OKLAHOMA
Office of Management
& Enterprise Services

API Management Standard

Introduction

MuleSoft is the standard for integrations, ESB, API management, API gateway, API catalog and message brokers at OMES.

Purpose

The purpose of this document is to provide a roadmap of standard policy and best practices when developing on the MuleSoft platform for the state. This standard defines and outlines the procedures MuleSoft developers should use when building integrations, APIs, deploying apps, publishing apps to Exchange, managing consumption and monitoring and alerting when developed by or for OMES.

Definitions

ESB – Enterprise Service Bus.
API – Application Programming Interface.
MuleSoft – Software for connecting SaaS and enterprise applications in the cloud and on-premises.
C4E – Center 4 Enablement.
VPC – Virtual Private Cloud.
CloudHub – Integration platform as a service.
HTTP – Hypertext Transfer Protocol
TLS – Transport Layer Security
MUnit – Testing software designed to test individual units of source code to see if they are fit for use or not.

Standard

General

- The State of Oklahoma provides the Anypoint platform to all agencies within the MuleSoft Anypoint organization called ok-omes.
- The Anypoint platform offers agencies separate tenants that are independently accessed through business groups and are secured trough the Teams feature.
- Mule applications run in CloudHub or on-premises with approval from C4E.
- New Mule applications shall be developed using the latest version.
- Existing Mule applications are expected to run on a version of Mule that is covered by extended support.

Architecture

- Each agency defines local environments in its own Anypoint business group.
  - This allows agencies to adapt to the logical Anypoint environment construct to their specific needs.
- MuleSoft applications need to follow the design patterns developed by the OMES architecture group to optimize experience, scalability and promote reuse.
- The architecture of the current VPC configuration is available for review and discussion during the development on-boarding and is available here.
- Any proposed platform solutions need to be presented and approved by the C4E.

Network

- Mule applications are deployed in one of two dedicated OMES AWS Virtual Private Clouds that are USA based.
- OMES provides one VPC for production applications and another for non-production applications.
- Each agency must designate the non-production VPC as its default VPC and explicitly map the production environment to the production VPC.
- Each VPC configures firewall rules to specifically allow inbound traffic to the CloudHub workers where the Mule applications run.
    - These firewall rules apply to the entire VPC and therefore affect all agencies' business groups.
- Each VPC is connected to the OMES network using IPSec.
    - As additional OMES networks require connectivity with CloudHub VPCs, the IPSec tunnel routing must be explicitly updated to including appropriate routes.
- Each agency's APIs are access to subdomains that reflect the agency's name.
    - E.g., oesc.oklahoma.gov

Security

- User access to the Anypoint platform control plane is governed by security roles and permissions mapping.
    - The latest documented guidelines are located here.
    - Inbound and outbound traffic to each VPC, which constitutes the runtime plane, is principally allowed in OMES Palo Alto firewalls that are owned by Network Operations.
- The CloudHub Dedicated Load Balancer must be configured with OMES-signed SSL certificates that are provisioned by the OMES Entrust Tenant.
- To make an API accessible, an OMES Anypoint administrator must configure a specific mapping rule in the CloudHub Dedicated Load Balancer.
- All publicly available APIs require HTTP over TLS 1.2.
- A Mule application should call another Mule API through the CloudHub Dedicated Load Balancer using HTTP over TLS 1.2.
- Mule APIs are, by default, reachable from the public internet.
- Exposing Mule APIs to external consumers over the internet is a controlled process that requires the documented approval of CyberCommand.
- APIs must be protected by a client ID enforcement policy or a suitable alternative. Using a dedicated set of credentials that is issued by the Anypoint platform and is maintained by Anypoint platform users is recommended.
- Alternative out-of-the-box or custom security policies may be configured with the approval of CyberCommand.
- Credentials are issued by the Anypoint platform to an Anypoint user.
    - Specifically, production credentials are encrypted in source-code configuration files in GitHub and are included in the deployed application archive in their encrypted form.
- Mule application credentials are encrypted in source-code configuration files in GitHub and are included in the deployed application archive in their encrypted form.
- Each agency has one or more production encryption keys that are used to encrypt secrets for all applications controlled by that agency.
- Azure Key Vault is approved as a preferred alternative to encrypting secret in source code.
- Each agency has a set of Azure Key Vaults that are environment specific.
- Mule applications use agency-specific service principles to differentially enable access to production and non-production key vaults.

- Users access the Anypoint Platform Control Plane based on their group membership in Azure Active Directory.
- Azure DevOps agents use the Anypoint platform API to deploy Mule applications with a connected app that acts on its own behalf.
- Deployment to production is only performed through the Azure DevOps release pipeline.
    - Deployment to test/user access test should be performed through the Azure DevOps release pipeline.

Development

- MuleSoft integrations should be designed according to API Led Connectivity.
- APIs are implemented as Mule applications using APIKit.
- Mule applications include automated tests within MUnit.
- A default template for an OMES Mule application is in Anypoint Exchange.
- Agency-specific templates should be published to their respective Anypoint Exchange business group.
- Published guidelines for logging and error handling may be found here.
- All Mule application source code is maintained in the agency's assigned GitHub.com tenant or a shared OMES-owned tenant.

Development Environment

- Anypoint Studio is used to develop Mule applications using OMES issued devices or virtual machines.
    - The minimum version of Anypoint Studio is 7.12.0.
    - Download it here.
- Anypoint Studio is specifically configured to support the development of OMES compliant Mule applications.

Monitoring

- Applications are expected to log to OMES Splunk, CloudHub and Anypoint Monitoring.
- CloudHub applications are expected to log to Splunk using the OMES Splunk System API and not all logs are expected to be directed to Splunk.
- Applications must avoid logging sensitive information to any of the log destinations.
- Logs should be traceable across Mule applications and, where possible, more broadly across the entire network.
    - i.e., API clients and backends.
- The CloudHub worker monitoring agent should be enabled for each CloudHub application.

CICD

- Applications are built using Apache Maven leveraging a MuleSoft specific plugin.
- Applications are built in Azure DevOps build pipelines and are deployed by Azure DevOps release pipelines.
- Deployment to production requires an approved change control record.
- Steps to build and prepare release in Azure DevOps are provided here and here.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- Mule Application Development.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 1/31/2023	**Review cycle:** Annual
Last revised: 1/18/2023	**Last reviewed:** 8/14/2023
Approved by: Joe McIntosh, Chief Information Officer	