概念
SANtricity 11.8

NetApp
December 16, 2024

目录

概念

访问管理的工作原理

使用访问管理在Unified Manager中建立用户身份验证。

配置工作流

访问管理配置的工作原理如下：

1. 管理员使用包含安全管理员权限的用户配置文件登录到Unified Manager。

   对于首次登录、系统会自动显示用户名 `admin`、并且无法更改。 `admin`用户可以完全访问系统中的所有功能。必须在首次登录时设置密码。

2. 管理员可在用户界面中导航到访问管理、其中包括预配置的本地用户角色。这些角色是对RBAC (基于角色的访问控制)功能的实施。
3. 管理员配置以下一种或多种身份验证方法：
   - 本地用户角色—身份验证通过RBAC功能进行管理。本地用户角色包括具有特定访问权限的预定义用户和角色。管理员可以使用这些本地用户角色作为单一身份验证方法、也可以将其与目录服务结合使用。除了为用户设置密码之外、无需进行任何配置。
   - 目录服务—身份验证通过LDAP (轻型目录访问协议)服务器和目录服务(例如Microsoft的Active Directory)进行管理。管理员连接到LDAP服务器、然后将LDAP用户映射到本地用户角色。
   - * SAML *-身份验证通过使用安全断言标记语言(SAML) 2.0的身份提供程序(IdP)进行管理。管理员在IdP系统和存储阵列之间建立通信、然后将IdP用户映射到存储阵列中嵌入的本地用户角色。
4. 管理员为用户提供Unified Manager的登录凭据。
5. 用户通过输入凭据登录到系统。登录期间、系统将执行以下后台任务：
   - 根据用户帐户对用户名和密码进行身份验证。
   - 根据分配的角色确定用户的权限。
   - 使用户能够访问用户界面中的功能。
   - 在顶部横幅中显示用户名。

Unified Manager中提供的功能

对功能的访问权限取决于为用户分配的角色、这些角色包括：

- 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。

不可用的功能将灰显或不显示在用户界面中。

访问管理术语

了解访问管理术语如何应用于Unified Manager。

期限	说明
Active Directory	Active Directory (AD)是一种Microsoft目录服务、使用LDAP进行Windows域网络。
绑定	绑定操作用于向目录服务器对客户端进行身份验证。绑定通常需要帐户和密码凭据、但某些服务器允许匿名绑定操作。
CA	证书颁发机构(Certificate Authority、CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。
证书	出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。
LDAP	轻型目录访问协议(Lightweight Directory Access Protocol、LDAP)是一种用于访问和维护分布式目录信息服务的应用程序协议。此协议允许许多不同的应用程序和服务连接到LDAP服务器以验证用户。
RBAC	基于角色的访问控制(Role-Based Access Control、RBAC)是一种根据各个用户的角色来管理对计算机或网络资源的访问的方法。Unified Manager包含预定义角色。
SAML	安全断言标记语言(SAML)是一种基于XML的标准、用于在两个实体之间进行身份验证和授权。SAML支持多因素身份验证、在这种身份验证中、用户必须提供两个或更多项来证明其身份(例如密码和指纹)。存储阵列的嵌入式SAML功能在身份断言、身份验证和授权方面符合SAML2.0标准。
SSO	单点登录(SSO)是一种身份验证服务、允许一组登录凭据访问多个应用程序。
Web服务代理	Web服务代理可通过标准HTTPS机制提供访问、允许管理员为存储阵列配置管理服务。代理可以安装在Windows或Linux主机上。Unified Manager界面可用于Web服务代理。

