



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	1
使用憑證總覽來驗證遠端伺服器的身分識別	1
使用OCSP驗證數位憑證是否有效	1
檢視TLS型應用程式的預設憑證	3

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	<code>security config ocspl enable -app app name</code>

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	<code>security config ocsp disable -app app name</code>

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	<code>security config ocsp enable</code> <code>-app all</code>
已停用	<code>security config ocsp disable</code> <code>-app all</code>

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 oosp 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

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。