从Active Directory配置用户、组和计算机以与OpenDNS连接器服务同步

目录

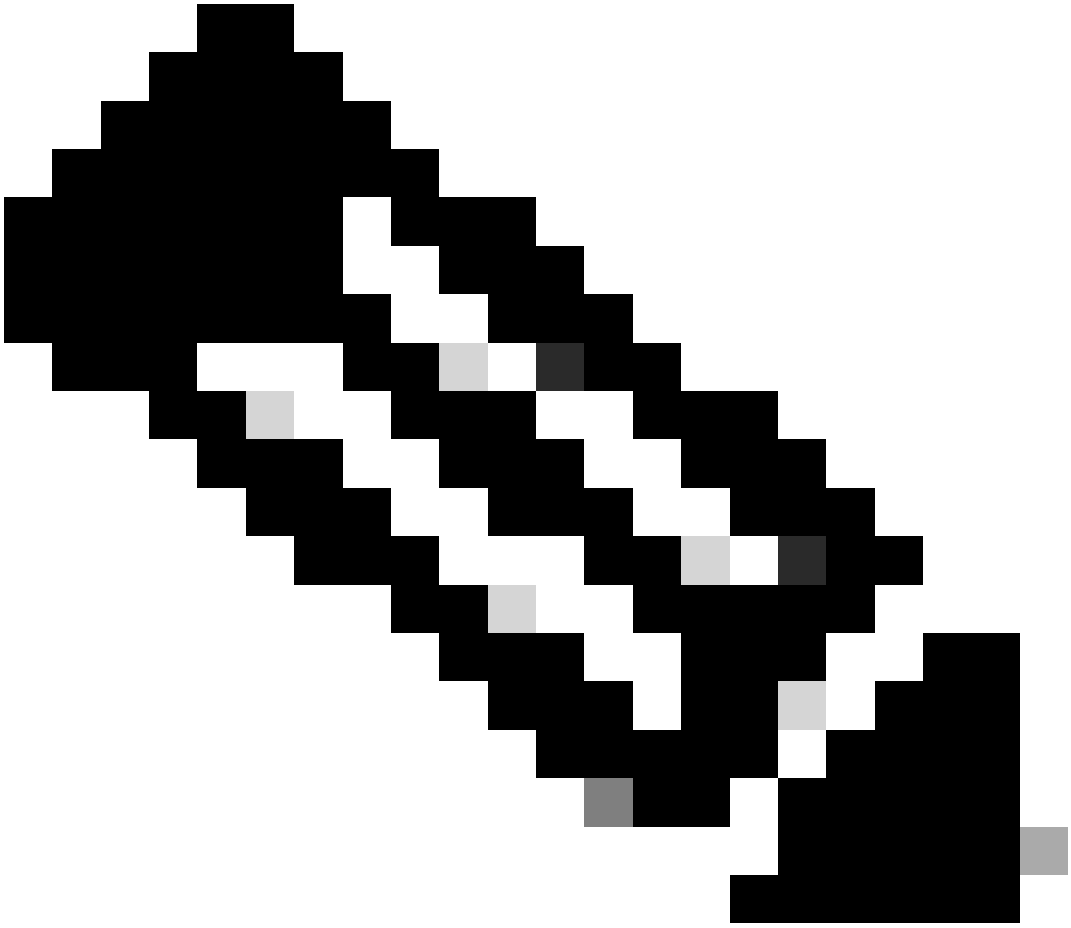
简介

本文档介绍如何使用OpenDNS连接器服务从Active Directory同步用户、组和计算机。

概述

作为操作的一部分，OpenDNS连接器服务使用LDAP协议从Active Directory同步用户、组和计算机的列表。 本文介绍如何检查OpenDNS_Connector帐户是否具有读取这些对象的正确权限。

Active Directory中的每个对象（用户/组/计算机）都有与其关联的ACL安全权限，并且每个对象必须允许OpenDNS_Connector用户帐户读取其属性。



