

UCS的中央印制厂LDAP认证配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[收集信息](#)

[捆绑用户详细信息](#)

[基本DN详细信息](#)

[供应商详细信息](#)

[过滤器属性](#)

[添加并且配置属性](#)

[添加CiscoAVPair属性](#)

[更新CiscoAVPair属性](#)

[更新预定义的属性](#)

[配置在UCS中央印制厂的LDAP认证](#)

[配置LDAP供应商](#)

[配置LDAP供应商组](#)

[更改本地验证规则](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文为思科统一计算系统的(UCS)中央印制厂轻量级目录访问协议(LDAP)验证提供一配置示例。步骤使用UCS中央图形用户界面(GUI)、bglucs.com一个示例域和testuser一示例用户名。

在UCS中央软件的版本1.0，LDAP是支持的唯一的远程验证协议。版本1.0有非常远程验证和IDAP配置的UCS中央的有限支持。然而，您能使用UCS中央印制厂为了配置UCS管理的UCS管理器域的所有选项中央印制厂。

UCS中央远程验证的限制包括：

- 不支持RADIUS和TACACS。
- LDAP多个域控制器的分配和LDAP供应商组不支持角色的组成员映射。
- LDAP使用CiscoAVPair属性或仅所有未使用属性为了通过角色。通过的角色是其中一在UCS中央印制厂本地数据库的预定义的作用。
- 不支持多次认证域/协议。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- UCS中央印制厂部署。
- Microsoft Active Directory部署。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- UCS中央版本1.0
- Microsoft Active Directory

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

收集信息

此部分汇总您需要收集的信息，在您开始配置前。

注意： 使用 [命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

绑定用户详细信息

捆绑用户可以是访问读访问域的域的所有LDAP用户;捆绑用户为IDAP配置要求。UCS中央印制厂使用捆绑用户的用户名和密码为了连接和查询激活目录(AD)用户认证等等。此示例使用管理员帐户作为捆绑用户。

此步骤描述LDAP管理员如何能使用激活目录服务接口(ADSI)编辑器为了查找DN。

1. 打开ADSI编辑器。
2. 寻找捆绑用户。用户在路径和一样AD的。
3. 用鼠标右键单击用户，并且选择**属性**。
4. 在Properties对话框中，请双击**distinguishedName**。
5. 复制从Value字段的DN。
6. 点击**取消**为了关上所有windows。

要得到捆绑用户的密码，与AD管理员联系。

根据DN详细信息

基础DN是搜索关于用户和用户详细信息开始组织单位(OU)或容器的DN。您在AD能使用创建的

OU的DN UCS或UCS中央印制厂。然而，您可以发现它更加简单使用DN域根。

此步骤描述LDAP管理员如何能使用ADSI编辑器为了查找基础DN。

1. 打开ADSI编辑器。
2. 查找作为基础DN或容器将使用的OU。
3. 用鼠标右键单击OU或容器，并且选择**属性**。
4. 在Properties对话框中，请双击**distinguishedName**。
5. 复制从Value字段的DN，并且注释您需要的所有其他详细信息。
6. 点击**取消**为了关上所有windows。

[供应商详细信息](#)

供应商播放在LDAP认证的一在UCS中央印制厂的关键角色和授权。供应商是UCS中央查询为了搜索和验证用户和为了获得用户详细信息例如角色信息的其中一个AD服务器。请务必采集供应商AD服务器的主机名或IP地址。

[过滤属性](#)

过滤器领域或属性用于为了搜索AD数据库。用户ID被输入在登录通过回到AD并且对过滤器比较。

您能使用sAMAccountName=\$userid，过滤器值。sAMAccountName是在AD的一个属性并且有同一个值作为AD用户ID，用于为了登陆到UCS中央印制厂GUI。

[添加并且配置属性](#)

此部分汇总您需要为了添加CiscoAVPair属性的信息(如果必须)和更新CiscoAVPair属性或其他，预定义的属性，在您开始LDAP配置前。

属性字段指定AD属性(在用户属性下)，通行证返回将分配的角色到用户。在UCS中央软件的版本1.0a中，自定义属性CiscoAVPair或在AD的其他未使用属性可以统一化为了通过此角色。

注意： 使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

[添加CiscoAVPair属性](#)

为了添加新团体到域，展开域的模式和添加属性到，在本例中，是用户)的类(。

此步骤描述如何展开在Windows AD服务器的模式和添加CiscoAVPair属性。

1. AD服务器的洛金。
2. 点击**Start > Run**，键入**mmc**，并且按回车为了打开一个空微软管理控制台(MMC)控制台。
3. 在MMC中，请点击**File>添加/删除管理单元>Add**。
4. 在添加独立卡扣式对话框中，请选择**激活目录方案**，并且单击**添加**。
5. 在MMC中，请展开**激活目录方案**，用鼠标右键单击**属性**，并且选择**创建属性**。创建新团体对话框出现
6. 创建在远程验证服务中命名的CiscoAVPair属性。在公用名称和LDAP显示Name字段，请输入**CiscoAVPair**。在唯一500对象ID字段，输入**1.3.6.1.4.1.9.287247.1**。在说明字段、回车**UCS角色和现场**。在语法字段，请选择从下拉列表的**Unicode字符串**。点击OK键为了保存属性

