

AMIS



AMIS



ORACLE MANAGEMENT CLOUD: OPERATIONAL MANAGEMENT IN A DEVOPS WORLD

Lucas Jellema (CTO AMIS & Oracle ACE Director)
26 January 2017, Nieuwegein

WHAT IS **IT** ALL ABOUT?



WHAT'S HAPPENING

- Intricate application and infrastructure architecture
 - Multi-tier, mobile, SOA, virtualization, microservices
- Hybrid landscape
 - Mix of technologies and vendors
 - Cloud, multiple clouds, on premises
- Agility and the constancy of change
 - DevOps (you build it, you run it, you fix it)
- Big Time – Big Data and Real Time
 - IoT, IoP, Social Media, 24/7

OPERATIONAL MANAGEMENT OBJECTIVES

- Keep business value of IT available as required | promised
- Need to know if and when (preferably predict before) something goes wrong
 - At end user | business | functional level
- Analyse (looming) problem – in order to fix it
 - What, where, when, why, who, why?
 - Across IT landscape
- Areas of operational interest
 - Functionality
 - Security
 - QA & Compliance
 - Infrastructure efficiency



Smarter insight.



Swifter action.

OPERATIONAL MANAGEMENT CLOUD

- Gather metrics and logs across IT landscape to central store
- Expose, visualize and explore
- Report
- Analyze
- Predict (machine learning) & Recommend



AGENDA

THE WORLD OF DEVOPS AND
THE NECESSITY FOR
MONITORING & ANALYTICS

FIRST STEPS WITH OMC – HOW
[TO GET | WE GOT] STARTED



OVERVIEW OF ORACLE
MANAGEMENT CLOUD AND ITS
CONSTITUENTS

DRINKS & DINNER

HANDSON OMC - APPLICATION
PERFORMANCE MONITORING &
LOG ANALYTICS

LIVE DEMONSTRATION OF THE
FUNCTIONALITY OF OMC



HANDSON OMC –
INFRASTRUCTURE
MONITORING & IT ANALYTICS

AGENDA

THE WORLD OF DEVOPS
AND THE NECESSITY FOR
MONITORING & ANALYTICS

FIRST STEPS WITH OMC – HOW
[TO GET | WE GOT] STARTED



OVERVIEW OF ORACLE
MANAGEMENT CLOUD AND ITS
CONSTITUENTS

DRINKS & DINNER

HANDSON OMC - APPLICATION
PERFORMANCE MONITORING &
LOG ANALYTICS

LIVE DEMONSTRATION OF THE
FUNCTIONALITY OF OMC



HANDSON OMC –
INFRASTRUCTURE
MONITORING & IT ANALYTICS

AGENDA

THE WORLD OF DEVOPS AND
THE NECESSITY FOR
MONITORING & ANALYTICS

FIRST STEPS WITH OMC – HOW
[TO GET | WE GOT] STARTED



OVERVIEW OF ORACLE
MANAGEMENT CLOUD
AND ITS CONSTITUENTS

DRINKS & DINNER

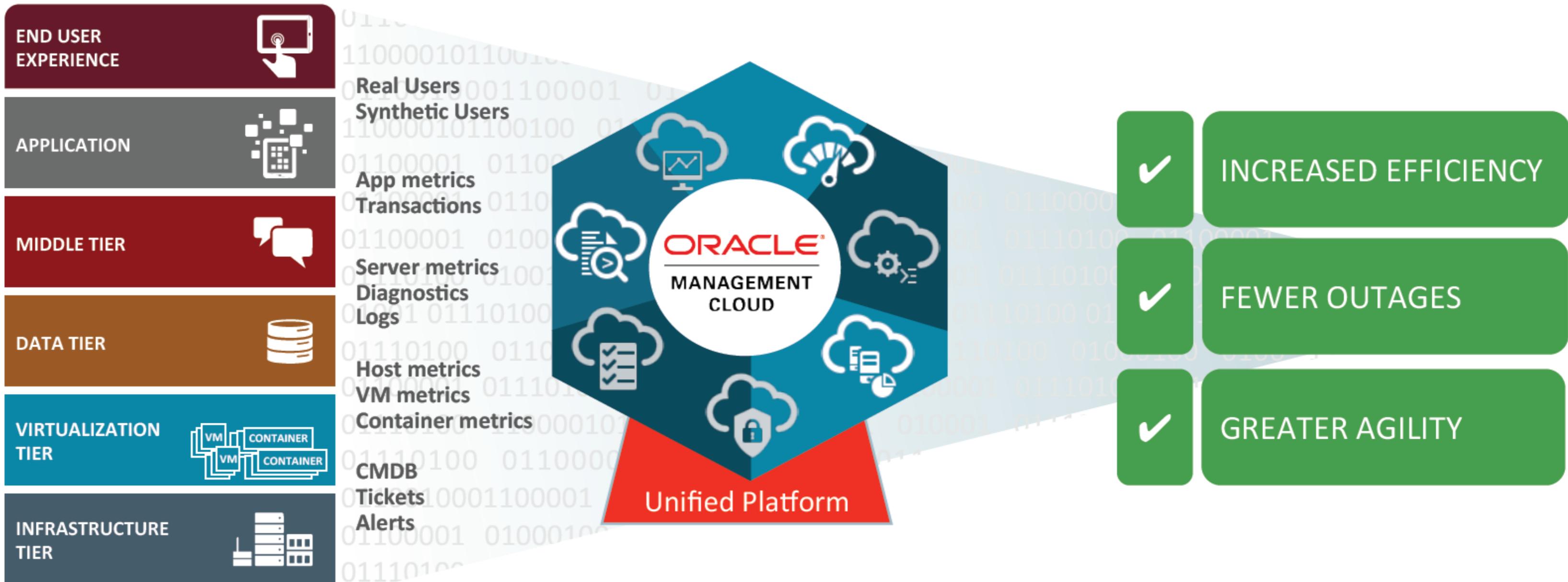
HANDSON OMC - APPLICATION
PERFORMANCE MONITORING &
LOG ANALYTICS

LIVE DEMONSTRATION OF THE
FUNCTIONALITY OF OMC

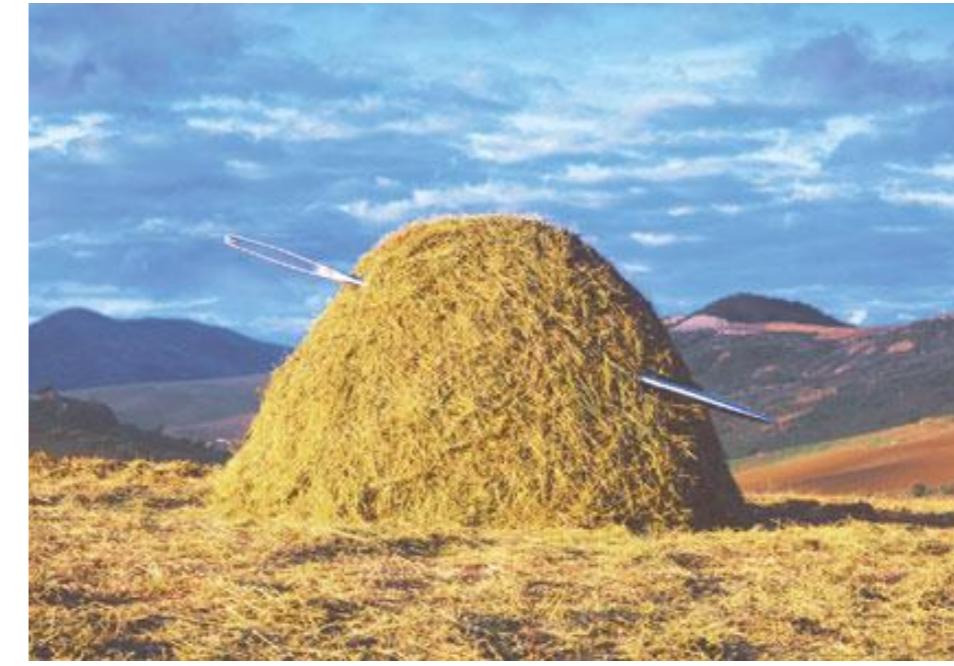
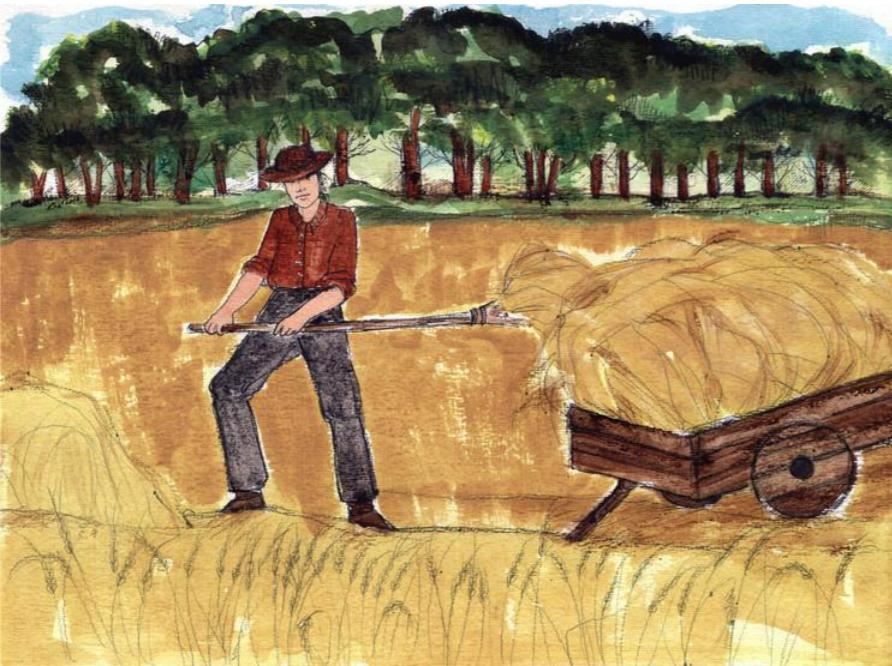


HANDSON OMC –
INFRASTRUCTURE
MONITORING & IT ANALYTICS

ORACLE MANAGEMENT CLOUD: FROM METRICS AND LOGS TO BUSINESS OBJECTIVES



OMC: GATHER THE HAY AND FIND THE NEEDLE(S)



ORACLE MANAGEMENT CLOUD E PLURIBUS UNUM

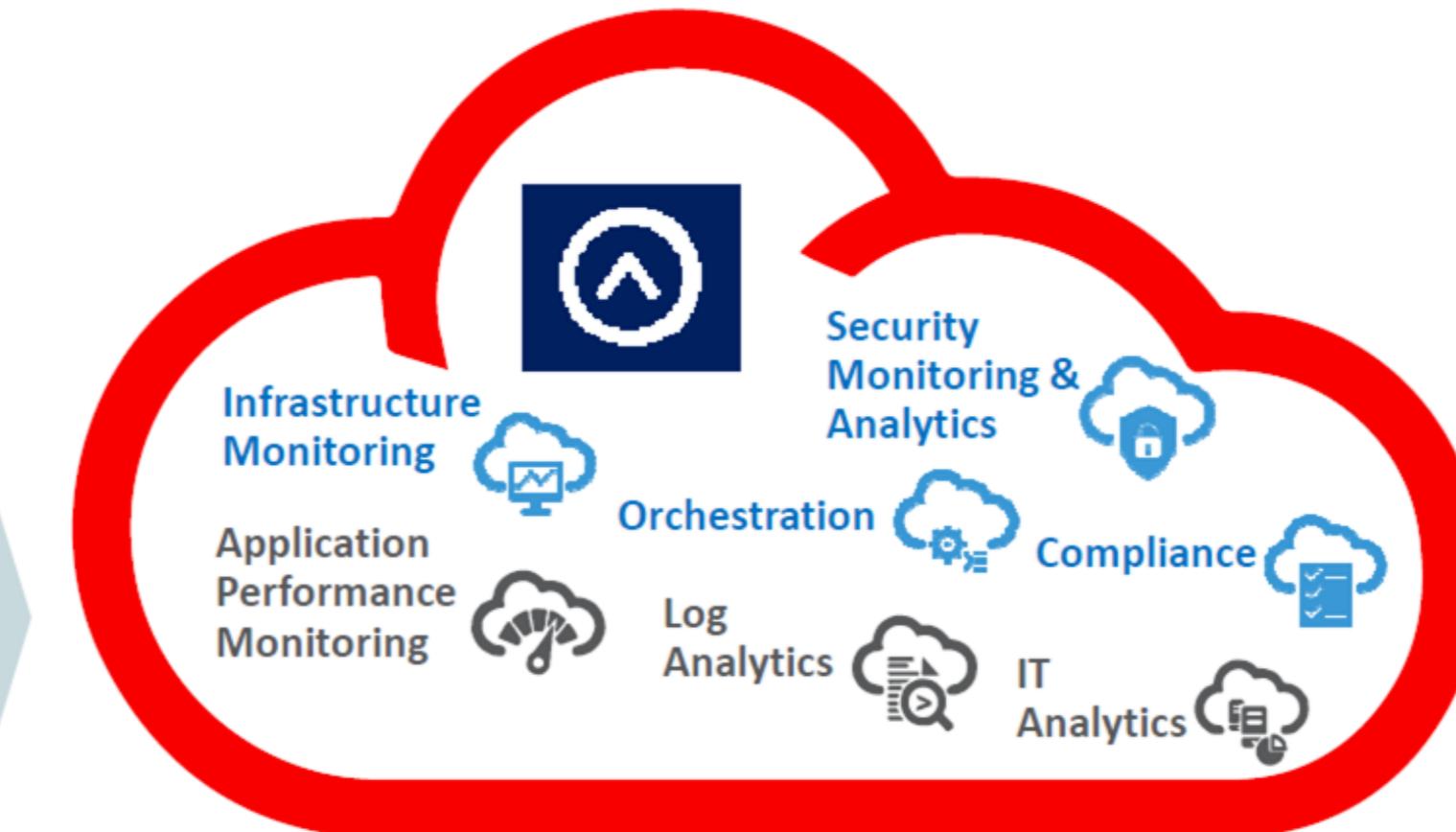
ORACLE®
MANAGEMENT
CLOUD

ORACLE®
CLOUD

Microsoft Azure



On Premise



AMIS

E PLURIBUS UNUM

☰ ORACLE Management Cloud Service Admin ▾

Management Cloud Service Dashboard Security Monitoring and Analytics Compliance Orchestration Workflows Application Performance Monitoring Infrastructure Monitoring Log Analytics IT Analytics

Status All Targets

Target with Status

- Up (1210)
- Down (0)
- Under Blackout (13)

1223

Incidents

UPDATES Breakdown of incidents updated (last 7 days)

Category	24 hours	7 Days
Availability	140	65
Performance	6	4
Security	1	6
Others	120	153

Security Events

Global Status by Application

ORider	Billing	Support	Finance
--------	---------	---------	---------

Last 24 Hours Snapshot

7 Incidents	5 Auto-Remediated	5 High Risk Users	3 High Risk Assets
-------------	-------------------	-------------------	--------------------

Orchestrations

6 Running Executions 120 Completed Executions 5 Scheduled Executions

Compliance

91.38% ▲0.78% Average Compliance Score

Application Performance SLAs

Application	Views/day	Response SLAs	% change in SLAs
ORider	89M	100%	0%
Billing	4M	95%	10%
Support	83K	85%	11%
Finance	3K	100%	0%

Log Events

Application	Events/day	Critical Errors/day	% change in Errors
ORider	943M	0	0%
Billing	43M	0	0%
Support	5M	0	0%
Finance	1M	0	0%

Global Status by Application

ORider	Billing	Support	Finance
--------	---------	---------	---------

Last 24 Hours Snapshot

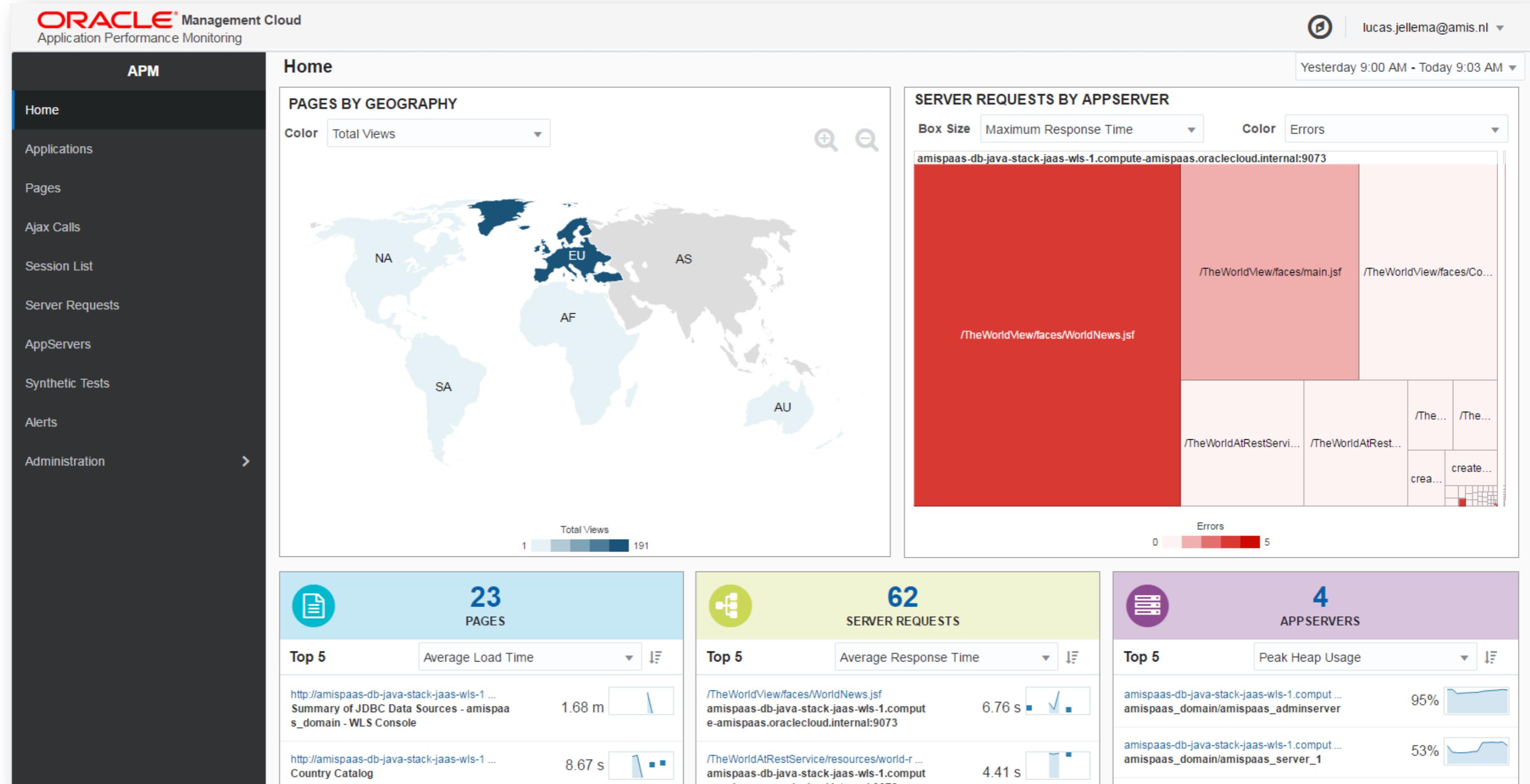
1 Critical Violation	17 Auto-Remediated	3 Failed Rules Set	3 Failed Assets
----------------------	--------------------	--------------------	-----------------

