SAML SSO Setup com exemplo de configuração da autenticação de Kerberos

Índice

Introdução

Este documento descreve como configurar a versão 2.0 do serviço do diretório ativo e da federação do diretório ativo (AD FS) a fim permiti-la de usar a autenticação de Kerberos por clientes do Jabber (Microsoft Windows somente), que permite que os usuários entrem com seu fazer logon de Microsoft Windows e não sejam alertados para credenciais.

> Cuidado: Este documento é baseado em um ambiente de laboratório e supõe que você está ciente do impacto das mudanças que você faz. Refira a documentação do produto relevante a fim compreender o impacto das mudanças que você faz.

Pré-requisitos

Requisitos

Cisco recomenda que você tem:

- Versão 2.0 AD FS instalada e configurada com Produtos da colaboração do Cisco como a confiança de confiança do partido
- O Produtos da Colaboração tal como o gerente das comunicações unificadas de Cisco (CUCM) IM e presença, Cisco Unity Connection (UCXN), e CUCM permitido a fim usar o linguagem de marcação da afirmação da Segurança (SAML) escolhe Sinal-em (o SSO)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Diretório ativo 2008 (hostname: ADFS1.ciscolive.com)
- Versão 2.0 AD FS (hostname: ADFS1.ciscolive.com)
- CUCM (hostname: CUCM1.ciscolive.com)
- Versão do Microsoft internet Explorer 10
- Versão 34 de Mozilla Firefox
- Versão 4 do violinista de Telerik

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Configurar AD FS

1. Configurar a versão 2.0 AD FS com nome principal do serviço (SPN) a fim permitir o computador de cliente em que o Jabber é instalado para pedir bilhetes, que permite por sua vez o computador de cliente de se comunicar com um serviço AD FS.

   Refira AD FS 2.0: Como configurar o SPN (servicePrincipalName) para o serviço esclareça mais informação.

2. Assegure-se de que a configuração da autenticação padrão para o serviço AD FS (em **C:\inetpub\adfs\ls\web.config**) seja **autenticação do Windows integrada**. Assegure-se de que não esteja mudada à **autenticação Formulário-baseada**.

3. Selecione a **autenticação do Windows** e clique **ajustes avançados** sob o painel correto. Em ajustes avançados, desmarcar **permitem a autenticação Núcleo-MODE**, certificam-se que a proteção prolongada está, e **APROVAÇÃO do** clique.

4. Assegure-se de que a versão 2.0 AD FS apoie o protocolo Kerberos e o protocolo do gerenciador de LAN de NT (NTLM) porque todos os clientes não-Windows não podem usar o Kerberos e confiar no NTLM.

   No painel correto, os **fornecedores** seletos e certificam-se que **para negociar** e o **NTLM** esta presente sob fornecedores permitidos:

Nota: O AD FS passa o encabeçamento da Segurança do negócio quando a autenticação do Windows integrada é usada a fim autenticar pedidos do cliente. O encabeçamento da Segurança do negócio deixa os clientes seletos entre a autenticação de Kerberos e a autenticação de NTLM. O processo do negócio seleciona a autenticação de Kerberos a menos que uma destas circunstâncias for verdadeira:

- Um dos sistemas que é envolvido na autenticação não pode usar a autenticação de Kerberos.

- O aplicativo de chamada não fornece a informação suficiente para usar a autenticação de Kerberos.

- A fim permitir o processo do negócio de selecionar o protocolo Kerberos para a autenticação de rede, o aplicativo do cliente deve fornecer um SPN, um nome principal do usuário (UPN), ou um nome da conta de Network Basic Input/Output System (NetBIOS) como o nome de destino. Se não, o processo do negócio seleciona sempre o protocolo NTLM como o método de autenticação preferido.

Configurar o navegador

Microsoft Internet explorer

1. Assegure-se de que o **internet explorer > avance > permita a autenticação do Windows integrada** esteja verificado.

2. Adicionar AD FS URL sob **zonas > locais do >Intranet da Segurança**.

3. Adicionar o CUCM, o IMP, e os nomes de host do Unity aos **locais >Trusted Segurança**.

4. Assegure-se de que > segurança de **Exporer do Internet** > de > segurança do **intranet local ajustes** > autenticação de usuário **- o fazer logon** é configurado a fim usar as credenciais entradas para locais do intranet.

Mozilla Firefox

1. Abra Firefox e entre-o **aproximadamente: configuração na** barra de endereços.

2. Clique **eu serei cuidadoso, eu prometo!**

3. Fazer duplo clique o nome **network.negotiate-auth.allow-non-fqdn para retificar e network.negotiate-auth.trusted-uris da** preferência a **ciscolive.com,adfs1.ciscolive.com em ordem** a alterar.

4. Feche Firefox e reabra-o.

Verificar

A fim certificar-se do SPNs para o server AD FS esteja criado corretamente, incorpore o comando do **setspn** e veja a saída.

Verifique se as máquinas cliente têm bilhetes do Kerberos:

Termine estas etapas a fim verificar que autenticação (Kerberos ou autenticação de NTLM) é no uso.

1. Transfira a ferramenta do violinista a sua máquina cliente e instale-a.

2. Feche todos os indicadores do Microsoft Internet explorer.

3. Execute a ferramenta do violinista e certifique-se da opção do **tráfego da captação** esteja permitida sob o menu de arquivo. O violinista trabalha como a passagem-através do proxy entre a máquina cliente e o server e escuta todo o tráfego.

4. Abra o Microsoft Internet explorer, consulte em seu CUCM, e clique alguns links a fim gerar o tráfego.

5. Consulte de volta à janela principal do violinista e escolha um dos quadros onde o resultado é **200** (sucesso) e você pode ver o Kerberos como o mecanismo da autenticação

6. Se o tipo do autenticação é NTLM, a seguir você vê **para negociar - NTLMSSP** no início do quadro, como mostrado aqui.

Troubleshooting

Se toda a configuração e passos de verificação estão terminados como descrito neste documento e você ainda tem edições do início de uma sessão, a seguir você deve consultar um administrador do diretório ativo de Microsoft Windows/AD FS.