访问管理

SANtricity 11.5

NetApp
February 12, 2024

目录

访问管理 1
- 概念 1
- 操作说明 6
- 常见问题解答 24

访问管理

概念

访问管理的工作原理

访问管理是在SANtricity System Manager中建立用户身份验证的一种方法。身份验证要求用户使用分配的凭据登录到这些系统。

访问管理配置和用户身份验证的工作原理如下：

1. 管理员使用具有安全管理员权限的用户配置文件登录到System Manager。

   首次登录时、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。

2. 管理员可在用户界面中导航到访问管理。存储阵列已预先配置为使用本地用户角色、这是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—身份验证通过在存储阵列中强制实施的RBAC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。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用户映射到存储阵列中嵌入的本地用户角色。
   - * 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System Manager的登录凭据。
5. 用户通过输入凭据登录到系统。

   如果使用SAML和SSO (单点登录)管理身份验证、则系统可能会绕过System Manager登录对话框。

   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。
   - 为用户提供对用户界面中任务的访问权限。
   - 显示界面右上角的用户名。

System Manager中提供的任务

任务访问权限取决于用户分配的角色、这些角色包括：

- 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。

不可用的任务将灰显或不显示在用户界面中。例如、具有"监控"角色的用户可以查看有关卷的所有信息、但无法访问用于修改该卷的功能。诸如*复制服务*和*添加到工作负载*等功能的选项卡将灰显；只有查看/编辑设置可用。

用户对**SANtricity** 存储管理器的访问权限

配置本地用户角色和目录服务后、用户必须先输入凭据、然后才能在企业管理窗口(EMW)中执行以下任一功能：

- 重命名存储阵列
- 正在升级控制器固件
- 正在加载存储阵列配置
- 正在执行脚本
- 正在尝试在未使用的会话超时时时执行活动操作

如果为存储阵列配置了SAML、则用户无法使用EMW发现或管理该阵列的存储。

访问管理术语

了解访问管理术语如何应用于存储阵列。

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
IdP	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。
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。RBAC控制会在存储阵列上强制实施、并包括预定义的角色。
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功能符合SAML2.0标准、可用于身份断言、身份验证和授权。
SP	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。
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。

映射角色的权限

在存储阵列上强制实施的RBAC (基于角色的访问控制)功能包括预定义的用户配置文件、其中一个或多个角色映射到这些配置文件。每个角色都具有访问SANtricity System Manager中任务的权限。

用户配置文件和映射的角色可从任一System Manager的用户界面中的菜单：设置[访问管理>本地用户角色]进行访问。

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。

如果用户没有执行某个任务的权限、则该任务将灰显或不会显示在用户界面中。

具有本地用户角色的访问管理

对于访问管理、管理员可以使用在存储阵列中强制实施的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

已为存储阵列预先配置本地用户角色。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SANtricity 系统管理器。

   `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

对于访问管理、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SANtricity 系统管理器。

   `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服务器和存储阵列之间进行身份验证。

4. 建立服务器连接后、管理员会将用户组映射到存储阵列的角色。这些角色是预定义的、无法修改。
5. 管理员测试LDAP服务器与存储阵列之间的连接。
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。

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. 管理员使用具有安全管理员权限的用户配置文件登录到System Manager。

   `admin`用户可以完全访问System Manager中的所有功能。

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、管理员将从IdP系统下载IdP元数据文件、然后使用System Manager将此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、管理员可以使用System Manager导出每个控制器的服务提供商元数据文件。然后、管理员从IdP系统将这些元数据文件导入到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、管理员可以使用System 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System Manager中、管理员为存储阵列启用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、以下客户端将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

操作说明

查看本地用户角色

在本地用户角色选项卡中、您可以查看用户配置文件与默认角色的映射。这些映射是在存储阵列中强制实施的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

无法更改用户配置文件和映射。只能修改密码。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*本地用户角色*选项卡。