注意：本文假设已检查“OpenDNS_Connector”帐户的正常前提条件。如果仪表板中缺少AD用户/组，请先阅读此文章：
Umbrella控制面板中缺少的AD用户/组。

默认权限

默认情况下，所有经过身份验证的用户都可以读取用户/组/计算机的属性，因此OpenDNS_Connector用户不需要任何额外的权限来执行LDAP同步。

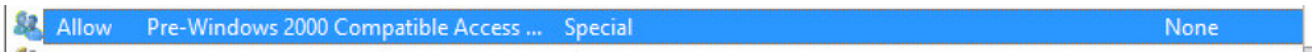
默认权限通常按如下方式设置：

1)在域上为“后代用户对象”、“后代组对象”和“后代计算机对象”分配了“Pre-Windows 2000 Compatible Access”组的读取（读取所有属性）权限。

您可以按如下方式仔细检查：

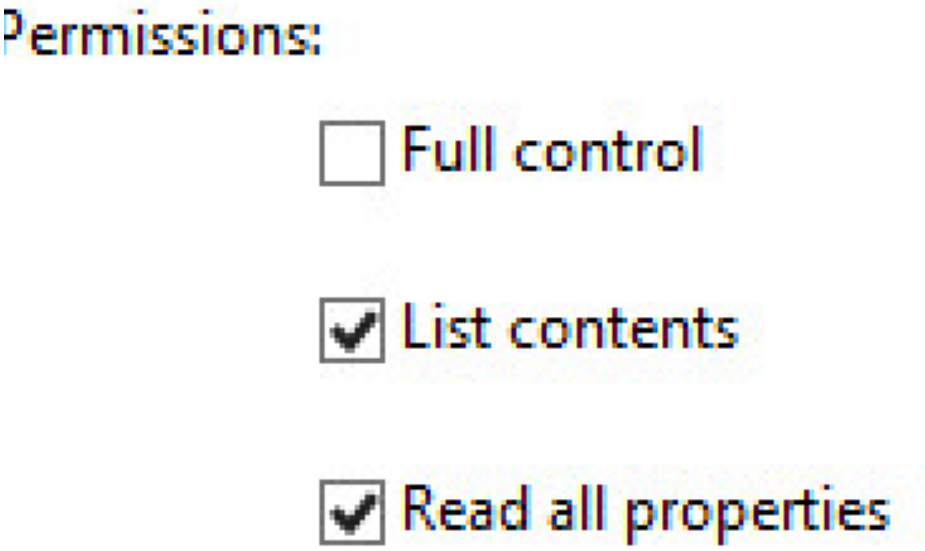
- 打开Active Directory用户和计算机
- 点击“查看”并选中“高级功能”选项。

