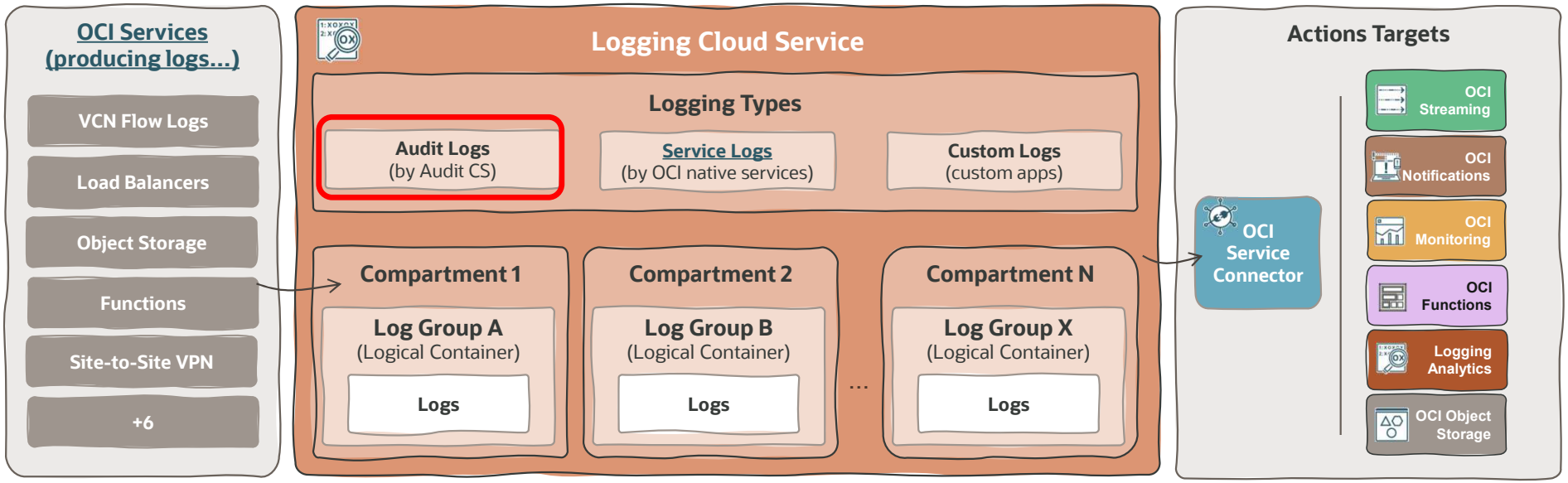
Audit Logs integration Patterns Microsoft Sentinel

Date:

Author:

OCI LOGGING | CLOUD NATIVE LOGGING

<<workflow>>



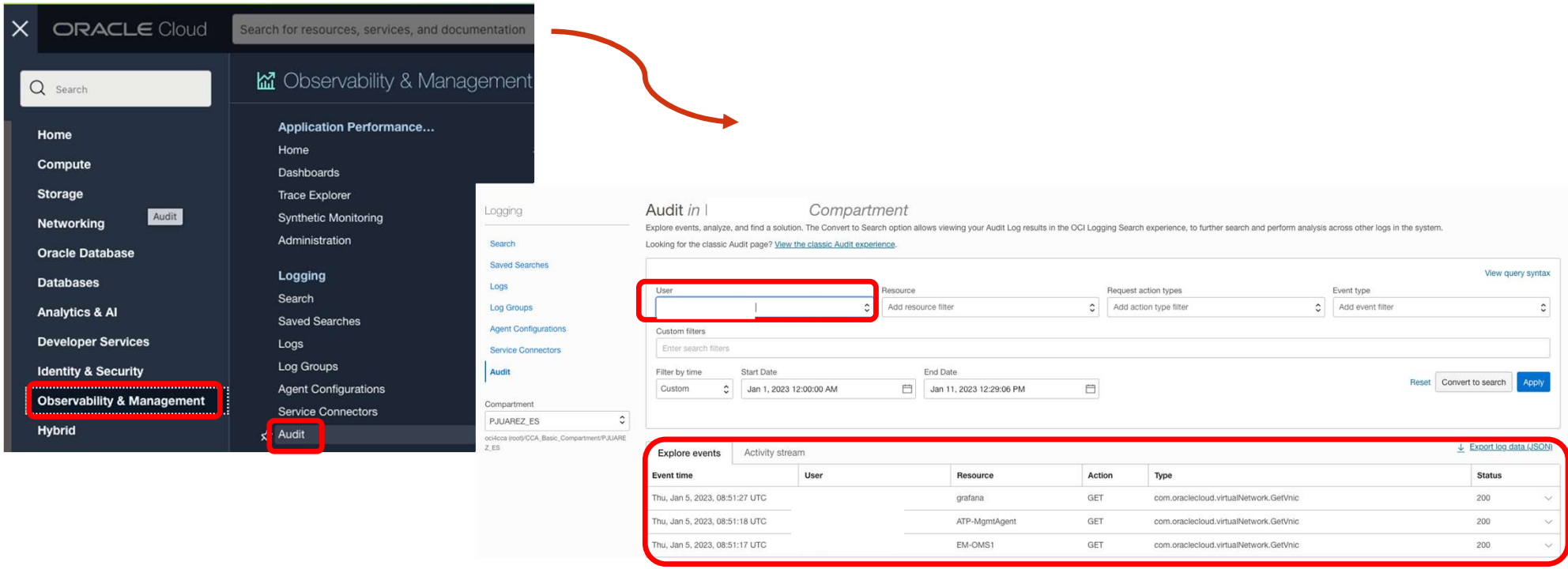
AUDIT LOGS EVENTS

Logs related to events emitted by the Oracle Cloud Infrastructure Audit service.

