排除Secure Access AD连接器同步问题

目录

问题

安装在域控制器上的AD连接器未与思科安全访问正确同步。连接器遇到多个同步故障，包括：

- 增量同步失败并出现“访问被拒绝”错误(COMException 0x80070005)。
- DC事件日志读取失败，出现“UnauthorizedAccessException:已尝试执行未经授权的操作”。
- 下载清单时显示“无效URI格式”的云注册问题。
- 同步尝试期间特定AssetID出现HTTP 404 "object_not_found"错误。

连接器似乎可以连接到Cisco Secure Access云服务，但在Active Directory权限端和云注册配置上都失败。

环境

- 带AD连接器的思科安全访问
- AD连接器版本1.15.2
- 安装在域控制器上的AD连接器
- 自定义服务帐户(svcCiscoUmbrella)，而不是默认的Cisco_Connector帐户
- 测试/试用环境设置

分辨率

解决方案涉及通过完整的重新安装过程解决Active Directory权限问题和云注册问题：

步骤 1：验证和清理现有AD连接器条目

在Secure Access控制面板中，验证主机的AD连接器条目，并删除同一服务器的所有过时或重复条目（如果有）。

步骤 2：确保完全卸载

完全卸载现有的AD连接器服务，确保没有剩余可能导致注册问题的配置。

步骤 3：运行域控制器脚本

在重新安装连接器之前，请运行正确的域控制器配置脚本以确保设置适当的权限。需要在每个适用的域控制器上运行脚本，尽管连接器本身可以驻留在其他加入域的计算机上的域控制器之外。

步骤 4：配置服务帐户权限

向服务帐户授予所需的Active Directory权限：

- AD同步权限（域/根作用域，视情况而定）：
    - 读取
    - 复制目录更改
    - 复制目录全部更改（如果环境需要）
    - 在过滤集中复制目录更改（如果环境需要）
- 域控制器上的事件日志访问:
    - 将服务帐户添加到事件日志读取器组。
    - 确保具有同等的、基于策略的权限来读取安全日志。

步骤 5：重新安装AD连接器

重新安装AD连接器服务以生成新的清单和有效的AssetID，从而确保正确的云注册。

步骤 6：重新启动和验证

安装和权限配置后：

1. 重新启动AD连接器服务。
2. 监控连接器日志以确认访问被拒绝和未授权错误停止。
3. 验证日志中是否显示成功的同步条目(例如，“ADSync LDIF RESPONSE:200 Success”)。

原因

同步问题是由两个主要因素引起的：

1. Active Directory权限不足：自定义服务帐户(svcCiscoUmbrella)缺少增量同步和DC事件日志访问所需的AD权限，导致“拒绝访问”和“UnauthorizedAccessException”错误。
2. 云注册问题：连接器实例注册错误或指向无效/旧资产ID，导致下载清单时出现“Invalid URI format”错误，同步尝试期间出现HTTP 404“object_not_found”错误。

安装连接器前未正确执行域控制器配置脚本的安装过程不完整，使得这些问题更加复杂。

相关内容

- 思科安全接入AD连接器配置
- AD连接器权限要求
- AD连接器安装指南

- AD连接器故障排除
- AD连接器服务帐户配置
- 思科技术支持和下载

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）。