在集群上为 **HTTPS** 启用 **FIPS 140-2**

Element Software

NetApp
October 01, 2024

目录

在集群上为 HTTPS 启用 FIPS 140-2 1
了解更多信息 1
SSL 密码 1

在集群上为 HTTPS 启用 FIPS 140-2

您可以使用 EnableFeature API 方法为 HTTPS 通信启用 FIPS 140-2 操作模式。

借助 NetApp Element 软件，您可以选择在集群上启用联邦信息处理标准（ Federal Information Processing Standards ， FIPS ） 140-2 操作模式。启用此模式将激活NetApp加密安全模块(NetApp Cryptographic Security Module、NCSM)、并对通过HTTPS与NetApp Element UI和API进行的所有通信使用FIPS 140-2 1级认证加密。

> 启用 FIPS 140-2 模式后，无法将其禁用。启用 FIPS 140-2 模式后，集群中的每个节点都会重新启动并运行自检，以确保 NCSM 已正确启用并在 FIPS 140-2 认证模式下运行。这会导致集群上的管理和存储连接中断。您应仔细规划，并且只有在您的环境需要此模式提供的加密机制时才启用此模式。

有关详细信息，请参见 Element API 信息。

以下是用于启用 FIPS 的 API 请求示例：

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

启用此操作模式后，所有 HTTPS 通信都将使用 FIPS 140-2 批准的密码。

了解更多信息

- SSL 密码
- "使用 Element API 管理存储"
- "SolidFire 和 Element 软件文档"
- "适用于 vCenter Server 的 NetApp Element 插件"

SSL 密码

SSL 密码是主机用来建立安全通信的加密算法。Element 软件支持标准密码，而启用 FIPS 140-2 模式时则支持非标准密码。

以下列表提供了 Element 软件支持的标准安全套接字层（ SSL ）密码以及启用 FIPS 140-2 模式时支持的 SSL 密码：

- 已禁用 * FIPS 140-2 *

tls_DHE_RSA_WIT_AES_128_CBC_SHA256 （DH 2048） - A

tls_DHE_RSA_WIT_AES_128_GCM_SHA256 （DH 2048） - A

tls_DHE_RSA_WIT_AES_256_CBC_SHA256 （DH 2048） - A

tls_DHE_RSA_WIT_AES_256_GCM_SHA384 （DH 2048）— A

tls_ECDHE_RSA_WITE_AES_128_CBC_SHA256 （secp256r1）— A

tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256 （secp256r1）— A

tls_ECDHE_RSA_WITE_AES_256_CBC_SHA384 （secp256r1）— A

tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384 （secp256r1）— A

tls_rsa_and_3DES_EDE_CBC_SHA （RSA 2048） - C

tls_rsa_and_aes_128_cbc_sha （RSA 2048）— A

tls_rsa_and_aes_128_cbc_SHA256 （RSA 2048） - A

tls_rsa_and_aes_128_gcm_SHA256 （RSA 2048）— A

tls_rsa_and_aes_256_cbc_sha （RSA 2048）— A

tls_rsa_and_aes_256_cbc_SHA256 （RSA 2048） - A

tls_rsa_and_aes_256_gcm_SHA384 （RSA 2048）— A

tls_rsa_and_Camellia_128_CBC_SHA （RSA 2048）— A

tls_rsa_and_Camellia_256_CBC_SHA （RSA 2048）— A

tls_rsa_and_ide_cbc_sha （RSA 2048）— A

tls_rsa_and_rc4_128_md5 （RSA 2048） - C

tls_rsa_and_rc4_128_sha （RSA 2048） - C

tls_rsa_and_seed_cbc_sha （RSA 2048）— A

- 已启用 * FIPS 140-2

tls_DHE_RSA_WIT_AES_128_CBC_SHA256 （DH 2048） - A

tls_DHE_RSA_WIT_AES_128_GCM_SHA256 （DH 2048） - A

tls_DHE_RSA_WIT_AES_256_CBC_SHA256 （DH 2048） - A

tls_DHE_RSA_WIT_AES_256_GCM_SHA384 （DH 2048）— A

tls_ECDHE_RSA_WITE_AES_128_CBC_SHA256 （sect571r1）— A

tls_ECDHE_RSA_WITE_AES_128_CBC_SHA256 （ secp256r1 ） — A

tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256 （ secp256r1 ） — A

tls_ECDHE_RSA_WIT_AES_128_GCM_SHA256 （ sect571r1 ） — A

tls_ECDHE_RSA_WITE_AES_256_CBC_SHA384 （ sect571r1 ） — A

tls_ECDHE_RSA_WITE_AES_256_CBC_SHA384 （ secp256r1 ） — A

tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384 （ secp256r1 ） — A

tls_ECDHE_RSA_WIT_AES_256_GCM_SHA384 （ sect571r1 ） — A

tls_rsa_and_3DES_EDE_CBC_SHA （ RSA 2048 ） - C

tls_rsa_and_aes_128_cbc_sha （ RSA 2048 ） — A

tls_rsa_and_aes_128_cbc_SHA256 （ RSA 2048 ） - A

tls_rsa_and_aes_128_gcm_SHA256 （ RSA 2048 ） — A

tls_rsa_and_aes_256_cbc_sha （ RSA 2048 ） — A

tls_rsa_and_aes_256_cbc_SHA256 （ RSA 2048 ） - A

tls_rsa_and_aes_256_gcm_SHA384 （ RSA 2048 ） — A

了解更多信息

在集群上为 HTTPS 启用 FIPS 140-2