使用ADFS IdP配置的SAML断言过期SSO故障排除

目录

简介

本文档介绍在登录到Cisco Webex App/Cisco Webex Control Hub时排除SSO错误“SAML断言已过期”。

先决条件

要求

Cisco 建议您了解以下主题：

- 单点登录配置
- Webex Control Hub
- ADFS服务器和Powershell

使用的组件

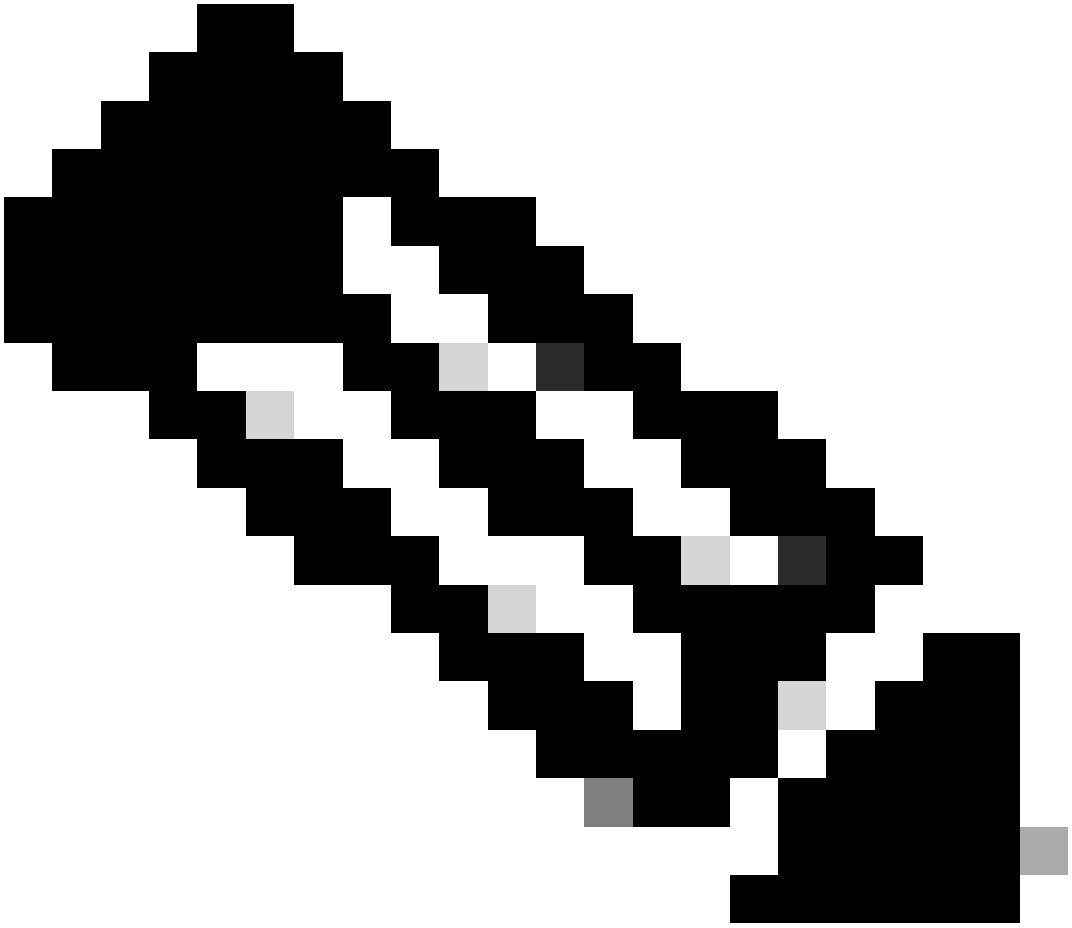
本文档中的信息基于以下软件和硬件版本：

- Windows ADFS服务器2022
- Webex Control Hub

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

本文档介绍在登录到Cisco Webex App/Cisco Webex Control Hub（在输入邮件ID并完成SSO流程后显示自身）时排除单点登录(SSO)“SAML断言已过期”错误的故障。



