使用差异IDP对思科安全访问中的用户/组身份同步进行故障排除

目录

问题

本文档介绍如何对使用不同身份提供程序(IdP)（例如Okta、Microsoft Entra ID和IBM Cloud）的Cisco Secure Access中的用户和组身份同步进行故障排除。

环境

- 思科安全访问 — SCIM调配集成
- 适用于SCIM 2.0 IdP连接器(Okta、Azure AD)

分辨率

概述

Cisco Secure Access支持使用SCIM 2.0标准直接从Okta和Microsoft Entra ID（以前称为Azure AD）调配用户和组身份，无需为纯云身份源部署本地Active Directory(AD)连接器。本文整合了现场工程师和管理员在部署或维护此集成时最常遇到的架构假设、常见故障模式和故障排除指南。

本文档分为四个部分：

- 配置 — 在哪里获取官方设置说明

- 如果违反架构假设，会导致静默或难以诊断的故障
- 提供商特定的问题（Okta与Entra ID）
- 无论IdP如何都适用的通用SCIM协议问题

配置

本文侧重于故障排除，而非初始设置。使用本文档中的官方Cisco TechNotes进行分步配置：

- 要使用Microsoft Entra ID(Azure AD)配置思科安全访问，请参阅以下链接：调配用户和组以通过Entra ID保护访问
- 要使用Okta配置思科安全访问，请参阅以下链接：调配用户和组以通过OKTA保护访问

两个文档都涉及在安全访问中生成SCIM令牌和调配URL、在IdP中配置相应的应用以及运行初始调配同步。

架构初级版

在排除故障之前，请确认部署符合这些核心假设。大多数同步失败都追溯到这些假设之一。

一次一个身份源

不支持从本地AD连接器和云IdP（Okta或Entra ID）并行调配相同的用户或组，从而导致策略实施不一致。如果从AD连接器迁移到云IdP:

- 停止本地AD连接器服务。
- 在启用云IdP调配之前，确认没有剩余同步作业正在运行。

虚拟设备是例外

Entra ID或Okta无法为虚拟设备(VA)提供身份集成，因为IdP无法查看VA所需的专用IP到用户映射。VA部署仍需要本地AD连接器，无论其他组件使用什么工具。

分配与推送

- 操作：向应用程序分配用户或组
    - 它实际执行的操作：将该组的成员用户设置为安全访问
- 操作：推送组(Okta)
    - 它实际执行的操作：设置组对象本身（用于策略目标）。 它不会同步任何用户。

注意：不要推送也分配给应用进行用户调配的组。这会创建重复或冲突的组状态。

组和用户限制

从任一IdP调配的用户数量没有硬性限制。

组被封顶。过去，每个组织有200个组，分别来自Okta或Entra ID;目前的一些文件显示，具体来说，Okta的最高上限较高（最高可达1000个）。确切数字应视环境而定，并向Cisco技术支持中心(TAC)或当前的Cisco文档确认。不会以静默方式调配超过上限的组，也不会出现任何错误。

如果您需要更广泛的覆盖范围，请使用动态“所有用户”(Entra ID)或“所有人”(Okta)组，而不是尝试逐个推送每个组。

SCIM令牌生命周期

在Cisco Secure Access中，当您选择Connect > Users， Groups and Endpoint Devices > Configuration Management > Integrate Directory时会生成令牌。令牌在创建时只显示一次。

重新生成令牌时，它会立即中断IdP端的调配，直到在Microsoft Entra ID或Okta的调配配置中输入新令牌。没有宽限期，并且IdP端错误通常是通用的（身份验证失败），而不是令牌过期消息。

