



設定伺服器憑證

StorageGRID 11.5

NetApp
April 11, 2024

目錄

設定伺服器憑證	1
支援的自訂伺服器憑證類型	1
負載平衡器端點的憑證	1
為Grid Manager和Tenant Manager設定自訂伺服器憑證	1
還原Grid Manager和Tenant Manager的預設伺服器憑證	2
設定自訂伺服器憑證、以連線至儲存節點或CLB服務	3
還原S3和Swift REST API端點的預設伺服器憑證	4
複製StorageGRID 該系統的CA憑證	4
設定StorageGRID 支援FabricPool 的支援功能證書	5
為管理介面產生自我簽署的伺服器憑證	6

設定伺服器憑證

您可以自訂StorageGRID 由該系統使用的伺服器憑證。

本系統使用安全性憑證來實現多種不同目的StorageGRID：

- 管理介面伺服器憑證：用於保護網格管理程式、租戶管理程式、網格管理API及租戶管理API的存取安全。
- 儲存API伺服器憑證：用於保護存取儲存節點和閘道節點的安全、API用戶端應用程式會使用這些節點來上傳和下載物件資料。

您可以使用安裝期間建立的預設憑證、或是將這些預設類型的憑證或兩者都取代為您自己的自訂憑證。

支援的自訂伺服器憑證類型

支援使用RSA或ECDSA（Elliptic曲線數位簽章演算法）加密的自訂伺服器憑證StorageGRID。

如需StorageGRID 更多關於如何保護REST API用戶端連線的資訊、請參閱S3或Swift實作指南。

負載平衡器端點的憑證

可分別管理負載平衡器端點所使用的憑證。StorageGRID若要設定負載平衡器憑證、請參閱設定負載平衡器端點的指示。

相關資訊

["使用S3"](#)

["使用Swift"](#)

["設定負載平衡器端點"](#)

為Grid Manager和Tenant Manager設定自訂伺服器憑證

您可以使用StorageGRID 單一自訂伺服器憑證來取代預設的支援伺服器憑證、讓使用者能夠存取Grid Manager和租戶管理程式、而不會遇到安全性警告。

關於這項工作

根據預設、每個管理節點都會核發由網格CA簽署的憑證。這些CA簽署的憑證可由單一通用的自訂伺服器憑證和對應的私密金鑰取代。

由於所有管理節點都使用單一自訂伺服器憑證、因此如果用戶端在連線至Grid Manager和Tenant Manager時需要驗證主機名稱、則必須將憑證指定為萬用字元或多網域憑證。定義自訂憑證、使其符合網格中的所有管理節點。

您需要在伺服器上完成組態、視您使用的根憑證授權單位（CA）而定、使用者可能也需要在網頁瀏覽器中安裝根CA憑證、以便存取Grid Manager和租戶管理程式。



為了確保作業不會因為伺服器憑證故障而中斷、當此伺服器憑證即將過期時、會觸發*Management Interface*警示伺服器憑證過期、以及舊版管理介面憑證過期 (MCEP) 警示。如有需要、您可以選取*支援*>*工具*>*網格拓撲*、以檢視目前服務憑證過期的天數。然後選取「主管理節點_>* CMN*>*資源*」。



如果您使用網域名稱而非IP位址來存取Grid Manager或Tenant Manager、則瀏覽器會顯示憑證錯誤、且在發生下列任一情況時、不會出現跳過的選項：

- 您的自訂管理介面伺服器憑證將過期。
- 您可以從自訂管理介面伺服器憑證還原為預設的伺服器憑證。

步驟

1. 選擇*組態*>*網路設定*>*伺服器憑證*。
2. 在「管理介面伺服器憑證」區段中、按一下「安裝自訂憑證」。
3. 上傳所需的伺服器憑證檔案：
 - 伺服器憑證：自訂伺服器憑證檔案 (.crt) 。
 - 伺服器憑證私密金鑰：自訂伺服器憑證私密金鑰檔 (.key) 。



