SAML SSO voor Jabber-clients Configuratievoorbeeld inschakelen

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco Jabber-clients en de Infrastructuur servers voor Security Association Markup Language (SAML) Single Sign-on (SSO) dient te configureren.

Voorwaarden

Infrastructuurservers zoals Cisco Unified Communications Manager (CUCM) IM and Presence, Cisco Unity Connection (UCXN) en CUCM moeten worden provisioneerd voor Jabber-gebruikers en de basisconfiguratie van Jabber-clients moeten zijn geïnstalleerd.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM IM and Presence versie 10.5(1) of hoger
- UCXN versie 10.5(1) of hoger
- CUCM 10.5(1) of hoger
- Cisco Jabber Client versie 10.5

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

Configureren

Netwerkdiagram

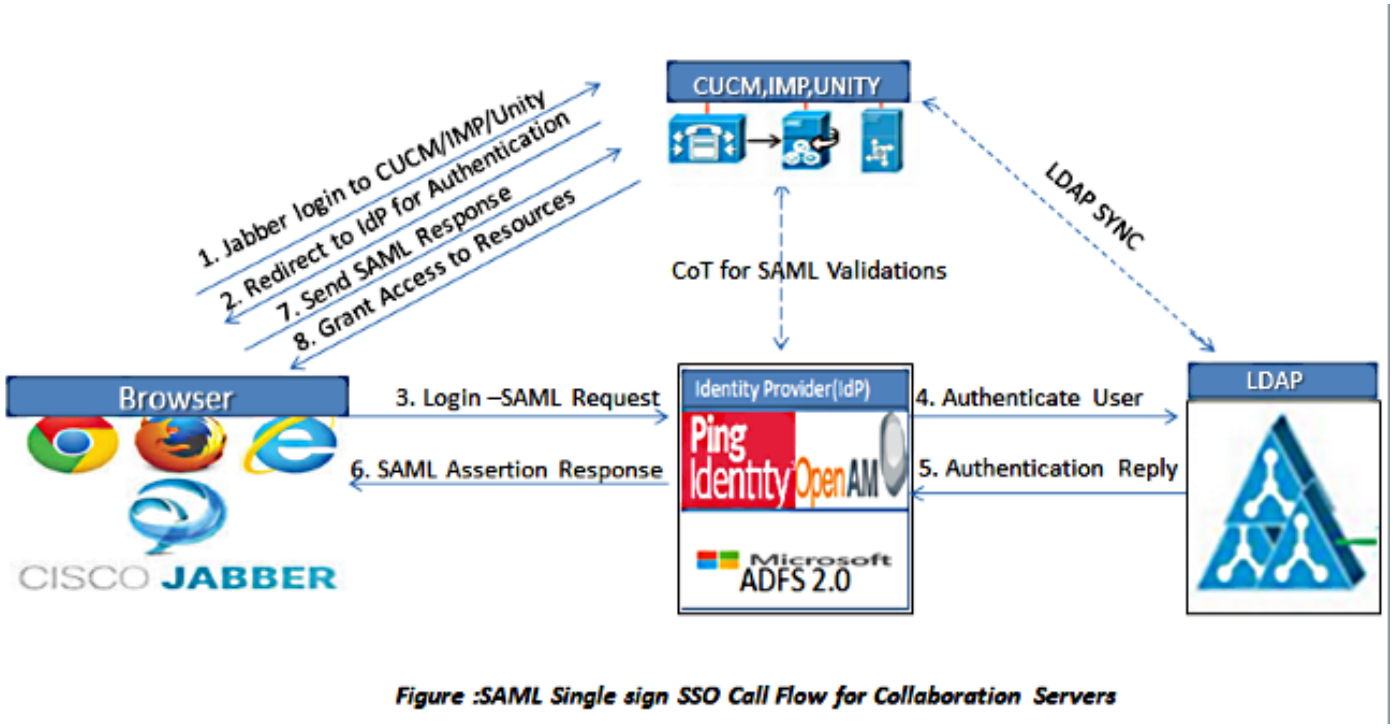

Figure :SAML Single sign SSO Call Flow for Collaboration Servers

1. het implementeren van certificaten voor alle servers zodat het certificaat kan worden gevalideerd door een webbrowser; anders ontvangen gebruikers waarschuwingsberichten over ongeldige certificaten. Raadpleeg voor meer informatie over certificatie de certificaatvalidatie.

2. Zorgen voor servicedetectie van SAML SSO in de client. De klant gebruikt de standaardservicedetectie om de SAML SSO in de client mogelijk te maken. Detectie van service met deze configuratieparameters inschakelen: **ServicesDomain**, **VoiceServicesDomain**, en **ServiceDiscovery-services** waren **uitgesloten**.

   Raadpleeg voor meer informatie over het inschakelen van servicedetectie hoe de klant de services lokaliseert.

3. Raadpleeg het voorbeeld van Unified Communications Manager, versie 10.5 van SAML SLB, om Jabber in staat te stellen SSO voor telefoonservices te gebruiken.

4. Raadpleeg het voorbeeld van Unified Communications Manager, versie 10.5 van SAML SSO-configuratie om Jabber in staat te stellen SSO voor IM-functies te gebruiken.

5. Raadpleeg Unity Connection versie 10.5 SAML SSO Configuration Voorbeeld om Jabber in te schakelen van SSO voor voicemail.

6. Raadpleeg SAML SSO Setup met Kerberos-verificatievoorbeeld om de clientmachine voor automatische aanmelding te configureren (alleen Jabber voor Windows)

7. Nadat SSO op CUCM en IMP is ingeschakeld, tekenen alle Jabber-gebruikers standaard in bij SSO. Beheerders kunnen dit per gebruiker wijzigen, zodat bepaalde gebruikers geen SSO gebruiken en in plaats daarvan met hun Jabber-gebruikersnamen en -wachtwoorden intekenen. Om SSO voor een Jabber-gebruiker uit te schakelen, stelt u de waarde van de SSO_Enabled parameter in op **FALSE**.

   Als u Jabber hebt ingesteld om gebruikers niet naar hun e-mailadres te vragen, dan is hun eerste inloggen bij Jabber mogelijk niet-SSO. Bij sommige implementaties moet de parameter ServicesDomainSsoEmailPrompt op **ON** worden ingesteld. Dit waarborgt dat Jabber over de informatie beschikt die vereist is om een SSO-teken voor het eerst uit te voeren. Als gebruikers zich eerder aan Jabber hebben aangemeld, hoeft deze melding niet te worden gebruikt omdat de benodigde informatie beschikbaar is.

Verifiëren

Wanneer Jabber voor Windows is gestart, dient u automatisch in te loggen zonder te vragen of er voldoende aanmeldingsgegevens of hulpstukken aanwezig zijn. Voor andere Jabber-clients wordt u slechts één keer gevraagd naar aanmeldingsgegevens.

Problemen oplossen

Als u een probleem tegenkomt, verzamelt u een Jabber Problemen rapport en neemt u contact op met Cisco Technical Assistance Center (TAC).