August 2022

Enterprise Log Aggregation

Matt Boardman

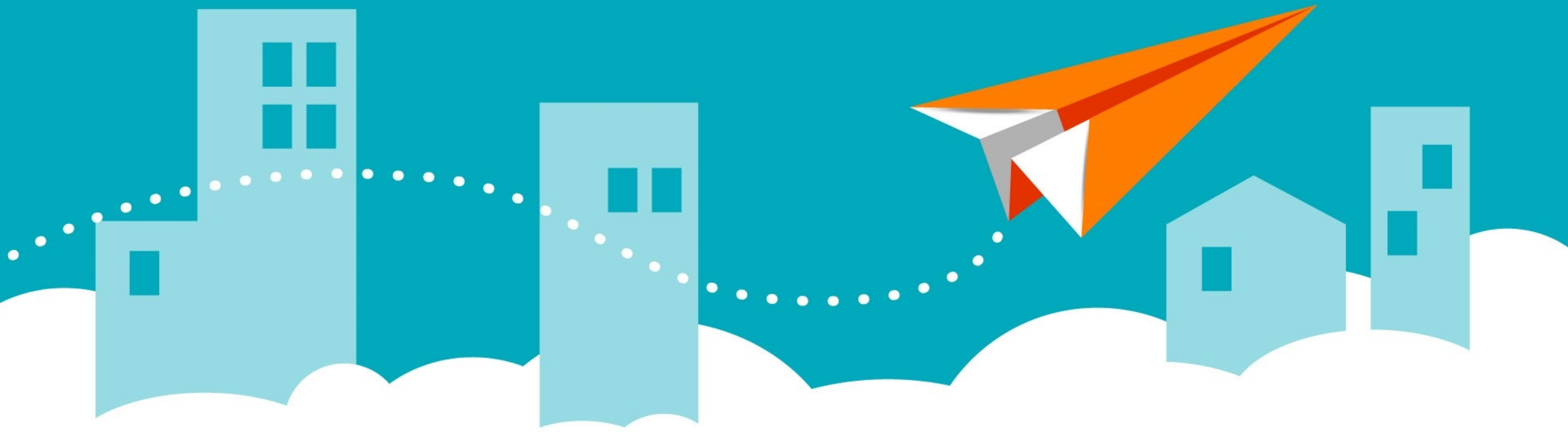
Informatica Professional Services

Agenda

What is Enterprise Log Aggregation?
ICDM Operational Insights Service
Example Solution Architecture
Informatica ICDM Platform API
Demo: Extract Logs from Informatica Cloud
Demo: Example Dashboard using Microsoft Power BI
Using a Document Store Database (MongoDB)
Demo: Extract Logs from Secure Agents
Reference: Links to ICDM API Documentation

Informatica

Enterprise Log Aggregation



Informatica

Enterprise Log Aggregation

- Gain Insight into Cross-Application Operational Metrics at an Enterprise Level

- Objectives
  - Tuning and Optimization, Process Orchestration, Predictive Analytics
  - Security, Real-Time Threat Detection, Auditing, Regulatory Compliance

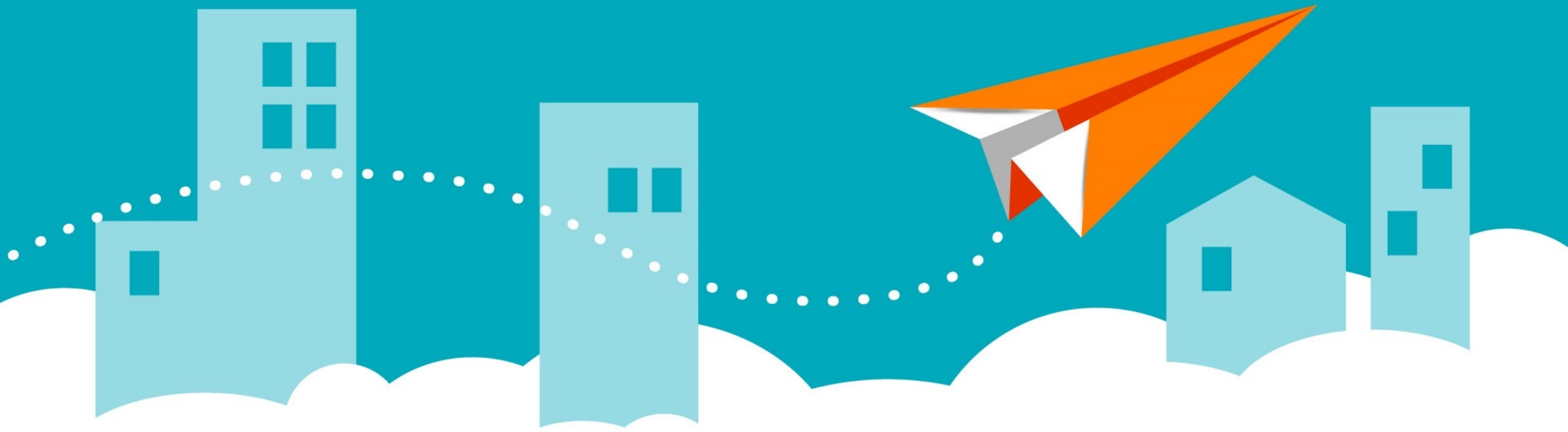
- Commercial Log Aggregation Tools
  - Splunk Enterprise
  - ELK Stack: Elasticsearch, Logstash, Kibana (Open Source)
  - AWS CloudWatch
  - Azure Monitor (formerly Azure Log Analytics)
  - Google Cloud Logging

Informatica

Enterprise Log Aggregation

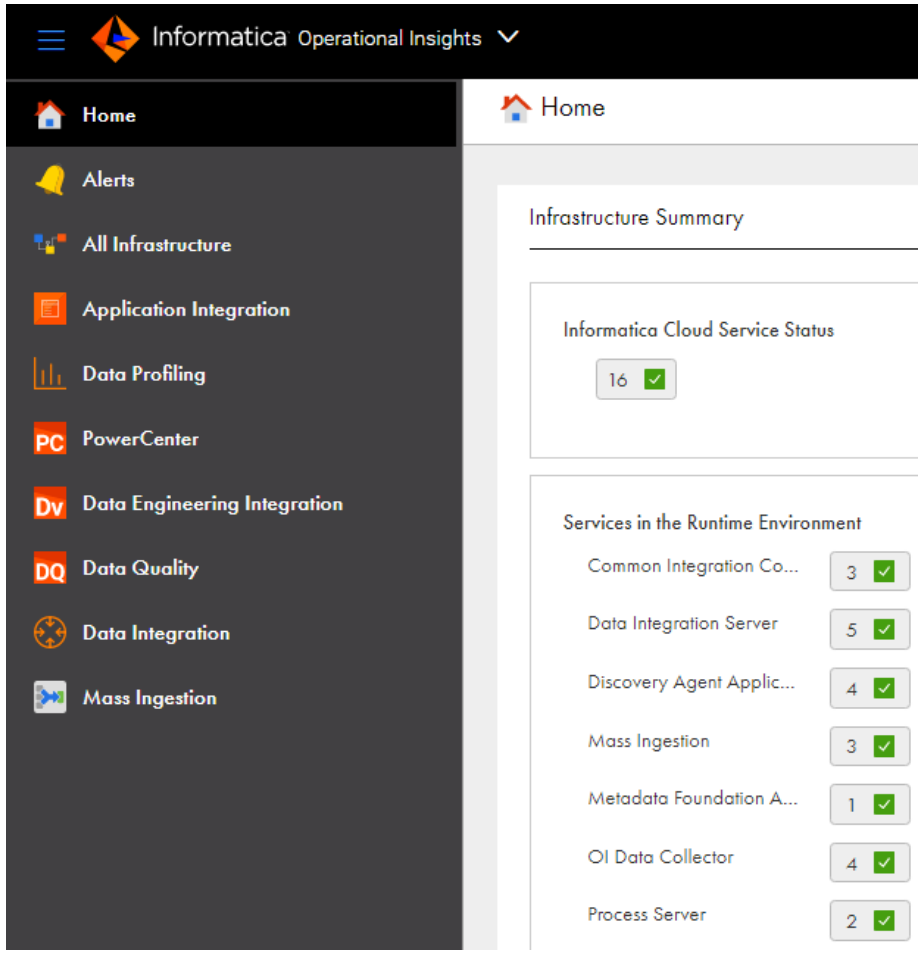
- Operations:
  - Single at-a-glance dashboard, one place to check
  - RCA of Intermittent Failures: what else is happening when a process fails on one system
  - Network failure prediction: identify outages and disruptions before they happen
- Developers:
  - Long-running processes: Informatica doesn't know if an Oracle index gets dropped
  - Slowly-increasing runtimes: Informatica doesn't know if an Oracle tablespace is growing larger
  - Process orchestration tuning and optimization across multiple applications

ICDM Operational Insights



Informatica

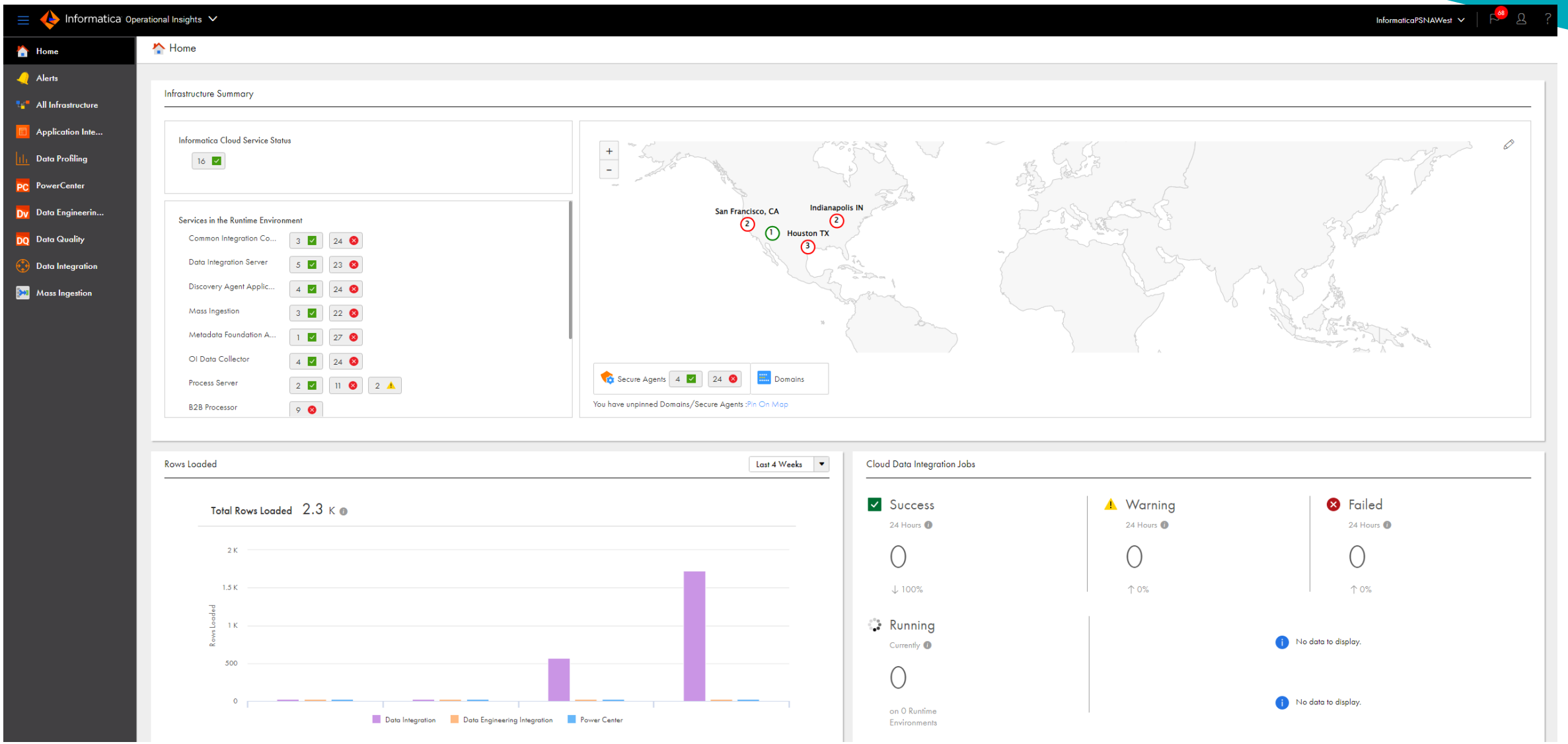
Operational Insights Service



- Provides Informatica Status Dashboards
  - ICDM Cloud Status, Secure Agents Status
  - Infrastructure Monitoring: PC, IDQ, DEI, IICS
  - CDP: Data Profiling
  - CDI: Data Integration
  - CAI: Application Integration
  - CMI: Mass Ingestion
- Provides Infrastructure Email Alerts
  - IICS Secure Agent offline
  - CPU, Memory, Disk over threshold