   下表显示了用户配置文件：

   - * root admin*(admin)—超级管理员、有权访问系统中的所有功能。此用户配置文件包含所有角色。
   - 存储管理(存储)—负责所有存储配置的管理员。此用户配置文件包括以下角色：存储管理员、支持管理员和监控。
   - 安全性管理(安全性)—负责安全配置的用户、包括访问管理、证书管理和启用了安全保护的驱动器功能。此用户配置文件包括以下角色：安全管理员和监控。
   - 支持管理(支持)—负责硬件资源、故障数据和固件升级的用户。此用户配置文件包括以下角色：Support Admin和Monitor。

◦ 监控(监控)—对系统具有只读访问权限的用户。此用户配置文件仅包含监控角色。

更改密码

您可以在Access Management中更改每个用户配置文件的用户密码。

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、密码中的后缀空格不会被删除。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。

> 在System Manager中更改密码也会在命令行界面(CLI)中进行更改。此外、密码还会将发生原因用户的活动会话更改为终止。

步骤

1. 选择菜单：设置[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、则可以选中此框以要求选定用户输入密码以访问存储阵列、然后您可以键入选定用户的新密码。
6. 输入本地管理员密码、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

您可以为存储阵列上的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在不输入密码的情况下访问存储阵列。

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存储阵列、请勿设置密码的最小长度。

步骤

1. 选择菜单：设置[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*按钮。

   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存储阵列、请取消选中"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 * 。

添加目录服务器

要为访问管理配置身份验证、您可以在存储阵列和LDAP服务器之间建立通信、然后将LDAP用户组映射到阵列的预定义角色。

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存储阵列的预定义角色。

在操作步骤 添加LDAP服务器期间、原有管理界面将被禁用。原有管理界面(符号)是存储阵列与管理客户端之间的一种通信方法。禁用后、存储阵列和管理客户端将使用更安全的通信方法(基于https的REST API)。

步骤

1. 选择菜单：设置[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
输入用于访问LDAP服务器的URL、格式为`ldap：//*host*：*port*`。	上传证书(可选)
只有在上述服务器URL字段中指定了LDAPS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"cn=bindAcct、cn=users、DC=cpoc、DC=local"等值。	绑定密码(可选)
输入上述绑定帐户时、将显示此字段。 输入绑定帐户的密码。	添加前测试服务器连接
如果要确保存储阵列可以与您输入的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、通常形式为`CN=Users、DC=cOPC、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`。

正在设置 ...	Description
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)。	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System Manager将无法正常运行。

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. 选择菜单：设置[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。

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
用于访问LDAP服务器的URL、格式为`ldap：//*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
检查存储阵列是否可以与LDAP服务器配置进行通信。单击对话框底部的保存后、将进行测试。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取消选中此复选框、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`CN=Users、DC=cOPC、DC=local`的形式。
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。

正在设置 ...	Description
映射	组DN
要映射的LDAP用户组的域名。	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System Manager将无法正常运行。

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存储阵列之间的连接、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. 选择菜单：设置[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. 在字段中键入`remove`、然后单击*删除*。

   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。

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。

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System 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。

*正在编辑和禁用。*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
- 第2步：导出服务提供商文件
- 第3步：映射角色
- 第4步：测试SSO登录
- 第5步：启用SAML

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System Manager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。
- 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保持同步(通过NTP服务器或通过调整控制器时钟设置)。
- IdP元数据文件从IdP系统下载、并可从用于访问System Manager的本地系统上获得。

关于此任务

在此任务中、您将元数据文件从IdP上传到System Manager。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。您只需为存储阵列上传一个元数据文件、即使有两个控制器也是如此。

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。

开始之前

- 您知道存储阵列中每个控制器的IP地址或域名。

关于此任务

在此任务中、您将从控制器导出元数据(每个控制器一个文件)。IdP需要使用此元数据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。如果存储阵列包含两个控制器、请对*控制器B*字段中的第二个控制器重复此步骤。

   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. 在本地系统中、找到您导出的服务提供商元数据文件。

   每个控制器都有一个XML格式的文件。

4. 从IdP服务器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System 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System Manager中。
- 每个控制器的服务提供商元数据文件都会导入到IdP系统中以建立信任关系。