- 右键单击域对象并选择“属性”，然后选择“安全>高级”
- 选择具有“特殊”权限的“Windows 2000前兼容访问”条目：



115011616667

- 单击“编辑”可详细查看这些权限。
- 在“应用到”部分中选择“后代用户对象”
- 查找以下权限：

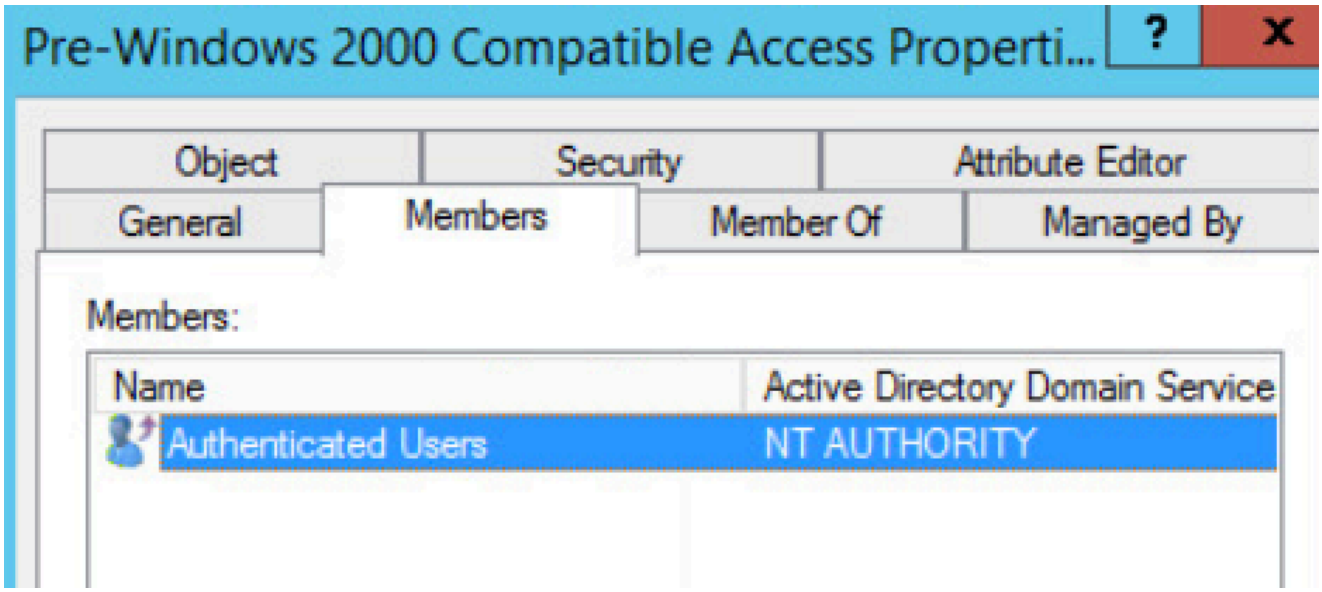


115011616687

- 对“后代组对象”和“后代计算机对象”重复这些步骤

2)所有“经过身份验证的用户”(All 'Authenticated Users')组是“Pre-Windows 2000 Compatible Access”(Windows 2000之前兼容访问)组的成员，该组向所有用户提供这些设置。

