

August 2022

Enterprise Log Aggregation

Matt Boardman

Informatica Professional Services



Informatica®

Agenda

What is Enterprise Log Aggregation?

ICDM Operational Insights Service

Example Solution Architecture

Informatica ICDM Platform API

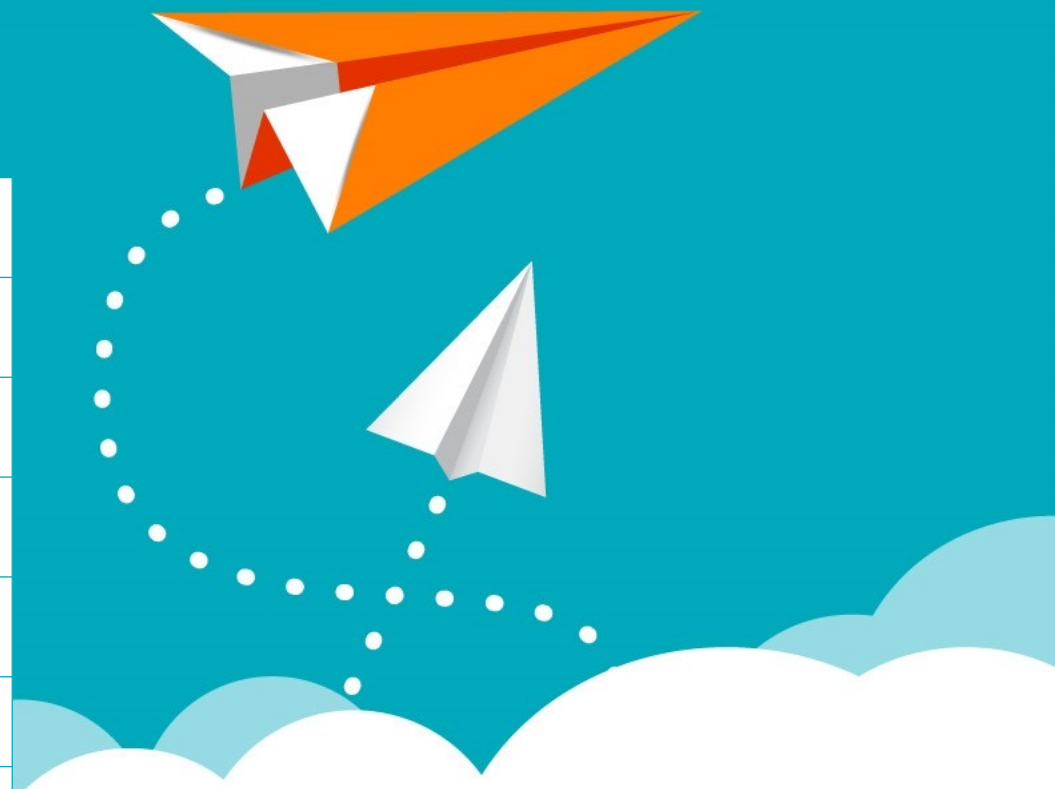
Demo: Extract Logs from Informatica Cloud

Demo: Example Dashboard using Microsoft Power BI

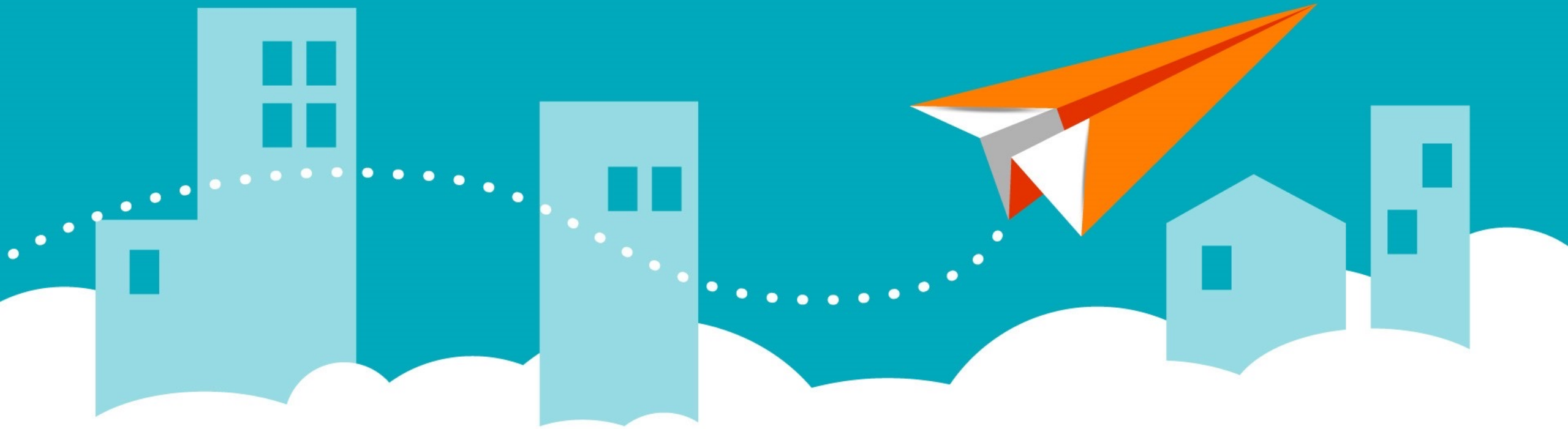
Using a Document Store Database (MongoDB)

Demo: Extract Logs from Secure Agents

Reference: Links to ICDM API Documentation



Enterprise Log Aggregation



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

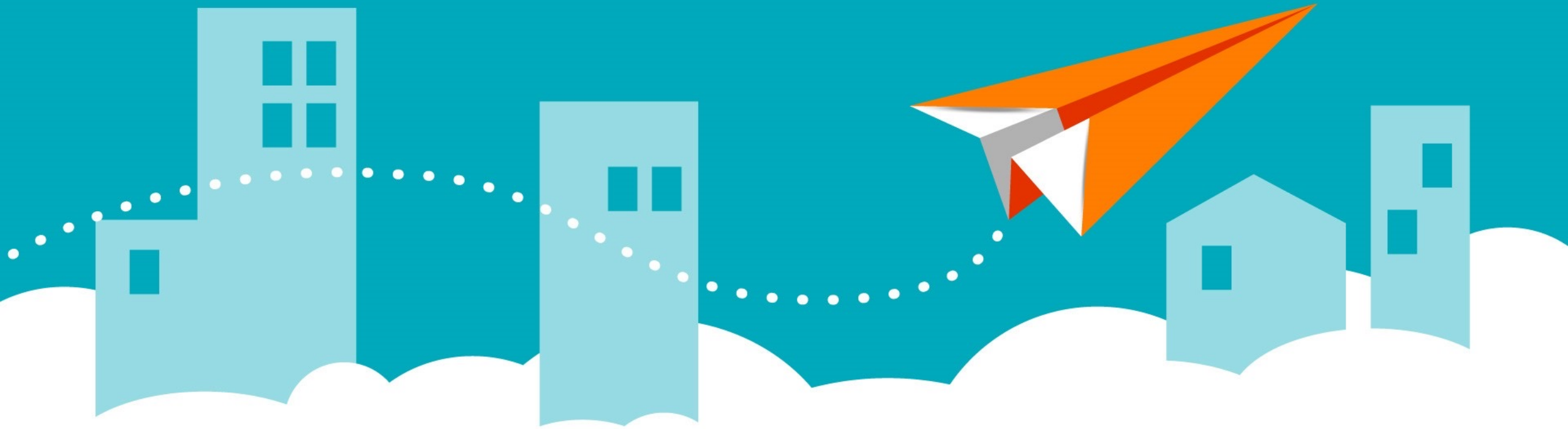


Enterprise Log Aggregation

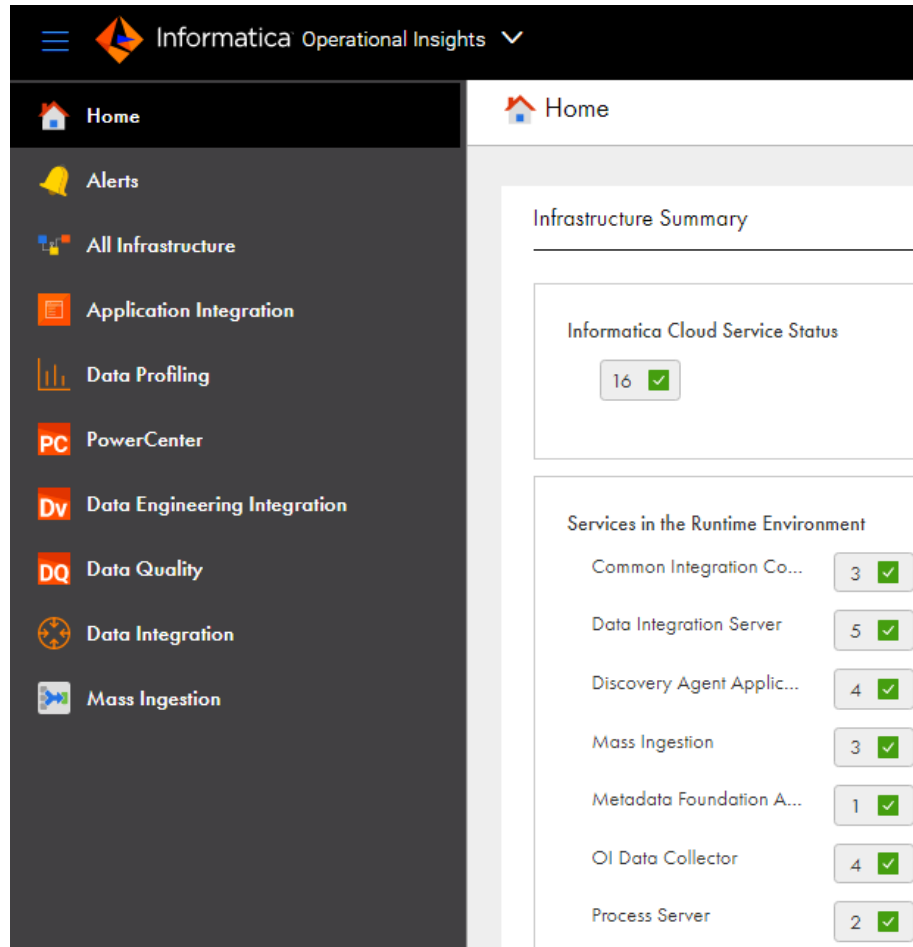


- Operations:
 - Single at-a-glance dashboard, one place to check
 - RCA of Intermittent Failures: what else is happening when a process fails on one system
 - Network failure prediction: identify outages and disruptions before they happen
- Developers:
 - Long-running processes: Informatica doesn't 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

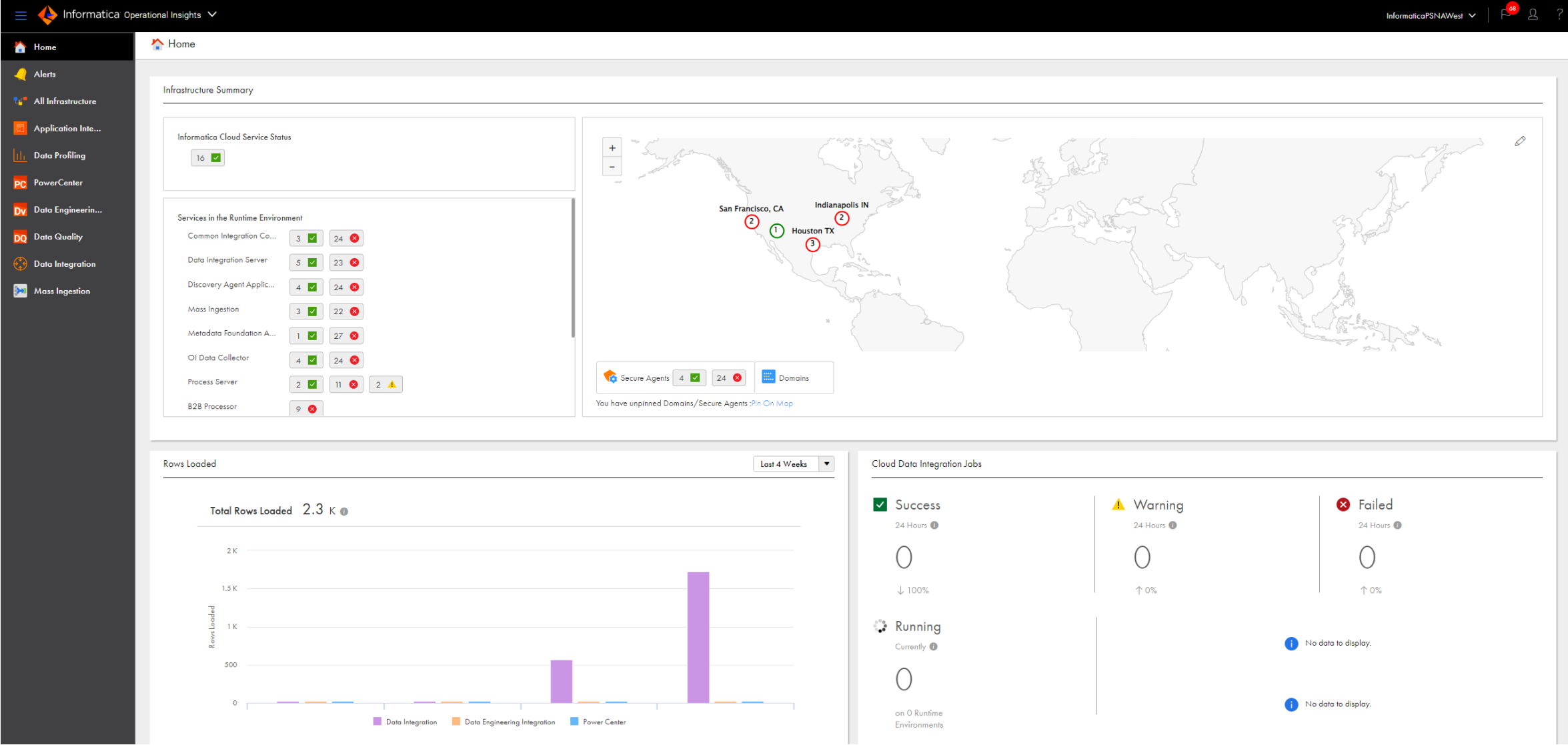


Operational Insights Service



- 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

Cloud Status Dashboard



Infrastructure Alerts

Informatica Operational Insights

InformaticaPSNAWest

68

Home

Alerts

All Infrastructure

Application Integration

Data Profiling

PowerCenter

Data Engineering Integration

Data Quality

Data Integration

Mass Ingestion

Alerts

Alerts Received

Infrastructure Alerts

Data Integration Alerts

PowerCenter Alerts

Mass Ingestion Alerts

Secure Agents

Ashutosh

asnawestinfan01

asnawestinfan02_bkp

DESKTOP-4KDPV9A

infa-server

infaserver009

invlx53ips2.informatica.com

ip-172-31-22-171.us-west-1.compute.internal

LAPTOP-G0UQPCT5

LAPTOP-OHUFMIQ5

lithium-hlg

localhost.localdomain

MNakasima

ochen

ochen - USWPF2QN9C0-AAD

psvlxprof2.informatica.com

RRG_CD1_1

USW1PFOXQCPA

USW1PFOZDRGS

USWPF0MD8E1-AAD

USWPF1SGELW-AAD

USWPF1SGETF-AAD

Alert settings for Secure Agent : MNakasima

Disable All

Reset Values

Secure Agent Alerts

☒

Secure Agent is unavailable.

