证书和身份验证

SANtricity 11.6

NetApp
February 12, 2024

目录

证书和身份验证

证书管理

概念

证书的工作原理

证书是数字文件、用于标识网站和服务器等在线实体、以实现Internet上的安全通信。

签名证书

证书可确保Web通信仅在指定服务器和客户端之间以加密格式单独传输、不会被更改。使用Unified Manager、您可以管理主机管理系统上的浏览器证书以及发现的存储阵列中的控制器证书。

证书可以由可信的颁发机构签名、也可以是自签名证书。"签名"只是指有人验证了所有者的身份并确定其设备可以受信任。存储阵列会在每个控制器上随附一个自动生成的自签名证书。您可以继续使用自签名证书、也可以获取CA签名证书、以便在控制器和主机系统之间建立更安全的连接。

> 虽然CA签名证书可提供更好的安全保护(例如、防止中间人攻击)、但如果您的网络较大、则还需要支付昂贵的费用。相比之下、自签名证书的安全性较低、但它们是免费的。因此、自签名证书最常用于内部测试环境、而不是生产环境。

签名证书由可信的第三方组织证书颁发机构(CA)进行验证。签名证书包括有关实体(通常是服务器或网站)所有者的详细信息、证书问题描述 和到期日期、实体的有效域以及由字母和数字组成的数字签名。

当您打开浏览器并输入Web地址时、系统会在后台执行证书检查过程、以确定您是否要连接到包含有效的CA签名证书的网站。通常、使用签名证书进行安全保护的站点会在地址中包含挂锁图标和https标志。如果您尝试连接到不包含CA签名证书的网站、浏览器将显示一条警告、指出此站点不安全。

CA会在应用程序过程中执行一些步骤来验证您的身份。他们可能会向您的注册业务发送电子邮件、验证您的业务地址以及执行HTTP或DNS验证。应用程序过程完成后、CA会向您发送数字文件、以便在主机管理系统上加载。通常、这些文件包括以下信任链：

- 根-层次结构顶部是根证书、其中包含用于对其他证书进行签名的专用密钥。根标识特定的CA组织。如果对所有网络设备使用相同的CA、则只需要一个根证书。
- 中间证书—从根分层是中间证书。CA颁发一个或多个中间证书、充当受保护根证书和服务器证书之间的中间人。
- 服务器—链的底部是服务器证书、用于标识您的特定实体、例如网站或其他设备。存储阵列中的每个控制器都需要一个单独的服务器证书。

自签名证书

存储阵列中的每个控制器都包含一个预安装的自签名证书。自签名证书与CA签名证书类似、只是它由实体所有者而非第三方进行验证。与CA签名证书一样、自签名证书也包含自己的专用密钥、并确保数据经过加密并通过HTTPS连接在服务器和客户端之间发送。

自签名证书不受浏览器"`信任`"。每次尝试连接到仅包含自签名证书的网站时、浏览器都会显示一条警告消息。您必须单击警告消息中允许您继续访问网站的链接；这样、您实际上就是在接受自签名证书。

Unified Manager的证书

Unified Manager界面随Web服务代理一起安装在主机系统上。打开浏览器并尝试连接到Unified Manager时、浏览器会尝试通过检查数字证书来验证主机是否为可信源。如果浏览器找不到服务器的CA签名证书、则会打开一条警告消息。从该站点、您可以继续访问该网站以接受该会话的自签名证书。或者、您也可以从CA获取签名的数字证书、以便不再显示警告消息。

控制器的证书

在Unified Manager会话期间、当您尝试访问没有CA签名证书的控制器时、可能会看到其他安全消息。在这种情况下、您可以永久信任自签名证书、也可以为控制器导入CA签名证书、以便Web服务代理服务器可以对来自这些控制器的传入客户端请求进行身份验证。

证书术语

以下术语适用于证书管理。

期限	**Description**
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。
CSR	证书签名请求(CSR)是从申请人发送给证书颁发机构(CA)的一条消息。CSR会验证CA对证书进行问题描述 所需的信息。
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。
证书链	一种文件层次结构、用于向证书添加一层安全保护。通常、此链包含一个位于层次结构顶部的根证书、一个或多个中间证书以及用于标识实体的服务器证书。
中间证书	一个或多个中间证书从证书链中的根分支。CA颁发一个或多个中间证书、充当受保护根证书和服务器证书之间的中间人。
密钥库	密钥库是主机管理系统上的存储库、其中包含私钥及其对应的公有 密钥和证书。这些密钥和证书用于标识您自己的实体、例如控制器。
根证书	根证书位于证书链中的层次结构顶部、其中包含用于对其他证书签名的专用密钥。根标识特定的CA组织。如果对所有网络设备使用相同的CA、则只需要一个根证书。
签名证书	由证书颁发机构(CA)验证的证书。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。此外、签名证书还包括实体所有者的详细信息(通常为服务器或网站)以及由字母和数字组成的数字签名。签名证书使用信任链、因此最常用于生产环境。也称为"CA签名证书"或"管理证书"。