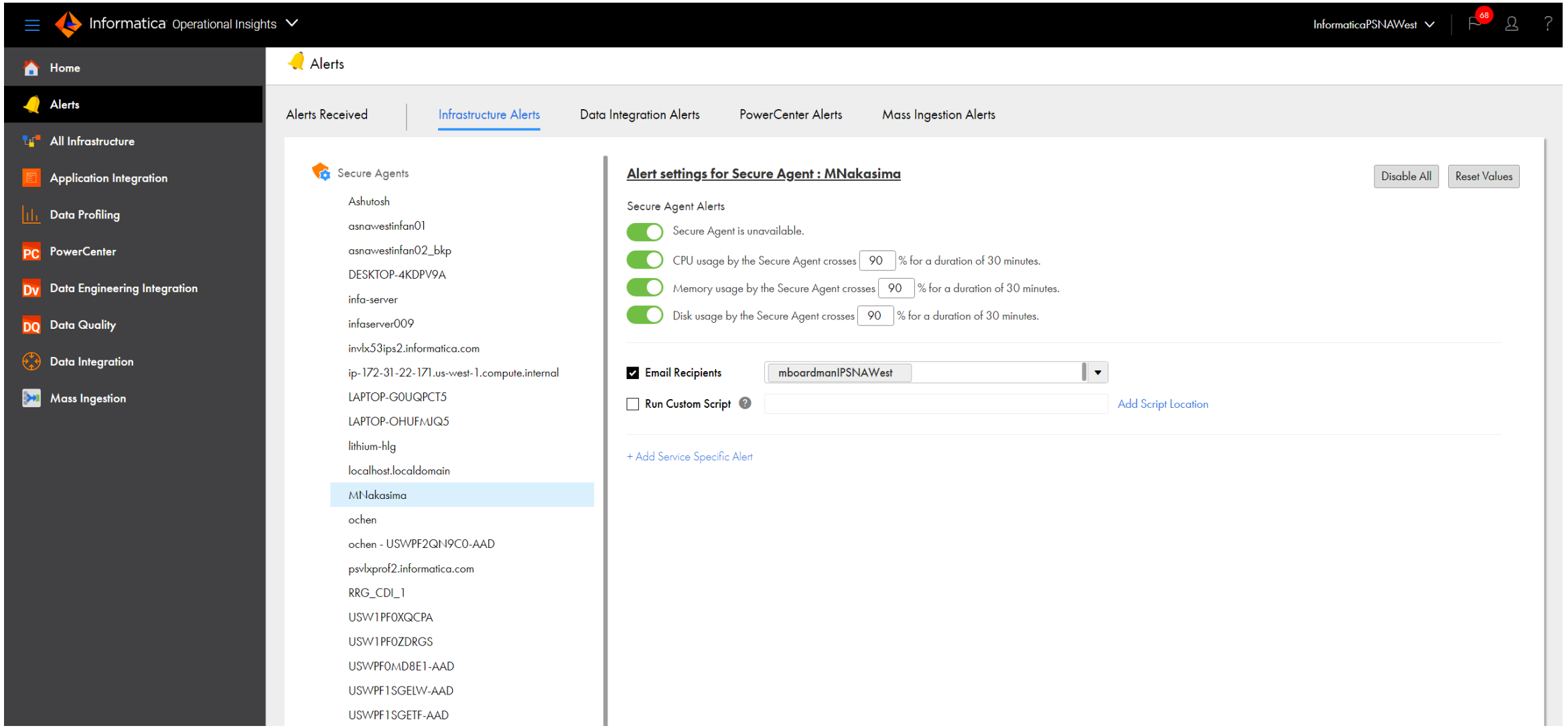
Informatica

Cloud Status Dashboard



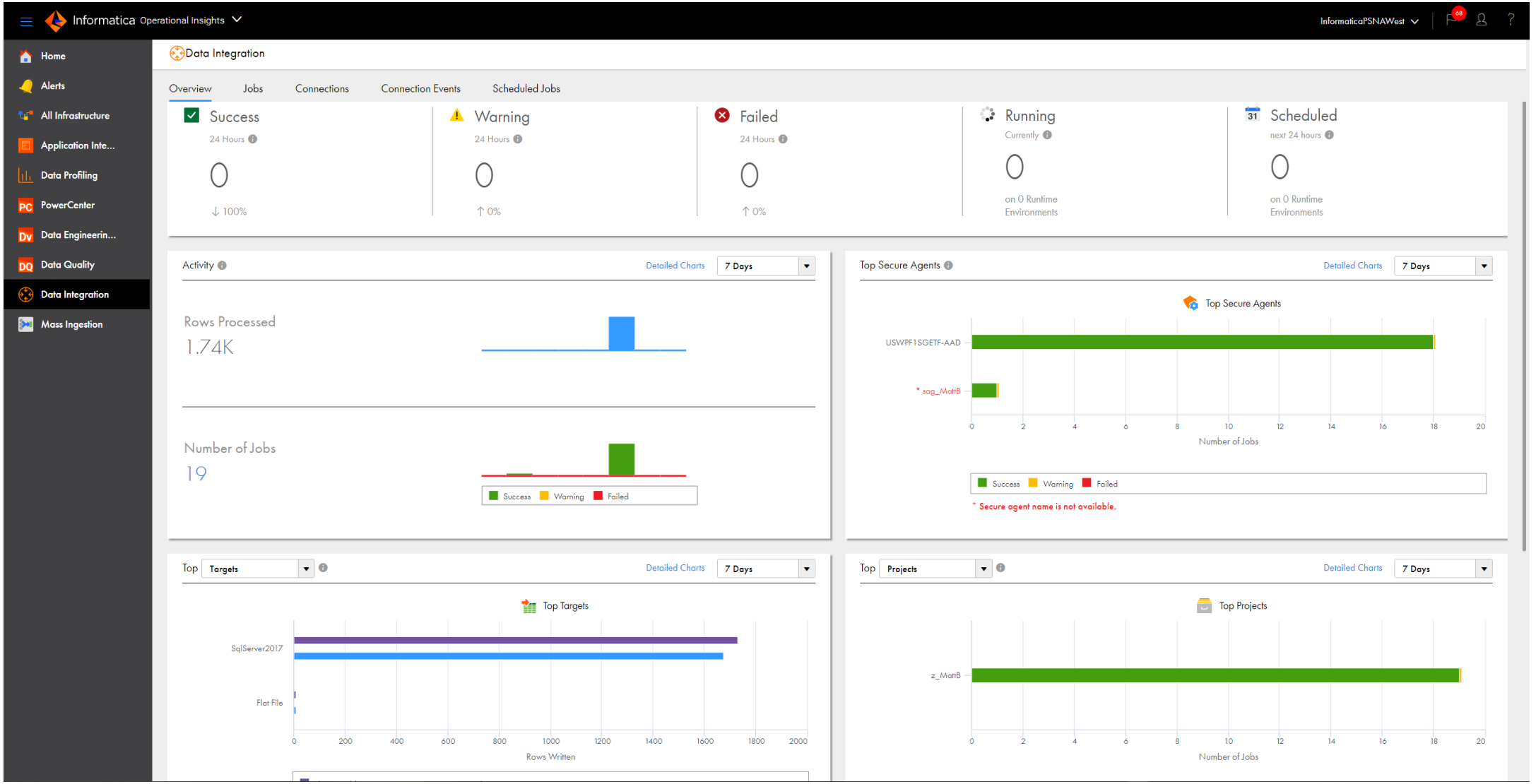
Informatica

Infrastructure Alerts



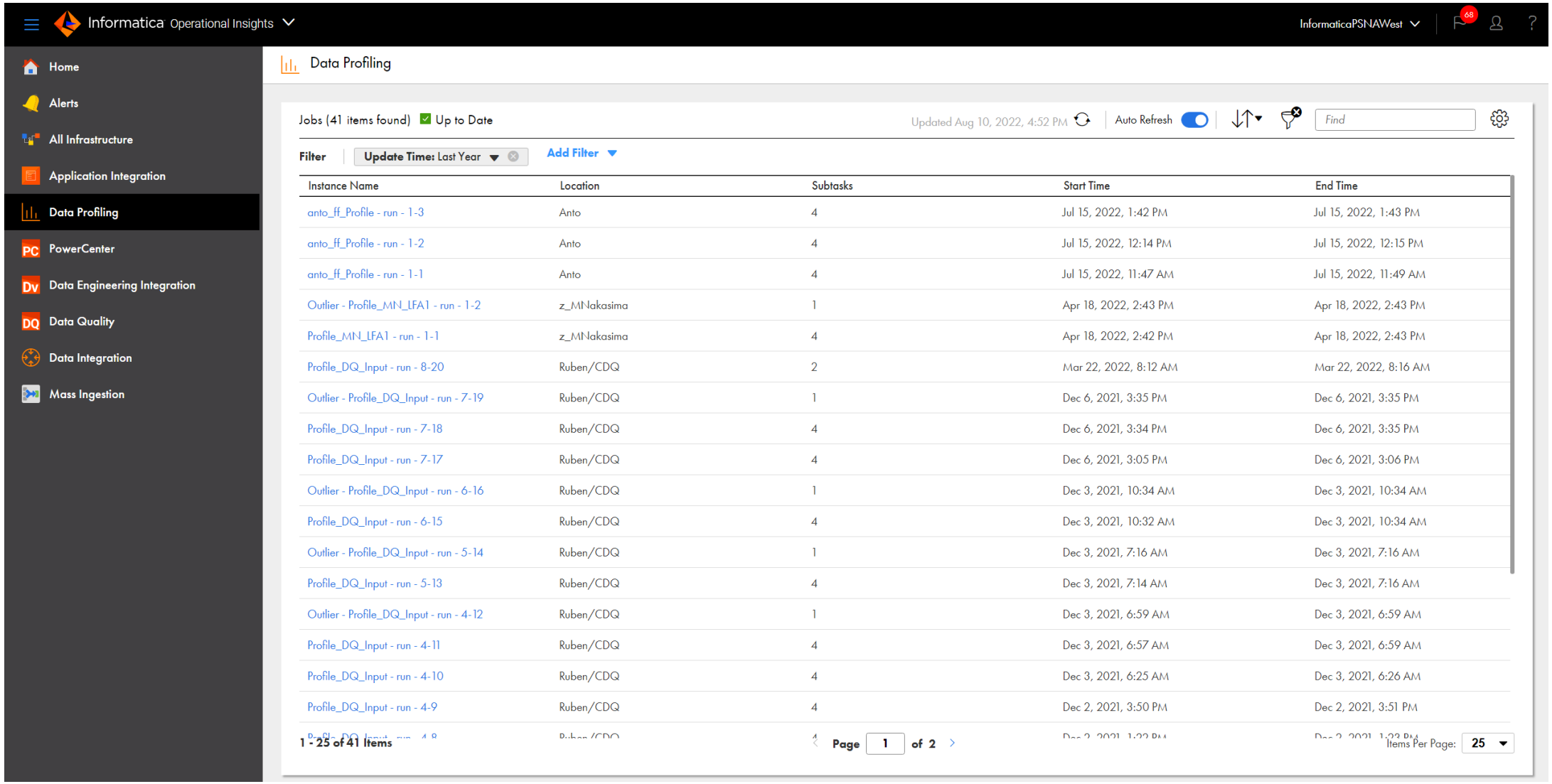
Informatica

Cloud Data Integration



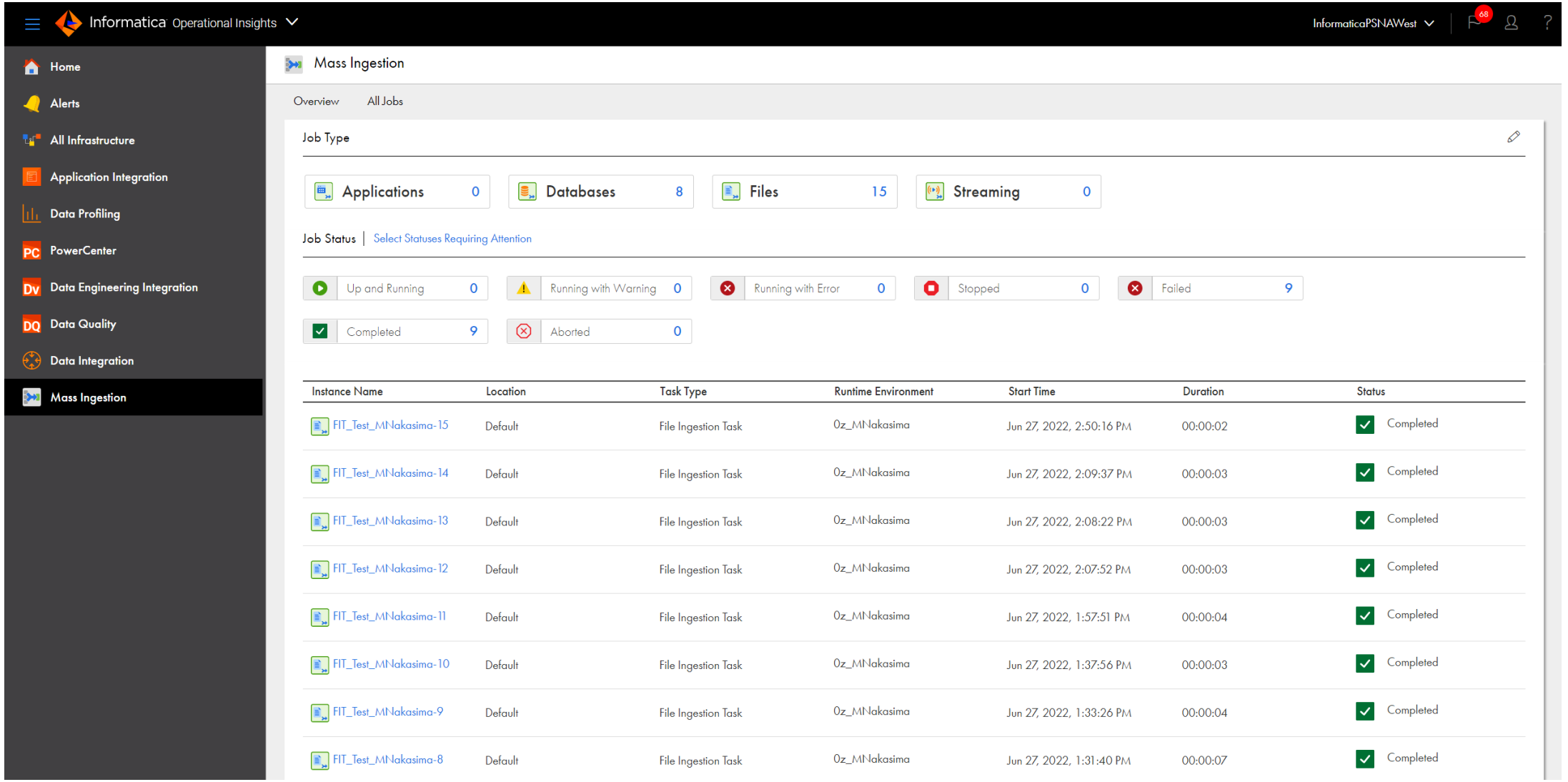
Informatica

Cloud Data Profiling



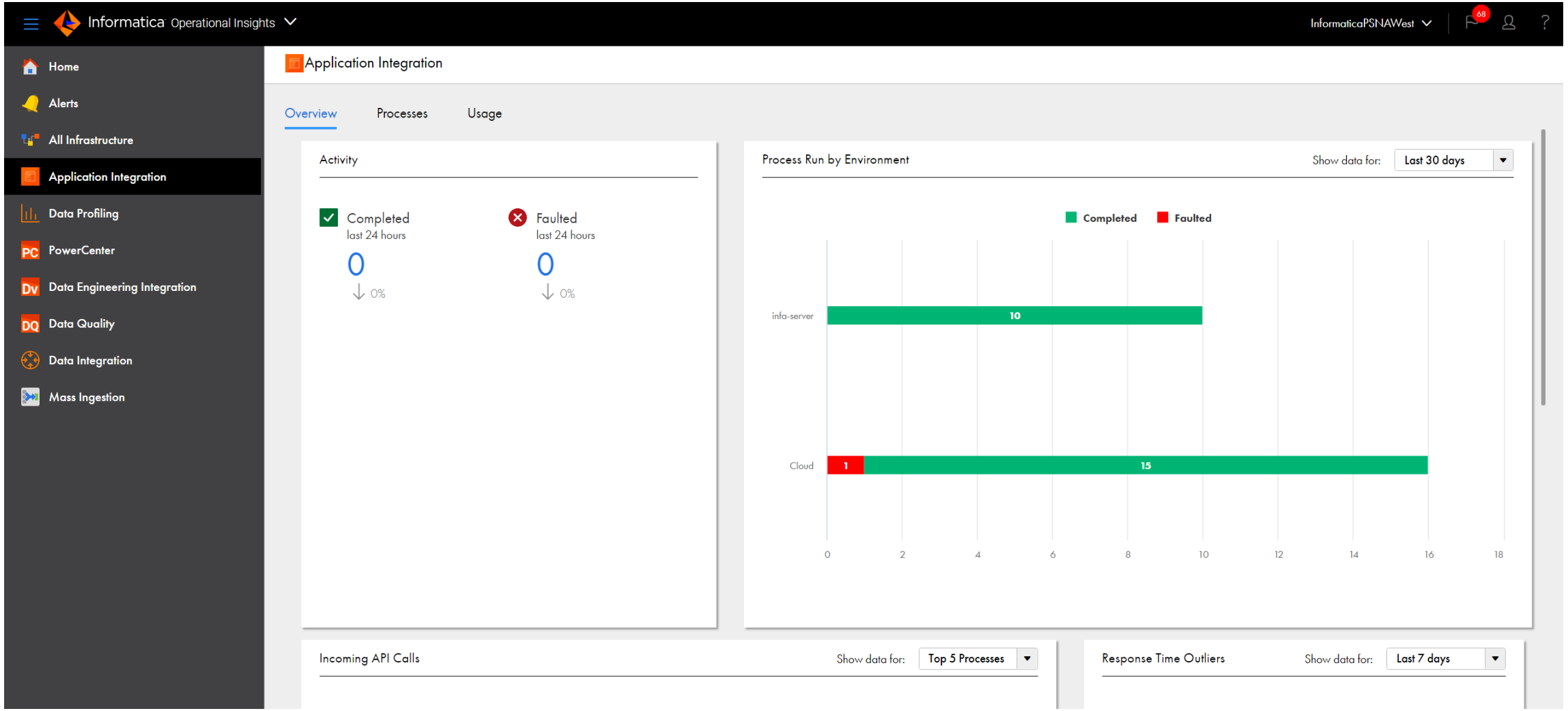
Informatica

Cloud Mass Ingestion



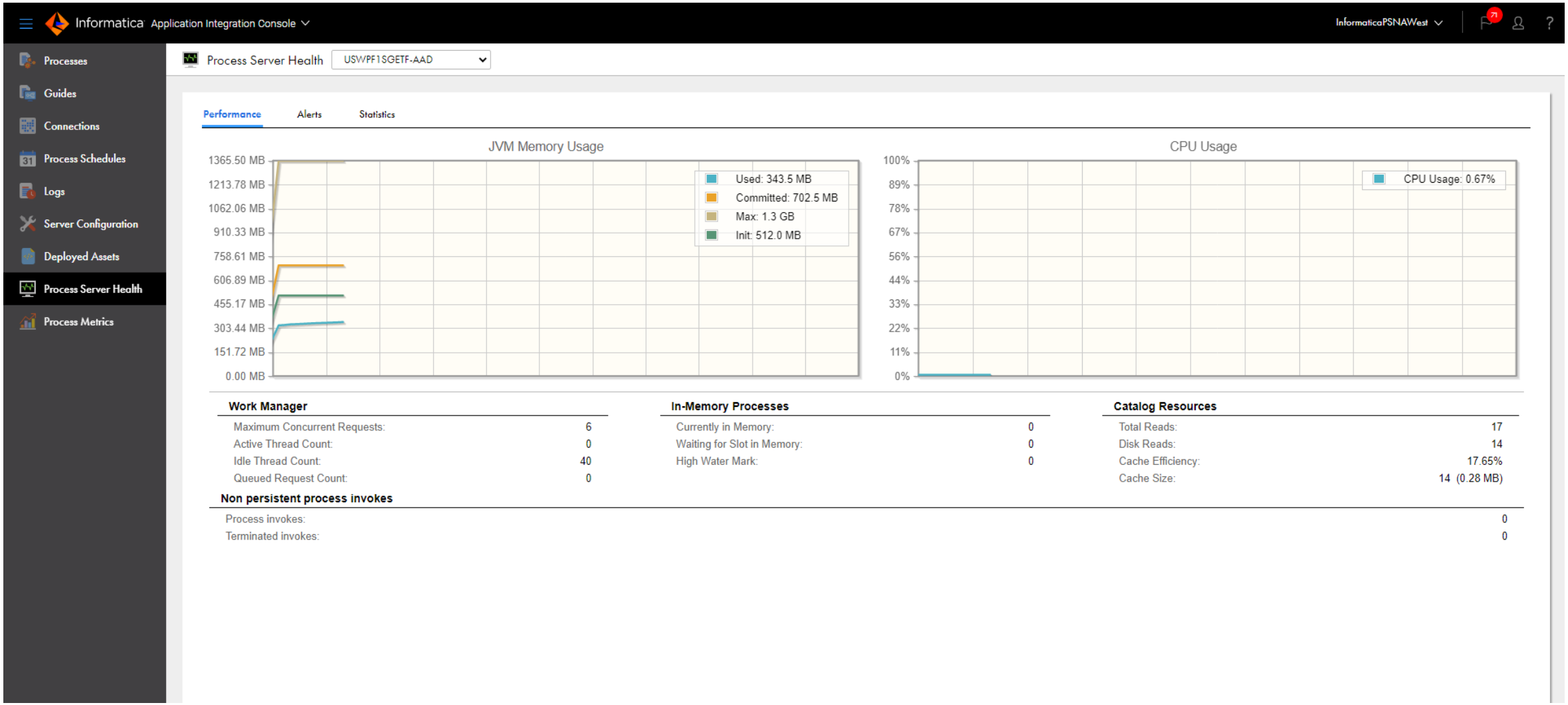
Informatica

Cloud Application Integration



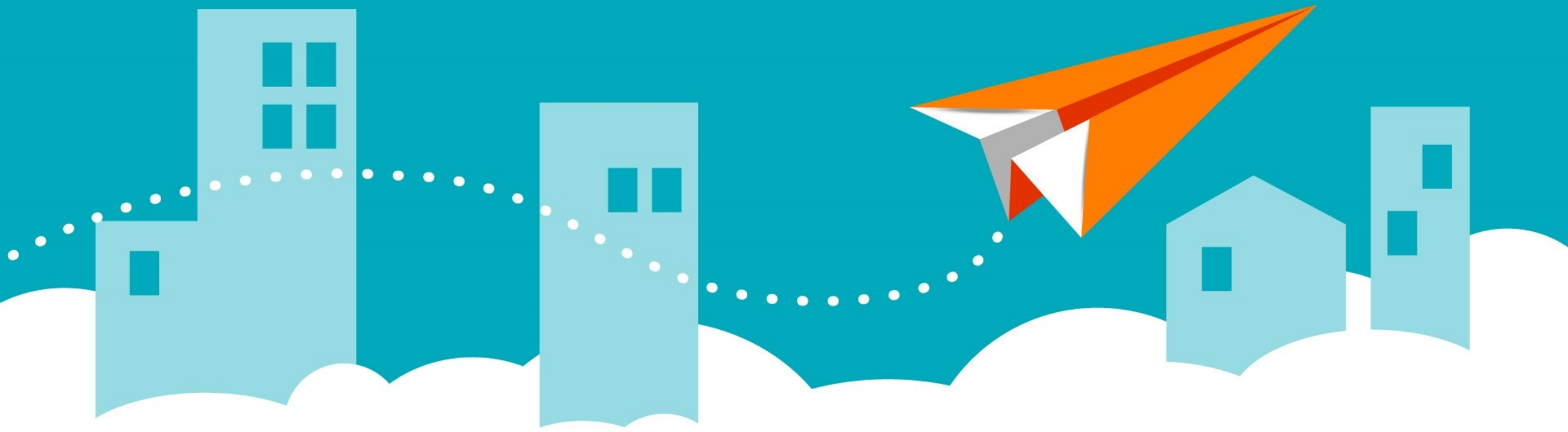
Informatica

CAI Console



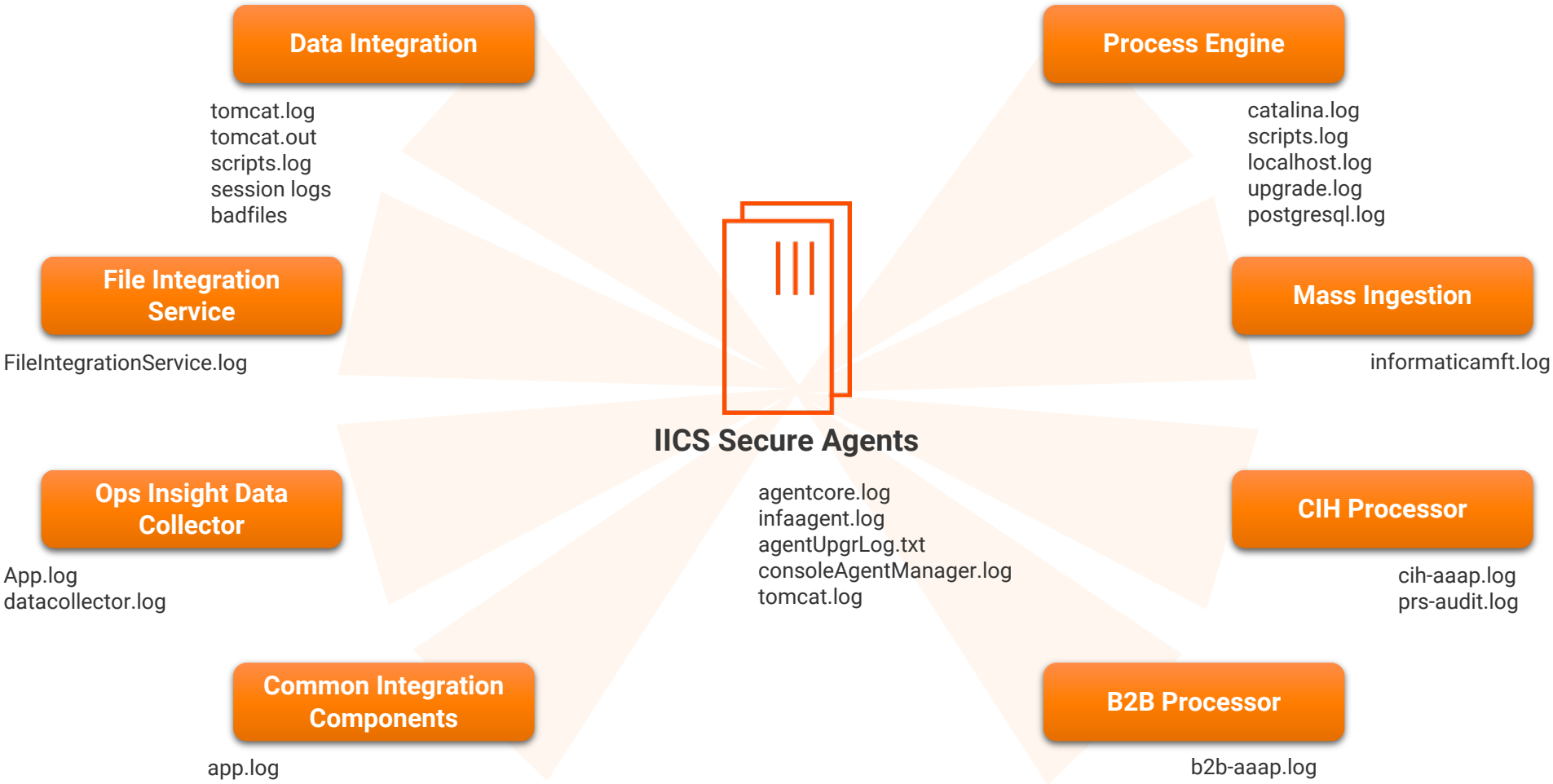
