Understand and Troubleshoot ISE Node 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.

ISE Replication Alarms

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 Node Replication Alarms

Replication Failed

The Replication Failed alarm is generated when the secondary nodes in the deployment are unable to consume the messages which are replicated by the Primary Administration node in the deployment. This alarm indicates that the replication process has failed and the affected node no longer have the latest configuration or operational data.

Unlike certificate-specific replication alarms, this alarm represents a failure in the general replication framework and can impact multiple configuration objects and services across the deployment.

Reason for Alarm

The Replication Failed alarm can occur when Cisco ISE is unable to successfully transfer or apply replicated data. Common causes include:

- **Network communication issues:** Packet loss, high network latency, firewall restrictions, routing issues, or MTU mismatches disrupting communication between ISE nodes.
- **Replication service issues:** RabbitMQ, JGroups, or other internal replication services are unavailable, restarting, or not functioning correctly.
- **Node communication issues:** The destination node is offline, restarting, de-registered, disconnected from the deployment, or otherwise unreachable.

- **Database synchronization issues:** The destination node is unable to commit the replicated data because of database errors or synchronization failures.
- **System resource constraints:** High CPU utilization, memory pressure, insufficient disk space, or heavy disk I/O delaying replication processing.
- **DNS or hostname resolution issues:** Incorrect forward or reverse DNS resolution preventing successful communication between nodes.
- **Version or deployment inconsistencies:** Replication fails if nodes are not operating on supported software versions or if the deployment is in an inconsistent state after an upgrade or node registration.
- **Admin Certificate Expiry:** Admin certificate for the ISE nodes is expired /corrupted / invalid because of which the communication between the nodes is at stake leading to the replication failure.
- **Queue Link Errors:** The deployment or the affected node(s) are showing the queue link errors where the ISE messaging certificate / ISE Root CA chain is corrupted or invalid on the port 8671.
- **Stunnel service is disabled / offline:** Stunnel service runs in all the nodes of the distributed deployment. Disabled / not running status of the Stunnel service results in the Replication failed alarms.
- **Replication ports are blocked:** The ports 12001, 8671,443 8443 and 6379 must be open between the nodes in the deployment and network for seamless Replication procedures in the deployment.

Impact of the Alarm

The impact depends on the type of data being replicated. Replication failures can result in inconsistent configuration across ISE nodes, delayed propagation of administrative changes, outdated policies, missing network devices or identity information, certificate synchronization failures, and inconsistent endpoint data. If replication remains unsuccessful for an extended period, administrative operations and policy consistency across the deployment can be affected.

Replication Stopped

The "Replication Stopped" alarm is generated when the Primary Administration Node is unable to replicate the information to the secondary nodes of the deployment. This alarm indicates that the replication process has failed and the affected node(s) no longer have the latest configuration or operational data.

Reason for Alarm

The "Replication Stopped" alarm can occur when Primary Administration Node is unable to successfully transfer the replicated data. Common causes include:

- **Network communication issues:** Packet loss, high network latency, firewall restrictions, routing issues, or MTU mismatches disrupting communication between ISE nodes.
- **Replication service issues:** RabbitMQ, JGroups, or other internal replication services are unavailable,

restarting, or not functioning correctly in the Primary Administration node.

- **System resource constraints:** High CPU utilization, memory pressure, insufficient disk space, or heavy disk I/O delaying replication processing in the Primary Administration Node.
- **DNS or hostname resolution issues:** Incorrect forward or reverse DNS resolution preventing successful communication between nodes.
- **Version or deployment inconsistencies:** Replication fails if nodes are not operating on supported software versions or if the deployment is in an inconsistent state after an upgrade or node registration.
- **Admin Certificate Expiry:** Admin certificate for the ISE nodes is expired /corrupted / invalid because of which the communication between the nodes is at stake leading to the replication failure.
- **Queue Link Errors:** The deployment or the affected node(s) are showing the queue link errors where the ISE messaging certificate / ISE Root CA chain is corrupted or invalid on the port 8671.
- **Stunnel service is disabled / offline:** Stunnel service runs in all the nodes of the distributed deployment. Disabled / not running status of the Stunnel service results in the Replication failed alarms.
- **Replication ports are blocked:** The ports 12001, 8671,443 8443 and 6379 must be open between the nodes in the deployment and network for seamless Replication procedures in the deployment.

Impact of the Alarm

When replication stops, the nodes in the deployment no longer receives configuration updates from the Primary Administration Node. This can result in inconsistent policies, outdated network device definitions, missing endpoint information, certificate synchronization delays, and configuration mismatches across the deployment. If replication remains stopped for an extended period, administrative changes made on the Primary PAN cannot take effect on the affected node until synchronization is restored.

