



建立安全通信 Element Software

NetApp
November 12, 2025

目錄

- 建立安全通信 1
 - 在您的叢集上啟用 HTTPS 的 FIPS 140-2 標準 1
 - 查找更多信息 1
- SSL密碼 1
 - 查找更多信息 3

建立安全通信

在您的叢集上啟用 HTTPS 的 FIPS 140-2 標準

您可以使用 EnableFeature API 方法為 HTTPS 通訊啟用 FIPS 140-2 操作模式。

使用 NetApp Element 軟體，您可以選擇在叢集上啟用聯邦資訊處理標準 (FIPS) 140-2 操作模式。啟用此模式將啟動 NetApp 加密安全模組 (NCSM)，並利用 FIPS 140-2 1 級認證加密，透過 HTTPS 對所有與 NetApp Element UI 和 API 的通訊進行加密。



啟用 FIPS 140-2 模式後，無法停用。啟用 FIPS 140-2 模式後，叢集中的每個節點都會重新啟動並執行自檢，以確保 NCSM 已正確啟用並在 FIPS 140-2 認證模式下運作。這會導致叢集上的管理連線和儲存連線中斷。您應該仔細規劃，只有當您的環境需要它提供的加密機制時才啟用此模式。

更多資訊請參閱 Element API 資訊。

以下是啟用 FIPS 的 API 請求範例：

```
{
  "method": "EnableFeature",
  "params": {
    "feature" : "fips"
  },
  "id": 1
}
```

啟用此操作模式後，所有 HTTPS 通訊均使用 FIPS 140-2 核准的密碼。

查找更多信息

- [SSL 密碼](#)
- ["使用 Element API 管理存儲"](#)
- ["SolidFire 和 Element 軟體文檔"](#)
- ["NetApp Element vCenter Server 插件"](#)

SSL 密碼

SSL 密碼是主機用來建立安全通訊的加密演算法。Element 軟體支援標準密碼，啟用 FIPS 140-2 模式時也支援非標準密碼。

以下列表提供了 Element 軟體支援的標準安全通訊端層 (SSL) 密碼套件，以及啟用 FIPS 140-2 模式時支援的 SSL 密碼套件：

- **FIPS 140-2** 已停用

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) -A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) -A
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A

- 符合**FIPS 140-2**標準

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) -A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) -A
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (sect571r1) - A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (sect571r1) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (sect571r1) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (sect571r1) - A
TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A

查找更多信息

[在您的叢集上啟用 HTTPS 的 FIPS 140-2 標準](#)

版權資訊

Copyright © 2025 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。