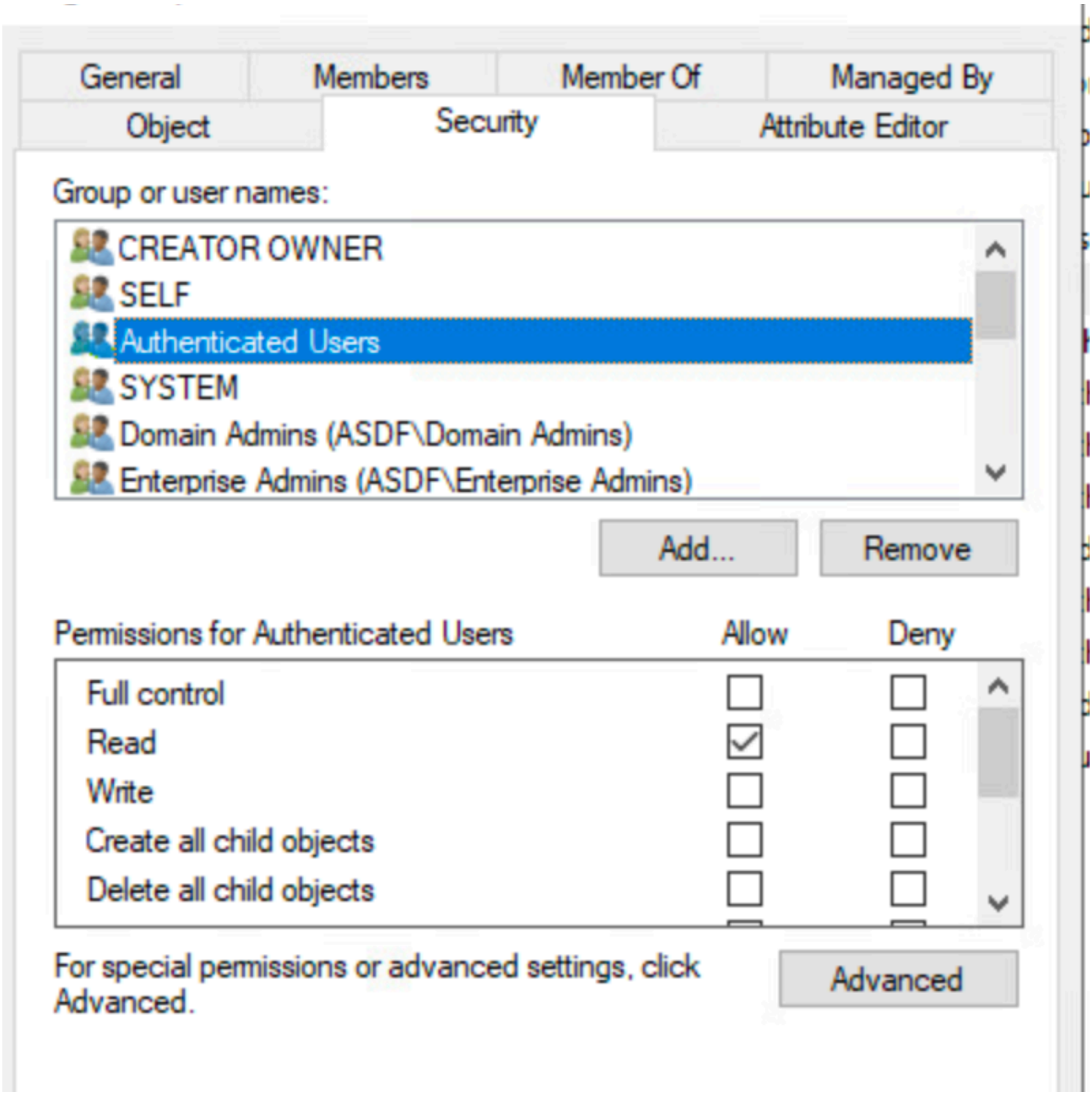
- 右键单击Pre-Windows 2000 Compatible Access组，该组通常位于内置AD容器中。
- 选择“属性”，然后转到“成员”选项卡。
- 检查“Authenticated Users”是否已列出。



115011616707

但是，在某些AD环境中，此权限模型可能已更改，且已通过身份验证的用户已被删除。这可能会表现为某些用户在Umbrella Dashboard中丢失，或者组成员不正确。如果出现这种情况，请将OpenDNS_Connector用户添加到此组，重新启动连接器服务，Umbrella中将显示缺少的项目。

在某些极少数情况下，这仍无法解决问题。如果您发现这种情况，请检查active directory中的groups security选项卡，确保您看到此处列出的已验证用户具有检入读取访问权限。如果未选中此复选框，则将其关闭并重新启动连接器服务以查看组成员是否显示。此外，如果他们发现所有组都缺少此安全设置，他们需要批量将更改应用到全局的所有组。



28728163336852

查看有效访问

您可以使用Windows的“有效访问”工具来查看OpenDNS_Connector用户是否能够读取缺少的特定对象（或组成员资格不正确）。

- 打开Active Directory用户和计算机
- 点击“查看”并选中“高级功能”选项。
- 查找用户对象，然后右键单击以选择“属性”
- 转到“Security > Advanced > Effective Access”(这可以是“Effective Permissions”)

