MULECLIENTCERT Renewal SOP

Overview

Renewing the MULECLIENTCERT is a critical task that requires careful planning and execution to ensure minimal downtime and a smooth transition. As a Site Reliability Engineer (SRE), you should follow a Standard Operating Procedure (SOP) to perform the MULECLIENTCERT renewal. Below is a general outline for the MULECLIENTCERT renewal SOP for an SRE:

Pre-Renewal Preparation:

Verify Certificate Expiration:

* Check the current expiration date of the MULECLIENTCERT.
* Plan the renewal process at least 30 days before the expiration date.

Take Pre-Renewal Backup:

* Take a backup of the existing MULECLIENTCERT and its configuration.
* Store the backup securely in case of any issues during the renewal process.

Rollback Plan:

* Have a rollback plan in case any issues arise. This may involve reverting to the previous MULECLIENTCERT or using other mitigation strategies.

Check Compatibility:

* Ensure the new MULECLIENTCERT is compatible with the current Mulesoft Runtime Fabric (RTF) version.

Communication:

Notify Stakeholders:

* Inform all relevant stakeholders about the upcoming MULECLIENTCERT renewal, including API developer team, support and operations teams, and other relevant parties like executives and managers.

**NOTE**: There must be a contact list and method of contact maintained centrally for such communication/notification.

Change Control Process:

* Follow the Change Control process and get approval from the Change Control board to execute the change.

Schedule Downtime:

* Schedule a maintenance window for the renewal, considering the least impactful time for your users.
* The maintenance window should be within the approved change window (10:00PM PST -- 4:00AM PST).

Renewal Process:

Generate New MULECLIENTCERT:

* Generate a new MULECLIENTCERT following the Mulesoft documentation and best practices.

Update MULECLIENTCERT Configuration:

* Update the MULECLIENTCERT configuration in the Mulesoft Runtime Fabric.
* Ensure all necessary components are configured to use the new MULECLIENTCERT.

Validation:

* Validate the renewed MULECLIENTCERT by running tests against critical workloads and applications.
* Check APIs and proxies are running properly with the new MULECLIENTCERT.

Post-Renewal Tasks:

Verify System Health:

* Check the current health of the Mulesoft Runtime Fabric and associated components.
* Continue monitoring the system post-renewal to catch any issues that might arise.

Notify Stakeholders:

* Inform all relevant stakeholders about the successful MULECLIENTCERT renewal and request them for sanity and regression testing.

Incident Response Plan (IRP):

Incident Identification:

* **Responsibility:** Monitoring Team, SRE Team
* **Procedure:**
  + Use monitoring tools to identify any issues related to the MULECLIENTCERT renewal.
  + Set up alerts for certificate-related failures or application health.

Incident Triage and Escalation:

* **Responsibility:** Incident Response Team
* **Procedure:**
  + Quickly assess the severity of the incident and assign priorities based on impact and urgency.
  + Escalate to relevant teams (e.g., Mulesoft support, application teams) based on the nature of the incident.

Incident Mitigation:

* **Responsibility:** SRE Team, Operations Team
* **Procedure:**
  + Follow the rollback plan if necessary, reverting to the previous MULECLIENTCERT.
  + Apply temporary fixes or workarounds to minimize impact.
  + Communicate ongoing actions to the Incident Response Team.

Communication Plan:

* Establish a communication plan for notifying stakeholders in case of issues and keep them informed about progress.
* Define the frequency of updates and include key information: incident description, current status, next steps.
* Identify key stakeholders and their contact details, including the Mulesoft Operations Team, Development Teams, Product Managers, Customer Support, and Executive Team.
* Determine the communication methods, such as email, Slack channels, and phone/text alerts.

Post-Mortem:

* Conduct a post-mortem analysis after the MULECLIENTCERT renewal to identify areas of improvement and prevent similar issues in future renewals.
* Follow the post-mortem process, including post-incident analysis, post-mortem meeting, documenting findings, action items, sharing lessons learned, and continuous improvement.