关于此任务

在此任务中、您可以使用System Manager将IdP组映射到本地用户角色。

步骤

1. 单击链接以映射System Manager角色。

   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

正在设置 ...	Description
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System Manager将无法正常运行。

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System Manager中。
- 每个控制器的服务提供商元数据文件都会导入到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**

最后一步是启用SAML用户身份验证。

开始之前

- IdP元数据文件将导入到System Manager中。
- 每个控制器的服务提供商元数据文件都会导入到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。

关于此任务

此任务介绍如何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。

*正在编辑和禁用。*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*启用*。
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时、您不会删除权限、否则您将无法访问System Manager。

字段详细信息

正在设置 ...	Description
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System Manager将无法正常运行。

5. *可选：*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商元数据并将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(每个控制器一个文件)。IdP需要使用此元数据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. 对于每个控制器、单击*导出*将元数据文件保存到本地系统。

每个控制器的域名字段均为只读字段。

记下文件的存储位置。

5. 在本地系统中、找到您导出的服务提供商元数据文件。

   每个控制器都有一个XML格式的文件。

6. 从IdP服务器导入服务提供商元数据文件。您可以直接导入文件、也可以手动输入文件中的控制器信息。
7. 单击 * 关闭 * 。

查看审核日志活动

通过查看审核日志、具有安全管理员权限的用户可以监控用户操作、身份验证失败、无效登录尝试以及用户会话生命周期。

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。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*审核日志*选项卡。

   *审核日志*活动以表格形式显示、其中包括以下信息列：

   - 日期/时间-存储阵列检测到事件的时间戳(GMT)。
   - 用户名-与事件关联的用户名。对于存储阵列上的任何未经身份验证的操作、"N/A"将显示为用户名。未经过身份验证的操作可能由内部代理或其他机制触发。
   - 状态代码—操作的HTTP状态代码(200、400等)以及与事件关联的描述性文本。
   - "已访问**URL**"-完整URL (包括主机)和查询字符串。
   - 客户端**IP**地址-与事件关联的客户端的IP地址。
   - 源—与事件关联的日志记录源、可以是System Manager、CLI、Web服务或支持Shell。
3. 使用审核日志页面上的选项可查看和管理事件。

选择详细信息

选择	Description
显示事件	按日期范围(过去24小时、过去7天、过去30天或自定义日期范围)显示的限制事件。
筛选器	限制按字段中输入的字符显示的事件。请使用引号("")来精确匹配字词、输入`或`返回一个或多个字词、或者输入短划线("-")来省略字词。
刷新	选择*刷新*可将页面更新为最新事件。
查看/编辑设置	选择*查看/编辑设置*以打开一个对话框、在此可以指定完整的日志策略以及要记录的操作级别。
删除事件	选择*删除*以打开一个对话框、在此可以从页面中删除旧事件。
显示/隐藏列	单击*显示/隐藏*列图标 可选择其他列以显示在表中。其他列包括： • 方法- HTTP方法(例如POST、GET、DELETE等)。 • 已执行命令行界面命令—为安全命令行界面请求执行的命令行界面命令(语法)。 • 命令行界面返回状态—命令行界面状态代码或客户端请求输入文件。 • *符号操作步骤 *—符号操作步骤 已执行。 • * SSH事件类型*-安全Shell (SSH)事件类型、例如login、logout和login_fail。 • * SSH会话PID*—SSH会话的进程ID号。 • * SSH会话持续时间*-用户登录的秒数。
切换列筛选器	单击*切换*图标 打开每个列的筛选字段。在列字段中输入字符、以限制这些字符显示的事件。再次单击图标以关闭筛选字段。
撤消更改	单击*撤消*图标 以将此表恢复为默认配置。
导出	单击*导出*将表数据保存到逗号分隔值(CSV)文件。

定义审核日志策略

您可以更改覆盖策略以及审核日志中记录的事件类型。

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

此任务介绍如何更改审核日志设置、其中包括用于覆盖旧事件的策略以及用于记录事件类型的策略。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*审核日志*选项卡。
3. 选择*查看/编辑设置*。

