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

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

Informações sobre marcas comerciais