相互驗證叢集和 KMIP 伺服器

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/system-admin/mutually-authenticating-cluster-kmip-server-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目錄

相互驗證叢集和 KMIP 伺服器

相互驗證叢集和KMIP伺服器總覽

相互驗證叢集和外部金鑰管理程式（例如金鑰管理互通性傳輸協定（KMIP）伺服器）、可讓金鑰管理程式使用KMIP over SSL與叢集進行通訊。當應用程式或特定功能（例如儲存加密功能）需要安全金鑰來提供安全的資料存取時、您就會這麼做。

為叢集產生憑證簽署要求

您可以使用安全性憑證 `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。

您需要的產品

您必須是叢集管理員或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

   如需完整的命令語法、請參閱手冊頁。

   下列命令會建立CSR、其中包含由SHA256雜湊功能所產生的2、048位元私密金鑰、供公司IT部門的軟體群組使用、其自訂通用名稱為server1.companyname.com、位於美國加州桑尼維爾。SVM聯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。

```
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-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please 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。

為叢集安裝CA簽署的伺服器憑證

若要讓SSL伺服器將叢集或儲存虛擬機器（SVM）驗證為SSL用戶端、請在叢集或SVM上安裝具有用戶端類型的數位憑證。然後將用戶端CA憑證提供給SSL伺服器管理員、以便在伺服器上安裝。

您需要的產品

您必須已在叢集上安裝 SSL 伺服器的根憑證、或是在上安裝 SVM `server-ca` 憑證類型。

步驟

1. 若要使用自我簽署的數位憑證進行用戶端驗證、請使用 `security certificate create` 命令 `type client` 參數。

2. 若要使用CA簽署的數位憑證進行用戶端驗證、請完成下列步驟：

   a. 使用安全性憑證產生數位憑證簽署要求（ CSR ） `generate-csr` 命令。

      包含憑證要求和私密金鑰的CSR輸出會顯示出來、並提醒您將輸出複製到檔案、以供日後參考。ONTAP

   b. 將CSR輸出的憑證要求以電子形式（例如電子郵件）傳送至信任的CA進行簽署。

      您應該保留一份私密金鑰和CA簽署憑證的複本、以供日後參考。

   在處理您的要求之後、CA會將簽署的數位憑證傳送給您。

   a. 使用安裝 CA 簽署的憑證 `security certificate install` 命令 `-type client` 參數。
   b. 在系統提示時輸入憑證和私密金鑰、然後按* Enter *。
   c. 在出現提示時輸入任何其他根或中繼憑證、然後按* Enter *。

      如果從信任的根CA開始且以核發給您的SSL憑證結束的憑證鏈結遺失中繼憑證、您可以在叢集或SVM上安裝中繼憑證。中繼憑證是由信任的根所核發的次要憑證、專門用於發行終端實體伺服器憑證。結果是憑證鏈結從信任的根CA開始、經過中繼憑證、最後以核發給您的SSL憑證結束。

3. 提供 `client-ca` 將叢集或 SVM 的憑證交給 SSL 伺服器的管理員、以便在伺服器上安裝。

   的安全性憑證 show 命令 `-instance` 和 `-type client-ca` 參數會顯示 `client-ca` 憑證資訊。

為KMIP伺服器安裝CA簽署的用戶端憑證

金鑰管理互通性傳輸協定（KMIP）的憑證子類型（-subtype kmip-cert參數）、以及用戶端和伺服器-ca類型、都會指定該憑證用於互動驗證叢集和外部金鑰管理程式、例如KMIP伺服器。

關於這項工作

安裝KMIP憑證、將KMIP伺服器驗證為叢集的SSL伺服器。

步驟

1. 使用 `security certificate install` 命令 `-type server-ca` 和 `-subtype kmip-cert` 用於為 KMIP 伺服器安裝 KMIP 憑證的參數。
2. 出現提示時、請輸入憑證、然後按Enter。

   提醒您保留一份憑證複本、以供日後參考。ONTAP

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


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

cluster1::>
```

版權資訊

Copyright © 2024 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。