EC私密金鑰必須大於或等於224位元。RSA私密金鑰必須大於或等於2048位元。

- * CA產品組合*：單一檔案、包含來自每個中繼發行憑證授權單位 (CA) 的憑證。檔案應包含以憑證鏈順序串聯的每個由PEE編碼的CA憑證檔案。

4. 按一下「* 儲存 *」。

自訂伺服器憑證會用於所有後續的新用戶端連線。

選取索引標籤以顯示有關預設StorageGRID 的伺服器認證或上傳的CA簽署認證的詳細資訊。



上傳新的憑證後、請允許清除任何相關的憑證過期警示 (或舊版警示) 一天。

5. 重新整理頁面以確保網頁瀏覽器已更新。

還原Grid Manager和Tenant Manager的預設伺服器憑證

您可以恢復使用Grid Manager和租戶管理程式的預設伺服器憑證。

步驟

1. 選擇*組態*>*網路設定*>*伺服器憑證*。
2. 在「管理介面伺服器憑證」區段中、按一下「使用預設憑證」。
3. 按一下確認對話方塊中的*確定*。

還原預設伺服器憑證時、您設定的自訂伺服器憑證檔案將會刪除、無法從系統中還原。預設伺服器憑證會用於所有後續的新用戶端連線。

4. 重新整理頁面以確保網頁瀏覽器已更新。

設定自訂伺服器憑證、以連線至儲存節點或CLB服務

您可以取代用於S3或Swift用戶端連線至儲存節點或閘道節點上CLB服務（已過時）的伺服器憑證。置換的自訂伺服器憑證是您組織專屬的。

關於這項工作

根據預設、每個儲存節點都會核發由網格CA簽署的X·509伺服器憑證。這些CA簽署的憑證可由單一通用的自訂伺服器憑證和對應的私密金鑰取代。

所有儲存節點都使用單一自訂伺服器憑證、因此如果用戶端在連線至儲存端點時需要驗證主機名稱、則必須將憑證指定為萬用字元或多網域憑證。定義自訂憑證、使其符合網格中的所有儲存節點。

在伺服器上完成組態之後、使用者可能還需要在S3或Swift API用戶端上安裝根CA憑證、以供存取系統、視您使用的根憑證授權單位（CA）而定。



為了確保作業不會因為失敗的伺服器憑證而中斷、當根伺服器憑證即將過期時、會觸發* Storage API端點的伺服器憑證過期*警示和舊版Storage API服務端點憑證過期（SCEP）警示。如有必要、您可以選取*支援*工具 Grid拓撲*、以檢視目前服務憑證過期的天數。然後選取「主要管理節點_CMN* Resources *」。

只有在用戶端使用StorageGRID 閘道節點上過時的CLB服務連線至功能區、或直接連線至儲存節點時、才會使用自訂憑證。使用StorageGRID 管理節點或閘道節點上的負載平衡器服務連線至支援功能的S3或Swift用戶端、會使用針對負載平衡器端點所設定的憑證。



負載平衡器端點認證*到期時會觸發即將到期的負載平衡器端點警示。

步驟

1. 選擇*組態*>*網路設定*>*伺服器憑證*。
2. 在「物件儲存API服務端點伺服器憑證」區段中、按一下「安裝自訂憑證」。
3. 上傳所需的伺服器憑證檔案：
 - 伺服器憑證：自訂伺服器憑證檔案 (.crt)。
 - 伺服器憑證私密金鑰：自訂伺服器憑證私密金鑰檔 (.key)。



EC私密金鑰必須大於或等於224位元。RSA私密金鑰必須大於或等於2048位元。

- * CA產品組合*：單一檔案、包含來自每個中繼發行憑證授權單位（CA）的憑證。檔案應包含以憑證鏈順序串聯的每個由PEE編碼的CA憑證檔案。
4. 按一下「* 儲存 *」。

自訂伺服器憑證會用於所有後續的新API用戶端連線。

選取索引標籤以顯示有關預設StorageGRID 的伺服器認證或上傳的CA簽署認證的詳細資訊。



上傳新的憑證後、請允許清除任何相關的憑證過期警示（或舊版警示）一天。

5. 重新整理頁面以確保網頁瀏覽器已更新。

相關資訊

["使用S3"](#)

["使用Swift"](#)

["設定S3 API端點網域名稱"](#)

還原S3和Swift REST API端點的預設伺服器憑證

您可以還原為使用S3和Swift REST API端點的預設伺服器憑證。

步驟

1. 選擇*組態*>*網路設定*>*伺服器憑證*。
2. 在「物件儲存API服務端點伺服器憑證」區段中、按一下「使用預設憑證」。
3. 按一下確認對話方塊中的*確定*。

