



访问管理

SANtricity 11.8

NetApp
December 16, 2024

目录

访问管理	1
访问管理概述	1
概念	1
使用本地用户角色	6
使用目录服务	8
使用SAML	15
常见问题解答	20

访问管理

访问管理概述

访问管理是一种在Unified Manager中配置用户身份验证的方法。

有哪些身份验证方法可用？

可以使用以下身份验证方法：

- 本地用户角色—身份验证通过RBAC (基于角色的访问控制)功能进行管理。本地用户角色包括预定义的用户配置文件以及具有特定访问权限的角色。
- 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。
- * SAML *-身份验证通过使用SAML 2.0的身份提供程序(Identity Provider、IdP)进行管理。

了解更多信息。

- ["访问管理的工作原理"](#)
- ["访问管理术语"](#)
- ["映射角色的权限"](#)
- ["SAML"](#)

如何配置访问管理？

SANtricity 软件已预先配置为使用本地用户角色。如果要使用LDAP、可以在访问管理页面下对其进行配置。

了解更多信息。

- ["具有本地用户角色的访问管理"](#)
- ["使用目录服务进行访问管理"](#)
- ["配置SAML"](#)

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 workflow

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。

期限	说明
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端之间建立安全连接。
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 workflow

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 workflow

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 workflow

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

使用本地用户角色

查看本地用户角色

在本地用户角色选项卡中、您可以查看用户与默认角色的映射。这些映射是Unified Manager Web服务代理中强制实施的RBAC (基于角色的访问控制)的一部分。

开始之前

您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

关于此任务

无法更改用户和映射。只能修改密码。

步骤

1. 选择*访问管理*。
2. 选择*本地用户角色*选项卡。

下表显示了这些用户：

- 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。
- 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。
- 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。
- 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。

- 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。
- 读/写—此用户包括以下角色：存储管理员、支持管理员和监控。
- * ro *(只读)—此用户仅包含监控角色。

更改本地用户配置文件的密码

您可以在Access Management中更改每个用户的用户密码。

开始之前

- 您必须以本地管理员身份登录、其中包括root管理员权限。
- 您必须知道本地管理员密码。

关于此任务

选择密码时、请记住以下准则：

- 任何新的本地用户密码必须满足或超过当前最低密码设置(在"查看/编辑设置"中)。
- 密码区分大小写。
- 设置密码时、不会从密码中删除尾随空格。如果密码中包含空格、请小心操作。
- 为了提高安全性、请至少使用15个字母数字字符并频繁更改密码。

步骤

1. 选择*访问管理*。
2. 选择*本地用户角色*选项卡。
3. 从表中选择一个用户。

更改密码按钮将变为可用。

4. 选择 * 更改密码 * 。

此时将打开更改密码对话框。

5. 如果未为本地用户密码设置最小密码长度、则可以选中此复选框以要求用户输入密码以访问系统。
6. 在两个字段中输入选定用户的新密码。
7. 输入本地管理员密码以确认此操作、然后单击*更改*。

结果

如果用户当前已登录、则更改密码会导致用户的活动会话终止。

更改本地用户密码设置

您可以为所有新的或更新的本地用户密码设置所需的最小长度。您还可以允许本地用户访问系统而无需输入密码。

开始之前

您必须以本地管理员身份登录、其中包括root管理员权限。

关于此任务

设置本地用户密码的最小长度时、请记住以下准则：

- 设置更改不会影响现有本地用户密码。
- 本地用户密码的最小长度设置必须介于0到30个字符之间。
- 任何新的本地用户密码都必须满足或超过当前的最小长度设置。
- 如果希望本地用户在不输入密码的情况下访问系统、请勿设置密码的最小长度。

步骤

1. 选择*访问管理*。
2. 选择*本地用户角色*选项卡。
3. 选择*查看/编辑设置*。

此时将打开本地用户密码设置对话框。

4. 执行以下操作之一：
 - 要允许本地用户在不输入密码的情况下访问系统、请清除"至少需要所有本地用户密码"复选框。
 - 要为所有本地用户密码设置最小密码长度、请选中"要求所有本地用户密码至少为"复选框、然后使用spinner框设置所有本地用户密码所需的最小长度。

任何新的本地用户密码都必须满足或超过当前设置。

5. 单击 * 保存 *。

使用目录服务

添加目录服务器

要为访问管理配置身份验证、请在LDAP服务器与运行适用于Unified Manager的Web服务代理的主机之间建立通信。然后、将LDAP用户组映射到本地用户角色。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 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。