   此时将打开*审核日志设置*对话框。

4. 更改覆盖策略或记录的事件类型。

   字段详细信息

正在设置 ...	Description
覆盖策略	确定达到最大容量时用于覆盖旧事件的策略： • 允许在审核日志已满时覆盖审核日志中最早的事件-当审核日志达到50、000条记录时覆盖旧事件。 • 需要手动删除审核日志事件-指定不会自动删除事件；而是以设置的百分比显示阈值警告。必须手动删除事件。 如果禁用了覆盖策略、并且审核日志条目达到最大限制、则没有安全管理员权限的用户将无法访问System Manager。要还原没有安全管理员权限的用户的系统访问权限、分配有安全管理员角色的用户必须删除旧事件记录。 如果为归档审核日志配置了系统日志服务器、则覆盖策略不适用。
要记录的操作级别	确定要记录的事件类型： • 仅记录修改事件-仅显示用户操作涉及在系统中进行更改的事件。 • 记录所有修改和只读事件-显示所有事件、包括涉及读取或下载信息的用户操作。

5. 单击 * 保存 * 。

从审核日志中删除事件

您可以清除旧事件的审核日志、从而使搜索事件更易于管理。删除后、您可以选择将旧事件保存到CSV (逗号分隔值)文件中。

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。

关于此任务

此任务介绍如何从审核日志中删除旧事件。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*审核日志*选项卡。
3. 选择 * 删除 * 。

   此时将打开*删除审核日志对话框*。

4. 选择或输入要删除的最旧事件的数量。
5. 如果要将已删除的事件导出到CSV文件(建议)、请保持选中状态。在下一步中单击*删除*时、系统将提示您输入文件名和位置。否则、如果您不想将事件保存到CSV文件、请单击复选框以取消选中它。
6. 单击 * 删除 * 。

   此时将打开确认对话框。

7. 在字段中键入`delete`、然后单击*删除*。

   最早的事件将从审核日志页面中删除。

为审核日志配置系统日志服务器

如果要将审核日志归档到外部系统日志服务器、则可以配置该服务器与存储阵列之间的通信。建立连接后、审核日志会自动保存到系统日志服务器。

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。
- 系统日志服务器地址、协议和端口号必须可用。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
- 如果您的服务器使用安全协议(例如TLS)、则本地系统上必须具有证书颁发机构(CA)证书。CA证书用于标识服务器和客户端之间安全连接的网站所有者。

步骤

1. 选择菜单：设置[访问管理]。
2. 从*审核日志*选项卡中、选择*配置系统日志服务器*。

   此时将打开*配置系统日志服务器*对话框。

3. 单击 * 添加 * 。

   此时将打开*添加系统日志服务器*对话框。

4. 输入服务器的信息、然后单击*添加*。
   - 服务器地址—输入完全限定域名、IPv4地址或IPv6地址。
   - protocol—从下拉列表中选择一个协议(例如TLS、UDP或TCP)。
   - upload certificate (可选)—如果您选择了TLS协议但尚未上传签名的CA证书、请单击浏览上传证书文件。如果没有可信证书、则不会将审核日志归档到系统日志服务器。

     如果证书稍后变得无效、TLS握手将失败。因此、将向审核日志发布错误消息、并且不再向系统日志服务器发送消息。要解决此问题描述 、您必须修复系统日志服务器上的证书、然后转到菜单：设置(审核日志>配置系统日志服务器>测试全部)。

   - port -输入系统日志接收器的端口号。单击*添加*后、*配置系统日志服务器*对话框将打开、并在页面上显示已配置的系统日志服务器。
5. 要测试服务器与存储阵列的连接、请选择*全部测试*。

结果

配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。

编辑审核日志记录的系统日志服务器设置

您可以更改用于归档审核日志的系统日志服务器的设置、也可以为该服务器上传新的证书颁发机构(CA)证书。

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。
- 系统日志服务器地址、协议和端口号必须可用。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
- 如果要上传新的CA证书、则此证书必须在本地系统上可用。

