解决与思科ISE集成的IOS-XE设备上的CTS配置文件不完整和SGACL下载故障

目录

问题

即使存在CTS服务器列表和环境数据，您也会在网络设备上观察到部分或不完整的Cisco TrustSec(CTS)配置文件。网络设备无法下载安全组访问控制列表(SGACL)访问控制条目(ACE)。

此问题影响使用Cisco IOS® XE网络设备(例如Catalyst 9000系列交换机、无线局域网控制器(WLC)和带有身份服务引擎(ISE)的路由器)的部署。

网络设备日志中出现以下错误：

```
%CTS-2-AUTHZ_POLICY_SGACL_ACE_FAILED: Failed to download ACEs for SGACL '<ACLname>' for SGT='<SGTnumber
```

环境

- ISE 3.5补丁2
- ISE 3.3补丁8
- ISE 3.2补丁9
- CTS环境
- IOS-XE网络设备，如Cat9k、WLC和路由器

分辨率

方案 A：升级ISE（推荐）

要永久解决此问题，请将Cisco ISE升级到已解决Cisco Bug ID CSCws51319的固定版本。

- 已修复版本:
  - ISE 3.5补丁3或更高版本
  - ISE 3.3补丁9或更高版本
  - ISE 3.2补丁10或更高版本

方案 B：手动策略刷新（解决方法）

如果无法立即进行升级，则每次在ISE中进行策略更改时，都必须手动触发网络设备上的策略刷新。

1.访问受影响网络设备的CLI。

2.运行此命令以验证CTS PAC状态。

```
show cts pac
```

3.要验证CTS环境数据是否存在，请运行命令：

```
show cts environment data
```

4.要检查当前策略权限，请运行：

```
show cts role-based permissions
```

5.运行命令刷新策略：

```
cts refresh policy
```

6.等待几分钟，等待下载完成。

7.检查当前策略条件并确认是否使用以下命令下载了所有权限：

```
show cts role-based permissions
```

原因

此问题是由Cisco Bug ID CSCws51319引起的。

相关内容

- 思科漏洞ID CSCws51319
- 思科技术支持和下载

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）。