与Active Directory和Microsoft EntraID的思科安全访问身份同步

目录

问题

用户尝试在Cisco安全访问中调配来自两个具有相同域名的身份源的用户和组时遇到问题。特定场景涉及同步本地Active Directory和Microsoft EntraID（以前称为Azure AD）的身份，其中两个源使用相同的域名(例如，domain.com)。

主要关注事项包括：

- 了解当两个身份源中存在相同用户和组时，身份所有权和组成员身份映射的行为方式
- 确保为访问本地和云资源的混合用户实施一致的安全访问策略
- 在此混合身份配置中为用户保持内部IP可视性
- 确定两个源的并发同步是否会导致生产环境出现问题

文档显示“不支持从Cisco AD Connector和Cisco User Management for Secure Access应用并行同步相同用户和组，从而导致访问规则实施不一致”。

环境

- 采用AD连接器和EntraID集成的思科安全访问
- 具有与EntraID域匹配的域名的本地Active Directory
- Microsoft EntraID(Azure AD)，与本地AD具有相同的域名
- 用于联合身份验证的SAML SSO配置
- 用于策略实施的安全网络网关(SWG)模块

- 需要同时访问本地和云资源的混合环境

分辨率

已确认从Active Directory和EntraID源进行并发同步的以下行为：

组同步行为

当同步来自两个源的具有相同名称的组时：

- 在Cisco Secure Access中创建两个单独的组对象 — 每个源一个
- 在访问策略中，组可以根据其源前缀进行区分
- 本地AD组显示为：AD域/组名
- EntraID组显示为：组名

实验室验证显示同步成功，并显示消息“成功”。**<<<<** Synced"表示来自多个EntraID域的组。

用户同步行为

当同步来自两个源的具有相同用户ID的用户时：

- 用户身份在同步期间被覆盖
- 在安全访问中仅有一个唯一用户ID保持可见
- 最终同步源决定用户的属性和组成员身份
- 配置本地AD时，EntraID同步通常优先于本地AD

访问策略配置

两种组类型都可用于访问策略：

- 使用完整路径引用本地AD组：AD域/组名
- 使用简单名称引用EntraID组：组名
- 策略可以根据用户的组成员身份源来区分用户

后续设置对许多客户都非常有效。

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

原因

在我们的测试中，我们确认，无论何时从本地AD连接器同步用户，它都会在Umbrella控制面板中有效“声明”该身份。如果通过Azure AD同步已存在同一用户，本地同步将覆盖现有的EntraID用户数据。

此行为是有案可查的限制。根据Cisco官方技术文档：https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

“不支持从Umbrella AD连接器和Cisco Umbrella Azure AD应用并行同步相同的用户和组身份，从而导致策略实施不一致。”

结论:所需的设置（Azure和On-Prem中现有用户的VA可见性）被确认为不受支持的配置。路径转发需要使用漫游客户端以确保一致的标识实施。

相关内容

- 从Azure AD调配身份 — Cisco Umbrella文档
- 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）。