



启用多因素身份验证 Element Software

NetApp
January 15, 2024

This PDF was generated from https://docs.netapp.com/zh-cn/element-software-123/storage/task_system_manage_mfa_set_up_multi_factor_authentication.html on January 15, 2024. Always check docs.netapp.com for the latest.

目录

- 启用多因素身份验证 1
 - 设置多因素身份验证 1
 - 用于多因素身份验证的追加信息 1

启用多因素身份验证

多因素身份验证（MFA）通过安全断言标记语言（Security Assertion Markup Language，SAML）使用第三方身份提供程序（IdP）来管理用户会话。通过 MFA，管理员可以根据需要配置其他身份验证因素，例如密码和文本消息以及密码和电子邮件消息。

设置多因素身份验证

您可以通过 Element API 使用这些基本步骤来设置集群以使用多因素身份验证。

有关每个 API 方法的详细信息，请参见 "[Element API 参考](#)"。

1. 通过调用以下 API 方法并以 JSON 格式传递 IdP 元数据，为集群创建新的第三方身份提供程序（IdP）配置：CreateIdpConfiguration

从第三方 IdP 检索纯文本格式的 IdP 元数据。需要验证此元数据，以确保其在 JSON 中格式正确。您可以使用多种 JSON 格式化程序应用程序，例如：<https://freeformatter.com/json-escape.html>。

2. 通过 spMetadataUrl 检索集群元数据，通过调用以下 API 方法复制到第三方 IdP：
ListIdpConfigurations

spMetadataUrl 是一个 URL，用于从集群中为 IdP 检索服务提供商元数据，以便建立信任关系。

3. 在第三方 IdP 上配置 SAML 断言，使其包含 "NameID" 属性，以便为审核日志记录和单点注销正确识别用户。
4. 通过调用以下 API 方法创建一个或多个经过第三方 IdP 身份验证的集群管理员用户帐户以进行授权：
AddIdpClusterAdmin



IdP 集群管理员的用户名应与 SAML 属性名称 / 值映射匹配以获得所需效果，如以下示例所示：

- email=bob@company.com —其中 IdP 配置为释放 SAML 属性中的电子邮件地址。
- group=cluster-administrator —其中 IdP 配置为释放所有用户都应具有访问权限的组属性。请注意，出于安全考虑，SAML 属性名称 / 值配对区分大小写。

5. 通过调用以下 API 方法为集群启用 MFA：EnableIdpAuthentication

了解更多信息

- "[SolidFire 和 Element 软件文档](#)"
- "[适用于 vCenter Server 的 NetApp Element 插件](#)"

用于多因素身份验证的追加信息

您应了解以下与多因素身份验证相关的注意事项。

- 要刷新不再有效的 IdP 证书，您需要使用非 IdP 管理员用户调用以下 API 方法：

- MFA 与长度小于 2048 位的证书不兼容。默认情况下，系统会在集群上创建 2048 位 SSL 证书。调用 API 方法时，应避免设置较小的证书： `setSSLCertificate`



如果集群使用的证书在升级前小于 2048 位，则在升级到 Element 12.0 或更高版本后，必须使用 2048 位或更高版本的证书更新集群证书。

- IdP 管理员用户不能用于直接调用 API（例如通过 SDK 或 Postman）或用于其他集成（例如 OpenStack Cinder 或 vCenter 插件）。如果需要创建具有这些功能的用户，请添加 LDAP 集群管理员用户或本地集群管理员用户。

了解更多信息

- ["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"](#)

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，本文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。