ISE RADIUS Context Exhaustion Causes Node to Stop Responding

Contents

Issue

A Cisco Identity Services Engine (ISE) node intermittently stops responding to RADIUS authentication requests, causing network devices to mark it as "RADIUS DEAD". The affected node receives RADIUS requests (confirmed via firewall logs and packet captures) but fails to respond. The following symptoms are observed:

- RADIUS retransmission messages on network devices
- "Radius Context Allocation Failed" critical alarms appearing in ISE
- Log messages indicating "Hit context count limit. Dropping request!"
- ISE GUI becomes inaccessible during the issue despite all services showing as running
- Node restarts temporarily resolve the issue for approximately 30 minutes before it recurs

Specific error messages observed include:

```
033057: Mar 11 09:33:59.015: RADIUS: Retransmit to (10.0.5.11:1812,1813) for id 1645/127
033058: Mar 11 09:33:59.015: RADIUS: PAC key found while sending request (rctx:0x75EB6A555690)
033059: Mar 11 09:33:59.015: RADIUS: Message Authenticator encoded
033060: Mar 11 09:33:59.015: RADIUS(00000000): Started 4 sec timeout
```

And in ISE logs:

```
RadiusListener,2026-06-28 23:21:22,149,WARN ,0x7efea2055700,NIL-CONTEXT,Hit context count limit. Droppi
```

Environment

- Cisco Identity Services Engine (ISE) version 3.5.0.331 (Patch 3)
- Node serving multiple roles: Primary Administration Node (PAN), Session Management and Troubleshooting (SMNT), and Policy Service Node (PSN)
- Authentication methods: Both 802.1X and MAB enabled on access switch ports
- External identity sources: Microsoft Entra ID integration
- Network devices configured with ISE as RADIUS server for authentication

Resolution

The issue was resolved by applying a Cisco-provided hotfix that addresses a deadlock condition in the ISE SessionUpdater process. Follow these steps to implement the resolution:

Step 1: Obtain and Install the Hotfix

Download the hotfix files from Cisco and transfer them to your ISE node repository. The hotfix files are:

- ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz (installation file)
- ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz (rollback file)

Step 2: Apply the Hotfix

Install the hotfix using the CLI command:

```
application install ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

⚠**Caution**: Possible. The details mentioned here appears to contain procedures or commands that could cause significant impact if executed. Please ensure the above procedures or commands have been evaluated by an SME or Business Unit before executing or recommending.

Step 3: Verify Installation

Verify the hotfix installation using one of these commands:

```
show logging application hotpatch.log
```

Or:

```
show version
```

Step 4: Monitor the System

After installation, monitor the ISE node for a minimum of two weeks to ensure the issue does not recur. The hotfix installation requires a service restart, so plan the installation during a maintenance window.

Optional: Rollback Procedure

If needed, the hotfix can be removed using the rollback command:

```
application install ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

Troubleshooting Commands for Monitoring

To monitor RADIUS context allocation, use:

```
show logging application prrt-server.log | include ContextN
```

Enable runtime AAA debugs before any future troubleshooting:

```
debug aaa runtime
```

Cause

The root cause was identified as a deadlock condition in the ISE SessionUpdater process. When simultaneous accounting start and stop events occurred for the same session, two threads entered a circular wait scenario:

- Thread-162: owned cacheLock, waited for SessionInfo lock
- Thread-125: owned SessionInfo lock, waited for cacheLock

This circular wait led to ContextN leaks and a continuously growing RADIUS processing queue. The queue buildup eventually exhausted available RADIUS contexts, causing authentication latency and network devices to mark the ISE node as RADIUS DEAD.

The issue is documented in Cisco bug ID CSCwv71473.

Related Content

- Cisco bug ID CSCwv71473
- Cisco Technical Support & Downloads