使用Azure Entra ID排除SNA Manager SSO身份验证故障

目录

问题

在将Azure Entra ID集成为SAML身份验证的身份提供程序(IdP)后，用户尝试登录到SNA Manager时遇到SSO身份验证失败。显示的特定错误消息为：

“身份验证服务无法完成您的请求。如果此问题仍然存在，请与管理员联系。"

在设置过程中，导入SP（服务提供商）元数据文件后，SNA Manager FQDN自动从原始SNA Manager URL更改为包含“/fedlet”，从而导致身份验证设置失败。系统审核日志确认身份验证失败，显示“未知用户”错误，表明SNA管理器未识别从Azure传输的SAML响应中传输的用户名。

环境

- 思科安全网络分析(SNA)管理器7.6.0版
- 配置为SAML标识提供程序的Microsoft Azure Entra ID

分辨率

解决方法涉及更正Azure Entra ID和SNA Manager中的SAML NameID属性配置，以确保正确的用户名格式匹配。

步骤 1：执行SAML跟踪分析

使用浏览器开发工具执行SAML跟踪并检查Azure中的IdP响应，以确定传输的NameID格式。跟踪显示Azure正在发送NameID属性中的完整用户主体名称(UPN):

<#root>

<Subject><NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent" SPNameQualifier="https:/

username@example.com<

/NameID>

步骤 2：查看SNA Manager审核日志

检查SNA Manager审核日志，确认与格式错误的NameID相关的身份验证失败：

Aug 3 06:53:36 device AuditLogger[1480861]: AuditLogger: osaxsd/1480861,4003,2026-08-03T06:53:36TZD+000

步骤 3：修改Azure SAML NameID配置

在Azure Entra ID SAML配置中，将NameID属性从默认用户主体名称更改为使用“本地SAM帐户名称”。 这可确保NameID仅包含不带域后缀的用户名（username@example.com成为用户名）。

步骤 4：更新SNA Manager SAML ID配置

导航到SNA Manager用户管理页面，并更新SAML ID值以匹配配置更改后Azure传输的已更正的NameID格式。

步骤 5：验证SSO身份验证

尝试通过SAML工作流程登录，测试SSO身份验证。用户现在已成功进行身份验证，没有收到以前的错误消息。

原因

身份验证失败是由于Azure Entra ID发送的NameID格式与SNA Manager预期的用户名格式不匹配造成的。Azure配置为在SAML NameID属性中以“username@example.com”格式发送用户主体名称(UPN)，而SNA Manager仅期望用户名部分，不带域后缀。这种格式差异导致SNA Manager将传入的身份验证请求视为来自无法识别的用户，导致“未知用户”身份验证失败。

相关内容

- 为Microsoft Azure SAML集成配置SNA Manager
- 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）。