管理安全性憑證

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

目錄

管理安全性憑證

您可以在Unified Manager伺服器中設定HTTPS、以便透過安全連線監控及管理叢集。

檢視**HTTPS**安全性憑證

您可以將HTTPS憑證詳細資料與瀏覽器中擷取的憑證進行比較、以確保瀏覽器與Unified Manager的加密連線不會被攔截。

您需要的是什麼

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內容、或檢視可從中存取Unified Manager的主體替代名稱（SAN）。

步驟

1. 在左導覽窗格中、按一下*一般*>* HTTPS憑證*。

   HTTPS憑證會顯示在頁面頂端

如果您需要檢視安全性憑證的詳細資訊、而非HTTPS憑證頁面所顯示的詳細資訊、您可以在瀏覽器中檢視連線憑證。

正在下載**HTTPS**憑證簽署要求

您可以下載目前HTTPS安全性憑證的認證簽署要求、以便將檔案提供給憑證授權單位進行簽署。CA簽署的憑證有助於預防攔截式攻擊、並提供比自我簽署憑證更好的安全保護。

您需要的是什麼

您必須具有應用程式管理員角色。

步驟

1. 在左導覽窗格中、按一下*一般*>* HTTPS憑證*。
2. 按一下*下載HTTPS憑證簽署要求*。
3. 儲存 `<hostname>.csr` 檔案：

您可以將檔案提供給「憑證授權單位」進行簽署、然後安裝簽署的憑證。

安裝**CA**簽署並傳回**HTTPS**憑證

您可以在「憑證授權單位」簽署並傳回安全性憑證之後、再上傳及安裝安全性憑證。您上傳和安裝的檔案必須是現有自我簽署憑證的簽署版本。CA簽署的憑證有助於預防攔截式攻擊、並提供比自我簽署憑證更好的安全保護。

您需要的是什麼

您必須完成下列動作：

- 已下載「憑證簽署要求」檔案、並由「憑證授權單位」簽署
- 已將憑證鏈結儲存為PEE格式
- 包括鏈中的所有憑證、從Unified Manager伺服器憑證到根簽署憑證、包括任何存在的中繼憑證

您必須具有應用程式管理員角色。

如果建立CSR的憑證有效時間超過3997天、則CA在簽署並傳回憑證之前、將會將有效時間減至3997天

步驟

1. 在左導覽窗格中、按一下*一般*>* 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...*以找出要上傳的檔案。
4. 選取檔案、然後按一下「安裝」以安裝檔案。

   如需相關資訊、請參閱 "安裝使用外部工具產生的HTTPS憑證"。

範例憑證鏈結

下列範例顯示憑證鏈結檔案的顯示方式：

```
-----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

您可以安裝自我簽署或CA簽署的憑證、並使用OpenSSL、BoringSSL、LetsEncrypt等外部工具產生。

您應該將私密金鑰與憑證鏈結一起載入、因為這些憑證是由外部產生的公開私密金鑰配對。允許的金鑰配對演算

法為「'rSA'」和「'EC'」。「一般」區段下方的「HTTPS憑證」頁面提供「安裝**HTTPS**憑證」選項。您上傳的檔案應採用下列輸入格式。

1. 屬於Active IQ Unified Manager 該伺服器的私有金鑰
2. 與私密金鑰相符的伺服器憑證
3. CA的憑證會反轉至根憑證、用於簽署上述憑證

以**EC**金鑰配對載入憑證的格式

允許的曲線為「prime256v1」和「cep384r1」。外部產生EC配對的憑證範例：

```
 -----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-----
```

載入具有 **RSA** 金鑰配對之憑證的格式

屬於主機憑證的RSA金鑰配對允許金鑰大小為2048、3072和4096。具有外部產生* RSA金鑰組*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 更新以使變更生效。

上傳外部產生的憑證時進行檢查

系統會在上傳使用外部工具產生的憑證時執行檢查。如果有任何檢查失敗、則會拒絕該憑證。產品內的CSR產生的憑證以及使用外部工具產生的憑證也包含驗證功能。

- 輸入中的私密金鑰會根據輸入中的主機憑證進行驗證。
- 主機憑證中的「Common Name（CN）（一般名稱（CN））」會對照主機的FQDN進行檢查。
- 主機憑證的一般名稱（CN）不應為空白或空白、且不應設定為localhost。
- 有效開始日期不應為未來日期、而且憑證的有效到期日不應為過去日期。
- 如果存在中介CA或CA、則憑證的有效開始日期不應為未來日期、而且有效到期日不應為過去日期。

輸入中的私密金鑰不應加密。如果有任何私密金鑰已加密、則系統會拒絕這些金鑰。

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-----
```

憑證管理的頁面說明

您可以使用「HTTPS憑證」頁面來檢視目前的安全性憑證、並產生新的HTTPS憑證。

HTTPS憑證頁面

「HTTPS憑證」頁面可讓您檢視目前的安全性憑證、下載憑證簽署要求、產生新的自我簽署HTTPS憑證、或安裝新的HTTPS憑證。

如果您尚未產生新的自我簽署HTTPS憑證、則此頁面上顯示的憑證是安裝期間所產生的憑證。

命令按鈕

命令按鈕可讓您執行下列作業：

- 下載**HTTPS**憑證簽署要求

  下載目前安裝之HTTPS憑證的認證要求。您的瀏覽器會提示您儲存.csr檔案、以便將檔案提供給憑證授權單位進行簽署。

- 安裝**HTTPS**憑證

  可讓您在「憑證授權單位」簽署並傳回安全性憑證之後、再上傳及安裝安全性憑證。重新啟動管理伺服器後、新的憑證即會生效。

- 重新產生**HTTPS**憑證

  可讓您產生新的自我簽署HTTPS憑證、取代目前的安全性憑證。重新啟動Unified Manager之後、新的憑證即會生效。

重新產生**HTTPS**憑證對話方塊

「重新產生HTTPS憑證」對話方塊可讓您自訂安全性資訊、然後使用該資訊產生新

的HTTPS憑證。

目前的憑證資訊會顯示在此頁面上。

「使用目前的憑證屬性重新產生」和「更新目前的憑證屬性」選項可讓您以目前的資訊重新產生憑證、或是以新資訊產生憑證。

- 通用名稱

  必要。您要保護的完整網域名稱（FQDN）。

  在Unified Manager高可用度組態中、使用虛擬IP位址。

- 電子郵件

  選用。聯絡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

  選用。通常是貴公司的註冊名稱。

- 部門

  選用。貴公司部門的名稱。

- 城市

  選用。貴公司的城市位置。

- 州

  選用。貴公司的州或省位置（非縮寫）。

- 國家

  選用。貴公司的國家/地區位置。這通常是國家/地區的兩個字母ISO代碼。

- 替代名稱

  必要。除了現有的localhost或其他網路位址之外、還可用來存取此伺服器的其他非主要網域名稱。以逗號分隔每個替代名稱。

  如果您要從憑證的替代名稱欄位中移除本機識別資訊、請選取「排除本機識別資訊（例如localhost）」核取方塊。如果選中此複選框，則只有您在字段中輸入的內容才用於替代名稱字段。如果保留空白、則產生的憑證將完全沒有替代名稱欄位。

- 金鑰大小（金鑰演算法：**RSA**）

  金鑰演算法設定為RSA。您可以從其中一個金鑰大小中選取：2048、3072或4096位元。預設金鑰大小設為2048位元。

- 有效期間

預設的有效期間為397-97天。如果您已從舊版升級、則先前的憑證有效性可能會維持不變。

如需詳細資訊、請參閱 "產生HTTPS憑證"。

版權資訊

商標資訊