步骤

1. 选择菜单：设置[访问管理]。
2. 从*审核日志*选项卡中、选择*配置系统日志服务器*。

   已配置的系统日志服务器将显示在页面上。

3. 要编辑服务器信息、请选择服务器名称右侧的*编辑*(铅笔)图标、然后在以下字段中进行所需的更改：
   - 服务器地址—输入完全限定域名、IPv4地址或IPv6地址。
   - protocol—从下拉列表中选择一个协议(例如TLS、UDP或TCP)。
   - port -输入系统日志接收器的端口号。
4. 如果将协议更改为安全TLS协议(从UDP或TCP)、请单击*导入可信证书*以上传CA证书。
5. 要测试与存储阵列的新连接、请选择*全部测试*。

结果

配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。

常见问题解答

为什么我无法登录?

如果在尝试登录到System Manager时收到错误、请查看这些可能的原因。

System Manager登录错误可能是由于以下原因之一：

- 您输入的用户名或密码不正确。
- 您的权限不足。
- 目录服务器(如果已配置)可能不可用。如果是这种情况、请尝试使用本地用户角色登录。
- 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。
- 已触发锁定条件、并且您的审核日志可能已满。转至访问管理并从审核日志中删除旧事件。
- 已启用SAML身份验证。刷新浏览器以登录。

由于以下原因之一、可能会在远程存储阵列上登录错误以执行镜像任务：

- 您输入的密码不正确。
- 您尝试多次登录失败、从而触发锁定模式。请等待10分钟以重新登录。
- 已达到控制器上使用的最大客户端连接数。检查是否存在多个用户或客户端。

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、请确保满足以下要求。

- 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、请查看以下准则。

存储阵列的嵌入式RBAC (基于角色的访问控制)功能包括以下角色：

- 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。

目录服务

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。
- 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System Manager将无法正常运行。

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。
- 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System Manager将无法正常运行。

哪些外部管理工具可能会受到此更改的影响?

在System Manager中进行某些更改时、例如切换管理界面或使用SAML进行身份验证方法、某些外部工具和功能可能会受到限制、无法使用。

管理接口

除非启用旧版管理接口设置、否则直接与旧版管理界面(符号)通信的工具(例如SANtricity SMI-S Provider或OnCommand Insight (OCI))无法正常工作。此外、如果禁用了此设置、则不能使用传统CLI命令或执行镜像操作。

有关详细信息，请联系技术支持。

SAML 身份验证

启用SAML后、以下客户端将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

有关详细信息，请联系技术支持。

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保持同步(通过NTP服务器或通过调整控制器时钟设置)。
- IdP元数据文件从IdP系统下载、并可从用于访问System Manager的本地系统上获得。
- 您知道存储阵列中每个控制器的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

审核日志中记录了哪些类型的事件?

审核日志可以记录修改事件、也可以同时记录修改和只读事件。

根据策略设置、将显示以下类型的事件:

- 修改事件- System Manager中涉及系统更改的用户操作、例如配置存储。
- 修改和只读事件-涉及系统更改的用户操作以及涉及查看或下载信息的事件、例如查看卷分配。

在配置系统日志服务器之前、我需要了解哪些信息？

您可以将审核日志归档到外部系统日志服务器。

在配置系统日志服务器之前、请记住以下准则。

- 确保您知道服务器地址、协议和端口号。服务器地址可以是完全限定域名、IPv4地址或IPv6地址。
- 如果您的服务器使用安全协议(例如TLS)、则本地系统上必须具有证书颁发机构(CA)证书。CA证书用于标识服务器和客户端之间安全连接的网站所有者。
- 配置后、所有新审核日志都会发送到系统日志服务器。不会传输先前的日志。
- "覆盖策略*"设置(可从"查看/编辑设置"访问)不会影响使用系统日志服务器配置管理日志的方式。
- 审核日志采用RFC 5424消息格式。

系统日志服务器不再接收审核日志。我该怎么办？

如果您为系统日志服务器配置了TLS协议、则如果证书因任何原因而无效、则服务器将无法接收消息。审核日志中会发布一条有关此无效证书的错误消息。

要解决此问题描述 、必须先修复系统日志服务器的证书。建立有效的证书链后、转到菜单：设置[审核日志>配置系统日志服务器>测试全部]。