Aktivieren Sie FIPS 140-2 für HTTPS auf dem Cluster

Element Software

NetApp
January 15, 2024

Inhalt

Aktivieren Sie FIPS 140-2 für HTTPS auf dem Cluster

Sie können die API-Methode EnableFeature verwenden, um den FIPS 140-2-Betriebsmodus für HTTPS-Kommunikation zu aktivieren.

NetApp Element ermöglicht die Aktivierung des Betriebsmodus Federal Information Processing Standards (FIPS) 140-2 auf dem Cluster. Wenn Sie diesen Modus aktivieren, wird das NetApp Cryptographic Security Module (NCSM) aktiviert und für die gesamte Kommunikation über HTTPS mit der NetApp Element UI und API auf FIPS 140-2 Level 1 zertifizierte Verschlüsselung genutzt.

Nach Aktivierung des FIPS 140-2-Modus kann dieser nicht deaktiviert werden. Wenn FIPS 140-2-Modus aktiviert ist, wird jeder Node im Cluster neu gebootet und läuft über einen Selbsttest, ob das NCSM korrekt aktiviert ist und im FIPS 140-2-zertifizierten Modus betrieben wird. Dies führt zu einer Unterbrechung der Management- und Storage-Verbindungen auf dem Cluster. Sie sollten diesen Modus sorgfältig planen und nur aktivieren, wenn Ihre Umgebung die von ihm angebotenen Verschlüsselungsmechanismen benötigt.

Weitere Informationen finden Sie unter Element API Informationen.

Dies ist ein Beispiel für die API-Anforderung zur Aktivierung von FIPS:

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

Nach Aktivierung dieses Betriebsmodus werden alle HTTPS-Kommunikationen mit den nach FIPS 140-2 genehmigten Chiffren verwendet.

Weitere Informationen

- SSL-Chiffren
- "Storage-Management mit der Element API"
- "Dokumentation von SolidFire und Element Software"
- "NetApp Element Plug-in für vCenter Server"

SSL-Chiffren

SSL-Chiffren sind Verschlüsselungsalgorithmen, die von Hosts zur Einrichtung einer sicheren Kommunikation verwendet werden. Es gibt Standardchiffren, die Element Software unterstützt und nicht-Standardchiffren, wenn der FIPS 140-2-Modus aktiviert ist.

Die folgenden Listen enthalten die von der Element-Software unterstützten Standard-SSL-Chiffren (Secure Socket Layer) und die SSL-Chiffren, die unterstützt werden, wenn der FIPS 140-2-Modus aktiviert ist:

- **FIPS 140-2 deaktiviert**

  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 aktiviert**

  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

Weitere Informationen

Aktivieren Sie FIPS 140-2 für HTTPS auf dem Cluster