Informatica

Example Solution Architecture



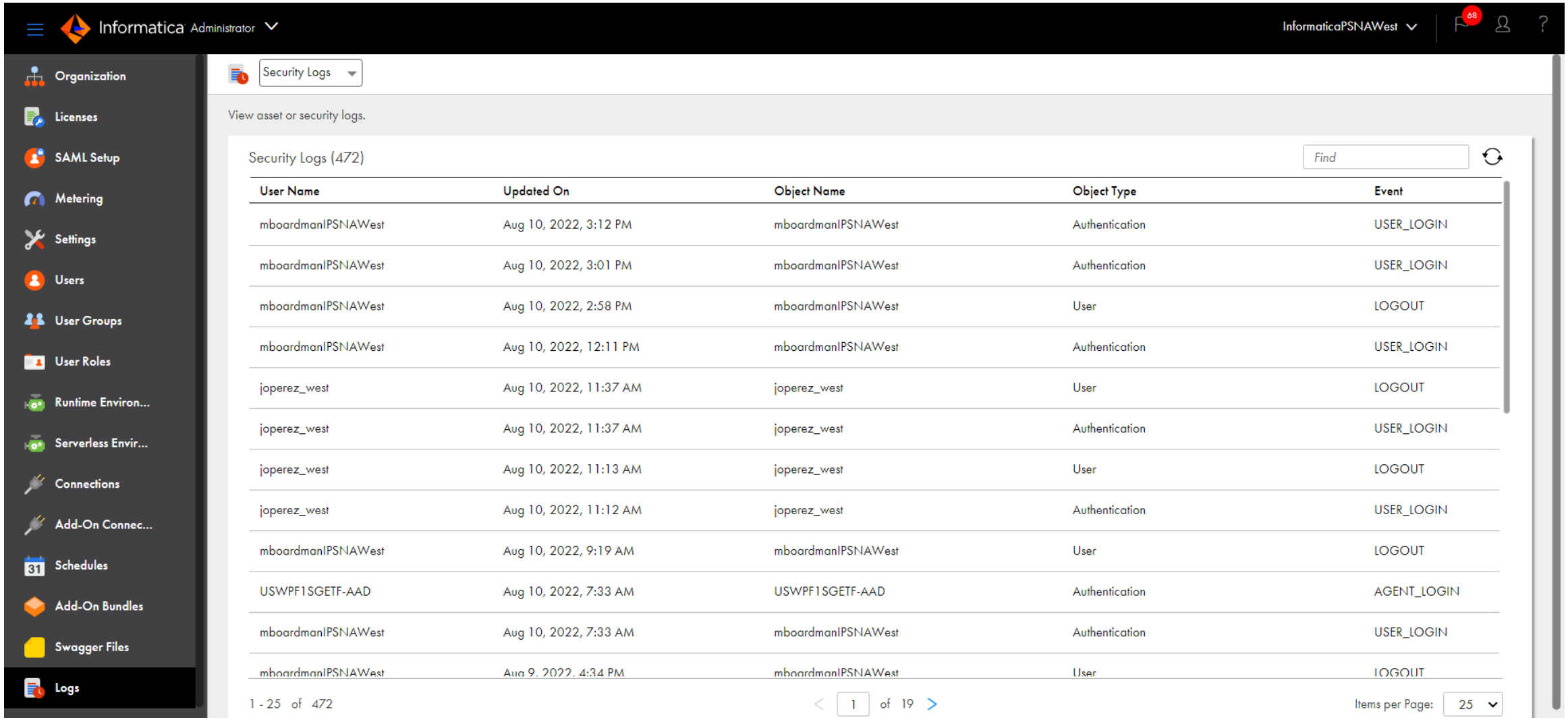
Informatica

Service Logs on Informatica Secure Agents



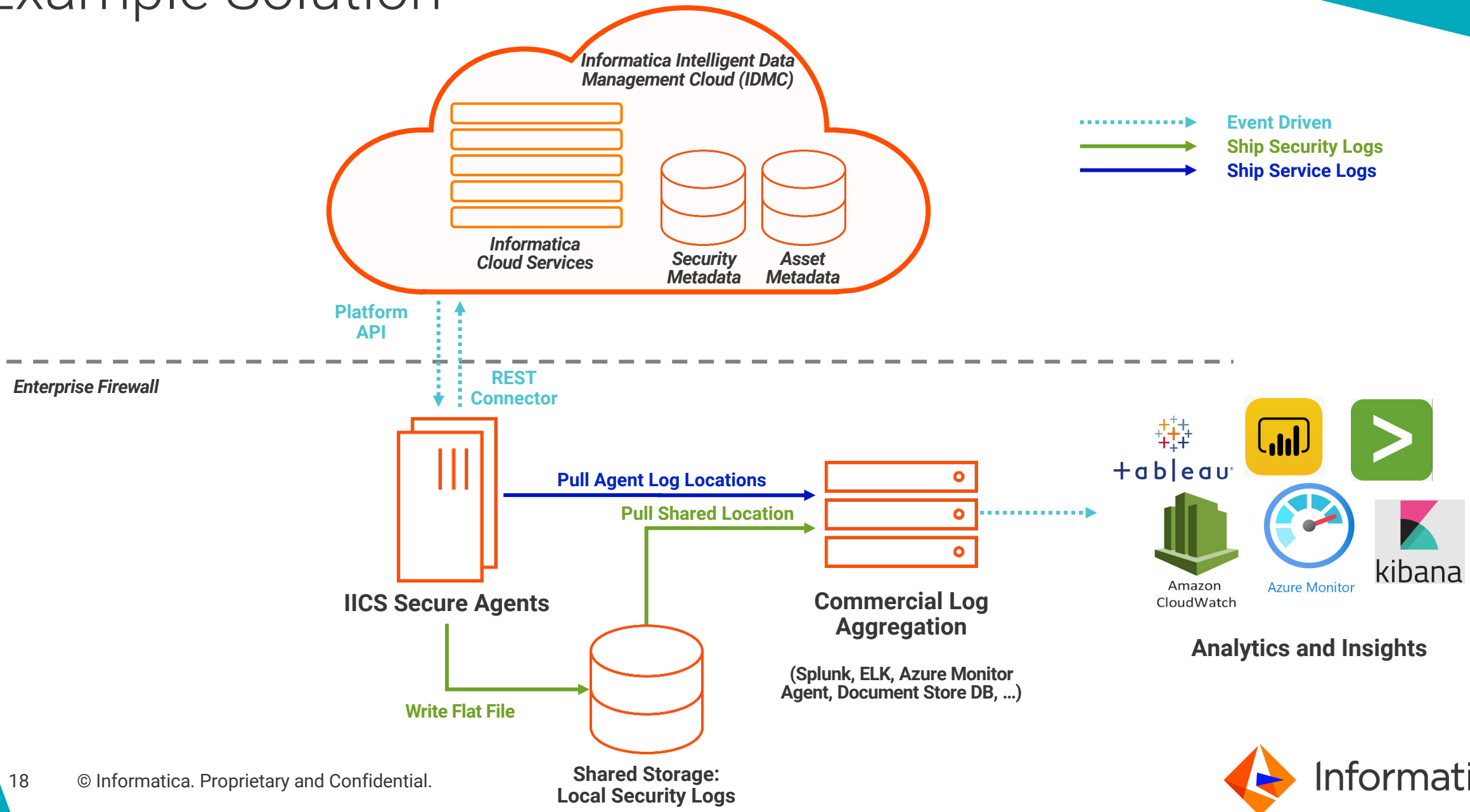
Informatica

Asset and Security Logs in Administrator Applet



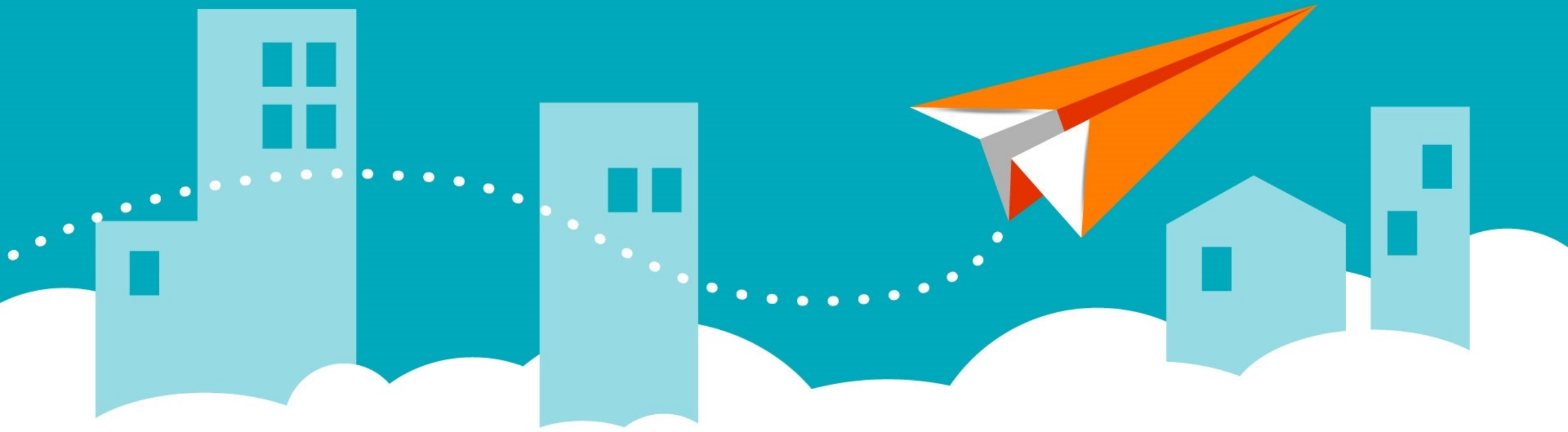
Informatica

Example Solution



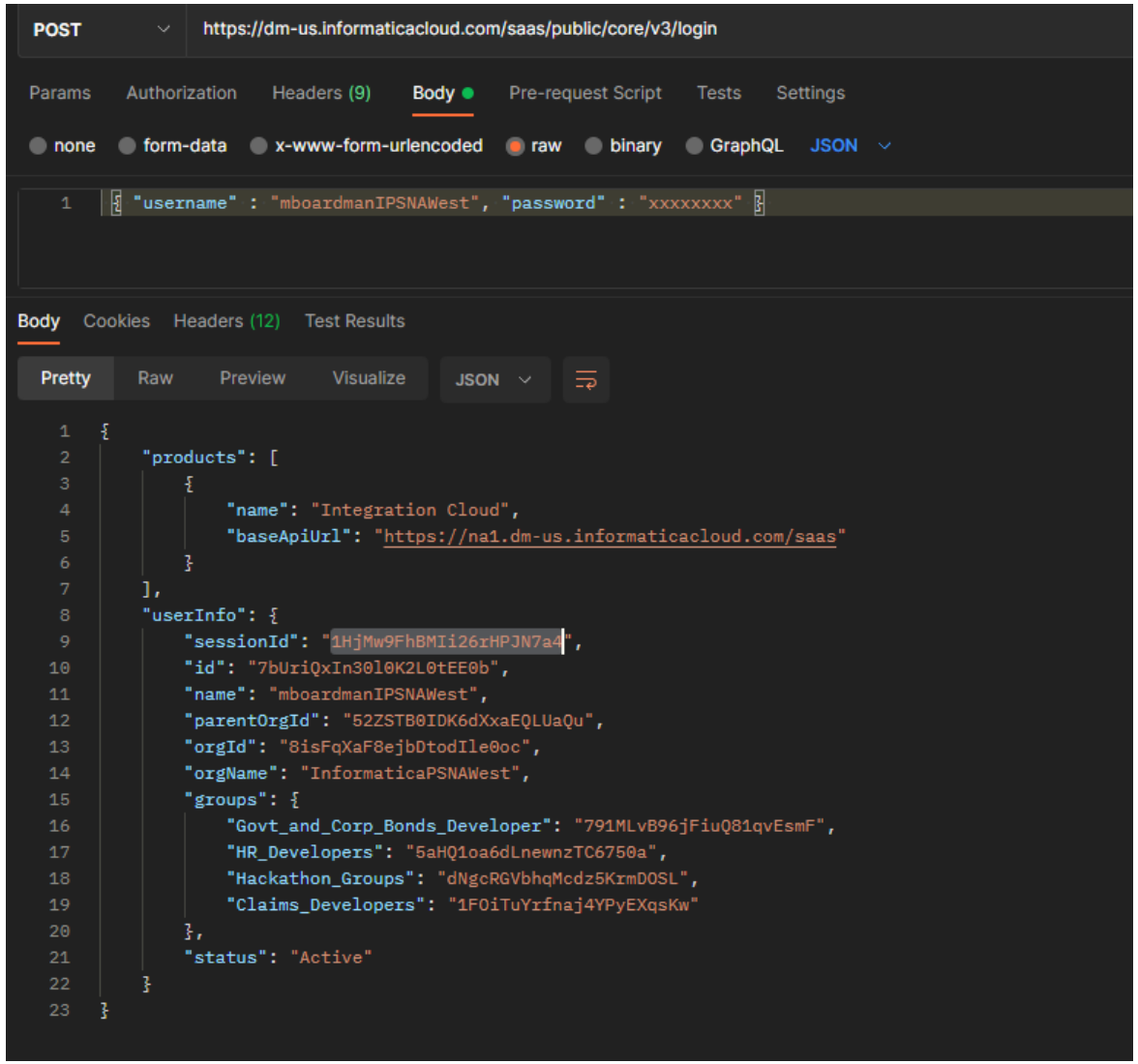
Informatica

Informatica ICDM Platform API



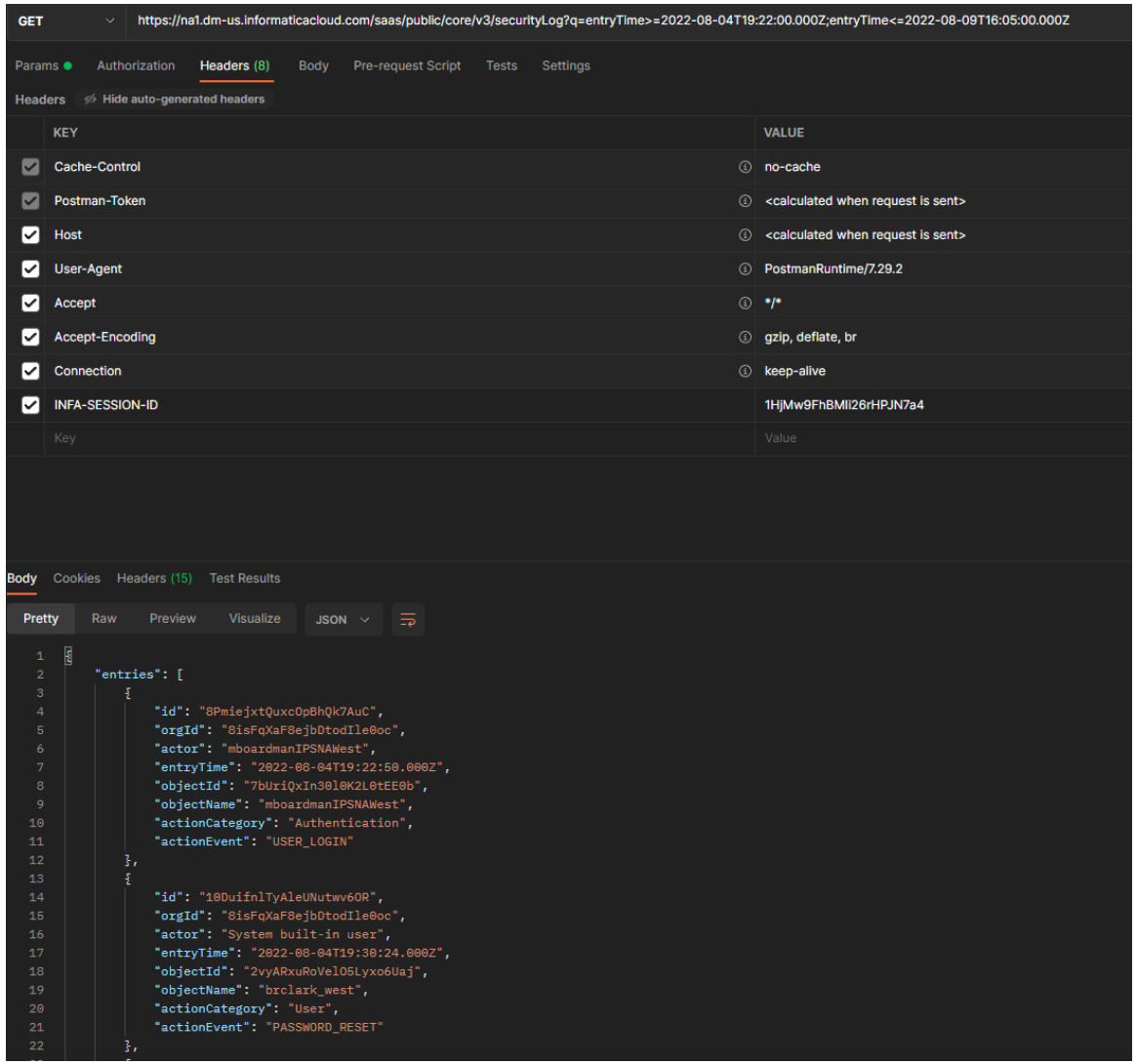
Informatica

Cloud Platform API - Login



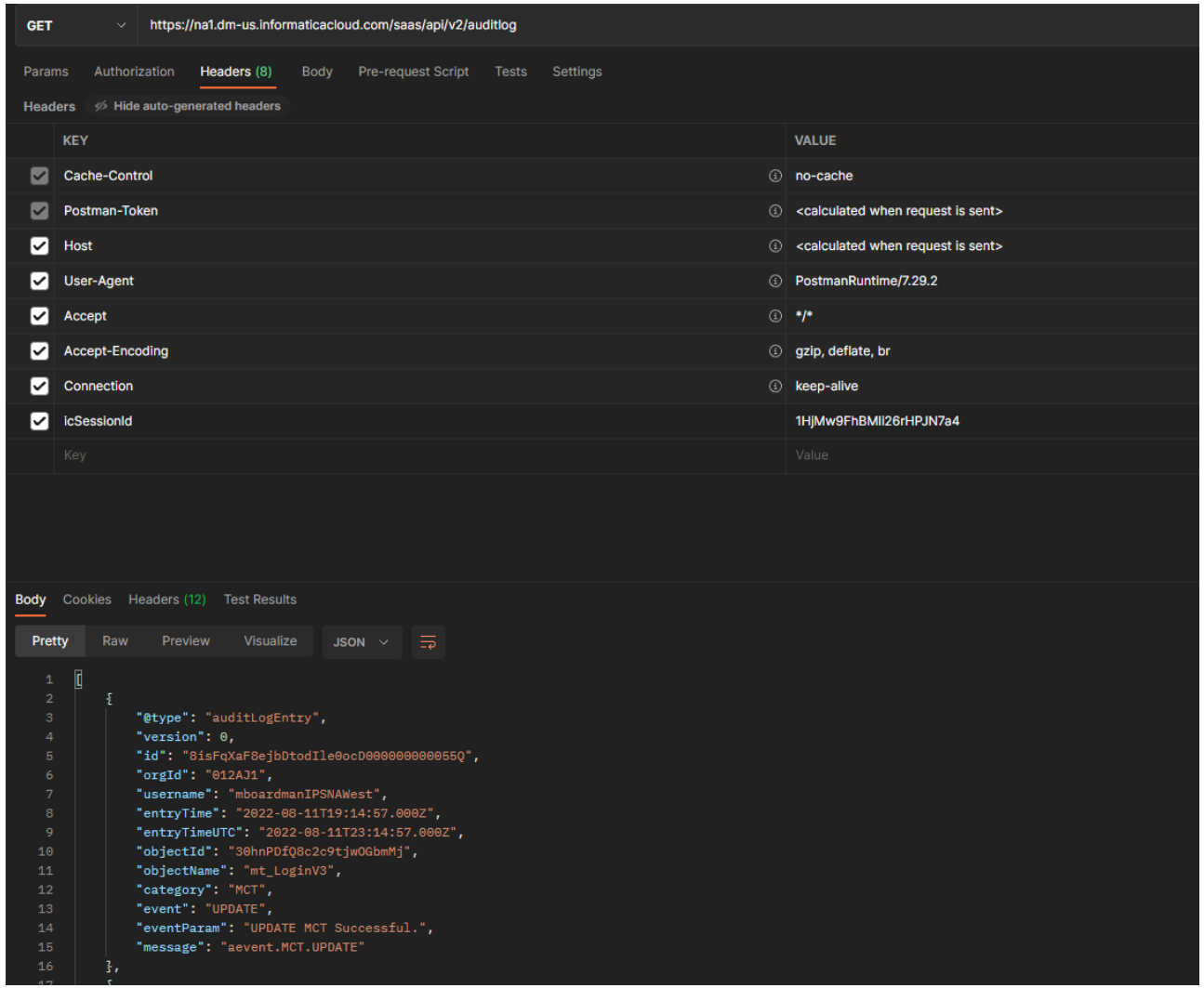
Informatica

