



使用目录服务 SANtricity 11.8

NetApp
December 16, 2024

目录

使用目录服务	1
添加目录服务器	1
编辑目录服务器设置和角色映射	4
删除目录服务器	6

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。

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

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。

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	<p>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：</p> <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。

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。