Troubleshoot ISE TACACS+ Authentication Failures Due to System Overload

Contents

Issue

Cisco Identity Services Engine (ISE) Terminal Access Controller Access-Control System Plus (TACACS+) authentications stop working intermittently, and cause network device logins to fall back to local users instead of TACACS+ authentication. During the outages, failure reasons of "TACACS+ request was dropped because of system overload" display in the Live Logs. The authentication failures occur without any configuration changes being made to ISE for TACACS+ or on the network devices regarding TACACS+ configuration.

Environment

- Cisco Identity Services Engine (ISE) version 3.3 patch 7
- Distributed ISE deployment with specific PSNs for Device Administration
- TACACS+ authentication service for administrative access
- Transmission Control Protocol (TCP) Syslog target configuration

Resolution

Enabling runtime-AAA debugs on the Policy Service Node (PSN) during the issue and reviewing prrt-server.log reveals extremely high ContextN values indicating that processing on the PSN is backed-up:

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

The AcsLoggerReactorThread and TCPSyslogReactorThread are the threadpools that are elevated and causing the back-up:

```
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
```

The TACACS+ connections are dropped due to the space limit being hit:

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

Any TCP Syslog targets enabled under **Administration > System > Logging > Remote Logging Targets** with the setting "Buffer Messages When Server Down" enabled in the configuration must not be unreachable for extended periods of time due to Cisco defect CSCwt35414. If reachability cannot be guaranteed, either a fixed version of ISE must be installed or the "Buffer Messages When Server Down" feature should be deselected on the TCP Syslog target to prevent this behavior.

Cause

The root cause was identified as Cisco defect CSCwt35414. This defect causes authentication processing on the PSN to become blocked whenever the configured buffer on the TCP Syslog target becomes full. Logs are written to the buffer when the TCP Syslog target is unreachable or unresponsive to be sent once it is responding again, but if the target is unreachable for long periods of time with heavy traffic on the PSN, the buffer will fill up and authentication processing is affected.

Related Content

- Cisco defect CSCwt35414
- Remote Logging Targets settings