从思科安全云产品收集SAML日志

目录

简介

本文档介绍从Cisco安全云产品收集SAML日志的步骤，TAC团队使用这些SAML日志来排查登录问题。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题：

思科TAC使用SAML日志来排除与思科安全云产品登录相关的故障。
利用SAML日志中的信息，TAC可以分析对思科安全云产品后端服务器进行的跟踪，并有效解决此问题。

解决方案：

SAML日志集合将取决于用于获取这些日志的浏览器。

铬

1.从Add extension部分下载SAML Tracer，导航到Home > Extension > SAML-tracer，选择Add to Chrome > Add extension
2.添加扩展名后，导航至浏览器右上角的三个点> 更多工具>开发人员工具
3.选择“开发工具”部分顶部中的选项“>>”，然后选择“SAML”
4.重现问题

5.单击Show only SAML复选框
6.保存输出并与TAC共享

Firefox

1.与前面步骤相似，将SAML-tracer工具添加到Firefox，在显示权限弹出窗口时单击“添加”，然后单击“确定”，如果要在专用窗口上使用扩展名，则选中此复选框
2.在浏览器的右上角，您可以看到SAML-tracer图标，选择它。
3.选择后，将出现另一个窗口，此时您现在可以重现登录问题，在复制场景后，复制输出或将其导入以将文件上传到Support Case Manage中，并将信息共享给TAC团队，以供进一步调查

相关信息

- 技术支持和文档 - Cisco Systems

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）。