Understand and Troubleshoot ISE Certificate Replication Alarms

Contents

Introduction

This document describes the replication alarms and its troubleshooting in Cisco Identity Services Engine® (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge on Cisco Identity Services Engine® (ISE).

Components Used

The information in this document is based on these hardware and software versions.

- Cisco Identity Services Engine® (ISE) 3.4 and higher versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Replication Alarm

Replication alarms in Cisco ISE provide visibility into the health and synchronization status of the replication framework across the deployment. These alarms help identify conditions that can affect data consistency, node communication, or replication processes, enabling administrators to detect and resolve issues before they impact system operations. Understanding the purpose and significance of replication alarms is essential for maintaining a healthy ISE deployment and ensuring that configuration and operational data remain synchronized across all nodes.

ISE Certificate Replication Alarms

Certificate Replication Failed

The **Certificate Replication Failed** alarm is generated when Cisco ISE fails to replicate certificate-related data from the **Primary Administration Node (PAN)** to one or more nodes in the deployment. ISE automatically replicates certificates and their associated configuration whenever certificates are imported, generated, renewed, or modified on the Primary PAN to maintain consistency across all nodes. This alarm indicates that the replication process was unsuccessful, resulting in inconsistent certificate configuration on the affected node(s).

Reason for Alarm

The Certificate Replication Failed alarm can occur when Cisco ISE is unable to successfully transfer, validate, or install certificate-related data on one or more nodes. Common causes include

- **Network communication issues:** Packet loss, high network latency, firewall restrictions blocking replication traffic, routing issues between ISE nodes, or an MTU mismatch causing packet fragmentation or drops can interrupt certificate replication.
- **Replication service issues:** Certificate replication can fail if RabbitMQ, JGroups, or other internal replication services are unavailable, restarting, or not functioning correctly.
- **Certificate validation failures:** Replication can fail if the certificate chain is incomplete, CA or intermediate certificates are missing, the certificate is expired or corrupted, or it contains unsupported key usage or an invalid format.
- **Node communication issues:** If the destination node is offline, restarting, de-registered, disconnected from the deployment, or unreachable, certificate replication cannot be completed.
- **Insufficient disk space:** The destination node do not have enough available disk space to import and install the replicated certificate.
- **Internal database issues:** Replication can fail if the ISE configuration database is unable to store or update the certificate metadata.

Impact of the Alarm

The impact of this alarm depends on the type of certificate being replicated and the services that rely on it. Failed certificate replication can result in inconsistent certificate configuration across ISE nodes, HTTPS certificate mismatches, EAP authentication failures, pxGrid trust establishment issues, SCEP enrollment or certificate provisioning failures, inconsistencies in the trusted certificate store, and TLS validation failures with external integrations.

Certificate Replication Temporarily Failed

The Certificate Replication Temporarily Failed alarm is generated when Cisco ISE is temporarily unable to replicate certificate-related data from the Primary Administration Node (PAN) to one or more nodes in the deployment. Unlike the Certificate Replication Failed alarm, this alarm indicates that the replication failure is considered transient, and Cisco ISE automatically retries the replication operation when the underlying condition is resolved.

Reason for Alarm

The alarm is typically generated due to transient conditions that temporarily prevent certificate replication. Common causes include:

- **Temporary network communication issues:** Brief network interruptions, packet loss, high latency, firewall delays, or temporary routing issues between ISE nodes.
- **Replication service initialization or restart:** RabbitMQ, JGroups, or other internal replication services are restarting or temporarily unavailable.
- **Temporary node unavailability:** The destination node is booting, restarting application services, rejoining the deployment, or is temporarily unreachable.
- **Temporary system resource constraints:** High CPU utilization, memory pressure, or disk I/O contention temporarily delays replication processing.
- **Concurrent administrative operations:** Certificate replication can be delayed while another certificate import, backup, restore, patch installation, or deployment synchronization is in progress.
- **Temporary database or replication queue delays:** Internal database operations or replication queues are temporarily busy processing other synchronization requests.

Impact of the Alarm

In most cases, this alarm has minimal operational impact because Cisco ISE automatically retries the replication operation. However, until replication completes successfully, temporary inconsistencies can exist between nodes, including:

- Delayed propagation of newly imported or renewed certificates
- Temporary certificate configuration mismatch across the deployment
- Delayed availability of certificate-based services on the affected node
- Temporary delays in HTTPS, EAP, pxGrid, or SCEP services if they depend on the replicated certificate

If the alarm persists or repeatedly occurs, it leads to Certificate Replication Failed alarm.

Troubleshoot ISE Certificate Replication Alarms

These are the common factors which are to be verified when troubleshooting or verifying Certificate Replication Alarms in ISE.