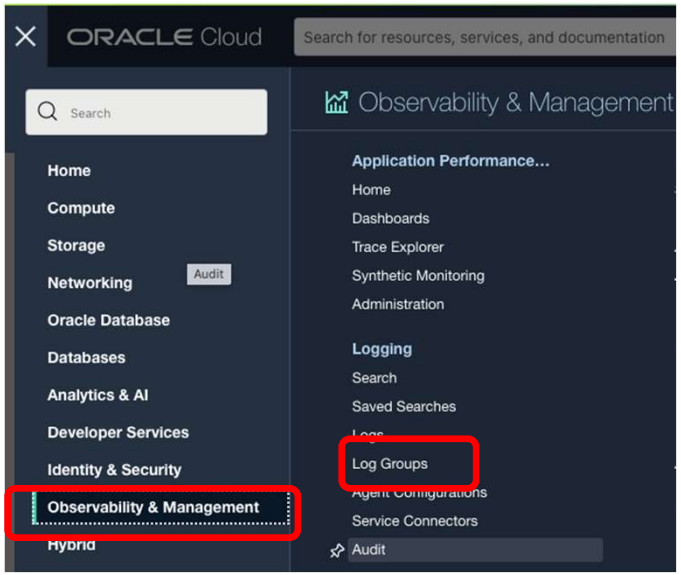
These logs are available from the Logging **Audit** page, or are searchable on the **Search** page alongside the rest of your logs.

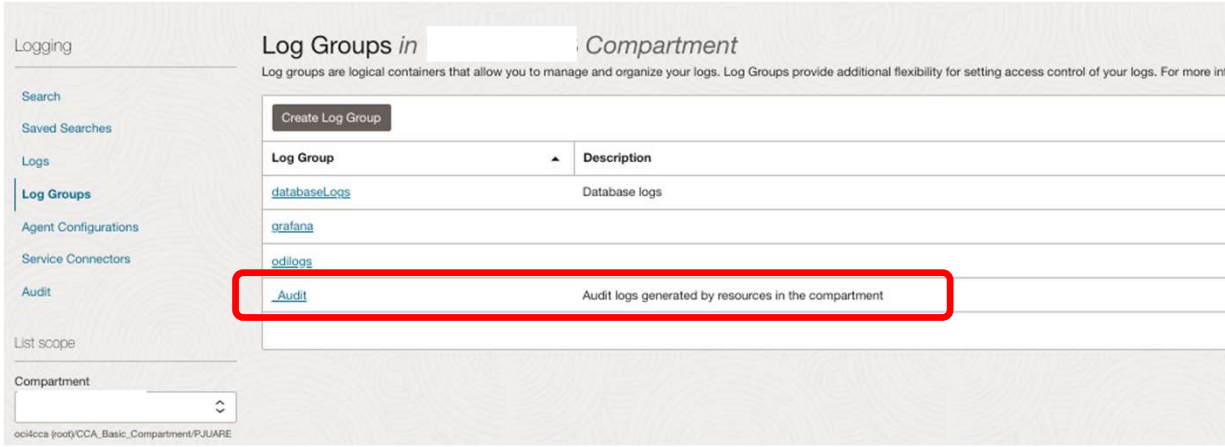
Audit logs capture the information about API calls made to public endpoints throughout your tenancy. These include API calls made by the Console, Command Line Interface (CLI), Software Development Kits (SDK), your own custom clients, or other Oracle Cloud Infrastructure services.

