Duo SAML集成时安全访问RAVPN身份验证失败

目录

问题

当尝试使用Duo作为身份提供者(IDP)并在后台集成Active Directory连接到思科安全访问远程访问VPN(RAVPN)时，尽管在Duo门户级别成功进行身份验证，但用户仍会遇到身份验证失败。

具体症状包括：

- Duo门户显示身份验证成功消息。
- Duo成功后，Cisco SecureClient立即显示“身份验证失败”错误消息。
- Duo日志显示“已授予访问权限”状态。
- 思科安全访问门户日志显示“AAA故障”状态。

这将创建一个断开连接，其中外部身份提供程序确认身份验证成功，但VPN客户端由于安全访问基础设施中的身份验证验证失败而无法建立连接。

环境

- 思科安全访问RAVPN部署
- 作为SAML身份提供者的双安全设置
- Active Directory与双核集成
- 用于VPN连接的Cisco SecureClient
- 基于SAML的身份验证流程

分辨率

通过更正Duo和Cisco Secure Access之间的用户属性映射解决了身份验证故障。接下来几节中概述的步骤用于识别和解决问题。

步骤 1：检查活动搜索

1. — 登录思科安全访问控制面板。单击Monitor>远程访问日志。

2. — 检查授权检查失败消息下的用户名字段。

3. — 将其与Connect > User and Groups下的UPN值进行匹配。

思科安全访问查看授权检查的用户主体名称值。

从Duo传递的用户主体名称与该用户在User and Groups下的用户主体名称值不匹配。

调查显示：

- 用户电邮地址：user@gmail.com
- 用户主体名称(UPN用户名

步骤 2：Duo配置调整

解决方案涉及修改Duo SAML配置以确保正确的用户属性映射：

- 访问Duo Admin Panel。
- 导航至思科安全访问的SAML应用配置。
- 修改用户属性映射以发送邮件地址，该地址必须与该用户的User Principal Name值在User and Groups下。
- 保存配置更改。

步骤 4：确认

调整Duo配置后，验证流程已经过测试，并且验证成功。用户可以使用远程访问VPN进行连接，而不会发生身份验证失败。

原因

身份验证失败的根本原因是双方SAML断言和思科安全访问期望之间的用户属性映射不匹配。Duo配置为在SAML断言中以用户主体名称(UPN)发送用户名，而Cisco Secure Access配置为预期用户邮件地址。这种不匹配导致身份验证在安全访问级别失败，尽管身份验证在Duo IDP级别成功，导致在Secure Access中记录了“AAA故障”，而Duo日志显示为“已授予访问权限”。

相关内容

- 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）。