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

Element Software

NetApp
January 15, 2024

목차

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