Segurança da Web da nuvem: Configurar ADFS para incluir grupos específicos na altura da autenticação

Índice

Introdução

Este documento descreve como configurar os serviços federados microsoft ative directory (ADFS) como um fornecedor da identidade (IdP), que envia detalhes específicos do grupo ao serviço da Segurança da Web da nuvem de Cisco (o CWs), um pouco do que uma lista completa das membrasias do clube.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de segurança da Web da nuvem com o portal de ScanCenter
- Autenticação do linguagem de marcação da afirmação da Segurança (SAML)
- A administração do server de Microsoft ADFS

Componentes Utilizados

A informação neste documento é baseada na versão 2.0 de Microsoft ADFS, essas corridas em Windows Server 2008 R2.

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

Quando o processo de autenticação entre um navegador cliente ocorrer, o server ADFS (o IdP) e CWs (o provedor de serviços (o SP)), toda a informação é cifrada e adicionada à série de URL no navegador cliente. Isto significa que a série de URL é mais longa quando mais informação é enviada ao CWs.

Quando você configura a autenticação de SAML (com Microsoft ADFS) para o uso com o serviço CWs, você deve configurar uma confiança de confiança do partido para fornecer a informação username e de grupo. Segurança da Web da nuvem: Configurar o usuário/atributos de grupo com PingFederate e ADFS enquanto usando SAML descreve esta etapa com maiores detalhes.

O número de grupos que um usuário é adicionado a aumenta o tamanho URL. Se um usuário pertence a um grande número grupos do diretório ativo (AD), a URL vem um tamanho por meio de que o limite imposto navegador URL é alcançado, e o processo de autenticação falha.

Cada navegador pôde definir seu próprio comprimento reservado máximo URL. O RFC 2616 não especifica um comprimento máximo, mas os limite práticos são impostos por vendedores do navegador.

> Nota: Não é possível definir explicitamente um número máximo de grupos porque um grupo não tem um número fixo de caráteres. Por exemplo, GroupA tem menos caráteres do que Test_Group_A. Para definir um número de grupos que fica abaixo do limite URL depende da contagem de caráter do Domain Name + do nome do grupo.

Configurar

Você pode configurar o server de Microsoft ADFS para incluir grupos específicos no processo de autenticação. Tipicamente você selecionaria somente os grupos usados nas regras de filtragem da Web CWs. Quando você executa uma auditoria das políticas que existem, ajudam a determinar os grupos que são já dentro uso.

Novo e as disposições que já existem deve seguir a configuração do melhor prática que fornece estes benefícios:

- Mantém o tamanho URL a um mínimo
- Acelera o processo de autenticação entre o IdP (ADFS) e o SP (o CWs)
- Salvar a largura de banda em cada pedido de autenticação

Configuração do melhor prática

As confianças do fornecedor das reivindicações abertas e criam dois que a aceitação transforma regras:

O molde da regra da reivindicação do uso envia atributos LDAP como reivindicações

Loja do atributo: AD;

Atributo LDAP: Token-grupos - Nomes incompetentes;

Tipo que parte da reivindicação: Grupo

O molde da regra da reivindicação do uso envia atributos LDAP como reivindicações

Loja do atributo: AD;

Atributo LDAP: SAM-Conta-nome;

Tipo que parte da reivindicação: Nome

Crie a emissão transformam regras abrindo confianças de confiança da parte e criando dois transforme regras:

O uso transforma um molde entrante da reivindicação

Tipo entrante da reivindicação: Nome

Formato: não especificado

Tipo que parte da reivindicação: Nome ID

Formato: Não especificado

Selecione a passagem com todos os valores da reivindicação

Use a transmissão ou filtre uma reivindicação entrante

Tipo entrante da reivindicação: Grupo

Passagem seleta com somente os valores da reivindicação que começam com um valor específico:

Especifique seus nomes do grupo AD

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

- Quando entrado como o utilizador final, consulte a http://whoami.scansafe.net.
- A saída deve alistar somente os grupos especificados no procedimento previamente mencionado, um pouco do que uma lista completa das membrasias do clube.

Troubleshooting

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