SAML SSO installé avec l'exemple de configuration d'authentification Kerberos

Contenu

Introduction

Ce document décrit comment configurer la version 2.0 active de service de fédération de répertoire et de répertoire d'Active (AD FS) afin de lui permettre d'utiliser l'authentification Kerberos par des clients de Jabber (Microsoft Windows seulement), qui permet à des utilisateurs pour ouvrir une session avec leur connexion de Microsoft Windows et pour ne pas être incitée pour des qualifications.

> **Attention** : Ce document est basé sur un environnement de travaux pratiques et suppose que vous vous rendez compte de l'incidence des modifications que vous apportez. Référez-vous à la documentation du produit appropriée afin de comprendre l'incidence des modifications que vous apportez.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez :

- Version 2.0 FS d'AD installée et configurée avec des Produits de Cisco Collaboration en tant que confiance comptante d'interlocuteur
- Les Produits de Collaboration tels que Cisco Unified Communications Manager (CUCM) IM et présence, Cisco Unity Connection (UCXN), et CUCM ont activé afin d'utiliser l'ouverture de

session simple du Langage SAML (SAML) (SSO)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Répertoire actif 2008 (adresse Internet : ADFS1.ciscolive.com)
- Version 2.0 (adresse Internet FS d'AD : ADFS1.ciscolive.com)
- CUCM (adresse Internet : CUCM1.ciscolive.com)
- Version 10 de Microsoft Internet Explorer
- Version 34 de Mozilla Firefox
- Version 4 de violoneur de Telerik

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.

Configurez

Configurez l'AD FS

1. Configurez la version 2.0 FS d'AD avec le nom principal de service (SPN) afin d'activer l'ordinateur client sur lequel le Jabber est installé pour demander des tickets, qui permet consécutivement à l'ordinateur client de communiquer avec un service FS d'AD.

   Référez-vous à l'AD FS 2.0 : Comment configurer le SPN (servicePrincipalName) pour le service expliquez plus d'informations.

2. Assurez-vous que la configuration d'authentification par défaut pour le service FS d'AD (dans **C:\inetpub\adfs\ls\web.config**) est **authentification intégrée de Windows**. Assurez-vous qu'il n'a pas été changé à l'**authentification forme Forme**.

3. **Paramètres avancés** choisis d'**authentification** et de clic de **Windows** sous le volet de droite. Dans les paramètres avancés, décochez l'**authentification de mode noyau d'enable**, s'assurent que la protection étendue est éteinte, et cliquent sur OK.

4. Assurez-vous que la version 2.0 FS d'AD prend en charge le protocole de Kerberos et le protocole du LAN Manager NT (NTLM) parce que tous les clients de Non-Windows ne peuvent pas utiliser le Kerberos et compter sur NTLM.

Dans le volet de droite, les **fournisseurs** choisis et s'assurent que **négocier** et **NTLM** sont présents sous les fournisseurs activés :

Note: L'AD FS passe l'en-tête de Sécurité de négociation quand l'authentification intégrée de Windows est utilisée afin d'authentifier des demandes de client. L'en-tête de Sécurité de négociation permet des clients choisis entre l'authentification Kerberos et l'authentification NTLM. Le processus de négociation sélectionne l'authentification Kerberos à moins qu'une de ces conditions soit vraie :

- Un des systèmes qui est impliqué dans l'authentification ne peut pas utiliser l'authentification Kerberos.

- L'application appelante ne fournit pas des informations suffisantes pour utiliser l'authentification Kerberos.

- Afin de permettre au processus de négociation de sélectionner le protocole de Kerberos pour l'authentification de réseau, l'application cliente doit fournir un SPN, un nom principal d'utilisateur (UPN), ou un nom du compte de Basic Input/Output System de réseau (Netbios) comme nom cible. Autrement, le processus de négociation sélectionne toujours le protocole NTLM comme méthode d'authentification préférée.

Configurez le navigateur

Microsoft Internet Explorer

1. Assurez-vous que l'**Internet Explorer > a avancé > authentification de Windows intégrée par enable** est vérifié.

2. Ajoutez l'URL FS d'AD sous des **zones >** des **sites de >Intranet de Sécurité**.

3. Ajoutez le CUCM, le PIM, et les adresses Internet d'Unity aux **sites >Trusted par Sécurité**.

4. Assurez-vous qu'**Internet Exporer > Sécurité > intranet local > paramètres de sécurité >** authentification de l'utilisateur **- la connexion** est configurée afin d'utiliser les qualifications ouvertes une session pour des sites d'intranet.

Mozilla Firefox

1. Ouvrez Firefox et entrez **environ : config** dans la barre d'adresses.

2. Le clic **I fera attention, je promets !**

3. Double-cliquer le nom **network.negotiate-auth.allow-non-fqdn pour rectifier et network.negotiate-auth.trusted-uris de** préférence à **ciscolive.com,adfs1.ciscolive.com dans la commande** à modifier.

4. Clôturez Firefox et rouvrez.

Vérifiez

Afin de vérifier que le SPNs pour le serveur FS d'AD sont correctement créés, sélectionnez la commande de **setspn** et visualisez la sortie.

Vérifiez si les machines cliente ont des tickets Kerberos :

Terminez-vous ces étapes afin de vérifier qui l'authentification (Kerberos ou authentification NTLM) est en service.

1. Téléchargez l'outil de violoneur à votre machine cliente et installez-le.

2. Fermez toutes les fenêtres de Microsoft Internet Explorer.

3. Exécutez l'outil de violoneur et vérifiez que l'option du **trafic de capture** est activée sous le menu File. Le violoneur travaille comme proxy d'intercommunication entre la machine cliente et le serveur et écoute tout le trafic.

4. Ouvrez Microsoft Internet Explorer, parcourez dans votre CUCM, et cliquez sur quelques liens afin de générer le trafic.

5. Renvoyez à la fenêtre principale de violoneur et choisissez une des vues où le résultat est **200** (succès) et vous pouvez voir le Kerberos comme mécanisme d'authentification

6. Si le type d'authentification est NTLM, alors vous voyez **pour négocier - NTLMSSP** au début de la trame, comme affiché ici.

Dépannez

Si toutes les étapes de configuration et de vérification sont terminées comme décrit dans ces document et vous ayez toujours les questions de procédure de connexion, alors vous devez consulter un Répertoire actif de Microsoft Windows/l'administrateur FS d'AD.