☒

CPU usage by the Secure Agent crosses 90 % for a duration of 30 minutes.

☒

Memory usage by the Secure Agent crosses 90 % for a duration of 30 minutes.

☒

Disk usage by the Secure Agent crosses 90 % for a duration of 30 minutes.

☒ Email Recipients

mboardman@PSNAWest

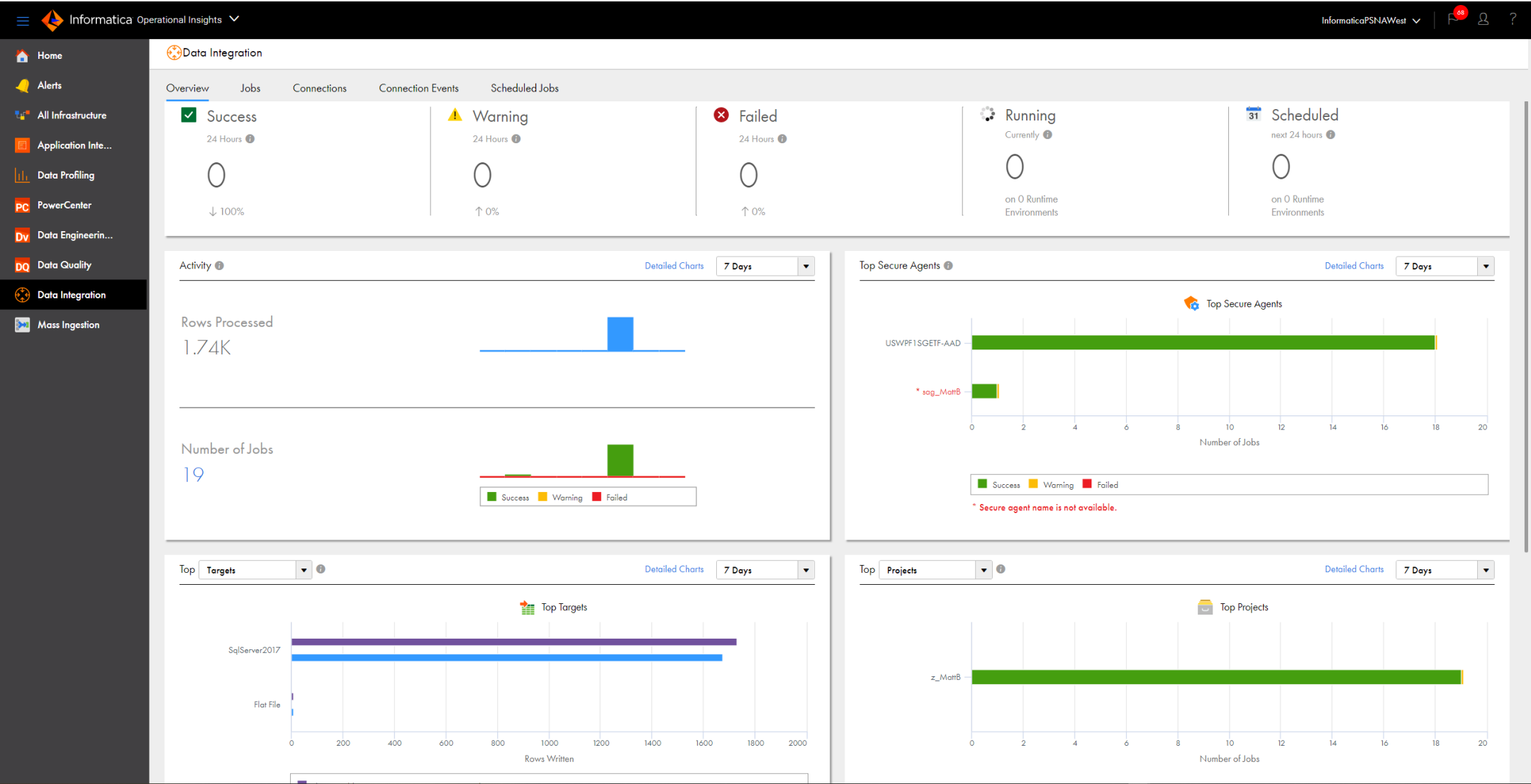
☐ Run Custom Script

Add Script Location

+ Add Service Specific Alert



Cloud Data Integration



Cloud Data Profiling

Informatica Operational Insights

Home

Alerts

All Infrastructure

Application Integration

Data Profiling

PowerCenter

Data Engineering Integration

Data Quality

Data Integration

Mass Ingestion

Data Profiling

Jobs (41 items found) Up to Date Updated Aug 10, 2022, 4:52 PM Auto Refresh Find

Filter

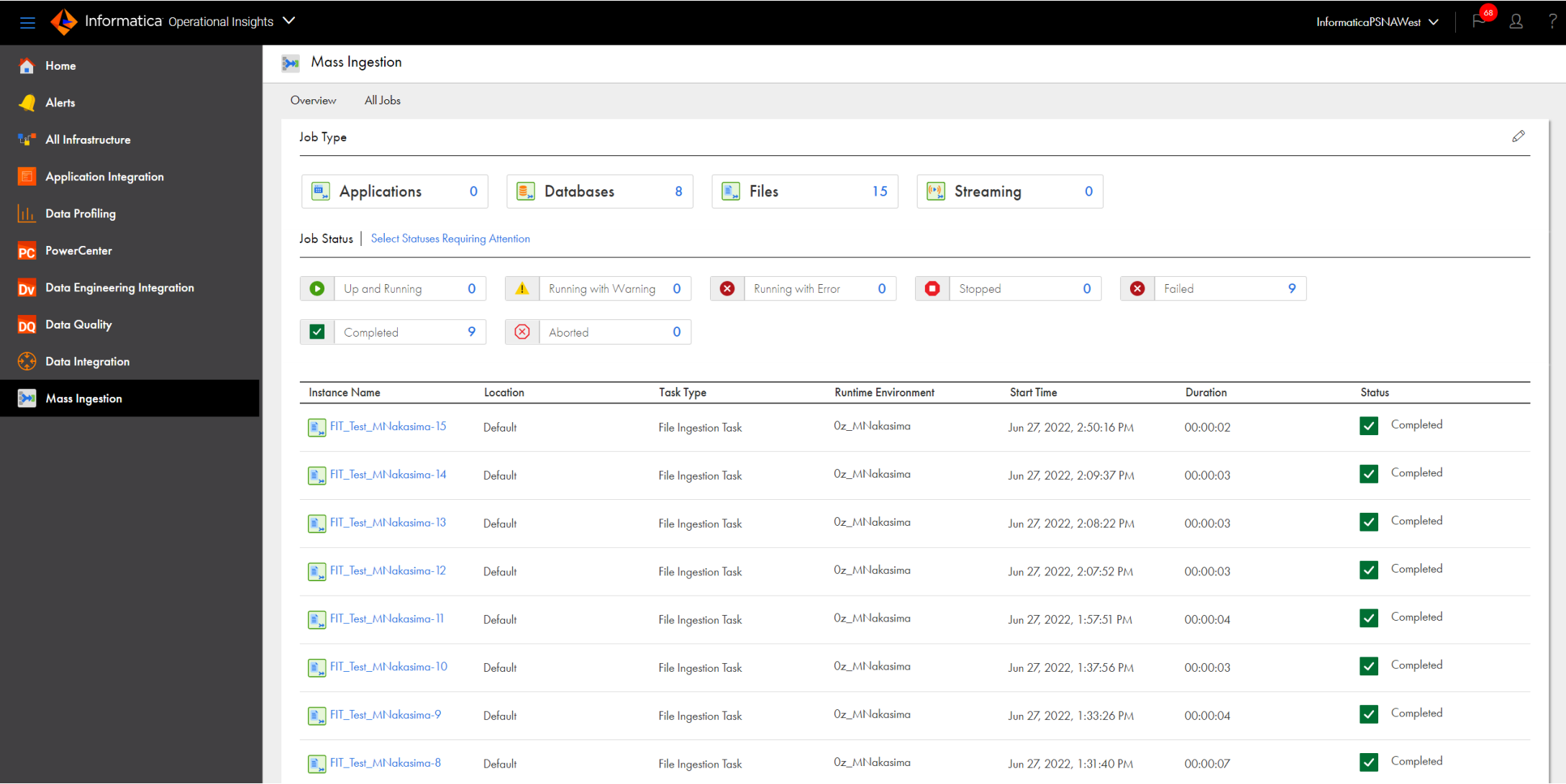
Update Times: Last Year Add Filter

Instance Name	Location	Subtasks	Start Time	End Time
anto_ff_Profile - run - 1-3	Anto	4	Jul 15, 2022, 1:42 PM	Jul 15, 2022, 1:43 PM
anto_ff_Profile - run - 1-2	Anto	4	Jul 15, 2022, 12:14 PM	Jul 15, 2022, 12:15 PM
anto_ff_Profile - run - 1-1	Anto	4	Jul 15, 2022, 11:47 AM	Jul 15, 2022, 11:49 AM
Outlier - Profile_MN_LFA1 - run - 1-2	z_MNakasima	1	Apr 18, 2022, 2:43 PM	Apr 18, 2022, 2:43 PM
Profile_MN_LFA1 - run - 1-1	z_MNakasima	4	Apr 18, 2022, 2:42 PM	Apr 18, 2022, 2:43 PM
Profile_DQ_Input - run - 8-20	Ruben/CDQ	2	Mar 22, 2022, 8:12 AM	Mar 22, 2022, 8:16 AM
Outlier - Profile_DQ_Input - run - 7-19	Ruben/CDQ	1	Dec 6, 2021, 3:35 PM	Dec 6, 2021, 3:35 PM
Profile_DQ_Input - run - 7-18	Ruben/CDQ	4	Dec 6, 2021, 3:34 PM	Dec 6, 2021, 3:35 PM
Profile_DQ_Input - run - 7-17	Ruben/CDQ	4	Dec 6, 2021, 3:05 PM	Dec 6, 2021, 3:06 PM
Outlier - Profile_DQ_Input - run - 6-16	Ruben/CDQ	1	Dec 3, 2021, 10:34 AM	Dec 3, 2021, 10:34 AM
Profile_DQ_Input - run - 6-15	Ruben/CDQ	4	Dec 3, 2021, 10:32 AM	Dec 3, 2021, 10:34 AM
Outlier - Profile_DQ_Input - run - 5-14	Ruben/CDQ	1	Dec 3, 2021, 7:16 AM	Dec 3, 2021, 7:16 AM
Profile_DQ_Input - run - 5-13	Ruben/CDQ	4	Dec 3, 2021, 7:14 AM	Dec 3, 2021, 7:16 AM
Outlier - Profile_DQ_Input - run - 4-12	Ruben/CDQ	1	Dec 3, 2021, 6:59 AM	Dec 3, 2021, 6:59 AM
Profile_DQ_Input - run - 4-11	Ruben/CDQ	4	Dec 3, 2021, 6:57 AM	Dec 3, 2021, 6:59 AM
Profile_DQ_Input - run - 4-10	Ruben/CDQ	4	Dec 3, 2021, 6:25 AM	Dec 3, 2021, 6:26 AM
Profile_DQ_Input - run - 4-9	Ruben/CDQ	4	Dec 2, 2021, 3:50 PM	Dec 2, 2021, 3:51 PM

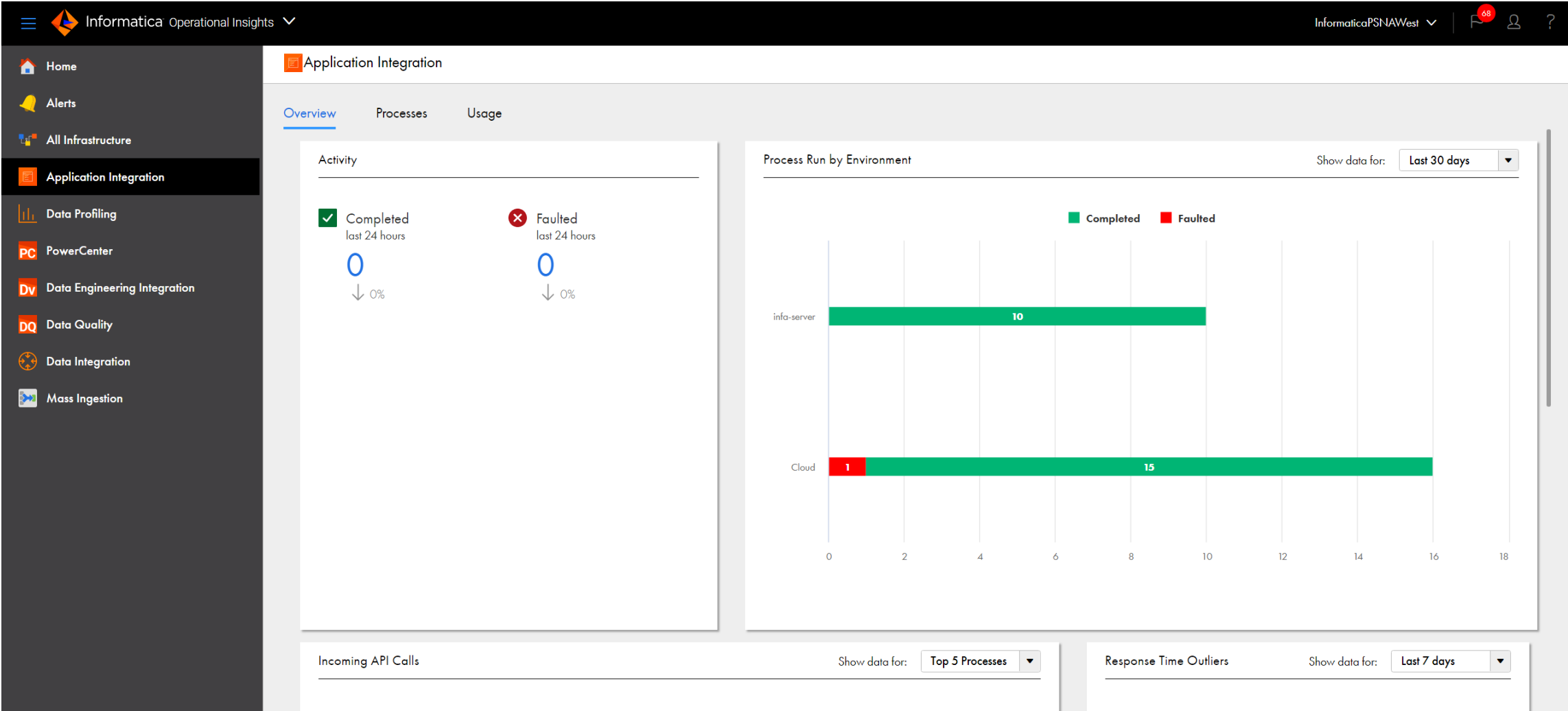
1 - 25 of 41 items Page 1 of 2 Items Per Page: 25