還原物件儲存API端點的預設伺服器憑證時、您設定的自訂伺服器憑證檔案將會刪除、無法從系統中還原。預設伺服器憑證會用於所有後續的新API用戶端連線。

4. 重新整理頁面以確保網頁瀏覽器已更新。

複製StorageGRID 該系統的CA憑證

使用內部憑證授權單位 (CA) 來保護內部流量StorageGRID。如果您上傳自己的憑證、此憑證不會變更。

您需要的產品

- 您必須使用支援的瀏覽器登入Grid Manager。
- 您必須擁有特定的存取權限。

關於這項工作

如果已設定自訂伺服器憑證、用戶端應用程式應使用自訂伺服器憑證來驗證伺服器。他們不應該從StorageGRID這個系統複製CA憑證。

步驟

1. 選擇*組態*>*網路設定*>*伺服器憑證*。
2. 在「內部CA憑證」區段中、選取所有的憑證文字。

您必須包含 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE----- 在您的選擇中。

Internal CA Certificate

StorageGRID uses an internal Certificate Authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

To export the internal CA certificate, copy all of the certificate text (starting with -----BEGIN CERTIFICATE----- and ending with -----END CERTIFICATE-----), and save it as a .pem file.

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT
Certificate: -----BEGIN CERTIFICATE-----
MIIEETjCCAzagAwIBAgIJAjMIM8F7i7AKQMh0GCSqGSIb3DQEBCwUAMHcxZjBmNV
BAYTA1VTMRMwEQYDVQKIExwDyYkxpZm9ybm1hMRIwEAYDVQQHEw1TdW5ueXZhbG91
FDASBgNVBAoTC051dEFwCzBjbmMuMRswGQYDVQQLEExJOZXRBRcHAgU3RvcnFmZnZl
SUQxODDAKBgNVBAMTA0dQVDAeFw0yMDA5MDYyMDE2MDBaFw0zODAxMTcyMDE2MDBa
MHcxZjBmNVBAYTA1VTMRMwEQYDVQKIExwDyYkxpZm9ybm1hMRIwEAYDVQQHEw1T
dW5ueXZhbG91FDASBgNVBAoTC051dEFwCzBjbmMuMRswGQYDVQQLEExJOZXRBRcH
AgU3RvcnFmZnZlSUQxODDAKBgNVBAMTA0dQVDAeFw0yMDA5MDYyMDE2MDBaFw0z
ODAxMTcyMDE2MDBaA4790hstckFq34WHkrSgatsWz6RXm1gQv8CAwEAaA0B3DCB2TAdBgNVHQ4EFQU
fiTcKt2l0ccoen9sx4B0R5TLgYwgakGA1UdIw5BoTCBnoAUFiTCkT2l0ccoen9s
x4B0R5TLgahE6R5MHcxZjBmNVBAYTA1VTMRMwEQYDVQKIExwDyYkxpZm9ybm1h
MRIwEAYDVQQHEw1TdW5ueXZhbG91FDASBgNVBAoTC051dEFwCzBjbmMuMRswGQY
VQLEExJOZXRBRcHAgU3RvcnFmZnZlSUQxODDAKBgNVBAMTA0dQVDAeFw0yMDA5MDYy
MDE2MDBaFw0zODAxMTcyMDE2MDBaMawGA1UdEwQFMAMBaf8wDQYJKoZIhvcNAQELBQADggEBANNsvJQaCs72UzQONjpu
cZKai1iUQr+S2h9RjfsY3jKwu7+SBh9A2Phgmu8p1gA1q55a7bE3+7Ye3TwtD1l
acb8aB3Iuh1xvLpq5QYDvRS7YtQ4cKaSwongy+yyxoU0MTzn6DFXGd4i4pr5+xS
/qccXWekopYzfUtK5wqfjRqUsdFc58djp+adDqI8F5m9ZXGvwYdJgBuyUjwgdkw
109bWlH++AKcELR8cgxg/B6RzoAGE4Km1BvVw+rJrxu0//NCU3u5KaGte862+fG
I37X9GEzFtqnnhkXvo2BZ/OLyGgYbgiksad1nFU3VAjK9iVGHHLPd6BQ8ZxQhYgc
aHlM=
-----END CERTIFICATE-----
```

