



# **Estabelecer comunicação segura**

## **Element Software**

NetApp

November 12, 2025

# Índice

- Estabelecer comunicação segura ..... 1
  - Habilite o padrão FIPS 140-2 para HTTPS no seu cluster. .... 1
    - Encontre mais informações ..... 1
- Cifras SSL ..... 1
  - Encontre mais informações ..... 3

# Estabelecer comunicação segura

## Habilite o padrão FIPS 140-2 para HTTPS no seu cluster.

Você pode usar o método de API EnableFeature para habilitar o modo de operação FIPS 140-2 para comunicações HTTPS.

Com o software NetApp Element , você pode optar por ativar o modo de operação FIPS 140-2 (Federal Information Processing Standards) em seu cluster. Habilitar este modo ativa o Módulo de Segurança Criptográfica da NetApp (NCSM) e utiliza criptografia certificada FIPS 140-2 Nível 1 para toda a comunicação via HTTPS com a interface do usuário e a API do NetApp Element .



Depois de ativar o modo FIPS 140-2, ele não poderá ser desativado. Quando o modo FIPS 140-2 está ativado, cada nó do cluster reinicia e executa um autoteste para garantir que o NCSM esteja corretamente habilitado e operando no modo certificado FIPS 140-2. Isso causa uma interrupção nas conexões de gerenciamento e armazenamento no cluster. Você deve planejar cuidadosamente e habilitar esse modo somente se o seu ambiente precisar do mecanismo de criptografia que ele oferece.

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

Segue abaixo um exemplo de solicitação à API para habilitar o FIPS:

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

Após a ativação desse modo de operação, toda a comunicação HTTPS utiliza as cifras aprovadas pelo padrão FIPS 140-2.

### Encontre mais informações

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

## Cifras SSL

Os códigos SSL são algoritmos de criptografia usados pelos servidores para estabelecer uma comunicação segura. Existem cifras padrão que o software Element suporta e cifras 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) - UMA  
TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (dh 2048) - UMA  
TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (dh 2048) - UMA  
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

- **Ativado para FIPS 140-2**

TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (dh 2048) - A  
TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (dh 2048) - UMA  
TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (dh 2048) - UMA  
TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (dh 2048) - UMA

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

[Habilite o padrão FIPS 140-2 para HTTPS no seu cluster.](#)

## **Informações sobre direitos autorais**

Copyright © 2025 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 INTERRUPÇÃO 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.