Adicionar UID de Atributo Necessário ao Servidor ADFS Manualmente

Contents

Introdução

Este documento descreve como adicionar manualmente um UID de Atributo no objeto de confiança de terceira parte confiável do ADFS usando um síntex.

Pré-requisitos

Requisitos

- servidor ADFS
- Hub de controle

Componentes Utilizados

- servidor ADFS
- Cisco Webex Control Hub
- AD no local

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Isso é útil caso haja um problema ao adicionar uma Declaração de Atributo no ADFS devido a um atributo existente.

Cenário 1

Você tem um objeto de confiança de terceira parte confiável existente que tem uma Regra de declaração criada com o atributo UID ou Uid.

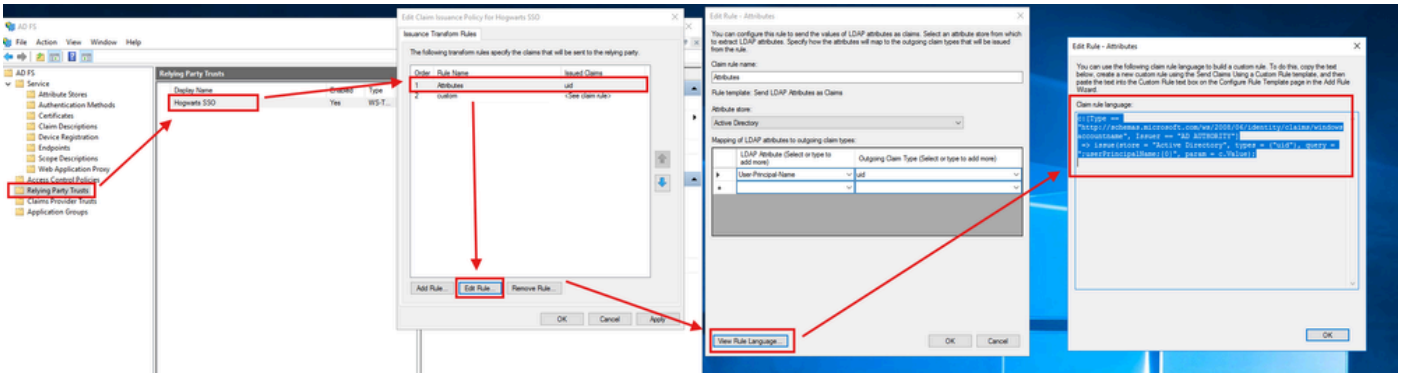
Isso falha na Autenticação, pois o Webex (SP) diferencia maiúsculas de minúsculas sobre o atributo necessário e ele precisa ser uid e deve passar o emailAddress do usuário na resposta SAML.

Cenário 2

Você tem uma confiança da parte que tem uma regra de Declaração passando um atributo chamado uid, mas associado a um atributo diferente no AD do que é necessário (emailAddress/UserPrincipleName). Isso cria problemas.

Configurações

Em uma configuração ideal de acordo com o Guia do Cisco Webex, a configuração do ADFS deve ser semelhante a esta:



Os administradores do ADFS podem visitá-lo de suas Confianças da Terceira Parte Confiável-> Confiança que eles criaram para o Webex -> Editar Política de Emissão de Declaração -> Editar Regra -> Atributos -> Exibir Idioma da Regra.

A linguagem da regra em texto sem formatação é:

c:[Digite == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Emitente == "AUTORIDADE AD"]
=> issue(store = "Ative Diretory", tipos = ("uid"), query = ";userPrincipalName;{0}", param = c.Value);

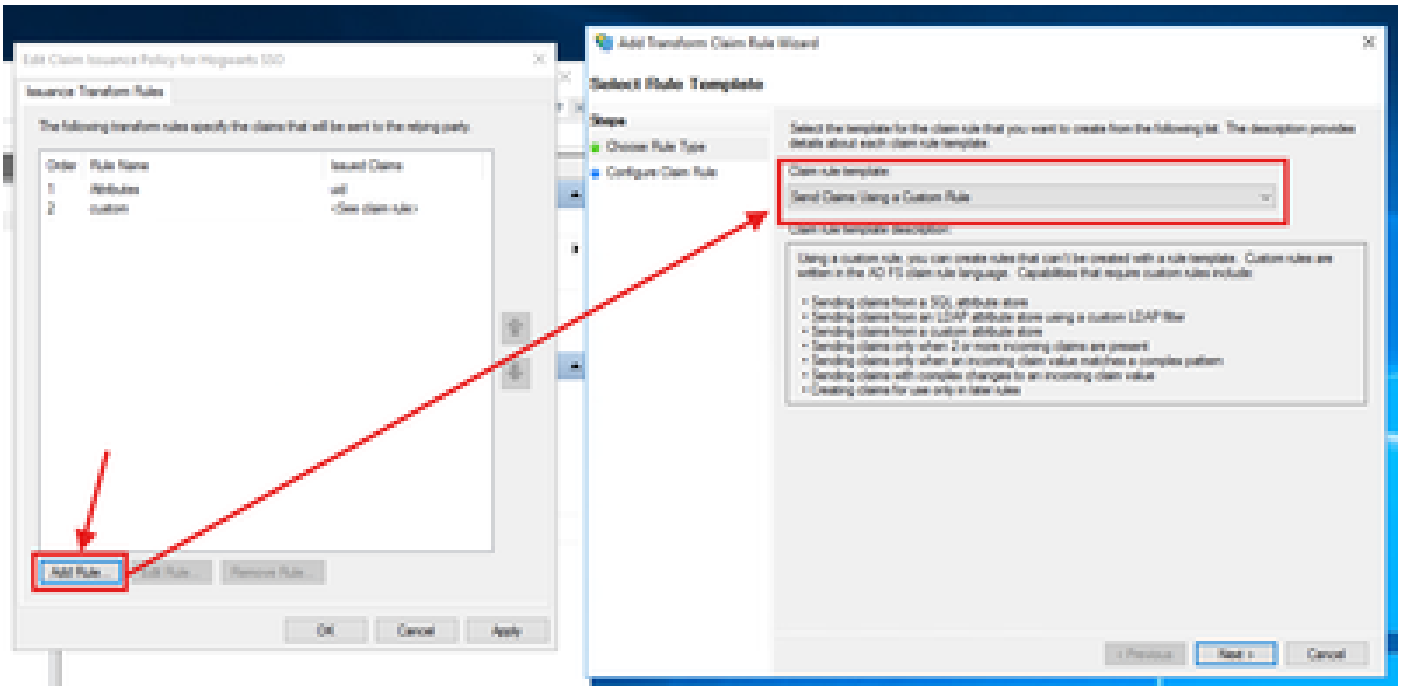
Como a configuração não é exibida corretamente, crie manualmente essa regra usando o texto sem formatação do idioma da regra.

Adicionar uma Regra de Declaração Personalizada no Servidor ADFS sob Confiança da Terceira Parte Confiável do Webex

Etapas para criar esta regra

1. No painel principal do ADFS, selecione a relação de confiança que você criou e, em seguida, selecione Editar Regras de Declaração. Na guia Regras de transformação de emissão, selecione Adicionar regra.
2. Selecione Send Claims Using a Custom Rule e, em seguida, selecione Next.
3. Copie a regra do editor de texto (iniciando em c:) e cole-a na caixa de regra personalizada no servidor ADFS.

Ele deve ter a seguinte aparência:



Depois que isso for feito, você poderá testar o SSO a partir do Hub de controle e isso deverá funcionar como esperado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.