关于此任务

添加目录服务器分为两步。首先输入域名和URL。如果服务器使用安全协议、则如果CA证书由非标准签名颁发机构签名、则还必须上传此CA证书以进行身份验证。如果您拥有绑定帐户的凭据、则还可以输入您的用户帐户名称和密码。接下来、将LDAP服务器的用户组映射到本地用户角色。

步骤

1. 选择*访问管理*。
2. 从*目录服务*选项卡中、选择*添加目录服务器*。

此时将打开添加目录服务器对话框。

3. 在*服务器设置*选项卡中、输入LDAP服务器的凭据。

字段详细信息

设置	说明
配置设置	域
输入LDAP服务器的域名。对于多个域、请在逗号分隔列表中输入域。域名用于登录(<i>username@domain</i>)以指定要对其进行身份验证的目录服务器。	服务器URL
以的形式输入用于访问LDAP服务器的URL <code>ldap[s]://host:*port*</code> 。	上传证书(可选)
<div style="display: flex; align-items: center;">  <div> <p>只有在上述服务器URL字段中指定了LDAP S协议时、才会显示此字段。</p> </div> </div> <p>单击*浏览*并选择要上传的CA证书。这是用于对LDAP服务器进行身份验证的可信证书或证书链。</p>	绑定帐户(可选)
输入一个只读用户帐户、用于对LDAP服务器进行搜索查询以及在组中进行搜索。以LDAP类型格式输入帐户名称。例如，如果绑定用户名为“bindacct”，则可以输入一个值，例如 <code>CN=bindacct,CN=Users,DC=cpoc,DC=local</code> 。	绑定密码(可选)

设置	说明
 <p>输入绑定帐户时会显示此字段。</p> <p>输入绑定帐户的密码。</p>	添加前测试服务器连接
<p>如果要确保系统可以与您输入的LDAP服务器配置进行通信、请选中此复选框。单击对话框底部的*添加*后、将进行测试。</p> <p>如果选中此复选框且测试失败、则不会添加配置。您必须解决此错误或取消选中此复选框、才能跳过测试并添加配置。</p>	权限设置
搜索基础DN	输入LDAP环境以搜索用户，通常以的形式 CN=Users, DC=cpoc, DC=local。
username属性	输入绑定到用户ID的属性以进行身份验证。例如： sAMAccountName。
组属性	输入用户上的组属性列表、用于组到角色映射。例如： memberOf, managedObjects。

- 单击*角色映射*选项卡。
- 将LDAP组分配给预定义角色。一个组可以分配多个角色。

字段详细信息

设置	说明
映射	组DN
为要映射的LDAP用户组指定组可分辨名称(DN)。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： \ [] {} ()<>*+.=! ? ^\$\	角色



包括管理员在内的所有用户都需要"监控"角色。

6. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
7. 完成映射后、单击*添加*。

系统将执行验证、以确存储阵列和LDAP服务器可以进行通信。如果显示错误消息、请检查在对话框中输入的凭据、并根据需要重新输入信息。

编辑目录服务器设置和角色映射

如果您之前在Access Management中配置了目录服务器、则可以随时更改其设置。设置包括服务器连接信息和组到角色映射。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 必须定义目录服务器。

步骤

1. 选择*访问管理*。
2. 选择*目录服务*选项卡。
3. 如果定义了多个服务器、请从表中选择要编辑的服务器。
4. 选择*查看/编辑设置*。

此时将打开目录服务器设置对话框。

5. 在*服务器设置*选项卡中、更改所需设置。

字段详细信息

设置	说明
配置设置	域
LDAP服务器的域名。对于多个域、请在逗号分隔列表中输入域。域名用于登录(<i>username@domain</i>)以指定要对其进行身份验证的目录服务器。	服务器URL
用于访问LDAP服务器的URL，格式为 ldap[s]://host:port。	绑定帐户(可选)
用于对LDAP服务器进行搜索查询以及在组内进行搜索的只读用户帐户。	绑定密码(可选)
绑定帐户的密码。(输入绑定帐户时会显示此字段。)	保存前测试服务器连接
检查系统是否可以与LDAP服务器配置进行通信。单击*保存*后会进行测试。如果选中此复选框且测试失败、则不会更改配置。您必须解决此错误或清除此复选框、才能跳过测试并重新编辑配置。	权限设置
搜索基础DN	用于搜索用户的LDAP环境，通常采用的形式 CN=Users, DC=cpoc, DC=local。
username属性	绑定到用户ID进行身份验证的属性。例如： sAMAccountName。
组属性	用户上的组属性列表、用于组到角色映射。例如： memberOf, managedObjects。