Troubleshoot Replication Failed and Replication Stopped Alarm

Slow Replication Alarm

Whenever a configuration change is made on the Primary PAN, Cisco ISE places the change in the replication queue and synchronizes it to the secondary nodes. Under normal conditions, replication is completed within a short period. However, if the replication queue begins to build up or the destination node takes longer than expected to process replication requests, Cisco ISE generates a Slow Replication alarm.

Cisco ISE classifies these alarms into three severity levels:

- Slow Replication Info
- Slow Replication Warning
- Slow Replication Error

Reason for Alarm

The "Slow Replication" alarm is typically generated due to temporary conditions that delay replication processing. Common causes include:

- **Temporary system resource utilization:** Short periods of high CPU utilization, memory usage, or increased disk I/O can delay replication processing.
- **Network latency:** Brief increases in network latency or minor packet loss between ISE nodes can slow data transfer.
- **Large configuration changes:** Bulk endpoint imports, policy updates, certificate imports, or other large administrative changes increase the amount of data to be replicated.
- **Background system operations:** Backup, restore, purge, patch installation, or upgrade activities temporarily increase system load.
- **Replication queue backlog:** Multiple configuration changes performed within a short period can temporarily increase the replication queue.
- **Temporary service delays:** RabbitMQ, JGroups, or database services experience brief processing delays while continuing to function normally.

Slow Replication Alarm - Info

Slow or stuck replication is detected when the pending message count exceeds 10000 or time taken to replicate messages is more than an hour.

Verification: Verify the pending synchronization message count. Navigate to **Administration > System > Deployment**, select the affected node, and click the **Information (i)** icon to review the number of pending replication messages.

Slow Replication Alarm - Warning

Slow or stuck replication is detected when the pending message count is greater than 20000 or the time taken to replicate messages exceeds three hours.

Verification: Verify the pending synchronization message count. Navigate to **Administration > System > Deployment**, select the affected node, and click the **Information (i)** icon to review the number of pending replication messages.

Slow Replication Alarm - Error

Slow or stuck replication is detected when the pending message count is greater than 40000 or the time taken to replicate messages exceeds five hours.

Verification: Verify the pending synchronization message count. Navigate to **Administration > System > Deployment**, select the affected node, and click the **Information (i)** icon to review the number of pending replication messages.

Troubleshoot Node Replication Alarms

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 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.

5. 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.

6. Verify DNS Resolution

Cisco ISE replication relies on successful communication between all nodes in the deployment. For inter-node communication to function correctly, the nodes must be reachable, and both forward and reverse DNS resolution must be configured and functioning properly. DNS resolution issues can prevent nodes from communicating, resulting in replication failures.

To verify the DNS resolution in the ISE nodes, Log in to the Cisco ISE CLI and use the **nslookup** command to verify both forward and reverse DNS resolution for each node in the deployment.

For example:

- **Forward DNS lookup:** The command **nslookup www.example.com** must return the IP address of the corresponding Cisco ISE node.
- **Reverse DNS lookup:** The command **nslookup 10.x.x.1** must return the fully qualified domain name (FQDN) of the corresponding Cisco ISE node.

7. Admin & ISE Messaging Certificate Verification

Cisco ISE uses the **Admin certificate** and the **ISE Messaging certificate** to establish secure inter-node communication required for replication. If either certificate is **invalid**, **expired**, **corrupted**, or **untrusted**, replication between the deployment nodes can fail.

To verify the certificate status, navigate to **Administration > System > Certificates**, select the affected node, and review the **Admin** and **ISE Messaging** certificates. Verify that the certificates are valid, have not expired, are trusted, and are in a healthy state.

If either the **Admin certificate** or the **ISE Messaging certificate** is invalid, corrupted, or expired, replace or renew the certificate. Once the certificate issue is resolved, replication resumes after secure communication between the nodes is re-established.

Note: Refer ISE Queue Link errors and Install Certificates in ISE for more information on the renewal of certificates.

---

8. Verify the status of ISE Stunnel service

The **Stunnel** service in Cisco ISE is an internal service that provides **secure SSL/TLS tunneling** for communication between ISE components and external services. Rather than implementing TLS encryption independently in every application, ISE uses Stunnel as a wrapper that adds SSL/TLS encryption to services that communicate over plain TCP. This improves security while simplifying the implementation of secure communications.

The **Stunnel** service must be in the **Running** state on all nodes in the Cisco ISE deployment for replication to function correctly. The service depends on valid **ISE Admin** and **ISE Messaging** certificates to establish secure TLS communication between nodes during the replication process. The service status can be verified from the Cisco ISE CLI using the command **show tech-support | include stunnel**

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