和关闭对话框。一旦属性被添加到模式，在用户分类必须映射或包括。这允许您编辑用户属性和指定值将通过的角色。

7. 在用于AD模式扩展的同样MMC中，请展开类，用鼠标右键单击用户，并且选择属性。
8. 在用户属性对话框中，请点击Attributes选项，并且单击添加。
9. 在挑选模式对象对话框中，请点击CiscoAVPair，并且单击OK键。
10. 在用户属性对话框中，请单击应用。
11. 用鼠标右键单击激活目录方案，并且选择重新加载模式为了包括新的更改。
12. 如果需要，请使用ADSI编辑器更新模式。用鼠标右键单击Localhost，并且当前选择更新模式。

更新CiscoAVPair属性

此步骤描述如何更新CiscoAVPair属性。语法是shell roles= " <role>"。

1. 在ADSI Edit对话框中，请找出需要对UCS中央的访问的用户。
2. 用鼠标右键单击用户，并且选择属性。
3. 在Properties对话框中，请点击属性编辑器选项卡，点击CiscoAVPair，并且单击编辑。
4. 在多值的字符串编辑器对话框中，请输入值shell : roles= " admin"在值字段和单击OK键。
5. 单击OK键为了保存更改和关闭Properties对话框。

更新预定义的属性

此步骤描述如何更新一个预定义的属性，角色是其中一个在UCS中央印制厂的预定义的用户角色。此示例使用属性公司为了通过角色。语法是shell roles= " <role>"。

1. 在ADSI Edit对话框中，请找出需要对UCS中央的访问的用户。
2. 用鼠标右键单击用户，并且选择属性。
3. 在Properties对话框中，请点击属性编辑器选项卡，点击公司，并且单击编辑。
4. 在字符串属性编辑器对话框中，请输入值shell : roles= " admin"在Value字段，和单击OK键。
5. 单击OK键为了保存更改和关闭Properties对话框。

配置在UCS中央印制厂的LDAP认证

在UCS中央印制厂的IDAP配置完成在操作管理下。

1. UCS的中央印制厂洛金在本地帐户下。
2. 点击操作管理，展开域组，并且点击可操作的策略> Security。
3. 为了配置LDAP认证，请采取这些步骤：[配置LDAP供应商](#)。[配置LDAP供应商组](#)(不可用在版本1.0a)。[更改本地验证规则](#)。

配置LDAP供应商

1. 点击LDAP，用鼠标右键单击供应商，并且选择创建LDAP供应商。
2. 在创建LDAP供应商对话框中，请添加这些详细信息，被采集前。供应商的主机名或IP捆绑DN基准 DN过滤器属性(CiscoAVPair或一个预定义的属性例如公司密码(用于捆绑DN的用户的密码))
3. 单击OK键为了保存配置和关闭对话框。

注意： 其他值在此屏幕不需要被修改。LDAP组规则不为在此版本的UCS中央验证支持。

[配置LDAP供应商组](#)

注意： 在版本1.0a中，不支持供应商组。此步骤描述如何配置一假的供应商组在后的配置里使用。

1. 点击**LDAP**，用鼠标右键单击**供应商组**，并且选择**创建LDAP供应商组**。
2. 在创建LDAP供应商组对话框中，请在Name字段输入名称对于组。
3. 从可用的供应商列表在左边的，比符号请选择供应商，并且点击极大(>)为了移动该供应商向在右边的已分配供应商。
4. 点击OK键为了保存更改和结束屏幕。

[更改本地验证规则](#)

版本1.0a不支持多次认证域正如在UCS管理器。为了在此附近工作，您需要修改本地验证规则。

本地验证有选项修改默认登录或控制台登录的验证。因为不支持多个域，您能使用本地帐户或LDAP帐户，但是不是两个。更改值领域为了使用本地或LDAP作为验证来源。

1. 点击**验证**，用鼠标右键单击**本地验证**，并且选择**属性**。
2. 确定是否想要默认验证，控制台验证或者两个。请使用默认验证GUI和命令行界面(CLI)。请使用控制台验证虚拟机基于内核的虚拟机(KVM)视图。
3. 从领域下拉列表选择**ldap**。值领域确定本地或LDAP是否是验证来源。
4. 点击OK键为了关闭页。
5. 在Policies页，如果必须请单击**“Save”**为了保存更改。

注意： 不您的当前会话注销或修改控制台验证，直到您验证LDAP认证正确地运作。控制台验证提供一方式复原给先前配置。参考[Verify部分](#)。

[验证](#)

此步骤描述如何测试LDAP认证。

1. 打开在UCS中央印制厂的一个新会话，并且输入用户名和密码。您不需要在用户名前包括域或字符。此示例使用testucs作为从域的用户。
2. 如果看到UCS中央印制厂控制板，LDAP认证是成功的。用户显示在页底端。

[故障排除](#)

目前没有针对此配置的故障排除信息。

[相关信息](#)

- [技术支持和文档 - Cisco Systems](#)