定期刷新令牌以确保安全卫生，并在轮换后立即在IdP端测试连接。

特定于Okta的问题

- 症状：组不显示在安全访问中
    - 根本原因:推送组仅调配组对象；它不会同步成员。
    - 解决方案：确保将相关组成员单独分配到“分配”下的应用程序。
- 症状：用户已调配，但属性缺失或不正确
    - 根本原因:“仅安全访问”(Secure Access only)曲面“显示名称”(Display Name)和“用户名”(Username);给定和族名称未列出。
    - 解决方案：确认已明确选择所需属性进行同步；不要假定所有Okta配置文件字段都会传播。
- 症状：无提示调配不会执行任何操作
    - 根本原因:“创建用户”、“更新用户属性”或“停用用户”切换未启用。
    - 解决方案：验证是否在Okta管理员控制台的Provisioning > To App下选中所有三项。
- 症状：objectGUID或自定义属性未同步
    - 根本原因:未通过User Profile Mapping添加和映射属性。
    - 解决方案：如果需要此标识符，请添加objectGUID属性并创建相应的配置文件映射。
- 症状：同步在令牌循环后停止
    - 根本原因:SCIM 或API令牌在安全访问中重新生成，但在Okta中未更新。
    - 解决方案：在Provisioning > Configure API Integration下输入新令牌，然后再次运行Test API Credentials。
- 症状：无法确定特定用户或组失败的原因
    - 根本原因:未首先检查日志。
    - 解决方案：在上报之前，请选中Reports > System Log（已过滤至Cisco User Management Connector应用程序）。
- 症状：组计数超过上限，有些缺少但没有错误
    - 根本原因:组织包含的组数超过安全访问支持的组数。
    - 解决方案：将范围缩小到仅与策略相关的组，或与Cisco TAC联系，以获得更高级别的组支持。

Microsoft Entra ID特定问题

- 症状：动态组成员身份未反映在安全访问中
    - 根本原因:动态组规则配置错误，或组不在调配的作用域中。
    - 解决方案：在您假设Secure Access同步Bug之前，直接在Entra ID中验证动态成员身份规则。
- 症状：SAML SSO有望推动SWG身份
    - 根本原因:AnyConnect安全网络网关(SWG)不支持根据Entra ID进行安全断言标记语言(SAML)身份验证；它使用与本地AD相同的被动身份验证机制。
    - 解决方案：不要针对Entra ID进行SAML驱动的SWG身份设计；使用被动身份验证（如所记录）。
- 症状：用户错误地显示已停用
    - 根本原因:已发送的Entra ID处于活动状态：false，因为用户超出分配的组范围，或者活动属性映射配置错误。
    - 解决方案：检查用户是否已从作用域组中删除；验证活动映射(通常必须为Not([isSoftDeleted]))。
- 症状：应用已隔离，所有调配已停止
    - 根本原因:目标应用程序返回了重复的不符合SCIM的响应。
    - 解决方案：检查隔离标志的企业应用调配状态，然后确定各个用户发生故障。
- 症状：初始调配周期完全失败
    - 根本原因:首次运行时出现临时同步故障。
    - 解决方案：从“概述”(Overview)页面中单击重新启动调配(Restart Provisioning)，以强制Entra ID再次尝试初始同步。
- 症状：重复的用户意外合并
    - 根本原因:两个源身份共享相同的电子邮件或用户主体名称(UPN)。
    - 解决方案：确保源目录中的电子邮件和UPN唯一性；验证邮件属性是否来自已验证的域。
- 症状：架构更改后，属性停止更新
    - 根本原因:目标端的属性类型已更改（例如，字符串更改为布尔值），但未更新Entra ID映射。

    - 解决方案：手动更正属性映射下的高级设置中的类型。
- 症状：从不填写经理参考
    - 根本原因:用户在其经理离职之前处于作用域中；调配不会自动回填。
    - 解决方案：重新启动调配，以强制对范围内的所有用户进行完全重新评估。

IBM安全验证特定问题

- 症状：用户调配，但组从不出现在安全访问中
    - 根本原因:验证自定义SCIM连接器是否仅发出用户操作；从未发送过POST /Groups呼叫（帐户调配功能差距，不是映射错误）。
    - 解决方案：捕获连接器踪迹，并确认是否发生任何/组调用；如果没有，则通过Cisco AD Connector、CSV导入或针对Secure Access SCIM终端的计划脚本调配组。
- 症状：使用400或404时组成员身份更新失败
    - 根本原因:members[].value引用验证内部用户ID，而不是在用户创建时返回的SCIM ID安全访问。
    - 解决方案：更正成员映射以使用安全访问SCIM ID并再次运行完全同步。
- 症状：组出现，但为空
    - 根本原因:在安全访问中存在成员用户之前推入的组;membership PATCH引用未知用户。
    - 解决方案：如果用户存在，请再次运行完全同步；确保同步排序在组之前创建用户。
- 症状：SAML登录循环或重复重定向
    - 根本原因:验证IdP端点是否由SWG代理或解密，这会中断身份验证流程。
    - 解决方案：绕过来自SAML或解密（外部域列表或选择性解密）的验证IdP URL。
- 症状：用户通过SAML进行身份验证，但没有基于用户的策略匹配
    - 根本原因:SAML NameID与调配的用户authName不匹配。
    - 解决方案：将验证SAML应用程序中的NameID >格式与authName属性映射（通常为邮件或UPN）对齐；再次测试。
- 症状：经过几周或几个月的稳定后，调配会停止工作
    - 根本原因:SCIM令牌在Secure Access中已旋转或过期，但在Verify连接器中未更新。