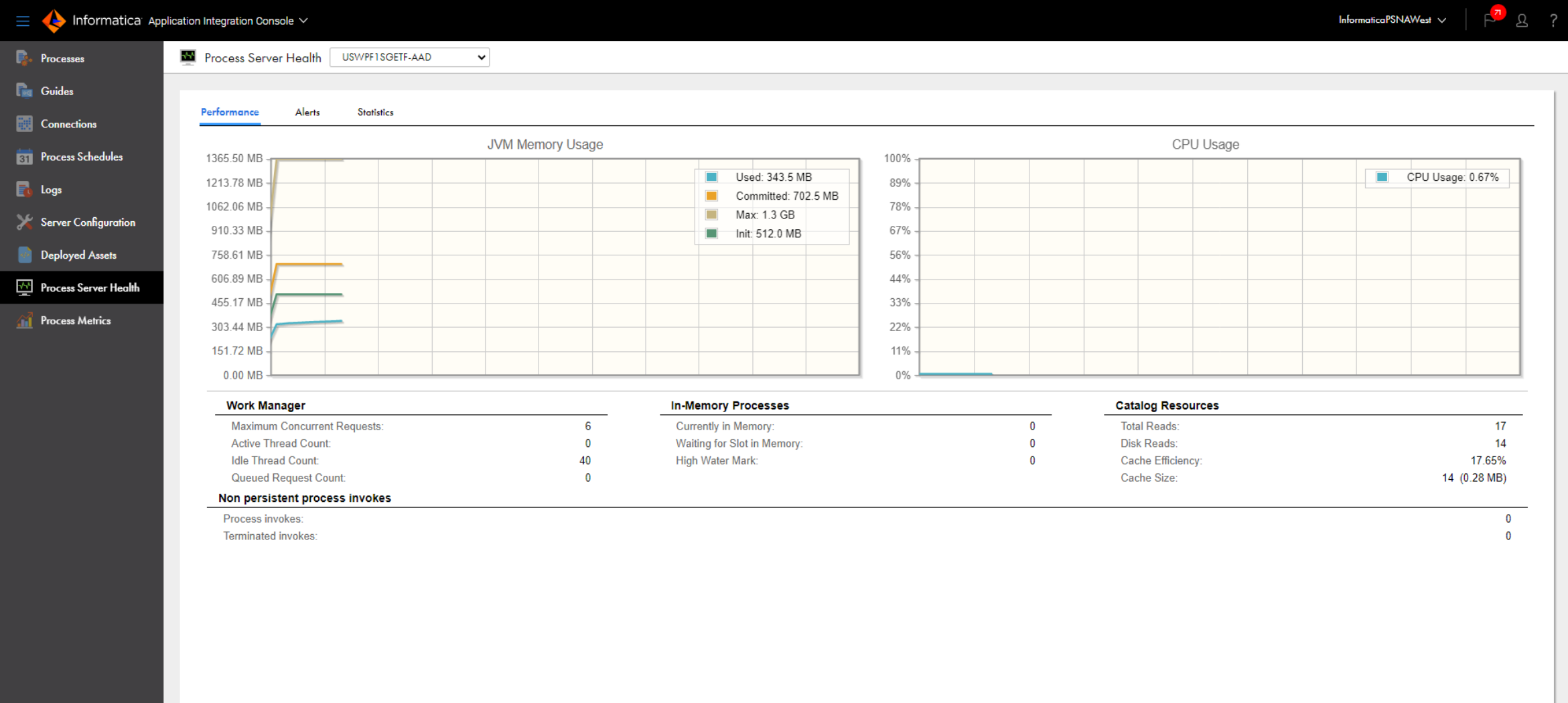
Cloud Mass Ingestion



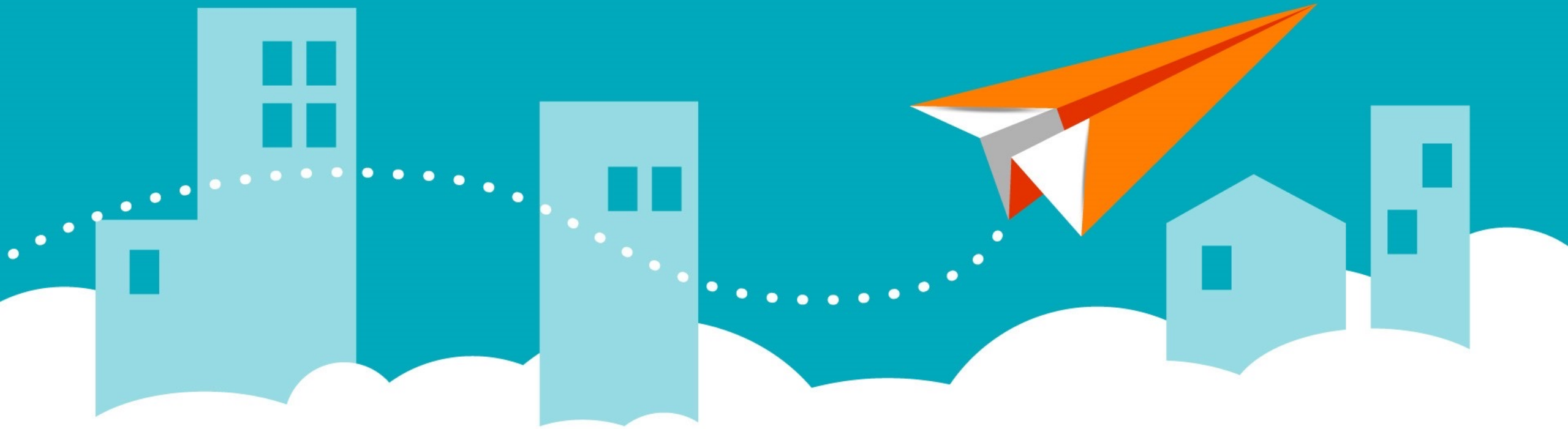
Cloud Application Integration



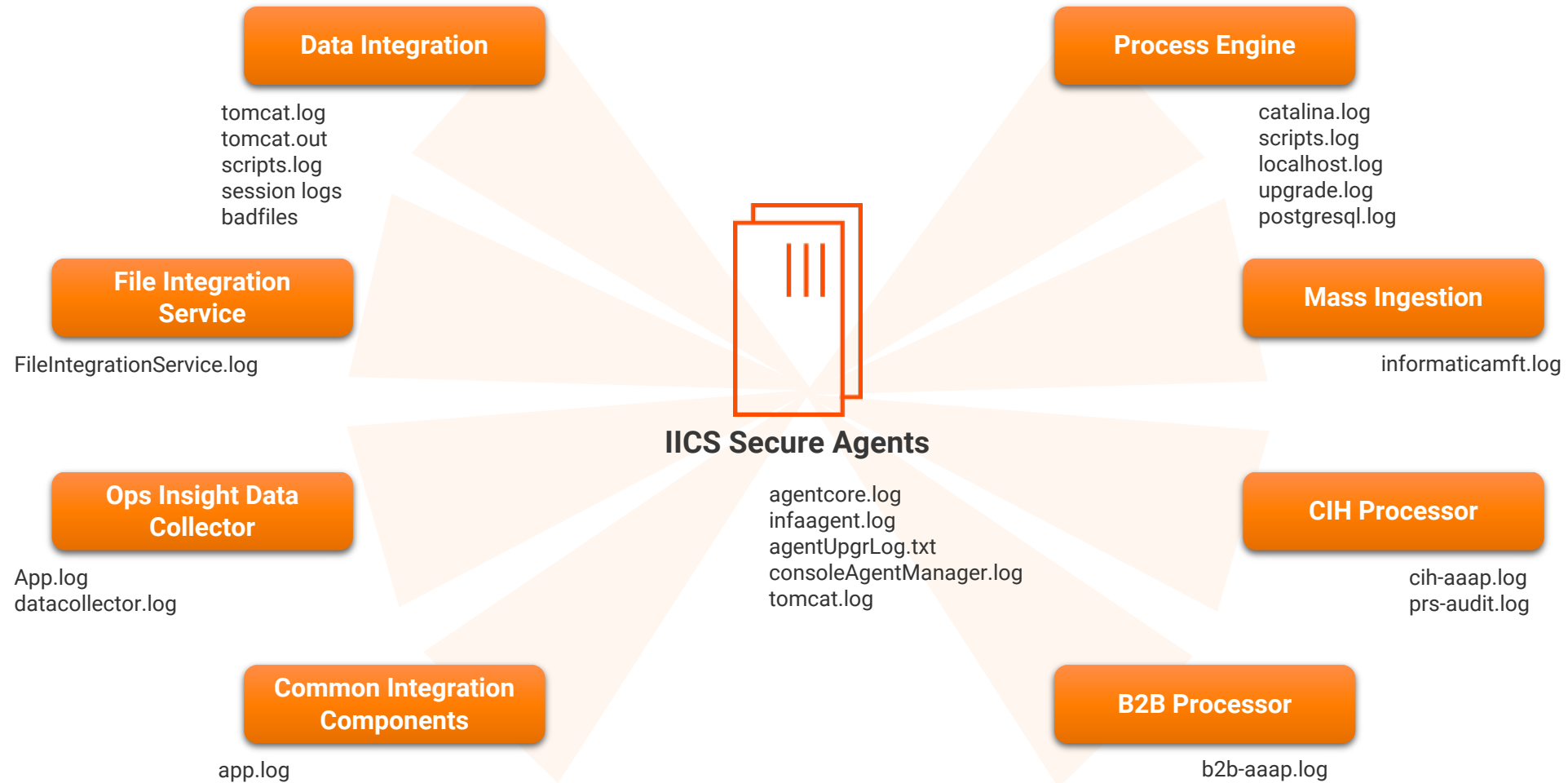
CAI Console



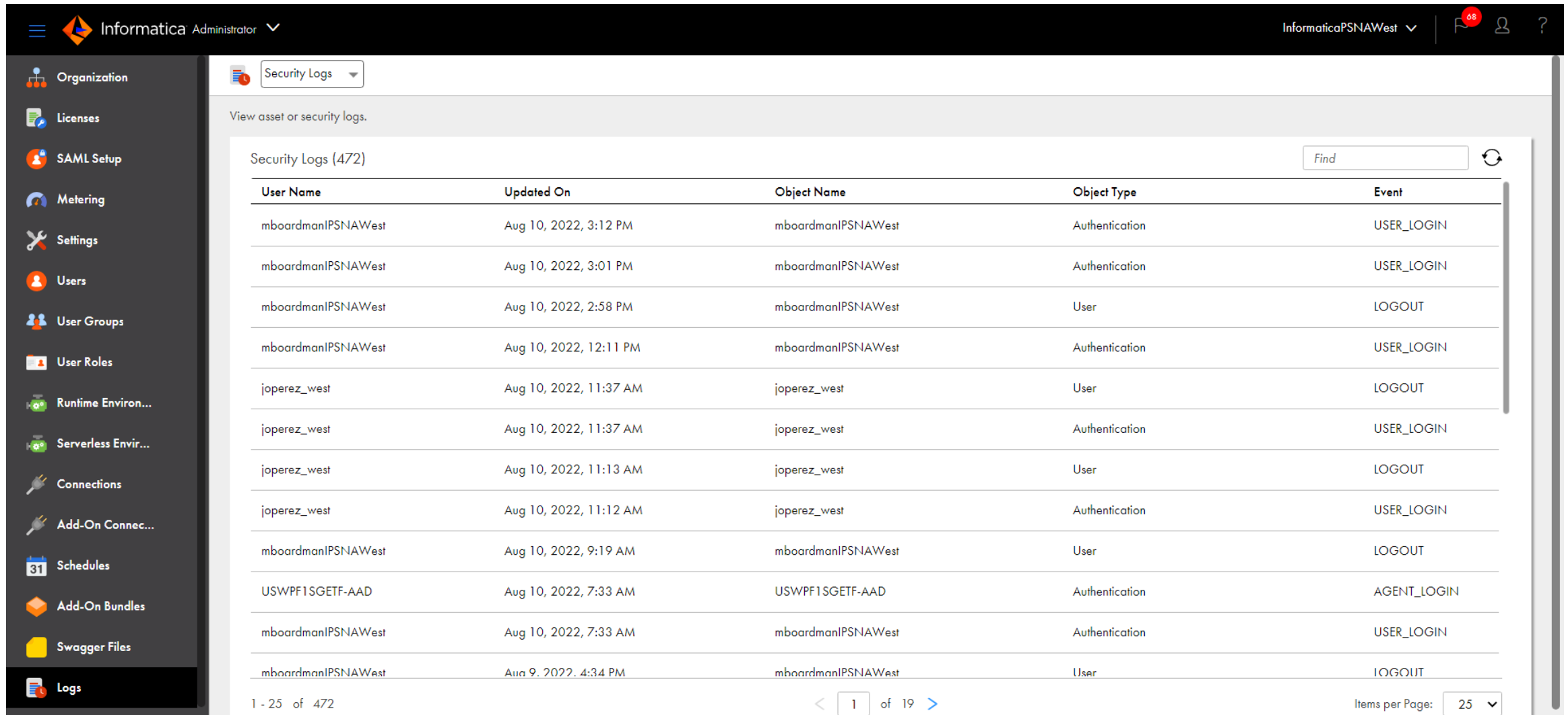
Example Solution Architecture



Service Logs on Informatica Secure Agents



Asset and Security Logs in Administrator Applet



Informatica Administrator

InformaticaPSNAWest

Security Logs

View asset or security logs.