Cloud Platform API – Security Logs



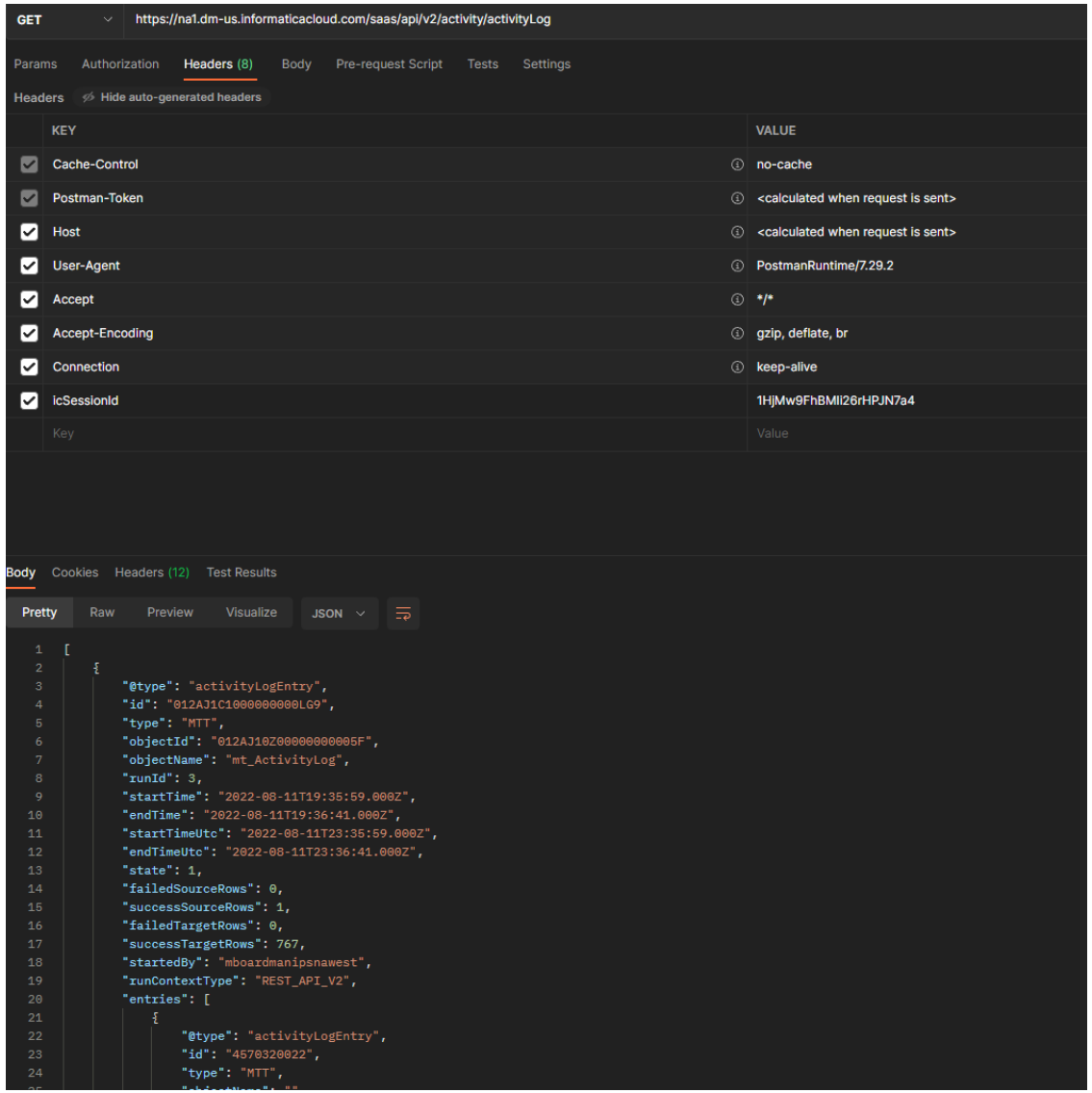
Informatica

Cloud Platform API – Asset (Audit) Logs



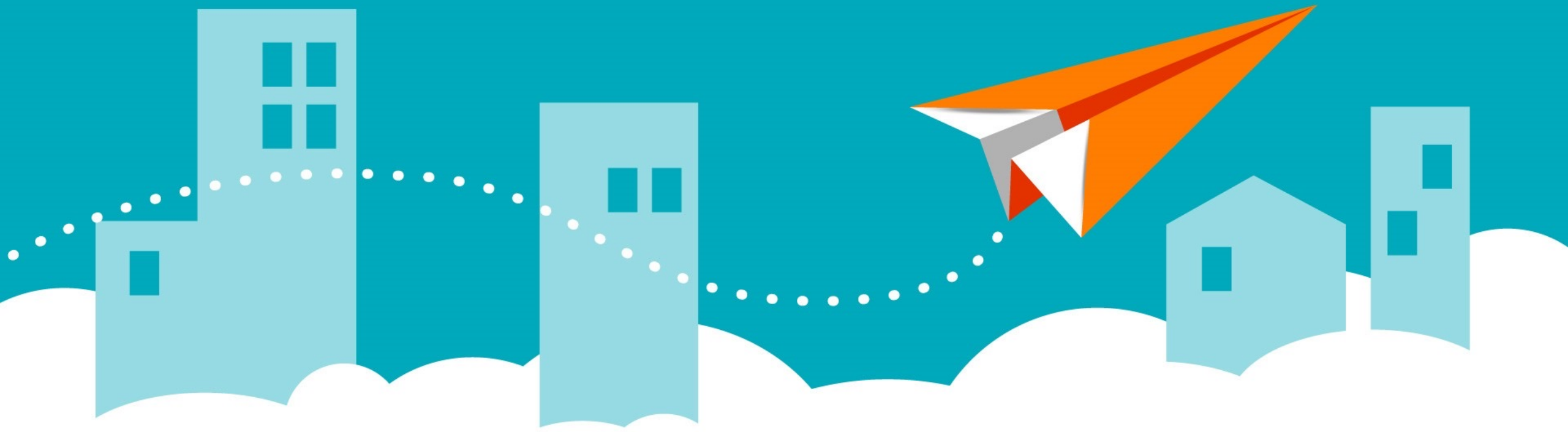
Informatica

Cloud Platform API – CDI Job Logs



Informatica

Extract Logs from Informatica Cloud



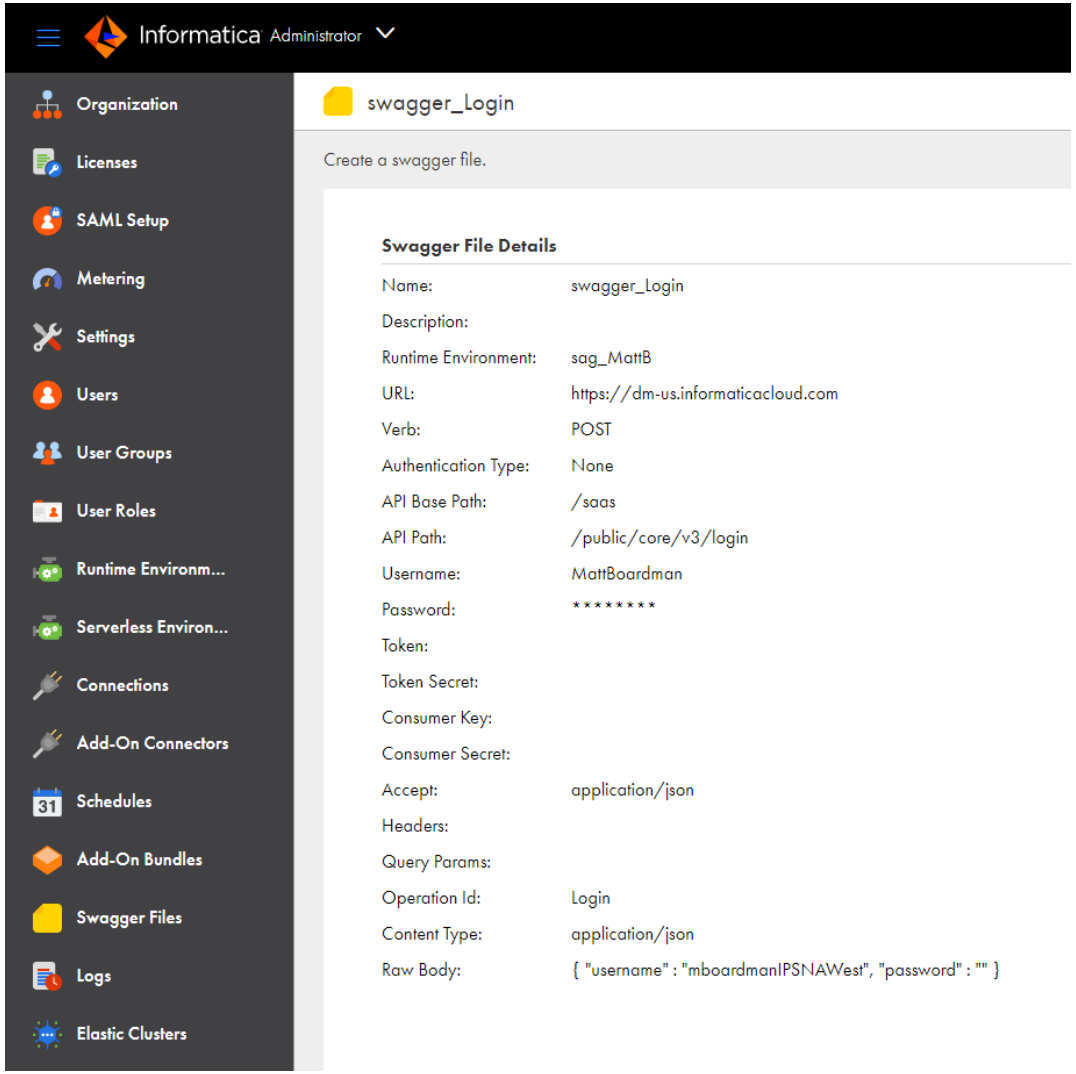
Informatica

Steps using Data Integration

- Create Swagger Files (Describe REST API)
- Create REST v2 Connectors
- Build Mappings and Mapping Tasks
  - Login to get Session Token
  - Extract Security Log
  - Extract Asset Log
  - Extract CDI Job Log
- Build Taskflow

