



Activez FIPS 140-2 pour HTTPS sur votre cluster

Element Software

NetApp
March 01, 2023

Table des matières

- Activez FIPS 140-2 pour HTTPS sur votre cluster 1
- Trouvez plus d'informations 1
- Chiffrement SSL 1

Activez FIPS 140-2 pour HTTPS sur votre cluster

Vous pouvez utiliser la méthode de l'API EnableFeature pour activer le mode de fonctionnement FIPS 140-2 pour les communications HTTPS.

Avec le logiciel NetApp Element, vous avez le choix d'activer le mode de fonctionnement FIPS (Federal Information Processing Standards) 140-2 sur votre cluster. L'activation de ce mode active NetApp Cryptographic Security module (NCSM) et exploite le chiffrement certifié FIPS 140-2 de niveau 1 pour toutes les communications via HTTPS vers l'interface utilisateur et l'API de NetApp Element.



Une fois le mode FIPS 140-2 activé, celui-ci ne peut pas être désactivé. Lorsque le mode FIPS 140-2-2 est activé, chaque nœud du cluster redémarre et s'exécute automatiquement pour assurer le bon fonctionnement de NCSM en mode certifié FIPS 140-2. Cela entraîne une interruption des connexions de stockage et de gestion du cluster. Vous devez planifier soigneusement et activer ce mode uniquement si votre environnement a besoin du mécanisme de chiffrement qu'il offre.

Pour plus d'informations, voir les informations de l'API Element.

Voici un exemple de demande d'API pour activer la norme FIPS :

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

Une fois ce mode de fonctionnement activé, toutes les communications HTTPS utilisent le chiffrement approuvé FIPS 140-2.

Trouvez plus d'informations

- [Chiffrement SSL](#)
- ["Gérez le stockage avec l'API Element"](#)
- ["Page Ressources SolidFire et Element"](#)
- ["Plug-in NetApp Element pour vCenter Server"](#)

Chiffrement SSL

Le chiffrement SSL sont des algorithmes de cryptage utilisés par les hôtes pour établir une communication sécurisée. Le logiciel Element prend en charge les chiffrements standard et non standard lorsque le mode FIPS 140-2 est activé.

Les listes suivantes fournissent le chiffrement SSL (Secure Socket Layer) standard pris en charge par le logiciel Element et le chiffrement SSL pris en charge lorsque le mode FIPS 140-2 est activé :

• **FIPS 140-2 désactivé**

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.

• **FIPS 140-2 activé**

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.

Trouvez plus d'informations

[Activez FIPS 140-2 pour HTTPS sur votre cluster](#)

Informations sur le copyright

Copyright © 2023 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.