访问管理
SANtricity 11.7

NetApp
February 12, 2024

目录

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。

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"

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"

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、为用户名 `admin` 将自动显示、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。
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	**Description**
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。

期限	Description
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。
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未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

正在设置 ...	Description
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(*username@domain*)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 `ldap[s]://**host**:*port*`。	上传证书(可选)
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。 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。	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 `CN=bindacct,CN=Users,DC=cpoc,DC=local`。	绑定密码(可选)

正在设置 ...	Description
输入绑定帐户时会显示此字段。 输入绑定帐户的密码。	添加前测试服务器连接
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。 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。	权限设置
搜索基础DN	输入LDAP环境以搜索用户、通常采用的形式 `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`。

4. 单击*角色映射*选项卡。
5. 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

正在设置 ...	Description
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	单击此字段、然后选择要映射到组DN的本地用户角色之一。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。映射的角色包括以下权限： • 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。

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、以确保存储阵列和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

正在设置 ...	Description
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(*username*@*domain*)以指定要对其进行身份验证的目录服务器。	服务器URL
用于以形式访问LDAP服务器的URL `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

正在设置 ...	Description
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： • 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. Type `remove` 在字段中，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。

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。

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。

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。