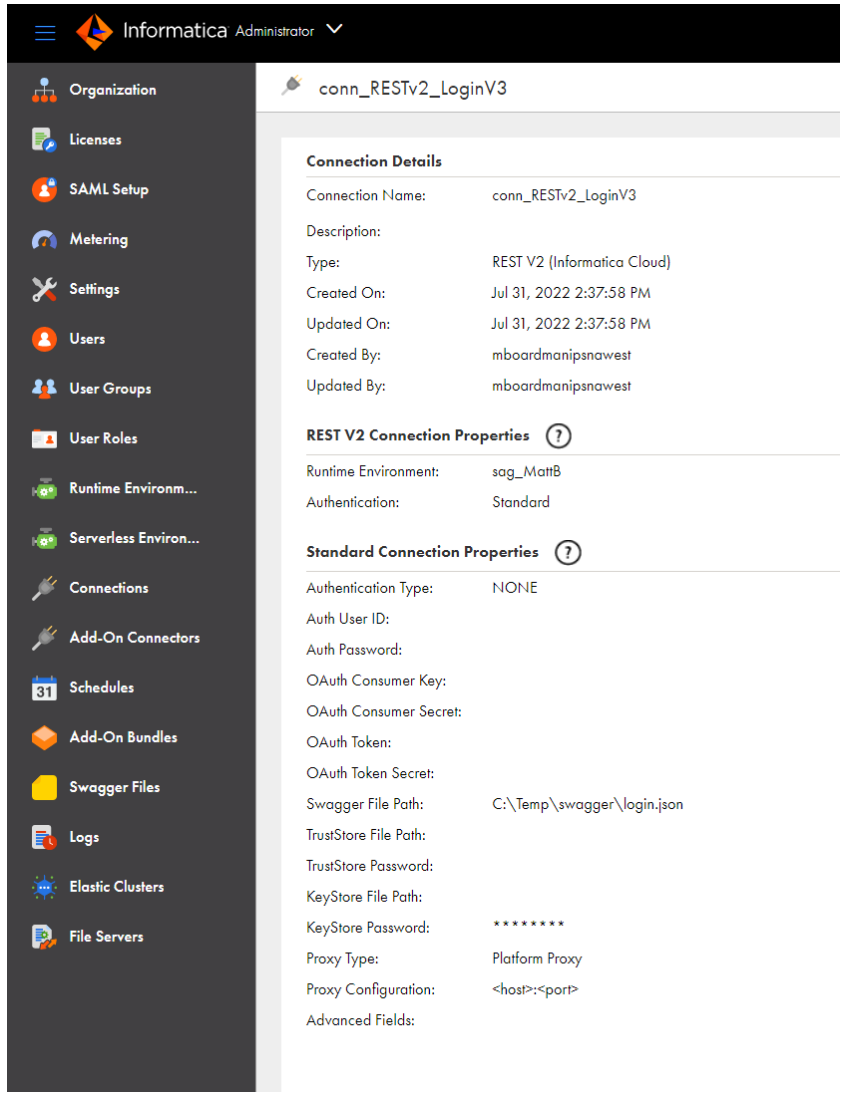
Informatica

Swagger Files



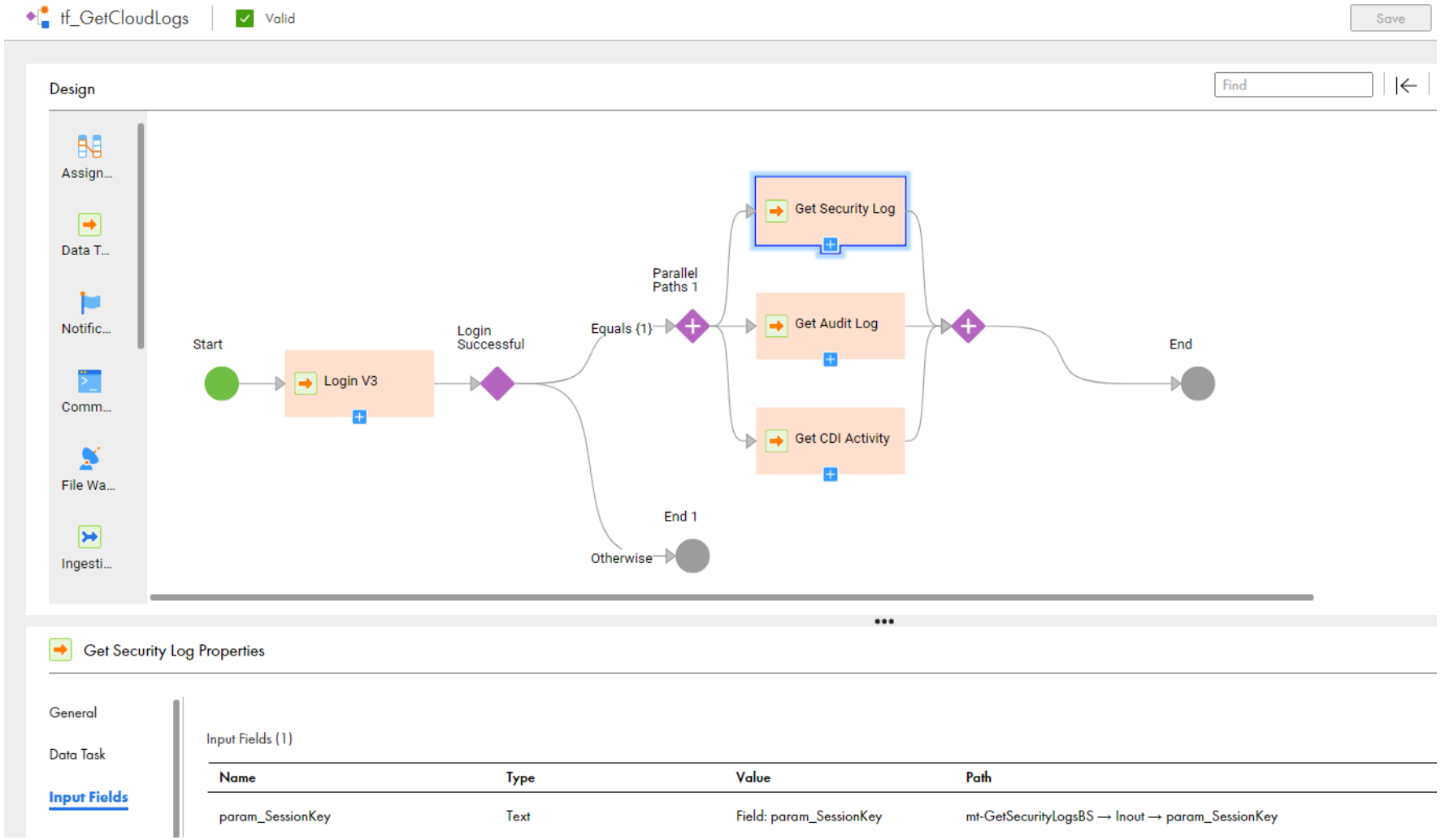
Informatica

REST v2 Connections



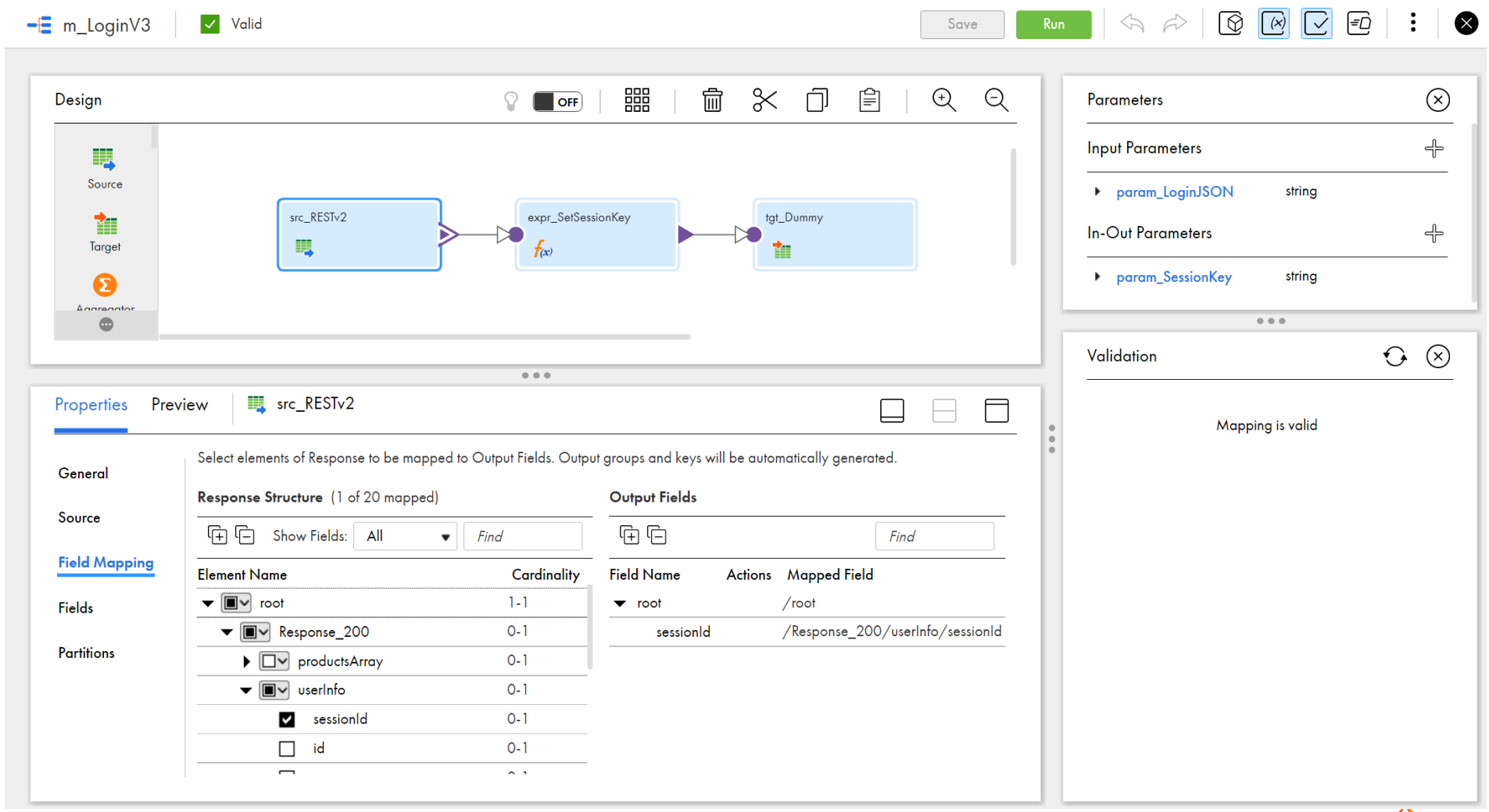
Informatica

Taskflow



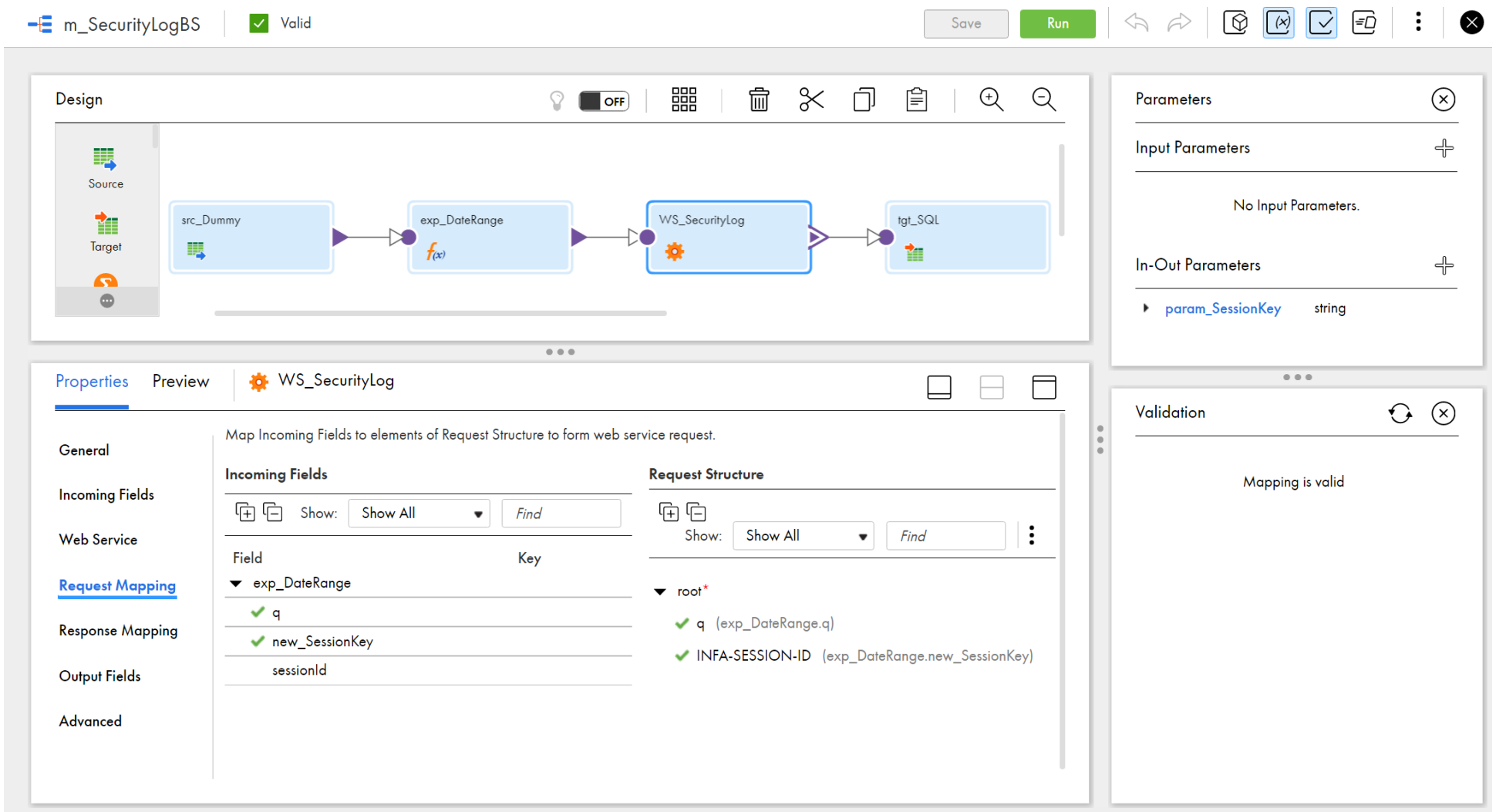
Informatica

Mapping: Login to get Session Key



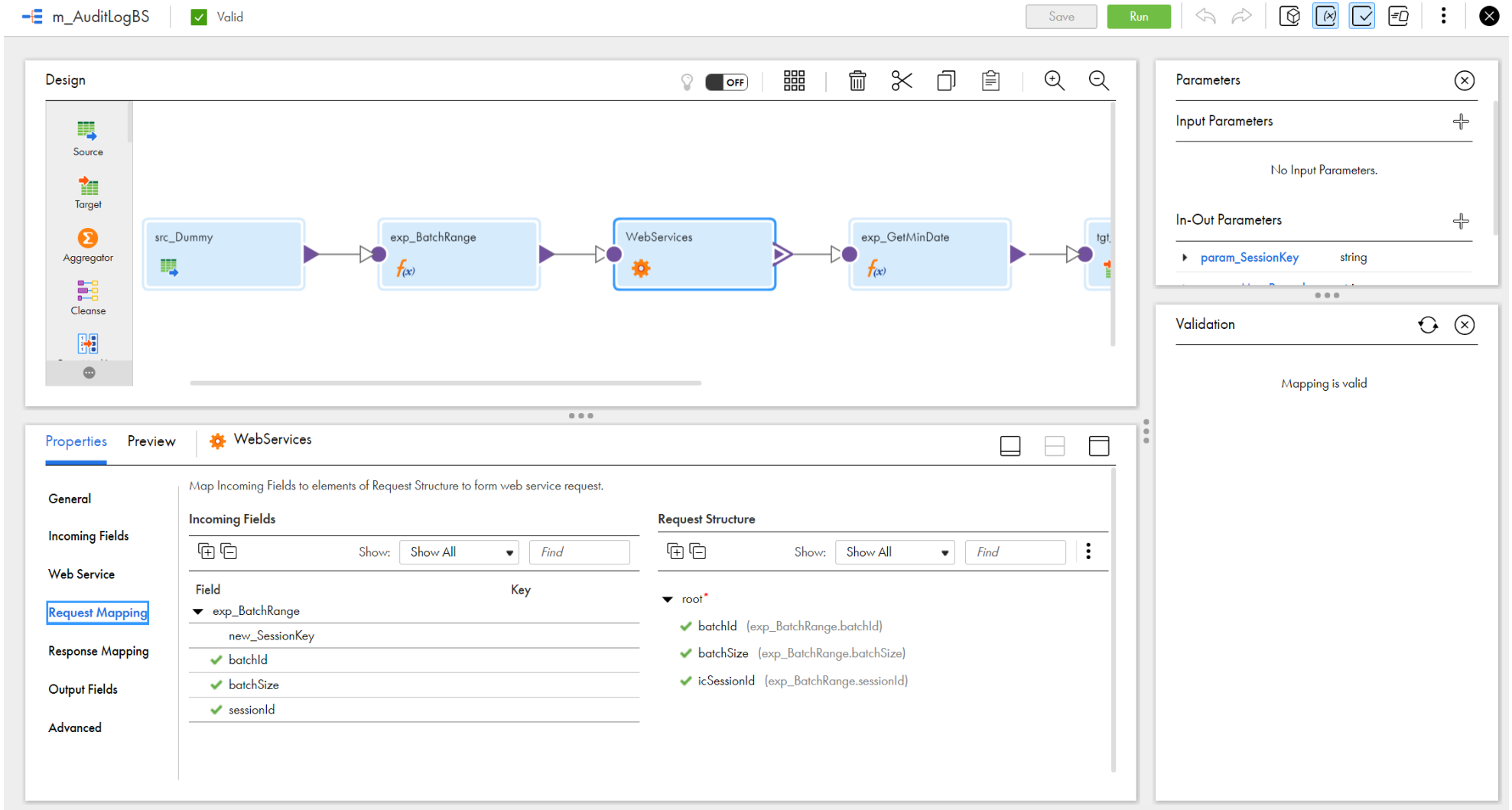
Informatica

Mapping: Extract Security Log



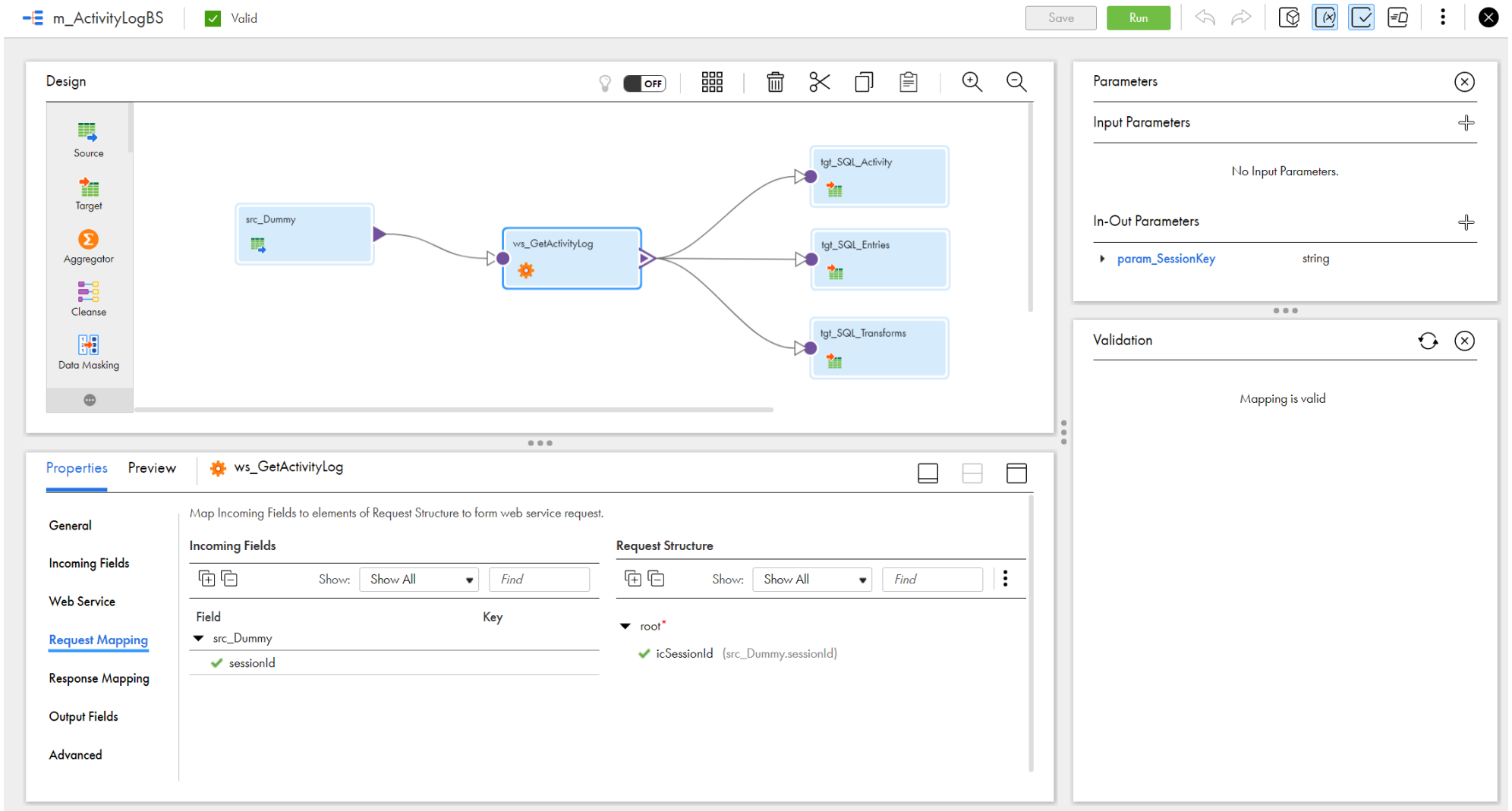
Informatica

Mapping: Extract Asset (Audit) Log



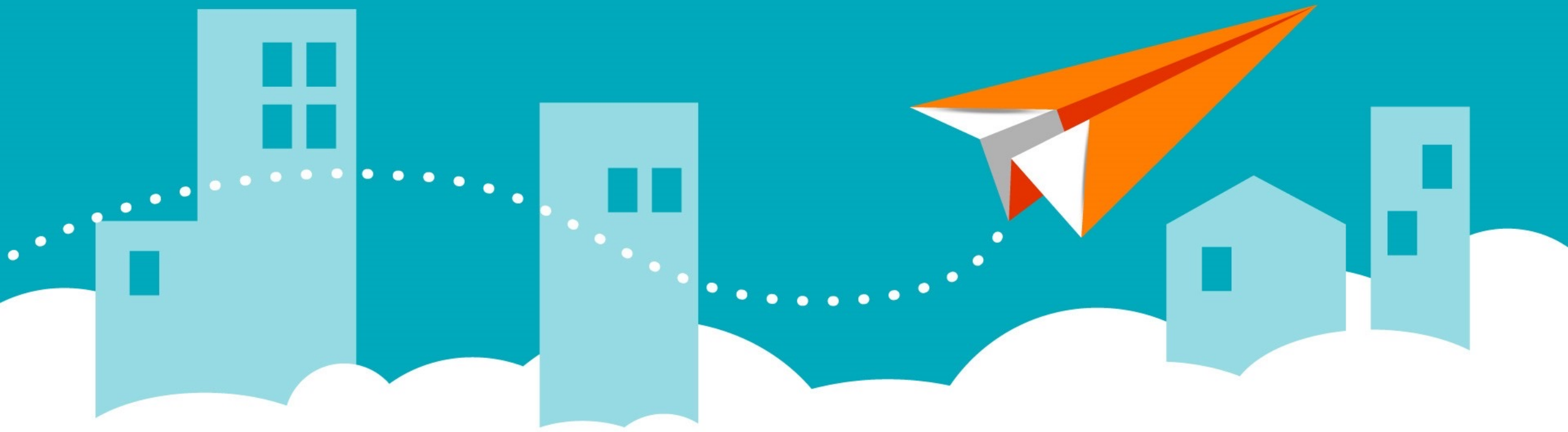
Informatica

Mapping: Extract Data Integration Jobs Log



Informatica

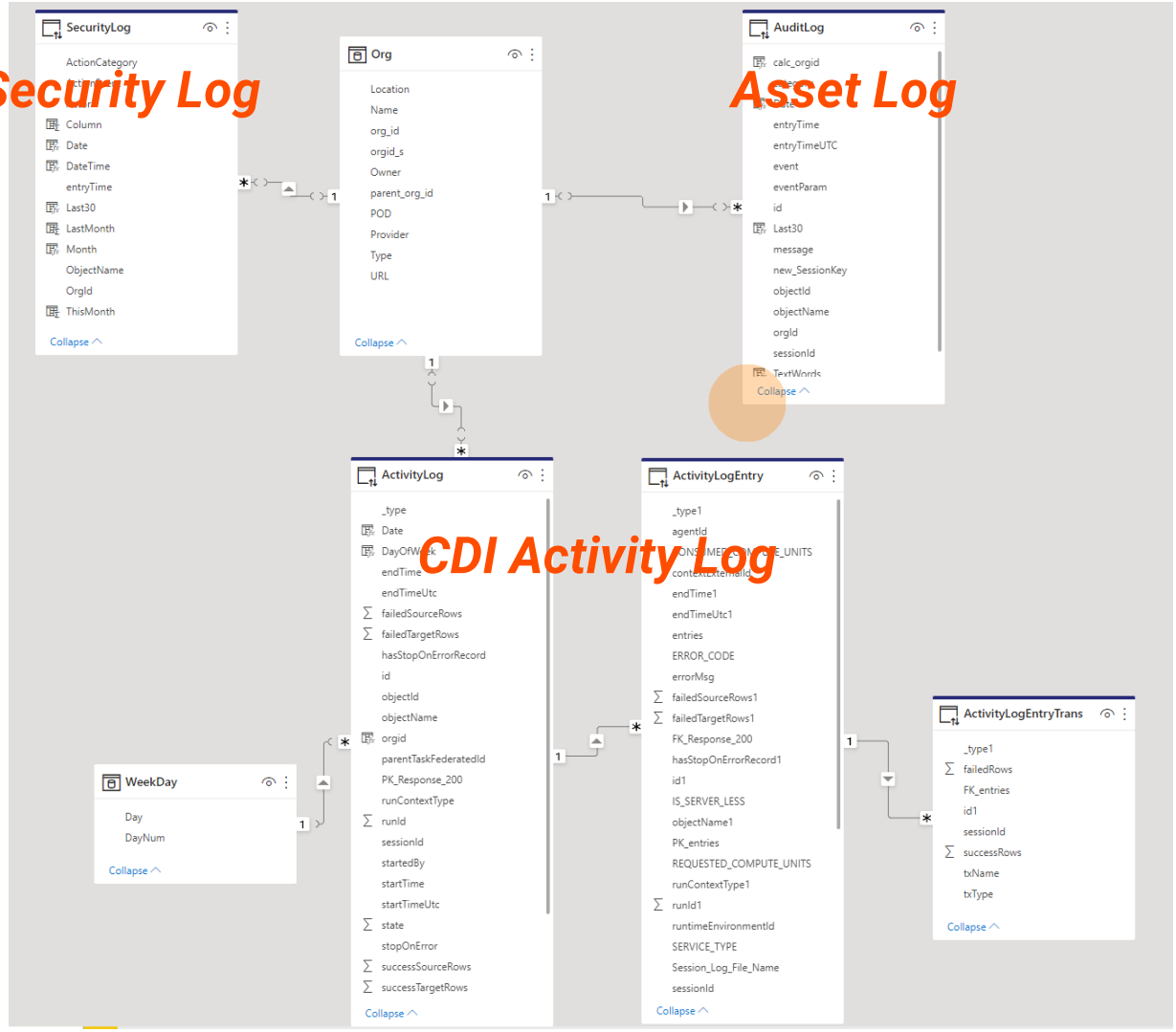
Example Dashboard using Microsoft Power BI



Informatica

Example Data Model

- From Power BI:
  - Complete Security Log from API
  - Complete Asset (Audit) Log from API
  - Three-Level Activity Log from CDI API
    - Activity Log
    - Activity Log Events
    - Activity Log Transforms (Source/Target)
  - Reference Tables
    - IICS Org Locations
    - Weekday Names



Informatica

Example Dashboard – From Security Logs

IICS Org Administration Dashboard - Security

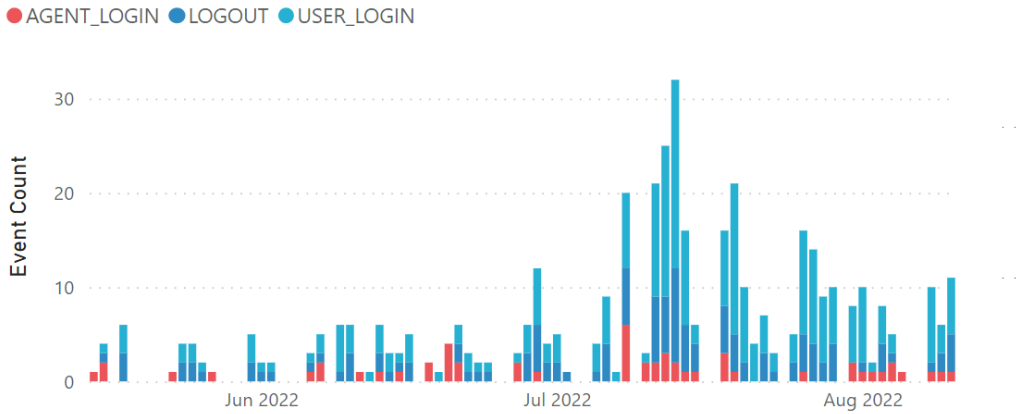
1	5	15	12
Orgs	Distinct Agents	Distinct Users	Users Created

Org Locations

Available Orgs

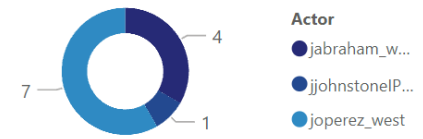
- na1
  - InformaticaPSNAWest
- usw1
  - C360.SaaS - Early Adopter Core
  - IPS Training Org 2

Last 90 Days Login Events



Last 30 Days Logins

Last 30 Days Administration



Users and Groups

DateTime	Actor	ActionEvent	ObjectName
7/14/2022 9:08:06 PM	joperez_west	CREATE	abhshukla_west
7/13/2022 1:48:18 PM	jjohnstoneIPSNAWestEnv	CREATE	bthompsonIPSNAWestEnv
7/12/2022 8:15:13 PM	jabraham_west	CREATE	brclark_west
7/12/2022 8:14:29 PM	jabraham_west	CREATE	rsouth_west
7/12/2022 8:13:33 PM	jabraham_west	CREATE	ekleyn_west

Agent Login Events

DateTime	ActionCategory	ActionEvent	ObjectName
8/10/2022 2:33:41 PM	Authentication	AGENT_LOGIN	USWPF1SGETF-AAD
8/9/2022 2:44:24 PM	Authentication	AGENT_LOGIN	USWPF1SGETF-AAD
8/8/2022 8:45:17 PM	Authentication	AGENT_LOGIN	USWPF1SGETF-AAD
8/5/2022 2:22:43 PM	Authentication	AGENT_LOGIN	USWPF1SGETF-AAD
8/4/2022 1:03:23 PM	Authentication	AGENT_LOGIN	USWPF1SGETF-AAD
8/4/2022 2:25:14 AM	Authentication	AGENT_LOGIN	LAPTOP-G0UQPCT5
8/3/2022 7:50:31 PM	Authentication	AGENT_LOGIN	USWPF1SGETF-AAD