映射角色的权限

RBAC (基于角色的访问控制)功能包括已映射一个或多个角色的预定义用户。每个角色都具有访问Unified Manager中任务的权限。

这些角色可为用户提供对任务的访问权限、如下所示：

- 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。

如果用户没有对某个功能的权限、则该功能不可供选择或不会显示在用户界面中。

具有本地用户角色的访问管理

管理员可以使用Unified Manager中强制实施的RBAC (基于角色的访问控制)功能。这些功能称为"本地用户角色"。

配置工作流

本地用户角色已在系统中预先配置。要使用本地用户角色进行身份验证、管理员可以执行以下操作：

1. 管理员使用包含安全管理员权限的用户配置文件登录到Unified Manager。

> `admin`用户可以完全访问系统中的所有功能。

2. 管理员会查看用户配置文件、这些配置文件是预定义的、无法修改。
3. 管理员也可以为每个用户配置文件分配新密码。
4. 用户使用分配的凭据登录到系统。

管理

如果仅使用本地用户角色进行身份验证、则管理员可以执行以下管理任务：

- 更改密码。
- 设置密码的最小长度。
- 允许用户在不使用密码的情况下登录。

使用目录服务进行访问管理

管理员可以使用LDAP (轻型目录访问协议)服务器和目录服务、例如Microsoft的Active Directory。

配置工作流

如果在网络中使用LDAP服务器和目录服务、则配置的工作原理如下：

1. 管理员使用包含安全管理员权限的用户配置文件登录到Unified Manager。

> `admin`用户可以完全访问系统中的所有功能。

2. 管理员输入LDAP服务器的配置设置。设置包括域名、URL和绑定帐户信息。
3. 如果LDAP服务器使用安全协议(LDAPS)、则管理员将上传证书颁发机构(CA)证书链、以便在LDAP服务器与安装了Web服务代理的主机系统之间进行身份验证。
4. 建立服务器连接后、管理员会将用户组映射到本地用户角色。这些角色是预定义的、无法修改。
5. 管理员测试LDAP服务器与Web服务代理之间的连接。
6. 用户使用其分配的LDAP/Directory服务凭据登录到系统。

管理

使用目录服务进行身份验证时、管理员可以执行以下管理任务：

- 添加目录服务器。
- 编辑目录服务器设置。
- 将LDAP用户映射到本地用户角色。
- 删除目录服务器。
- 更改密码。
- 设置密码的最小长度。
- 允许用户在不使用密码的情况下登录。

使用SAML进行访问管理

对于访问管理、管理员可以使用阵列中嵌入的安全断言标记语言(Security Assertion Markup Language、SAML) 2.0功能。

配置工作流

SAML配置的工作原理如下：

1. 管理员使用包含"安全管理员"权限的用户配置文件登录到Unified Manager。

> `admin`用户对System Manager中的所有功能具有完全访问权限。

2. 管理员转到访问管理下的* SAML *选项卡。
3. 管理员配置与身份提供程序(Identity Provider、IdP)的通信。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。要配置与存储阵列的通信、管理员需要从Idp系统下载Idp元数据文件、然后使用Unified Manager将该文件上传到存储阵列。
4. 管理员在服务提供商和IdP之间建立信任关系。服务提供商负责控制用户授权；在这种情况下、存储阵列中的控制器充当服务提供商。要配置通信、管理员可使用Unified Manager导出控制器的服务提供商元数据文件。然后、管理员会从Idp系统将元数据文件导入到Idp中。

> 管理员还应确保IdP支持在身份验证时返回名称ID。

5. 管理员会将存储阵列的角色映射到IdP中定义的用户属性。为此、管理员使用Unified Manager创建映射。
6. 管理员测试对IdP URL的SSO登录。此测试可确保存储阵列和IdP能够进行通信。

> 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。

7. 在Unified Manager中、管理员可为存储阵列启用SAML。
8. 用户使用其SSO凭据登录到系统。

管理

使用SAML进行身份验证时、管理员可以执行以下管理任务：

- 修改或创建新角色映射
- 导出服务提供商文件

访问限制

启用SAML后、用户无法从原有Storage Manager界面发现或管理该阵列的存储。

此外、以下客户端无法访问存储阵列服务和资源：

- 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