« État 401 de HTTP - Échec de l'authentification : Erreur validant le message SAML » quand vous utilisez SSO

Contenu

Introduction

Ce document décrit une question où vous recevez « un message d'erreur de l'état 401" de HTTP après une période d'inactivité où vous utilisez l'ouverture de session simple (SSO).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SSO
- Service de fédération de Répertoire actif (AD FS)
- CloudCenter

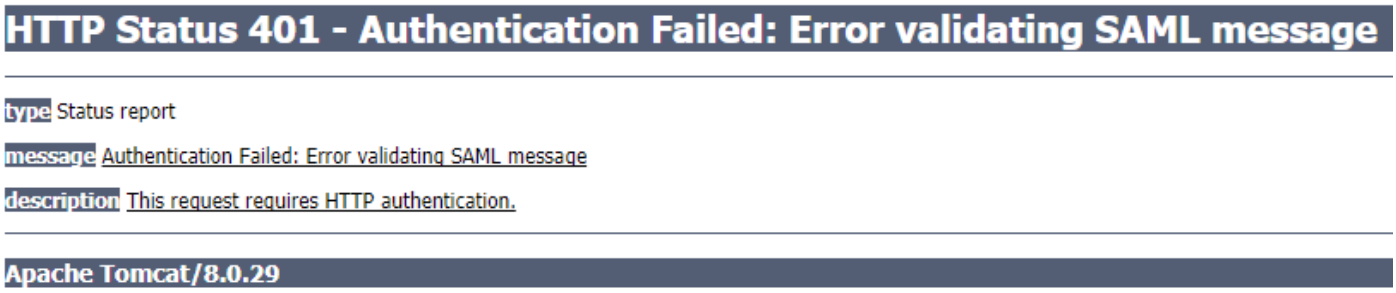
Composants utilisés

Ce document n'est pas limité à des versions de matériel ou de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème

Quand vous utilisez SSO, vous pouvez recevoir une erreur de "401" après une période d'inactivité, au lieu d'une demande pour ouvrir une session de nouveau suivant les indications de l'image.



La seule manière pour que vous puissiez ouvrir une session de nouveau est de fermer le navigateur Web entier et de le rouvrir.

Solution

Ceci est provoqué par par une non-concordance en valeurs du dépassement de durée entre CloudCenter et le serveur SSO.

Une amélioration permet le support de paramètres de ForceAuthn, qui peut permettre à une non-concordance entre les deux valeurs et CloudCenter pour se déconnecter avec élégance. Cette amélioration peut être ici dépisté https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752.

Le seul contournement est de retirer la non-concordance. Il y a trois emplacements où les valeurs du dépassement de durée doivent s'assortir. Les deux premiers sont sur le CCM lui-même.

1. Naviguez vers **/usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml**.
2. Modifiez le **<session-timeout>time_In_Minutes</session-timeout>** pour refléter le délai d'attente désiré en quelques minutes.
3. Naviguez vers **/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties**.
4. Modifiez le **saml.maxAuthenticationAge.seconds=timeout_in_seconds pour refléter le délai d'attente désiré en quelques** secondes.

Le tiers est sur le serveur SSO et l'emplacement peut varier qui dépend de quel type de serveur SSO s'exécute. La valeur de vie du Web SSO doit apparier les deux valeurs configurées sur CloudCenter.

Une fois chacune des correspondance trois, quand le délai d'attente s'est produit, vous êtes lâché de nouveau à l'écran de connexion avant laissé visualiser la page.