安全证书管理增强

目录

简介

本文档介绍可改善用户体验并允许证书删除集群范围的功能。

先决条件

要求

思科建议您了解Cisco Unified Communication Manager(CUCM)11.0及更高版本。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

CUCM和IM&P上有某些证书是透明复制的（管理员不知情）。 这意味着，如果证书由管理员上传到一台服务器上，则会将其推送到集群内的其他服务器。这是为了支持跨群集分机移动(EMCC)功能。

以前，在大型集群中，如果需要删除不需要的证书，管理员需要登录每台服务器并手动删除证书。此外，如果未在规定的窗口内完成此操作，则删除的证书可能会重新出现，因为每30分钟运行一次的CertSync服务可确保文件系统和证书表保持同步。为避免此问题，客户现在禁用所有节点上的CertSync服务，然后在所有节点上删除证书。这会使用户体验非常糟糕。

使用新功能增强功能时，不会出现此类实例。

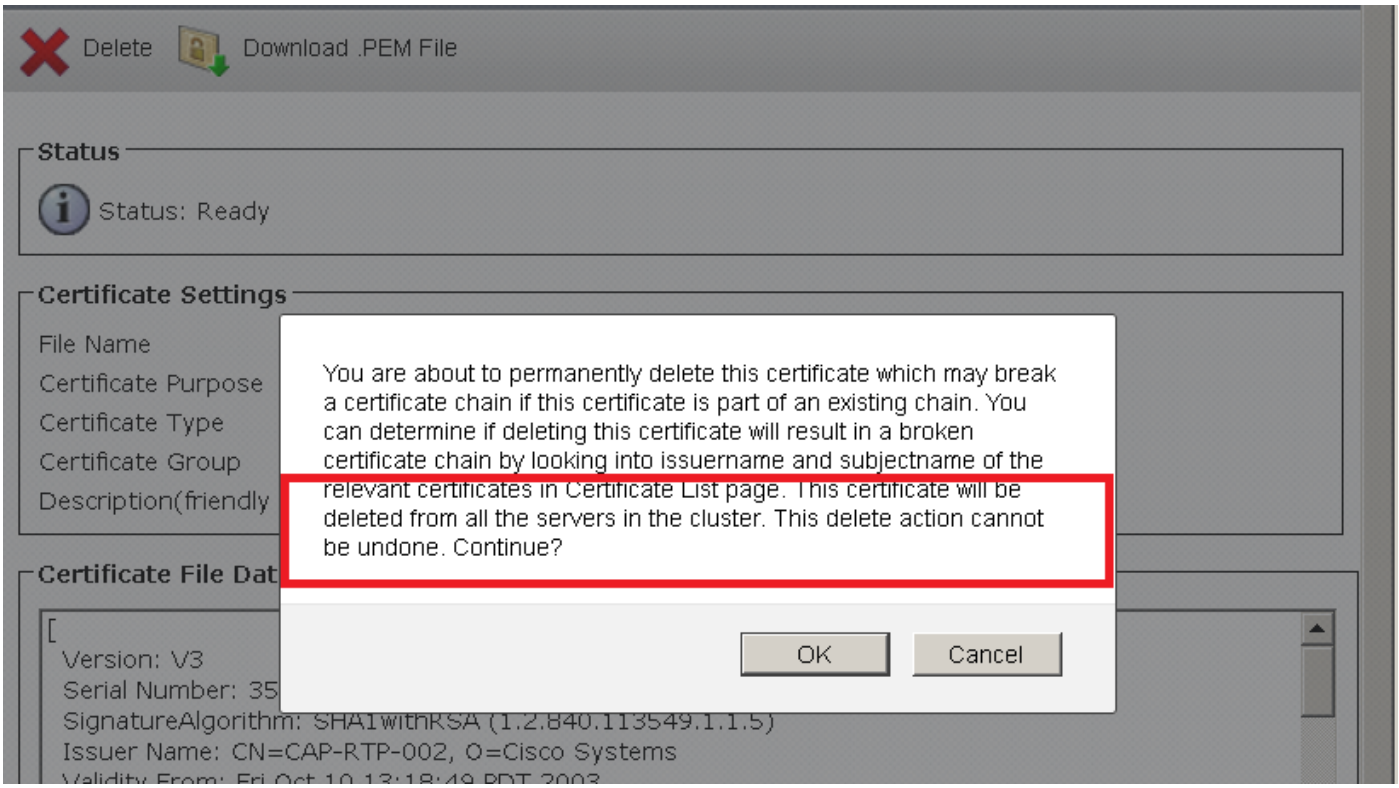
此功能增强到证书管理，使您能够从集群中的所有节点自动删除证书。

当证书从集群中的一个节点删除时，将从集群中的所有其他节点删除该证书。

配置

在Cisco Call Manager上，导航至Cisco Unified OS Administration **> Under Security > Certificate Management**

选择需要删除的证书。您将看到：



单击"**确定**"后，将执行以下步骤：

1.证书将在服务器上本地删除。

2.如果证书已成功删除，则将触发平台事件。此平台事件将发送到集群中的所有服务器（CUCM和IM&P）。 平台事件中的信息是设备类型（CallManager、Tomcat或Phone-SAST）以及证书的名称（例如RootCA.pem）。 平台事件使我们能够触发整个删除事件集群。

