«État HTTP 401 - Échec de l'authentification : Erreur lors de la validation du message SAML lorsque vous utilisez SSO

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Problème](#)
[Solution](#)

Introduction

Ce document décrit un problème dans lequel vous recevez un message d'erreur « HTTP Status 401 » après une période d'inactivité lorsque vous utilisez l'authentification unique (SSO).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- SSO
- Service de fédération Active Directory (AD FS)
- CloudCenter

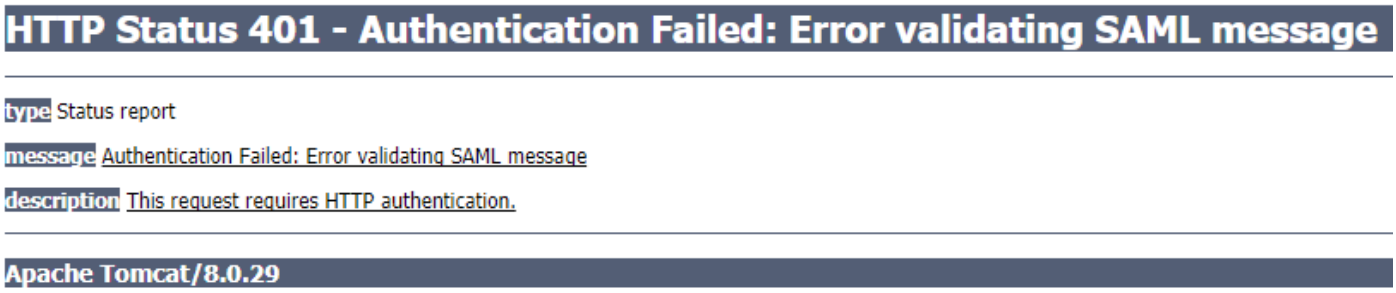
Components Used

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problème

Lorsque vous utilisez SSO, vous pouvez recevoir une erreur « 401 » après une période d'inactivité, au lieu d'une invite à vous reconnecter comme indiqué dans l'image.



La seule façon pour vous de pouvoir vous reconnecter est de fermer l'intégralité du navigateur Web et de le rouvrir.

Solution

Ceci est dû à une non-correspondance des valeurs de délai d'attente entre CloudCenter et le serveur SSO.

Une amélioration permet la prise en charge des paramètres ForceAuthn, ce qui peut permettre une non-correspondance entre les deux valeurs et CloudCenter de se déconnecter avec grâce. Cette amélioration peut être suivie ici https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752.

La seule solution consiste à supprimer la non-correspondance. Les valeurs de délai d'attente doivent correspondre à trois emplacements. Les deux premiers sont sur le CCM lui-même.

1. Accédez à **/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 souhaité en minutes.
3. Accédez à **/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties**.
4. Modifiez le **fichier saml.maxAuthenticationAge.seconds=timeout_in_seconds** pour refléter le délai d'attente souhaité en secondes.

La troisième se trouve sur le serveur SSO et l'emplacement peut varier en fonction du type de serveur SSO en cours d'exécution. La valeur de durée de vie du SSO Web doit correspondre aux deux valeurs configurées sur CloudCenter.

Une fois que les trois correspondances ont eu lieu, lorsque le délai d'attente a expiré, vous êtes renvoyé à l'écran de connexion avant d'être autorisé à afficher la page.