

Fehlerbehebung bei ISE TACACS+- Authentifizierungsfehlern aufgrund von Systemüberlastung

Inhalt

Problem

Die Authentifizierungen von Cisco Identity Services Engine (ISE) Terminal Access Controller Access-Control System Plus (TACACS+) laufen nicht mehr intermittierend ab und führen dazu, dass die Anmeldung bei Netzwerkgeräten auf lokale Benutzer und nicht auf die TACACS+-Authentifizierung zurückfällt. Während der Ausfälle werden in den Live-Protokollen die Fehlerursachen für die Meldung "TACACS+-Anfrage wurde wegen Systemüberlastung verworfen" angezeigt. Die Authentifizierungsfehler treten auf, ohne dass Konfigurationsänderungen an der ISE für TACACS+ oder an den Netzwerkgeräten hinsichtlich der TACACS+-Konfiguration vorgenommen werden.

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.3 Patch 7
- Verteilte ISE-Bereitstellung mit spezifischen PSNs für die Geräteadministration
- TACACS+-Authentifizierungsservice für Administratorzugriff
- Transmission Control Protocol (TCP) Syslog-Zielkonfiguration

Auflösung

Durch Aktivieren von Runtime-AAA-Debugging auf dem Policy Service Node (PSN) während des Problems und Überprüfen von prrt-server.log werden extrem hohe ContextN-Werte angezeigt, die

darauf hinweisen, dass die Verarbeitung auf dem PSN gesichert wird:

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

AcLoggerReactorThread und TCPSyslogReactorThread sind die Threadpools, die erhöht sind und die Sicherung verursachen:

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

Die TACACS+-Verbindungen werden aufgrund der folgenden Speicherplatzbeschränkung getrennt:

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

Alle TCP-Syslog-Ziele, die unter Administration > System > Logging > Remote Logging Targets mit der in der Konfiguration aktivierten Einstellung "Buffer Messages When Server Down" aktiviert sind, dürfen wegen des [Cisco Defekts CSCwt35414](#) über längere Zeiträume nicht unerreichbar sein. Wenn die Erreichbarkeit nicht gewährleistet werden kann, muss entweder eine feste Version von ISE installiert oder die Funktion "Puffermeldungen bei Serverausfall" sollte auf dem TCP-Syslog-Ziel deaktiviert werden, um dieses Verhalten zu verhindern.

Ursache

Die Ursache wurde als [Cisco-Defekt CSCwt35414](#) identifiziert. Dieser Defekt bewirkt, dass die Authentifizierungsverarbeitung auf dem PSN blockiert wird, sobald der konfigurierte Puffer auf dem TCP-Syslog-Ziel voll wird. Protokolle werden in den Puffer geschrieben, wenn das TCP-Syslog-Ziel nicht erreichbar ist oder nicht reagiert, um gesendet zu werden, sobald es erneut antwortet. Wenn das Ziel jedoch bei starkem Datenverkehr auf dem PSN längere Zeit nicht erreichbar ist, füllt sich der Puffer, und die Authentifizierungsverarbeitung wird beeinträchtigt.

Verwandte Inhalte

- [Cisco Fehler CSCwt35414](#)
- [Einstellungen für Remote-Protokollierungsziele](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.