對使用ADFS IdP配置的SAML斷言過期SSO進行故障排除

目錄

簡介

本文檔介紹在登入到Cisco Webex App/Cisco Webex Control Hub時排除SSO錯誤「SAML斷言已過期」。

必要條件

需求

思科建議您瞭解以下主題：

- 單一登入配置
- Webex Control Hub
- ADFS伺服器和Powershell

採用元件

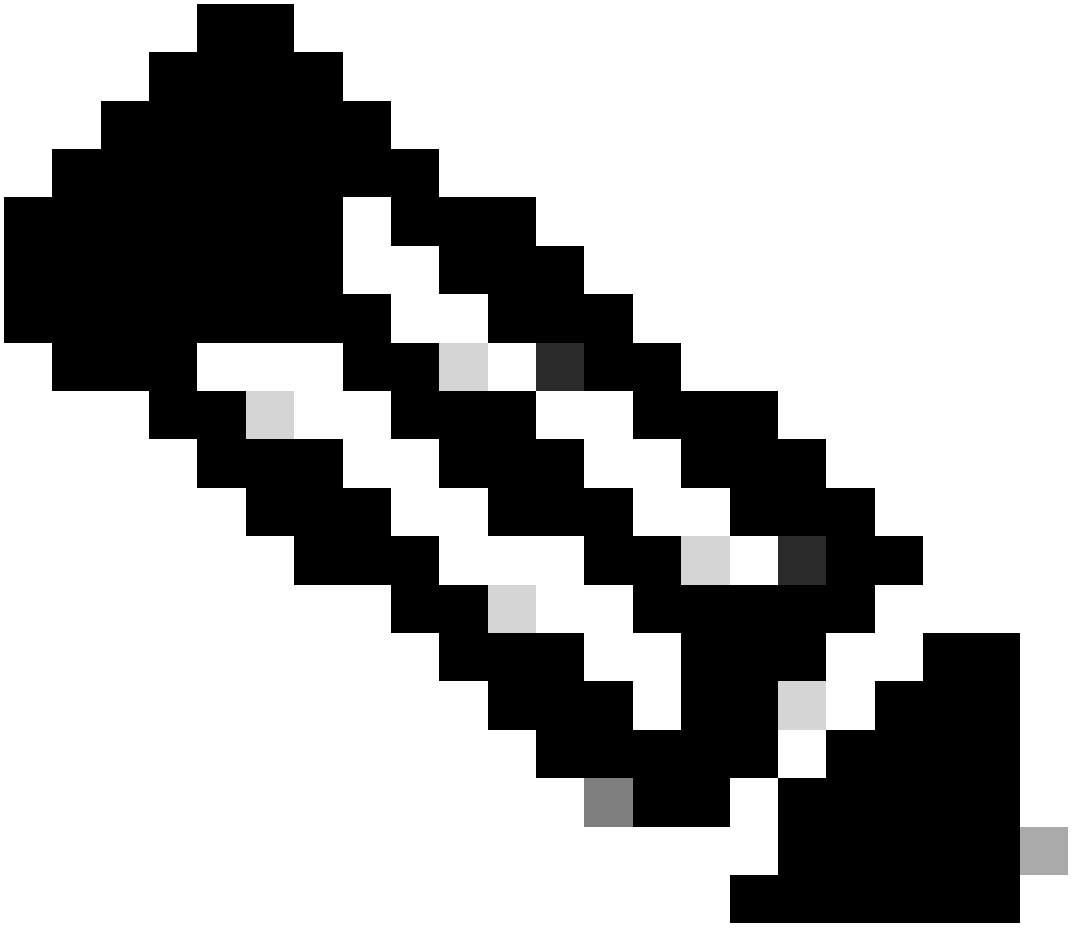
本文中的資訊係根據以下軟體和硬體版本：

- Windows ADFS伺服器2022
- Webex Control Hub

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

本文描述在登入到Cisco Webex App/Cisco Webex Control Hub（在輸入電子郵件ID並完成SSO流程後顯示自身）時，對單一登入(SSO)「SAML斷言過期」錯誤進行故障排除的過程。



