使用憑證驗證遠端伺服器的身分
ONTAP 9

NetApp
February 18, 2025

目錄

使用憑證驗證遠端伺服器的身分

使用憑證總覽來驗證遠端伺服器的身分識別

支援安全認證功能、可驗證遠端伺服器的身分。ONTAP

利用下列數位憑證功能與傳輸協定、支援安全連線：ONTAP

- 線上憑證狀態傳輸協定（OCSP）會使用ONTAP SSL和傳輸層安全（TLS）連線、驗證來自支援服務的數位憑證要求狀態。此功能預設為停用。
- 預設的一組信任根憑證會隨ONTAP 附於整套的軟體中。
- 金鑰管理互通性傳輸協定（KMIP）憑證可讓叢集和KMIP伺服器相互驗證。

使用**OCSP**驗證數位憑證是否有效

從ONTAP 功能為2的9.2開始、線上憑證狀態傳輸協定（OCSP）可讓ONTAP 使用傳輸層安全性（TLS）通訊的各種應用程式在啟用OCSP時、接收數位憑證狀態。您可以隨時啟用或停用特定應用程式的OCSP憑證狀態檢查。根據預設、OCSP憑證狀態檢查會停用。

您需要的產品

您需要進階權限層級存取權限才能執行此工作。

關於這項工作

OCSP支援下列應用程式：

- AutoSupport
- 事件管理系統（EMS）
- LDAP over TLS
- 金鑰管理互通性傳輸協定（KMIP）
- 稽核記錄
- FabricPool
- SSH （從 ONTAP 9.13.1 開始）

步驟

1. 將權限層級設為進階： `set -privilege advanced`。
2. 若要啟用或停用OCSP憑證狀態檢查以檢查特定ONTAP 的功能、請使用適當的命令。

如果您希望**OCSP**憑證狀態檢查某些應用程式...	使用命令...
已啟用	`security config ocsp enable -app app name`

如果您希望**OCSP**憑證狀態檢查某些應用程式...	使用命令...
已停用	`security config ocsp disable -app app name`

下列命令可支援AutoSupport OCSP for the flexf及EMS。

```
cluster::*> security config ocsp enable -app asup,ems
```

啟用OCSP時、應用程式會收到下列其中一個回應：

- 好-憑證有效且通訊繼續進行。
- 已撤銷：憑證由其核發的憑證授權單位永久視為不信任、且無法繼續通訊。
- 不明：伺服器沒有任何關於憑證的狀態資訊、而且無法繼續通訊。
- 憑證中缺少OCSP伺服器資訊-伺服器的運作方式如同OCSP已停用、並繼續進行TLS通訊、但不會進行狀態檢查。
- OCSP伺服器無回應-應用程式無法繼續。

3. 若要啟用或停用使用TLS通訊之所有應用程式的OCSP憑證狀態檢查、請使用適當的命令。

如果您希望**OCSP**憑證狀態檢查所有應用程式...	使用命令...
已啟用	`security config ocsp enable -app all`
已停用	`security config ocsp disable -app all`

啟用時、所有應用程式都會收到已簽署的回應、表示指定的憑證良好、已撤銷或不明。若憑證遭撤銷、應用程式將無法繼續進行。如果應用程式無法從OCSP伺服器接收回應、或伺服器無法連線、則應用程式將無法繼續進行。

4. 使用 `security config ocsp show` 顯示所有支援 OCSP 的應用程式及其支援狀態的命令。

```
cluster::*> security config ocsp show
         Application                         OCSP Enabled?
         --------------------                ---------------------
         autosupport                         false
         audit_log                           false
         fabricpool                          false
         ems                                 false
         kmip                                false
         ldap_ad                             true
         ldap_nis_namemap                    true
         ssh                                 true

         8 entries were displayed.
```

檢視TLS型應用程式的預設憑證

從使用支援功能支援功能支援功能的支援、ONTAP 到使用ONTAP 傳輸層安全性（TLS）的ONTAP 支援功能、以預設的信任根憑證集為基礎。

您需要的產品

預設憑證只會在系統管理SVM建立期間或升級ONTAP 至S9.2期間安裝在系統管理SVM上。

關於這項工作

目前做為用戶端且需要驗證憑證的應用程式包括AutoSupport ：FabricPool 和KMIP。

當憑證過期時、系統會呼叫一則EMS訊息、要求使用者刪除憑證。預設憑證只能在進階權限層級刪除。

> ⓘ 刪除預設憑證可能會導致部分ONTAP 功能不正常的應用程式（例如AutoSupport 、「可靠性記錄」和「稽核記錄」）。

步驟

1. 您可以使用安全性憑證show命令來檢視安裝在管理SVM上的預設憑證：

   security certificate show -vserver –type server-ca

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- --------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

版權資訊

商標資訊