解决由于系统过载导致的ISE TACACS+身份验证故障

目录

问题

思科身份服务引擎(ISE)终端访问控制器增强型访问控制系统(TACACS+)身份验证会间歇性停止工作，导致网络设备登录回本地用户而非TACACS+身份验证。在中断期间，实时日志中会显示“TACACS+请求因系统过载而被丢弃”的故障原因。身份验证失败发生时，不会对TACACS+的ISE或有关TACACS+配置的网络设备进行任何配置更改。

环境

- 思科身份服务引擎(ISE)版本3.3补丁7
- 使用特定PSN进行设备管理的分布式ISE部署
- 用于管理访问的TACACS+身份验证服务
- 传输控制协议(TCP)系统日志目标配置

分辨率

在问题期间在策略服务节点(PSN)上启用运行时AAA调试，并查看prrt-server.log会发现极高的ContextN值，表示已备份PSN上的处理：

```
ContextCounter,2026-05-05 12:17:08,442,DEBUG,0x7f42bead0700,ContextN incremented, number=113687,Context
```

AcsLoggerReactorThread和TCPSyslogReactorThread是提升的线程池，并导致备份：

```
EventHandler,2026-05-05 12:17:10,461,DEBUG,0x7f42bead0700,Passed event to the next thread pool name=Acs
EventHandler,2026-05-05 12:17:12,859,DEBUG,0x7f429b6d0700,Passed event to the next thread pool name=TCP
```

由于达到空间限制，TACACS+连接被丢弃：

```
TCPListener,2026-05-05 12:17:08,804,DEBUG,0x7f429b4cf700,NIL-CONTEXT,Hit space limit. Dropping request!
```

由于Cisco缺陷CSCwt35414，在配置中已启用“服务器关闭时缓冲消息”设置的Administration > System > Logging > Remote Logging Targets下的任何TCP系统日志目标在较长时间内不可访问。如果不能保证可访问性，则必须安装固定版本的ISE，或者在TCP系统日志目标上取消选择“服务器关闭时缓冲消息”功能，以防止此行为。

原因

根本原因标识为Cisco缺陷CSCwt35414。此缺陷导致PSN上的身份验证处理在TCP系统日志目标上配置的缓冲区变满时被阻止。当TCP Syslog目标不可达或再次响应后无法发送时，日志会写入缓冲区，但如果目标长时间无法到达，PSN上的流量过大，缓冲区将填满，身份验证处理将受到影响。

相关内容

- 思科缺陷CSCwt35414
- 远程日志记录目标设置

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）。