8/2/2022 2:52:38 PM	Authentication	AGENT_LOGIN	USWPF1SGETF-AAD
8/1/2022 3:43:48 PM	Authentication	AGENT_LOGIN	USWPF1SGETF-AAD

User Login Events

DateTime	ActionCategory	ActionEvent	Actor
8/10/2022 10:12:41 PM	Authentication	USER_LOGIN	mboardmanIPSNAWest
8/10/2022 10:01:04 PM	Authentication	USER_LOGIN	mboardmanIPSNAWest
8/10/2022 9:58:28 PM	User	LOGOUT	mboardmanIPSNAWest
8/10/2022 7:11:31 PM	Authentication	USER_LOGIN	mboardmanIPSNAWest
8/10/2022 6:37:34 PM	User	LOGOUT	joperez_west
8/10/2022 6:37:30 PM	Authentication	USER_LOGIN	joperez_west
8/10/2022 6:13:13 PM	User	LOGOUT	joperez_west
8/10/2022 6:12:46 PM	Authentication	USER_LOGIN	joperez_west
8/10/2022 4:19:48 PM	User	LOGOUT	mboardmanIPSNAWest

Informatica

Example Dashboard – From Asset Logs

IICS Org Administration Dashboard - Activity

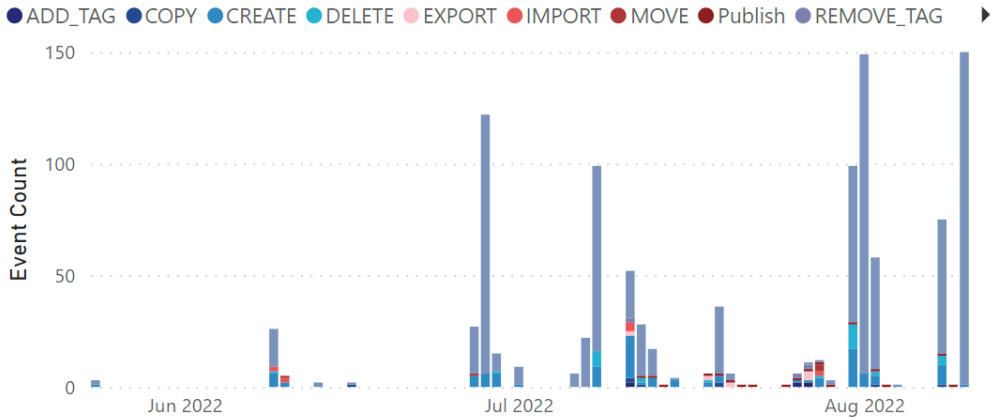
1	6	22	78
Orgs	Distinct Users	Object Types	Distinct Objects

Org Locations

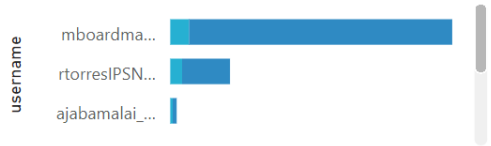
Available Orgs

- na1
  - InformaticaPSNAWest
- usw1
  - C360.SaaS - Early Adopter Core
  - IPS Training Org 2

Last 90 Days Activity

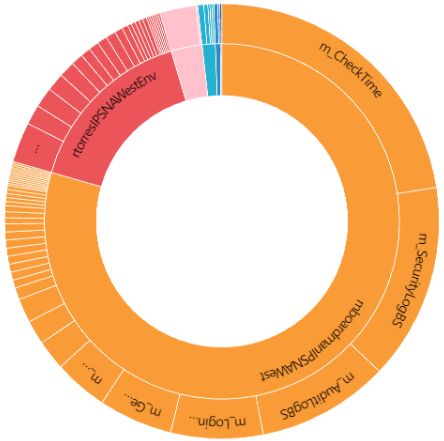


Last 30 Days Objects



Last 30 Days Popular Messages

Last 30 Days Development

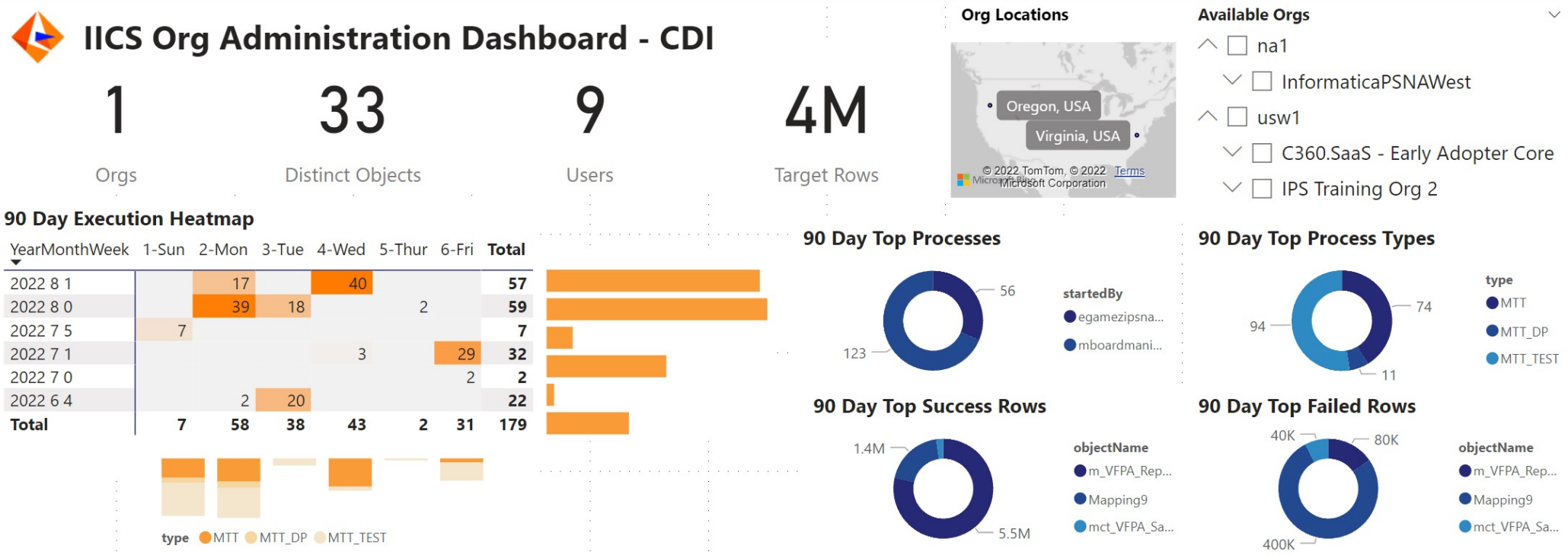


Activity Audit Log

entryTime	username	category	event	eventParam	message	objectId	objectName
2022-06-29T14:49:20.000Z	egamezIPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	UPDATE	UPDATE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.UPDATE	8lMwY2oaVFclsaA1uGH7Cx	0z_AjayDirects_CDIE
2022-07-08T14:46:24.000Z	egamezIPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	UPDATE	UPDATE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.UPDATE	8lMwY2oaVFclsaA1uGH7Cx	0z_AjayDirects_CDIE
2022-07-08T14:52:50.000Z	egamezIPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	UPDATE	UPDATE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.UPDATE	8lMwY2oaVFclsaA1uGH7Cx	0z_AjayDirects_CDIE
2022-07-08T14:54:42.000Z	egamezIPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	DELETE	DELETE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.DELETE	8lMwY2oaVFclsaA1uGH7Cx	0z_AjayDirects_CDIE
2022-07-08T14:57:51.000Z	egamezIPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	UPDATE	UPDATE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.UPDATE	0hMImdplunOiFJ5r15e6Uz	0z_AjayDirects-CDIE

