Kerberos avec ADFS 2.0 pour l'utilisateur final SAML SSO pour l'exemple de configuration de Jabber

Contenu

Introduction

Ce document décrit comment configurer le Kerberos avec les services de fédération de Répertoire actif (ADFS) 2.0.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et 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.

Informations générales

L'utilisateur final que le Langage SAML (SAML) simple se connectent la configuration (SSO) exige du Kerberos pour être configuré afin de permettre à l'utilisateur final SAML SSO pour que le Jabber fonctionne avec l'authentification de domaine. Quand SAML SSO est mis en application avec le Kerberos, le Protocole LDAP (Lightweight Directory Access Protocol) manipule toute la synchronisation d'autorisation et d'utilisateur, alors que le Kerberos gère l'authentification. Le Kerberos est un protocole d'authentification qui est censé pour être utilisé en même temps qu'un exemple LDAP-activé.

Sur les ordinateurs de Microsoft Windows et de Macintosh qui sont joints à un domaine de Répertoire actif, les utilisateurs peuvent sans faille se connecter dans le Cisco Jabber sans condition requise d'écrire un nom d'utilisateur ou mot de passe et ils ne voient pas même un écran de connexion. Les utilisateurs qui ne sont toujours pas connectés dans le domaine sur leurs ordinateurs voient une forme standard de procédure de connexion.

Puisque l'authentification utilise un jeton simple passé des systèmes d'exploitation, aucun réorientez est exigé. Le jeton est vérifié contre le contrôleur de domaine principal configuré (KDC), et s'il est valide, l'utilisateur est ouvert une session.

Configuration

Voici la procédure pour configurer le Kerberos avec ADFS 2.0.

1. Installez la Microsoft Windows Server 2008 R2 sur un ordinateur.

2. Installez les services de domaine de Répertoire actif (AJOUTE) et l'ADFS sur la même chose ordinateur.

3. Installez l'Internet Information Services (IIS) sur l'ordinateur de la Microsoft Windows Server 2008 R2-installed.

4. Créez un certificat auto-signé pour IIS.

5. Importez le certificat auto-signé dans IIS et utilisez-le comme le certificat de serveur HTTPS.

6. Installez Microsoft Windows7 sur un autre ordinateur et utilisez-le en tant que client.

   Changez le Domain Name Server (DN) à l'ordinateur où vous avez installé AJOUTE.

   Ajoutez cet ordinateur au domaine que vous avez créé à l'installation ADDS.

   Allez au **début**.**Ordinateur de** clic droit.Cliquez sur **Properties**.Cliquez sur les **configurations de modification du** côté droit de la fenêtre.Cliquez sur l'onglet **Computer Name**.Cliquez sur **Change**.Ajoutez le domaine que vous avez créé.

7. Vérifiez si le service de Kerberos se produit sur les deux ordinateurs.

Ouvrez une session comme administrateur sur l'ordinateur hôte et ouvrez l'invite de commande. Exécutez alors ces commandes :

cd \windows\System32Tickets de Klist

Ouvrez une session comme utilisateur de domaine sur la machine cliente et exécutez les mêmes commandes.

8. Créez l'identité de Kerberos ADFS sur l'ordinateur où vous avez installé AJOUTE.

   L'administrateur de Microsoft Windows connecté dans le domaine de Microsoft Windows (comme <domainname> \ administrateur), par exemple sur le contrôleur de domaine de Microsoft Windows, crée l'identité de Kerberos ADFS. Le service HTTP ADFS doit avoir une identité de Kerberos appelée un nom principal de service (SPN) dans ce format : HTTP/DNS_name_of_ADFS_server.

   Ce nom doit être tracé à l'utilisateur de Répertoire actif qui représente l'exemple de serveur HTTP ADFS. Utilisez l'utilitaire de setspn de Microsoft Windows, qui devrait être disponible par défaut sur un serveur de Microsoft Windows 2008.

   Procédure Enregistrez le SPNs pour le serveur ADFS. Sur le contrôleur de domaine de Répertoire actif, exécutez la commande de setspn.

   Par exemple, quand l'hôte ADFS est adfs01.us.renovations.com, et le domaine de Répertoire actif est US.RENOVATIONS.COM, la commande est :

   ```
   setspn -a HTTP/adfs01.us.renovations.com <ActiveDirectory user>
   setspn -a HTTP/adfs01 <ActiveDirectory user>
   ```

   La partie HTTP du SPN s'applique, quoique le serveur ADFS soit typiquement accédé à par Secure Sockets Layer (SSL), qui est HTTPS.

   Vérifiez que le SPNs pour le serveur ADFS sont correctement créés avec la commande de setspn et visualisez la sortie.

   ```
   setspn -L <ActiveDirectory user>
   ```

9. Configurez les configurations du navigateur du client de Microsoft Windows.

   Naviguez vers des outils > InternetOptions > a avancé afin d'activer l'authentification intégrée de Windows.

Cochez la **case d'authentification de Windows intégrée par enable** :

Naviguez vers des **outils > des options Internet > la Sécurité > intranet local > niveau fait sur commande…** afin de sélectionner la **connexion automatique seulement dans la zone d'intranet**.

Naviguez vers des **outils > des options Internet > la Sécurité > intranet local > sites > a avancé** afin d'ajouter l'URL de détection et de prévention d'intrusion (IDP) aux sites locaux d'intranet.

Remarque: Cochez toutes les cases dans la boîte de dialogue locale d'intranet et cliquez sur l'**onglet Avancé.**

Naviguez vers des **outils > la Sécurité > a fait confiance à des sites > à des sites** afin d'ajouter les adresses Internet CUCM aux sites de confiance :

Vérifiez

Cette section explique comment vérifier que l'authentification (Kerberos ou authentification du LAN Manager de NT (NTLM)) est utilisé.

1. Téléchargez l'outil de violoneur à votre machine cliente et installez-le.
2. Fermez toutes les fenêtres d'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, qui place temporairement vos configurations d'Internet Explorer comme ceci :

4. Ouvrez l'Internet Explorer, parcourez dans votre URL de serveur de gestion de la relation client (CRM), 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) :

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

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.