



管理安全性憑證

OnCommand Unified Manager 9.5

NetApp
December 20, 2023

目錄

管理安全性憑證	1
檢視HTTPS安全性憑證	1
產生HTTPS安全性憑證	1
正在下載HTTPS憑證簽署要求	3
安裝HTTPS安全性憑證	3
憑證管理的頁面說明	4

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。


開始之前

您必須OnCommand 具備「操作員」、「資訊管理員」或「儲存管理員」角色。

關於這項工作

檢視憑證可讓您驗證重新產生之憑證的內容、或檢視可用來存取Unified Manager的替代URL名稱。

步驟

1. 在工具列中、按一下、然後按一下*設定*功能表中的 HTTPS憑證*。

HTTPS憑證會顯示在頁面頂端

完成後

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。

產生HTTPS安全性憑證

您可能基於多種原因產生新的HTTPS安全性憑證、包括您想要使用不同的憑證授權單位簽署、或是目前的安全性憑證已過期。新憑證會取代現有的憑證。


開始之前

您必須OnCommand 扮演「管理員角色」。

關於這項工作

如果您無法存取Unified Manager Web UI、可以使用維護主控台重新產生具有相同值的HTTPS憑證。

步驟

1. 在工具列中、按一下、然後按一下*設定*功能表中的 HTTPS憑證*。
2. 按一下*重新產生HTTPS憑證*。

此時會顯示重新產生HTTPS憑證對話方塊。

3. 根據您要產生憑證的方式、選取下列其中一個選項：

如果您想要...	執行此動作...
以目前值重新產生憑證	按一下*使用目前的憑證屬性重新產生*選項。
使用不同的值產生憑證	<div style="border: 1px solid #ccc; padding: 10px;"><p>Click the *Update the Current Certificate Attributes* option. 如果您未輸入新值、「一般名稱」和「替代名稱」欄位會使用現有憑證的值。其他欄位不需要值、但如果您想要在憑證中填入這些值、您可以輸入城市、州和國家的值。</p></div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"><p> 如果您要從憑證的替代名稱欄位中移除本機識別資訊、可以選取「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。</p></div>

4. 按一下「是」以重新產生憑證。

5. 重新啟動Unified Manager伺服器、使新的憑證生效。

完成後

檢視HTTPS憑證來驗證新的憑證資訊。

重新啟動Unified Manager虛擬機器

您可以從Unified Manager的維護主控台重新啟動虛擬機器。您必須在產生新的安全性憑證之後重新啟動、或是虛擬機器發生問題時重新啟動。

開始之前

虛擬應用裝置已開啟電源。

您會以維護使用者的身分登入維護主控台。

關於這項工作

您也可以使用「*重新啟動來賓」選項、從vSphere重新啟動虛擬機器。如需詳細資訊、請參閱VMware文件。

步驟

1. 存取維護主控台。
2. 選擇*系統組態*>*重新開機虛擬機器*。


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。

開始之前

您必須OnCommand 扮演「管理員角色」。

步驟

1. 在工具列中、按一下、然後按一下*設定*功能表中的 HTTPS憑證*。
2. 按一下*下載HTTPS憑證簽署要求*。
3. 儲存 `<hostname>.csr` 檔案：

完成後

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HTTPS安全性憑證

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。


開始之前

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OnCommand 扮演「管理員角色」。

步驟

1. 在工具列中、按一下、然後按一下*設定*功能表中的 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。

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-----
```

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HTTPS憑證、或安裝新的HTTPS憑證。

如果您尚未產生新的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 <hostname>.csr 檔案、以便您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。

版權資訊

Copyright © 2023 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。