将安全访问AD连接器从传统身份验证迁移到API身份验证

目录

问题

使用Cisco Secure Access with Active Directory(AD)连接器的组织会收到通知，指出建议对Active Directory和虚拟设备使用API身份验证，且旧身份验证设置为在2026年5月29日到期。用户需要配置帮助才能在到期日期之前从传统身份验证迁移到API身份验证，并希望了解迁移过程中对AD和虚拟设备同步的潜在影响。主要问题是，在工作时间内实施此更改是否会导致可能影响身份和策略相关操作的AD和VA同步操作失败。

环境

- 思科安全访问（以前称为Cisco Umbrella）
- 已部署Active Directory连接器
- 当前使用的传统身份验证方法
- 在2026年5月29日之前需要API身份验证迁移
- 仅AD环境（某些情况下不使用虚拟设备）

分辨率

从传统身份验证迁移到API身份验证涉及在安全访问门户中生成API密钥并正确配置它们。此过程需要为AD连接器和虚拟设备创建管理API密钥和客户端API密钥。

步骤 1：生成管理API密钥

在安全访问门户中导航到Admin > API Keys，并生成新的Admin API Key和Admin Key Secret。在生成客户端API密钥对时需要安全地存储这些凭证。

步骤 2：生成客户端API密钥对

导航到用户和组>配置管理>高级设置，然后找到API身份验证部分。输入第1步中生成的Admin API Key和Admin Key Secret，然后单击Generate Client API Key Pair。这会生成AD连接器和虚拟设备使用的客户端API密钥和客户端密钥。

步骤 3：在高级设置中配置API身份验证

将生成的客户端API密钥和客户端密钥复制到安全访问门户的API身份验证高级设置部分。安全地保存这些凭证，因为所有AD连接器和虚拟设备配置都需要这些凭证。

步骤 4：更新AD连接器和虚拟设备

将新生成的客户端API密钥和客户端密钥应用于所有已部署的AD连接器和虚拟设备。这确保它们可以使用新的API身份验证方法针对注册和运行状况检查进行正确身份验证。

迁移影响和最佳实践

在安全访问门户中生成API密钥通常不会造成中断。但是，在切换期间，当AD连接器和虚拟设备更新为使用新的客户端API密钥和密钥时，会对操作产生影响。

转换期间的预期影响：

- 对于仍在使用旧版身份验证的组件，可能会发生临时同步和运行状况检查失败。
- AD/VA同步在转换窗口期间滞后或失败。
- 如果同步失败，依赖于新的身份/组数据的策略决策可能会受到影响。

推荐的实施方法：

- 在非工作时间或可能的维护时段执行迁移。
- 在工作时间实施方面，请使用受控滚动更新方法。
- 每次更新一个连接器/VA并在继续之前验证健康状态。
- 避免同时更新所有节点。
- 确保多个连接器/VA具有足够的冗余以进行滚动更新。

兼容性和要求：

- API身份验证适用于仅AD部署，不需要虚拟设备。
- 在迁移期间，传统身份验证方法和API身份验证方法均保持活动状态。
- AD连接器必须能够通过api.opendns.com与Umbrella同步并过渡到api.umbrella.com。

原因

思科安全访问正在从传统身份验证方法过渡到作为标准身份验证机制的API身份验证。传统身份验证方法的预定弃用日期为2026年5月29日。API身份验证最终成为唯一受支持的身份验证方法，组织必须在传统方法到期之前迁移，以避免服务中断和可能发生的AD/VA同步故障（可能需要完全重新安装才能恢复）。

相关内容

- 思科安全访问API身份验证文档
- 思科安全访问高级配置
- 思科安全访问配置管理
- 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）。