A configuração SAML para o Microsoft Azure AD não mapeia grupos.

Aplicabilidade

Nuvem Splunk

Descrição

A autenticação SAML é configurada de acordo com a documentação do Splunk:
Configure o SSO com o Microsoft Azure AD ou AD FS como seu Provedor de Identidade
No entanto, as permissões não foram mapeadas corretamente.

Investigação

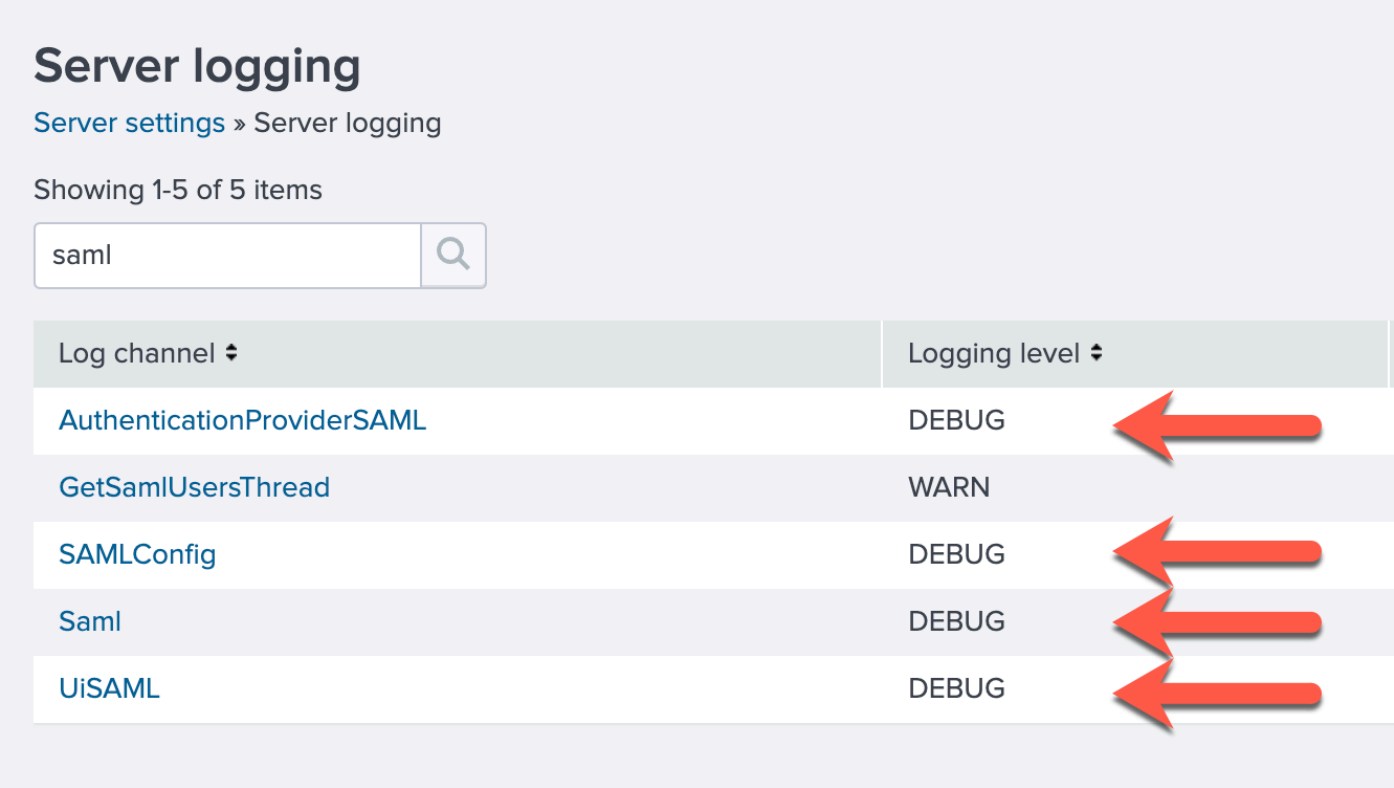
O seguinte erro é observado quando um usuário está tentando fazer logon na interface do usuário da Web de Splunk:

```
'no valid role found in local mapping'
```

Os grupos de mapeamento na Nuvem do Splunk não correspondem, o nome do grupo não corresponde ao ObjectId do grupo do Azure AD, os grupos de mapeamento do Splunk devem ser chamados com o ObjectId do Azure AD do grupo a ser mapeado no Splunk. Por exemplo, espera-se o seguinte:

ObjectId do Azure AD do grupo a ser mapeado: 99fvd7-fvddfv999-99999njhb
Nome do grupo de mapeamento de Splunk: 99fvd7-fvddfv999-99999njhb

Para validar os grupos que um usuário tem ao fazer logon, ative a depuração para SAML na GUI Splunk:



Em seguida, faça com que o usuário faça login novamente e execute o SPL a seguir para exibir os grupos que estão sendo retornados:

```
index=_internal sourcetype=splunkd samlp
```

A partir daqui, você pode ver se os mapeamentos saml no splunk correspondem ao que está sendo retornado pelo IdP.

Resolução

Neste cenário, os grupos de mapeamento existentes precisavam ser excluídos e criados novamente, para que a configuração fosse atualizada e correspondesse ao que está sendo retornado pelo grupo IdP do Azure AD. Assim que os usuários do grupo mapeado do Azure AD fizerem logon no Splunk Cloud, o usuário aparecerá na seção de autenticação, em Configurações > Controle de Acesso > Usuários com o tipo de autenticação SAML.

Links relacionados

Configure o SSO com o Microsoft Azure AD ou AD FS como seu Provedor de Identidade

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.