管理安全證書

Active IQ Unified Manager

NetApp
October 15, 2025

目錄

管理安全證書

您可以在 Unified Manager 伺服器中設定 HTTPS，以透過安全連線監控和管理您的叢集。

查看**HTTPS**安全證書

您可以將 HTTPS 憑證詳細資訊與瀏覽器中檢索到的憑證進行比較，以確保瀏覽器與 Unified Manager 的加密連線不會被攔截。

開始之前

您必須具有操作員、應用程式管理員或儲存管理員角色。

檢視憑證可讓您驗證重新產生的憑證的內容，或檢視可以從中存取 Unified Manager 的主題備用名稱 (SAN)。

步

1. 在左側導覽窗格中，按一下「常規」>「**HTTPS** 憑證」。

   HTTPS憑證顯示在頁面頂部

如果您需要查看比 HTTPS 憑證頁面上顯示的更多有關安全憑證的詳細信息，您可以在瀏覽器中查看連接憑證。

下載 **HTTPS** 憑證簽署請求

您可以下載目前 HTTPS 安全性憑證的認證簽章要求，以便將該檔案提供給憑證授權單位進行簽署。 CA 簽章憑證有助於防止中間人攻擊，並提供比自簽章憑證更好的安全保護。

開始之前

您必須具有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下「常規」>「**HTTPS** 憑證」。
2. 按一下「下載 HTTPS 憑證簽署請求」。
3. 儲存 `<hostname>.csr`文件。

您可以將該文件提供給證書頒發機構進行簽名，然後安裝已簽署的證書。

安裝 **CA** 簽署並傳回的 **HTTPS** 憑證

您可以在證書頒發機構簽署並返回安全證書後上傳並安裝該證書。您上傳並安裝的檔案必須是現有自簽名憑證的簽章版本。 CA 簽章憑證有助於防止中間人攻擊，並提供比自簽章憑證更好的安全保護。

*開始之前

您必須完成以下操作：

- 下載憑證簽署請求文件並由憑證授權單位簽名
- 以 PEM 格式儲存憑證鏈
- 包含鏈中的所有證書，從 Unified Manager 伺服器證書到根簽名證書，包括任何存在的中間證書

您必須具有應用程式管理員角色。

如果建立 CSR 的憑證有效期超過 397 天，則 CA 會在簽署並傳回憑證之前將有效期縮短至 397 天

步驟

1. 在左側導覽窗格中，按一下「常規」>「**HTTPS** 憑證」。
2. 按一下「安裝 HTTPS 憑證」。
3. 在顯示的對話方塊中，按一下「選擇檔案...」以找到要上傳的檔案。
4. 選擇文件，然後按一下*安裝*來安裝該文件。

   有關信息，請參閱"安裝使用外部工具產生的 HTTPS 憑證"。

證書鏈範例

以下範例顯示了憑證鏈檔案的可能外觀：

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

安裝使用外部工具產生的 **HTTPS** 憑證

您可以安裝自簽名或 CA 簽署的證書，並使用外部工具（如 OpenSSL、BoringSSL、LetsEncrypt）產生。

您應該將私鑰與憑證鏈一起加載，因為這些憑證是外部產生的公鑰-私鑰對。允許的金鑰對演算法是“RSA”和“EC”。在「常規」部分下的「HTTPS 憑證」頁面中提供了「安裝 **HTTPS** 憑證」選項。您上傳的文件應採用以下輸入格式。

