



# 클러스터에서 **HTTPS**에 **FIPS 140-2**를 사용하도록 설정합니다

## Element Software

NetApp  
January 15, 2024

# 목차

|   |   |
|---|---|
| 클러스터에서 HTTPS에 FIPS 140-2를 사용하도록 설정합니다 ..... | 1 |
| 자세한 내용을 확인하십시오 .....                        | 1 |
| SSL 암호 .....                                | 1 |

# 클러스터에서 HTTPS에 FIPS 140-2를 사용하도록 설정합니다

EnableFeature API 메소드를 사용하여 HTTPS 통신에 FIPS 140-2 작동 모드를 활성화할 수 있습니다.

NetApp Element 소프트웨어를 사용하면 클러스터에서 FIPS(Federal Information Processing Standards) 140-2 운영 모드를 사용하도록 선택할 수 있습니다. 이 모드를 활성화하면 NCSM(NetApp Cryptographic Security Module)이 활성화되고 HTTPS를 통해 NetApp Element UI 및 API에 연결되는 모든 통신에 FIPS 140-2 Level 1 인증 암호화를 활용합니다.



FIPS 140-2 모드를 활성화한 후에는 비활성화할 수 없습니다. FIPS 140-2 모드를 사용하도록 설정하면 클러스터의 각 노드가 재부팅되고 자체 테스트를 통해 실행되므로 NCSM이 FIPS 140-2 인증 모드에서 올바르게 설정 및 작동할 수 있습니다. 이로 인해 클러스터의 관리 및 스토리지 연결이 모두 중단됩니다. 환경에 암호화 메커니즘이 필요한 경우에만 신중하게 계획하고 이 모드를 활성화해야 합니다.

자세한 내용은 Element API 정보를 참조하십시오.

다음은 FIPS를 사용하도록 설정하는 API 요청의 예입니다.

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

이 작동 모드가 활성화된 후 모든 HTTPS 통신은 FIPS 140-2 승인 암호를 사용합니다.

## 자세한 내용을 확인하십시오

- [SSL 암호](#)
- ["Element API를 사용하여 스토리지를 관리합니다"](#)
- ["SolidFire 및 Element 소프트웨어 설명서"](#)
- ["vCenter Server용 NetApp Element 플러그인"](#)

## SSL 암호

SSL 암호화는 호스트가 보안 통신을 설정하는 데 사용하는 암호화 알고리즘입니다. FIPS 140-2 모드가 활성화된 경우 Element 소프트웨어가 지원하는 표준 암호와 비표준 암호가 있습니다.

다음 목록은 Element 소프트웨어에서 지원되는 표준 SSL(Secure Socket Layer) 암호와 FIPS 140-2 모드가 활성화된 경우 지원되는 SSL 암호를 제공합니다.

- \* FIPS 140-2 비활성화 \*

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\_WITED\_AES\_128\_CBC\_SHA(RSA 2048)-A  
TLS\_RSA\_WITED\_AES\_128\_CBC\_SHA256(RSA 2048)-A  
TLS\_RSA\_with\_AES\_128\_GCM\_SHA256(RSA 2048)-A  
TLS\_RSA\_WITED\_AES\_256\_CBC\_SHA(RSA 2048)-A  
TLS\_RSA\_WITED\_AES\_256\_CBC\_SHA256(RSA 2048)-A  
TLS\_RSA\_WITED\_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\_WITED\_RC4\_128\_MD5(RSA 2048)-C  
TLS\_RSA\_WITED\_RC4\_128\_SHA(RSA 2048)-C  
TLS\_RSA\_WITED\_SEED\_CBC\_SHA(RSA 2048)-A

- \* FIPS 140-2 활성화 \*

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\_WITED\_AES\_128\_CBC\_SHA(RSA 2048)-A  
TLS\_RSA\_WITED\_AES\_128\_CBC\_SHA256(RSA 2048)-A  
TLS\_RSA\_with\_AES\_128\_GCM\_SHA256(RSA 2048)-A  
TLS\_RSA\_WITED\_AES\_256\_CBC\_SHA(RSA 2048)-A  
TLS\_RSA\_WITED\_AES\_256\_CBC\_SHA256(RSA 2048)-A  
TLS\_RSA\_WITED\_AES\_256\_GCM\_SHA384(RSA 2048)-A

자세한 내용을 확인하십시오

[클러스터에서 HTTPS에 FIPS 140-2를 사용하도록 설정합니다](#)

## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.