APPLICATION PERFORMANCE MONITORING

- (near real time) Monitor end user activity and experience
- Compare actually experienced response times against thresholds
- Detect sessions with errors
- Send alerts
- Check health with synthetic tests
- Analyze problematic situations
 - Under which conditions do they occur?
 - What happens under the covers of the error?
 - Where in the multitier end to end chain is the bottleneck



APPLICATION PERFORMANCE MONITORING



APM - SESSIONS

ORACLE® Management Cloud
Application Performance Monitoring

APM

Session List

Browser Detail : contains Chrome

Sort: Session Health

Yesterday 9:00 AM - Today 9:03 AM

Date	User	Location	Browser Detail	Device	Duration	Page Views	Ajax Errors	JavaScript Errors	Session Health
Jan 24, 2017 7:40:12 PM	n/a, United Kingdom	Chrome Mobile 55.0		20s	4	0	9	0.75	
		Location	Browser Detail	Device					
		86.132.21.112	768x1024						
		Client IP	Screen Size						
Jan 24, 2017 9:46:11 PM	Zaventem, Belgium	Chrome 55.0		1h 47m 20s	3	0	0	0.80	
		Location	Browser Detail	Device					
		141.143.213.50	1600x900						
		Client IP	Screen Size						
Jan 24, 2017 9:08:42 PM	Nesoddtangen, Norway	Chrome 55.0		3m 11s	12	0	4	0.87	
		Location	Browser Detail	Device					
		84.213.35.251	1280x800						
		Client IP	Screen Size						
Jan 24, 2017 7:27:49 PM	Zaventem, Belgium	Chrome 55.0		34m 42s	24	0	8	0.89	
		Location	Browser Detail	Device					
		141.143.213.50	1600x900						
		Client IP	Screen Size						
Jan 24, 2017 6:42:41 PM	Zaventem, Belgium	Chrome 55.0		3m 4s	19	0	0	0.91	
		Location	Browser Detail	Device					
		141.143.213.38	1280x800						
		Client IP	Screen Size						
Jan 24, 2017 9:39:19 PM	Utrecht, Netherlands	Chrome 55.0		4h 27m 13s	68	0	0	0.94	
		Location	Browser Detail	Device					
		82.217.74.126	1536x864						
		Client IP	Screen Size						
Jan 24, 2017 5:59:59 PM	Zoetermeer	Chrome 55.0							

APM – SESSION DETAILS

ORACLE® Management Cloud
Application Performance Monitoring

Session ▲ Jan 24, 2017 7:40:12 PM Duration 20s

Summary

Device	Location	Page Views	Ajax Calls / Errors	JavaScript Errors
Tablet, iOS n/a n/a 86	n/a, United Kingdom BT Provider 86.132.21.112 Client IP	4	0 / 0	9

Timeline

7:40:13 PM 7:40:15 PM 7:40:17 PM 7:40:19 PM 7:40:21 PM 7:40:23 PM 7:40:25 PM 7:40:27 PM 7:40:29 PM 7:40:31 PM 7:40:33 PM

Jan 24, 2017

● Page Loads ● Page Clicks ● JavaScript Errors

Session Details

Time	User	Page	Page Name	Ajax Calls / Errors	JavaScript Errors	Page Clicks	Viewing Time	APdex
Jan 24, 2017 7:40:12 PM	Zoetermeer	Page	http://amispaaS-db-java-stack-jaas-wls-1.compute-amispaaS.oraclecloud.internal:9073/TheWorldView/superindex.html	0 / 0	0	0	0s	1.00
Jan 24, 2017 7:40:12 PM	Zoetermeer	Page	http://amispaaS-db-java-stack-jaas-wls-1.compute-amispaaS.oraclecloud.internal:9073/TheWorldView/superindex.html	0 / 0	3	0	10s	1.00
Jan 24, 2017 7:40:19 PM	Zoetermeer	JavaScript Error	:0	Script error.	Error Message			
Jan 24, 2017 7:40:21 PM	Zoetermeer	JavaScript Error	:0	Script error.	Error Message			

Jan 24, 2017 5:59:59 PM

Zoetermeer Chrome 55.0

Good Views

APdex

ALERTING BASED ON APM MONITORING

ORACLE Management Cloud

Update Alert Rule

* Name page takes too long to load on average

Add description

Conditions

Metric Average Page Response Time (Over last hour)	Unit ms	Operator >	Critical Threshold 4000	Warning Threshold 2000
---	------------	---------------	-------------------------------	------------------------------

+ Add Condition

E-mail Notification

E-mail notifications will be sent when the alert is first raised, worsens in severity and is closed. Multiple e-mail addresses should be separated by commas.

Addresses *

lucas.jellema@amis.nl, frank.houweling@amis.nl

lucas.jellema@amis.nl

Save Cancel

Critical Alert: APM Page <http://amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal:9073/TheWorldView/faces/main.jsf> has an average response time (over last hour) of 4.448 seconds; it is greater than expected value of 4.0 seconds.

To: no-reply@oracle.com

If there are problems with how this message is displayed, click here to view it in a web browser.

Sent: wo 25-1-2017 6:34

To: Lucas Jellema

ORACLE Management Cloud

Hello,

Oracle Management Cloud has reported an alert. Here are the details:

Alert Message APM Page <http://amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal:9073/TheWorldView/faces/main.jsf> has an average response time (over last hour) of 4.448 seconds; it is greater than expected value of 4.0 seconds.

Severity Critical

Raised On Wed, January 25, 2017 05:30:00 AM UTC

Alert Rule page takes too long to load on average

More Information [Review details](#)

Thank You,

LOG ANALYTICS



- So much could be known from the collected log sources
 - Business-wise
 - Application
 - IT platform and infrastructure



MULTI TIER, MULTI NODE LOG ENTRIES



Application

2015-05-10T12:59:52.212: INFO: OrderApp-3212: Order type: Failed, cust: 933373, order: 3997396, region: APAC

Order Number



<May 10, 2015 12:59:50 Error Message <Server> <BEA-002608> <The Listen Thread closed because of an error>
java.sql.SQLException: Closed Connection
at oracle.jdbc.driver.SQLStateMapping.newSQLException(SQLStateMapping.java:70)
at processOrders.acme.com(SubmitOrder.java:112)



Database

Time Stamp

Mon Aug 17 09:37:31 PDT 2016 Errors in file /ora_db_home/app/oracle/admin/ORCL/bdump/orcl1_dw04_1297.trc:
ORA-00600: internal error code, arguments: [kghstack_underflow_internal_3], [0x2AFA326CAFC0], [rpi role space],
[], [], [], [] ORA-19502: write error on file "/ora_common/orcl(exports/daily/orcl_full_20160718_05.exp", blockno
560899 (blocksize=4096) ORA-27072: File I/O error Linux-x86_64 Error: 28: No space left on device



May 10, 2015 22:04:29 myhost.acme.com: router dnsprobe[276]: dns query failed

May 10, 2015 22:04:30 myhost.acme.com: router dnsprobe[276]: Primary DNS server Is Down... Switching To
Secondary DNS server

Host Name

May 10, 2015 22:04:30 myhost.acme.com: router dnsprobe[276]: Switching Back To Primary DNS server

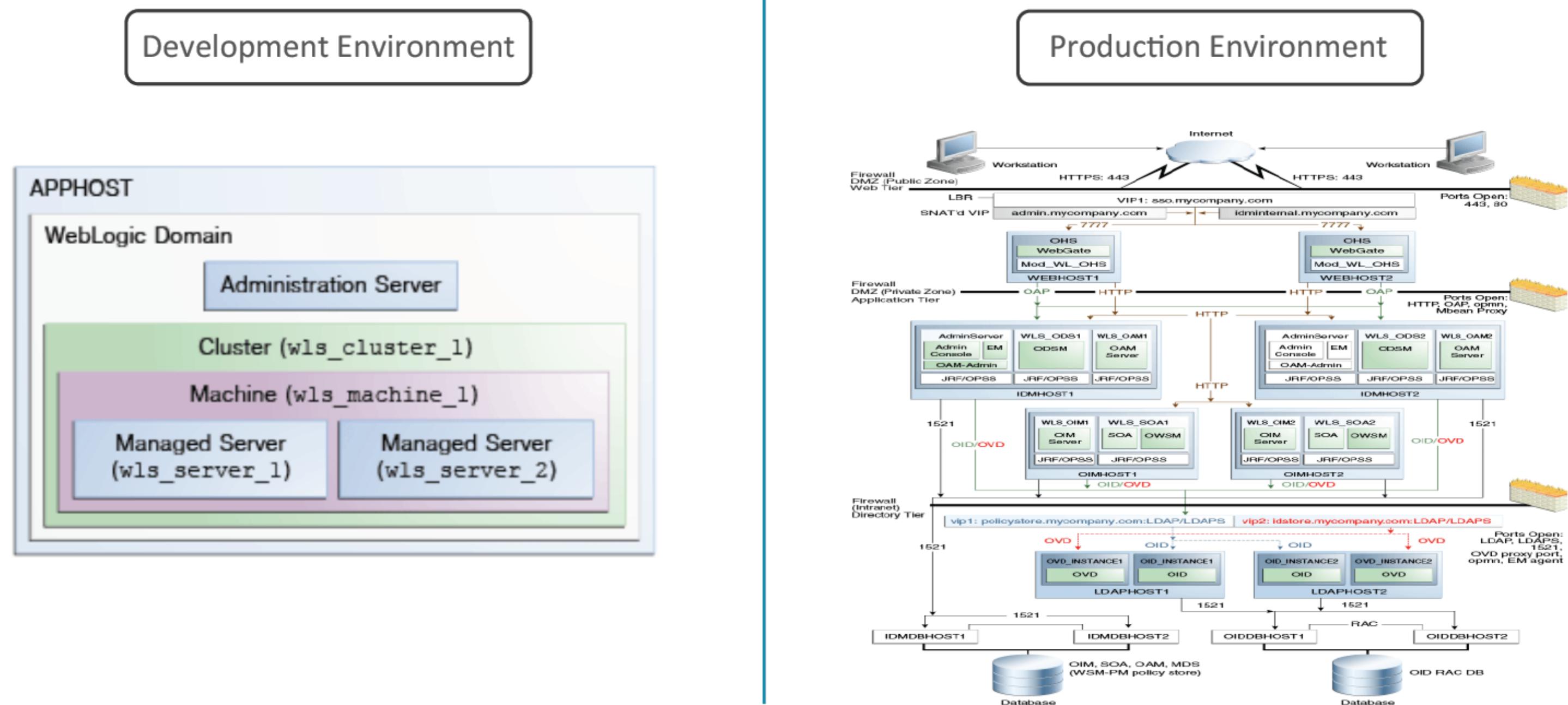
AMIS

TROUBLE SHOOTING AND TACTICAL ANALYSIS ON LOG DATA ARE HARD...

- Which log files to use
- How to access the contents of the log files
- How to understand (parse) and compare log files
- Which entries in which log files are related
 - In time, in location, in user session, in transaction, ...
- How to focus on the relevant entries
- How to handle huge volumes of logs
- How to find outliers and trends
- How to keep up with changes

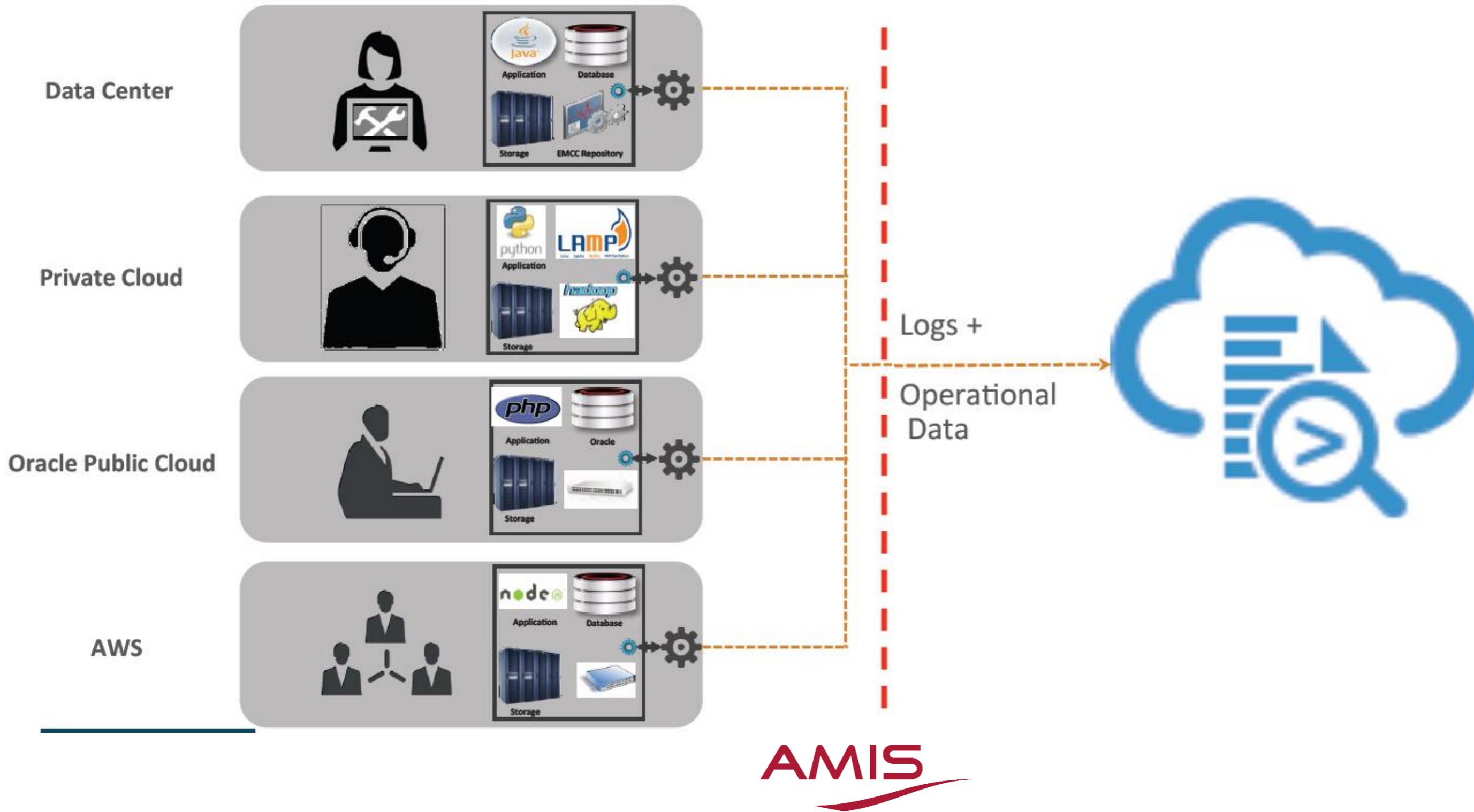


BUT*IT*WORKED*JUST*FINE *IN*DEVELOPMENT...*



AMIS

GATHERING LOG ENTRIES



LOG ANALYTICS

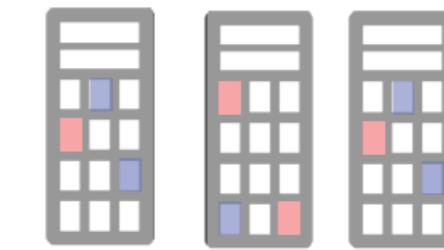
- Collect and process log entries from 120+ logging sources
 - Across platforms, technologies, locations and vendors
 - Customize and add log sources & parsers
- Parse, Analyze, Store, Manage a big stash of entries
- Expose, search, correlate, aggregate, visualize log entries
 - Across all logging sources
 - Find the threads, the correlated events, apply machine learning
 - Drill down from functional logging and business events to technical logging, stack traces and infrastructure issues
- Publish Alerts from real time findings in log files
- Drill down from APM to Log Analytics
 - To find log entries that belong to slow or faulted sessions