Security Logs (472)

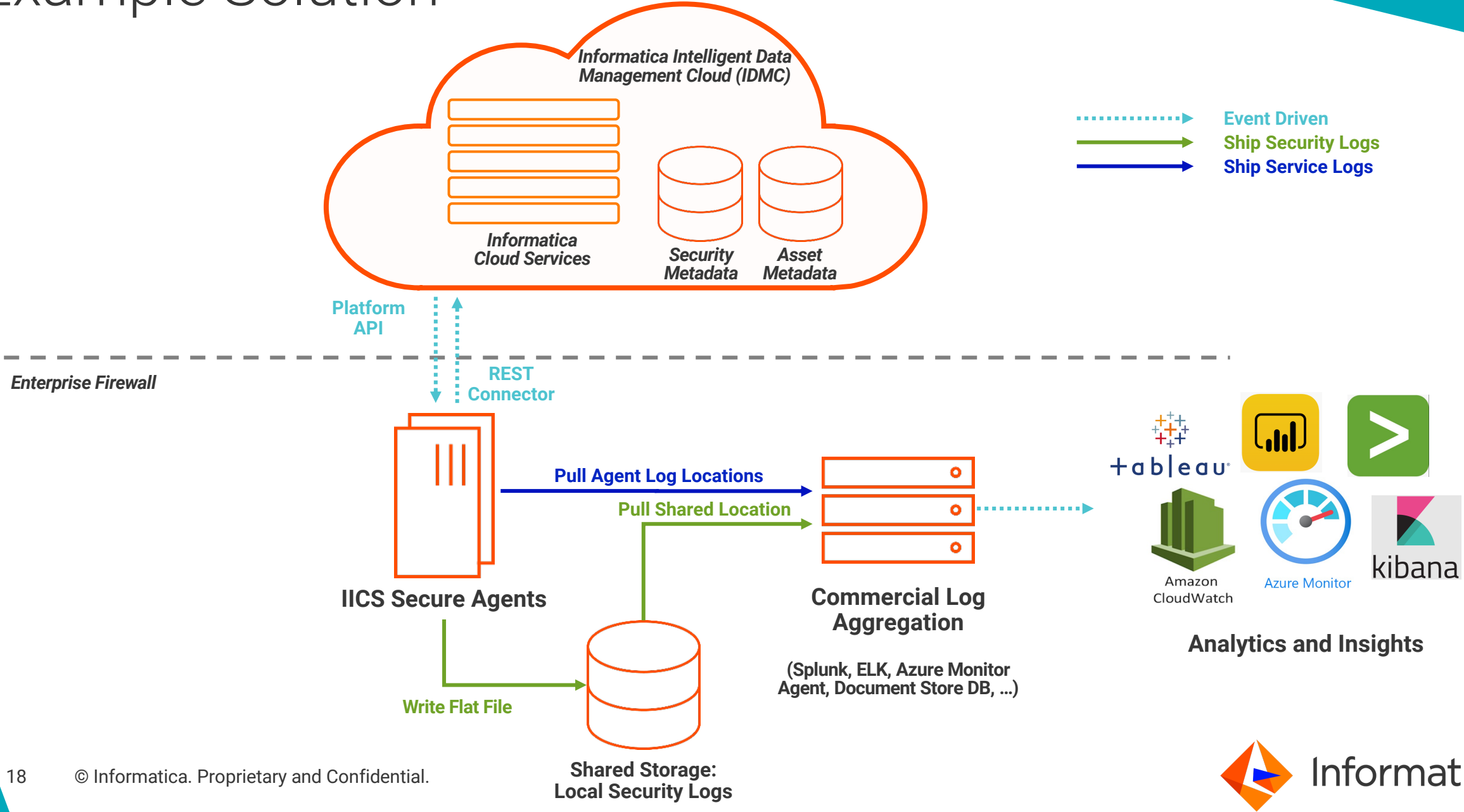
User Name	Updated On	Object Name	Object Type	Event
mboardmanIPSNWest	Aug 10, 2022, 3:12 PM	mboardmanIPSNWest	Authentication	USER_LOGIN
mboardmanIPSNWest	Aug 10, 2022, 3:01 PM	mboardmanIPSNWest	Authentication	USER_LOGIN
mboardmanIPSNWest	Aug 10, 2022, 2:58 PM	mboardmanIPSNWest	User	LOGOUT
mboardmanIPSNWest	Aug 10, 2022, 12:11 PM	mboardmanIPSNWest	Authentication	USER_LOGIN
joperez_west	Aug 10, 2022, 11:37 AM	joperez_west	User	LOGOUT
joperez_west	Aug 10, 2022, 11:37 AM	joperez_west	Authentication	USER_LOGIN
joperez_west	Aug 10, 2022, 11:13 AM	joperez_west	User	LOGOUT
joperez_west	Aug 10, 2022, 11:12 AM	joperez_west	Authentication	USER_LOGIN
mboardmanIPSNWest	Aug 10, 2022, 9:19 AM	mboardmanIPSNWest	User	LOGOUT
USWPF1SGETF-AAD	Aug 10, 2022, 7:33 AM	USWPF1SGETF-AAD	Authentication	AGENT_LOGIN
mboardmanIPSNWest	Aug 10, 2022, 7:33 AM	mboardmanIPSNWest	Authentication	USER_LOGIN
mboardmanIPSNWest	Aug 9, 2022, 4:34 PM	mboardmanIPSNWest	User	LOGOUT

1 - 25 of 472

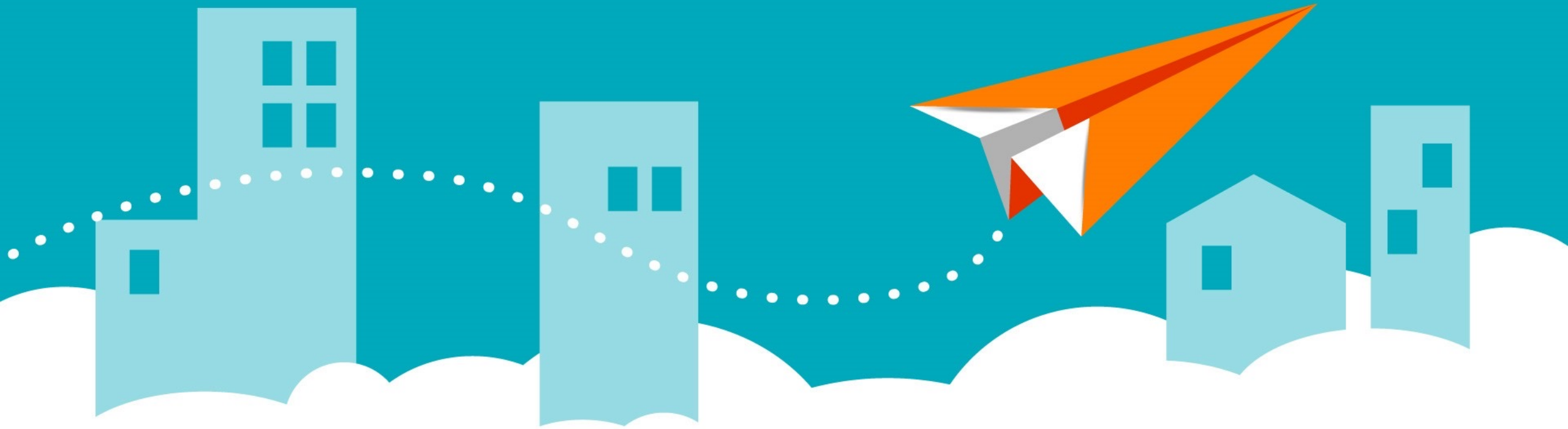
1 of 19

Items per Page: 25

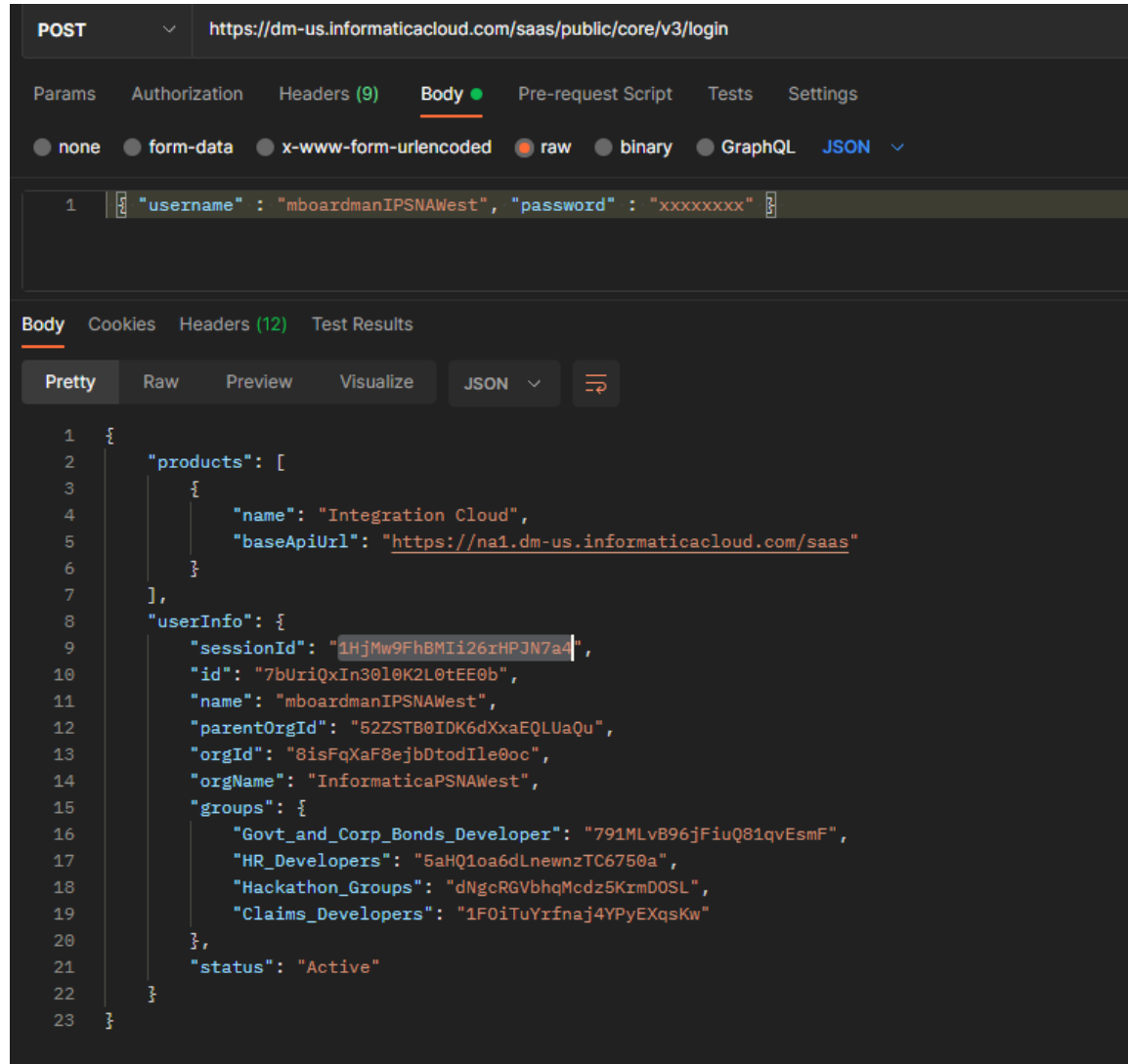
Example Solution



Informatica ICDM Platform API



Cloud Platform API - Login



The screenshot displays a REST client interface for a POST request to `https://dm-us.informaticacloud.com/saas/public/core/v3/login`. The request body is a JSON object with `username` and `password` fields. The response body is a JSON object containing product information and user details.

```
POST https://dm-us.informaticacloud.com/saas/public/core/v3/login

Body
  none form-data x-www-form-urlencoded raw binary GraphQL JSON
1 [{"username": "mboardmanIPSNWest", "password": "xxxxxxx"}]

Body Cookies Headers (12) Test Results
  Pretty Raw Preview Visualize JSON
1 {
2   "products": [
3     {
4       "name": "Integration Cloud",
5       "baseApiUrl": "https://na1.dm-us.informaticacloud.com/saas"
6     }
7   ],
8   "userInfo": {
9     "sessionId": "1HjMw9Fh8MIi26xHPJN7a4",
10    "id": "7bUriQxIn30l0K2L0tEE0b",
11    "name": "mboardmanIPSNWest",
12    "parentOrgId": "52ZSTB0IDK6dXxaEQLUaQu",
13    "orgId": "8isFqXaF8ejbDtodIle0oc",
14    "orgName": "InformaticaPSNAWest",
15    "groups": {
16      "Govt_and_Corp_Bonds_Developer": "791MLvB96jFiuQ81qvEsmF",
17      "HR_Developers": "5aHQ1oa6dLnewnzTC6750a",
18      "Hackathon_Groups": "dNgcRGVbhqMcdz5KxmDOSL",
19      "Claims_Developers": "1F0iTuYrfnaj4YPyEXqsKw"
20    },
21    "status": "Active"
22  }
23 }
```


Cloud Platform API – Security Logs

GET https://na1.dm-us.informaticacloud.com/saas/public/core/v3/securityLog?q=entryTime>=2022-08-04T19:22:00.000Z;entryTime<=2022-08-09T16:05:00.000Z

Params Authorization Headers (8) Body Pre-request Script Tests Settings

Headers Hide auto-generated headers

KEY	VALUE
Cache-Control	no-cache
Postman-Token	<calculated when request is sent>
Host	<calculated when request is sent>
User-Agent	PostmanRuntime/7.29.2
Accept	/*
Accept-Encoding	gzip, deflate, br
Connection	keep-alive
INFA-SESSION-ID	1HJMw9FhBMII26rHPJN7a4

Body Cookies Headers (15) Test Results

Pretty Raw Preview Visualize JSON

```
1  "entries": [  
2    {  
3      "id": "8Pmiejxt0uxc0p8hQk7AuC",  
4      "orgId": "8isFqXaF8ejbDtodIle0oc",  
5      "actor": "mboardmanIPSNWest",  
6      "entryTime": "2022-08-04T19:22:50.000Z",  
7      "objectId": "7bUriQxIn30l0K2L0tEE0b",  
8      "objectName": "mboardmanIPSNWest",  
9      "actionCategory": "Authentication",  
10     "actionEvent": "USER_LOGIN",  
11   },  
12   {  
13     "id": "10DuiInlTyAleUNutwv60R",  
14     "orgId": "8isFqXaF8ejbDtodIle0oc",  
15     "actor": "System built-in user",  
16     "entryTime": "2022-08-04T19:30:24.000Z",  
17     "objectId": "2vyARXuRoVe10SLyx06Uaj",  
18     "objectName": "brclark_west",  
19     "actionCategory": "User",  
20     "actionEvent": "PASSWORD_RESET",  
21   },  
22   ]  
}
```

Cloud Platform API – Asset (Audit) Logs

GET https://na1.dm-us.informaticacloud.com/saas/api/v2/auditlog

Params Authorization Headers (8) Body Pre-request Script Tests Settings

Headers Hide auto-generated headers

KEY	VALUE
☒ Cache-Control	no-cache
☒ Postman-Token	<calculated when request is sent>
☒ Host	<calculated when request is sent>
☒ User-Agent	PostmanRuntime/7.29.2
☒ Accept	/*/*
☒ Accept-Encoding	gzip, deflate, br
☒ Connection	keep-alive
☒ lcSessionId	1HJMw9FhBMII26rHPJN7a4
Key	Value

Body Cookies Headers (12) Test Results

Pretty Raw Preview Visualize JSON

```
1 {
2   "type": "auditLogEntry",
3   "version": 0,
4   "id": "8isFqXaF8ejbDtodIle0ocD0000000000055Q",
5   "orgId": "012AJ1",
6   "username": "mboardmanIPSNWest",
7   "entryTime": "2022-08-11T19:14:57.000Z",
8   "entryTimeUTC": "2022-08-11T23:14:57.000Z",
9   "objectId": "30hnPDfQ8c2c9tjw0GbmMj",
10  "objectName": "mt_LoginV3",
11  "category": "MCT",
12  "event": "UPDATE",
13  "eventParam": "UPDATE MCT Successful.",
14  "message": "aevent.MCT.UPDATE"
15 }
16 }
```

Cloud Platform API – CDI Job Logs

GET <https://na1.dm-us.informaticacloud.com/saas/api/v2/activity/activityLog>

Params Authorization Headers (8) Body Pre-request Script Tests Settings

Headers Hide auto-generated headers

KEY	VALUE
☒ Cache-Control	no-cache
☒ Postman-Token	<calculated when request is sent>
☒ Host	<calculated when request is sent>
☒ User-Agent	PostmanRuntime/7.29.2
☒ Accept	*/*
☒ Accept-Encoding	gzip, deflate, br
☒ Connection	keep-alive
☒ icSessionId	1HjMw9FhBMiI26rHPJN7a4

