



# 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\_WIT\_AES\_128\_CBC\_SHA256 ( secp256r1 ) — A  
tls\_ECDHE\_RSA\_WIT\_AES\_128\_GCM\_SHA256 ( secp256r1 ) — A  
tls\_ECDHE\_RSA\_WIT\_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\_WIT\_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](#)

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。