期限	Description
自签名证书	自签名证书由实体的所有者进行验证。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。它还包括由字母和数字组成的数字签名。自签名证书与CA签名证书使用的信任链不同、因此最常用于测试环境。也称为"预安装"证书。
服务器证书	服务器证书位于证书链的底部。它标识您的特定实体、例如网站或其他设备。存储系统中的每个控制器都需要一个单独的服务器证书。
信任存储库	信任存储库是一个存储库、其中包含来自CA等可信第三方的证书。
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界面与Web服务代理捆绑在一起。

操作说明

使用**CA**签名的证书

您可以获取并导入CA签名的证书、以安全访问托管Unified Manager的管理系统。

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、不会显示证书功能。

关于此任务

使用CA签名证书是一个两步操作步骤。

第**1**步：完成并提交**CSR**

您必须先生成证书签名请求(CSR)文件并将其发送到CA。

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、不会显示证书功能。

关于此任务

此任务介绍如何生成发送给CA的CSR文件、以接收托管Unified Manager和Web服务代理的系统的已签名管理证书。您必须提供有关您的组织的信息以及主机系统的IP地址或DNS名称。

> 提交给CA后、请勿生成新的CSR。生成CSR时、系统会创建一个专用密钥对和公有 密钥对。公有 密钥是CSR的一部分、而私钥则保留在密钥库中。当您收到签名证书并将其导入到密钥库中时、系统会确保私钥和公有 密钥都是原始对。因此、在向CA提交新的CSR后、您不能生成新的CSR。否则、控制器将生成新密钥、而从CA收到的证书将不起作用。

步骤

1. 选择*证书管理*。
2. 从*管理*选项卡中、选择*完成CSR*。

3. 输入以下信息、然后单击*下一步*：
    - 组织—贵公司或组织的法定全名。包括后缀、例如Inc.或Corp.
    - 组织单位(可选)—组织中负责处理证书的部门。
    - 城市/位置-主机系统或业务所在的城市。
    - 省/自治区/直辖市(可选)—主机系统或业务所在的省/自治区/直辖市。
    - 国家/地区ISO代码—您所在国家/地区的两位数ISO (国际标准化组织)代码、例如美国。
4. 输入有关主机系统的以下信息：
    - 公用名—安装了Web服务代理的主机系统的IP地址或DNS名称。请确保此地址正确无误；它必须与您在浏览器中输入的地址完全匹配才能访问Unified Manager。请勿包含http：//或https：//。
    - 备用IP地址-如果公用名称为IP地址、则可以选择为主机系统输入任何其他IP地址或别名。对于多个条目、请使用逗号分隔格式。
    - 备用DNS名称-如果公用名称为DNS名称、请输入主机系统的任何其他DNS名称。对于多个条目、请使用逗号分隔格式。如果没有备用DNS名称、但您在第一个字段中输入了DNS名称、请将此名称复制到此处。
5. 单击 * 完成 * 。

    此时、CSR文件将下载到本地系统。下载内容的文件夹位置取决于您的浏览器。

6. 将CSR文件提交到CA并请求PEM或DER格式的签名证书。

完成后

等待CA返回证书文件、然后转到 "第2步：导入管理证书"。

第2步：导入管理证书

收到签名证书后、导入安装了Unified Manager界面的主机系统的证书链。

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、不会显示证书功能。
- 您已生成证书签名请求(.csr文件)并将其发送到CA。
- CA返回了可信证书文件。
- 证书文件安装在本地系统上。
- 如果CA提供了链式证书(例如.p7b文件)、则必须将链式文件解压缩到各个文件中：根证书、一个或多个中间证书以及服务器证书。您可以使用Windows `certmgr`实用程序解压缩文件(右键单击并选择*菜单：所有任务[导出]*)。导出完成后、系统将为链中的每个证书文件显示一个CER"文件。

步骤

1. 选择*证书管理*。
2. 从*管理*选项卡中、选择*导入*。

    此时将打开一个对话框、用于导入证书文件。

3. 单击*浏览*以首先选择根文件和中间文件、然后选择服务器证书。

文件名将显示在对话框中。

4. 单击 * 导入 * 。

结果

这些文件将上传并进行验证。证书信息将显示在证书管理页面上。

重置管理证书

您可以将管理证书还原到原始出厂自签名状态。

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、不会显示证书功能。

关于此任务

此任务将从安装了Web服务代理和SANtricity 统一管理器的主机系统中删除当前管理证书。重置证书后、主机系统将恢复为使用自签名证书。

步骤

1. 选择*证书管理*。
2. 从*管理*选项卡中、选择*重置*。

   此时将打开一个*确认重置管理证书*对话框。

3. 在字段中键入`reset`、然后单击*重置*。

   浏览器刷新后、浏览器可能会阻止对目标站点的访问并报告此站点正在使用HTTP严格传输安全性。切换回自签名证书时会出现此情况。要清除阻止访问目标的条件、您必须从浏览器中清除浏览数据。