Informatica

Example Dashboard – From CDI Job Logs



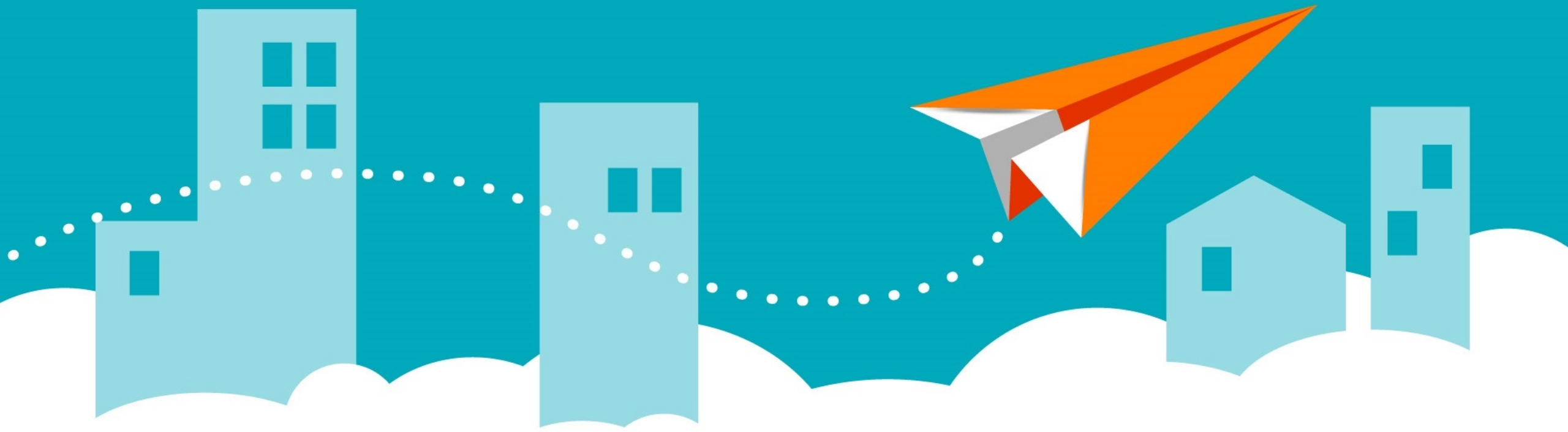
Session Activity

id	type	objectId	objectName	runId	Date	startTime	endTime
012AJ1C1000000000JX2	MTT	012AJ10Z000000000005E	mt_AuditLogBS	6	8/10/2022	2022-08-10T18:12:47.000Z	2022-08-10T18:13:07.000Z
012AJ1C1000000000KP7	MTT	012AJ10Z000000000005C	mt_GetSecurityLogsBS	13	8/10/2022	2022-08-10T18:12:47.000Z	2022-08-10T18:13:04.000Z
012AJ1C1000000000KU7	MTT	012AJ10Z000000000059	mt_LoginV3	19	8/10/2022	2022-08-10T18:12:26.000Z	2022-08-10T18:12:43.000Z
012AJ1C1000000000KU6	MTT_TEST	012AJ10Z000000000005G	m_CheckTime	32	8/10/2022	2022-08-10T17:24:22.000Z	2022-08-10T17:24:34.000Z
012AJ1C1000000000K8C	MTT_TEST	012AJ10Z000000000005G	m_CheckTime	31	8/10/2022	2022-08-10T17:14:09.000Z	2022-08-10T17:14:22.000Z
012AJ1C1000000000K8B	MTT_TEST	012AJ10Z000000000005G	m_CheckTime	30	8/10/2022	2022-08-10T17:12:10.000Z	2022-08-10T17:12:23.000Z
012AJ1C1000000000KJG	MTT_TEST	012AJ10Z000000000005G	m_CheckTime	29	8/10/2022	2022-08-10T17:11:14.000Z	2022-08-10T17:11:27.000Z
012AJ1C1000000000KDZ	MTT_TEST	012AJ10Z000000000005G	m_CheckTime	28	8/10/2022	2022-08-10T17:04:31.000Z	2022-08-10T17:04:44.000Z
012AJ1C1000000000K8A	MTT_TEST	012AJ10Z000000000005G	m_CheckTime	27	8/10/2022	2022-08-10T16:51:31.000Z	2022-08-10T16:51:43.000Z
012AJ1C1000000000JX1	MTT_DP	012AJ117000000000005D	m_CheckTime	5	8/10/2022	2022-08-10T16:50:03.000Z	2022-08-10T16:50:15.000Z

Errors

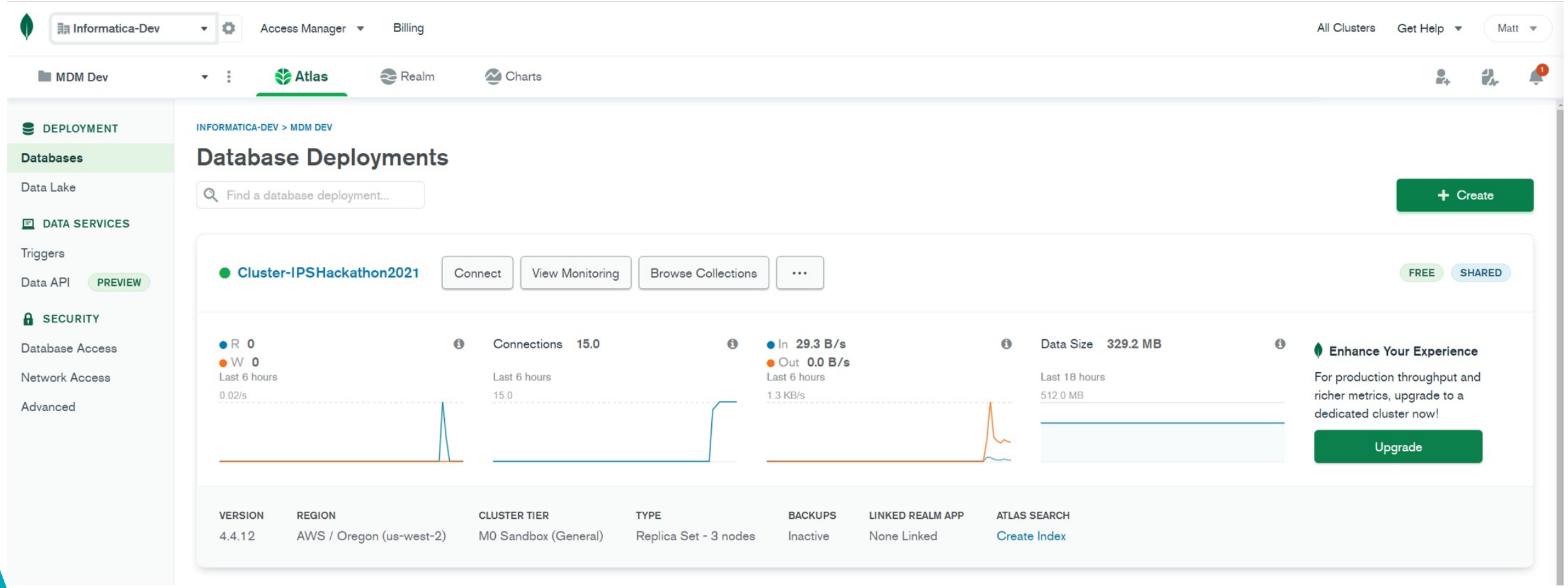
Informatica

Using a Document Store Database (MongoDB)



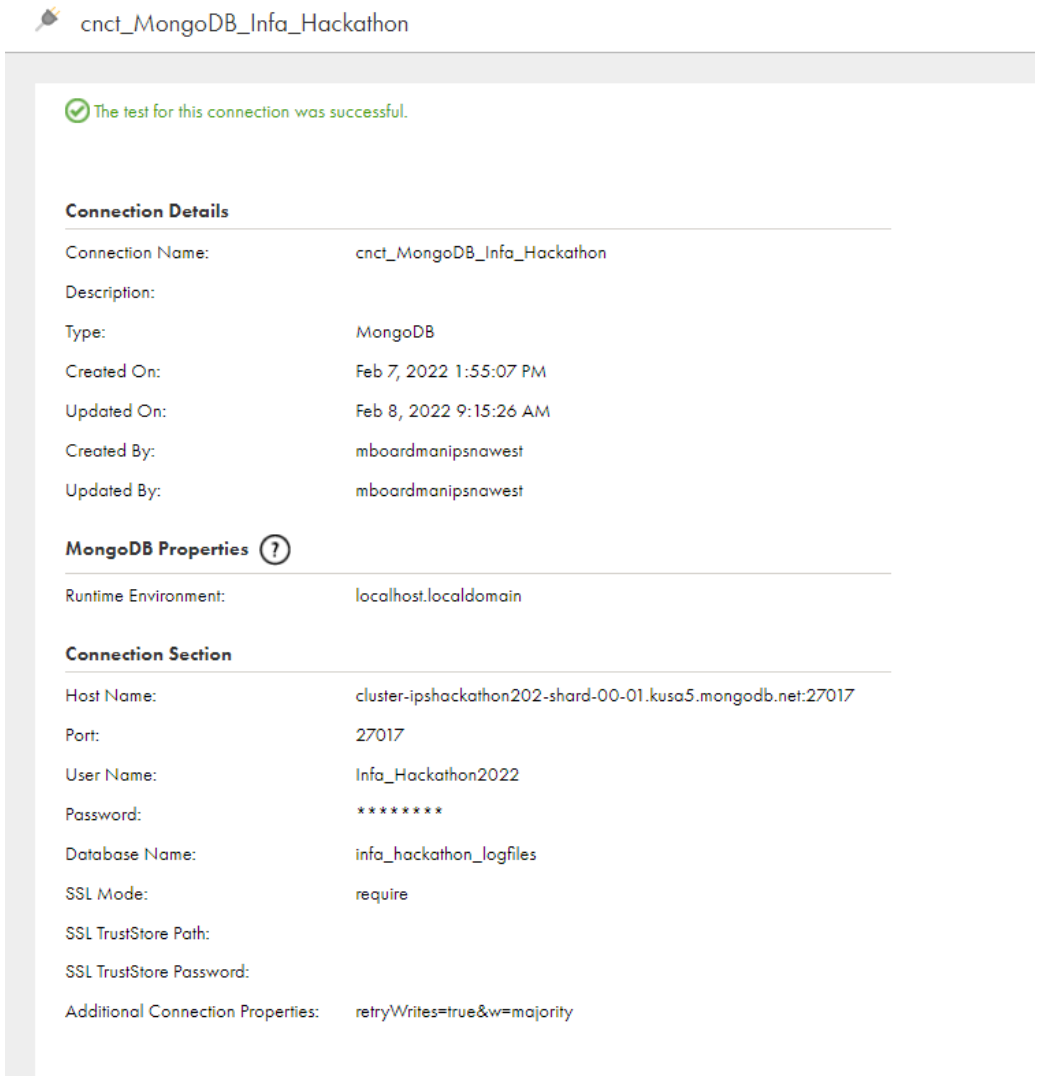
Informatica

Example: Hosted MongoDB (Atlas)



Informatica

IICS agent connection for MongoDB

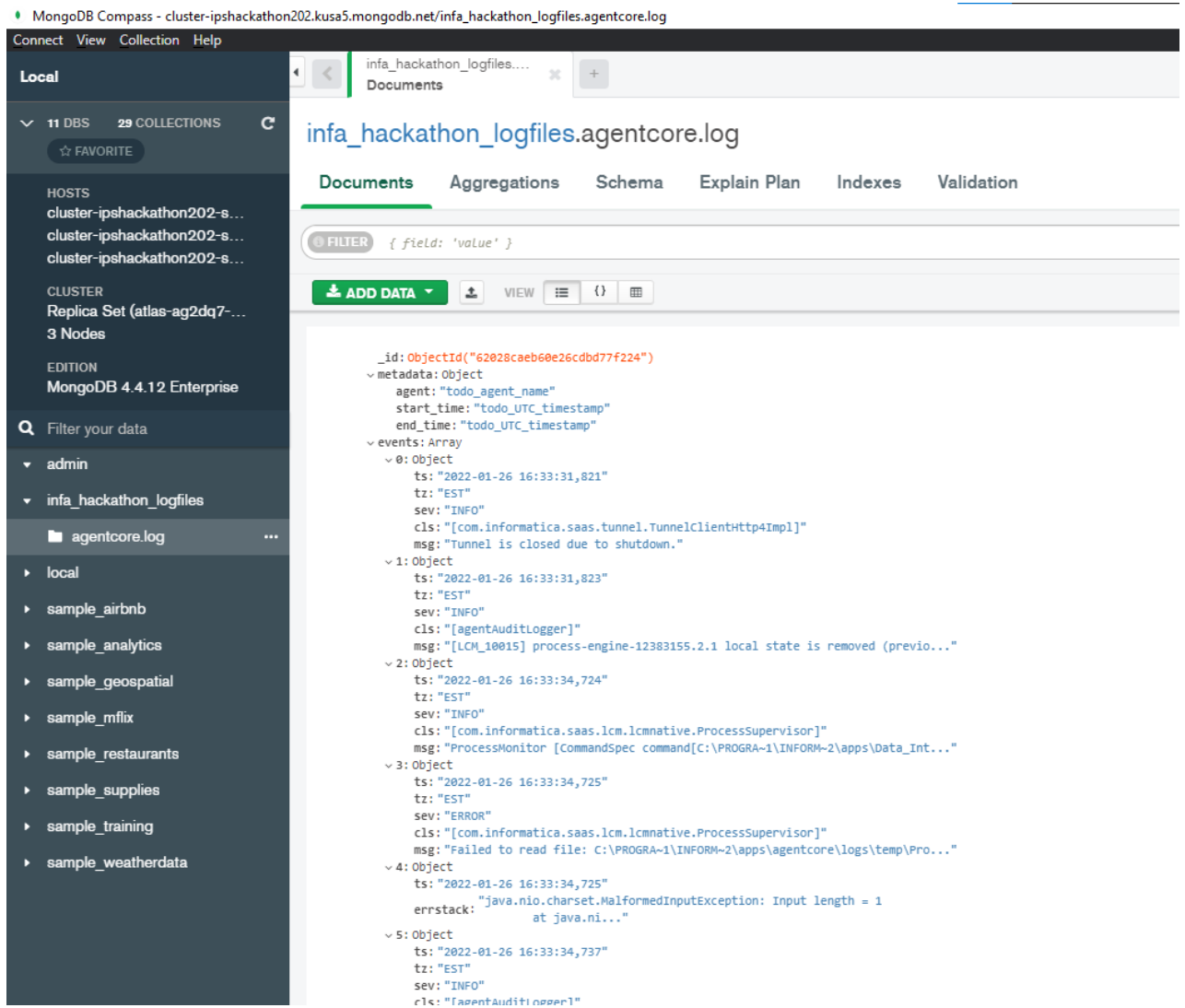


- Require SSL mode
- Connect to primary shard rather than the cluster
- Whitelist secure agent IP from Atlas
- Additional connection parameters:
  - retryWrites=true
  - w=majority

Informatica

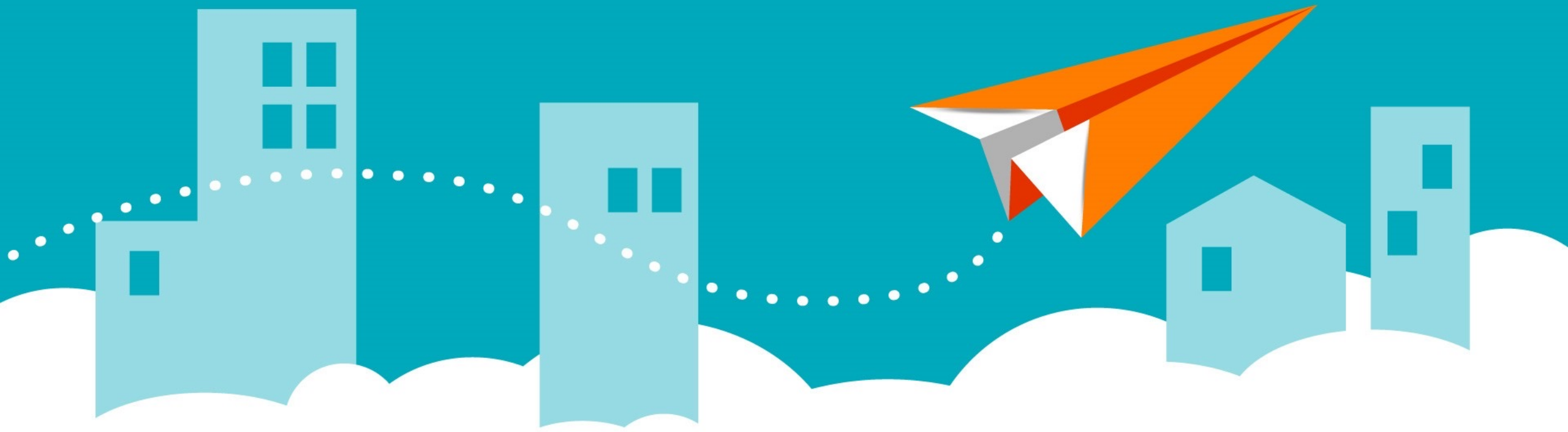
Viewing Secure Agent Log Data

- MongoDB Compass
  - View logs in canonical format
  - View complete error messages (may span multiple lines in log)
- MongoDB BI Connector
  - Plugin to allow SQL queries