6. 在*角色映射*选项卡中、更改所需的映射。

字段详细信息

设置	说明
映射	组DN
要映射的LDAP用户组的域名。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： \ [] {} (<>*+==! ? ^\$	
角色	要映射到组DN的角色。您必须单独为此组选择要包含的每个角色。要登录到SANtricity Unified Manager、需要将监控角色与其他角色结合使用。这些角色包括： <ul style="list-style-type: none">• 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。

7. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
8. 单击 * 保存 *。

结果

完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

删除目录服务器

要中断目录服务器与Web服务代理之间的连接、您可以从"访问管理"页面中删除服务器信息。如果您配置了新服务器、然后要删除旧服务器、则可能需要执行此任务。

开始之前

您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

关于此任务

完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

步骤

1. 选择*访问管理*。
2. 选择*目录服务*选项卡。
3. 从列表中、选择要删除的目录服务器。
4. 单击 * 删除 *。

此时将打开删除目录服务器对话框。

5. 键入 `remove` 字段，然后单击*Remove*。

此时将删除目录服务器配置设置、权限设置和角色映射。用户无法再使用此服务器的凭据登录。

使用SAML

配置SAML

要为访问管理配置身份验证、您可以使用存储阵列中嵌入的安全断言标记语言(SAML)功能。此配置将在身份提供程序和存储提供程序之间建立连接。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 您必须知道存储阵列中控制器的IP地址或域名。
- IdP管理员已配置IdP系统。
- 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、并可在用于访问Unified Manager的本地系统上使用。

关于此任务

身份提供程序(IdP)是一种外部系统、用于向用户请求凭据并确定该用户是否已成功通过身份验证。可以将IdP配置为提供多因素身份验证并使用任何用户数据库、例如Active Directory。您的安全团队负责维护IdP。服务提供商(Service Provider、SP)是一个控制用户身份验证和访问的系统。使用SAML配置访问管理时、存储阵列充当服务提供商、向身份提供程序请求身份验证。要在IdP和存储阵列之间建立连接、您需要在这两个实体之间共享元数据文件。接下来、将IdP用户实体映射到存储阵列角色。最后、在启用SAML之前、您需要测试连接和SSO登录。



- SAML和目录服务*。如果在将目录服务配置为身份验证方法时启用SAML、则SAML将取代Unified Manager中的目录服务。如果稍后禁用SAML、则目录服务配置将返回到其先前的配置。



- *编辑和禁用。*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。

配置SAML身份验证是一个多步骤操作步骤。

第1步：上传IdP元数据文件

要为存储阵列提供Idp连接信息、请将Idp元数据导入到Unified Manager中。IdP系统需要使用此元数据将身份验证请求重定向到正确的URL并验证收到的响应。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*SAML*选项卡。

此页面将显示配置步骤的概述。

3. 单击*导入身份提供程序(IdP)文件*链接。

此时将打开导入身份提供程序文件对话框。

4. 单击*浏览*以选择您复制到本地系统的IdP元数据文件并将其上传。

选择文件后、将显示IdP实体ID。

5. 单击 * 导入 *。

第2步：导出服务提供商文件

要在IdP和存储阵列之间建立信任关系、请将服务提供商元数据导入到IdP中。Idp需要此元数据才能与控制器建立信任关系并处理授权请求。此文件包含控制器域名或IP地址等信息、以便IdP可以与服务提供商进行通信。

步骤

1. 单击*导出服务提供商文件*链接。

此时将打开导出服务提供商文件对话框。

2. 在*控制器A*字段中输入控制器IP地址或DNS名称、然后单击*导出*将元数据文件保存到本地系统。

单击*导出*后、服务提供商元数据将下载到本地系统。记下文件的存储位置。

3. 从本地系统中、找到您导出的XML格式的服务提供商元数据文件。
4. 从Idp服务器中、导入服务提供商元数据文件以建立信任关系。您可以直接导入文件、也可以手动输入文件中的控制器信息。

