"HTTP-status 401 - verificatie is mislukt: Fout bij valideren SAML-bericht" bij gebruik van SSO

Inhoud

Inleiding

Dit document beschrijft een probleem waarin u een foutbericht "HTTP-status 401" ontvangt na een periode van inactiviteit wanneer u Single aanmelding (SSO) gebruikt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

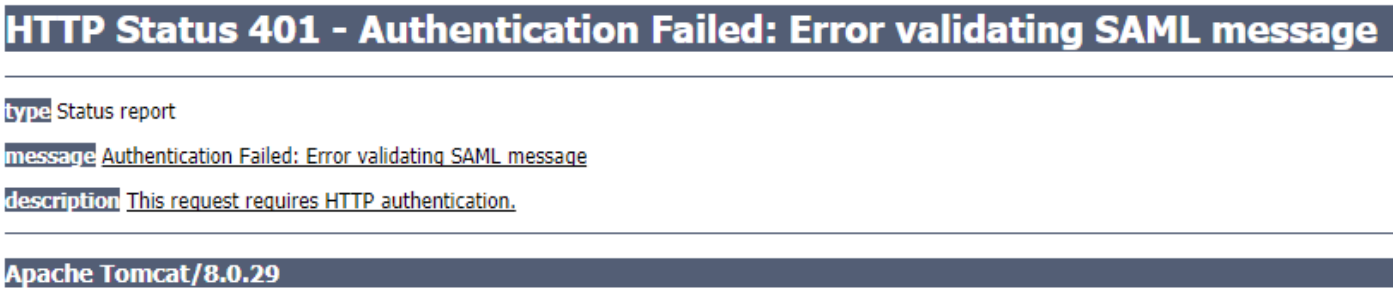
Gebruikte componenten

Dit document is niet beperkt tot specifieke software- of hardwareversies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Probleem

Wanneer u SSO gebruikt, kunt u een "401"-fout ontvangen na een periode van inactiviteit, in plaats van een melding om opnieuw in te loggen zoals in de afbeelding.



De enige manier waarop u opnieuw kunt inloggen is het sluiten van de hele webbrowser en het opnieuw openen.

Oplossing

Dit wordt veroorzaakt door een foutieve combinaties in de time-out waarden tussen CloudCenter en de SSO-server.

Een verbetering staat de steun van de parameters ForceAuthn toe, die een mismatch tussen de twee waarden en CloudCenter om elegant uit te loggen kan toestaan. Deze verbetering kan hier https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752 worden gevolgd.

De enige manier om dit te doen is door de verkeerde combinaties te verwijderen. Er zijn drie locaties waar de timeout waarden moeten matchen. De eerste twee zijn op het CCM zelf.

1. Navigeer naar **/usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml**.
2. Wijzig de **<sessie-timeout>time_in_Minutes</sessie-timeout>** om de gewenste tijd in minuten weer te geven.
3. Navigeer naar **/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties**.
4. Wijzig de **saml.maxAuthenticationAge.seconden=timeout_in_seconden** om de time-out te laten zien die in seconden gewenst is.

Het derde is op de SSO-server en de locatie kan variëren, afhankelijk van het type SSO-server dat wordt uitgevoerd. De levensduur van web SSO moet overeenkomen met de twee waarden die in CloudCenter zijn ingesteld.

Zodra alle drie de partijen, wanneer de tijdelijke versie is opgetreden, wordt u teruggebracht naar het inlogscherm voordat u de pagina kunt bekijken.