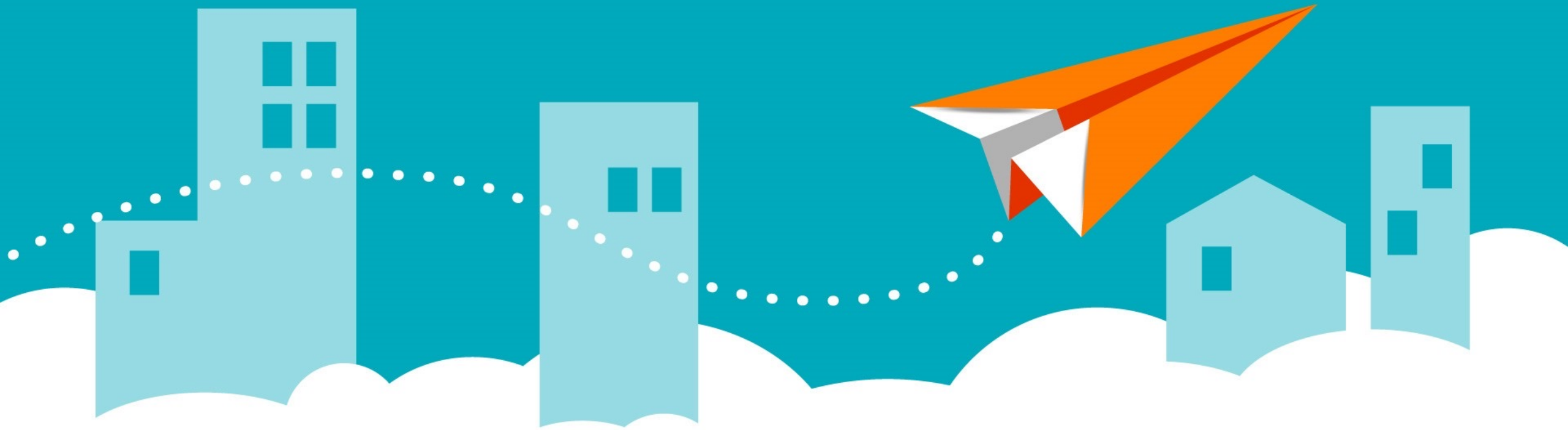
Key Value

Body Cookies Headers (12) Test Results

Pretty Raw Preview Visualize JSON

```
1 [
2   {
3     "@type": "activityLogEntry",
4     "id": "012AJ1C10000000000LG9",
5     "type": "MTT",
6     "objectId": "012AJ10Z000000000005F",
7     "objectName": "mt_ActivityLog",
8     "runId": 3,
9     "startTime": "2022-08-11T19:35:59.000Z",
10    "endTime": "2022-08-11T19:36:41.000Z",
11    "startTimeUtc": "2022-08-11T23:35:59.000Z",
12    "endTimeUtc": "2022-08-11T23:36:41.000Z",
13    "state": 1,
14    "failedSourceRows": 0,
15    "successSourceRows": 1,
16    "failedTargetRows": 0,
17    "successTargetRows": 767,
18    "startedBy": "mboardmanipsnawest",
19    "runContextType": "REST_API_V2",
20    "entries": [
21      {
22        "@type": "activityLogEntry",
23        "id": "4570320022",
24        "type": "MTT",
25        "objectId": "012AJ10Z000000000005F",
26        "objectName": "mt_ActivityLog",
27        "runId": 3,
28        "startTime": "2022-08-11T19:35:59.000Z",
29        "endTime": "2022-08-11T19:36:41.000Z",
30        "startTimeUtc": "2022-08-11T23:35:59.000Z",
31        "endTimeUtc": "2022-08-11T23:36:41.000Z",
32        "state": 1,
33        "failedSourceRows": 0,
34        "successSourceRows": 1,
35        "failedTargetRows": 0,
36        "successTargetRows": 767,
37        "startedBy": "mboardmanipsnawest",
38        "runContextType": "REST_API_V2",
39        "entries": []
40      }
41    ]
42  }
43 ]
```

Extract Logs from Informatica Cloud



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



Swagger Files

The screenshot shows the Informatica Administrator web interface. On the left is a dark sidebar with a menu of options: Organization, Licenses, SAML Setup, Metering, Settings, Users, User Groups, User Roles, Runtime Environ..., Serverless Environ..., Connections, Add-On Connectors, Schedules, Add-On Bundles, Swagger Files, Logs, and Elastic Clusters. The 'Swagger Files' option is highlighted. The main content area has a header 'swagger_Login' and a sub-header 'Create a swagger file.'. Below this is a section titled 'Swagger File Details' containing the following information:

Name:	swagger_Login
Description:	
Runtime Environment:	sag_MattB
URL:	https://dm-us.informaticacloud.com
Verb:	POST
Authentication Type:	None
API Base Path:	/saas
API Path:	/public/core/v3/login
Username:	MattBoardman
Password:	*****
Token:	
Token Secret:	
Consumer Key:	
Consumer Secret:	
Accept:	application/json
Headers:	
Query Params:	
Operation Id:	Login
Content Type:	application/json
Raw Body:	{ "username": "mboardmanIPSNWest", "password": "" }

REST v2 Connections

The screenshot displays the Informatica Administrator web interface. On the left is a dark sidebar with navigation icons and labels: Organization, Licenses, SAML Setup, Metering, Settings, Users, User Groups, User Roles, Runtime Environm..., Serverless Environ..., Connections, Add-On Connectors, Schedules, Add-On Bundles, Swagger Files, Logs, Elastic Clusters, and File Servers. The main content area is titled 'conn_RESTv2_LoginV3'. It contains three sections: 'Connection Details', 'REST V2 Connection Properties', and 'Standard Connection Properties'. The 'Connection Details' section lists: Connection Name (conn_RESTv2_LoginV3), Description, Type (REST V2 (Informatica Cloud)), Created On (Jul 31, 2022 2:37:58 PM), Updated On (Jul 31, 2022 2:37:58 PM), Created By (mboardmanipsnawest), and Updated By (mboardmanipsnawest). The 'REST V2 Connection Properties' section lists: Runtime Environment (sag_MattB) and Authentication (Standard). The 'Standard Connection Properties' section lists: Authentication Type (NONE), Auth User ID, Auth Password, OAuth Consumer Key, OAuth Consumer Secret, OAuth Token, OAuth Token Secret, Swagger File Path (C:\Temp\swagger\login.json), TrustStore File Path, TrustStore Password, KeyStore File Path, KeyStore Password (masked with asterisks), Proxy Type (Platform Proxy), Proxy Configuration (<host>:<port>), and Advanced Fields.

Informatica Administrator

Organization

Licenses

SAML Setup

Metering

Settings

Users

User Groups

User Roles

Runtime Environm...

Serverless Environ...

Connections

Add-On Connectors

Schedules

Add-On Bundles

Swagger Files

Logs

Elastic Clusters

File Servers

conn_RESTv2_LoginV3

Connection Details

Connection Name: conn_RESTv2_LoginV3

Description:

Type: REST V2 (Informatica Cloud)

Created On: Jul 31, 2022 2:37:58 PM

Updated On: Jul 31, 2022 2:37:58 PM

Created By: mboardmanipsnawest

Updated By: mboardmanipsnawest

REST V2 Connection Properties ?

Runtime Environment: sag_MattB

Authentication: Standard

Standard Connection Properties ?

Authentication Type: NONE

Auth User ID:

Auth Password:

OAuth Consumer Key:

OAuth Consumer Secret:

OAuth Token:

OAuth Token Secret:

Swagger File Path: C:\Temp\swagger\login.json

TrustStore File Path:

TrustStore Password:

KeyStore File Path:

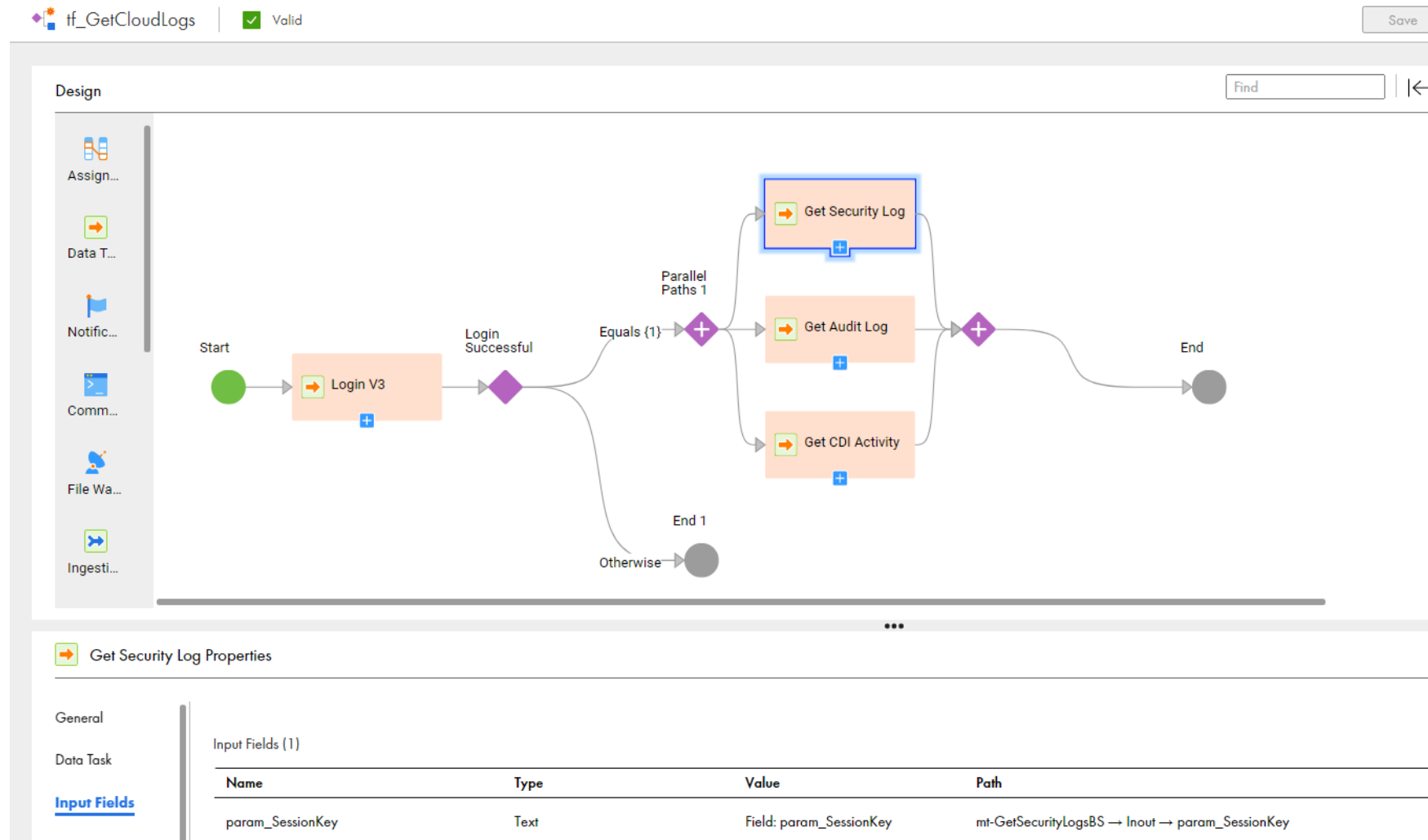
KeyStore Password: *****

Proxy Type: Platform Proxy

Proxy Configuration: <host>:<port>

Advanced Fields:

Taskflow



Mapping: Login to get Session Key

m_LoginV3 | Valid

Save Run

Design

Source Target Aggregator

src_RESTv2

expr_SetSessionKey

tgt_Dummy

Parameters

Input Parameters

param_LoginJSON string

In-Out Parameters

param_SessionKey string

Validation

Mapping is valid

Properties Preview src_RESTv2

General

Source

Field Mapping

Fields

Partitions

Select elements of Response to be mapped to Output Fields. Output groups and keys will be automatically generated.

Response Structure (1 of 20 mapped)

Show Fields: All Find

Element Name	Cardinality
root	1-1
Response_200	0-1
productsArray	0-1
userInfo	0-1
sessionId	0-1
id	0-1

Output Fields

Find

Field Name	Actions	Mapped Field
root		/root
sessionId		/Response_200/userInfo/sessionId

Mapping: Extract Security Log

m_SecurityLogBS Valid Save Run

Design

Source Target

src_Dummy exp_DateRange WS_SecurityLog tgt_SQL

Parameters

Input Parameters

No Input Parameters.

In-Out Parameters

param_SessionKey string

Properties Preview WS_SecurityLog

General

Incoming Fields

Web Service

Request Mapping

Response Mapping

Output Fields

Advanced

Map Incoming Fields to elements of Request Structure to form web service request.

Incoming Fields

Show: Show All Find

Field Key

exp_DateRange

q

new_SessionKey

sessionId

Request Structure

Show: Show All Find

root*

q (exp_DateRange.q)

INFA-SESSION-ID (exp_DateRange.new_SessionKey)

Validation

Mapping is valid

Mapping: Extract Asset (Audit) Log

m_AuditLogBSValid

SaveRun

Design

SourceTargetAggregatorCleanse

src_Dummyexp_BatchRangeWebServicesexp_GetMinDatetgt

PropertiesPreviewWebServices

GeneralIncoming FieldsWeb ServiceRequest MappingResponse MappingOutput FieldsAdvanced

Map Incoming Fields to elements of Request Structure to form web service request.

Incoming Fields

FieldKey

exp_BatchRange

new_SessionKey

batchId

batchSize

sessionId

Request Structure

root

batchId (exp_BatchRange.batchId)

batchSize (exp_BatchRange.batchSize)

icSessionId (exp_BatchRange.sessionId)

Parameters

Input Parameters

No Input Parameters.

In-Out Parameters

param_SessionKeystring

Validation

Mapping is valid



Mapping: Extract Data Integration Jobs Log

m_ActivityLogBSValid

SaveRun

Design

SourceTargetAggregatorCleanseData Masking

src_Dummy

ws_GetActivityLog

Igt_SQL_Activity

Igt_SQL_Entries

Igt_SQL_Transforms

Parameters

Input Parameters

No Input Parameters.

In-Out Parameters

param_SessionKeystring

Validation

Mapping is valid

PropertiesPreviewws_GetActivityLog

General

Incoming Fields

Web Service

Request Mapping

Response Mapping

Output Fields

Advanced

Map Incoming Fields to elements of Request Structure to form web service request.

