



Abilitare FIPS 140-2 per HTTPS sul cluster

Element Software

NetApp
January 15, 2024

Sommario

- Abittare FIPS 140-2 per HTTPS sul cluster 1
- Trova ulteriori informazioni 1
- Crittografie SSL 1

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 crittografie 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

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.