1. 屬於Active IQ Unified Manager主機的伺服器的私鑰

2. 與私鑰匹配的伺服器憑證
3. 反向直到根的 CA 證書，用於簽署上述證書

載入帶有 **EC** 金鑰對的憑證的格式

允許的曲線是“prime256v1”和“secp384r1”。具有外部產生的 EC 對的憑證樣本：

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

使用 **RSA** 金鑰對載入憑證的格式

屬於主機憑證的 RSA 金鑰對允許的金鑰大小為 2048、3072 和 4096。具有外部產生的 **RSA** 金鑰對 的憑證：

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

上傳憑證後，您應該重新啟動Active IQ Unified Manager實例以使變更生效。

上傳外部產生的憑證時進行檢查

系統在上傳使用外部工具產生的憑證時執行檢查。如果任何檢查失敗，則證書被拒絕。還包括產品內 CSR 產生的憑證和使用外部工具產生的憑證的驗證。

- 輸入中的私鑰根據輸入中的主機憑證進行驗證。
- 主機憑證中的通用名稱 (CN) 與主機的 FQDN 進行檢查。
- 主機憑證的通用名稱（CN）不能為空或空白，且不能設定為localhost。
- 證書的有效期限起始日期不應為日後日期，且證書的有效期限到期日不應為過去日期。
- 如果存在中級 CA 或 CA，則憑證的有效期開始日期不應在未來，有效期到期日不應在過去。

輸入中的私鑰不應該被加密。如果有任何私鑰被加密，那麼系統就會拒絕它們。

範例 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

範例 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

範例 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

如果憑證安裝失敗，請參閱知識庫 (KB) 文章：https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager 無法安裝外部產生的憑證"^]

證書管理的頁面描述

您可以使用 HTTPS 憑證頁面查看目前的安全性憑證並產生新的 HTTPS 憑證。

HTTPS 憑證頁面

HTTPS 憑證頁面可讓您查看目前安全性憑證、下載憑證簽署要求、產生新的自簽名 HTTPS 憑證或安裝新的 HTTPS 憑證。

如果您尚未產生新的自簽名 HTTPS 證書，則此頁面上顯示的證書是安裝期間產生的證書。

命令按鈕

命令按鈕使您能夠執行以下操作：

- 下載 **HTTPS** 憑證簽署請求

  下載目前安裝的 HTTPS 憑證的認證請求。您的瀏覽器會提示您儲存 <hostname>.csr 文件，以便您可以將該文件提供給憑證授權單位進行簽署。

- 安裝 **HTTPS** 憑證

  使您能夠在證書頒發機構簽署並返回安全證書後上傳並安裝該證書。重新啟動管理伺服器後，新憑證將生效。

- 重新產生 **HTTPS** 憑證

  使您能夠產生新的自簽名 HTTPS 證書，以取代目前的安全性證書。重新啟動 Unified Manager 後，新憑證將生效。

重新產生 **HTTPS** 憑證對話框

「重新產生 HTTPS 憑證」對話方塊可讓您自訂安全訊息，然後使用該資訊產生新的 HTTPS 憑證。

當前證書資訊出現在此頁面上。

「使用目前憑證屬性重新產生」和「更新目前憑證屬性」選擇可讓您使用目前資訊重新產生憑證或使用新資訊產生憑證。

- 通用名稱

  必需的。您希望保護的完全限定網域名稱 (FQDN)。

  在 Unified Manager 高可用性設定中，使用虛擬 IP 位址。

- 電子郵件

  選修的。用於聯絡您組織的電子郵件地址；通常是憑證管理員或 IT 部門的電子郵件地址。

- 公司

  選修的。通常是您公司的註冊名稱。

- 部門

  選修的。貴公司部門的名稱。

- 城市

  選修的。貴公司所在的城市。

- 狀態

  選修的。貴公司所在的州或省位置（不縮寫）。

- 國家

  選修的。貴公司所在的國家。這通常是該國家的兩個字母的 ISO 代碼。

- 其他名稱

  必需的。除了現有的本地主機或其他網路位址之外，還可用於存取此伺服器的附加非主要網域名稱。用逗號分隔每個備用名稱。

  如果您想要從憑證中的備用名稱欄位中刪除本機識別訊息，請勾選「排除本機識別資訊（例如 localhost）」複選框。選取此核取方塊後，只有您在欄位中輸入的內容才會在備用名稱欄位中使用。當留空時，產生的憑證將根本沒有備用名稱欄位。

- 金鑰大小（金鑰演算法：**RSA**）

  金鑰演算法設定為RSA。您可以從下列密鑰大小中選擇一個：2048、3072 或 4096 位元。預設密鑰大小設

定為 2048 位元。

- 有效期限

  預設有效期為397天。如果您從先前的版本升級，您可能會看到先前的憑證有效性保持不變。

有關詳細信息，請參閱 "產生 HTTPS 憑證"。