"HTTP Status 401 - Authentifizierung fehlgeschlagen: Fehler beim Validieren der SAML-Nachricht" bei Verwendung von SSO

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Problem](#)
[Lösung](#)

Einführung

Dieses Dokument beschreibt ein Problem, bei dem Sie nach einer Inaktivität eine Fehlermeldung vom Typ "HTTP Status 401" erhalten, wenn Sie Single Sign-On (SSO) verwenden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- SSO
- Active Directory Federation Service (AD FS)
- CloudCenter

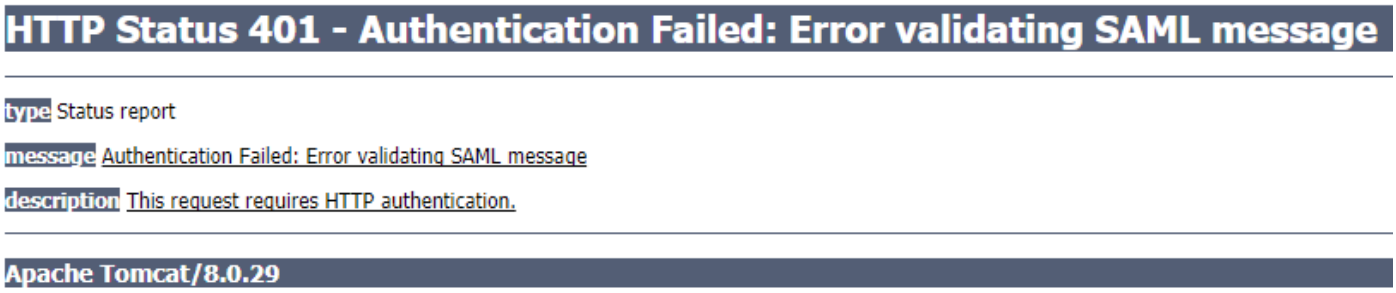
Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- oder Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem

Wenn Sie SSO verwenden, können Sie nach einer Inaktivität einen "401"-Fehler erhalten, anstatt eine Aufforderung, sich erneut anzumelden, wie im Bild gezeigt.



Sie können sich nur erneut anmelden, wenn Sie den gesamten Webbrowser schließen und ihn erneut öffnen.

Lösung

Dies wird durch eine Diskrepanz zwischen den Timeout-Werten zwischen CloudCenter und dem SSO-Server verursacht.

Eine Erweiterung ermöglicht die Unterstützung von ForceAuthn Parameters, wodurch sich eine Abweichung zwischen den beiden Werten und CloudCenter ordnungsgemäß abmelden kann. Diese Erweiterung kann hier nachverfolgt werden https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752.

Die einzige Lösung besteht darin, die Diskrepanz zu beseitigen. An drei Stellen müssen die Timeoutwerte übereinstimmen. Die ersten beiden befinden sich im CCM selbst.

1. Navigieren Sie zu **/usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml**.
2. Ändern Sie die **<session-timeout>time_In_Minutes</session-timeout>**, um die gewünschte Zeitüberschreitung in Minuten wiederzugeben.
3. Navigieren Sie zu **/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties**.
4. Ändern Sie **saml.maxAuthenticationAge.seconds=timeout_in_seconds**, um das gewünschte Timeout in Sekunden wiederzugeben.

Die dritte betrifft den SSO-Server, und der Speicherort kann variieren, je nachdem, welcher SSO-Servertyp ausgeführt wird. Der Lebensdauerwert der Web-SSO muss mit den beiden in CloudCenter konfigurierten Werten übereinstimmen.

Wenn alle drei Übereinstimmungen übereinstimmen und die Zeitüberschreitung aufgetreten ist, werden Sie zum Anmeldungsbildschirm zurückgesetzt, bevor Sie die Anzeige der Seite zulassen können.