1. Verify Deployment Status for the Node

For certificate replication to succeed, the secondary node must be in a **Connected** state within the Cisco ISE deployment. Navigate to **Administration > System > Deployment** and verify the status of the affected node. Hover over the **Information (i)** icon next to the node status to review the synchronization details and any pending replication messages.

The synchronization status displayed for each node indicates its current replication and connectivity state:

- **Green** – The node is synchronized with the deployment, and replication is operating normally.
- **Yellow** – The node is out of synchronization, node registration has failed, or cluster connectivity has been lost. This status indicates that the node has not been reachable by the cluster for the past five minutes.
- **Red** – The node is unreachable and cannot be contacted through network connectivity checks, such as ICMP ping or HTTPS.

If the node displays a **Yellow** or **Red** status, it indicates a replication or connectivity issue affecting that node. Additionally, verify the replication message count displayed in the node information. The pending message count must be **5,000 or fewer**. A queue containing more than **5,000** pending messages indicates that the replication queue has accumulated, which can delay or prevent successful replication.

2. Verify Queue Link Alarm in the Deployment

Successful replication in Cisco ISE depends on the availability and communication of the **RabbitMQ** messaging service and **JGroups** cluster communication framework. If either component encounters communication issues, Cisco ISE generates **Queue Link Errors**, which can interrupt replication between deployment nodes.

To verify the alarm status, navigate to **Operations > Dashboard > Alarms** and check for **Queue Link Errors** on the affected nodes.

If Queue Link Errors are present, renew the Cisco ISE **Root CA certificate**, as certificate-related communication failures commonly result in Queue Link Errors. Once the certificate issue is resolved, replication typically resumes automatically without requiring additional intervention.

Note: Refer to the ISE Queue Link Errors documentation for detailed information on Queue Link Errors.

3. Verify Network Latency and Connectivity

Cisco ISE replication relies on stable network connectivity between deployment nodes. High network latency or intermittent connectivity can delay replication and can result in synchronization failures, particularly in geographically distributed deployments.

Verify the network latency between the affected nodes using connectivity tests such as **ping**. For reliable replication, the round-trip latency between nodes must remain within approximately **300 ms**. Latency consistently exceeding this threshold can adversely affect replication performance and synchronization.Also verify that there are no intermittent network outages, packet loss, or firewall restrictions affecting communication between the deployment nodes.

4. Verify that the Certificate Is Not Already Present on the Affected Node

Certificate replication can fail if the certificate being replicated already exists on the secondary node.

Navigate to **Administration > System > Certificates**, select the affected node, and verify whether the certificate is already installed. If the certificate is present, review its properties to ensure that it matches the certificate being replicated and determine whether any duplicate or conflicting certificates exist.

5. Verify System Resource Utilization

High system resource utilization can impact Cisco ISE performance and delay replication tasks. Excessive CPU, memory, or disk utilization can prevent replication processes from completing successfully.

Verify that the affected node has sufficient system resources available and that resource utilization remains within the recommended operating limits. If resource utilization is consistently high, allocate additional resources or reduce the workload on the node to restore normal replication performance.

Note: Refer to the Performance and Scalability Guide for the recommended hardware sizing and resource allocation guidelines for Cisco ISE deployments.

6. Verify Port Availability in the Deployment and Network

Cisco ISE replication requires specific TCP ports to remain open between all nodes in the deployment to ensure uninterrupted communication and successful replication. If any of these ports are blocked by a firewall, access control policy, or network device, replication failures or synchronization issues can occur.

Verify these TCP ports are open and reachable between all Cisco ISE nodes:

- **TCP 443** – HTTPS communication
- **TCP 8443** – Administrative communication
- **TCP 12001** – JGroups cluster communication and replication
- **TCP 6379** – Internal messaging services
- **TCP 8671** – Cisco ISE Messaging (RabbitMQ)

Log in to the Cisco ISE CLI and run the command **show ports** to verify the mentioned ports allowed in the node.

Confirm that the required ports are enabled on the Cisco ISE node and ensure that they are permitted across the network path. Verify that no intermediate firewalls, security devices, or network policies are blocking communication on these ports between the deployment nodes.

Log Collection for Replication Alarms

These are the common components that are to be set in **debug** mode to isolate and troubleshoot replication alarms in Cisco ISE.

- Replication-Deployment (replication.log and ise-psc.log)
- Replication-JGroup (replication.log and ise-psc.log)
- Replication Tracker (tracking.log)
- hibernate (hibernate.log)
- JMS (replication.log)

Reference

- Cisco Identity Services Engine Administrator Guide, Release 3.5
- Troubleshoot and Enable Debugs on ISE
- Collect Support Bundle on the Identity Services Engine