Visualizzazione del messaggio di errore "HTTP Status 401 - Authentication Failed: Error validating SAML Message" quando si usa SSO

Sommario

Introduzione

In questo documento viene descritto un problema in cui viene visualizzato il messaggio di errore "HTTP Status 401" dopo un periodo di inattività durante il quale viene utilizzato Single Sign-On (SSO).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SSO
- ADFS (Active Directory Federation Service)
- CloudCenter

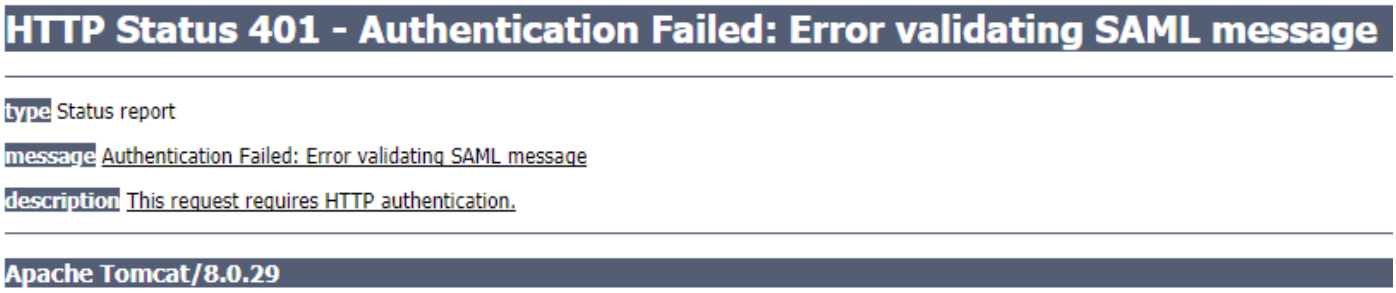
Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Quando si utilizza SSO, è possibile ricevere un errore "401" dopo un periodo di inattività, invece di una richiesta di accesso successivo, come mostrato nell'immagine.



L'unico modo per poter accedere di nuovo è chiudere l'intero browser Web e riaprirlo.

Soluzione

Ciò è causato da una mancata corrispondenza nei valori di timeout tra CloudCenter e il server SSO.

Un miglioramento consente il supporto di ForceAuthn Parameters, che può consentire una mancata corrispondenza tra i due valori e CloudCenter di disconnettersi normalmente. Per informazioni su questo miglioramento, visitare il sito https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvg36752.

L'unica soluzione è rimuovere la mancata corrispondenza. I valori di timeout devono corrispondere in tre posizioni. I primi due sono sulla stessa CCM.

1. Passare a **/usr/local/tomcat/webapps/ROOT/WEB-INF/web.xml**.
2. Modificare il valore di **<session-timeout>time_In_Minutes</session-timeout>** in modo che rifletta il timeout desiderato in minuti.
3. Passare a **/usr/local/tomcat/webapps/ROOT/WEB-INF/mgmt.properties**.
4. Modificare **saml.maxAuthenticationAge.seconds=timeout_in_seconds** in modo che rifletta il timeout desiderato in secondi.

La terza si trova sul server SSO e la posizione può variare a seconda del tipo di server SSO in esecuzione. Il valore della durata dell'SSO Web deve corrispondere ai due valori configurati in CloudCenter.

Una volta che tutte e tre le corrispondenze, quando si è verificato il timeout, si torna alla schermata di accesso prima di poter visualizzare la pagina.