OCI Logging | How To | Example with Audit logs



OCI Logging | How To | Example with Audit logs

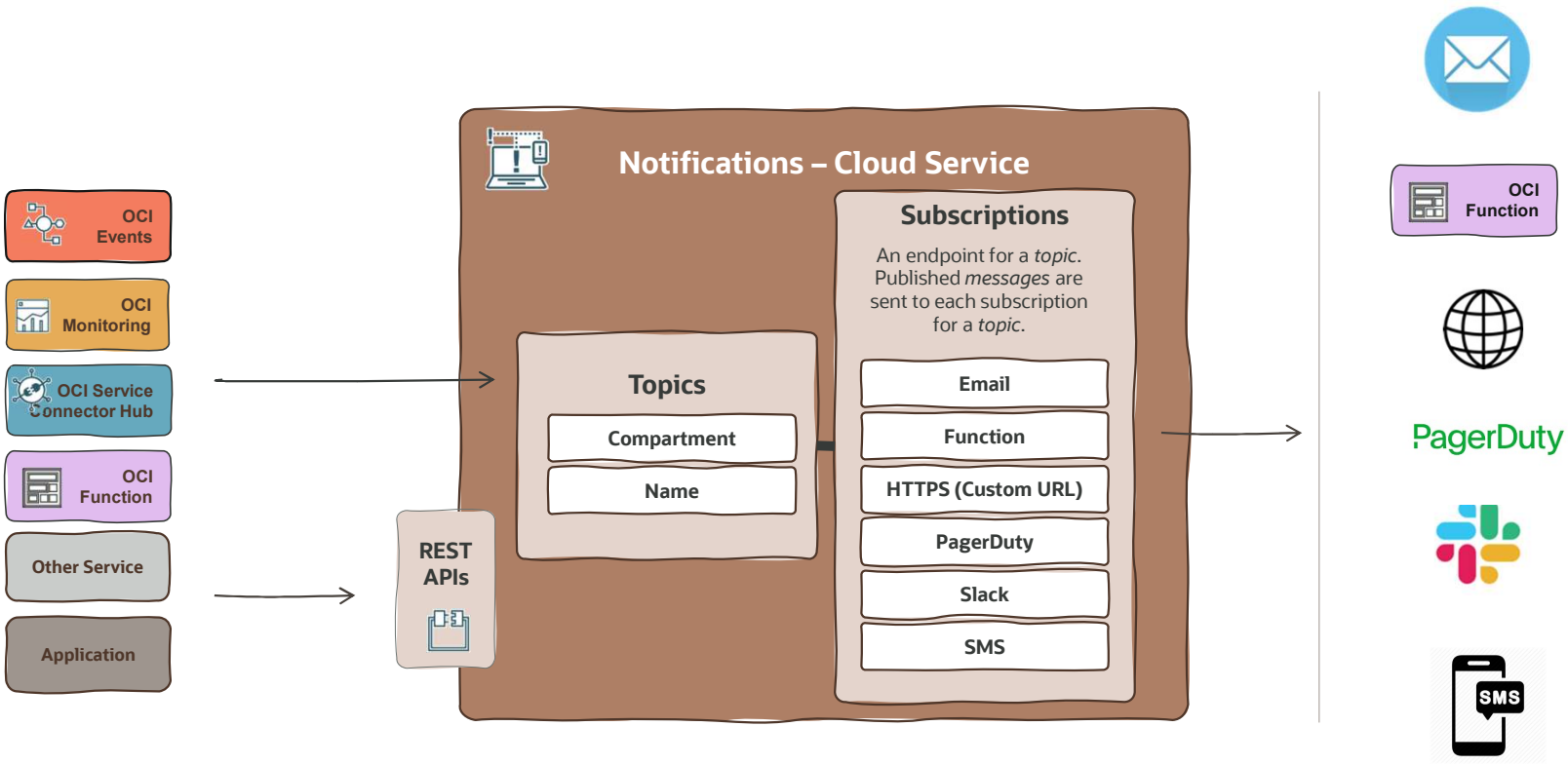




2. SENTINEL-OCI INTEGRATION

2.1 OCI INTREGRATION SERVICES

OCI NOTIFICATION | Basic Integrations

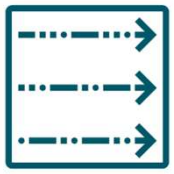


OCI SERVICES | Custom Integrations

OCI FUNTIONS

- Oracle Functions is a fully managed, multi-tenant, highly scalable, on-demand, **Functions-as-a-Service** platform. It is built on enterprise-grade OCI and powered by the **Fn Project** open source engine.
- **Use Oracle Functions** when you integrate solutions or systems, transform messages payload, aggregate data, code business rules or specific requirements, extend existing behaviours or data flows, etc…

OCI STREAMING



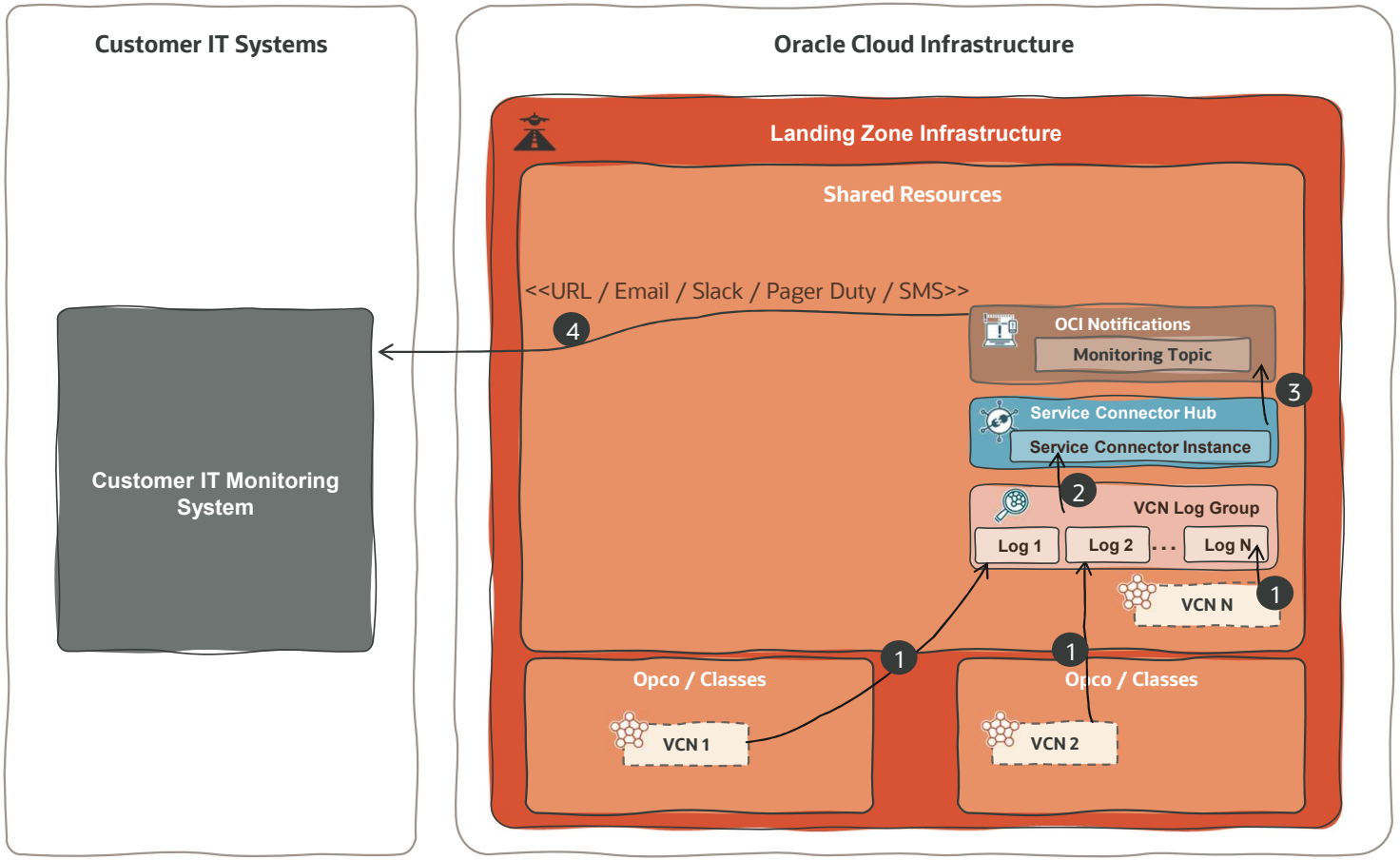
- This service provides a fully managed, scalable, and durable solution for **ingesting and consuming high-volume data streams in real-time**.
- **Use Streaming** for any use case in which data is produced and processed continually and sequentially in a publish-subscribe messaging model.

