



Ative o FIPS 140-2 para HTTPS no cluster

Element Software

NetApp
November 21, 2024

Índice

- Ative o FIPS 140-2 para HTTPS no cluster 1
- Encontre mais informações 1
- Cifras SSL 1

Ative o FIPS 140-2 para HTTPS no cluster

Você pode usar o método EnableFeature API para ativar o modo operacional FIPS 140-2 para comunicações HTTPS.

Com o software NetApp Element, você pode optar por ativar o modo operacional FIPS (Federal Information Processing Standards) 140-2 no cluster. Ativar este modo ativa o módulo de segurança criptográfica (NCSM) do NetApp e aproveita a criptografia com certificação FIPS 140-2 nível 1 para todas as comunicações via HTTPS para a IU e API do NetApp Element.



Depois de ativar o modo FIPS 140-2, ele não pode ser desativado. Quando o modo FIPS 140-2 está ativado, cada nó no cluster reinicializa e executa um autoteste, garantindo que o NCSM esteja corretamente ativado e funcionando no modo certificado FIPS 140-2. Isso causa uma interrupção nas conexões de gerenciamento e armazenamento no cluster. Você deve Planejar com cuidado e apenas ativar esse modo se seu ambiente precisar do mecanismo de criptografia que ele oferece.

Para obter mais informações, consulte as informações da API Element.

Veja a seguir um exemplo da solicitação de API para habilitar o FIPS:

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

Depois que este modo de funcionamento estiver ativado, todas as comunicações HTTPS utilizam as cifras aprovadas pelo FIPS 140-2.

Encontre mais informações

- [Cifras SSL](#)
- ["Gerencie o storage com a API Element"](#)
- ["Documentação do software SolidFire e Element"](#)
- ["Plug-in do NetApp Element para vCenter Server"](#)

Cifras SSL

As cifras SSL são algoritmos de criptografia usados pelos hosts para estabelecer uma comunicação segura. Existem cifras padrão que o software Element suporta e não padrão quando o modo FIPS 140-2 está ativado.

As listas a seguir fornecem as cifras SSL (Secure Socket Layer) padrão suportadas pelo software Element e as cifras SSL suportadas quando o modo FIPS 140-2 está ativado:

- **FIPS 140-2 desativado**

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 ativado**

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.

Encontre mais informações

[Ative o FIPS 140-2 para HTTPS no cluster](#)

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPTÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.