Abilitare FIPS 140-2 per HTTPS sul cluster

Element Software

NetApp
January 15, 2024

Sommario

Abilitare FIPS 140-2 per HTTPS sul cluster

È possibile utilizzare il metodo API EnableFeature per attivare la modalità operativa FIPS 140-2 per le comunicazioni HTTPS.

Con il software NetApp Element, è possibile attivare la modalità operativa FIPS (Federal Information Processing Standards) 140-2 sul cluster. L'attivazione di questa modalità attiva il modulo di sicurezza crittografica NetApp (NCSM) e sfrutta la crittografia certificata FIPS 140-2 livello 1 per tutte le comunicazioni via HTTPS all'interfaccia utente e all'API NetApp Element.

> Una volta attivata la modalità FIPS 140-2, non è possibile disattivarla. Quando la modalità FIPS 140-2 è attivata, ciascun nodo del cluster si riavvia ed esegue un autotest che garantisce che NCSM sia abilitato e funzioni correttamente nella modalità certificata FIPS 140-2. Ciò causa un'interruzione delle connessioni di gestione e di storage sul cluster. È necessario pianificare attentamente e attivare questa modalità solo se l'ambiente richiede il meccanismo di crittografia che offre.

Per ulteriori informazioni, vedere le informazioni sull'API Element.

Di seguito viene riportato un esempio della richiesta API per attivare FIPS:

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

Una volta attivata questa modalità operativa, tutte le comunicazioni HTTPS utilizzano le crittografia approvate da FIPS 140-2.

Trova ulteriori informazioni

- Crittografie SSL
- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Crittografie SSL

Le crittografie SSL sono algoritmi di crittografia utilizzati dagli host per stabilire una comunicazione sicura. Esistono cifrari standard supportati dal software Element e non standard quando è attivata la modalità FIPS 140-2.

I seguenti elenchi forniscono le crittografie standard SSL (Secure Socket Layer) supportate dal software Element e le crittografie SSL supportate quando la modalità FIPS 140-2 è attivata:

- **FIPS 140-2 disattivato**

  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 abilitato**

  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.

Trova ulteriori informazioni

Abilitare FIPS 140-2 per HTTPS sul cluster

Informazioni sul copyright

Informazioni sul marchio commerciale