OCI SERVICE CONNECTOR HUB

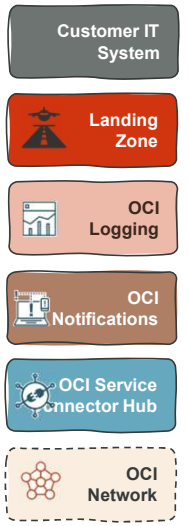
- OCI Service Connector Hub is a **cloud message bus** platform that offers a single pane of glass for describing, executing, and monitoring interactions when moving data between Oracle Cloud Infrastructure services.
- **Use the Service Connector Hub service** to transfer data between services in Oracle Cloud Infrastructure.

2.2 LOG GENERIC INTEGRATION PATTERNS

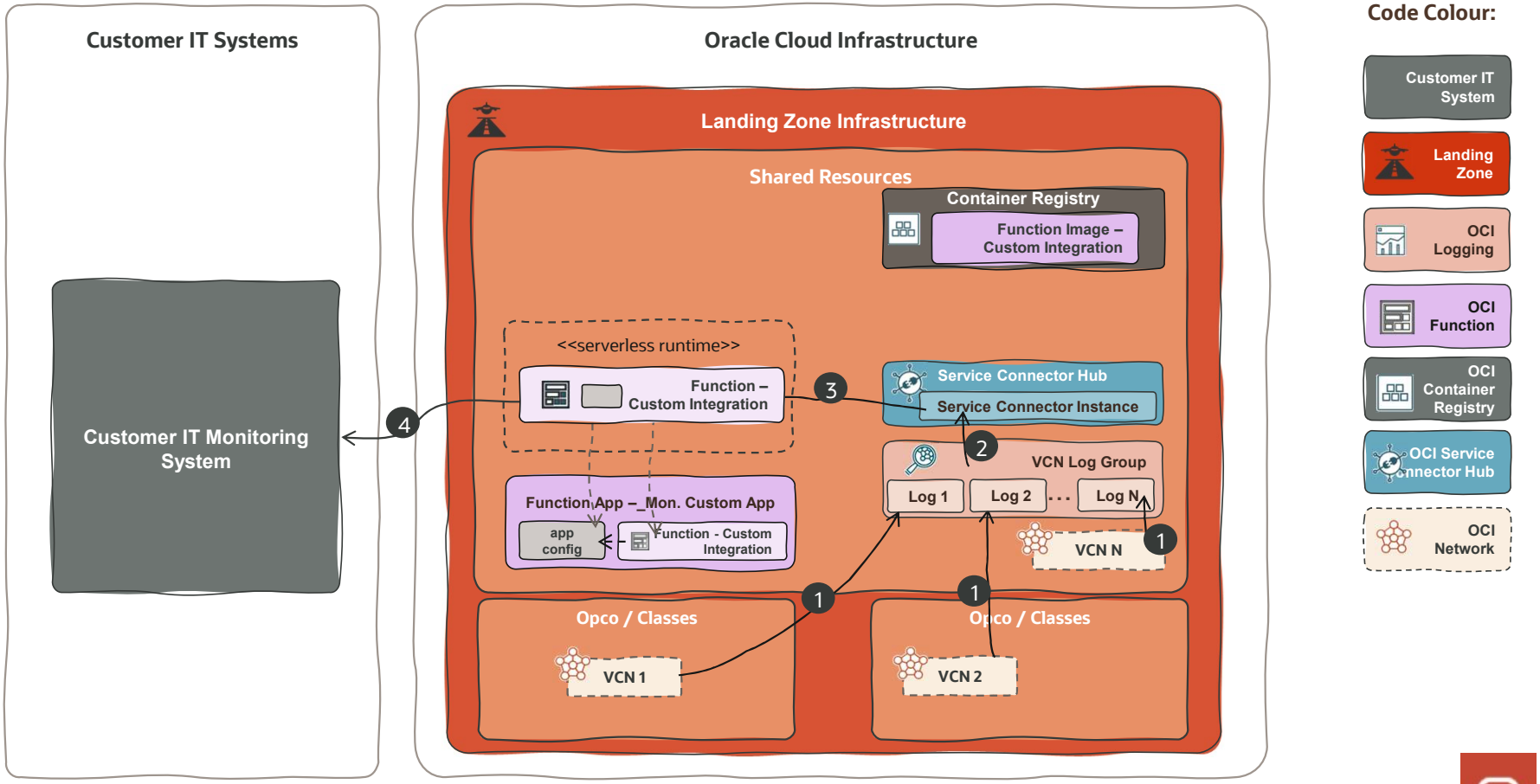
Pushing OCI Logs to a Third-Party | Notifications (OOTB)