第3步：映射角色

要为用户提供对Unified Manager的授权和访问权限、您必须将Idp用户属性和组成员资格映射到存储阵列的预定义角色。

开始之前

- IdP管理员已在IdP系统中配置用户属性和组成员资格。
- Idp元数据文件将导入到Unified Manager中。
- 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。

步骤

1. 单击*映射Unified Manager*角色的链接。

此时将打开角色映射对话框。

2. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。

字段详细信息

设置	说明
映射	用户属性
指定要映射的SAML组的属性(例如、"member for")。	属性值
指定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,则必须使用反斜杠转义: \\ [] { } () < > * + = ! ? ^ \$	
角色	<p>单击此字段、然后选择要映射到此属性的存储阵列角色之一。您必须单独选择要包括的每个角色。要登录到Unified Manager、需要将"监控"角色与其他角色结合使用。至少一个组还需要安全管理员角色。</p> <p>映射的角色包括以下权限:</p> <ul style="list-style-type: none">• 存储管理—对存储对象(例如卷和磁盘池)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、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。• 支持管理—访问存储阵列上的所有硬件资源、故障数据、MEL事件和控制器固件升级。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。如果没有"监控"角色、则Unified Manager将无法对任何用户正常运行。

3. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。



启用SAML后、可以修改角色映射。

4. 完成映射后、单击*保存*。

第4步：测试SSO登录

为了确保IdP系统和存储阵列可以进行通信、您可以选择测试SSO登录。在启用SAML的最后一步中、也会执行此测试。

开始之前

- Idp元数据文件将导入到Unified Manager中。
- 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。

步骤

1. 选择*测试SSO登录*链接。

此时将打开一个对话框、用于输入SSO凭据。

2. 输入具有安全管理员权限和监控权限的用户的登录凭据。

在系统测试登录时、将打开一个对话框。

3. 查找Test Successful消息。如果测试成功完成、请转至下一步以启用SAML。

如果测试未成功完成、则会显示一条错误消息、其中包含更多信息。请确保：

- 该用户属于具有安全管理员和监控权限的组。
- 您为IdP服务器上传的元数据正确无误。
- SP元数据文件中的控制器地址正确。

第5步：启用SAML

最后一步是完成用户身份验证的SAML配置。在此过程中、系统还会提示您测试SSO登录。上一步介绍了SSO登录测试过程。

开始之前

- Idp元数据文件将导入到Unified Manager中。
- 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。
- 至少配置了一个监控器和一个安全管理员角色映射。



*编辑和禁用。*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。

步骤

1. 从* SAML *选项卡中、选择*启用SAML *链接。

此时将打开确认启用SAML对话框。

2. 键入 enable, 然后单击*Enable*。
3. 输入用于SSO登录测试的用户凭据。

结果

系统启用SAML后、它将终止所有活动会话并开始通过SAML对用户进行身份验证。

更改SAML角色映射

如果先前已为访问管理配置SAML、则可以更改IdP组与存储阵列的预定义角色之间的角色映射。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- IdP管理员已在IdP系统中配置用户属性和组成员资格。
- 已配置并启用SAML。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*SAML*选项卡。
3. 选择*角色映射*。

此时将打开角色映射对话框。

4. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。



请注意、在启用SAML的情况下、不要删除您的权限、否则您将无法访问Unified Manager。

字段详细信息

设置	说明
映射	用户属性
指定要映射的SAML组的属性(例如、"member for")。	属性值
指定要映射的组的属性值。	角色



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。

5. 或者、也可以单击*添加另一个映射*以输入更多组到角色的映射。
6. 单击 * 保存 *。

结果

完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

导出SAML服务提供程序文件

如有必要、您可以导出存储阵列的服务提供程序元数据、然后将该文件重新导入到身份提供程序(Identity Provider、Idp)系统中。

开始之前

- 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
- 已配置并启用SAML。

关于此任务

在此任务中、您将从控制器导出元数据。Idp需要此元数据才能与控制器建立信任关系并处理身份验证请求。此文件包含IdP可用于发送请求的控制器域名或IP地址等信息。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*SAML*选项卡。
3. 选择*导出*。

此时将打开导出服务提供商文件对话框。

4. 单击*Export*将元数据文件保存到本地系统。



域名字段为只读。

记下文件的存储位置。

5. 从本地系统中、找到您导出的XML格式的服务提供商元数据文件。
6. 从Idp服务器中、导入服务提供商元数据文件。您可以直接导入文件、也可以手动输入控制器信息。
7. 单击 * 关闭 *。

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。