



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	1
詳細については、こちらをご覧ください	1
SSL 暗号	1

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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。