“Estatus 401 HTTP - Autenticación fallada: Error que valida SAML el mensaje” cuando usted utiliza el SSO

Contenido

Introducción

Este documento describe un problema donde usted recibe “un mensaje de error del estatus el 401" HTTP después de un período de inactividad en que usted utiliza solo Muestra-en (SSO).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- SSO
- Servicio de la federación del Active Directory (AD FS)
- CloudCenter

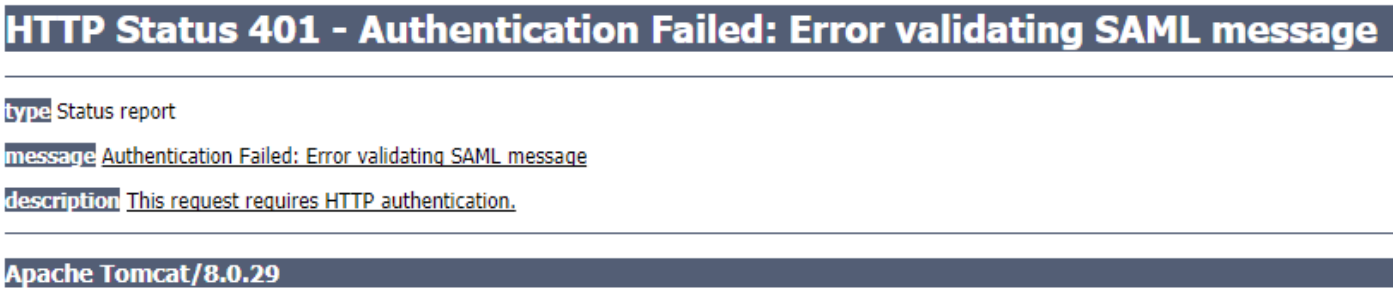
Componentes Utilizados

Este documento no se limita a una versión específica de software o de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

Cuando usted utiliza el SSO, usted puede recibir un error del "401" después de un período de inactividad, en vez de un prompt para iniciar sesión otra vez tal y como se muestra en de la imagen.



La única forma para que usted pueda iniciar sesión otra vez es cerrar al buscador Web entero y abrirlo de nuevo.

Solución

Esto es causada por una discordancía en los valores de agotamiento del tiempo entre CloudCenter y el servidor SSO.

Una mejora permite el soporte de los parámetros de ForceAuthn, que puede permitir que una discordancía entre los dos valores y CloudCenter termine la sesión agraciado. Esta mejora puede ser aquí seguido https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752.

La única solución alternativa es quitar la discordancía. Hay tres ubicaciones en donde los valores de agotamiento del tiempo necesitan hacer juego. Los primeros dos están en CCM sí mismo.

1. Navegue a **/usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml**.
2. Modifique el **<session-timeout>time_In_Minutes</session-timeout>** para reflejar el descanso deseado en los minutos.
3. Navegue a **/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties**.
4. Modifique el **saml.maxAuthenticationAge.seconds=timeout_in_seconds para reflejar el descanso deseado en los** segundos.

El tercero está en el servidor SSO y la ubicación puede variar que depende de qué tipo de servidor SSO se está ejecutando. El valor del curso de la vida de la red SSO debe hacer juego los dos valores configurados en CloudCenter.

Una vez que la coincidencia tres, cuando ha ocurrido el descanso, usted se cae de nuevo a la pantalla de inicio de sesión antes de permitido ver la página.