Troubleshoot ISE 3.4 VPN and RADIUS Authentication Failures

Contents

Issue

ISE 3.4 Patch 4 deployments experience authentication failures when a Secondary Administration Node (SAN) experiences an outage. Authentication requests directed to the Primary Policy Administration Node (PPAN) also fail, causing disruptions for ASA VPN connections and RADIUS authentications. The SAN node displays as disconnected in the ISE deployment dashboard, and logs indicate EAP/TLS-related errors and session-tracking issues.

Environment

- Cisco Identity Services Engine (ISE)
- Network Access Devices (NADs): Includes Meraki devices and/or ASA firewall
- Topology: Multi-node ISE deployment with SAN and PPAN

Resolution

1.- Remove all personas from the SAN node via the Cisco ISE Administration interface by navigating to **Administration > System > Deployment**. This halts authentication attempts to the failed node and allows unaffected nodes to resume processing.

Note: After persona removal, the SAN node continues to display as disconnected (Red X) in the deployment dashboard.

2.- Manually force the ASA firewall to consider the SAN node as FAILED, preventing further authentication attempts from being directed toward the unavailable SAN. This action is performed on the ASA configuration, ensuring failover to operational ISE nodes.

3.- Review the ISE deployment for proper synchronization and monitor health metrics, including CPU, memory, and disk utilization.

4.- Verify that authentication services are operational by checking that new Dot1x and RADIUS requests are processed by the unaffected ISE nodes.

5.- Collect DEBUG logs and packet captures during authentication failures to analyze EAP/TLS negotiation timing and session resets.

6.- Continue monitoring ISE system health metrics and authentication behavior after SAN failover events.

7.- Validate Meraki RADIUS failover behavior, noting that ISE does not support "Status-Server" RADIUS packets for server availability detection.

Example Log Messages

```
Accounting start was received for non-existing session
```

```
Error getting peer certificate from SSL Connection
```

```
packet for this endpoint 58-6D-67-XX-XX-XX is being processed right now so drop the new EAP session
```

```
Long step latency ;2=57290
```

```
Endpoint 58-6D-67-XX-XX-XX abandoned EAP session xxxxxxxxx/552628443/4183334 and started EAP session
```

Cause

The root cause is a SAN node outage due to an ISP link failure, which leads to session-tracking inconsistencies and EAP/TLS negotiation errors between the supplicant, NAD, and ISE nodes. Additionally, Meraki devices rely on "Status-Server" RADIUS packets for failover detection, which Cisco ISE does not support, resulting in continued authentication attempts to the failed SAN node.

Related Content

- How To: Integrate Meraki Networks with ISE
- Configure Remote Access VPN with RADIUS Authentication on ISE and Group-Policy Mapping
- Cisco Technical Support & Downloads