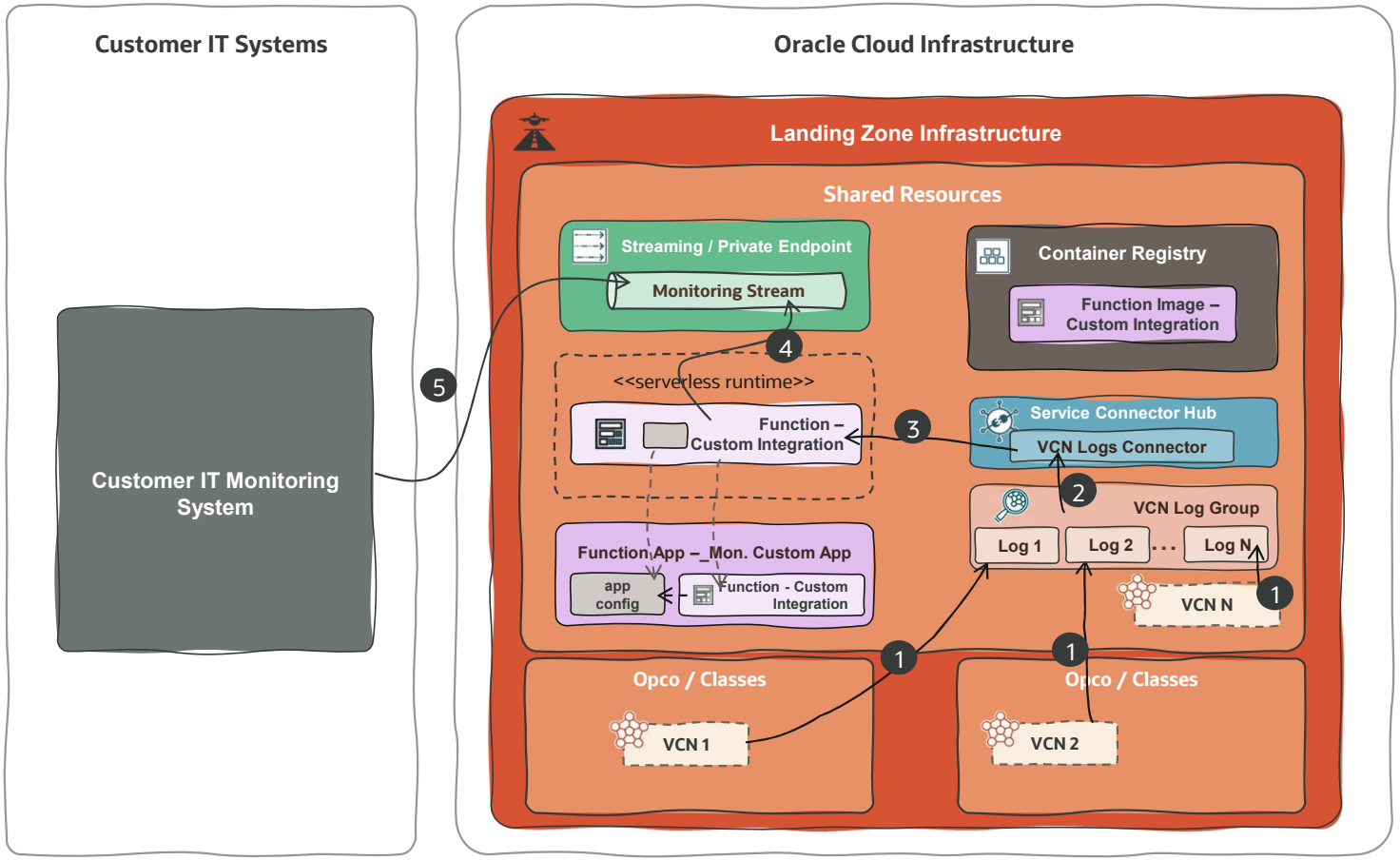
Code Colour:



Pushing OCI Logs to a Third-Party | Functions



Streaming OCI Logs to a Third-Party

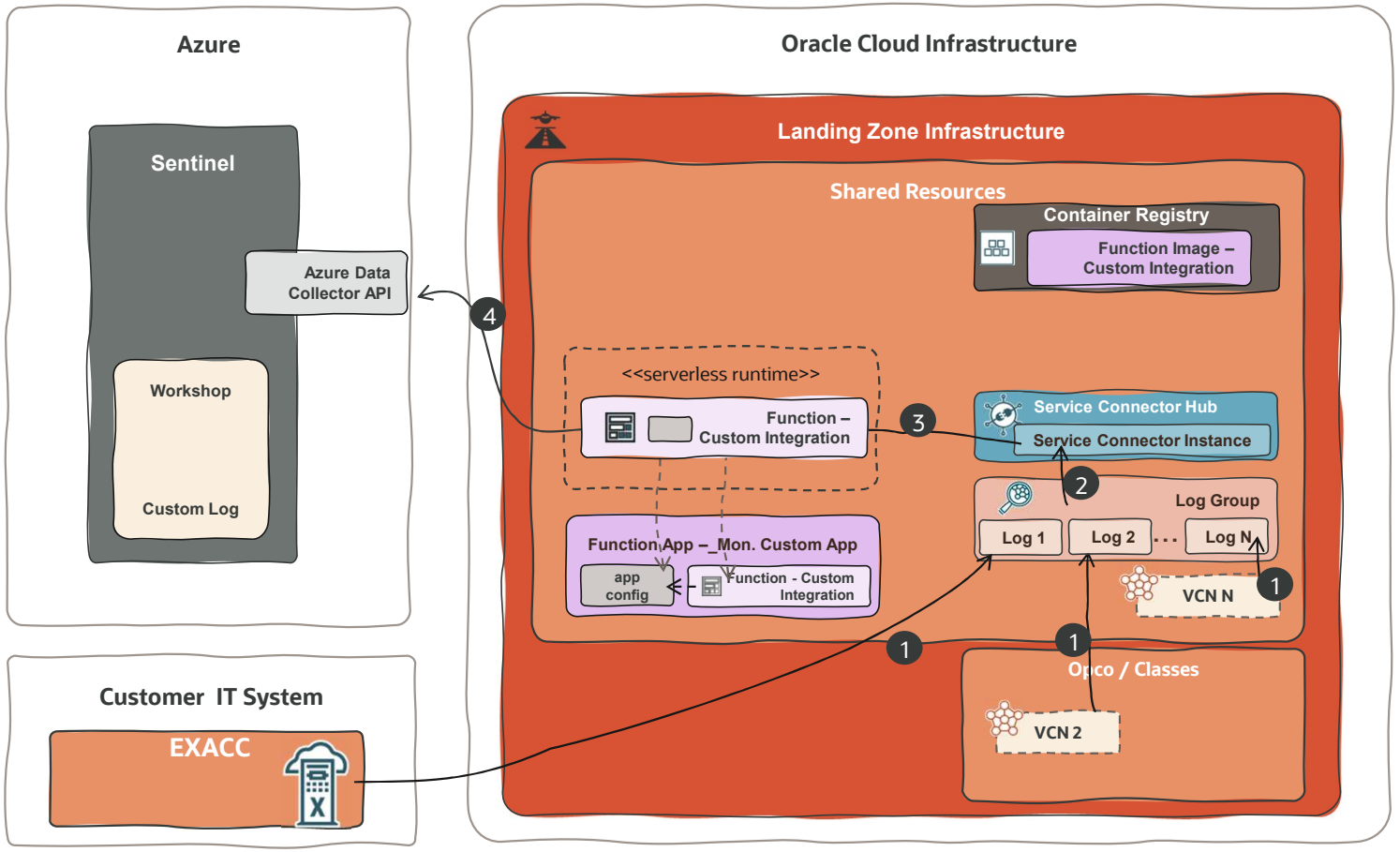


Code Colour:

- Customer IT System
- Landing Zone
- OCI Logging
- OCI Streaming
- OCI Function
- OCI Container Registry
- OCI Service Connector Hub
- OCI Network

2.3 OCI LOGGING -> SENTINEL

Option A) Pushing OCI Audit Logs to Azure Sentinel | Functions



Code Colour:

