Falhas de inscrição da ZTNA para usuários convidados com contas pessoais do Google no Cisco Secure Access

Contents

Problema

Durante a implantação do Acesso Privado com o ZTNA (Zero Trust Network Access), a inscrição de um usuário convidado com uma conta pessoal do Google falha após o registro bem-sucedido no ID da Entra e o provisionamento no Secure Access. Os sintomas específicos encontrados incluem:

- Registro baseado em cliente: O processo de inscrição alcança a autenticação SSO, as credenciais são fornecidas, mas a ZTNA exibe um "erro de I/O" e o processo de inscrição fica travado
- Acesso sem cliente: Retorna a mensagem de erro "Cisco Secure Access Login failure. Check IDP Configuration" juntamente com um ID de transação

Essas falhas impedem o acesso a recursos privados e impactam o teste da funcionalidade ZTNA para acesso ao estilo do contratante usando identidades não corporativas.

Ambiente

- Cisco Secure Access com implantação ZTNA
- Microsoft Entra ID (antigo Azure AD) como Provedor de Identidade
- Conta pessoal do Google (@gmail.com) registrada como usuário convidado na ID da Entra
- Conta de convidado provisionada e visível no Secure Access
- Autenticação SAML configurada entre Entra ID e Cisco Secure Access

Resolução

A falha de registro foi resolvida com a modificação da configuração de mapeamento de atributo SAML no Microsoft Entra ID. Foram tomadas as seguintes medidas para resolver o problema:

Passo 1: Analisar o pacote DART e o comportamento do cliente

Revise o pacote DART para confirmar se os componentes Cisco Secure Client e ZTA estão operando normalmente. A análise deve verificar se o fluxo de inscrição alcança com êxito o Cisco Secure Access e se a falha ocorre durante a autenticação SAML com o Provedor de Identidade.

Passo 2: Examinar Logs de Autenticação do Entra ID

Verifique os logs de autenticação do Entra ID para confirmar se o processo de autenticação foi concluído com êxito da perspectiva do Provedor de identidade. Os logs devem mostrar a autenticação bem-sucedida, mas o Secure Access rejeita o login devido à incompatibilidade de atributos.

Passo 3: Identificar Problema de Mapeamento de Atributos SAML

Determine se a ID da Entra está emitindo o UPN (Nome UPN) como a declaração SAML, que não corresponde à identidade da conta pessoal do Gmail esperada pelo Secure Access. O atributo IdP declarado não corresponde ao identificador de usuário esperado.

Passo 4: Modificar mapeamento de atributos SAML

Altere o mapeamento de atributo SAML na ID do Microsoft Entra de UPN para Endereço de Email. Isso garante que a reivindicação do endereço de e-mail corresponda à identidade da conta pessoal do Google.

Passo 5: Verificar o sucesso da inscrição

Depois de implementar a alteração de mapeamento de atributo, repita o processo de registro ZTNA. O Cisco Secure Access ZTA agora deve reconhecer o endereço do Gmail e permitir que a inscrição seja concluída com êxito.

Causa

A falha de inscrição foi causada por uma incompatibilidade entre o atributo SAML que está sendo declarado pela ID do Microsoft Entra e o identificador de usuário esperado no Cisco Secure Access. A ID da Entra foi configurada para enviar o UPN (Nome Principal do Usuário) como a declaração SAML, mas para contas pessoais do Google (@gmail.com), esse UPN não correspondeu à identidade do endereço de email real. O Cisco Secure Access esperava receber o endereço de e-mail como o atributo de identificação para comparar com a conta de usuário convidado provisionada, resultando em rejeição de autenticação apesar da autenticação de IdP bem-sucedida.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

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.