



## 常见问题解答 SANtricity 11.8

NetApp  
December 16, 2024

# 目录

常见问题解答 .....	1
为什么我无法登录? .....	1
在添加目录服务器之前、我需要了解哪些信息? .....	1
关于映射到存储阵列角色、我需要了解哪些信息? .....	1
在配置和启用SAML之前、我需要了解哪些信息? .....	2
本地用户有哪些? .....	3

# 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,则必须使用反斜线转义:

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

- 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。

## 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。