常见问题解答
SANtricity 11.8

NetApp
June 24, 2024

目录

常见问题解答

为什么我无法登录?

如果在尝试登录时收到错误、请查看这些可能的原因。

出现登录错误的原因可能如下：

- 您输入的用户名或密码不正确。
- 您的权限不足。
- 您尝试多次登录失败、从而触发锁定模式。等待10分钟以重新登录。
- 已启用SAML身份验证。刷新浏览器以登录。

在添加目录服务器之前、我需要了解哪些信息?

在Access Management中添加目录服务器之前、您必须满足特定要求。

- 必须在目录服务中定义用户组。
- LDAP服务器凭据必须可用、包括域名、服务器URL以及可选的绑定帐户用户名和密码。
- 对于使用安全协议的LDAPS服务器、必须在本地计算机上安装LDAP服务器的证书链。

关于映射到存储阵列角色、我需要了解哪些信息?

在将组映射到角色之前、请查看相关准则。

RBAC (基于角色的访问控制)功能包括以下角色：

- 存储管理—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
- 安全管理—访问访问管理和证书管理中的安全配置。
- 支持管理—访问存储阵列上的所有硬件资源、故障数据和MEL事件。无法访问存储对象或安全配置。
- 监控—对所有存储对象的只读访问、但无法访问安全配置。

> 包括管理员在内的所有用户都需要"监控"角色。

如果您使用的是LDAP (轻型目录访问协议)服务器和目录服务、请确保：

- 管理员已在目录服务中定义用户组。
- 您知道LDAP用户组的组域名。

SAML

如果您使用的是存储阵列中嵌入的安全断言标记语言(SAML)功能、请确保：

- 身份提供程序(Identity Provider、IdP)管理员已在IdP系统中配置用户属性和组成员资格。
- 您知道组成员资格名称。
- 您知道要映射的组的属性值。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(\)进行转义：

```
\.[]{}()<>*+-=!?^$|
```

- 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则Unified Manager将无法对任何用户正常运行。

在配置和启用**SAML**之前、我需要了解哪些信息？

在配置和启用安全断言标记语言(SAML)身份验证功能之前、请确保满足以下要求并了解SAML限制。

要求

开始之前、请确保：

- 已在网络中配置身份提供程序(Identity Provider、IdP)。IdP是一种外部系统、用于向用户请求凭据并确定用户是否已成功通过身份验证。您的安全团队负责维护IdP。
- IdP管理员已在IdP系统中配置用户属性和组。
- IdP管理员已确保IdP支持在身份验证时返回名称ID。
- 管理员已确保IdP服务器和控制器时钟同步(通过NTP服务器或通过调整控制器时钟设置)。
- Idp元数据文件将从Idp系统下载、并在用于访问Unified Manager的本地系统上可用。
- 您知道存储阵列中控制器的IP地址或域名。

限制

除了上述要求之外、请确保您了解以下限制：

- 启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。建议您先测试SSO登录、然后再在最终配置步骤中启用SAML。(系统还会在启用SAML之前执行SSO登录测试。)
- 如果您将来禁用SAML、则系统会自动还原先前的配置(本地用户角色和/或目录服务)。
- 如果当前已为用户身份验证配置目录服务、则SAML将覆盖此配置。
- 配置SAML后、以下客户端将无法访问存储阵列资源：
  - 企业管理窗口(EMW)
  - 命令行界面（ CLI ）
  - 软件开发人员套件(SDK)客户端
  - 带内客户端

- HTTP基本身份验证REST API客户端
- 使用标准REST API端点登录

本地用户有哪些?

本地用户在系统中预定义、并包括特定权限。

本地用户包括：

- 管理员—超级管理员、有权访问系统中的所有功能。此用户包括所有角色。必须在首次登录时设置密码。
- 存储—负责所有存储配置的管理员。此用户包括以下角色：存储管理员、支持管理员和监控。在设置密码之前，此帐户将被禁用。
- 安全性—负责安全性配置的用户、包括访问管理和证书管理。此用户包括以下角色：安全管理员和监控。在设置密码之前，此帐户将被禁用。
- 支持—负责硬件资源、故障数据和固件升级的用户。此用户包括以下角色：支持管理员和监控。在设置密码之前，此帐户将被禁用。
- 监控—对系统具有只读访问权限的用户。此用户仅包含监控角色。在设置密码之前，此帐户将被禁用。
- 读/写—此用户包括以下角色：存储管理员、支持管理员和监控。在设置密码之前，此帐户将被禁用。
- * ro *(只读)—此用户仅包含监控角色。在设置密码之前，此帐户将被禁用。