Kerberos com ADFS 2.0 para o utilizador final SAML SSO para o exemplo de configuração do Jabber

Índice

Introdução

Este documento descreve como configurar o Kerberos com serviços da federação do diretório ativo (ADFS) 2.0.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Informações de Apoio

Sinal do linguagem de marcação da afirmação da Segurança do utilizador final o único (SAML) na configuração (SSO) exige o Kerberos ser configurado a fim permitir que o utilizador final SAML SSO para que o Jabber trabalhe com autenticação do domínio. Quando SAML SSO é executado com Kerberos, o Lightweight Directory Access Protocol (LDAP) segura toda a sincronização da autorização e do usuário, quando o Kerberos controlar a autenticação. O Kerberos é um protocolo de autenticação que seja significado ser usado conjuntamente com um exemplo LDAP-permitido.

Nas máquinas de Microsoft Windows e de Macintosh que são juntadas a um domínio do diretório ativo, os usuários podem continuamente registrar em Cisco o Jabber sem a exigência incorporar um username ou uma senha e veem nem sequer uma tela de login. Os usuários que não são registrados no domínio em seus computadores ainda veem um formulário padrão do início de uma sessão.

Porque a autenticação usa um único token passado dos sistemas operacionais, nenhuns reoriente é exigido. O token é verificado contra o controlador de domínio chave configurado (KDC), e se é válido, o usuário é entrado.

Configuração

Está aqui o procedimento para configurar o Kerberos com ADFS 2.0.

1. Instale o Microsoft Windows server 2008 R2 em uma máquina.

2. Instale serviços do domínio do diretório ativo (ADICIONA) e ADFS na mesma máquina.

3. Instale o Internet Information Services (IIS) na máquina do Microsoft Windows server 2008 R2-installed.

4. Crie um certificado auto-assinado para o IIS.

5. Importe o certificado auto-assinado no IIS e use-o como o certificado de servidor HTTPS.

6. Instale Microsoft Windows7 em uma outra máquina e use-o como um cliente.

   Mude o Domain Name Server (DNS) à máquina aonde você instalou ADICIONA.

   Adicionar esta máquina ao domínio que você criou na instalação ADDS.

   Vá ao **começo**.Clicar com o botão direito o **computador**.Clique em Propriedades.Clique **ajustes da mudança no** lado direito do indicador.Clique a **aba do nome de computador**.Clique a **mudança**.Adicionar o domínio que você criou.

7. Verifique se o serviço de kerberos gerencia em ambas as máquinas.

   Entre como o administrador na máquina do servidor e abra o comando prompt. Execute então estes comandos:

CD \windows\System32Bilhetes de Klist

Entre como o usuário de domínio na máquina cliente e execute os mesmos comandos.

8. Crie a identidade do Kerberos ADFS na máquina aonde você instalou ADICIONA.

   O administrador de Microsoft Windows registrado no domínio de Microsoft Windows (como o <domainname> \ administrador), por exemplo no controlador de domínio de Microsoft Windows, cria a identidade do Kerberos ADFS. O serviço ADFS HTTP deve ter uma identidade do Kerberos chamada um nome principal do serviço (SPN) neste formato: HTTP/DNS_name_of_ADFS_server.

   Este nome deve ser traçado ao usuário de diretório ativo que representa o exemplo do Server do HTTP ADFS. Use a utilidade do setspn de Microsoft Windows, que deve estar disponível à revelia em um server de Microsoft Windows 2008.

   Procedimento Registrar o SPNs para o server ADFS. No controlador de domínio do diretório ativo, execute o comando do setspn.

   Por exemplo, quando o host ADFS é adfs01.us.renovations.com, e o domínio do diretório ativo é US.RENOVATIONS.COM, o comando é:

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

   A parcela HTTP do SPN aplica-se, mesmo que o server ADFS seja alcançado tipicamente pelo secure sockets layer (SSL), que é HTTPS.

   Certifique-se do SPNs para o server ADFS esteja criado corretamente com o comando do setspn e veja-se a saída.

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

9. Configurar as configurações do navegador do cliente de Microsoft Windows.

   Navegue às ferramentas > ao InternetOptions > avançou a fim permitir a autenticação do Windows integrada.

Verifique a **caixa de verificação integrada possibilidade da autenticação do Windows**:

Navegue às **ferramentas > ao > segurança > ao intranet local > ao costume das opções de internet em nível…** a fim selecionar o **fazer logon automático somente na zona do intranet**.

Navegue às **ferramentas > ao > segurança > ao intranet local > aos locais das opções de internet > avançou** a fim adicionar a intrusion detection & a prevenção (IDP) URL aos locais do intranet local.

Note: Verifique todas as caixas de seleção na caixa de diálogo do intranet local e clique o **guia avançada**.

Navegue ao **ferramentas > segurança > às sites confiável > aos locais** a fim adicionar os nomes de host CUCM às sites confiável:

Verificar

Esta seção explica como verificar que autenticação (Kerberos ou de gerenciador de LAN de NT autenticação (NTLM)) é usado.

1. Transfira a ferramenta do violinista a sua máquina cliente e instale-a.
2. Feche todos os indicadores do 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, que ajusta temporariamente seus ajustes do internet explorer como este:

4. Abra o internet explorer, consulte em seu server URL do gerenciamento de relacionamento com o cliente (CRM), 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):

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

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.