Habilite FIPS 140-2 para HTTPS en el clúster

Element Software

NetApp
January 15, 2024

Tabla de contenidos

Habilite FIPS 140-2 para HTTPS en el clúster

Puede utilizar el método API EnableFeature para habilitar el modo operativo FIPS 140-2 para las comunicaciones HTTPS.

Con el software NetApp Element, puede optar por habilitar el modo operativo estándar de procesamiento de información federal (FIPS) 140-2 en el clúster. Al habilitar este modo, se activa el módulo de seguridad criptográfica de NetApp (NCSM) y se utiliza el cifrado certificado FIPS 140-2 de nivel 1 para toda la comunicación mediante HTTPS a la interfaz de usuario y la API de NetApp Element.

> Después de habilitar el modo FIPS 140-2-2, no puede deshabilitarse. Cuando se habilita FIPS 140-2-Mode, cada nodo del clúster se reinicia y ejecuta una prueba automática, lo que garantiza que NCSM se habilite correctamente y funcione en el modo certificado FIPS 140-2-2. Esto provoca una interrupción de las conexiones de gestión y almacenamiento en el clúster. Debe planificar con cuidado y activar este modo únicamente si su entorno necesita el mecanismo de cifrado que ofrece.

Para obtener más información, consulte la información sobre la API de Element.

A continuación se muestra un ejemplo de la solicitud de API para habilitar FIPS:

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

Una vez habilitado este modo operativo, todas las comunicaciones HTTPS utilizan los cifrados aprobados FIPS 140-2.

Obtenga más información

- Cifrados SSL
- "Gestione el almacenamiento con la API de Element"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Cifrados SSL

Los cifrados SSL son algoritmos de cifrado que utilizan los hosts para establecer una comunicación segura. Hay cifrados estándar que el software Element admite y no estándar cuando esté habilitado el modo FIPS 140-2-2.

Las siguientes listas proporcionan los cifrados estándar de capa de socket seguro (SSL) que admite el software Element y los cifrados SSL que se admiten cuando el modo FIPS 140-2 está habilitado:

- **FIPS 140-2 desactivado**

  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 habilitado**

  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.

Obtenga más información

Habilite FIPS 140-2 para HTTPS en el clúster

Información de copyright

Información de la marca comercial