Exemplo de configuração de SAML SSO da versão 10.5 da conexão de unidade

ID do Documento: 118772

Atualizado em: janeiro 21, 2015

Contribuído por A.M.Mahesh Babu, engenheiro de TAC da Cisco.

Produtos Relacionados

- Cisco Unity Connection
- Cisco Unified Communications Manager (CallManager)

Índice

Introdução

Este documento descreve como configurar e para verificar o linguagem de marcação da afirmação da Segurança (SAML) escolha Sinal-em (SSO) para o Cisco Unity Connection (UCXN).

Pré-requisitos

Requisitos

Instalação do Network Time Protocol (NTP)

Para SAML SSO a trabalhar, você deve instalar o NTP correto setup e certificar-se de que a diferença de horário entre o fornecedor da identidade (IdP) e os aplicativos de comunicações unificadas não excedem três segundos. Para obter informações sobre de sincronizar pulsos de disparo, veja a seção dos ajustes NTP no Guia de Administração do sistema operacional das comunicações unificadas de Cisco.

Domain Name Server (DNS) Setup

Os aplicativos de comunicações unificadas podem usar o DNS a fim resolver nomes de domínio totalmente qualificados (FQDNs) aos endereços IP de Um ou Mais Servidores Cisco ICM NT. Os provedores de serviços e o IdP devem ser solucionáveis pelo navegador.

A versão 2.0 do serviço da federação do diretório ativo (AD FS) deve ser instalada e configurado a fim segurar pedidos de SAML.

Componentes Utilizados

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

- Versão 2.0 AD FS como IdP
- UCXN como o provedor de serviços
- Versão do Microsoft internet Explorer 10

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

SAML é um com base em XML, formato de dados do padrão aberto para o intercâmbio de dados. É um protocolo de autenticação usado por provedores de serviços a fim autenticar um usuário. A informação da autenticação da Segurança é passada entre um IdP e o provedor de serviços.

SAML é um padrão aberto que permita clientes de autenticar contra todo o serviço SAML-permitido da Colaboração (ou unificou uma comunicação) apesar da plataforma de cliente.

Todo o Cisco unificou interfaces da WEB de uma comunicação, tais como o gerente das comunicações unificadas de Cisco (CUCM) ou o UCXN, protocolo da versão 2.0 de SAML do uso

na característica de SAML SSO. A fim autenticar o usuário do Lightweight Directory Access Protocol (LDAP), UCXN delega um pedido de autenticação ao IdP. Este pedido de autenticação gerado pelo UCXN é um pedido de SAML. O IdP autentica e retorna uma afirmação de SAML. A afirmação de SAML mostra ou sim (autenticado) ou nenhum (autenticação falhada).

SAML SSO permite que um usuário LDAP registre em aplicativos do cliente com um nome de usuário e senha que autentique no IdP. Um login do usuário a alguns dos aplicativos de web apoiados no Produtos unificado de uma comunicação, depois que você permite a característica de SAML SSO, igualmente acede a estes aplicativos de web em UCXN (independentemente de CUCM e CUCM IM e presença):

Usuários da conexão de unidade	Aplicativos de web
Usuários LDAP com direitos do administrador	• A administração UCXN • Utilidade de Cisco UCXN • Cisco unificou a utilidade • Cisco Personal Communications Assistant • Caixa de entrada da Web • Mini caixa de entrada da Web (versão da área de trabalho)
Usuários LDAP sem direitos do administrador	• Cisco Personal Communications Assistant • Caixa de entrada da Web • Mini caixa de entrada da Web (versão da área de trabalho) • Cisco Jabber clientes

Configurar

Diagrama de Rede

Configurando diretórios

1. Assine na página de administração UCXN e no **LDAP** seleto e clique a **instalação LDAP**.

2. A verificação **permite a sincronização do servidor ldap** e clica a **salvaguarda**.

3. Clique **LDAP**.

4. **Configuração do diretório LDAP do** clique.

5. O clique **adiciona novo**.

6. Configurar estes artigos:

   Ajustes da conta do diretório LDAPAtributos de usuário a ser sincronizadosPrograma̧ão da

sincronizaçãoHostname do servidor ldap ou endereço IP de Um ou Mais Servidores Cisco ICM NT e número de porta

7. Verifique o **uso SSL** se você quer usar o Secure Socket Layer (SSL) a fim se comunicar com o diretório LDAP.

   Dica: Se você configura o LDAP sobre o SSL, transfira arquivos pela rede o certificado do diretório LDAP em CUCM. Refira o índice do diretório LDAP no gerente SRND das comunicações unificadas de Cisco para obter informações sobre do mecanismo de sincronização da conta para o Produtos específico LDAP e melhores prática gerais para a sincronização LDAP.