证书删除操作仅适用于以下证书：

CUCM

1.tomcat-trust

2. CallManager-trust

3. Phone-SAST-trust

CUCM即时消息和在线状态

1.tomcat-trust

验证

当前没有可用于此配置的验证过程。

故障排除

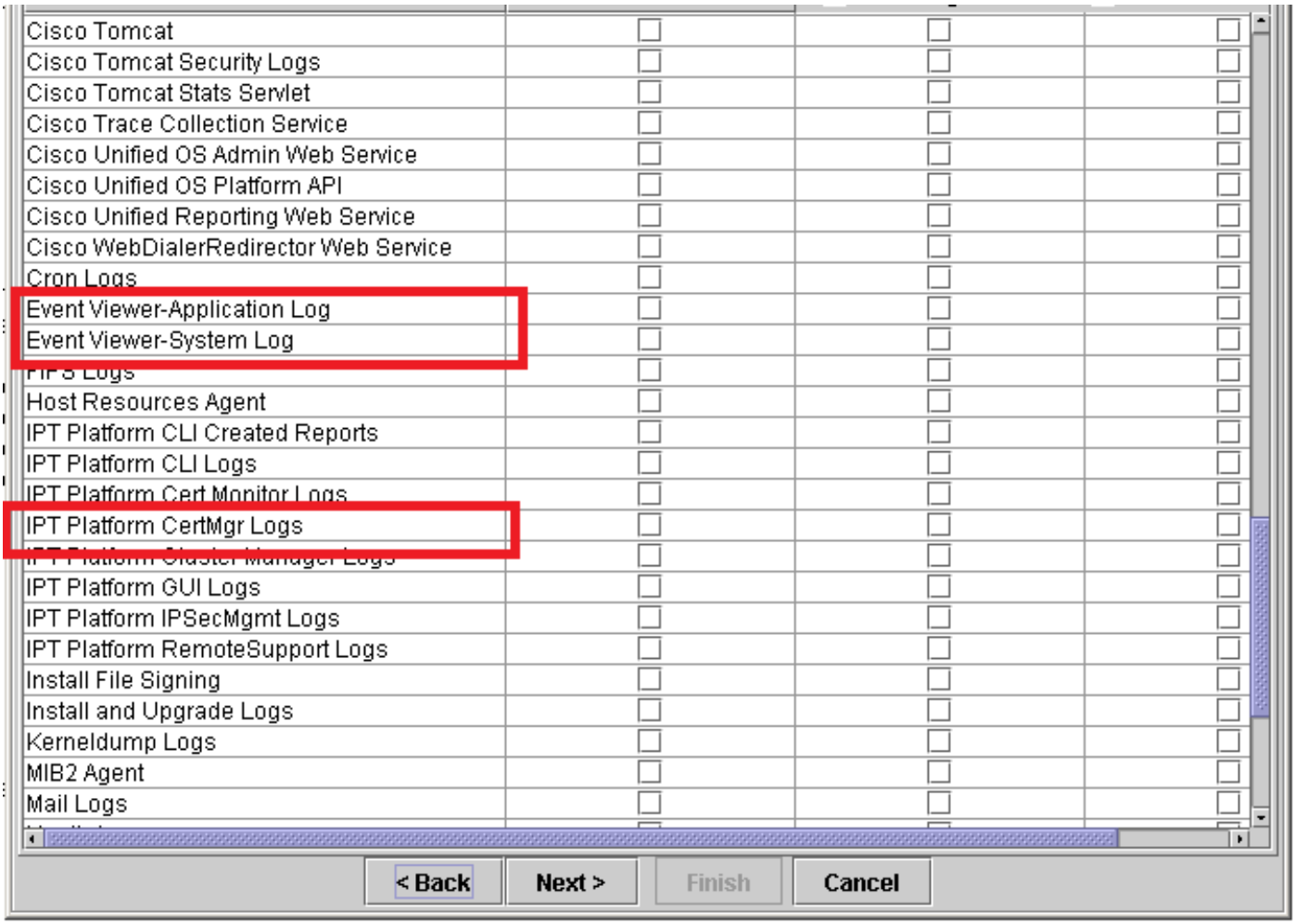
本部分提供的信息可用于对配置进行故障排除。

如果未删除集群中其他节点上的证书，请从RTMT收集这些日志以排除此问题。

1.事件查看器 — 应用程序日志

2.事件查看器 — 系统日志

3. IPT平台CertMgr日志



示例消息：

7月6日03:12:05 CM11用户6 ilog_impl:已收到平台事件请求(-no-wait platform-event-clusterwide-certificate-delete HOSTNAME=CM11Sub UNIT=tomcat-trust Type=certs-trust NAME=testcert.pem)。

此日志表示当证书在一个节点上删除时，集群中的其他节点已接收事件以删除证书testcert。

从certMgmt Logs中执行删除操作：

此日志显示证书管理已收到删除tomcat_trust中的certificate.pem的请求：

解码：　真

op:　delete

单元:　tomcat-trust

keystoreUnit:tomcat-trust

日志文件：　/var/log/active/platform/log/cert-mgmt.log

结果文件：/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

此日志显示证书已从数据库中删除：

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