Applications



Databases



Virtual Machines



Servers

EXPLORE LOGS

ORACLE Management Cloud
Log Analytics

Log Explorer: Untitled

+ New Save Open Configuration

Last 30 Days Run

Data Visualize Field Summary

Records with Histogram

Display Options

Show Message Field Records per Page 25

Display Fields

Entity Entity Type Log Source Host Name (Server) Severity

Collection Details

Label Log Entity Log Source Upload Name

Fields

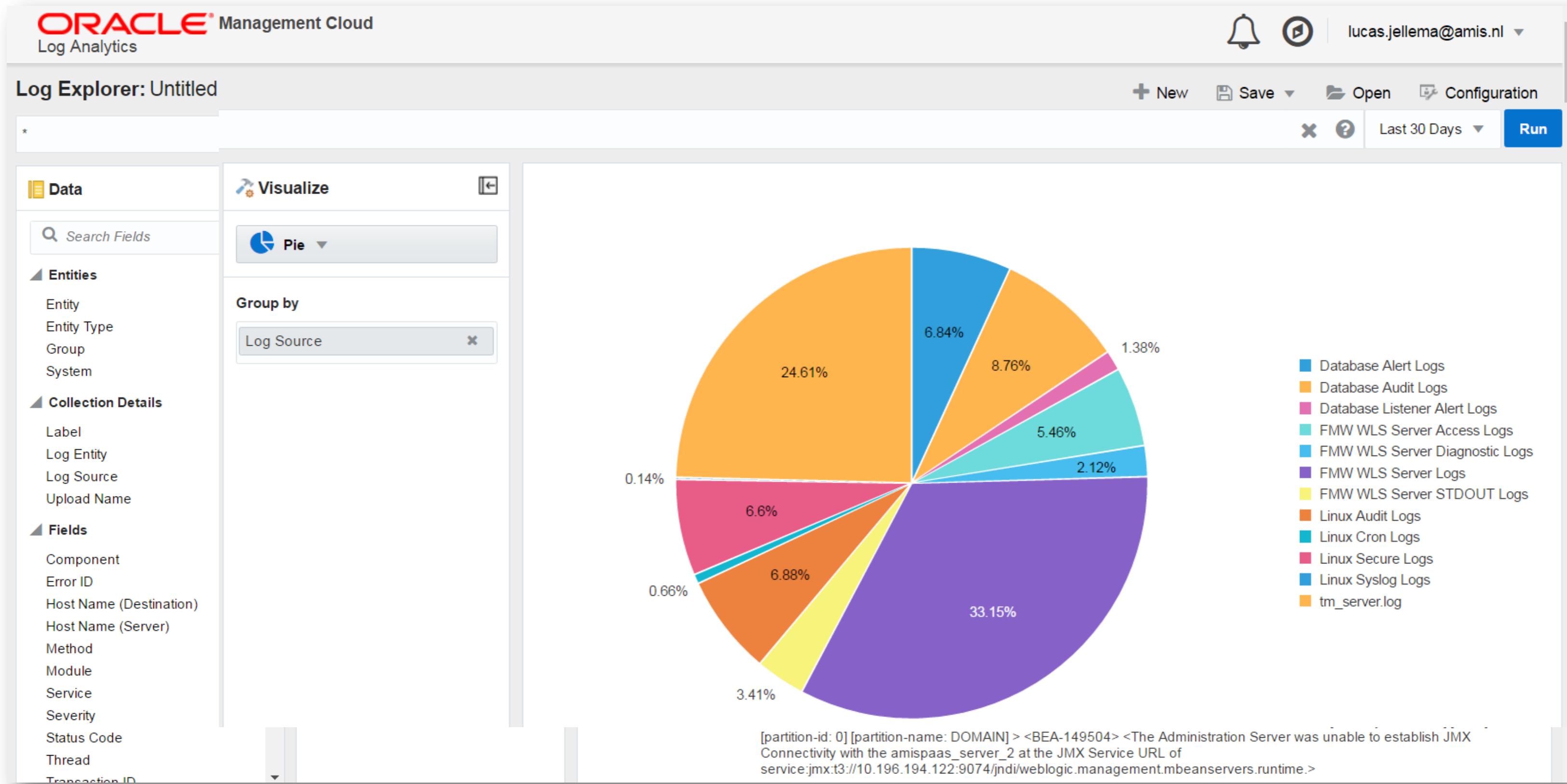
Component Error ID Host Name (Destination) Host Name (Server) Method Module Service Severity Status Code Thread Transaction ID

Histogram

Showing 1-25 of 1083297

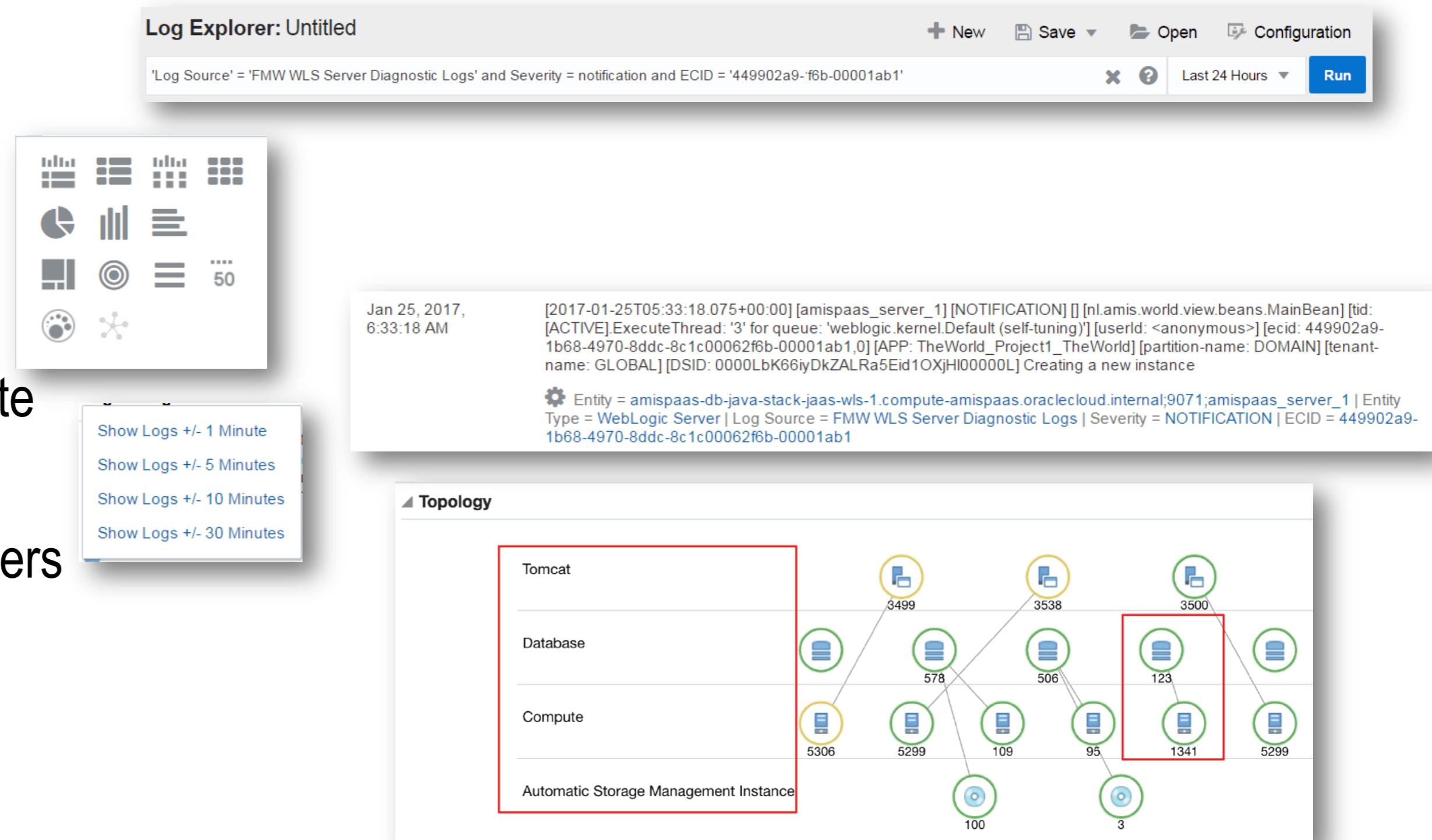
Time (UTC+1:00)	Original Log Content
Jan 25, 2017, 6:45:02 AM	####<Jan 25, 2017, 5:45:02,937 AM UTC> <Warning> <JMX> <amispaas-db-java-stack-jaas-wls-1> <amispaas_adminserver> <[ACTIVE] ExecuteThread: '34' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <86e148cd-565e-4f00-ab81-813632d0853a-00000ad8> <1485323102937> <[severity-value: 16] [rid: 0] [partition-id: 0] [partition-name: DOMAIN]> <BEA-149535> <JMX Resiliency Activity Server=amispaas_server_2 : Starting JMX connection. forceReconnect value: false>
Jan 25, 2017, 6:45:01 AM	####<Jan 25, 2017, 5:45:01,937 AM UTC> <Warning> <JMX> <amispaas-db-java-stack-jaas-wls-1> <amispaas_adminserver> <[ACTIVE] ExecuteThread: '34' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <86e148cd-565e-4f00-ab81-813632d0853a-00000ad8> <1485323101937> <[severity-value: 16] [rid: 0] [partition-id: 0] [partition-name: DOMAIN]> <BEA-149504> <The Administration Server was unable to establish JMX Connectivity with the amispaas_server_2 at the JMX Service URL of service:jmx:t3://10.196.194.122:9074/jndi/weblogic.management.mbeanservers.runtime.>

EXPLORE LOGS



EXPLORING LOG FILES

- Filter
- Aggregate
- Visualize
- Drilldown / Correlate
- Show Topology
- Save and reuse filters



SMART CLUSTERING

ORACLE Management Cloud
Log Analytics

Log Explorer: Untitled

Module = jdbc | cluster

+ New Save Open Configuration Last 24 Hours Run

Data Visualize Cluster

Search Fields

Entities

- Entity
- Entity Type
- Group
- System

Collection Details

- Label
- Log Entity
- Log Source
- Upload Name

Fields

- Error ID
- Module | Clear
- Severity
- Thread
- Transaction ID
- User Name
- Weblogic Server
- more...

Records per Page 25

9 AM 24 Jan 2017 12 PM 3 PM 6 PM 9 PM 12 AM 25 3 AM 6 AM

180
150
120
90
60
30
0

Show Similar Trends Show Records

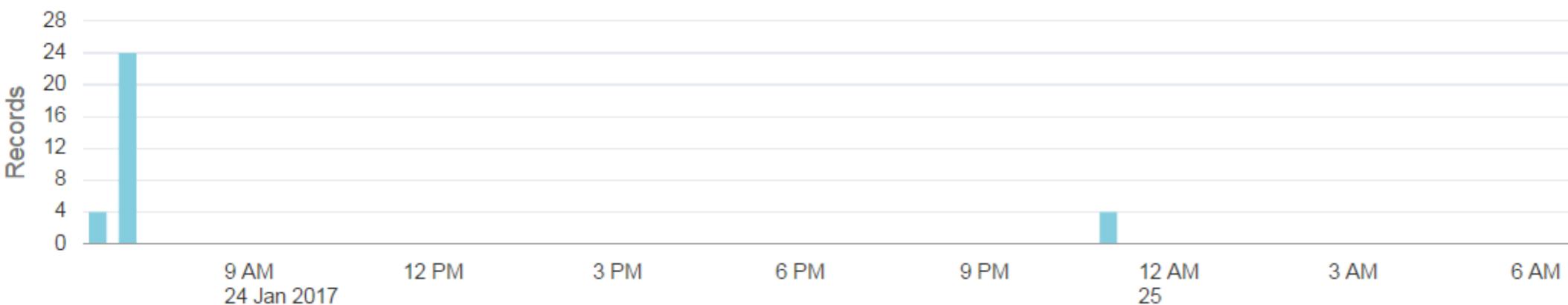
17 clusters

ID	Log Source
17	FMW WLS Server Logs
16	FMW WLS Server Logs
15	FMW WLS Server Logs
14	FMW WLS Server Logs
13	FMW WLS Server

Trend Count Sample Message

- 349 BEA-001128> <Connection for pool "mds-owsm" has been closed.
- 60 BEA-001513> <Destroying application-scoped data source java:comp/DefaultDataSource, created for Application wsm-pm, Module wsm-pmserver-wls.
- 32 BEA-001124> <Created Connection Pool named hrDS.
- 26 BEA-001508> <Destroying data source connection pool hrDS.

Histogram



[Back to Cluster](#)

Showing 1-25 of 32

Time (UTC+1:00) ▾ Original Log Content

Jan 24, 2017,
11:22:19 PM

####<Jan 24, 2017, 10:22:19,625 UTC> <Info> <JDBC> <amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal> <amispaas_server_1> <[STANDBY] ExecuteThread: '42' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <449902a9-1b68-4970-8ddc-8c1c00062f6b-00001290> <1485296539625> <[severity-value: 64] [rid: 0] [partition-id: 0] [partition-name: DOMAIN]> <BEA-001126> <Destroyed Connection Pool named **hrDS**.>

⚙ Entity = amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal;9071;amispaas_server_1 | Entity Type = WebLogic Server | Log Source = FMW WLS Server Logs | Severity = Info

Jan 24, 2017,
7:28:47 AM

####<Jan 24, 2017, 6:28:47,15 UTC> <Info> <JDBC> <amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal> <amispaas_server_1> <[ACTIVE] ExecuteThread: '6' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <449902a9-1b68-4970-8ddc-8c1c00062f6b-0000000a> <1485239327015> <[severity-value: 64] [rid: 0] [partition-id: 0] [partition-name: DOMAIN]> <BEA-001124> <Created Connection Pool named **opss-audit-viewDS**>

⚙ Entity = amispaas_server_1 | Entity Type = WebLogic Server | Log Source = FMW WLS Server Logs | Severity = Info

Jan 24, 2017,
7:28:46 AM

####<Jan 24, 2017, 6:28:46,257 UTC> <Info> <JDBC> <amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal> <amispaas_server_1> <[ACTIVE] ExecuteThread: '6' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <449902a9-1b68-4970-8ddc-8c1c00062f6b-0000000a> <1485239326257> <[severity-value: 64] [rid: 0] [partition-id: 0] [partition-name: DOMAIN]> <BEA-001124> <Created Connection Pool named **opss-audit-DBDS**.>

⚙ Entity = amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal;9071;amispaas_server_1 | Entity Type = WebLogic Server | Log Source = FMW WLS Server Logs | Severity = Info

Jan 24, 2017,
7:28:46 AM

####<Jan 24, 2017, 6:28:46,257 UTC> <Info> <JDBC> <amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal> <amispaas_server_1> <[ACTIVE] ExecuteThread: '6' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <449902a9-1b68-4970-8ddc-8c1c00062f6b-0000000a> <1485239326257> <[severity-value: 64] [rid: 0] [partition-id: 0] [partition-name: DOMAIN]> <BEA-001124> <Created Connection Pool named opss-audit-DBDS.>

⚙ Entity = amispaas_server_1 | Entity Type = WebLogic Server | Log Source = FMW WLS Server Logs | Severity = Info

Jan 24, 2017,
7:28:45 AM

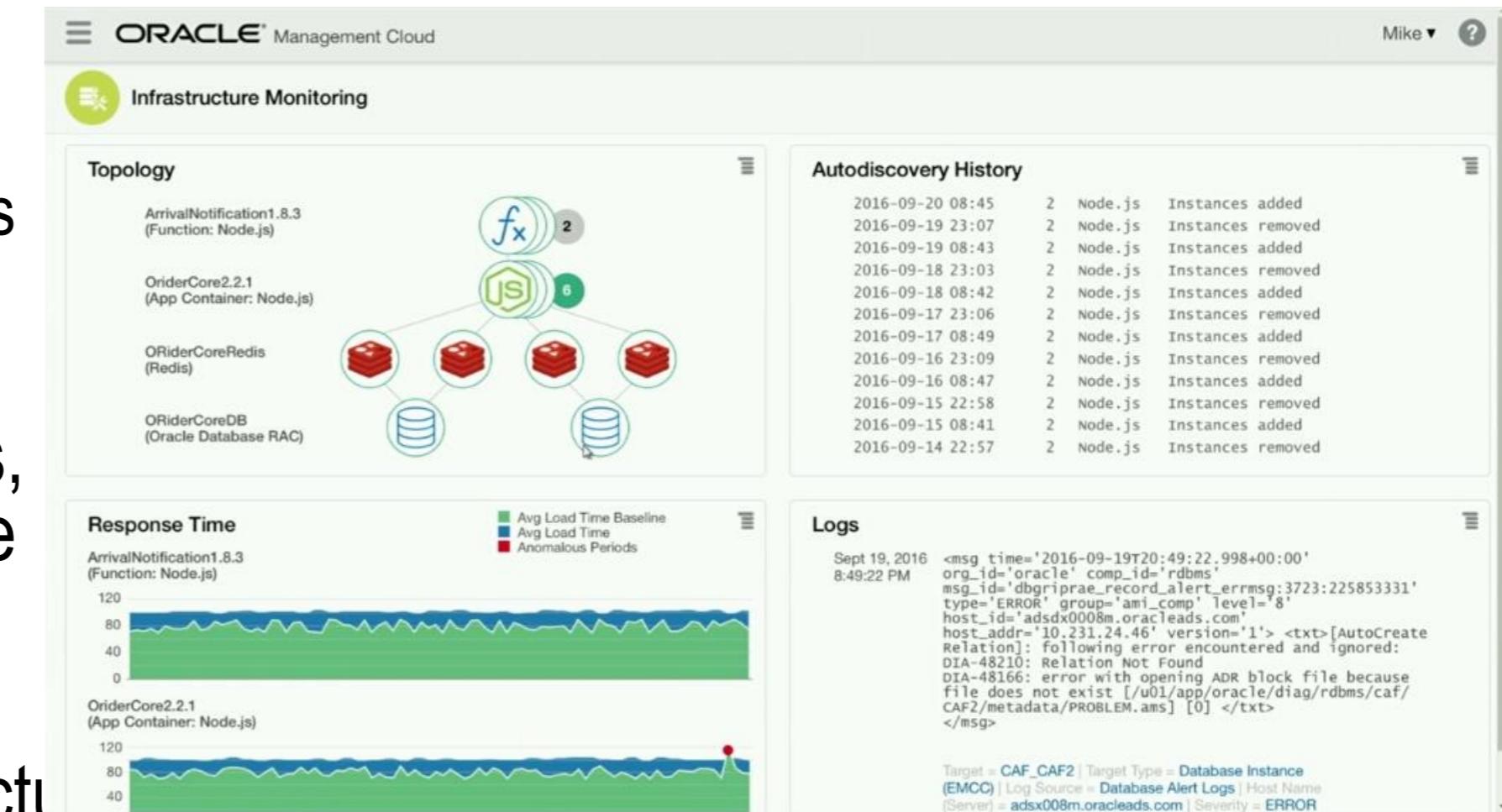
####<Jan 24, 2017, 6:28:45,501 UTC> <Info> <JDBC> <amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal> <amispaas_server_1> <[ACTIVE] ExecuteThread: '6' for queue: 'weblogic.kernel.Default (self-tuning)'> <<WLS Kernel>> <> <449902a9-1b68-4970-8ddc-8c1c00062f6b-0000000a> <1485239325501> <[severity-value: 64] [rid: 0] [partition-id: 0] [partition-name: DOMAIN]> <BEA-001124> <Created Connection Pool named **mds-owsm**.>

