



如何配置统一通信在多森林环境的管理器目录集成

目录

- 简介
- 先决条件
- 要求
- 使用的组件
- 规则
- 背景信息
- Unified CM 中的 Active Directory 多森林支持方案
- 域信任关系
- 安装 AD LDS
- 安装多森林支持实例
- 将来自每个域的架构复制到 ADAM
- 通过 User-Proxy 对象扩展 AD LDS 架构
- 将来自 AD DC 的用户导入 AD LDS
- 在 AD LDS 中为 Unified CM 同步和验证创建用户
- 配置绑定重定向
- 配置 Unified CM
- 在 Unified CM 中创建自定义 LDAP 过滤器
- 相关信息

简介

本文档讨论了如何在多森林环境中配置 Unified Communication Manager 目录集成。

先决条件

要求

请确保您满足以下要求：

- 具备部署和配置 Cisco Unified Communications Manager 目录集成的知识。
- 负责部署、配置和维护 Microsoft Active Directory Application Mode 2003 或 Microsoft Active Directory Lightweight Directory Services 2008。
- 每台 Unified CM 发布服务器需要同步的用户帐户数不得超过 60,000 个。如果需要同步的帐户数超过 60,000 个，必须使用 IP 电话服务 SDK 提供自定义目录。有关其他详细信息，请参阅 Cisco 开发人员网络。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Unified Communications Manager 版本 8.0(1) 或更高版本
- Microsoft Active Directory Application Mode 2003 或 Lightweight Directory Services 2008

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

Microsoft Active Directory Lightweight Directory Service (AD LDS) 以前称为 Active Directory Application Mode (ADAM)，可用于为支持目录的应用程序提供目录服务。不再需要使用组织的 Active Directory 域服务 (AD DS) 数据库储存支持目录的应用程序数据，可使用 AD LDS 储存数据。AD LDS 可与 AD DS 一起使用，因此，您可以使用中央位置储存安全帐户 (AD DS)，

并使用另一个位置支持应用程序配置和目录数据 (AD LDS)。使用 AD LDS 可以减少与 Active Directory (AD) 复制相关的开销。您不必为支持应用程序而扩展 AD 架构，并且可以对目录结构执行分区操作，从而仅对支持目录的应用程序所需的支持服务器部署 AD LDS 服务。

有关详细信息，请参阅如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的背景信息部分。

Unified CM 中的 Active Directory 多森林支持方案

如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的 Unified CM 中的 Active Directory 多森林支持方案部分对此方案进行了说明。

域信任关系

为成功验证用户，您需要在托管 ADAM 示例的域和托管用户帐户的其他域之间建立信任。根据需要，此信任可以是单向信任（从托管 ADAM 实例的域到托管用户帐户的域传出的信任）。因此，ADAM 实例可在这些帐户域中向 DC 转发验证请求。

有关详细信息，请参阅如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的域信任关系部分。

安装 AD LDS

如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的安装 AD LDS 部分对安装 AD LDS 的步骤进行了说明。

安装多森林支持实例

AD LDS 可在不同的端口运行不同的服务实例，因此，可在同一台计算机上运行不同用户目录的“应用程序”。默认情况下，AD LDS 将选择端口 389/LDAP 和 636/LDAP。但是，如果系统中已有任何类型的 LDAP 服务正在运行，则它会使用端口 50000/LDAP 和 50001/LDAPS。每个实例都有一对基于上一次使用数字而增加的端口。

有关详细信息，请参阅如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的安装多森林支持实例部分。

将来自每个域的架构复制到 ADAM

必须对需要同步的每个域重复执行此过程。

执行如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的将来自每个域的架构复制到 ADAM 部分中的步骤。

通过 User-Proxy 对象扩展 AD LDS 架构

需要创建代理验证的对象，不使用“user”对象类。创建的 userProxy 对象类允许绑定重定向。需要在 ldif 文件中创建对象类详细信息。有关详细信息，请参阅如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的通过 User-Proxy 对象扩展 AD LDS 架构部分。

将来自 AD DC 的用户导入 AD LDS

执行如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的将来自 AD DC 的用户导入 AD LDS 部分中的步骤。

在 AD LDS 中为 Unified CM 同步和验证创建用户

执行如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的在 AD LDS 中为 Unified CM 同步和验证创建用户部分中的步骤。

配置绑定重定向

默认情况下，通过绑定重定向绑定到 ADAM 需要一个 SSL 连接。SSL 要求在运行 ADAM 的计算机和作为客户端连接到 ADAM 的计算机上安装并使用证书。如果您的 ADAM 测试环境中没有安装证书，您也可以禁用对 SSL 的要求。

有关详细信息，请参阅如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的配置绑定重定向部分。

配置 Unified CM

Unified CM 版本 8.0(1) 和更高版本支持 ADAM/AD LDS 同步和验证。

执行如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的配置 Unified CM 部分中的步骤。

在 Unified CM 中创建自定义 LDAP 过滤器

执行如何在多森林环境中配置 Unified Communication Manager 目录集成文档中的在 Unified CM 中创建自定义 LDAP 过滤器部分中的步骤。

相关信息

- 如何在多森林环境中配置 Unified Communication Manager 目录集成
- 配置示例和技术说明

版权所有 ©1992-2015 思科系统

文件创建日期: 2015 年 7 月 16 日

http://www.cisco.com/cisco/web/support/CN/110/1108/1108036_ucm-multi-forest-00.html
