全資訊：

- 此資訊僅適用於SSH型登入。
- 對於群組型管理帳戶（例如LDAP/NIS和AD帳戶）、如果使用者所屬的群組被配置為ONTAP 位於Sof the SView的管理帳戶、則使用者可以檢視SSH登入資訊。

  不過、這些使用者無法顯示使用者帳戶角色變更的警示。此外、屬於AD群組的使用者ONTAP 若已在無法檢視上次登入後發生的不成功登入嘗試次數、則會被配置為在無法執行的系統管理帳戶。

- 當使用者帳戶從ONTAP 下列項目刪除時、系統會刪除為使用者維護的資訊：
- 除了SSH之外、不會顯示連線至應用程式的資訊。

SSH登入安全資訊範例

下列範例示範登入後顯示的資訊類型。

- 此訊息會在每次成功登入後顯示：

```
Last Login : 7/19/2018 06:11:32
```

- 如果自上次成功登入後嘗試登入失敗、則會顯示下列訊息：

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- 如果嘗試登入失敗、且自上次成功登入後您的權限已修改、則會顯示下列訊息：

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

啟用 ONTAP 叢集的 Telnet 或 RSH 存取

最佳安全性做法是預設停用 Telnet 和 RSH 。若要讓叢集能夠接受 Telnet 或 RSH 要求、您必須在預設管理服務原則中啟用該服務。

Telnet 和 RSH 不是安全的通訊協定；您應該考慮使用 SSH 來存取叢集。SSH提供安全的遠端Shell和互動式網路工作階段。如需詳細資訊、請 "使用 SSH 存取叢集"參閱。

關於這項工作

- ONTAP 每個節點最多可支援 50 個並行 Telnet 或 RSH 工作階段。

  如果叢集管理LIF位於節點上、則會與節點管理LIF共用此限制。

  如果傳入連線速度高於每秒10次、服務會暫時停用60秒。

- rsh 命令需要進階權限。

ONTAP 9 。 10.1 或更新版本

步驟

1. 確認已啟用 RSH 或 Telnet 安全性通訊協定：

   ```
   security protocol show
   ```

   a. 如果啟用了 RSH 或 Telnet 安全性通訊協定、請繼續下一步。

   b. 如果未啟用 RSH 或 Telnet 安全性通訊協定、請使用下列命令加以啟用：

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

   深入瞭解 `security protocol show`及 `security protocol modify` "指令參考資料ONTAP"。

2. 確認 `management-rsh-server` 或 `management-telnet-server` 服務存在於管理階層中：

   ```
   network interface show -services management-rsh-server
   ```

   或

   ```
   network interface show -services management-telnet-server
   ```

   如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

   a. 如果 `management-rsh-server` 或 `management-telnet-server` 服務存在、請繼續下一步。

   b. 如果 `management-rsh-server` 或 `management-telnet-server` 服務不存在、請使用下列命令加以新增：

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server

      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

   如"指令參考資料ONTAP"需詳細 `network interface service-policy add-service`資訊，請參閱。

ONTAP 9 9 或更早版本

關於這項工作

ONTAP 可防止您變更預先定義的防火 `mgmt`牆原則、但您可以複製預先定義的管理防火牆原則、然後在新原則下啟用 Telnet 或 RSH 來建立新原則。

步驟

1. 進入進階權限模式：

   ```
   set advanced
   ```

2. 啟用安全性傳輸協定（ RSH 或 Telnet ）：

```
security protocol modify -application security_protocol -enabled true
```

3. 根據 `mgmt`管理防火牆原則建立新的管理防火牆原則：

   ```
   system services firewall policy clone -policy mgmt -destination-policy
   policy-name
   ```

4. 在新的管理防火牆原則中啟用 Telnet 或 RSH ：

   ```
   system services firewall policy create -policy policy-name -service
   security_protocol -action allow -ip-list ip_address/netmask
   ```

   若要允許所有 IP 位址、您應該指定 `-ip-list 0.0.0.0/0`

5. 將新原則與叢集管理 LIF 建立關聯：

   ```
   network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
   -firewall-policy policy-name
   ```

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

使用 Telnet 要求存取 ONTAP 叢集

您可以向叢集發出遠端登入要求、以執行管理工作。預設會停用Telnet。

Telnet 和 RSH 不是安全的通訊協定；您應該考慮使用 SSH 來存取叢集。SSH提供安全的遠端Shell和互動式網路工作階段。如需詳細資訊、請 "使用 SSH 存取叢集"參閱。

開始之前

在使用Telnet存取叢集之前、必須符合下列條件：

- 您必須擁有一個叢集本機使用者帳戶、並設定為使用遠端登入作為存取方法。

  `-application`命令參數 `security login`會指定使用者帳戶的存取方法。如link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+login["指令參考資料ONTAP"^]需詳細 `security login`資訊，請參閱。

關於這項工作

- 支援每個節點最多50個並行的遠端登入工作階段。ONTAP

  如果叢集管理LIF位於節點上、則會與節點管理LIF共用此限制。

  如果傳入連線速度高於每秒10次、服務會暫時停用60秒。

- 如果您想ONTAP 要從Windows主機存取此功能、可以使用第三方公用程式、例如Putty。

- rsh 命令需要進階權限。

ONTAP 9 。 10.1 或更新版本

步驟

1. 確認已啟用 Telnet 安全性傳輸協定：

   ```
   security protocol show
   ```

   a. 如果已啟用 Telnet 安全性通訊協定、請繼續下一步。

   b. 如果未啟用 Telnet 安全性通訊協定、請使用下列命令加以啟用：

      ```
      security protocol modify -application telnet -enabled true
      ```

   深入瞭解 `security protocol show`及 `security protocol modify`"指令參考資料ONTAP"。

2. 確認管理階層中存在該 `management-telnet-server` 服務：

   ```
   network interface show -services management-telnet-server
   ```

   如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

   a. 如果 `management-telnet-server` 服務存在、請繼續下一步。

   b. 如果 `management-telnet-server` 服務不存在、請使用下列命令來新增服務：

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

   如"指令參考資料ONTAP"需詳細 `network interface service-policy add-service`資訊，請參閱。

ONTAP 9 9 或更早版本

開始之前

在使用Telnet存取叢集之前、必須符合下列條件：

- 叢集或節點管理生命里所使用的管理防火牆原則中、必須已啟用遠端登入、以便透過防火牆來處理遠端登入要求。

  預設會停用Telnet。 `system services firewall policy show`含有 `-service telnet`參數的命令會顯示是否已在防火牆原則中啟用 Telnet 。如"指令參考資料ONTAP"需詳細 `system services firewall policy`資訊，請參閱。

- 如果您使用IPv6連線、則必須在叢集上設定並啟用IPv6、而且防火牆原則必須已設定IPv6位址。

  此 `network options ipv6 show`命令會顯示是否已啟用 IPv6 。如"指令參考資料ONTAP"需詳細 `network options ipv6 show`資訊，請參閱。 `system services firewall policy show`命令會顯示防火牆原則。

步驟

1. 從管理主機輸入下列命令：

```
telnet hostname_or_IP
```

`hostname_or_IP`是叢集管理 LIF 或節點管理 LIF 的主機名稱或 IP 位址。建議使用叢集管理LIF。您可以使用IPv4或IPv6位址。

Telnet要求範例

以下範例顯示了名為「joe」的使用者（已設定 Telnet 存取權限）如何發出 Telnet 請求來存取叢集管理 LIF 為 10.72.137.28 的叢集：

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

使用 RSH 要求存取 ONTAP 叢集

您可以向叢集發出RSHE要求以執行管理工作。rsh並非安全傳輸協定、預設為停用。

Telnet 和 RSH 不是安全的通訊協定；您應該考慮使用 SSH 來存取叢集。SSH提供安全的遠端Shell和互動式網路工作階段。如需詳細資訊、請 "使用 SSH 存取叢集"參閱。

開始之前

您必須符合下列條件、才能使用RSH存取叢集：

- 您必須擁有一個叢集本機使用者帳戶、並將其設定為使用RSH作為存取方法。

  `-application`命令參數 `security login`會指定使用者帳戶的存取方法。如link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+login["指令參考資料ONTAP"^]需詳細 `security login`資訊，請參閱。

關於這項工作

- 支援每個節點最多50個並行的RSH工作階段。ONTAP

  如果叢集管理LIF位於節點上、則會與節點管理LIF共用此限制。

  如果傳入連線速度高於每秒10次、服務會暫時停用60秒。

- rsh 命令需要進階權限。

ONTAP 9 。 10.1 或更新版本

步驟

1. 確認已啟用 RSH 安全性通訊協定：

   ```
   security protocol show
   ```

   a. 如果啟用了 RSH 安全性通訊協定、請繼續下一步。

   b. 如果未啟用 RSH 安全性通訊協定、請使用下列命令加以啟用：

      ```
      security protocol modify -application rsh -enabled true
      ```

   深入瞭解 `security protocol show`及 `security protocol modify`"指令參考資料ONTAP"。

2. 確認管理階層中存在該 `management-rsh-server` 服務：

   ```
   network interface show -services management-rsh-server
   ```

   如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

   a. 如果 `management-rsh-server` 服務存在、請繼續下一步。

   b. 如果 `management-rsh-server` 服務不存在、請使用下列命令來新增服務：

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

   如"指令參考資料ONTAP"需詳細 `network interface service-policy add-service`資訊，請參閱。

ONTAP 9 9 或更早版本

開始之前

您必須符合下列條件、才能使用RSH存取叢集：

- Rsh必須已在叢集或節點管理生命體所使用的管理防火牆原則中啟用、以便讓RSHH要求能夠通過防火牆。

  依預設、 RSH 會停用。系統服務防火牆原則 show 命令及 `-service rsh`參數會顯示是否已在防火牆原則中啟用 RSH 。如"指令參考資料ONTAP"需詳細 `system services firewall policy`資訊，請參閱。

- 如果您使用IPv6連線、則必須在叢集上設定並啟用IPv6、而且防火牆原則必須已設定IPv6位址。

  此 `network options ipv6 show`命令會顯示是否已啟用 IPv6 。如"指令參考資料ONTAP"需詳細 `network options ipv6 show`資訊，請參閱。 `system services firewall policy show`命令會顯示防火牆原則。

步驟

1. 從管理主機輸入下列命令：

   ```
   rsh hostname_or_IP -l username:passwordcommand
   ```

`hostname_or_IP`是叢集管理 LIF 或節點管理 LIF 的主機名稱或 IP 位址。建議使用叢集管理LIF。您可以使用IPv4或IPv6位址。

`command`是您要透過 RSH 執行的命令。

RSH申請範例

下列範例顯示已設定 RSH 存取權限的使用者「 Joe 」如何發出 RSHE 要求來執行 `cluster show` 命令：

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

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

版權資訊

商標資訊