⚙ Entity = amispaas-db-java-stack-jaas-wls-1.compute-amispaas.oraclecloud.internal;9071;amispaas_server_1 | Entity Type = WebLogic Server | Log Source = FMW WLS Server Logs | Severity = Info

INFRASTRUCTURE MONITORING



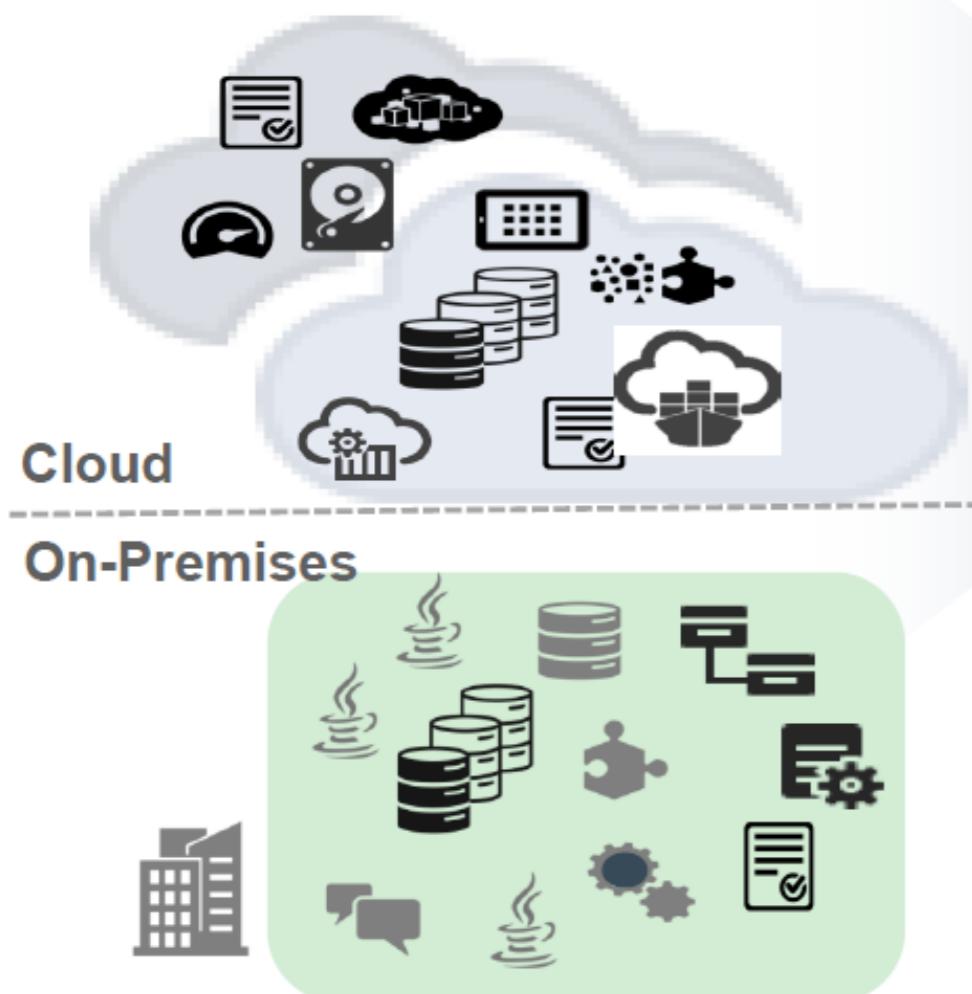
- Monitors the status and health of IT infrastructure in real time
 - on-premises or on the cloud and across stack tiers
- Proactive monitoring enables administrators to be alerted on issues, troubleshoot and resolve these before they impact end users.
- Similar to Application Performance Monitoring - focusing on the infrastructure components and their performance and behavior



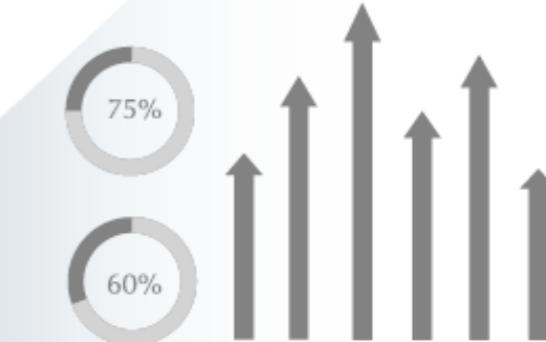
INFRASTRUCTURE MONITORING



Infra Status & Health, Associations



Panoramic, Unified Visibility



Problem Detection & Alerting

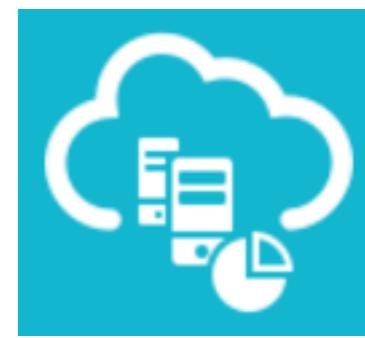


Correlation & Troubleshooting

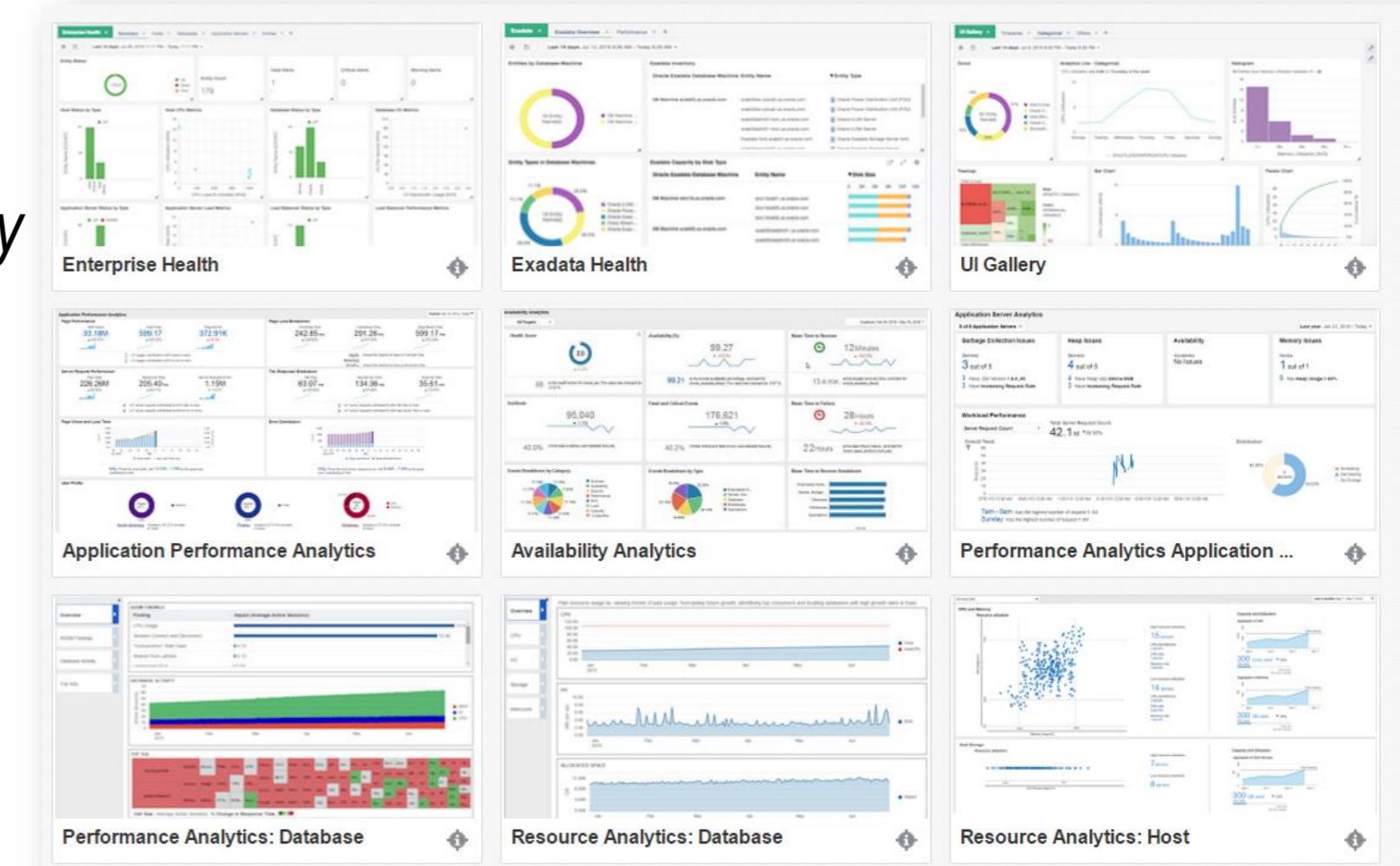


- Rapid deployment, quick time to value, scales on demand
- Broad, heterogeneous coverage
- Purpose-built dashboards
- Flexible Alerting
- Correlate and Troubleshoot
- Unified, Rich Data Model
- Rest APIs for custom metrics/data

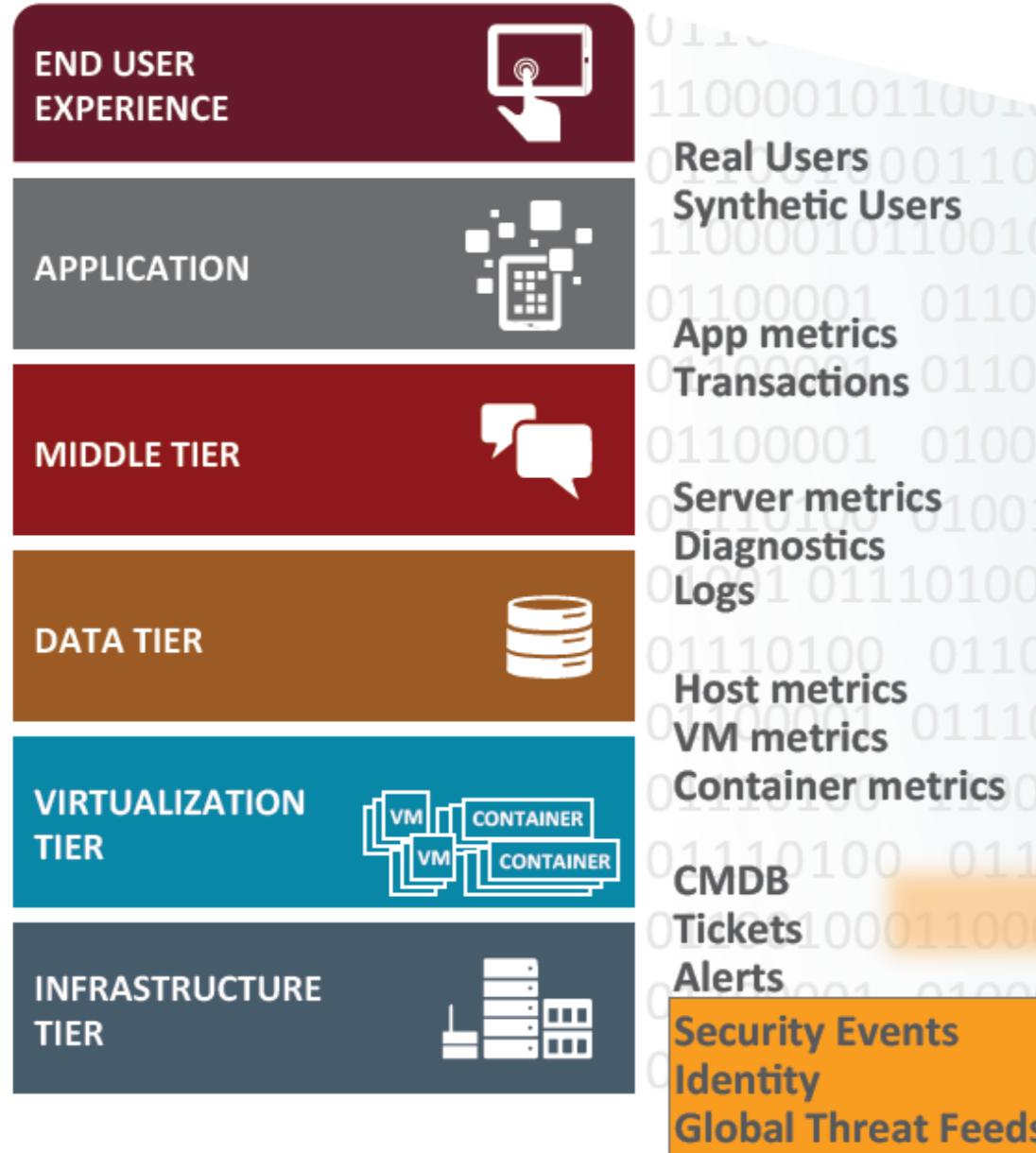
IT ANALYTICS – OPERATIONAL INTELLIGENCE FOR MODERN IT



- IT Analytics provides
 - 360-degree insight
 - into the *performance*, *availability*, and *capacity*
 - of applications and IT investments,
- enabling line-of-business executives, analysts, and administrators
- to make critical decisions about their IT operations based on comprehensive system and data analysis
- Out of the box and custom widgets & dashboards



SECURITY MONITORING & ANALYTICS

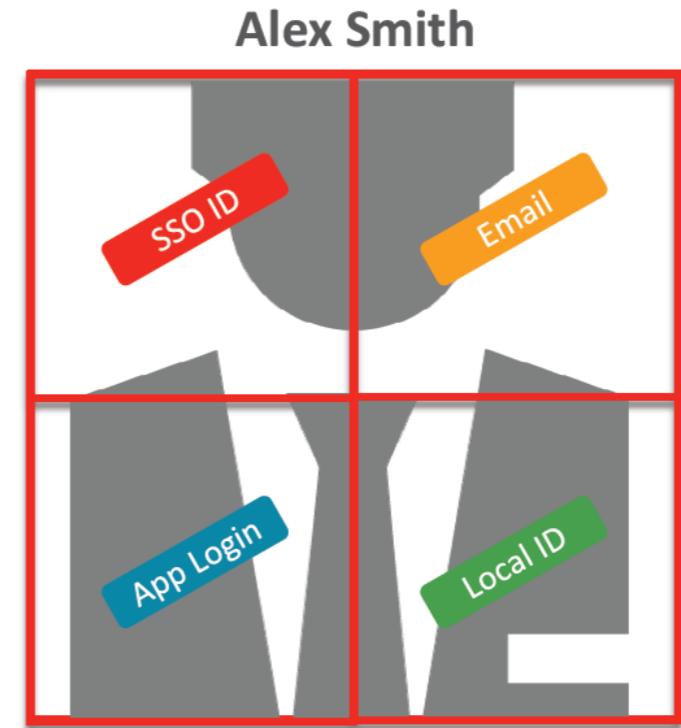
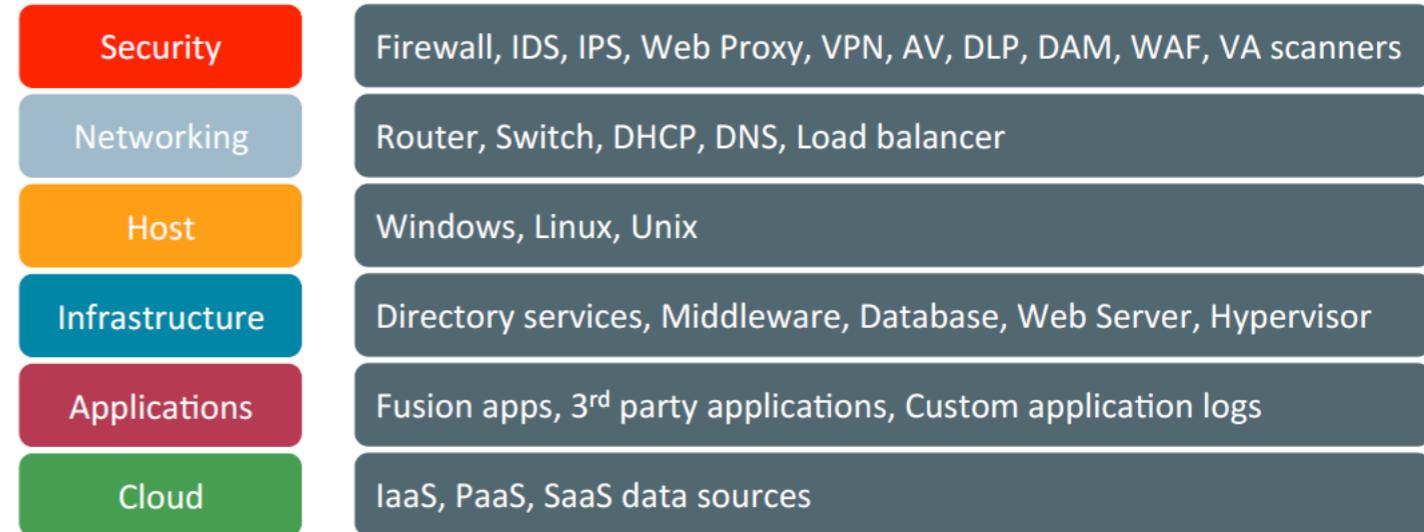