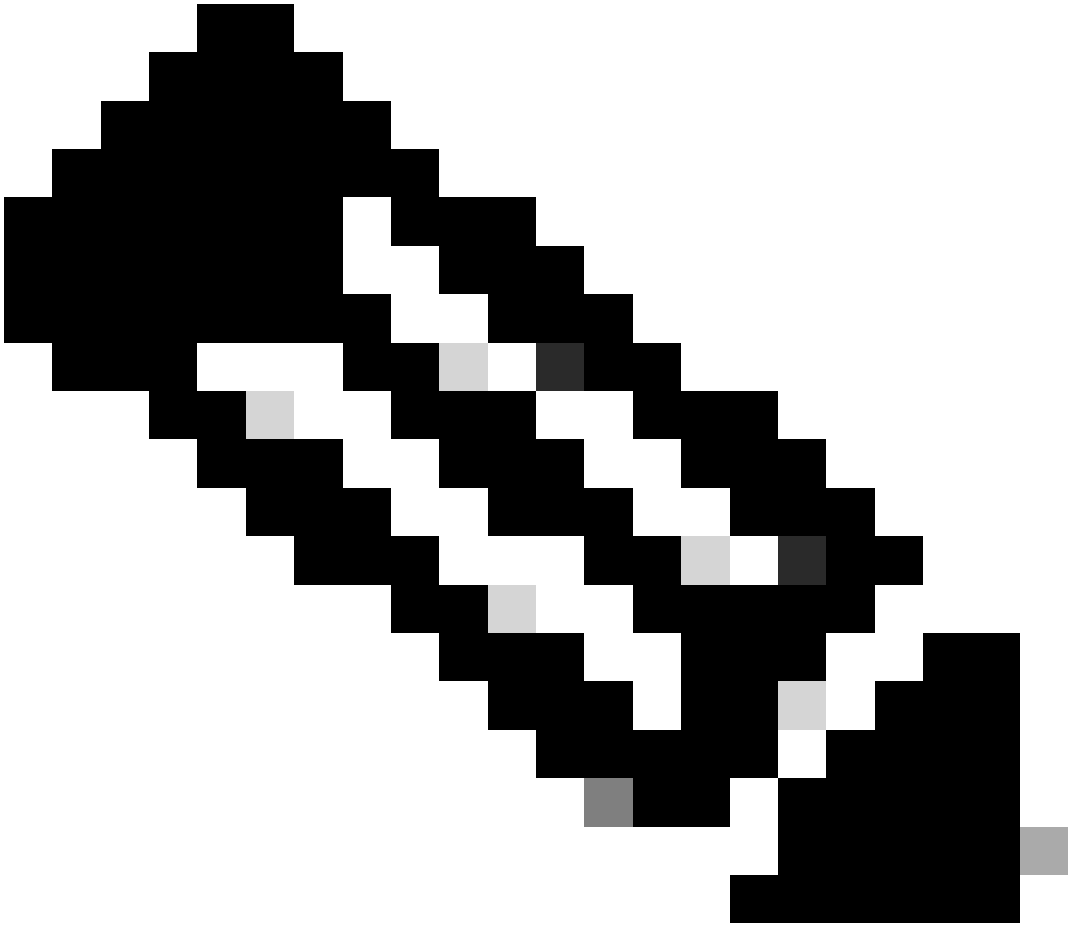
附註：此問題主要出現在ADFS伺服器上。本文檔僅特定於ADFS IdP。

疑難排解步驟

1. 確保可以使用管理員憑據登入到ADFS伺服器。
2. 檢查登入嘗試中出現的錯誤消息。理想情況下，這是一個簡單的修複方法，通過檢視錯誤消息本身，可以直接進行問題故障排除。
3. 只有當ADFS伺服器時間與本地電腦時間不匹配時，才會出現「SAML Assertion Expired」錯誤消息。這需要一個命令來修復時間差異。但是，您可以檢視本地電腦的HAR日誌，並且可以看到HAR響應中的差異。

日誌分析

您可以在HAR日誌中檢查登入時間和之前/之後時間：



附註：斷言時間必須介於「不早於：2025年4月07日09:00:37」和「Not After:2025年4月07日10:00:37 SAML」響應中提供的時間。

```
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

斷言時間：Apr 07 2025 09:00:07不在SAML響應中提供的不早於和不晚於的範圍內。

解決方案

在ADFS伺服器PowerShell上運行以下命令以解決問題：

Set-ADFSRelingPartyTrust -TargetIdentifier -NotBeforeSkew 3

不同組織可以使用此命令。獲取此命令的最佳方式是使用SP後設資料中的SP(Webex)實體ID代替命令中的URL。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。