启用多因素身份验证

Element Software

NetApp
October 01, 2024

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(Identity Provider、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。您可以使用许多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、以便通过调用以下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、创建一个或多个由第三方Idp进行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： `UpdateIdpConfiguration`

- 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

商标信息