Estabelecer comunicação segura

Element Software

NetApp
November 12, 2025

Índice

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

Informações sobre marcas comerciais