3. 在選取的文字上按一下滑鼠右鍵、然後選取*複製*。
4. 將複製的憑證貼到文字編輯器中。
5. 以副檔名儲存檔案 .pem 。

例如：storagegrid_certificate.pem

設定StorageGRID 支援FabricPool 的支援功能證書

如果S3用戶端執行嚴格的主機名稱驗證、但不支援停用嚴格的主機名稱驗證、例如ONTAP 使用FabricPool 支援功能的支援功能、則您可以在設定負載平衡器端點時、產生或上傳伺服器憑證。

您需要的產品

- 您必須擁有特定的存取權限。
- 您必須使用支援的瀏覽器登入Grid Manager。

關於這項工作

建立負載平衡器端點時、您可以產生自我簽署的伺服器憑證、或是上傳由已知憑證授權單位 (CA) 簽署的憑證。在正式作業環境中、您應該使用由已知CA簽署的憑證。由CA簽署的憑證可在不中斷營運的情況下循環。它們也更安全、因為它們能更有效地防範攔截式攻擊。

下列步驟為使用FabricPool 支援功能的S3用戶端提供一般準則。如需更多詳細資訊和程序、請參閱設定StorageGRID 用作FabricPool 支援功能的功能說明。



閘道節點上的個別連線負載平衡器 (CLB) 服務已過時、不再建議搭配FabricPool 使用。

步驟

1. 或者、設定高可用度 (HA) 群組FabricPool 以供使用。
2. 建立S3負載平衡器端點FabricPool 以供使用。

當您建立HTTPS負載平衡器端點時、系統會提示您上傳伺服器憑證、憑證私密金鑰和CA套件組合。

3. 在StorageGRID 整個過程中附加作雲端層的功能。ONTAP

指定負載平衡器端點連接埠、以及您上傳的CA憑證所使用的完整網域名稱。然後提供CA憑證。



如果中介CA核發StorageGRID 了此資訊證書、您必須提供中繼CA憑證。如果StorageGRID 此驗證是由根CA直接發出、您必須提供根CA憑證。

相關資訊

["設定StorageGRID 適用於FabricPool 靜態的"](#)

為管理介面產生自我簽署的伺服器憑證

您可以使用指令碼為需要嚴格主機名稱驗證的管理API用戶端、產生自我簽署的伺服器憑證。

您需要的產品

- 您必須擁有特定的存取權限。
- 您必須擁有 Passwords.txt 檔案：

關於這項工作

在正式作業環境中、您應該使用由已知憑證授權單位 (CA) 簽署的憑證。由CA簽署的憑證可在不中斷營運的情況下循環。它們也更安全、因為它們能更有效地防範攔截式攻擊。

步驟

1. 取得每個管理節點的完整網域名稱 (FQDN) 。
2. 登入主要管理節點：
 - a. 輸入下列命令：`ssh admin@primary_Admin_Node_IP`
 - b. 輸入中所列的密碼 Passwords.txt 檔案：
 - c. 輸入下列命令以切換至root：`su -`
 - d. 輸入中所列的密碼 Passwords.txt 檔案：

當您以root登入時、提示會從變更 \$ 至 # 。

3. 使用StorageGRID 新的自我簽署憑證來設定功能。

```
$ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
```

- 適用於 --domains、使用萬用字元代表所有管理節點的完整網域名稱。例如、
*.ui.storagegrid.example.com 使用*萬用字元表示 admin1.ui.storagegrid.example.com

和 `admin2.ui.storagegrid.example.com`。

- 設定 `--type` 至 `management` 設定 Grid Manager 和 Tenant Manager 使用的憑證。
- 根據預設、產生的憑證有效期間為一年（365天）、必須在到期前重新建立。您可以使用 `--days` 用於置換預設有效期間的引數。



憑證的有效期間始於何時 `make-certificate` 執行。您必須確保管理API用戶端與StorageGRID 其他來源同步、否則用戶端可能會拒絕該憑證。

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type  
management --days 365
```

產生的輸出包含管理API用戶端所需的公開憑證。

4. 選取並複製憑證。

在您的選擇中加入開始標記和結束標記。

5. 登出命令Shell。 `$ exit`

6. 確認已設定憑證：

- a. 存取 Grid Manager。
- b. 選擇 *組態* 伺服器憑證 *管理介面伺服器憑證*。

7. 設定您的管理API用戶端使用您複製的公用憑證。包括開始和結束標記。

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。