「HTTP Status 401 - Authentication Failed:SSO使用時のSAMLメッセージの検証エラー

内容

概要

このドキュメントでは、シングルサインオン(SSO)を使用しているときに、非アクティブ状態が続いた後に「HTTP Status 401」エラーメッセージが表示される問題について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SSO
- Active Directoryフェデレーションサービス(AD FS)
- CloudCenter

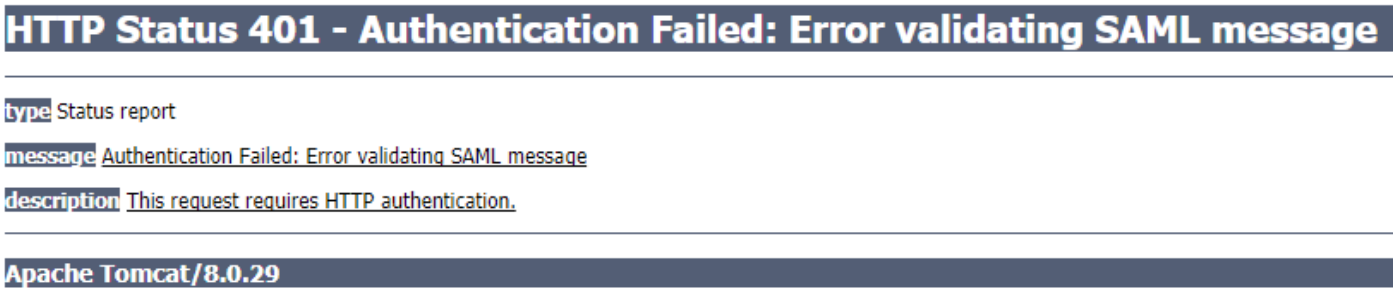
使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

問題

SSOを使用すると、図に示すように再度ログインを求めるプロンプトの代わりに、非アクティブ状態が続くと「401」エラーが表示される場合があります。



再度ログインする唯一の方法は、Webブラウザ全体を閉じて再度開くことです。

解決方法

これは、CloudCenterとSSOサーバ間のタイムアウト値が一致していないことが原因で発生します。

拡張機能により、ForceAuthn Parametersのサポートが可能になり、2つの値とCloudCenterの間の不一致が正常にログアウトされる可能性があります。この機能強化については、https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752を参照してください。

唯一の回避策は、不一致を削除することです。タイムアウト値を一致させる必要がある場所は3つあります。最初の2つはCCM自体にあります。

1. /usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml に移動します。
2. **<session-timeout>time_In_Minutes</session-timeout>を変更して、必要なタイムアウトを分単位で**反映します。
3. /usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties に移動します。
4. **saml.maxAuthenticationAge.seconds=timeout_in_secondsを変更して、必要なタイムアウトを秒**単位で反映します。

3つ目はSSOサーバにあり、実行しているSSOサーバのタイプによって場所が異なる場合があります。Web SSOライフタイム値は、CloudCenterで設定されている2つの値と一致する必要があります。

3つすべてが一致すると、タイムアウトが発生すると、ログイン画面に戻ってからページを表示できます。