ACS 5.x ：LDAP服务器配置示例

目录

简介

轻量级目录访问协议(LDAP)是在TCP/IP和UDP运行查询的一个网络协议和正在修改的目录服务。LDAP是访问的一个基于x.500的目录服务器一轻量级机制。RFC 2251 定义了LDAP。

思科安全访问控制系统(ACS) 5.x集成LDAP外部数据库(也呼叫标识存储)通过使用LDAP协议。有两个使用的方法连接到LDAP服务器：纯文本(简单)和SSL (已加密)连接。使用这两个方法， ACS 5.x可以配置连接到LDAP服务器。使用一简单连接，本文为连接ACS提供配置示例5.x给LDAP服务器。

先决条件

要求

本文假设， ACS 5.x有一个IP连接到LDAP服务器，并且端口TCP 389是开放的。

默认情况下， Microsoft Active Directory LDAP服务器配置接受在端口TCP 389的LDAP连接。如果使用其他LDAP服务器，请确保是正在运行和接受在端口TCP 389的连接。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Secure ACS 5.x

- Microsoft Active Directory LDAP服务器

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。

背景信息

目录服务

目录服务是用于的软件应用或套应用程序存储和组织关于计算机网络的用户和网络资源的信息。您能使用目录服务为了管理对这些资源的用户访问。

LDAP目录服务根据客户服务器模型。客户端连接到LDAP服务器为了启动LDAP会话，并且发送操作请求到服务器。服务器然后发送其答复。一个或更多LDAP服务器包含从LDAP目录树或LDAP支持者数据库的数据。

目录服务管理目录，是数据库保持信息。目录服务使用一个分布式型号为了存储信息，并且该信息通常复制在目录服务器之间。

LDAP目录在一个简单树型层次结构被组织，并且可以在许多服务器中被分配。每个服务器能有周期地同步总目录的一个复制的版本。

在树的一个条目包含一套属性，每个属性有一名称(attribute type或属性说明)和一个或更多值。属性在模式定义。

每个条目有呼叫其特有名(DN)的一个唯一标识符。此名称包含从在条目的属性(RDN)修建的相对辨别名称，跟随由parent条目的DN。您能设想DN作为一个全双工文件名和RDN作为在文件夹的一个相对文件名。

验证使用LDAP

ACS 5.x能利用LDAP标识存储验证负责人由执行在目录服务器的捆绑操作为了查找和验证负责人。如果验证成功， ACS能获取属于负责人的组和属性。获取的属性在ACS Web接口(LDAP页)可以配置。这些组和属性可以由ACS用于为了授权负责人。

为了验证用户或查询LDAP标识存储， ACS连接到LDAP服务器并且保养连接池。请参阅LDAP连接管理。

LDAP连接管理

ACS 5.x支持多个并发LDAP连接。连接在第一LDAP认证时打开根据要求。最大连接数为每个LDAP服务器配置。打开连接事先缩短验证时间。

您能设置最大连接数使用并发约束连接。打开的连接数量可以是不同的为每个LDAP服务器(主要的或附属)和根据管理连接的最大为每个服务器配置的确定。

ACS保留开放LDAP连接列表(包括捆绑信息)在ACS配置的每个LDAP服务器的。在认证过程中，连

接管理器尝试查找从池的一开放连接。

如果开放连接不存在，打开新的。如果LDAP服务器关闭连接，连接管理器报告错误在第一个呼叫期间搜索目录和尝试更新连接。

在认证过程完成后，连接管理器发布对连接管理器的连接。欲知更多信息，参考ACS 5.X用户指南。

配置

本部分提供有关如何配置本文档所述功能的信息。

配置LDAP的ACS 5.x

完成这些步骤为了配置LDAP的ACS 5.x ：

1. 选择**用户，并且标识存储>外部标识存储> LDAP**，并且单击**创建**为了创建一个新的LDAP连接。
2. 在常规选项卡，为新的LDAP请提供**名称**和**说明**(可选)，并且**其次**单击。
3. 在主服务器部分下的服务器连接选项卡，请提供**主机名、波尔特**， **Admin DN**和**密码**。单击**测验捆绑到服务器**。**注意：** LDAP的IANA分配的端口号是TCP 389。然而，请确认端口号您的LDAP服务器从您的LDAP Admin使用。应该提供Admin DN和密码给您由您的LDAP Admin。您的Admin DN在LDAP服务器的所有OU应该读了所有权限。
4. 此镜像显示**对服务器的连接测验捆绑**是成功的。**注意：** 如果测验捆绑不是成功的，请再验证**主机名、端口号**， **Admin DN**和**密码**从您的LDAP管理员。
5. 单击 **Next**。
6. 提供在目录组织选项卡的需要的细节在模式段下。同样地，请提供必填信息在目录结构部分下如所提供由您的LDAP Admin。点击**测验配置**。
7. 此镜像显示**配置测验**是成功的。**注意：** 如果配置测验不是成功的，请再验证在**模式**和**目录结构**提供的参数从您的LDAP管理员。
8. 单击 **完成**。
9. **LDAP服务器**顺利地创建。

配置标识存储

竞争步骤为了配置标识存储：

1. 选择**访问策略**>Access **Services**>服务使用LDAP服务器验证的**服务选择规则**，并且验证。在本例中， LDAP服务器验证使用**默认网络网络访问**服务。
2. 一旦验证在Step1的服务，请去特定服务并且点击**允许协议**。确保请**允许PAP/ASCII**选择，并且单击**提交**。**注意：** 您能有其他身份验证协议选择与一起允许PAP/ASCII。
3. 点击在Step1识别的服务，并且点击**标识**。在标识Source字段右边单击**精选**。
4. 选择新建立的LDAP服务器(**myLDAP**，在本例中)，并且点击OK键。
5. 点击**Save Changes**。
6. 去在Step1识别的服务的授权部分，并且确保有允许**验证**至少的一个规则。

故障排除

ACS发送捆绑请求利用LDAP服务器验证用户。捆绑请求包含用户的DN和用户密码在明文。用户验证，当用户的DN和密码匹配在LDAP目录的用户名和密码。

- **验证错误**- ACS记录在ACS日志文件的验证错误。
- **初始化错误**-请使用LDAP服务器超时设置为了配置ACS在确定那前等待从LDAP服务器的一答复连接或在该服务器的验证失败秒钟的数量。LDAP服务器的可能的来源能返回初始化错误是：不支持LDAP服务器发生故障服务器是在内存外面用户没有权限不正确管理员凭证配置
- **捆绑错误**- LDAP服务器的可能的来源能返回捆绑(验证)错误是：过滤错误一搜索使用过滤器标准发生故障参数错误无效参数被输入了用户帐户限制(禁用，锁定，超时，密码超时，等等)

这些错误被记录作为外部资源错误，指示一个可能的问题用LDAP服务器：

- 发生的连接错误
- 超时的超时
- 服务器发生故障
- 服务器是在内存外面

A错误不被记录作为未知用户错误。

错误被记录作为一个无效密码错误，用户存在，但是被发送的密码无效。

相关信息

- 思科安全访问控制系统
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems