Microsoft Azure AD的SAML配置不映射组。

适用范围

Splunk云

描述

根据Splunk文档配置SAML身份验证：
将Microsoft Azure AD或AD FS配置为身份提供程序
但是，权限映射不正确。

调查

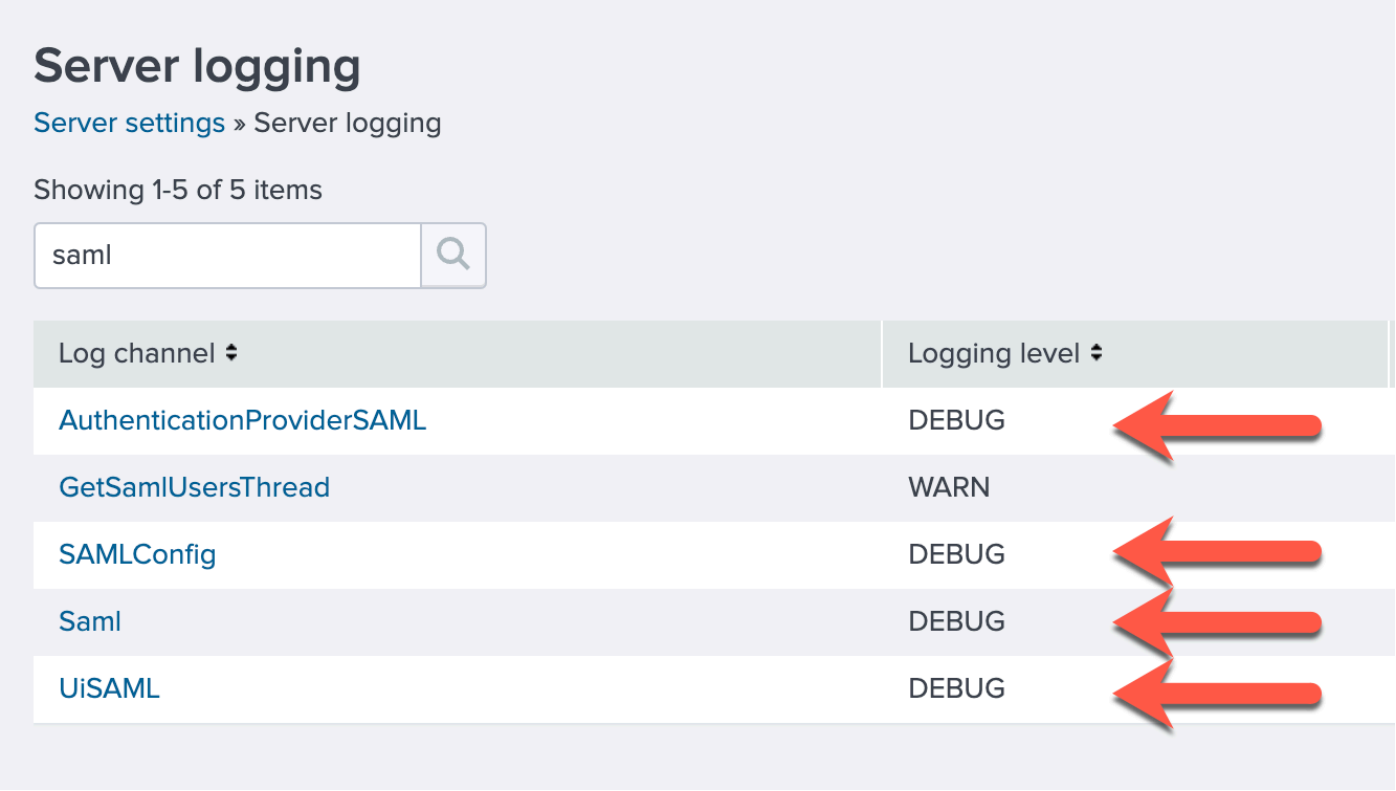
当用户尝试从Splunk Web UI登录时，出现以下错误：

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

Splunk云中的映射组不匹配，组名称与Azure AD组的ObjectId不匹配，Splunk映射组必须使用要在Splunk中映射的组的Azure AD ObjectId进行调用，例如，应执行以下操作：

要映射的组的Azure AD ObjectId:99fvd7-fvddfv999-99999njhb
Splunk映射组名称: 99fvd7-fvddfv999-99999njhb

要验证用户在登录时拥有的组，请在Splunk GUI中打开SAML调试：



然后让用户再次登录并运行以下SPL以查看返回的组：

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

从这里您可以看到splunk中的saml映射是否与IdP返回的内容匹配。

分辨率

在这种情况下，需要删除并再次创建现有映射组，以便更新配置并匹配IdP Azure AD组返回的内容。映射Azure AD组中的用户登录到Splunk Cloud后，用户即会出现在身份验证部分的设置>访问控制>具有SAML身份验证类型的用户中。

相关链接

[将Microsoft Azure AD或AD FS配置为身份提供程序]

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。