

A autenticação SAML de VPNaaS falha com "Falha nacriptografia do estado de retransmissão" Erro ao usar IdP Duo

Contents

Problema

Ao tentar estabelecer uma conexão VPNaaS usando o acesso remoto de cliente seguro com autenticação SAML e Duo como o provedor de identidade (IdP), este erro é observado:

- Falha ao processar a solicitação de autenticação SSO. Entre em contato com o administrador do sistema
- Falha nacriptografia de relaystate

A autenticação com a mesma configuração de IdP e Duo funciona com êxito para ZTNA (Zero Trust Network Access), mas falha para conexões VPN. Há dois aplicativos separados configurados em Duo para ZTNA e VPN, ambos usando o mesmo IdP.

Ambiente

- Tecnologia: Suporte à solução (SSPT - contrato necessário)
- Subtecnologia: Acesso seguro - Acesso remoto seguro do cliente (VPN, postura, recurso privado)
- método de autenticação: SAML com Duo IdP
- Dois aplicativos Duo configurados: um para ZTNA, um para VPN
- A autenticação funciona para ZTNA, falha para VPN
- Versão de software: TODOS
- Nenhuma alteração recente de versão de hardware/software especificada

Resolução

O problema foi resolvido com a correção da configuração da ID de entidade e da URL do Serviço de Consumidor de Asserção (ACS) no aplicativo Duo para VPN. Os metadados corretos foram baixados do Secure Access e carregados no aplicativo VPN Duo, o que resolveu o erro decriptografia de estado de retransmissão SAML.

1. Faça login no Painel CSA. Vá para Connect > Enduser Connectivity -> Virtual Private Networks. Descubra o Perfil ao qual você está conectado.
2. Clique nesse Perfil e Editar. Vá para a guia Autenticação.
3. Baixe os metadados SAML para acesso seguro.

4. Verifique entityID="<https://X.vpn.sse.cisco.com/saml/sp/metadata/saml>" e
<[AssertionConsumerService](#) index="0" isDefault="true"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://X.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=Profilename"></AssertionCo
5. Certifique-se de que entityID e AssertionConsumerService correspondam ao Aplicativo Duo configurado para Autenticação VPN SSO.

Causa

A configuração incorreta da ID da entidade e da URL do ACS no aplicativo Duo VPN resultou na falha de descryptografia do estado de retransmissão SAML. A configuração correta não estava presente no Duo para VPN, embora a autenticação ZTNA estivesse funcionando com o mesmo IdP. A atualização do aplicativo Duo VPN com metadados precisos do Secure Access resolveu o problema.

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.