使用 SSO 時出現「HTTP 狀態 401 - 驗證失敗：SAML 驗證錯誤訊息」

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[問題](#)
[解決方案](#)

簡介

本文描述使用單一登入(SSO)時，在一段非活動時間後出現「HTTP Status 401」錯誤消息的問題。

必要條件

需求

思科建議您瞭解以下主題：

- SSO
- Active Directory聯合身份驗證服務(AD FS)
- CloudCenter

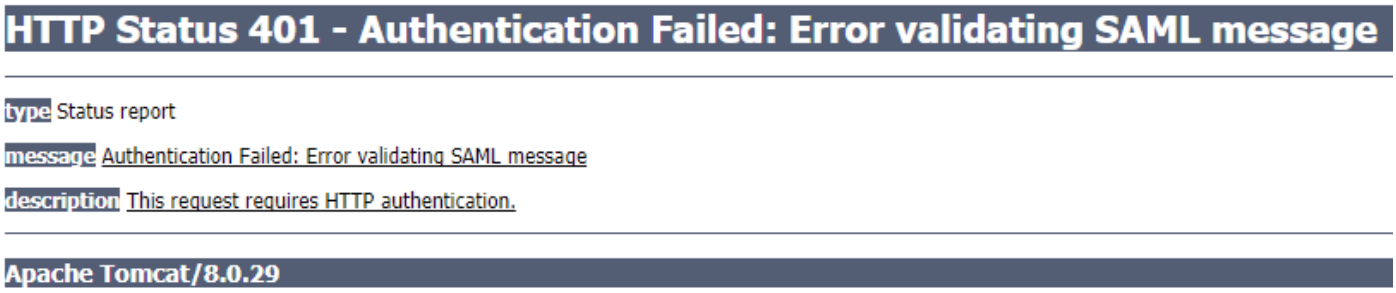
採用元件

本檔案所述內容不限於特定軟體或硬體版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

問題

使用SSO時，在一段非活動時間後可能會收到「401」錯誤，而不是如圖所示再次登入提示。



您可以再次登入的唯一方法是關閉整個Web瀏覽器並重新開啟它。

解決方案

這是由於CloudCenter和SSO伺服器之間的超時值不匹配。

增強功能允許ForceAuthn Parameters支援，這允許兩個值和CloudCenter之間的不匹配正常註銷。此增強功能可在https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752上找到。

唯一的解決方法是移除不匹配。有三個位置需要匹配超時值。前兩個位於CCM本身。

1. 導覽至**/usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml**。
2. 修改**<session-timeout>time_In_Minutes</session-timeout>以反映**所需的超時（分鐘）。
3. 導覽至**/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties**。
4. 修改**saml.maxAuthenticationAge.seconds=timeout_in_seconds**，以反映所需的超時（秒）。

第三個位置在SSO伺服器上，位置可能因所運行的SSO伺服器的型別而異。Web SSO生存期值必須與CloudCenter上配置的兩個值匹配。

一旦這三個條件都匹配，當發生超時時，系統就會將您拖回登入螢幕，然後才允許您檢視該頁面。