Incoming Fields

FieldKey

src_Dummy

sessionId

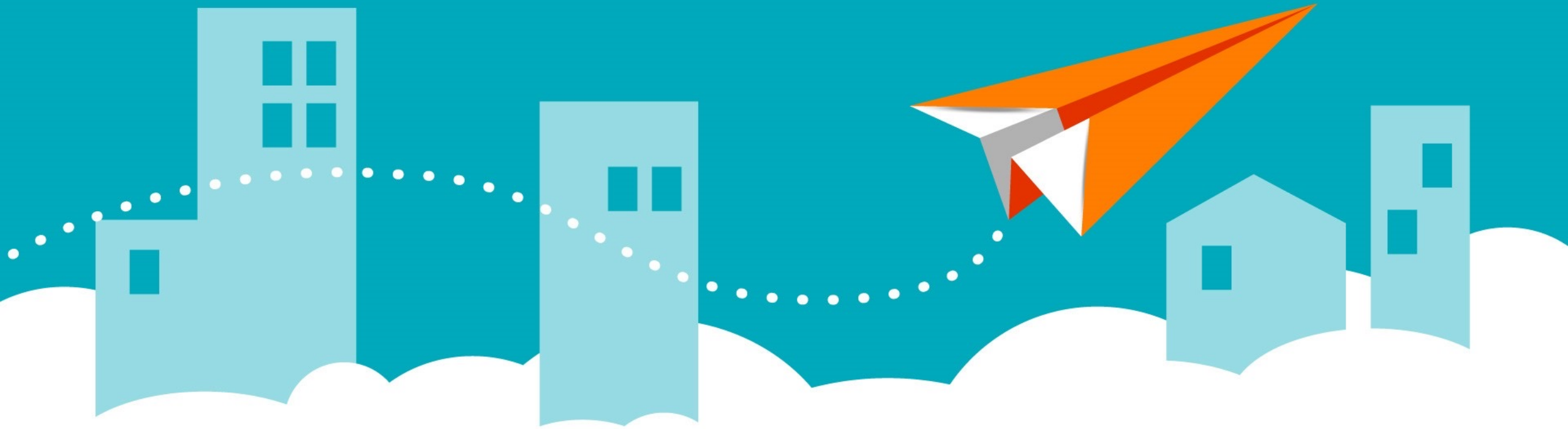
Request Structure

root*

icSessionId (src_Dummy.sessionId)

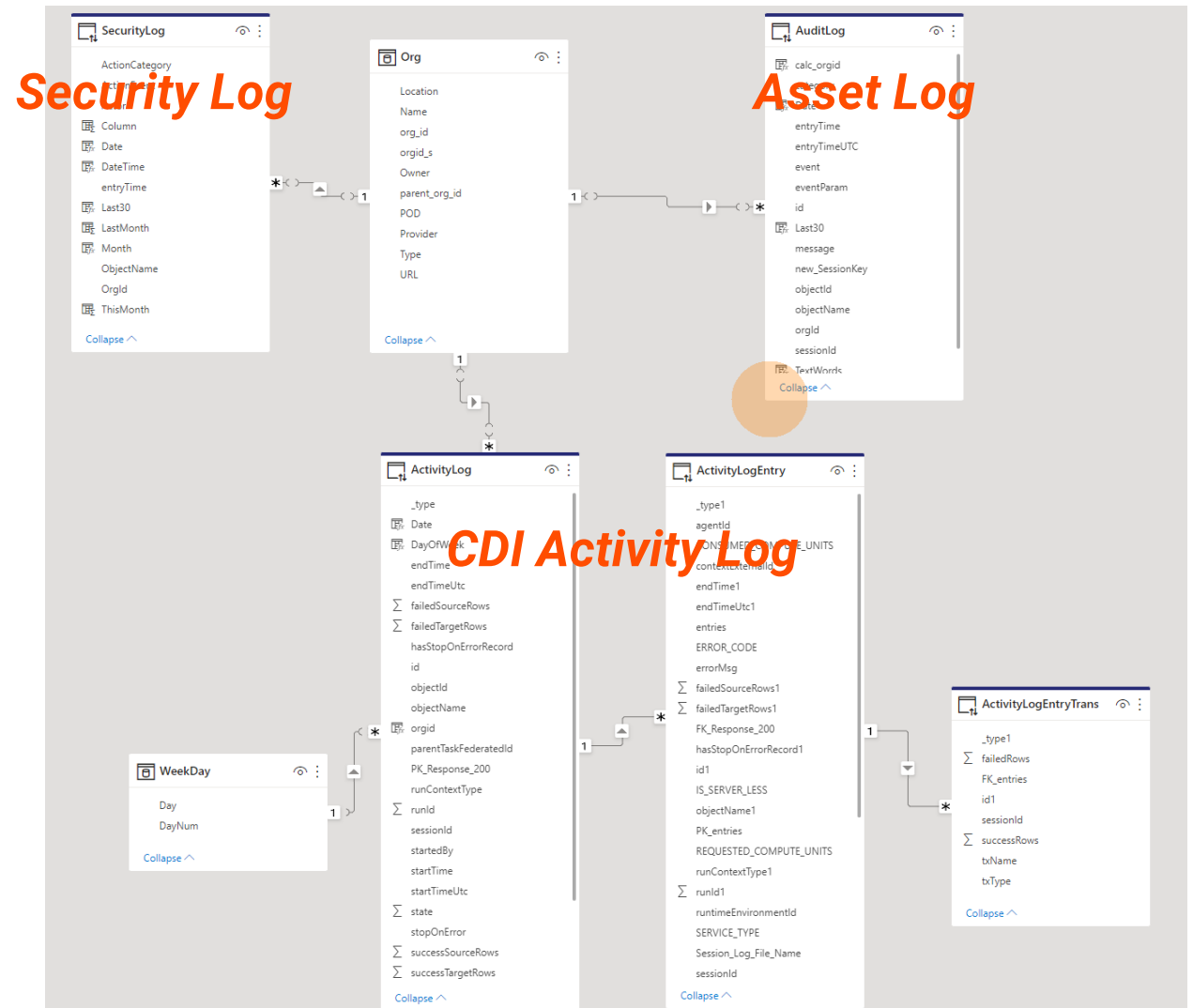


Example Dashboard using Microsoft Power BI

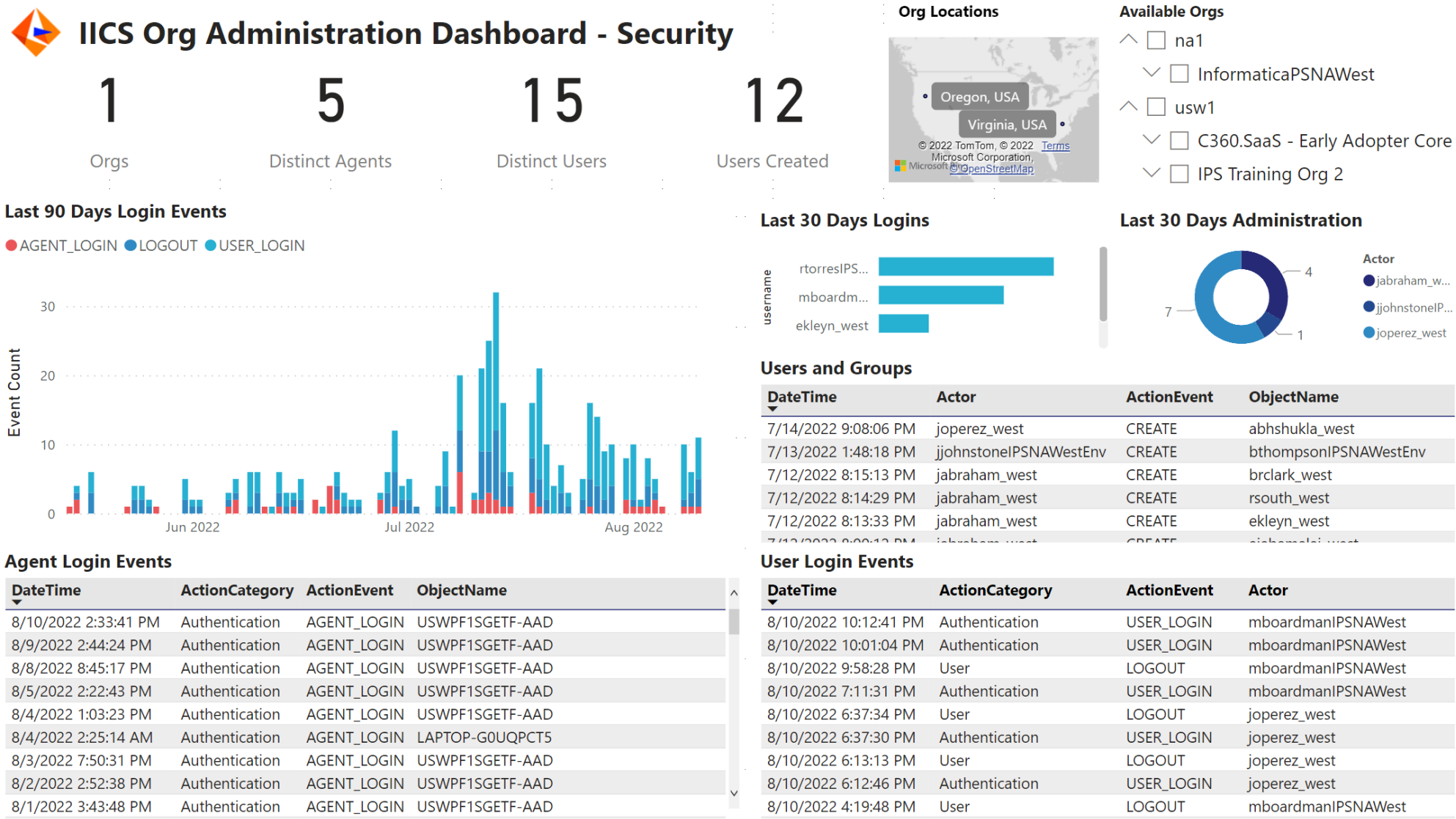


Example Data Model

- 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



Example Dashboard – From Security Logs



Last 90 Days Login Events

AGENT_LOGIN

LOGOUT

USER_LOGIN

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	jjohnstoneIPSNWestEnv	CREATE	bthompsonIPSNWestEnv
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
7/12/2022 8:00:13 PM	jabraham_west	CREATE	sishamalai_west

User Login Events

DateTime	ActionCategory	ActionEvent	Actor
8/10/2022 10:12:41 PM	Authentication	USER_LOGIN	mboardmanIPSNWest
8/10/2022 10:01:04 PM	Authentication	USER_LOGIN	mboardmanIPSNWest
8/10/2022 9:58:28 PM	User	LOGOUT	mboardmanIPSNWest
8/10/2022 7:11:31 PM	Authentication	USER_LOGIN	mboardmanIPSNWest
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	mboardmanIPSNWest

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

1

6

22

78

Distinct Objects

• Oregon, USA

Virginia, USA •

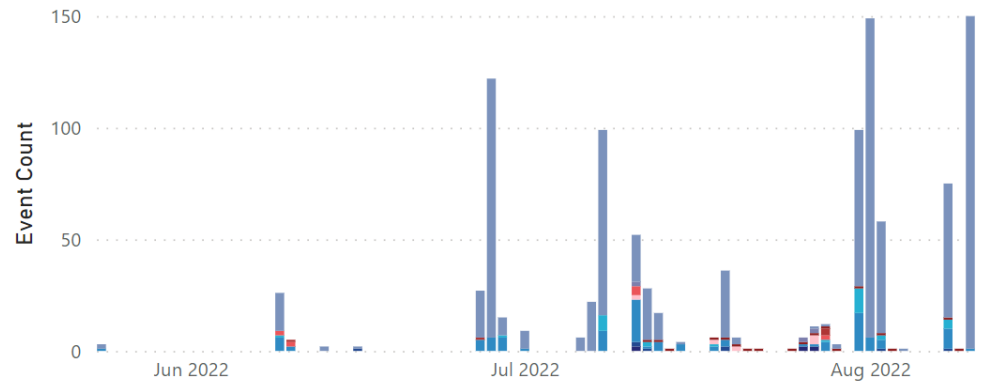
© 2022 TomTom, © 2022 Microsoft Corporation,
[OpenStreetMap](#) [Terms](#)

 $\wedge \square \text{ na1}$

^ □ usw1

IPS Training Org 2

● ADD_TAG ● COPY ● CREATE ● DELETE ● EXPORT ● IMPORT ● MOVE ● Publish ● REMOVE_TAG



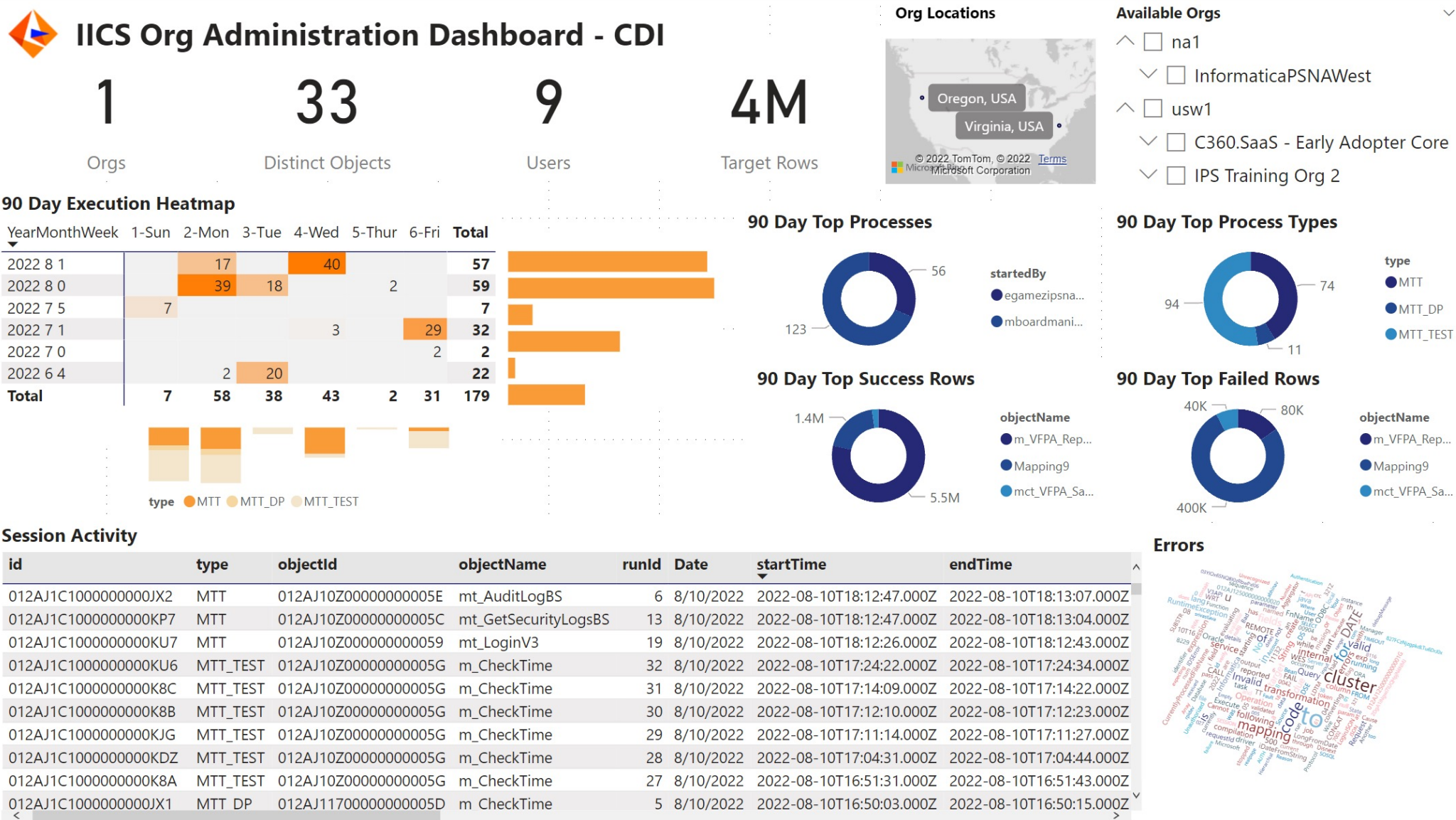
username	count
mboardman	10
rtorresIPSN	2
ajabamalai_...	1