8. O clique **executa a sincronização completa agora**.

   Nota: Certifique-se que serviço de **Cisco DirSync** está permitido no página da web da utilidade antes que você clique a salvaguarda.

9. Expanda **usuários** e selecione **usuários da importação**.

10. **No gerente que das comunicações unificadas do achado os utilizadores finais** alistam, selecionam o **diretório LDAP**.

11. Se você quer importar somente um subconjunto dos usuários no diretório LDAP com que você integrou UCXN, incorpore as especificações aplicáveis aos campos de busca.

12. Selecione o **achado**.

13. No baseado na lista do molde, selecione o **molde do administrador** que você quer UCXN se usar quando cria os usuários selecionado.

    Cuidado: Se você especifica um molde do administrador, os usuários não terão caixas postais.

14. Verifique as caixas de seleção para ver se há os usuários LDAP para quem você quer criar os usuários UCXN e a **importação do** clique **selecionados**.

Permita SAML SSO

1. Log na interface do utilizador da administração UCXN.

2. Escolha o **sistema** > o **SAML únicos Sinal-em** e a janela de configuração de SAML SSO abre.

3. A fim permitir SAML SSO no conjunto, o clique **permite SAML SSO**.

4. Na janela de aviso da restauração, o clique **continua.**

5. Na tela SSO, o clique **consulta** a fim importar o arquivo dos **metadata** XML **FederationMetadata.xml** com a **etapa dos Metadata de** DownloadIdp.

6. Uma vez que o arquivo dos metadata é transferido arquivos pela rede, clique **Metadata de IdP da importação** a fim importar a informação de IdP a UCXN. Confirme que a importação era bem sucedida e o clique **ao lado de** continua.

7. Clique o **Fileset dos Metadata da confiança da transferência** (faça isto somente se você não configurou ADFS já com Metadata UCXN) a fim salvar os metadata UCXN a uma pasta local e ir adicionar UCXN como a retransmissão da confiança do partido. Uma vez que a configuração AD FS é terminada, continue a etapa 8.

8. Selecione o **SSO** como o usuário administrativo e clique o **teste da corrida SSO**.

9. Ignore avisos do certificado e continue mais. Quando você é alertado para credenciais, incorpore o nome de usuário e senha do usuário SSO e clique a **APROVAÇÃO**.

   Nota: Este exemplo de configuração é baseado em certificados auto-assinados UCXN e AD FS. Caso que você usa Certificados do Certificate Authority (CA), os Certificados apropriados devem ser instalados em AD FS e em UCXN. Refira o gerenciamento certificado e a validação para mais informação.

10. Afinal as etapas estão completas, você recebem “o teste SSO sucedido!” mensagem. **Fim** e **revestimento do** clique a fim continuar.

    Você agora terminou com sucesso as tarefas de configuração permitir o SSO em UCXN com AD FS.

Nota imperativa: Execute o teste SSO para o subscritor UCXN se é um conjunto a fim permitir SAML SSO. O AD FS deve ser configurado para todos os Nós de UCXN em um conjunto.

Dica: Se você configura arquivos dos metadata XML de todos os Nós em IdP e você começa permitir a operação SSO em um nó, a seguir SAML SSO estará permitido em todos os Nós no conjunto automaticamente.

Você pode igualmente configurar CUCM e CUCM IM e presença para SAML SSO se você quer usar SAML SSO para clientes do Jabber de Cisco e dar uma experiência verdadeira SSO aos utilizadores finais.

Verificar

Abra um navegador da Web e incorpore o FQDN de UCXN e você vê uma opção nova sob os aplicativos instalados chamados **Recuperação URL para contornear único Sinal-em (SSO)**. Uma vez que você clica o link do **Cisco Unity Connection**, você está alertado para credenciais pelo AD FS. Depois que você incorpora credenciais do usuário SSO, você estará registrado com sucesso na página da administração de unidade, página unificada da utilidade.

Nota: SAML SSO não permite o acesso a estas páginas:
- Gerente licenciando principal
- A administração do OS
- Sistema da Recuperação de desastres

Troubleshooting

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

Refira a pesquisa de defeitos de SAML SSO para o Produtos 10.x da Colaboração para mais informação.

Cisco relacionado apoia discussões da comunidade

Cisco apoia a comunidade é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira convenções dos dicas técnicas da Cisco para obter informações sobre das convenções usadas neste documento.

Atualizado em: janeiro 21, 2015
ID do Documento: 118772