SAML SSO puesto con el ejemplo de configuración de la autenticación de Kerberos

Contenido

Introducción

Este documento describe cómo configurar la versión 2.0 del servicio del Active Directory y de la federación del Active Directory (AD FS) para permitirle para utilizar la autenticación de Kerberos de los clientes del Jabber (Microsoft Windows solamente), que permite que los usuarios inicien sesión con su inicio de Microsoft Windows y que no sean indicados para las credenciales.

> Precaución: Este documento se basa en un ambiente de laboratorio y asume que usted es consciente del impacto de los cambios que usted realiza. Refiera a la Documentación del Producto relevante para entender el impacto de los cambios que usted realiza.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene:

- Versión 2.0 AD FS instalada y configurada con los Productos de la colaboración de Cisco como confianza de confianza del partido
- Los Productos de la Colaboración tales como administrador de las Comunicaciones unificadas de Cisco (CUCM) IM y presencia, el Cisco Unity Connection (UCXN), y CUCM habilitado para utilizar el lenguaje de marcado de la aserción de la Seguridad (SAML)

escogen Muestra-en (el SSO)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Active Directory 2008 (nombre de host: ADFS1.ciscolive.com)
- Versión 2.0 (nombre de host AD FS: ADFS1.ciscolive.com)
- CUCM (nombre de host: CUCM1.ciscolive.com)
- Versión de Microsoft Internet Explorer 10
- Versión 34 de Firefox del Mozilla
- Versión 4 del Fiddler de Telerik

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Configuración AD FS

1. Configure la versión 2.0 AD FS con el nombre principal del servicio (SPN) para habilitar la computadora cliente en la cual el Jabber está instalado para pedir los boletos, que a su vez permite a la computadora cliente para comunicar con un servicio AD FS.

   Refiera a AD FS 2.0: Cómo configurar el SPN (servicePrincipalName) para el servicio explique más información.

2. Asegúrese de que la configuración de la autenticación predeterminada para el servicio AD FS (en **C:\inetpub\adfs\ls\web.config**) sea **autenticación de Windows integrada**. Asegúrese de que no se haya cambiado a la **autenticación Forma-basada**.

3. Seleccione la **autenticación de Windows** y haga clic las **configuraciones avanzadas** bajo el panel derecho. En las configuraciones avanzadas, desmarque la **autenticación del permiso Corazón-MODE**, aseegurese la protección extendida está apagado, y **AUTORIZACIÓN del** tecleo.

4. Asegúrese de que la versión 2.0 AD FS soporte el protocolo Kerberos y el protocolo del administrador de LAN de NT (NTLM) porque todos los clientes del no Windows no pueden

utilizar el Kerberos y confiar en el NTLM.

En el panel derecho, los **proveedores** selectos y se aseeguran **negociar** y el **NTLM** está presente bajo los proveedores habilitados:

Nota: El AD FS pasa la encabezado de la Seguridad de la negociación cuando la autenticación de Windows integrada se utiliza para autenticar los pedidos de cliente. La encabezado de la Seguridad de la negociación deja a los clientes selectos entre la autenticación de Kerberos y la autenticación NTLM. El proceso de la negociación selecciona la autenticación de Kerberos a menos que una de estas condiciones sea verdad:

- Uno de los sistemas que está implicado en la autenticación no puede utilizar la autenticación de Kerberos.

- La aplicación de llamada no proporciona la información suficiente para utilizar la autenticación de Kerberos.

- Para permitir al proceso de la negociación para seleccionar el protocolo Kerberos para la autenticación de red, la aplicación de cliente debe proporcionar un SPN, un nombre principal del usuario (UPN), o un nombre de la cuenta de Network Basic Input/Output System (NetBios) como el nombre objetivo. Si no, el proceso de la negociación selecciona siempre el protocolo NTLM como el método de autentificación preferido.

Navegador de la configuración

Microsoft Internet Explorer

1. Asegúrese de que el **Internet Explorer > avanzara > autenticación de Windows integrada permiso** esté marcado.

2. Agregue AD FS URL bajo las **zonas >** los **sitios del >Intranet de la Seguridad**.

3. Agregue el CUCM, el IMP, y los nombres de host del Unity a los **sitios >Trusted Seguridad**.

4. Asegúrese de que **>** Security (Seguridad) de **Exporer de Internet >** las **configuraciones >** autenticación de usuario del **>** Security (Seguridad) de la **Local Intranet (Intranet local) - el inicio** se configura para utilizar las credenciales abiertas una sesión para los sitios del intranet.

Mozilla FireFox

1. Abra Firefox y ingrese **alrededor: config** en la barra de dirección.

2. ¡El tecleo **I tendrá cuidado, prometo!**

3. Haga doble clic el nombre **network.negotiate-auth.allow-non-fqdn para verdad y network.negotiate-auth.trusted-uris de la** preferencia a **ciscolive.com,adfs1.ciscolive.com en la orden** a modificarse.

4. Cierre Firefox y abra de nuevo.

Verificación

Para marcar que el SPNs para el servidor AD FS está creado correctamente, ingrese el comando del **setspn** y vea la salida.

Marque si las máquinas del cliente tienen boletos del Kerberos:

Complete estos pasos para verificar que la autenticación (Kerberos o autenticación NTLM) sea funcionando.

1. Descargue la herramienta del Fiddler a su máquina del cliente y instalela.

2. Cierre todas las ventanas de Microsoft Internet Explorer.

3. Funcione con la herramienta del Fiddler y marque que la opción del **tráfico de la captura** está habilitada bajo menú de archivos. El Fiddler trabaja como proxy del paso entre la máquina del cliente y el servidor y escucha todo el tráfico.

4. Abra Microsoft Internet Explorer, hojee en su CUCM, y haga clic algunos links para generar el tráfico.

5. Refiérase de nuevo a la ventana principal del Fiddler y elija uno de los bastidores donde el resultado es **200** (éxito) y usted puede ver el Kerberos como mecanismo de autenticación

6. Si el tipo de autenticación es NTLM, después usted ve **para negociar - NTLMSSP** al principio del bastidor, como se muestra aquí.

Troubleshooting

Si se completan toda la configuración y pasos de verificación como descrito en este documento y usted todavía tenga problemas del login, después usted debe consultar a un administrador del Active Directory/AD FS de Microsoft Windows.