    - 解决方案：在Secure Access中刷新令牌，并在Verify custom应用中更新令牌;日历刷新频率。

- 症状：重新同步时创建的重复用户
    - 根本原因:externalId映射到可变或非唯一属性（例如，显示名称、可更改的电子邮件）。
    - 解决方案：将externalId映射到不可变的标识符（验证用户ID或objectGUID）；清除重复项，然后重新同步。
- 症状：已停用验证用户在Secure Access中保持活动状态
    - 根本原因:挂起操作未映射到active:false，或者禁用连接器中的操作。
    - 解决方案：启用停用操作并将挂起映射到active:false;使用测试用户进行验证。
- 症状：验证中的属性更改不传播
    - 根本原因:用户或属性超出调配策略范围，或者更新操作被禁用。
    - 解决方案：审核应用调配策略或授权；启用更新；触发手动同步。
- 症状：安全访问拒绝具有方案或501样式错误的请求
    - 根本原因:不符合SCIM的负载（缺少架构数组、错误的URN、不支持的操作）。
    - 解决方案：利用基线卷曲测试复制；更正负载或映射；如果连接器发出格式不正确的请求，则升级至IBM。
- 症状：漫游用户缺少SWG身份，尽管SAML正在工作
- 根本原因:希望SAML为使用被动或基于代理的身份的部署模式驱动身份。
- 解决方案：根据安全访问文档，确认每种部署模式的身份获取方法；请勿将SAML设计为唯一的身份源。

通用SCIM问题

这些不是特定于思科的，但始终显示在安全访问部署中，因为底层传输是标准SCIM 2.0:

- 隔离状态会掩蔽单个错误:如果同步似乎已完全停止而不是每个用户都失败，请在调查单个属性问题之前检查应用级别的隔离或暂停状态。
- 409停用冲突:IdP尝试停用用户和目标引发冲突的常见模式。这通常是活动属性映射或组范围问题，而不是真正的系统错误。

- 空白或清除的字段并不总是传播:某些SCIM服务器实现保留最后一个非空值；清除IdP中的字段时，可能需要首先将占位符值推入。
- URL或配置更改以静默方式使身份验证失效：对SCIM终端URL的任何更改通常都需要您再次提供承载令牌。错误显示为无效URL，即使实际问题是陈旧标记。
- 没有本地Webhook或事件流:要求实时推送用户或策略更改通知的自动化必须轮询报告API或通过思科XDR进行集成。安全访问不会发出出站调配Webhook。

如果之前的步骤无法解决问题，请通过IdP端提供的调配日志升级至Cisco TAC。安全访问端的后端调配日志通常需要TAC访问才能提取。

原因

由于承载令牌过期、属性映射不匹配、缺少目标组或调配范围不足，SCIM调配集成无法推送一个或多个记录。

相关内容

- 思科:调配用户和组以通过Entra ID保护访问
- 思科:调配用户和组以通过OKTA保护访问
- Microsoft了解：SCIM 2.0协议合规性的已知问题 — Microsoft Entra ID
- Microsoft了解：排除Microsoft Entra ID SCIM API错误
- 在身份提供程序中配置SAML SSO:https://www.ibm.com/docs/en/security-verify?topic=sign-configuring-saml-single-in-identity-provider
- 自定义(SCIM)应用的调配：https://www.ibm.com/docs/en/security-verify?topic=endpoints-configuring-provisioning-custom-applications
- 调配和监管概述（通用SCIM连接器）：https://docs.verify.ibm.com/verify/docs/use-cases-provisioning-and-governance
- 本地调配网桥（AD/LDAP源）：https://docs.verify.ibm.com/verify/docs/on-premises-provisioning

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）。