Contents

Introduction

This document describes the feature that improves user experience and allows certificate deletion cluster wide.

Prerequisites

Requirements

Cisco recommends that you have knowledge of

Components Used

This document is not restricted to specific software and hardware 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, make sure that you understand the potential impact of any command.

Background Information

There are certain certificates on CUCM and IM&P which are replicated transparently (without the Admin's knowledge). This means that if a certificate is uploaded by the Admin on one server, it is pushed to the other servers within the cluster. This is done to support the Extension Mobility Cross Cluster *(*EMCC) feature.

Previously, in a huge cluster if there was a requirement to delete an unrequired certificate, the admin needed to login into each of the servers and delete the certificate manually. Additionally, if this is not done within a stipulated window, the deleted certificate might reappear because of the CertSync service that runs every 30 minutes, which ensures that the file system and certificate tables are in sync. To avoid this issue, customers today disable the CertSync service on all the nodes followed by certificate deletion on all the nodes. This makes the user experience very bad.

With the new feature enhancement such instances will not occur.

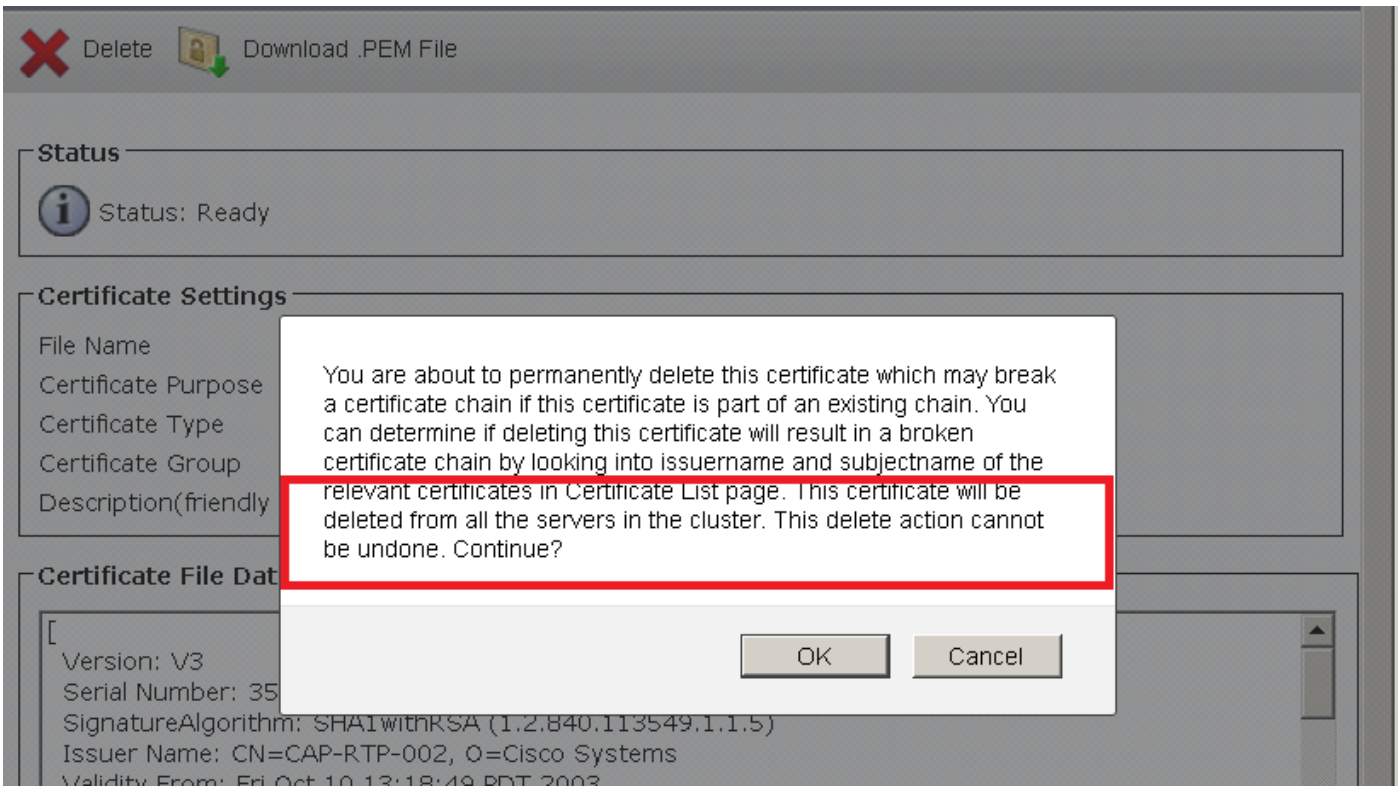
This feature ehancement to the certificate management provides you the ability to automatically delete a certificate from all the nodes in the cluster.

When a certificate is deleted from one node in the cluster, it will get deleted from all other nodes in the cluster.

Configure

On Cisco Call Manager, navigate to **Cisco Unified OS Administration > Under Security > Certificate Management**

Select the certificate which needs to be deleted. You will see this:



Once you click **OK**, these steps will take place:

1. The certificate will be deleted locally on the server.

2. If the certificate is deleted successfully, then the platform Event will be triggered. This platform event will be sent to all the servers in the cluster (CUCM and IM&P). The information present in the platform event is the unit type (CallManager, Tomcat or Phone-SAST) along with the name of the certificate (for example, RootCA.pem). The platform event gives us the ability to trigger the delete event cluster wide.