[illegible]

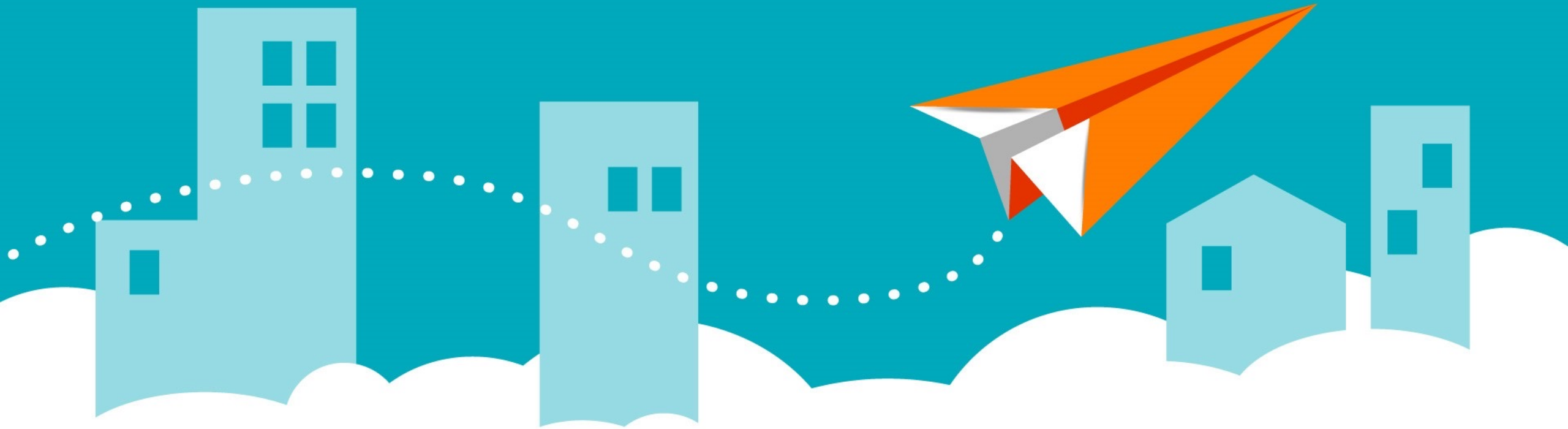
entryTime	username	category	event	eventParam	message	objectId	objectName
2022-06-29T14:49:20.000Z	egamezlPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	UPDATE	UPDATE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.UPDATE	8IMwY2oaVFclsaA1uGH7Cx	Oz_AjayDirects_CDIE
2022-07-08T14:46:24.000Z	egamezlPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	UPDATE	UPDATE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.UPDATE	8IMwY2oaVFclsaA1uGH7Cx	Oz_AjayDirects_CDIE
2022-07-08T14:52:50.000Z	egamezlPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	UPDATE	UPDATE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.UPDATE	8IMwY2oaVFclsaA1uGH7Cx	Oz_AjayDirects_CDIE
2022-07-08T14:54:42.000Z	egamezlPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	DELETE	DELETE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.DELETE	8IMwY2oaVFclsaA1uGH7Cx	Oz_AjayDirects_CDIE
2022-07-08T14:57:51.000Z	egamezlPSNAWestEnv	SAAS_RUNTIME_ENVIRONMENT	UPDATE	UPDATE SAAS_RUNTIME_ENVIRONMENT Successful.	aevent.SAAS_RUNTIME_ENVIRONMENT.UPDATE	0hMlmdplunOIFJ5r15e6Uz	Oz_AjayDirects-CDIE



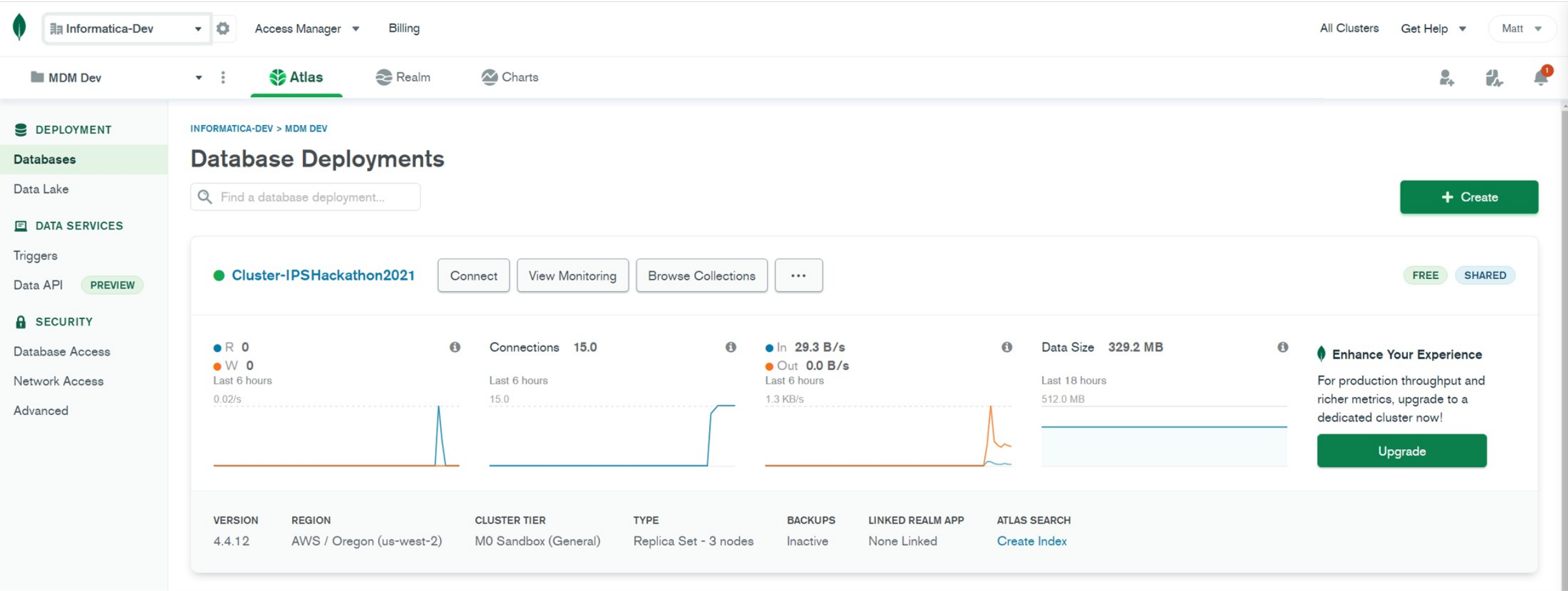
Example Dashboard – From CDI Job Logs



Using a Document Store Database (MongoDB)



Example: Hosted MongoDB (Atlas)



IICS agent connection for MongoDB

cnct_MongoDB_Infa_Hackathon

✓ The test for this connection was successful.

Connection Details

Connection Name:	cnct_MongoDB_Infa_Hackathon
Description:	
Type:	MongoDB
Created On:	Feb 7, 2022 1:55:07 PM
Updated On:	Feb 8, 2022 9:15:26 AM
Created By:	mboardmanipsnawest
Updated By:	mboardmanipsnawest

MongoDB Properties ?

Runtime Environment:	localhost.localdomain
----------------------	-----------------------

Connection Section

Host Name:	cluster-ipshackathon202-shard-00-01.kusa5.mongodb.net:27017
Port:	27017
User Name:	Infa_Hackathon2022
Password:	*****
Database Name:	infa_hackathon_logfiles
SSL Mode:	require
SSL TrustStore Path:	
SSL TrustStore Password:	
Additional Connection Properties:	retryWrites=true&w=majority

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

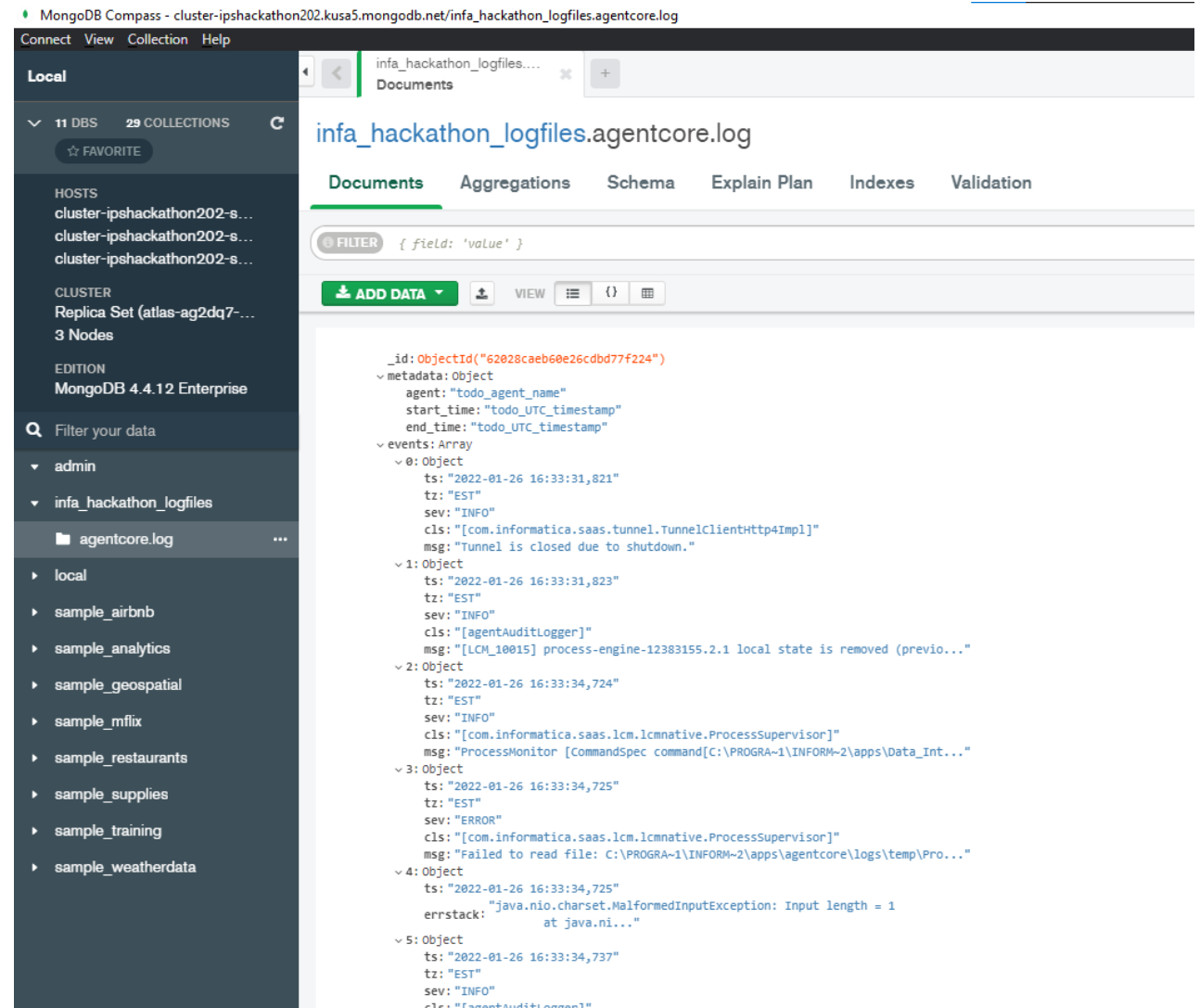
Viewing Secure Agent Log Data

- MongoDB Compass

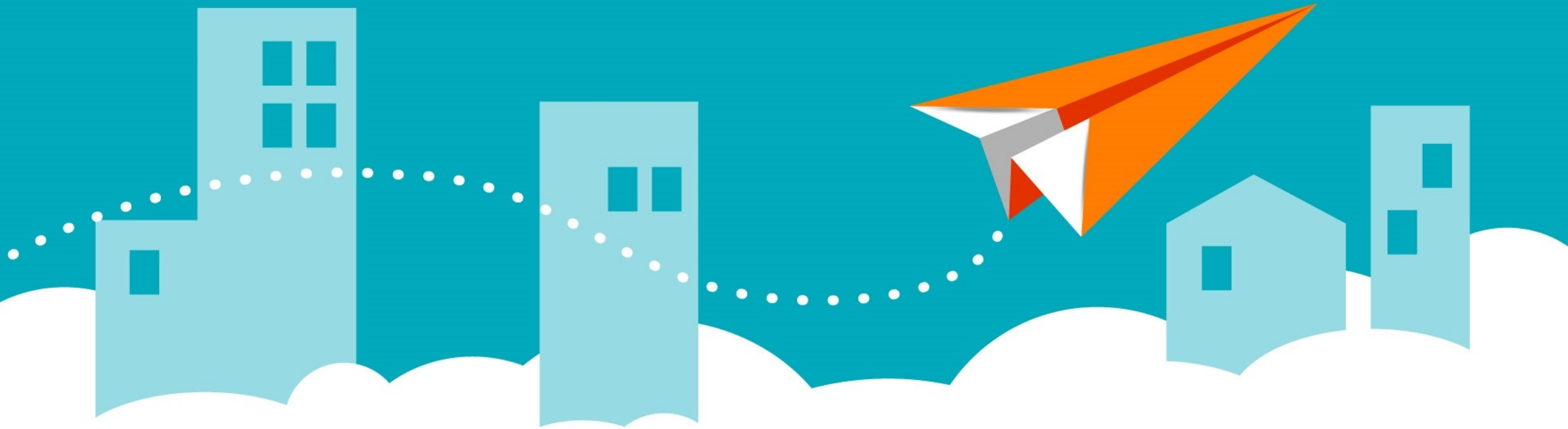
- View logs in canonical format
- View complete error messages (may span multiple lines in log)

