



# **Sichere Kommunikation herstellen**

## Element Software

NetApp  
November 12, 2025

# Inhalt

Sichere Kommunikation herstellen.....	1
Aktivieren Sie FIPS 140-2 für HTTPS auf Ihrem Cluster.....	1
Weitere Informationen .....	1
SSL-Verschlüsselungen.....	1
Weitere Informationen .....	3

# Sichere Kommunikation herstellen

## Aktivieren Sie FIPS 140-2 für HTTPS auf Ihrem Cluster.

Mit der EnableFeature-API-Methode können Sie den FIPS 140-2-Betriebsmodus für HTTPS-Kommunikation aktivieren.

Mit der NetApp Element Software können Sie den Betriebsmodus gemäß Federal Information Processing Standards (FIPS) 140-2 auf Ihrem Cluster aktivieren. Durch die Aktivierung dieses Modus wird das NetApp Cryptographic Security Module (NCSM) aktiviert und die FIPS 140-2 Level 1-zertifizierte Verschlüsselung für die gesamte Kommunikation über HTTPS mit der NetApp Element UI und API genutzt.

 Sobald der FIPS 140-2-Modus aktiviert ist, kann er nicht mehr deaktiviert werden. Wenn der FIPS 140-2-Modus aktiviert ist, startet jeder Knoten im Cluster neu und führt einen Selbsttest durch, um sicherzustellen, dass NCSM korrekt aktiviert ist und im FIPS 140-2-zertifizierten Modus arbeitet. Dies führt zu einer Unterbrechung sowohl der Management- als auch der Speicherverbindungen im Cluster. Sie sollten sorgfältig planen und diesen Modus nur dann aktivieren, wenn Ihre Umgebung den angebotenen Verschlüsselungsmechanismus benötigt.

Weitere Informationen finden Sie in der Element-API-Dokumentation.

Nachfolgend ein Beispiel für die API-Anfrage zur Aktivierung von FIPS:

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

Nach Aktivierung dieses Betriebsmodus verwendet die gesamte HTTPS-Kommunikation die nach FIPS 140-2 zugelassenen Verschlüsselungsverfahren.

### Weitere Informationen

- [SSL-Verschlüsselungen](#)
- ["Speicherverwaltung mit der Element-API"](#)
- ["SolidFire und Element-Softwaredokumentation"](#)
- ["NetApp Element Plug-in für vCenter Server"](#)

## SSL-Verschlüsselungen

SSL-Verschlüsselungsalgorithmen werden von Hosts verwendet, um eine sichere Kommunikation herzustellen. Die Element-Software unterstützt Standard-Verschlüsselungsverfahren sowie nicht standardmäßige Verfahren, wenn der FIPS 140-

2-Modus aktiviert ist.

Die folgenden Listen enthalten die von der Element-Software unterstützten Standard-SSL-Verschlüsselungsverfahren (Secure Socket Layer) sowie die SSL-Verschlüsselungsverfahren, die im FIPS 140-2-Modus unterstützt werden:

- **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-fähig**

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 Ihrem Cluster.

## **Copyright-Informationen**

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDERWEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

**ERLÄUTERUNG ZU „RESTRICTED RIGHTS“:** Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## **Markeninformationen**

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.