The Certificate delete operation is only applicable for these certificates:

CUCM

1. tomcat-trust

2. CallManager-trust

3. Phone-SAST-trust

CUCM IM& Presence

1. tomcat-trust

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

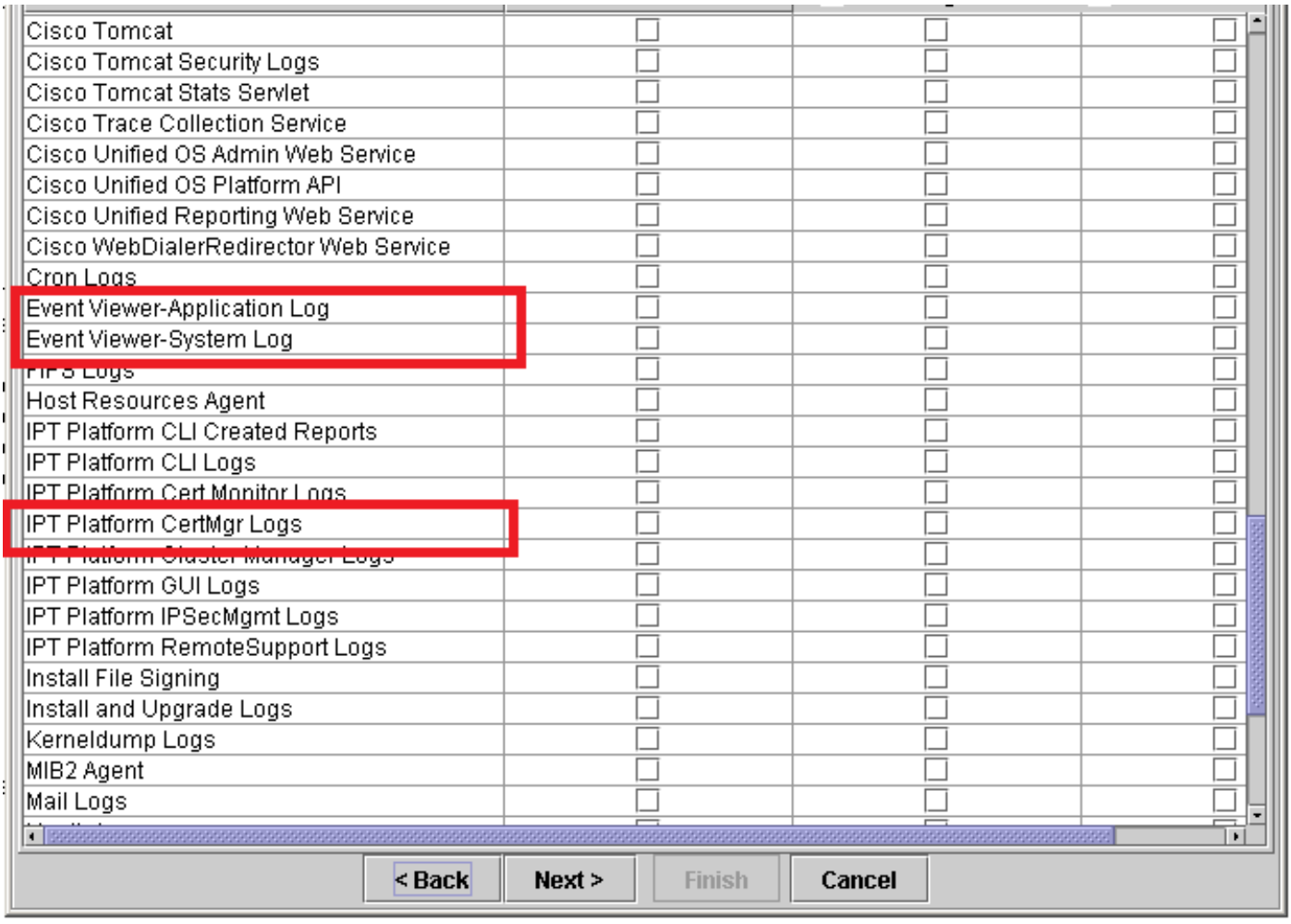
This section provides information you can use to troubleshoot your configuration.

If the certificates on the other nodes in the cluster are not deleted, collect these logs from RTMT, to troubleshoot this issue .

1. Event Viewer-Application Log

2. Event Viewer-System Log

3. IPT Platform CertMgr Logs



Sample message:

Jul 6 03:12:05 CM11 user 6 ilog_impl: Received request for platform-event (--no-wait platform-event-clusterwide-certificate-delete HOSTNAME=CM11Sub UNIT=tomcat-trust Type=certs-trust NAME=testcert.pem).

This log indicates that an event has been received by the other nodes in the cluster to delete the certificate testcert, when the certificate is deleted on one node.

From the certMgmt Logs for the delete operation:

This log shows that cert Mgmt has received the request for the deletion of the certificate certificate.pem in tomcat_trust:

decode: true

op: delete

unit: tomcat-trust

keystoreUnit:tomcat-trust

logFile: /var/log/active/platform/log/cert-mgmt.log

resultFile: /var/log/active/platform/log/certde-info.xml

keyDir: /usr/local/cm/.security/tomcat/keys

certDir: /usr/local/cm/.security/tomcat/trust-certs/Certificate.pem

This log shows that the certificates are deleted from the Database:

2016-07-06 01:31:55,374 INFO [main] - IN -- CertDBAction.java - deleteCertificateInDB(certInfo) -