- MongoDB BI Connector

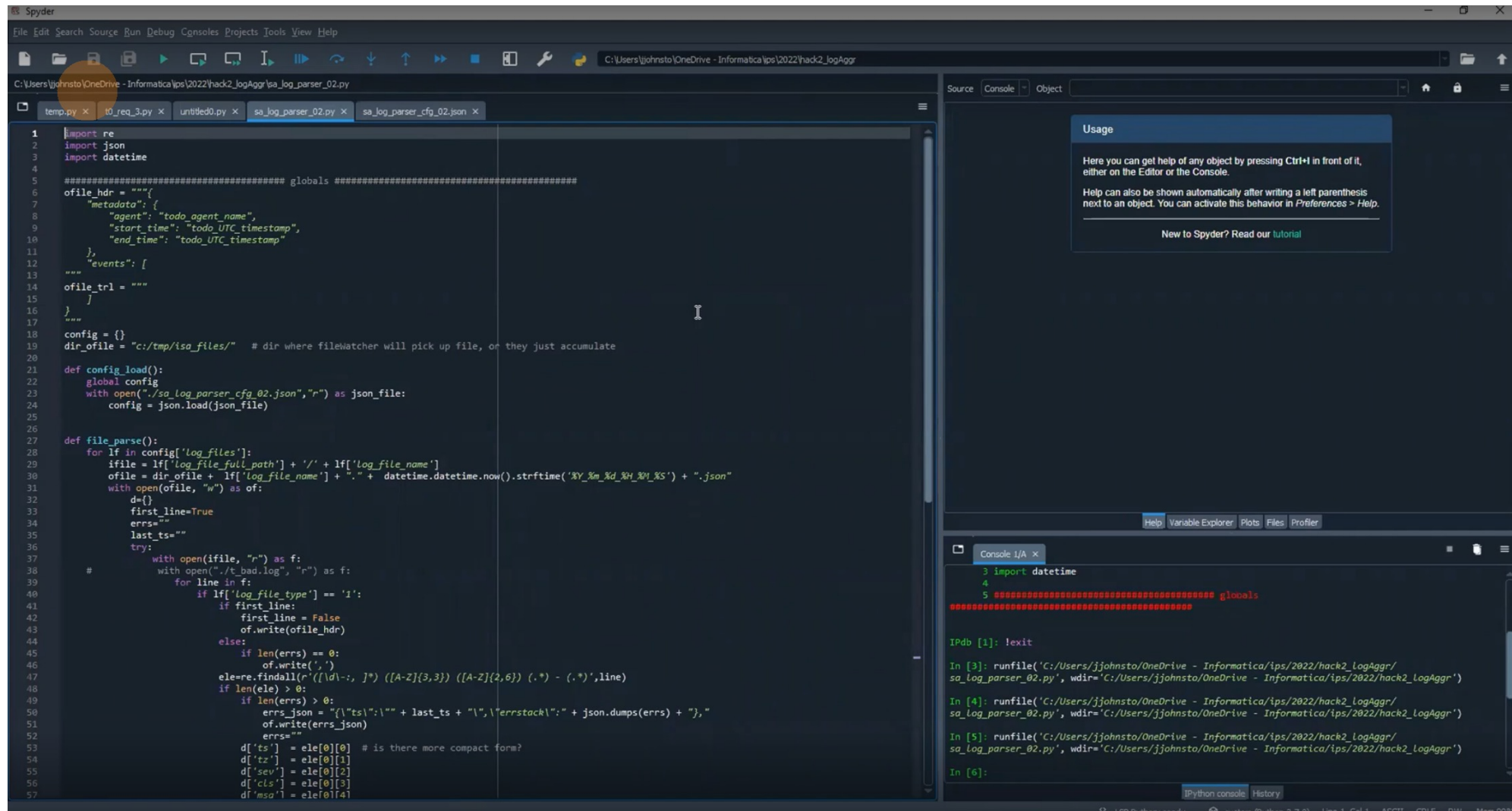
- Plugin to allow SQL queries



Demo: Extract Logs from Secure Agents



Python translation from Log4J to JSON format



```
1 import re
2 import json
3 import datetime
4
5 ##### globals #####
6 ofile_hdr = """
7     {
8         "metadata": {
9             "agent": "todo_agent_name",
10            "start_time": "todo_utc_timestamp",
11            "end_time": "todo_utc_timestamp"
12        },
13        "events": [
14        ]
15    }
16 """
17
18 config = {}
19 dir_ofile = "c:/tmp/isa_files/" # dir where filewatcher will pick up file, or they just accumulate
20
21 def config_load():
22     global config
23     with open("./sa_log_parser_cfg_02.json", "r") as json_file:
24         config = json.load(json_file)
25
26
27 def file_parse():
28     for lf in config['log_files']:
29         ifile = lf['log_file_full_path'] + '/' + lf['log_file_name']
30         ofile = dir_ofile + lf['log_file_name'] + "." + datetime.datetime.now().strftime('%Y_%m_%d_%H_%M_%S') + ".json"
31         with open(ofile, "w") as of:
32             d = {}
33             first_line = True
34             errs = ""
35             last_ts = ""
36             try:
37                 with open(ifile, "r") as f:
38                     with open("./t_bad.log", "r") as f:
39                         for line in f:
40                             if lf['log_file_type'] == 'I':
41                                 if first_line:
42                                     first_line = False
43                                     of.write(ofile_hdr)
44                                 else:
45                                     if len(errs) == 0:
46                                         of.write(',')
47                                     ele = re.findall(r'([\d-: , ]*) ([A-Z]{3,3}) ([A-Z]{2,2}) ([*]) ([*])', line)
48                                     if len(ele) > 0:
49                                         if len(errs) > 0:
50                                             errs_json = "(\\"ts\":" + last_ts + "\",\\"errstack\":" + json.dumps(errs) + \",\"
51                                             of.write(errs_json)
52                                             errs = ""
53                                         d['ts'] = ele[0][0] # is there more compact form?
54                                         d['tx'] = ele[0][1]
55                                         d['sev'] = ele[0][2]
56                                         d['cls'] = ele[0][3]
57                                         d['msg'] = ele[0][4]
```

Usage

Here you can get help of any object by pressing **Ctrl+I** in front of it, either on the Editor or the Console.

Help can also be shown automatically after writing a left parenthesis next to an object. You can activate this behavior in **Preferences > Help**.

[New to Spyder? Read our tutorial](#)

Console 1/A x

```
3 import datetime
4
5 ##### globals #####

IPdb [1]: !exit

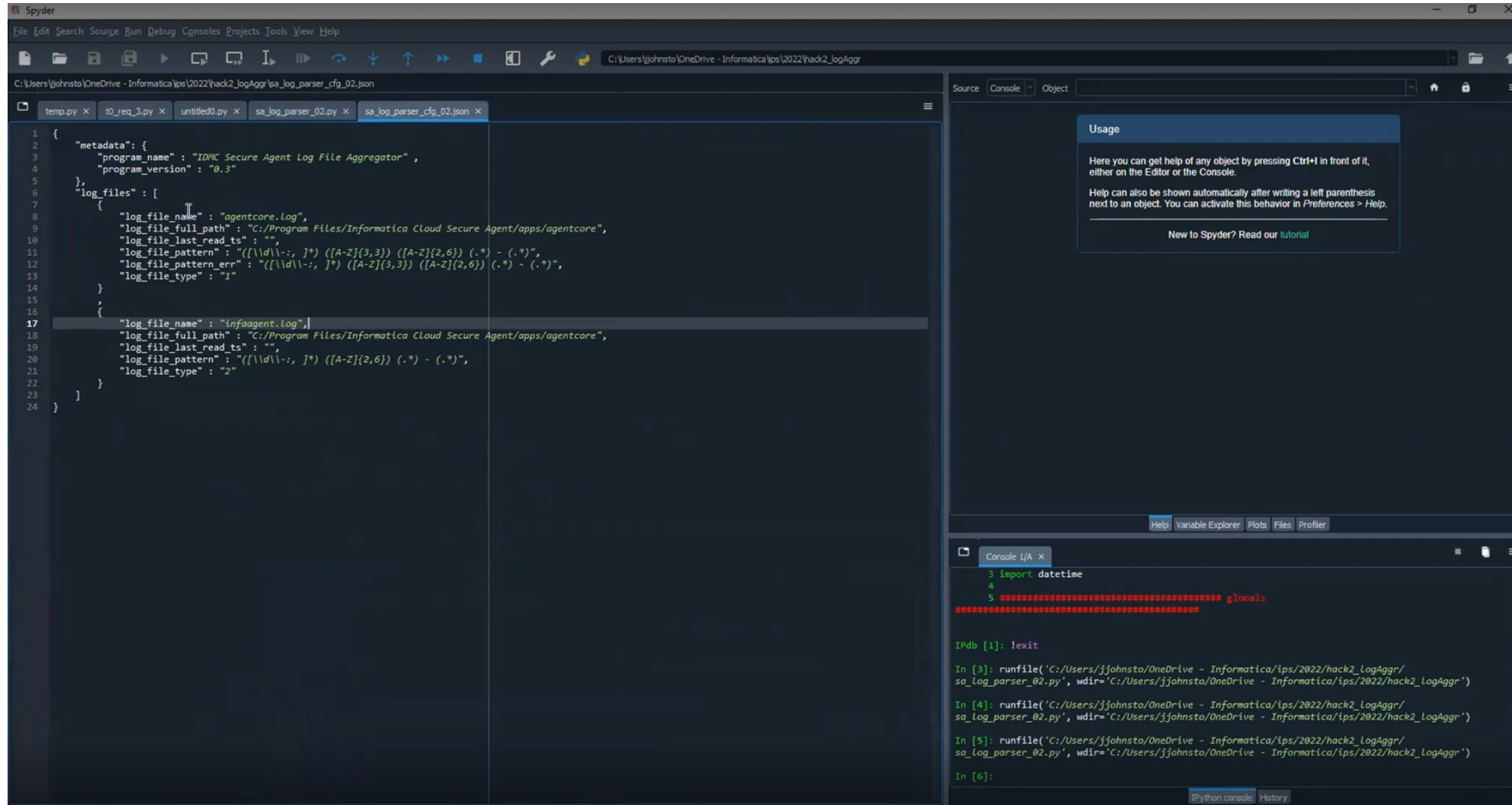
In [3]: runfile('C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr/sa_log_parser_02.py', wdir='C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr')

In [4]: runfile('C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr/sa_log_parser_02.py', wdir='C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr')

In [5]: runfile('C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr/sa_log_parser_02.py', wdir='C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr')

In [6]:
```

Python translation from Log4J to JSON format



The screenshot displays the Spyder Python IDE interface. The main editor window shows a JSON file named `sa_log_parser_cfg_02.json` with the following content:

```
1 {
2   "metadata": {
3     "program_name": "IOMC Secure Agent Log File Aggregator",
4     "program_version": "0.3"
5   },
6   "log_files": [
7     {
8       "log_file_name": "agentcore.Log",
9       "log_file_full_path": "C:/Program Files/Informatica Cloud Secure Agent/apps/agentcore",
10      "log_file_last_read_ts": "",
11      "log_file_pattern": "([\\d\\-:; ]*) ([A-Z]{3,3}) ([A-Z]{2,6}) (.*) - (.*)",
12      "log_file_pattern_err": "([\\d\\-:; ]*) ([A-Z]{3,3}) ([A-Z]{2,6}) (.*) - (.*)",
13      "log_file_type": "1"
14    },
15    {
16      "log_file_name": "infoagent.Log",
17      "log_file_full_path": "C:/Program Files/Informatica Cloud Secure Agent/apps/agentcore",
18      "log_file_last_read_ts": "",
19      "log_file_pattern": "([\\d\\-:; ]*) ([A-Z]{2,6}) (.*) - (.*)",
20      "log_file_type": "2"
21    }
22  ]
23 }
24 }
```

The right sidebar contains a 'Usage' panel with help text and a 'Console' panel showing the following IPython session:

```
3 import datetime
4
5 ##### globals #####
#####

IPdb [1]: !exit

In [3]: runfile('C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr/
sa_log_parser_02.py', wdir='C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr')

In [4]: runfile('C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr/
sa_log_parser_02.py', wdir='C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr')

In [5]: runfile('C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr/
sa_log_parser_02.py', wdir='C:/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr')

In [6]:
```


Python translation from Log4J to JSON format

```
{
  "metadata": {
    "program": "infaagent.log.2022_04_12_16_00_06.json"
  },
  "log_files": [
    {
      "ts": "2022-02-16 18:26:48,885",
      "cls": "Log4j2-AsyncAppenderEventDispatcher-1-asyncAppender",
      "sev": "ERROR",
      "msg": "Failed to log audit message due to: HTTP POST request failed due to IO error:..nal.dm-us.informaticacloud.com; nested exception is org.springframework.web.client.ResourceAccessException: I/O error on POST request for \\\"http://audit-service/saas/api/agent/v1/agent-log-entry\\\":..nal.dm-us.informaticacloud.com; nested exception is java.net.UnknownHostException: nal.dm-us.informaticacloud.com"
    },
    {
      "ts": "2022-02-16 18:26:48,903",
      "cls": "Log4j2-AsyncAppenderEventDispatcher-1-asyncAppender",
      "sev": "ERROR",
      "msg": "Failed to log audit message due to: HTTP POST request failed due to IO error:..nal.dm-us.informaticacloud.com; nested exception is org.springframework.web.client.ResourceAccessException: I/O error on POST request for \\\"http://audit-service/saas/api/agent/v1/agent-log-entry\\\":..nal.dm-us.informaticacloud.com; nested exception is java.net.UnknownHostException: nal.dm-us.informaticacloud.com"
    },
    {
      "ts": "2022-02-16 18:26:48,904",
      "cls": "Log4j2-AsyncAppenderEventDispatcher-1-asyncAppender",
      "sev": "ERROR",
      "msg": "Failed to log audit message due to: HTTP POST request failed due to IO error:..nal.dm-us.informaticacloud.com; nested exception is org.springframework.web.client.ResourceAccessException: I/O error on POST request for \\\"http://audit-service/saas/api/agent/v1/agent-log-entry\\\":..nal.dm-us.informaticacloud.com; nested exception is java.net.UnknownHostException: nal.dm-us.informaticacloud.com"
    },
    {
      "ts": "2022-02-16 18:26:48,906",
      "cls": "Log4j2-AsyncAppenderEventDispatcher-1-asyncAppender",
      "sev": "ERROR",
      "msg": "Failed to log audit message due to: HTTP POST request failed due to IO error:..nal.dm-us.informaticacloud.com; nested exception is org.springframework.web.client.ResourceAccessException: I/O error on POST request for \\\"http://audit-service/saas/api/agent/v1/agent-log-entry\\\":..nal.dm-us.informaticacloud.com; nested exception is java.net.UnknownHostException: nal.dm-us.informaticacloud.com"
    }
  ]
}
```

Python translation from Log4J to JSON format

The screenshot displays a development environment with three main components:

- Python Script (temp.py):** A script that defines a JSON structure for log files, including metadata, program details, and a list of log files.
- Terminal Window:** Shows the execution of a script that translates Log4J logs to JSON format. The output shows the successful insertion of log data into a MongoDB database.
- MongoDB Compass:** A graphical interface for MongoDB. It shows a collection named 'infa_hackathon_logfiles.agentcore.log' with 10 documents. The interface includes a search bar, a 'FIND' button, and a table of documents.

The terminal window shows the following commands and output:

```
johnsto@USW1PF1GDXTM /cygdrive/c/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr
$ ./t_post_mongo2.sh c:/tmp/isa_files/agentcore.log.test.json
{"insertedId": "6255d8cc0d7569258b6904cc"}
johnsto@USW1PF1GDXTM /cygdrive/c/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr
$ ./t_post_mongo2.sh c:/tmp/isa_files/agentcore.log.test.json
{"insertedId": "6255da7e1ca46385daec6ff"}
johnsto@USW1PF1GDXTM /cygdrive/c/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr
$ cat t_post_mongo2.sh
# _l does not work

curl --request POST \
  'https://data.mongodb-api.com/app/data-guzvy/endpoint/data/beta/action/insertone' \
  --header 'Content-Type: application/json' \
  --header 'Access-Control-Request-Headers: *' \
  --header 'api-key: S5qpsPVTZ0L1x9QtdirwEjDhH8jePQmcknfG89ZopnxDP9lkyGAbatz0sIb8juz' \
  --data-binary @sample_logs.json
johnsto@USW1PF1GDXTM /cygdrive/c/Users/jjohnsto/OneDrive - Informatica/ips/2022/hack2_logAggr
$
```

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

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/>