クラスタで **HTTPS** の **FIPS 140-2** を有効にしてください

Element Software

NetApp
January 15, 2024

目次

クラスタで **HTTPS** の **FIPS 140-2** を有効にしてください

EnableFeature API メソッドを使用すると、 HTTPS 通信の FIPS 140-2 動作モードを有効にできます。

NetApp Element ソフトウェアを使用すると、クラスタで Federal Information Processing Standard （ FIPS ；連邦情報処理標準） 140-2 動作モードを有効にすることができます。このモードを有効にすると、NetApp Cryptographic Security Module（NCSM）がアクティブになり、NetApp Element UIおよびAPIとのHTTPS経由の通信にFIPS 140-2レベル1認定の暗号化が適用されるようになります。

> 一度有効にした FIPS 140-2 モードを無効にすることはできません。FIPS 140-2 モードを有効にすると、クラスタ内の各ノードがリブートされてセルフテストが実行され、 NCSM が正しく有効化されて FIPS 140-2 認定モードで動作していることが確認されます。そのため、クラスタでは管理接続とストレージ接続の両方が中断されます。このモードは、提供する暗号化メカニズムが必要な環境でのみ、慎重に計画し、有効にしてください。

詳細については、 Element API の情報を参照してください。

FIPS を有効にする API 要求の例を次に示します。

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

この動作モードを有効にすると、すべての HTTPS 通信で FIPS 140-2 で承認された暗号が使用されるようになります。

詳細については、こちらをご覧ください

- SSL 暗号
- "Element API を使用してストレージを管理します"
- "SolidFire および Element ソフトウェアのドキュメント"
- "vCenter Server 向け NetApp Element プラグイン"

SSL 暗号

SSL 暗号は、ホストがセキュアな通信を確立するために使用する暗号化アルゴリズムです。Element ソフトウェアでサポートされる標準の暗号と、 FIPS 140-2 モードが有効な場合にサポートされる非標準の暗号があります。

以下に、 Element ソフトウェアでサポートされる標準の SSL 暗号と、 FIPS 140-2 モードが有効な場合にサポートされる SSL 暗号を示します。

- * FIPS 140-2 が無効になりました *

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 （ dh 2048 ） -A

  TLS_DHE_RSA_With _AES_128_CMG_SHA256 （ dh 2048 ） - A

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 （ dh 2048 ） -A

  TLS_DHE_RSA_With _AES_256_GCM_SH384 （ dh 2048 ） - A

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 （ secp256r1 ） A

  TLS_ECDHE_RSA_With _AES_128_CMG_SHA256 （ secp256r1 ） A

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SH384 （ secp256r1 ） - A

  TLS_ECDHE_RSA_With _AES_256_GCM_SH384 （ 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_SED_CBC_SHA （ RSA 2048 ） -A

- * FIPS 140-2 が有効になりました

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 （ dh 2048 ） -A

  TLS_DHE_RSA_With _AES_128_CMG_SHA256 （ dh 2048 ） - A

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 （ dh 2048 ） -A

TLS_DHE_RSA_With _AES_256_GCM_SH384 （ dh 2048 ） - A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 （ sectr571r1 ） A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 （ secp256r1 ） A

TLS_ECDHE_RSA_With _AES_128_CMG_SHA256 （ secp256r1 ） A

TLS_ECDHE_RSA_With _AES_128_GG_SHA256 （ sectr571r1 ） A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SH384 （ sectr571r1 ） -A

TLS_ECDHE_RSA_WITH_AES_256_CBC_SH384 （ secp256r1 ） - A

TLS_ECDHE_RSA_With _AES_256_GCM_SH384 （ secp256r1 ） - A

TLS_ECDHE_RSA_with _AES_256_GCM_SH384 （ sectr571r1 ） 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

詳細については、こちらをご覧ください

クラスタで HTTPS の FIPS 140-2 を有効にしてください

著作権に関する情報

商標に関する情報