- INCREASED EFFICIENCY**
- FEWER OUTAGES**
- GREATER AGILITY**
- BETTER SECURITY**

SECURITY MONITORING & ANALYTICS



- **Improved Security and Risk Posture**
 - Lower risk and cost of data breaches and security incidents
 - Early detection of known and unknown threats
 - Visibility across heterogeneous infrastructure, cloud assets
- **Greater SOC Efficiency**
 - Fewer false positives and negatives
 - Faster time to detection and remediation
 - Reduced learning curve for SOC analysts
- **Rapid Time to Value**
 - Delivered as a next-gen, auto-scaling cloud service
 - Pre-packaged content for security and compliance
 - Runbook templates for automation of SOC operations



SECURITY MONITORING & ANALYTICS



ORACLE Management Cloud Service Admin ▾

Security Monitoring and Analytics Service Dashboard Security Monitoring and Analytics Compliance Orchestration Workflows Application Performance Monitoring Infrastructure Monitoring Log Analytics IT Analytics

Last 24 Hours Snapshot

90.2M Log Records 7 Incidents 5 Auto-Remediated 5 High Risk Users 3 High Risk Assets

Global Threat Origin Map

Global Status by Application

ORider Billing Support Finance

Incidents – Last 24 Hours

Incident	Timestamp	Application	User	Severity	Threat Category	Status
31009	Sep 20, 2016 03:21:36	ORider	Alex Smith	High	Hijacked Account Kill Chain detected	Auto-Remediated: Account Locked
31007	Sep 20, 2016 00:40:08	ORider	–	High	DDOS Attack	Auto-Remediated: IP Range Black Listed
31003	Sep 19, 2016 12:31:32	ORider	Bob Jones	High	Sensitive Data Exfiltration	Auto-Remediated: Port Blocked
31005	Sep 19, 2016 15:33:46	Support	Charlie Taylor	Med	Anomalous Lateral Movement	Auto-Remediated: Password Reset
31004	Sep 19, 2016 15:21:53	Support	Diane Chan	Med	Malware	Investigation - SOC Level 2

High Med Low Search

Threat Intelligence Statistics

Time Since Last Update: 2s
Total Indicators: 60M
Number of Feeds: 3

Incident Trend - Last 7 Days

Incidents Auto-Remediated SOC Triaged

Day Ago	Incidents	Auto-Remediated	SOC Triaged
1	3	2	1
2	4	3	1
3	5	4	1
4	4	4	1
5	5	4	1
6	3	3	1
7	7	5	2

SECURITY MONITORING & ANALYTICS



ORACLE Management Cloud Service Admin ▾

Security Monitoring and Analytics Service Incidents / 31009

Last 24 Hours Snapshot

90.2M Log Records

Global Status by Application

ORider Bill

Incidents – Last 24 Hours

Incident	Timestamp	Appli	User	Risk	Description	Remediation
31009	Sep 20, 2016 03:21:36	ORider	Alex Smith	High	Hijacked Account Kill Chain detected	Auto-Remediated: Account Locked
31007	Sep 20, 2016 00:40:08	ORider	–	High	DDOS Attack	Auto-Remediated: IP Range Black Listed
31003	Sep 19, 2016 12:31:32	ORider	Bob Jones	High	Sensitive Data Exfiltration	Auto-Remediated: Port Blocked
31005	Sep 19, 2016 15:33:46	Support	Charlie Taylor	Med	Anomalous Lateral Movement	Auto-Remediated: Password Reset
31004	Sep 19, 2016 15:21:53	Support	Diane Chan	Med	Malware	Investigation - SOC Level 2

Timeline

- Machine Learning Trigger
Anomalous Hard Parses Against ORider database
- Sessionization Trigger
70 APM links Alex Smith to endpoint IP 192.168.11.91
- Threat Context Escalation
95 IP 192.168.11.91 accessed malicious external host
- App Topology Link
70 Middleware identifies user as Alex Smith
- User Risk Escalation
80 Alex Smith has recent entitlement changes

Number of Feeds: 3

Incident Trend - Last 7 Days

Day Ago	Incidents	Auto-Remediated	SOC Triaged
1	3	2	1
2	4	3	1
3	5	4	1
4	4	4	1
5	5	4	1
6	3	3	1
7	7	5	2

COMPLIANCE & CONTROL

Who



CIO, CFO
VP for Audit and
Compliance

What

How do I know that I
am STIG Compliant?

Value

Is the compliance posture
sufficiently improving?
What do I need to do to fix
SLAs Violations?

Information
Security
Officer



Am I meeting my LOB
compliance SLAs for Finance
and HR ?

Current security posture of
cloud and on-premise
resources?

Are my resources deployed
effectively?



Administrators &
IT Compliance
Analyst

What violations do I
need to remediate
at this moment?

What vulnerability
do I fix next based
on prioritization &
risk level?

COMPLIANCE DEFINE RULES – EVALUATE – REMEDIATE - REPORT



Enterprise Perspective	Operations Across IT Groups
 Timely score for the entire IT enterprise, compliance communications & trainings	 A score scoped to my assets vertically by application or horizontally by entity: database, middleware, hosts, ect.
 Prioritization of assets based on operational & data value	 Prioritized asset & violation work list
	 Continuous and measurable compliance score improvement & reporting
	 Very small known vulnerability time-windows
	 Manage enterprise compliance by exception
	 Align resources to achieve service levels
	 Score & report trends for my entities
	 Automated remediation at scale
	 3 rd party ticketing and violation assignment
	 Agree to an achievable service level with the business

COMPLIANCE

ORACLE Management Cloud Service Admin

Compliance Application Summary / ORider

Topology

Compliance

Average Compliance Score
91.38% ▲ 0.78%

Violation by Entity Types

Violation by Severity

Violations

Violation Type	Last Evaluated	Rule Set	Resource	Severity
Database Patch Inconsistency Configuration difference detected.	6 hours ago Last Evaluated	Database Patch Comparison Rule Set	database1531 Database Instance	critical
Missing Required OS Package Required Operating System package not found.	6 hours ago Last Evaluated	Secure Infrastructure Best Practices Rule Set	Prd_host123 Host	high
Application using non-standard port Unapproved port usage detected by application.	6 hours ago Last Evaluated	Product Application Best Practices Rule Set	order_app_prd Host	high

AMIS

COMPLIANCE

The screenshot displays the Oracle Management Cloud Service interface, specifically the Compliance Service section. The main title is "Database Patch Configuration Comparison". The top navigation bar shows "Admin" and the Oracle logo.

Compared Targets Differences:

- 13 Target Compared
- 1 Targets with Difference (highlighted in red)
- database1531 (1) (highlighted in red)
- database5341 (0)
- database6893 (0)
- databasee1293 (0)
- database6235 (0)
- database6822 (0)
- database6845 (0)
- database6846 (0)
- database6847 (0)

Configuration Properties for Database:

Configuration Item	Identifier	Property Name	Reference DB
Patches		Patch Number	23054246
			missing
			Apply

Configuration Items Differences:

- Patches
- Initialization Parameters
- Control Files
- Database Options
- Users

Compliance Score: 37

Alerts:

- Application using non-standard port (Unapproved port usage detected by application.)
- Last Evaluated: 6 hours ago
- Product Application Best Practices Rule Set: order_app_prd Host
- Severity: Critical (red)
- Severity: High (orange)
- Severity: High (orange)

AMIS

REMEDIATE COMPLIANCE FINDINGS

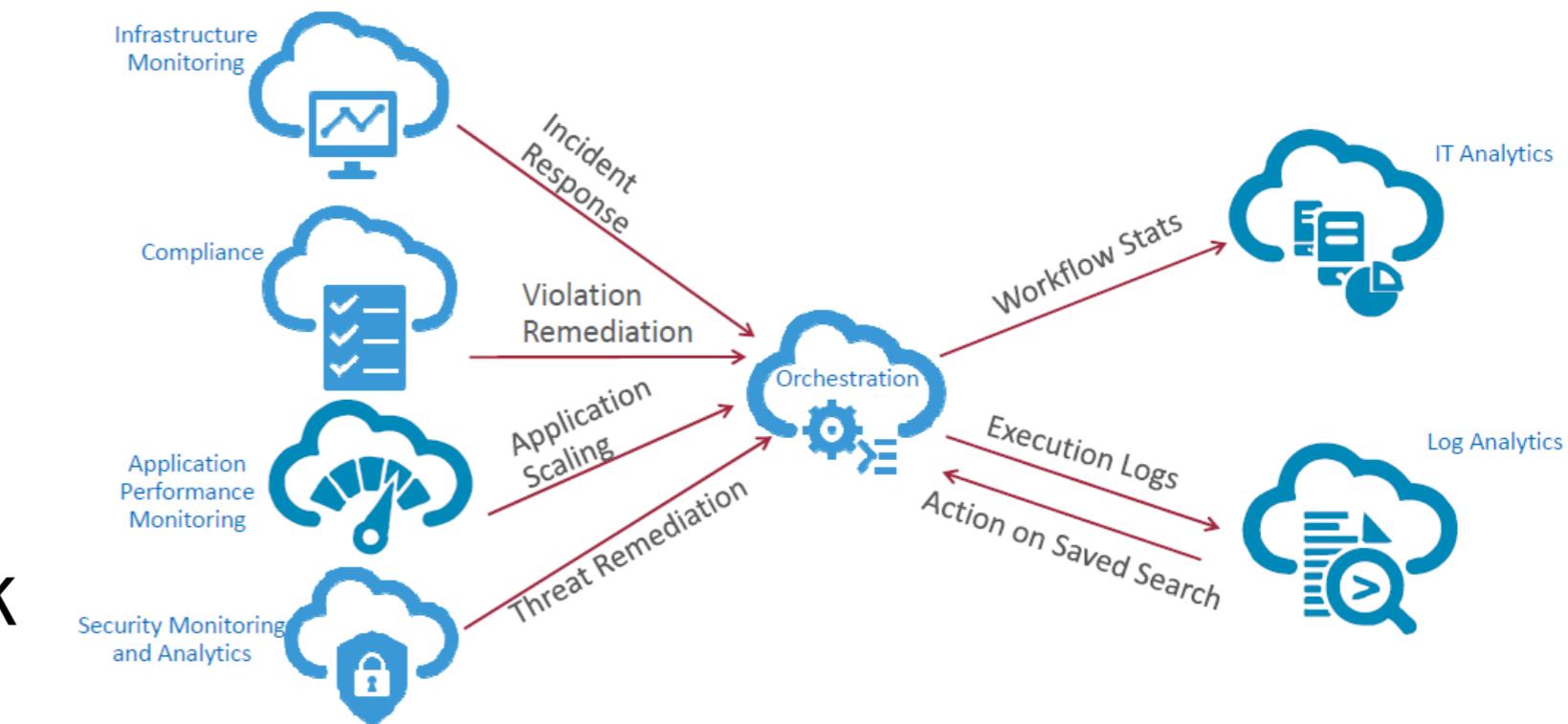
The screenshot displays two main Oracle Management Cloud Service interfaces:

- Database Patch Configuration Comparison:** This module shows a summary of differences between target databases. It indicates 13 Target Compared and 1 Target with Difference. A modal window titled "Orchestration Service Schedule Workflow" is open, titled "Apply Patch to database1531". The workflow details include:
 - Workflow Name:** Apply Patch to database1531
 - Patch Details:** 23054246 - Database Patch Set Update 12.1.0.2.160719
 - Deployment Option:** Out of place (recommended) (selected)
 - How to Deploy:** Rolling (selected)
 - Recurrence:** One-Time
 - Start Time:** ImmediatelyA message at the bottom of the modal says "Workflow 564738 has been successfully submitted!".
- Orchestration Service Schedule Workflow:** This module provides a dashboard view of patch deployment status. It includes a search bar, a table showing patch status (e.g., missing), and a large circular progress indicator showing a value of 37. Below the progress indicator, there are filters for "Selection Date: Old to New" and severity levels: critical (black), high (red), and medium (yellow).

AMIS

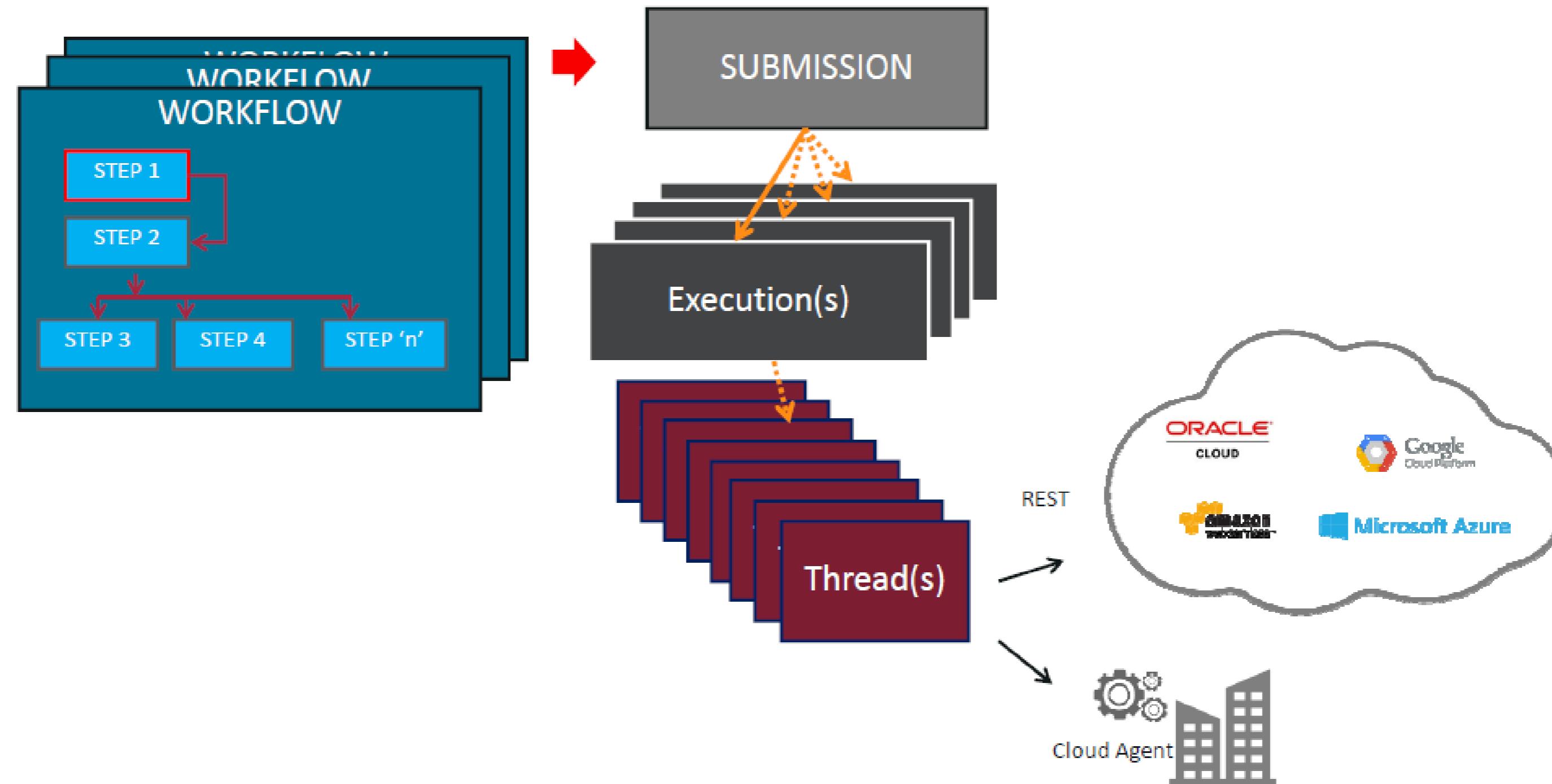
ORCHESTRATIONS == CRON ON THE CLOUD

- Cross stack | clouds Job Scheduler
- Orchestrate Provisioning and Deployment
 - Work with Chef, Puppet, OS script
- Execute workflows on behalf of other OMC services
 - E.g. compliance remediation
- Topology Aware workflow execution in bulk





ORCHESTRATION ARCHITECTURE





RUN WORKFLOW ON BEHALF OF SMA

The screenshot illustrates the Oracle Management Cloud Service interface, specifically the Security Monitoring and Analytics Service (SMA) module. A large blue arrow on the left side of the screen points from the main navigation bar down to the detailed incident timeline and event history sections.

The main navigation bar at the top includes links for Security Monitoring and Analytics Service, Dashboard, Security Monitoring and Analytics, Compliance, Orchestration Workflows, Application Performance Monitoring, Infrastructure Monitoring, Log Analytics, IT Analytics, and Admin.