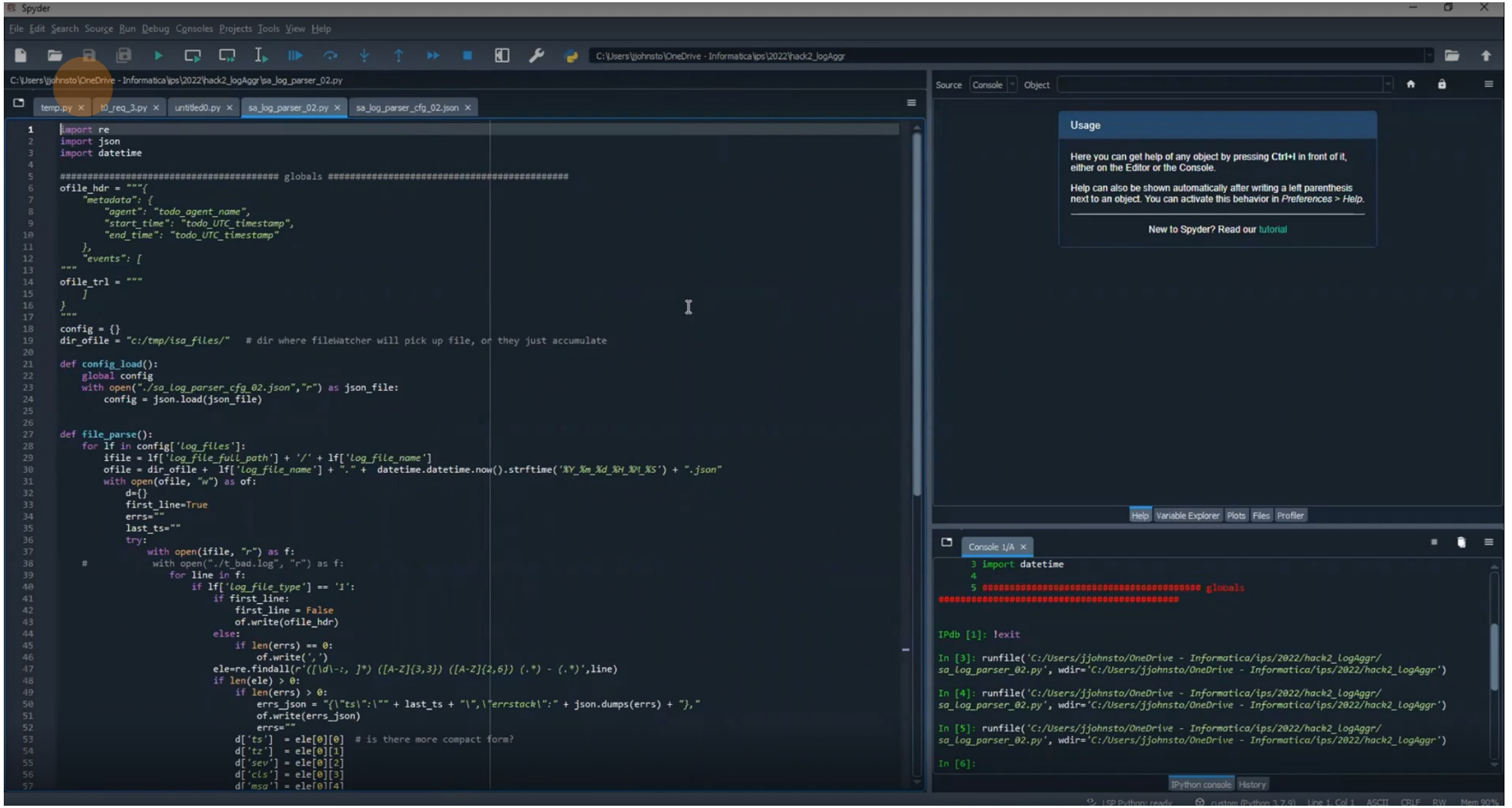
Informatica

Demo: Extract Logs from Secure Agents



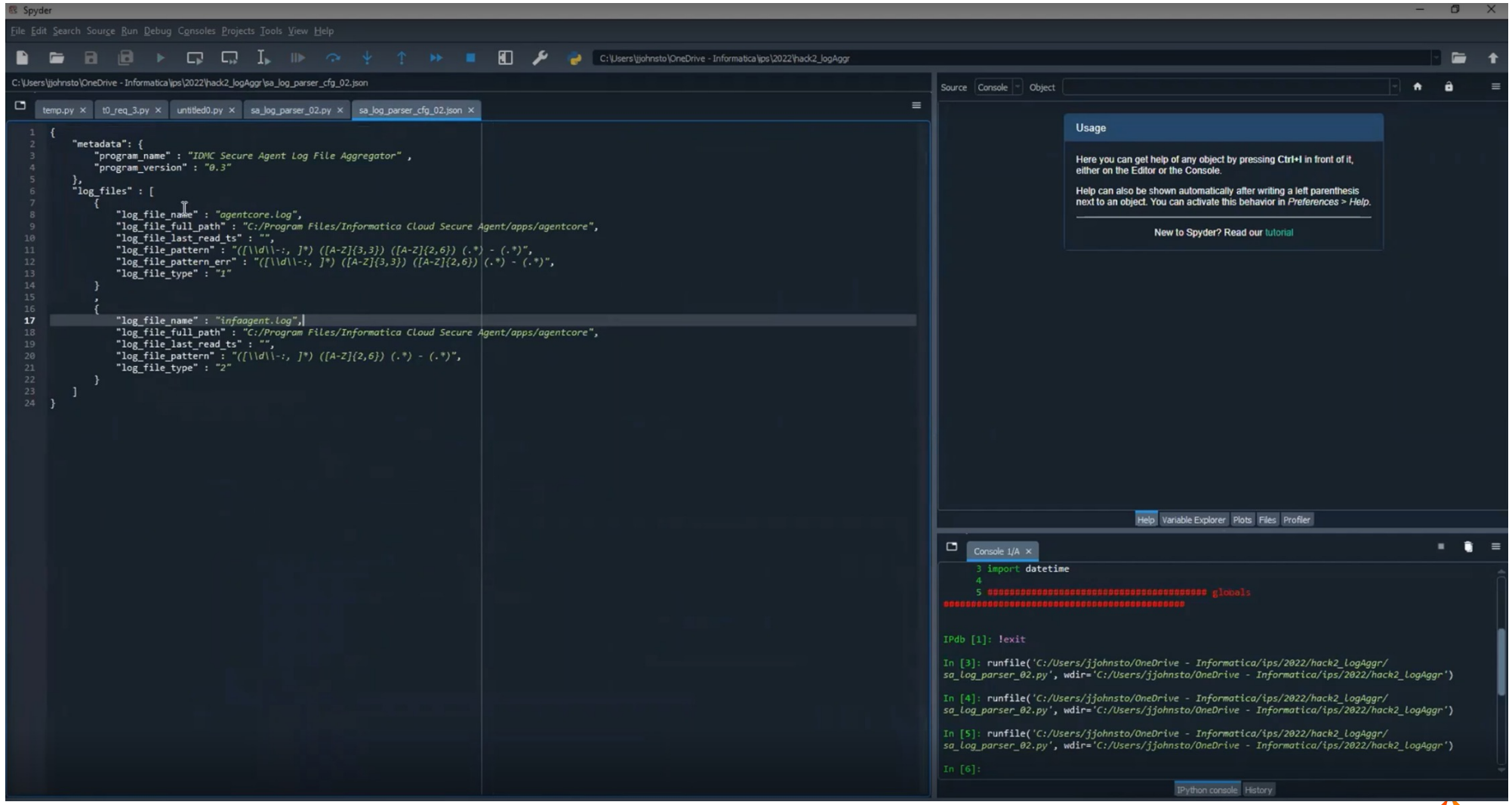
Informatica

Python translation from Log4J to JSON format



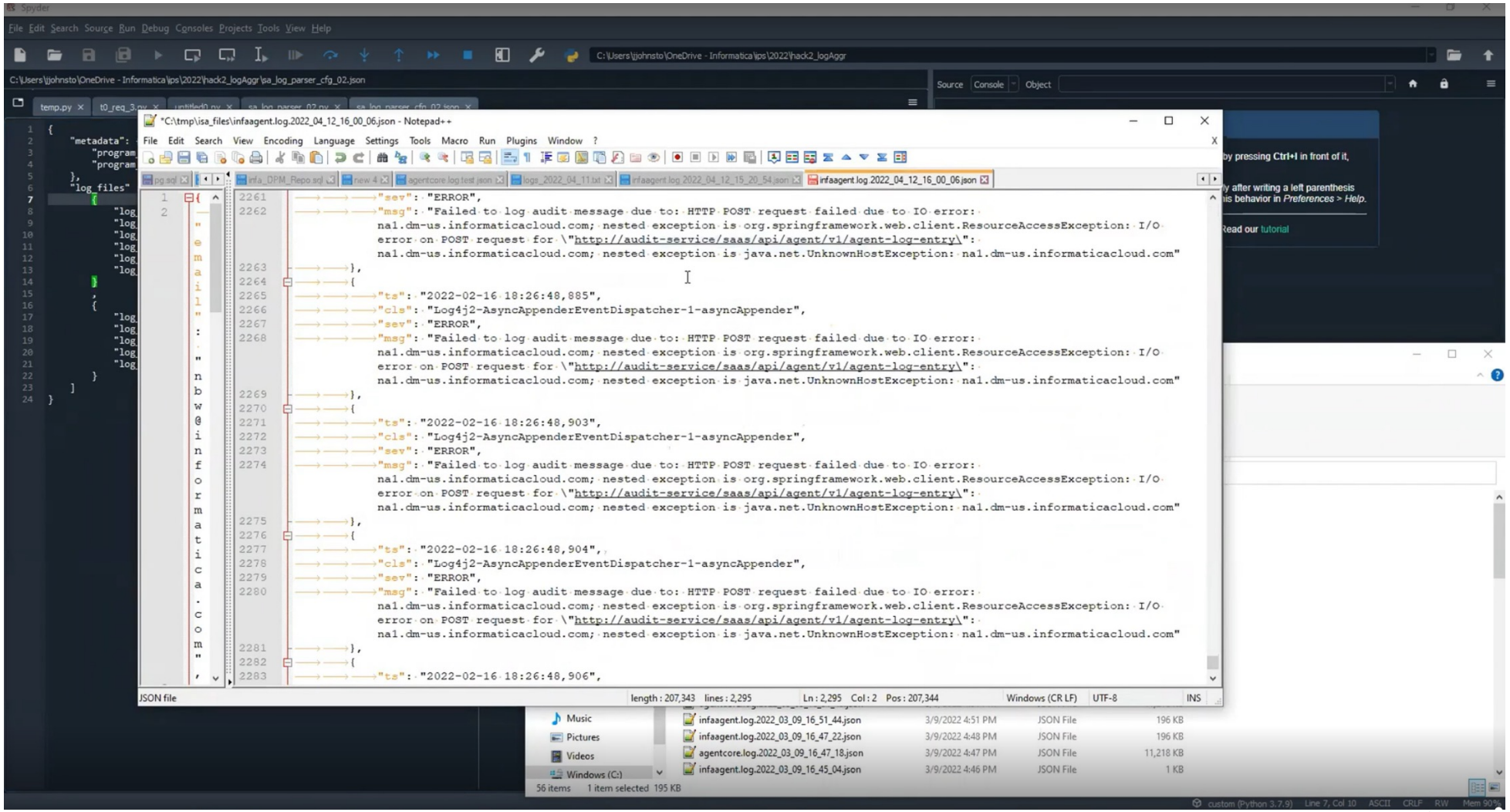
Informatica

Python translation from Log4J to JSON format



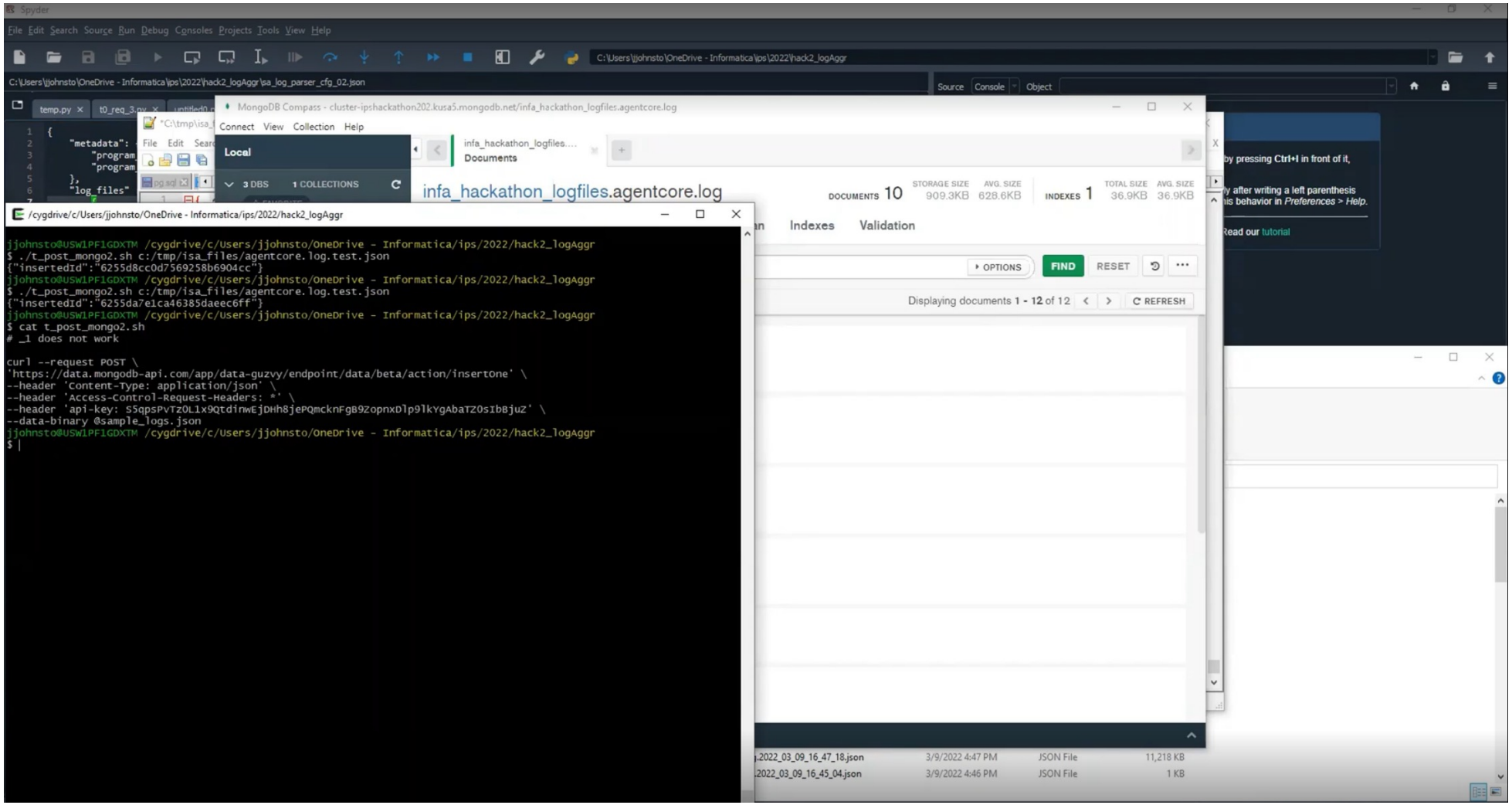
Informatica

Python translation from Log4J to JSON format



Informatica

Python translation from Log4J to JSON format



Informatica

Informatica Hackathon

- Cooperative learning environments
- Solve new and interesting challenges
- Initiatives with sales and product management teams


Matt Boardman


Ben Lee


Jim Johnstone


Srilakshmi Subramaniam


Masaki Nakasima

Informatica

Links to API Documentation

IICS Platform API:
https://docs.informatica.com/integration-cloud/cloud-platform/current-version/rest-api-reference/informatica-intelligent-cloud-services-rest-api.html

CDI API:
https://docs.informatica.com/integration-cloud/cloud-platform/current-version/rest-api-reference/data-integration-rest-api.html

CAI API:
https://docs.informatica.com/process-automation/informatica-activevos/current-version/7----apis--sdks--and-services/administration-api/other-server-admin-apis/process-monitoring-api.html

CMI API:
https://docs.informatica.com/integration-cloud/cloud-platform/current-version/rest-api-reference/mass-ingestion-files-rest-api.html

CIH API:
https://docs.informatica.com/integration-cloud/cloud-integration-hub/current-version/cloud-integration-hub/cloud-integration-hub-rest-apis.html

MDM SaaS:
https://docs.informatica.com/master-data-management-cloud/business-360-console/current-version/business-360-rest-api-reference/business-360-rest-api/rest-api-guidelines.html

MongoDB Connector:
https://docs.informatica.com/integration-cloud/cloud-data-integration-connectors/h2l/1251-configuring-the-simba-mongodb-jdbc-driver-options-for-mongo/configuring-the-simba-mongodb-jdbc-driver-options-for-mongodb-co/configure-the-simba-mongodb-jdbc-driver-options-in-a-mongodb-con/configure-the-simba-mongodb-jdbc-driver-properties.html

Thank you!

- Informatica Network: https://network.informatica.com/
- Informatica Product Documentation: https://docs.informatica.com/
- Informatica Velocity: https://velocity.informatica.com/

Informatica