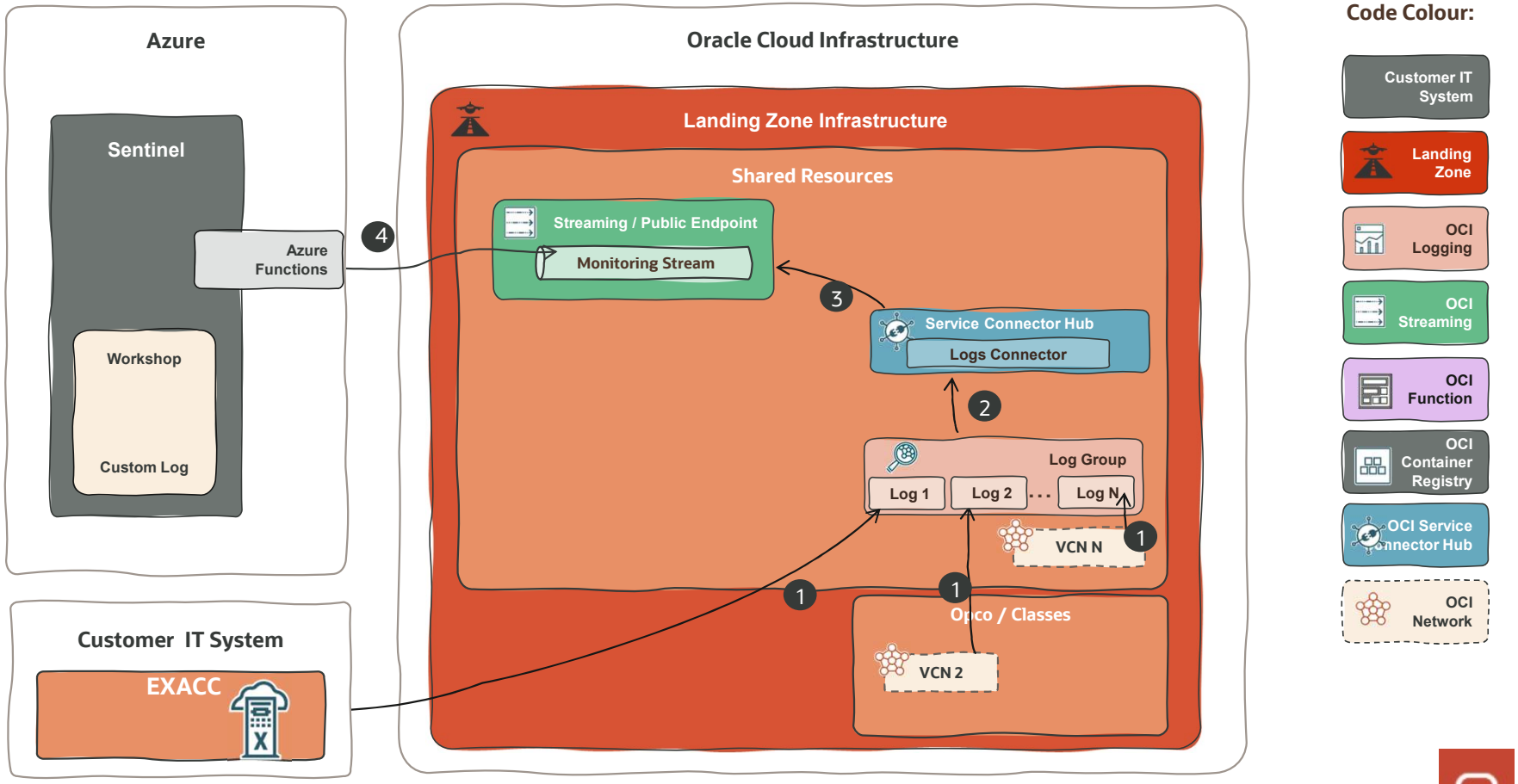
- Customer IT System
- Landing Zone
- OCI Logging
- OCI Function
- OCI Container Registry
- OCI Service Connector Hub
- OCI Network

Pushing OCI Audit Logs to a Azure Sentinel | Functions

https://blogs.oracle.com/cloud-infrastructure/post/using-microsoft-azure-sentinel-siem-tools-with-oci-logging-service

https://docs.oracle.com/en/learn/oci-logs-ms-azure-sentinel/index.html

Option B) Streaming OCI Logs to Azure Sentinel | Azure Functions (public)



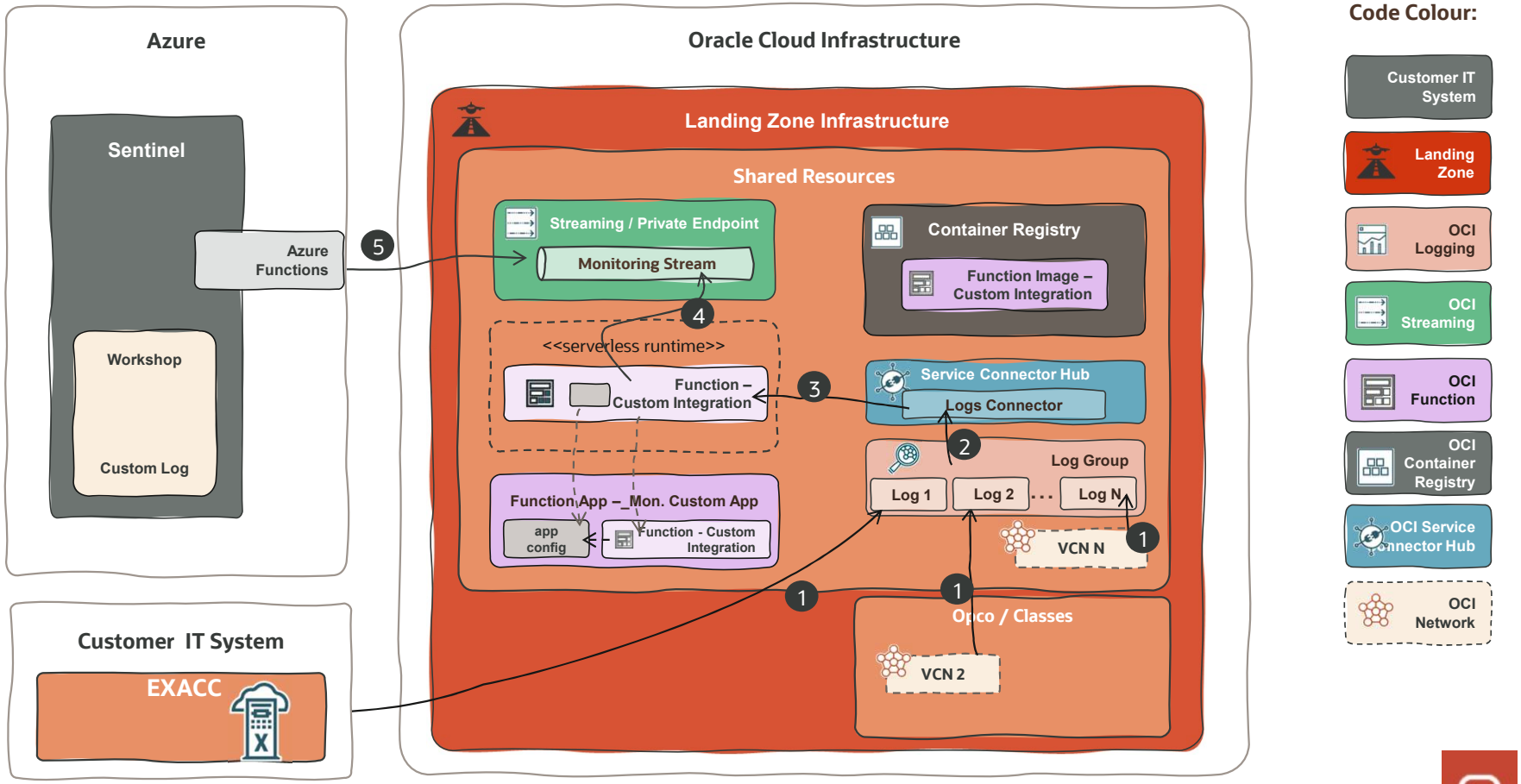
Streaming OCI Logs to Azure Sentinel | Functions

