在叢集上啟用FIPS 140-2 for HTTPS

Element Software

NetApp
January 15, 2024

目錄

在叢集上啟用FIPS 140-2 for HTTPS

您可以使用啟用功能API方法、啟用FIPS 140-2操作模式進行HTTPS通訊。

有了支援的軟體、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。NetApp Element啟用此模式會啟動NetApp密碼編譯安全模組（NCSM）、並將FIPS 140-2 Level 1認證加密用於透過HTTPS傳輸至NetApp Element 整套UI和API的所有通訊。

> 啟用FIPS 140-2模式之後、就無法停用。啟用FIPS 140-2模式時、叢集中的每個節點都會重新開機並執行自我測試、以確保NCSM已正確啟用、並以FIPS 140-2認證模式運作。這會中斷叢集上的管理和儲存連線。您應該仔細規劃、而且只有在環境需要它提供的加密機制時才啟用此模式。

如需詳細資訊、請參閱Element API資訊。

以下是啟用FIPS的API要求範例：

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

啟用此操作模式之後、所有HTTPS通訊都會使用FIPS 140-2核准的密碼。

如需詳細資訊、請參閱

- SSL密碼
- "使用Element API管理儲存設備"
- "零件與元件軟體文件SolidFire"
- "vCenter Server的VMware vCenter外掛程式NetApp Element"

SSL密碼

SSL密碼是主機用來建立安全通訊的加密演算法。啟用FIPS 140-2模式時、元素軟體支援的標準密碼和非標準密碼。

下列清單提供元素軟體支援的標準安全通訊端層（SSL）密碼、以及啟用FIPS 140-2模式時支援的SSL密碼：

- * FIPS 140-2已停用*

  TLS_DHE_RSA_with _AES-122_CBC_SHA256（DH2048）- A

  TLS_DHE_RSA_with _AES-122_GCM_SHA256（DH2048）- A

TLS_DHE_RSA_AT_AES-256_CBC_SHA256（DH2048）- A

TLS_DHE_RSA_AT_AES-256_GCM_SHA384（DH2048）- A

TLS_ECDHE_RSA_with _AES-122_CBC_SHA256（secp256r1）- A

TLS_ECDHE_RSA_with _AES-122_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_AT_3DE_EDE_CBC_SHA（RSA 2048）- C

TLS_RSA_AT_AES-122_CBC_SHA（RSA 2048）- A

TLS_RSA_AT_AES-122_CBC_SHA256（RSA 2048）- A

TLS_RSA_AT_AES-122_GCM_SHA256（RSA 2048）- A

TLS_RSA_AT_AES-256_CBC_SHA（RSA 2048）- A

TLS_RSA_AT_AES-256_CBC_SHA256（RSA 2048）- A

TLS_RSA_AT_AES-256_GCM_SHA384（RSA 2048）- A

TLS_RSA_with _Camella_128_CBC_SHA（RSA 2048）- A

TLS_RSA_with _Camella_256_CBC_SHA（RSA 2048）- A

TLS_RSA_AT_ID_CBC_SHA（RSA 2048）- A

TLS_RSA_AT_RC4_122_MD5（RSA 2048）- C

TLS_RSA_AT_RC4_128_SHa（RSA 2048）- C

TLS_RSA_AT_SEIN_CBC_SHA（RSA 2048）- A

- * FIPS 140-2已啟用*

  TLS_DHE_RSA_with _AES-122_CBC_SHA256（DH2048）- A

  TLS_DHE_RSA_with _AES-122_GCM_SHA256（DH2048）- A

  TLS_DHE_RSA_AT_AES-256_CBC_SHA256（DH2048）- A

  TLS_DHE_RSA_AT_AES-256_GCM_SHA384（DH2048）- A

  TLS_ECDHE_RSA_with _AES-122_CBC_SHA256（第571r1節）- A

  TLS_ECDHE_RSA_with _AES-122_CBC_SHA256（secp256r1）- A

  TLS_ECDHE_RSA_with _AES-122_GCM_SHA256（secp256r1）- A

TLS_ECDHE_RSA_with _AES-122_GCM_SHA256（第571r1節）- A

TLS_ECDHE_RSA_with _AES-256_CBC_SHA384（第571r1節）- 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（第571r1節）- A

TLS_RSA_AT_3DE_EDE_CBC_SHA（RSA 2048）- C

TLS_RSA_AT_AES-122_CBC_SHA（RSA 2048）- A

TLS_RSA_AT_AES-122_CBC_SHA256（RSA 2048）- A

TLS_RSA_AT_AES-122_GCM_SHA256（RSA 2048）- A

TLS_RSA_AT_AES-256_CBC_SHA（RSA 2048）- A

TLS_RSA_AT_AES-256_CBC_SHA256（RSA 2048）- A

TLS_RSA_AT_AES-256_GCM_SHA384（RSA 2048）- A

如需詳細資訊、請參閱

在叢集上啟用FIPS 140-2 for HTTPS