结果

系统将恢复为使用服务器中的自签名证书。因此、系统会提示用户为其会话手动接受自签名证书。

导入阵列的证书

如有必要、您可以导入存储阵列的证书、以便这些证书可以在托管SANtricity Unified Manager的系统中进行身份验证。证书可以由证书颁发机构(CA)签名、也可以是自签名证书。

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、不会显示证书功能。
- 如果要导入可信证书、则必须使用SANtricity 系统管理器为存储阵列控制器导入这些证书。

步骤

1. 选择*证书管理*。
2. 选择*可信*选项卡。

   此页面显示为存储阵列报告的所有证书。

3. 选择*菜单：导入[证书]*以导入CA证书、或者选择*菜单：导入[自签名存储阵列证书]*以导入自签名证书。

   要限制此视图、您可以使用*显示证书…*筛选字段、也可以单击列标题之一对证书行进行排序。

4. 在对话框中、选择证书、然后单击*导入*。

   已上传并验证此证书。

查看证书

您可以查看证书的摘要信息、其中包括使用证书的组织、颁发证书的机构、有效期以及指纹(唯一标识符)。

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、不会显示证书功能。

步骤

1. 选择*证书管理*。
2. 选择以下选项卡之一：
   - 管理-显示托管Web服务代理的系统的证书。管理证书可以是自签名证书、也可以由证书颁发机构(CA)批准。它允许安全访问Unified Manager。
   - 可信-显示Unified Manager可访问的存储阵列和其他远程服务器(例如LDAP服务器)的证书。证书可以从证书颁发机构(CA)颁发、也可以是自签名证书。
3. 要查看有关证书的详细信息、请选择其行、选择行末尾的省略号、然后单击*查看*或*导出*。

导出证书

您可以导出证书以查看其完整详细信息。

开始之前

要打开导出的文件、您必须具有证书查看器应用程序。

步骤

1. 选择*证书管理*。
2. 选择以下选项卡之一：
   - 管理-显示托管Web服务代理的系统的证书。管理证书可以是自签名证书、也可以由证书颁发机构(CA)批准。它允许安全访问Unified Manager。
   - 可信-显示Unified Manager可访问的存储阵列和其他远程服务器(例如LDAP服务器)的证书。证书可以从证书颁发机构(CA)颁发、也可以是自签名证书。
3. 从页面中选择一个证书、然后单击行末尾的省略号。
4. 单击*导出*、然后保存证书文件。
5. 在证书查看器应用程序中打开文件。

删除可信证书

您可以删除一个或多个不再需要的证书、例如已过期的证书。

开始之前

请先导入新证书、然后再删除旧证书。

> 请注意、删除根证书或中间证书可能会影响多个存储阵列、因为这些阵列可以共享相同的证书文件。

步骤

1. 选择*证书管理*。
2. 选择*可信*选项卡。
3. 在表中选择一个或多个证书、然后单击*删除*。

   > 对于预安装的证书、*删除*功能不可用。

   此时将打开确认删除可信证书对话框。

4. 确认删除、然后单击*删除*。

   此证书将从表中删除。

解析不可信的证书

如果存储阵列尝试建立与SANtricity Unified Manager的安全连接、但此连接无法确认为安全连接、则会发生不可信证书。在证书页面中、您可以通过从存储阵列导入自签名证书或导入可信第三方颁发的证书颁发机构(CA)证书来解析不可信的证书。

开始之前

- 您必须使用具有安全管理员权限的用户配置文件登录。
- 如果您计划导入CA签名的证书：
  - 您已为存储阵列中的每个控制器生成证书签名请求(.csr文件)、并将其发送给CA。
  - CA返回了可信证书文件。
  - 证书文件可在本地系统上使用。

关于此任务

如果满足以下任一条件、您可能需要安装其他受信任的CA证书：

- 您最近添加了一个存储阵列。
- 一个或两个证书均已过期。
- 一个或两个证书均已撤销。
- 一个或两个证书缺少根证书或中间证书。

步骤

1. 选择*证书管理*。
2. 选择*可信*选项卡。

   此页面显示为存储阵列报告的所有证书。

3. 选择*菜单：导入[证书]*。导入CA证书或*菜单：导入[自签名存储阵列证书]*以导入自签名证书。

   要限制此视图、您可以使用*显示证书…*筛选字段、也可以单击列标题之一对证书行进行排序。

4. 在对话框中、选择证书、然后单击*导入*。

   已上传并验证此证书。

访问管理

概念

访问管理的工作原理

使用访问管理在SANtricity 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。

   > 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。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适用于SANtricity 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。
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SANtricity 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SANtricity 统一管理器中强制实施的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. *可选：*管理员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SANtricity 统一管理器。

   `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。

操作说明

查看本地用户角色

在本地用户角色选项卡中、您可以查看用户与默认角色的映射。这些映射是在适用于SANtricity Unified Manager的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 * 。

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SANtricity 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
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`。
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。

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。

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

正在设置 ...	Description
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`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。

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. 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。

常见问题解答

为什么我无法登录?

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

Unified 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。

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、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。