The central part of the interface shows the "Incidents / 31009" page. It displays the "Machine Learning Trigger" (Anomalous Hard Parses Against Ride Share database), "Sessionization Trigger" (Middleware identified as Alex Smith), and "Threat Context Escalation". A modal window titled "Orchestration Service Workflow / 283745" is open, showing details for the "Blacklist IP Address" workflow:

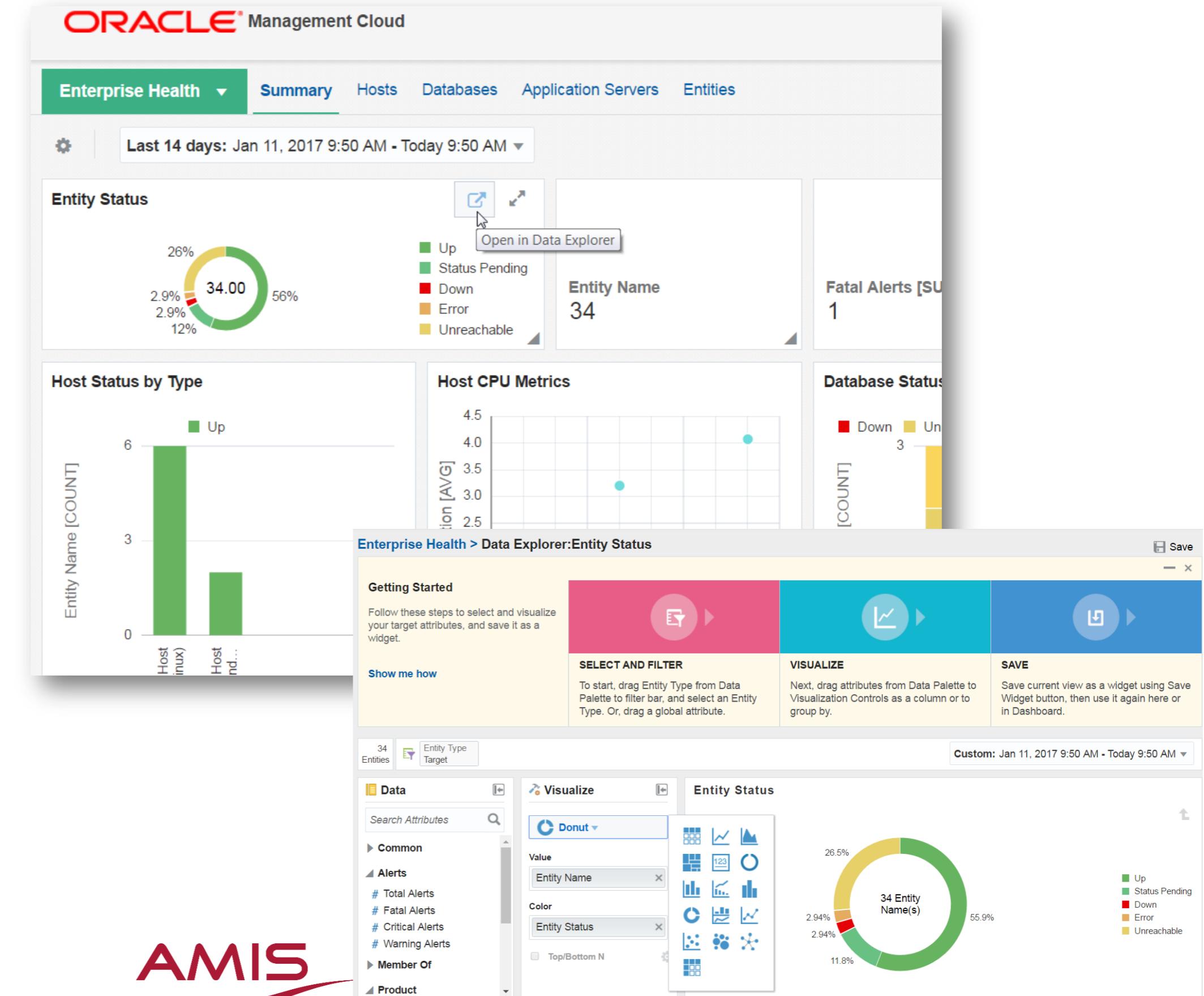
- Workflow Type: REST
- Owner: joh.doe@company.com
- Security Rule: orider_external_access
- Status: Succeeded
- Start Time: Sep 20, 2016 03:21:37
- End Time: Sep 20, 2016 03:21:48
- Elapsed Time: 11 seconds
- Target IP: 2.37.232.150
- Description: Known Malicious IP Accessed by User Alex Smith
- Notes: ASA-6-302013: Built outbound TCP connection 9 for outside: 10.1.2.1/22 (10.1.2.1/22) to inside: 192.168.11.91/53496 (192.168.11.91/53496)
- Entitlement Change for User Alex Smith
- IP Address Established for User Alex Smith

The "Event History" section below the modal lists several events:

Event Time	Source	Details
Sep 20, 2016 03:21:36	SMA	192.168.11.91 Alex Smith Known Malicious IP Accessed by User Alex Smith
Sep 20, 2016 03:21:36	SMA	192.168.11.91 Alex Smith %ASA-6-302013: Built outbound TCP connection 9 for outside: 10.1.2.1/22 (10.1.2.1/22) to inside: 192.168.11.91/53496 (192.168.11.91/53496)
Sep 20, 2016 03:21:36	FW	192.168.11.91 Alex Smith ASA-6-302013: Built outbound TCP connection 9 for outside: 10.1.2.1/22 (10.1.2.1/22) to inside: 192.168.11.91/53496 (192.168.11.91/53496)
Sep 20, 2016 03:17:21	SMA	192.168.11.91 Entitlement Change for User Alex Smith
Sep 20, 2016 03:28:30	IDM	192.168.11.91 IP Address Established for User Alex Smith
Sep 20, 2016 03:21:36	SMA	192.168.11.91 IP Address Established for User Alex Smith
Sep 20, 2016 03:28:30	APM	192.168.11.91 IP Address Established for User Alex Smith

DATA EXPLORING & VISUALIZATION

- Dashboards
- Data Explorer
- Create & Share Custom widgets



AMIS

AGENDA

THE WORLD OF DEVOPS AND
THE NECESSITY FOR
MONITORING & ANALYTICS

FIRST STEPS WITH OMC – HOW
[TO GET | WE GOT] STARTED



OVERVIEW OF ORACLE
MANAGEMENT CLOUD AND ITS
CONSTITUENTS

DRINKS & DINNER

HANDSON OMC - APPLICATION
PERFORMANCE MONITORING &
LOG ANALYTICS

LIVE DEMONSTRATION
OF THE FUNCTIONALITY
OF OMC



HANDSON OMC –
INFRASTRUCTURE
MONITORING & IT ANALYTICS

AGENDA

THE WORLD OF DEVOPS AND
THE NECESSITY FOR
MONITORING & ANALYTICS

FIRST STEPS WITH OMC
– HOW [TO GET | WE
GOT] STARTED



OVERVIEW OF ORACLE
MANAGEMENT CLOUD AND ITS
CONSTITUENTS

DRINKS & DINNER

HANDSON OMC - APPLICATION
PERFORMANCE MONITORING &
LOG ANALYTICS

LIVE DEMONSTRATION OF THE
FUNCTIONALITY OF OMC



HANDSON OMC –
INFRASTRUCTURE
MONITORING & IT ANALYTICS

(Y)OUR FIRST STEPS WITH OMC

- When and why?
- What do you need?
- Practical steps to get going
- How did we get started and what were the obstacles?



WHEN AND WHY (IS EXPLORING OMC RELEVANT)

- The real user experience (performance, availability) is important
- Insight in actual usage of the application(s) is relevant
- Optimal or at least efficient infrastructure resource usage is an objective
- It is desirable to be able to react (proact!) faster and more focused in case of incidents by analyzing and understanding root causes
 - The sumnum: predictive management
- The more complex the application and IT landscape, the more relevant Oracle Management Cloud is

WHAT DO YOU NEED?

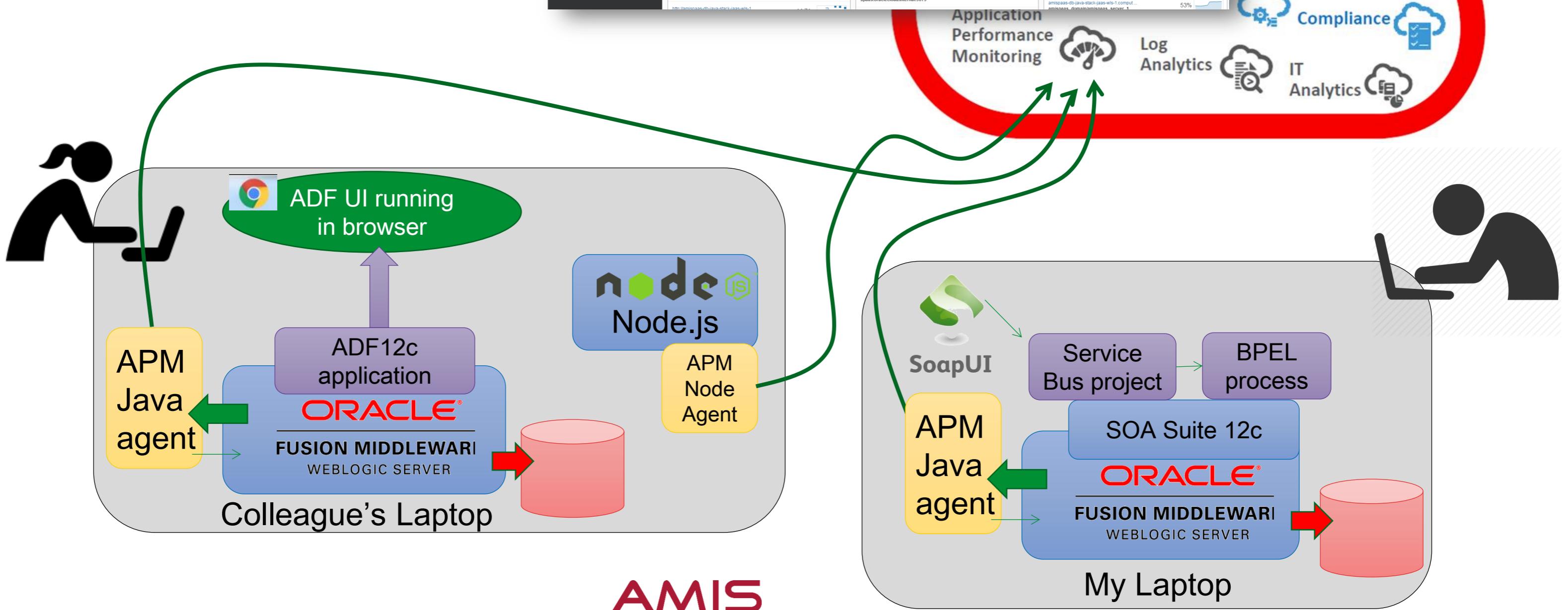
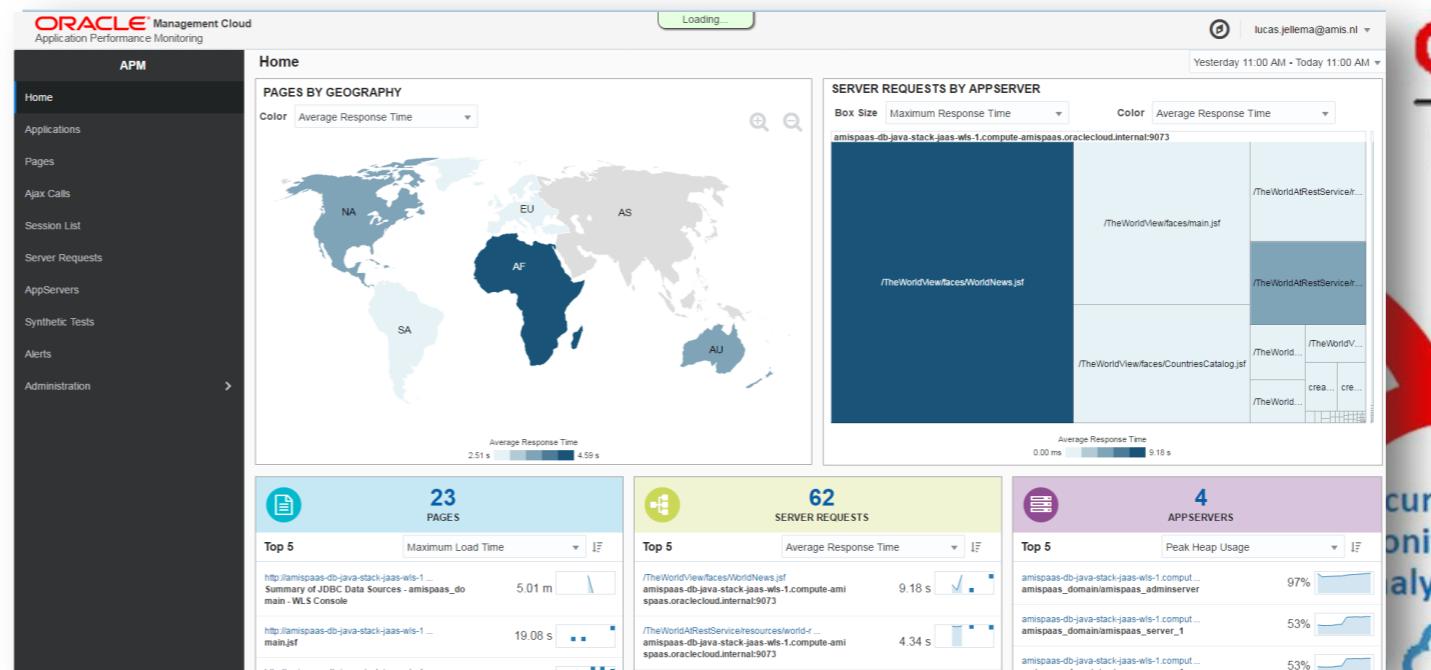
- Trial instance of Oracle Management Cloud
- Some OS skills (and ideally experience in DBA and WLS Admin) to install and configure the agents
- Applications and platform/infra components to test with
 - Optionally an Oracle PaaS Cloud instance and/or some 3rd party cloud) or even just a few laptops. Note: agents call out to OMC, OMC does not reach in
- Duh – a browser
- Note: no hardware is required to work with OMC –it is a cloud service!
- A plan based on underlying objectives:
 - what do you want to explore and try out? What is it you want to proof or learn? What is it you want to achieve that you believe OMC can help you with?
 - For example focus on User experience, outages, capacity planning, tracking of system events and human actions (for compliance), automating of IT management

PRACTICAL STEPS TO GET GOING

- Access the trial OMC environment
 - Create accounts for all collaborators
- Deploy agents for APM, Log Analytics, Infrastructure Monitoring
 - Perhaps Data Collector and Gateway
- Put meaningful load on application and platform
 - Perhaps intentionally cause some typical problems to find out how these can be identified through OMC
- Start with some simple analysis of very obvious issues
- Get support from someone who has been there (land of the blind...)

