在Windows Server上解决帐户不匹配的目录连接器身份验证故障

目录

问题

Windows Server上安装的Cisco Directory Connector在尝试使用不同于登录服务器的管理员帐户登录时身份验证失败。身份验证过程错误地尝试使用Windows服务器登录帐户而不是预期的Webex Control Hub管理员帐户，导致以下错误消息：

- 验证失败
- 您的帐户未获得授权。请与您的管理员联系。

后端日志显示SAML2映射错误：

```
com.sun.identity.saml2.common.SAML2UserNotFoundException: No local user being mapped.
```

目录连接器先前在登录期间提示选择帐户，但在问题出现后，此提示将失败，并且身份验证尝试使用不正确的帐户。应用程序重新安装、服务重新启动和服务器重新启动不会解决初始身份验证失败的问题。

环境

- Windows Server 2019 Standard上安装的Cisco Directory Connector
- 托管在Google Compute Engine VM上的服务器
- 专用于目录连接器的服务器，无其他主要服务
- Active Directory中的独立用户帐户：没有电子邮件权限的服务器管理员帐户和没有服务器登录权限的常规电子邮件帐户
- 使用增量同步计时配置的目录连接器同步计划
- BIOS模式设置为传统，不支持安全启动

分辨率

通过以下步骤解决了身份验证问题：

步骤 1：服务帐户配置

更改Directory Connector服务帐户，以使用具有适当Active Directory权限的域帐户：

1. 在Windows Server上打开services.msc。
2. 找到目录连接器服务。
3. 将运行帐户从本地系统更改为具有足够AD权限的域帐户。
4. 重新启动Directory Connector服务。

步骤 2：帐户映射验证

确保目录连接器的本地登录与Webex Control Hub中的管理员帐户匹配：

1. 验证用于Directory Connector的电子邮件帐户是否具有AD用户对象的读取权限。
2. 确认帐户具有连接到域控制器和读取Active Directory用户对象的权限。
3. 如有必要，请根据部署指南将管理员帐户添加为Active Directory中的备用电子邮件。

步骤 3：删除冗余实例

删除任何不需要的目录连接器实例：

1. 导航到Directory Connector界面。
2. 单击不需要实例的三点菜单。

3. 选择停用实例。

步骤 4：同步计划调整

根据环境需要，将增量同步计时从默认的24小时间隔调整为较短的首选间隔。

步骤 5：配置审核

检查并确认目录连接器配置和同步计划设置，以确保操作正确。

原因

主要根本原因是本地服务器登录帐户与目录连接器/Webex管理员帐户不匹配。目录连接器尝试使用Windows服务器登录帐户而不是预期的Webex Control Hub管理员帐户进行身份验证。此映射失败是由于Active Directory中的帐户分离，其中Directory Connector使用不同的管理员帐户登录到服务器时，无法正确映射Webex管理员帐户。SAML2身份验证过程失败，因为无法在服务器登录帐户和Webex Control Hub管理员帐户之间建立本地用户映射。

相关内容

- Webex Directory Connector部署指南
- 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）。