



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 1
- Obtenga más información 1
- Cifrados SSL 1

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

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.