OUR FIRST STEPS

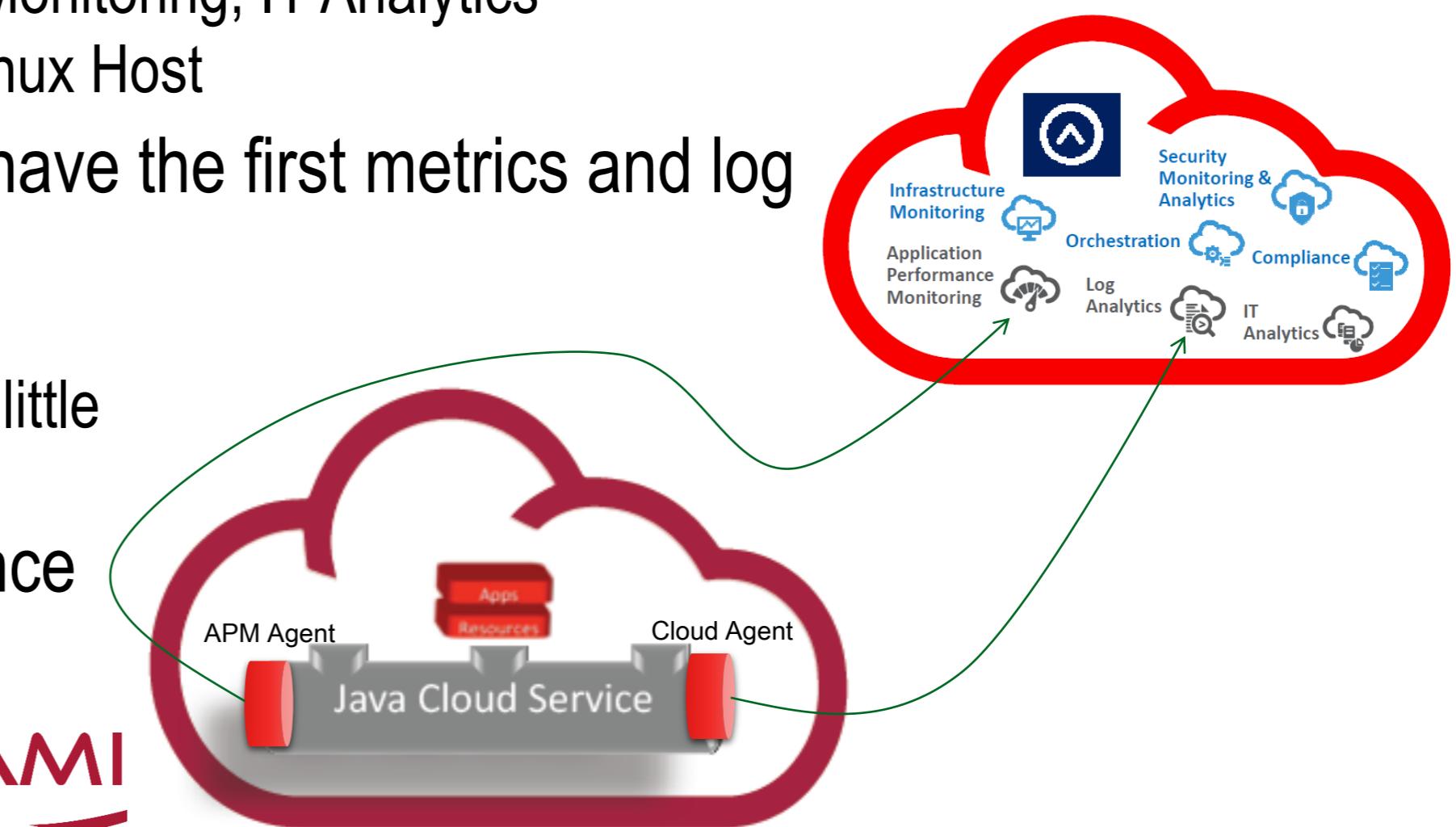
- Arranged trial through Dennis
- Created cloud accounts for all colleagues involved
- Deployed Cloud Agents on our own laptops
 - APM, Log Analytics, Infrastructure Monitoring, IT Analytics
 - For WebLogic, SOA Suite, Oracle Database, Linux Host, Node.js, ...
- It took very little time and effort to have the first metrics and log entries in the OMC instance
 - And to start analyzing
- Published some blog articles about our work



AMIS

OUR NEXT STEPS

- Request Oracle PaaS Trial Account
 - DBaaS, JCS, Compute, Storage,
- Deployed Cloud Agents Oracle Public Cloud Compute VMs
 - APM, Log Analytics, Infrastructure Monitoring, IT Analytics
 - For WebLogic, Oracle Database, Linux Host
- It took very little time and effort to have the first metrics and log entries in the OMC instance
 - And to start analyzing
 - Some Linux admin challenge and a little Cloud Agent script bug to fix
- We will use this PaaS Cloud instance in the handson workshop tonight



APM & LOG ANALYTICS EXPLORATIONS

- What can we learn about what our users are doing?
 - Which functionality is being used – when/from where/by whom
- What insight do we get about poor performance (sub standard) and errors our users run into?
 - Dashboard & alerts
- How can we enrich application level logging to be able to better understand and analyze run time behavior?
- What work instructions can we develop for application administrators (and DevOps team) to investigate issues?
- Bonus/Low hanging fruit: find errors and warnings in our application code, resolve deployment issues, learn about framework errors, learn about WLS and ADF behavior (package dbms_pickle)

LEARNING POINTS, ROUGH EDGES AND OBSTACLES

- It is deceptively simple to get going
 - And not so simple to find out how to extract the most value from what OMC has to offer
- Configuring the agents can be very smooth and straightforward
 - And sometimes requires careful investigation and configuration
- APM:
 - Does not carry business indicators
 - Not so easy to find a specific user's session
 - APM and ADF are not a perfect combination
 - APM works best on individual pages rather than single/few page applications
 - APM does not explicitly support API & Service calls – it focuses on UI requests
 - APM location map could be more detailed: The Netherlands is a granular as it gets

OMC EXPERIENCES

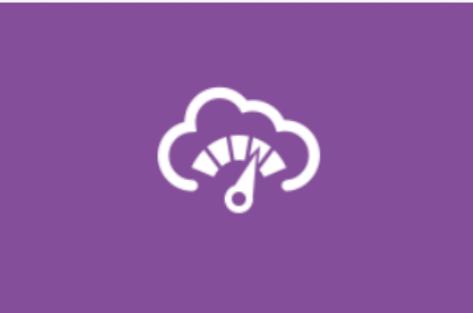
Service Detail X Landing Home - Oracle M... +

https://nlamistrial73269.management.us2.oraclecloud.com/emsasui/emcpdfui/welcome.html

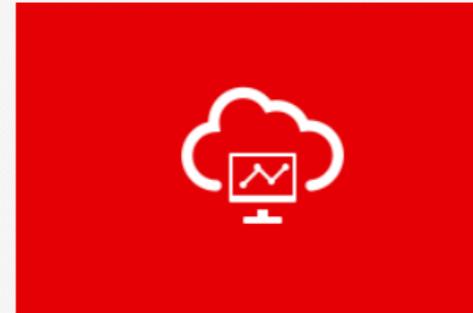
Zoeken job.oprel@amis.nl

ORACLE Management Cloud

Welcome to Oracle Management Cloud



Application Performance Monitoring
Rapidly identify, response, and resolve your software roadblocks



Infrastructure Monitoring
Monitor your entire IT infrastructure - on-premise or on the cloud - from one unified platform



Log Analytics
Topology aware log exploration and analytics for modern applications and infrastructure



IT Analytics
Operational big data intelligence for modern IT
Select ▾



Dashboards
Build custom dashboards using out-of-the-box widgets or your own visualization of data
Select ▾



Data Explorers
Search, analyze, and visualize data
Select ▾

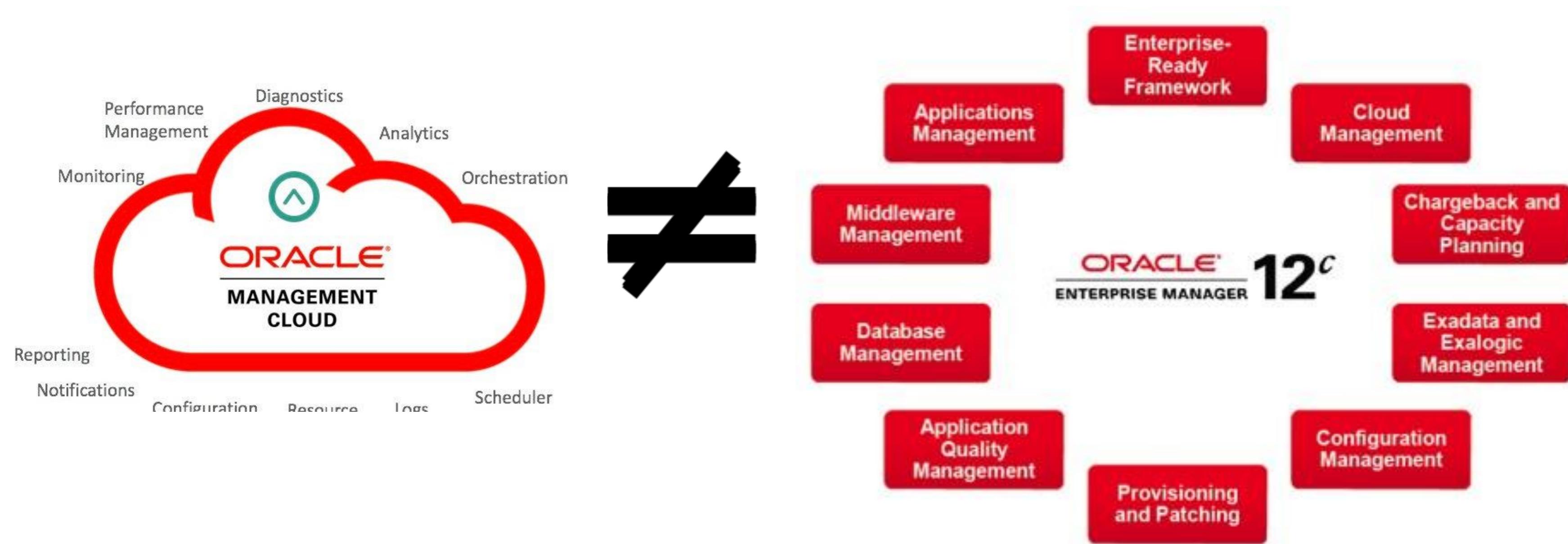
Learn More

- [How to get started](#)
- [Videos](#)
- [Service Offerings](#)

javascript: this.click()

12:26 26-1-2017

OMC = OEM IN THE CLOUD?



THE JOURNEY - START

My Services - Dashboard X +

https://myservices.us2.oraclecloud.com/mycloud/faces/dashboard.jspx?_adf.ctrl-state=s5qs3vqp8_4&_afrLoop=109933348948423 Zoeken

nlamistrial73269 | Preferences job.oprel@amis.nl

ORACLE® CLOUD My Services Dashboard Users Notifications

Dashboard Customize Dashboard

ACCOUNT MANAGEMENT Select a subscription to see associated services ?

CLOUD SERVICES Identity Domain: nlamistrial73269, Data Center: US Commercial 2 (Time zone: US/Central)

0 Important Notifications

loganalytictrial9016
Log Analytics

Total Index Size (GB)

Index	Value (GB)
1	3
2	3
3	3
4	3
5	3
6	3
7	3

itanalytictrial7042
IT Analytics

Processors Analyzed...

Processor	Value (processors)
1	1.5
2	1.5
3	1.5
4	1.5
5	1.5
6	1.5
7	1.5
8	1.5

infrastructuretrial9705
Infrastructure Monitoring

Number of Monitored Objects...

Object	Value (objects)
1	1.5
2	1.5
3	1.5
4	1.5
5	1.5
6	1.5
7	1.5
8	1.5

apmtrial3371
APM

Number of Agents (agents)

Agent	Value (agents)
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1

OMC GUI

nlamistrial73269 |

Service Details:infrastructuretrial9705
(Oracle Infrastructure Monitoring Cloud Service)

Overview
(for January 2017)
100% uptime
3 unplanned outages

Business Metrics
(as of 2 hours 21 minutes ago)
10 number of monitored o...

Service Status - January 2017
Month View | Quarterly View | Year View Current Month

Legend: Before Activation Service Up Planned Outage Service Incident

Additional Information

Plan: Infrastructure Monitoring S...	Data Center: US Commercial 2
Service Start Date: 7-Dec-2016	Version: 16.4.6.0.0
Service End Date: 7-Mar-2017	Status: Active
Subscription ID: 554044099	Service Instance URL: https://nlamistrial73269.it...
Customer Account: AMIS (GB)	Domain SFTP Host & Port: sftp.us2.cloud.oracle.com:22
CSI Number: Not available	Domain SFTP User Name: nlamis5C

Launch Infrastructure Monitoring Service

OMC GUI

ORACLE® Management Cloud
Set up Oracle Management Cloud

Set up Infrastructure Monitoring

The setup is in progress. You should now deploy a gateway and cloud agents, and add entities to be monitored. This page updates automatically.

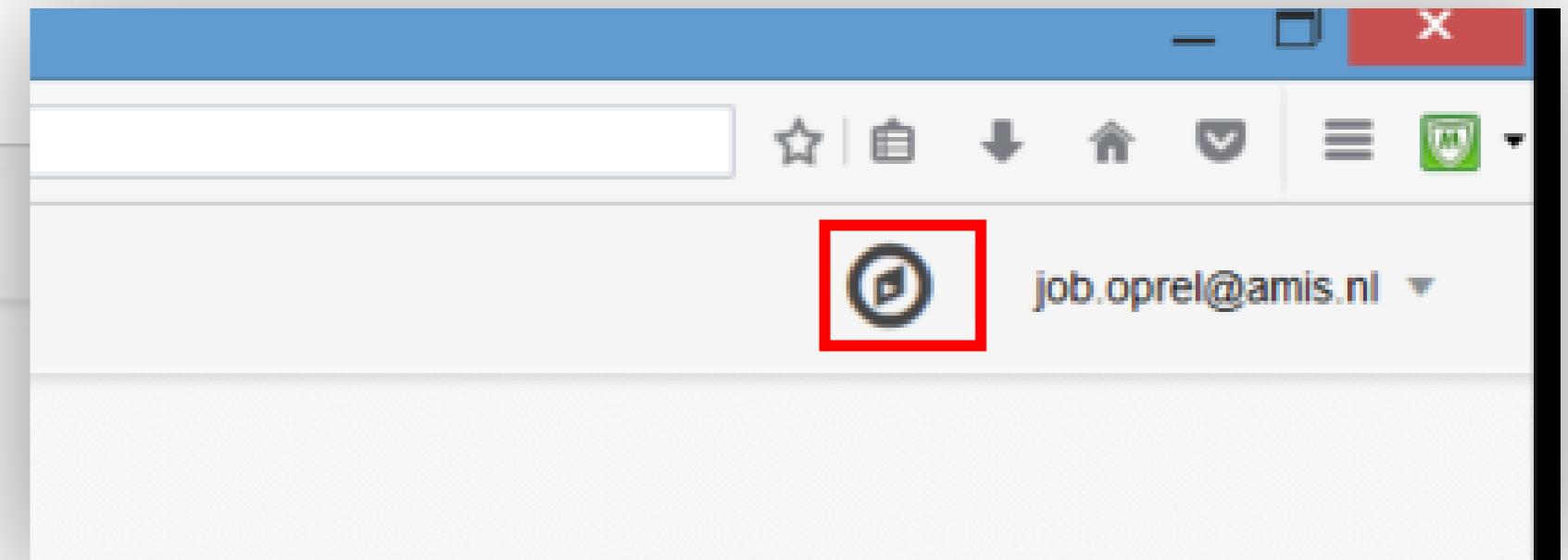
Detected Management Cloud Agents

- Gateways: 2
- Cloud Agents: 5
- Hosts with Cloud Agents: 0

[Go to Oracle Management Cloud](#)



Tip: Click Go to Oracle Management Cloud when at least one Gateway is deployed.



Cloud Services

[APM](#)

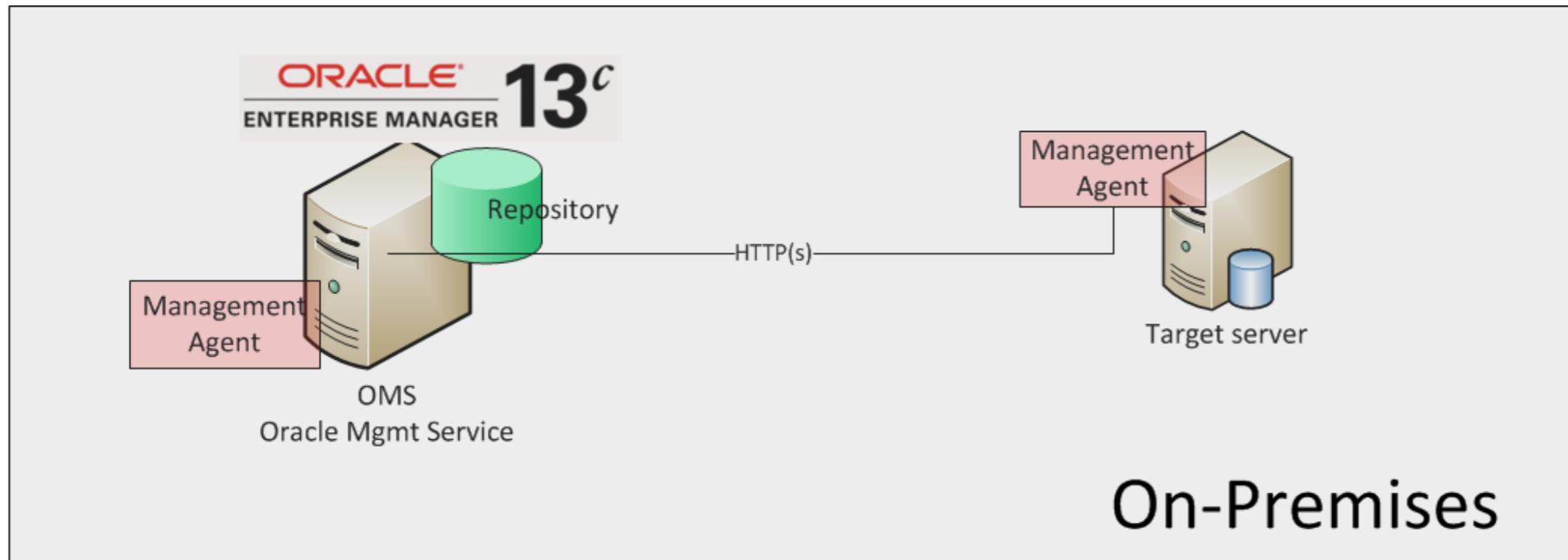
[IT Analytics](#)

[Log Analytics](#)

[Infrastructure Monitoring](#)