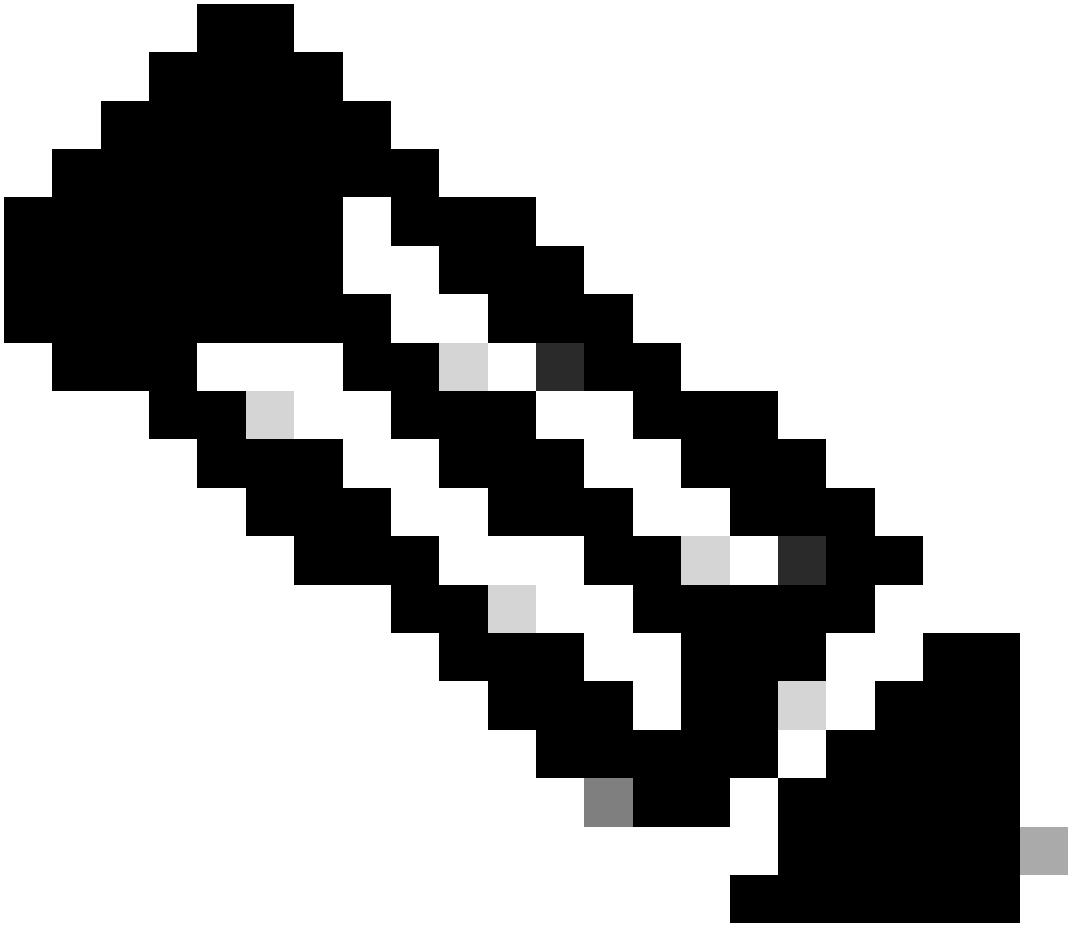
注意：此问题主要出现在ADFS服务器上。本文档仅特定于ADFS IdP。

故障排除步骤

1. 确保可以使用管理员凭据登录到ADFS服务器。
2. 检查登录尝试中出现的错误消息。理想情况下，这是一个简单的修复方法，可以通过查看错误消息本身来直接进行问题故障排除。
3. 只有当ADFS服务器时间与本地计算机时间不匹配时，才会出现“SAML Assertion Expired”错误消息。这需要一个命令来修复时间差异。但是，您可以查看本地计算机的HAR日志，可以看到在HAR响应中的差异。

日志分析

您可以在HAR日志中检查登录时间和之前/之后时间：



注意：断言时间必须介于“Not before:2025年4月07日09:00:37”和“Not After:2025年4月07日10:00:37 SAML”响应中提供的时间。

```
Not Before: Apr 07 2025 09:00:37
Not After: Apr 07 2025 10:00:37
Assertion Time: Apr 07 2025 09:00:07
```

根本原因

断言时间：Apr 07 2025 09:00:07不在SAML响应中提供的not before和not after的范围。

解决方案

在ADFS服务器PowerShell上运行此命令以解决此问题：

Set-ADFSRelyingPartyTrust -TargetIdentifier -NotBeforeSkew 3

此命令对于不同的组织可能不同。获取此命令的最佳方法是使用组织的SP元数据中的SP(Webex)实体ID代替命令中的URL。

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）。