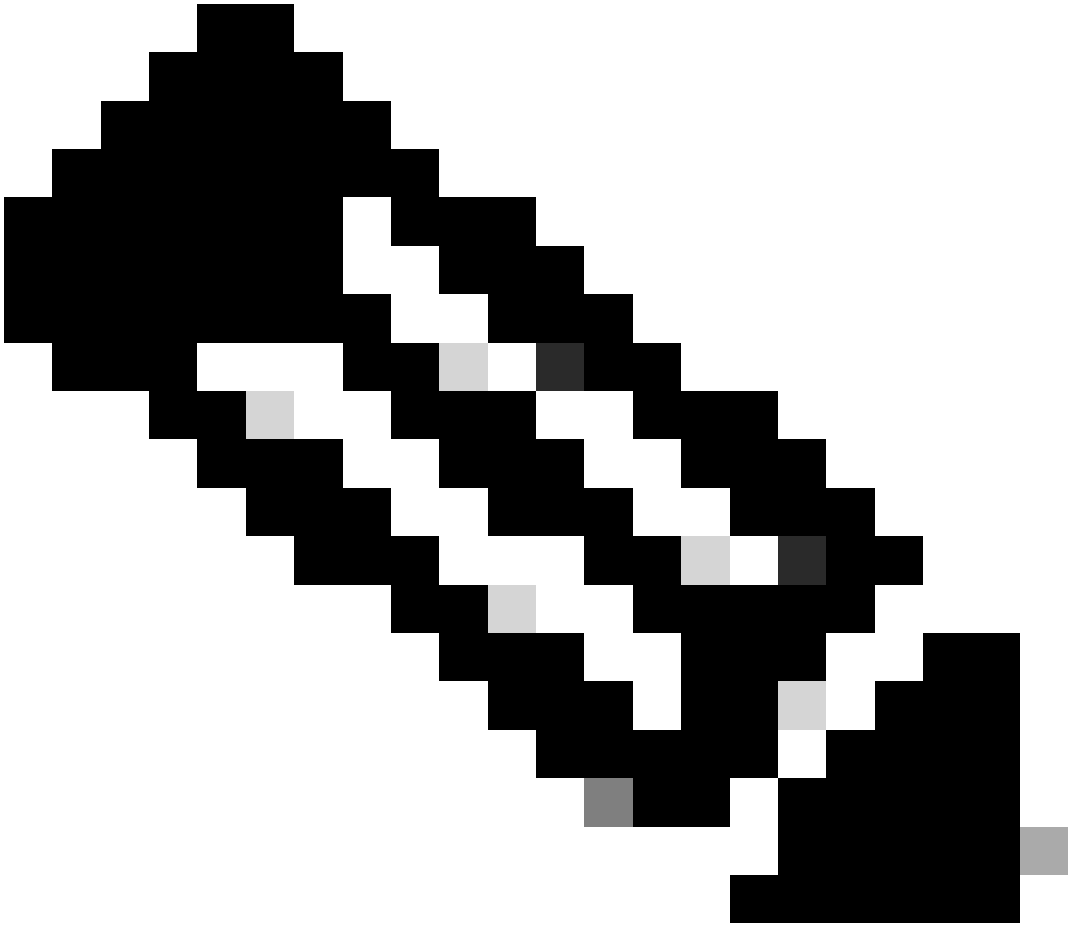
- 点击“选择用户”，然后选择“OpenDNS_Connector”用户帐户。
- 点击“确定”，然后“查看有效访问”
- 确保连接器用户能够读取所有属性:

115011616727

设置OpenDNS_Connector LDAP权限

AD中的“Delegate Control”（委派控制）向导是向“OpenDNS_Connector”用户分配所需权限的快速方法：

1)转至“管理工具”，打开“Active Directory用户和计算机”管理单元。
2)右键单击包含OpenDNS_Connector的域，然后选择“Delegate Control...”，然后点击Next。
3)添加OpenDNS_Connector用户，然后单击“下一步”。
4)选择“Read all user information”(阅读所有用户信息)，然后单击“Next”（下一步）。 [见图3。]
7)单击Finish。 [见图6。]



注意：如果在某些对象上禁用继承，这些步骤可能会失败。 对于这些对象，您需要手动设置权限。

userPerms脚本

附加的powershell脚本是获取特定对象(例如，用户)。 在联系Umbrella技术支持时，请包括此脚本的输出。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。