https://learn.microsoft.com/en-us/azure/sentinel/data-connectors/oracle-cloud-infrastructure-using-azure-function

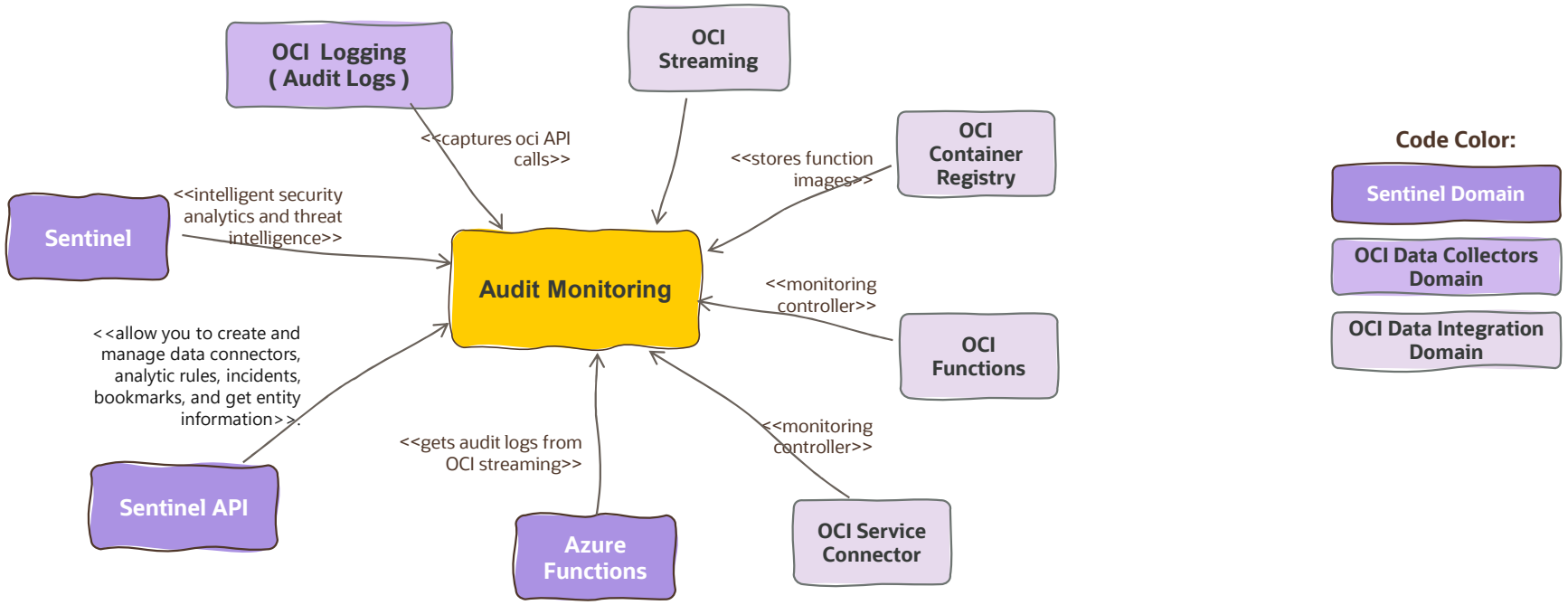
https://www.youtube.com/watch?v=tnBH0frIMP0

Option B) Streaming OCI Logs to Azure Sentinel | Azure Functions (private)

Requirement:
OCI - Azure interconnect (VPN)



Monitoring System Context



THANKS