AMIS

INSTALL AND SETUP – OUR WORLD



Oracle Enterprise Manager

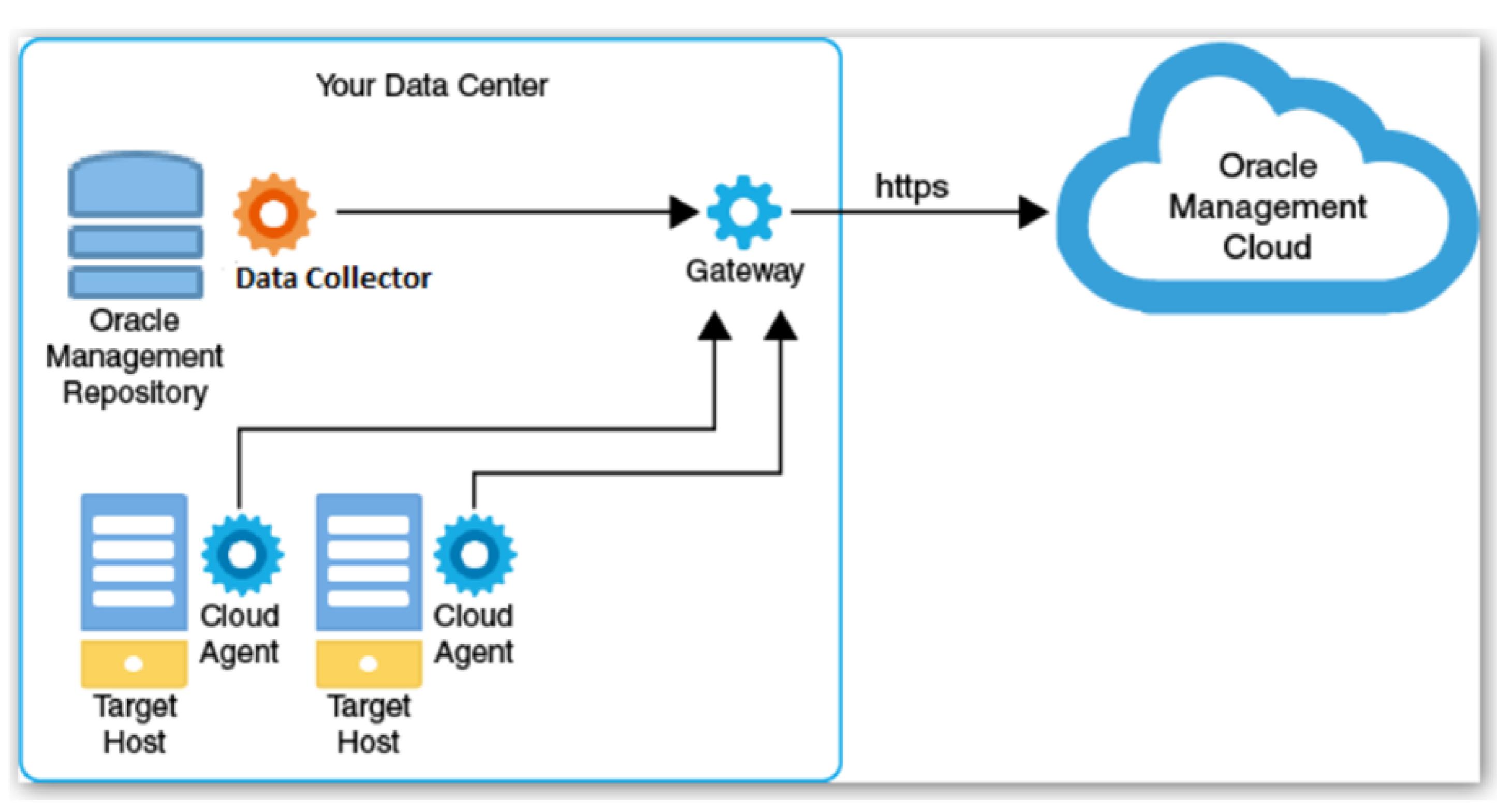
1. Push agent on target node from central node
2. Automatic Discovery process by agent on target node
3. Promote the interesting targets from central node

INSTALL AND SETUP OMC

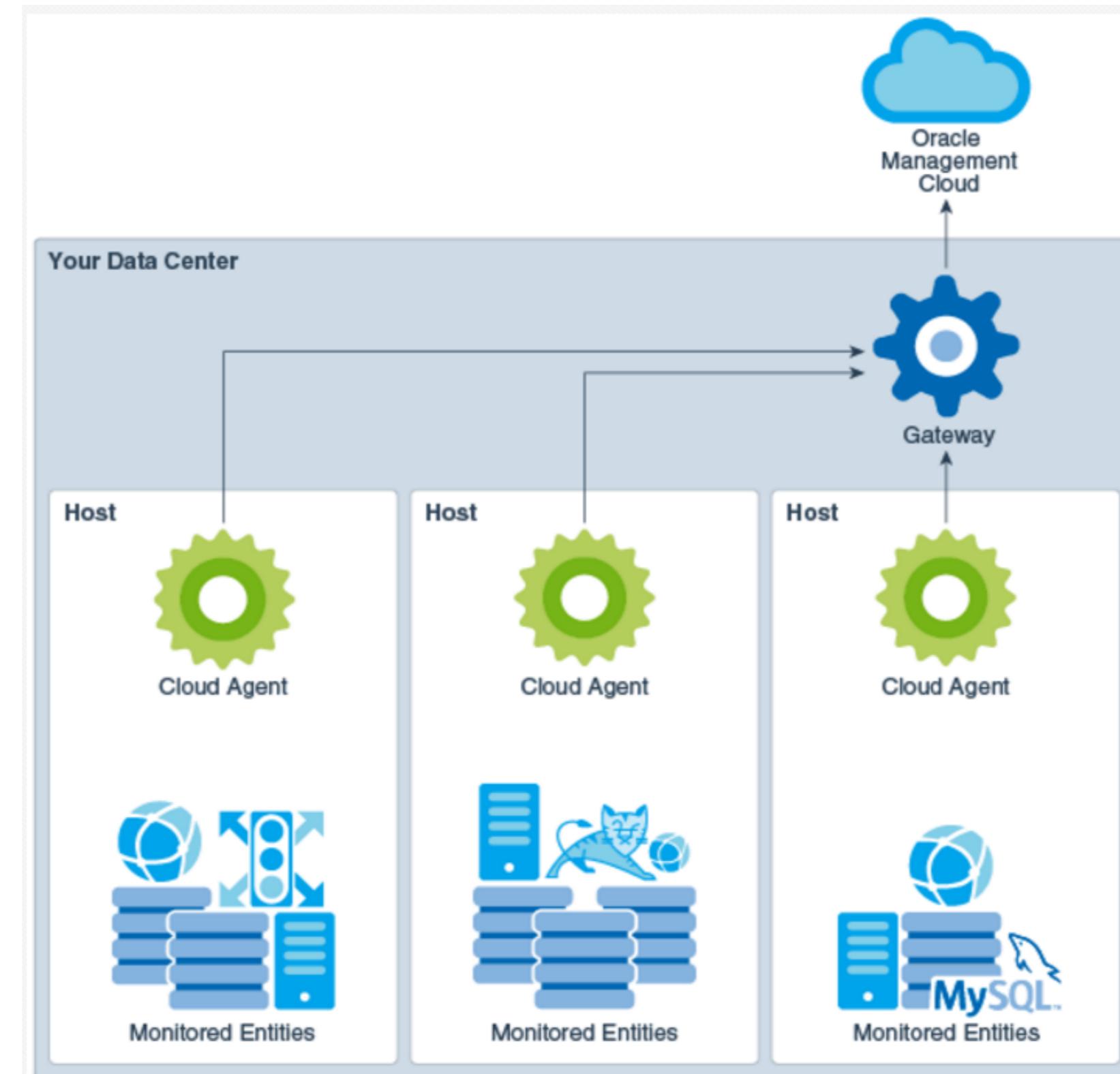
HOW HARD CAN IT BE

1. Plan where the agents will be installed
2. Download the Oracle Management Cloud Master Installer from this wizard
3. Install and set up the agents

BUT: DIFFERENT AGENTS



AND: DIFFERENT TARGETS



AMIS

1. AGENT – PLAN : KIND, WHAT TO DO

What we did:

Cloud Agents, Data Collector, Gateway on

- Laptops
- Oracle Cloud
- Server (VM) at AMIS network

Goal : Explore !!



2. DOWNLOAD OMC MASTER

ORACLE® Management Cloud
Set up Oracle Management Cloud

Set up Infrastructure Monitoring

[Cancel](#) [< Back](#)

Download

[!\[\]\(27dd1dc1dc12d3f2ceff930065ab1d45_img.jpg\) Download Master Installer](#)

Copy and save your registration key. You will need this key during the deployment process.

Registration Key [?](#)

After you download, in your data center:

- 1 Unzip the Master Installer.
- 2 Copy `AgentInstall.sh` (included in the Master Installer) to the gateway host and run it to deploy the gateway. [i](#)
- 3 Copy `AgentInstall.sh` (included in the Master Installer) to each host where you will deploy Cloud Agents and run it to deploy Cloud Agents. [i](#)
- 4 Add entities that will be monitored by your agents. [i](#)

3A. INSTALL AND SETUP THE AGENTS

Two ways:

- directly downloading and install
- download-only and then install



```
./AgentInstall.sh AGENT_TYPE=cloud_agent  
AGENT_REGISTRATION_KEY='RMxMm7chywi-J-VZ7_UfxY5XUU'  
AGENT_BASE_DIR=/omc_agent –staged
```

3B. INSTALL AND SETUP THE AGENTS



Promote the entities. Example : add a Linux Host.

1. Create two JSON-files per entity.
2. `./omc_agent/agent_inst/bin/omcli add_entity agent /omc_agent/omc_host_ovamisux159_linux.json -credential_file /omc_agent/omc_host_ovamisux159_linux_creds.json`



POSSIBLE ENTITIES TO PROMOTE

- Hosts:
 - Linux
 - Solaris
 - Windows
 - AIX
- DB:
 - MySQL
 - Oracle
 - Microsoft SQL
 - MongoDB
- Tomcat
- Weblogic Server, cluster, domain
- Docker Engine, container
- Traffic Director Instance, cluster

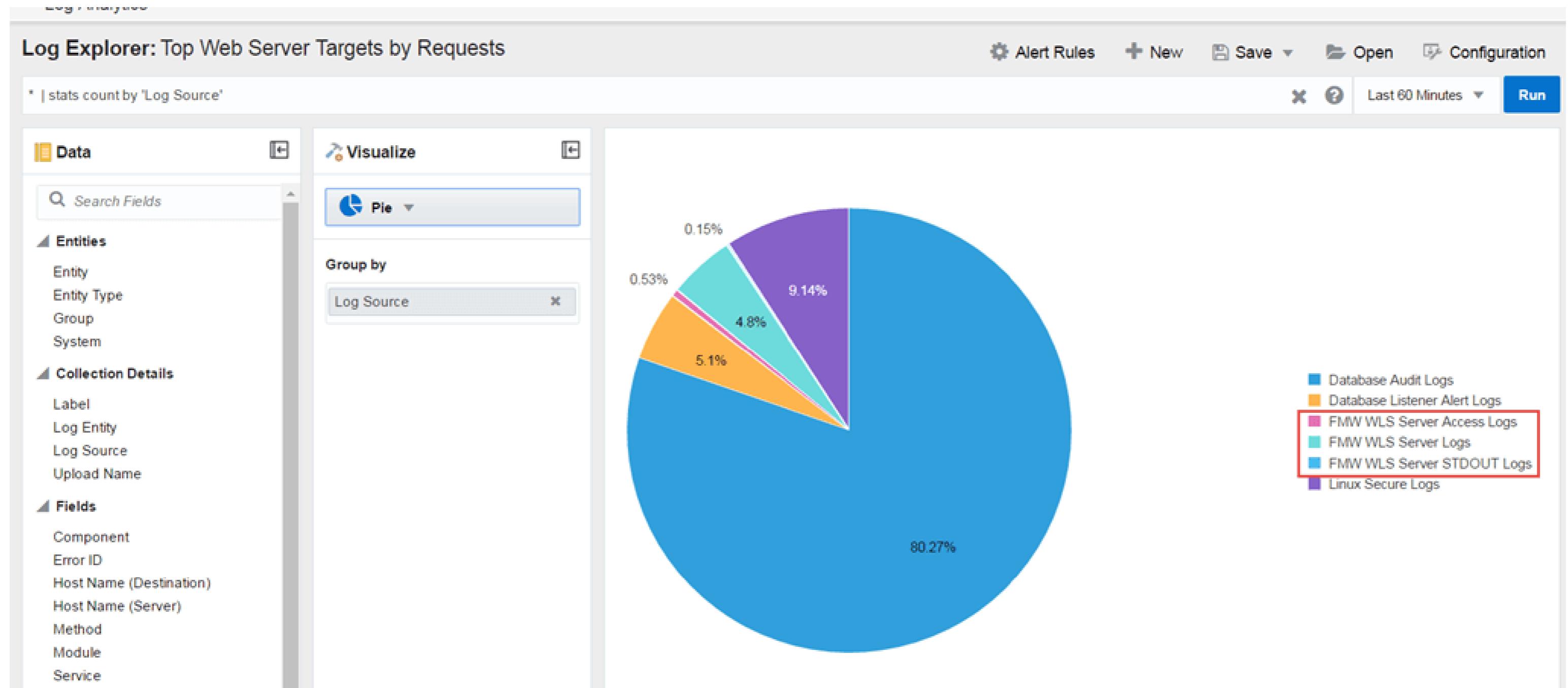
AND NOW THE DATA IS FLOWING – OR IS IT?

Example : ‘Obvious’ bug in logrules_os_file.xml:

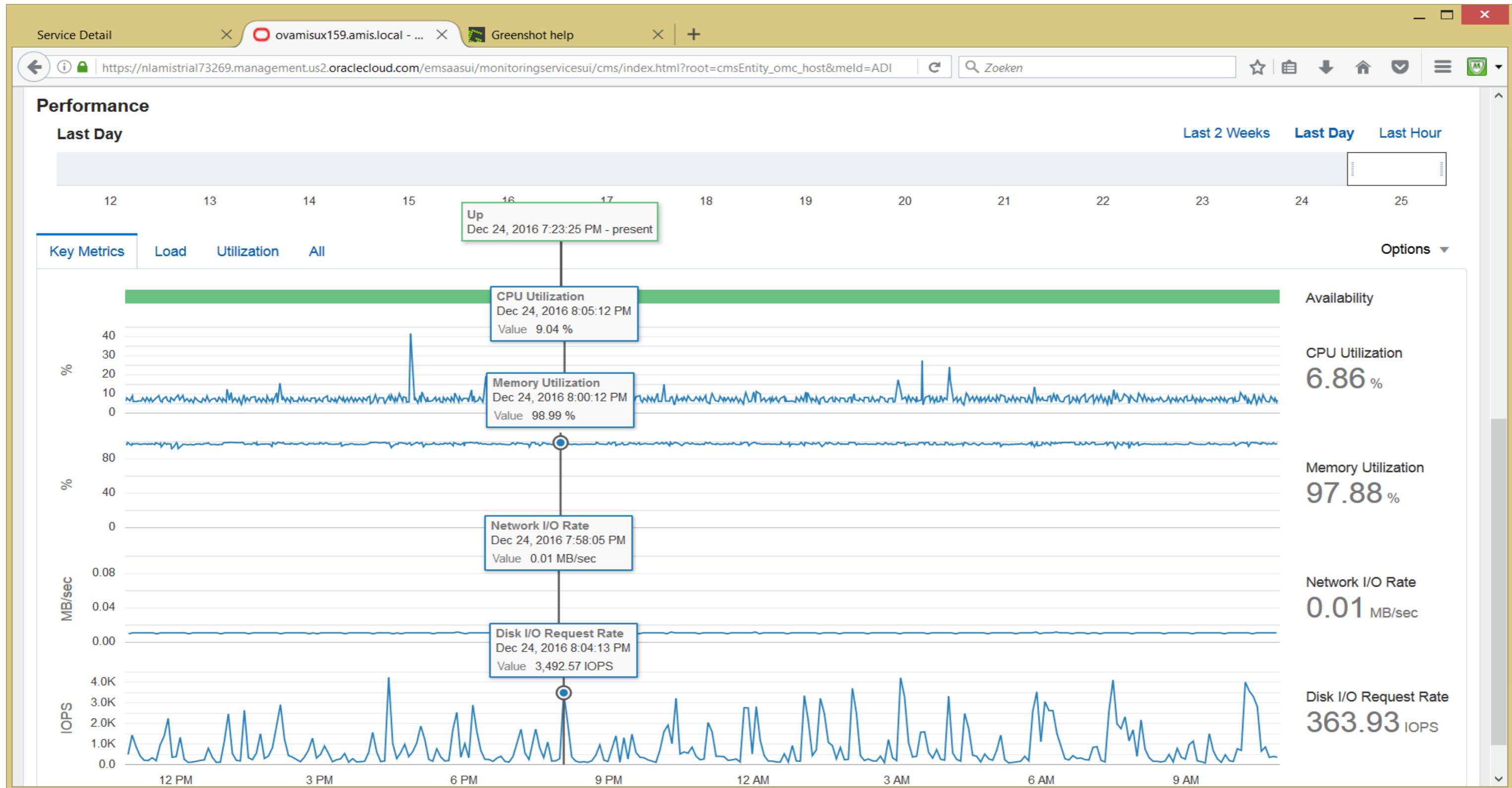
reg[ular]
expr[essio]n

```
<Name>tm_server.log</Name>  
<Regex>([\d]{2}:[\d]{2}:[\d]{2},[\d]{3})\s+(.*?)\s+\[(.*)\]\s+\[(.*)\]\s+  
([\d]{4})-([\d]{2})-  
([\d]{2})\s+([\d]{2}):([\d]{2}),([\d]{3})(.**)</Regex>
```

THERE IT IS !



ISOLATION



CONCLUSION

- Plan / goals before you start !
- Simple deployment - sometimes
- Number of agents
- GUI suboptimal
- Ton of potential
- More integrated
- Overview documentation

AGENDA

THE WORLD OF DEVOPS AND
THE NECESSITY FOR
MONITORING & ANALYTICS

FIRST STEPS WITH OMC – HOW
[TO GET | WE GOT] STARTED



OVERVIEW OF ORACLE
MANAGEMENT CLOUD AND ITS
CONSTITUENTS

DRINKS & DINNER

HANDSON OMC - APPLICATION
PERFORMANCE MONITORING &
LOG ANALYTICS

LIVE DEMONSTRATION OF THE
FUNCTIONALITY OF OMC



HANDSON OMC –
INFRASTRUCTURE
MONITORING & IT ANALYTICS

- Blog: technology.amis.nl
On Oracle, Cloud, SQL, PL/SQL, Java, JavaScript, Continuous Delivery, SOA, BPM & more
- Email: lucas.jellema@amis.nl
-  : lucasjellema
-  : lucas-jellema
-  : www.amis.nl, info@amis.nl
+31 306016000
Edisonbaan 15,
Nieuwegein