INOVASYS
ThinkBIG

(Log Analytics)

What does Azure Monitor Collect?

AZURE TENANT:

OPERATION OF TENANT-LEVEL AZURE SERVICES

AZURE SUBSCRIPTION:

OPERATION, MANAGEMENT, AND HEALTH OF AZURE

AZURE RESOURCE:

OPERATION OF AN AZURE RESOURCE

APPLICATION:

PERFORMANCE AND FUNCTIONALITY OF CODE

GUEST OS:

CLOUD/ON-PREMISES OS ON WHICH YOUR APPLICATION IS RUNNING

UNIFIED EXPERIENCE

COLLECT AND INDEX DATA | SEARCH AND INVESTIGATE | CORRELATE AND ANALYZE | VISUALIZE AND REPORT | MONITOR AND ALERT

Windows agents

SCOM

Linux / FluentD

REST Collection API

SaaS services

O365

Azure Storage /
Azure Diagnostics

Event Hub

Log Stash

- Log Analytics
- Automation
- Site Recovery
- Backup

Azure Monitor

Sample list of log/metrics that OMS collects:

- Custom Application/Infra logs
- Windows event logs
- Window performance counters
- Security Event Logs
- IIS Logs
- ETW logs
- Azure Diagnostics

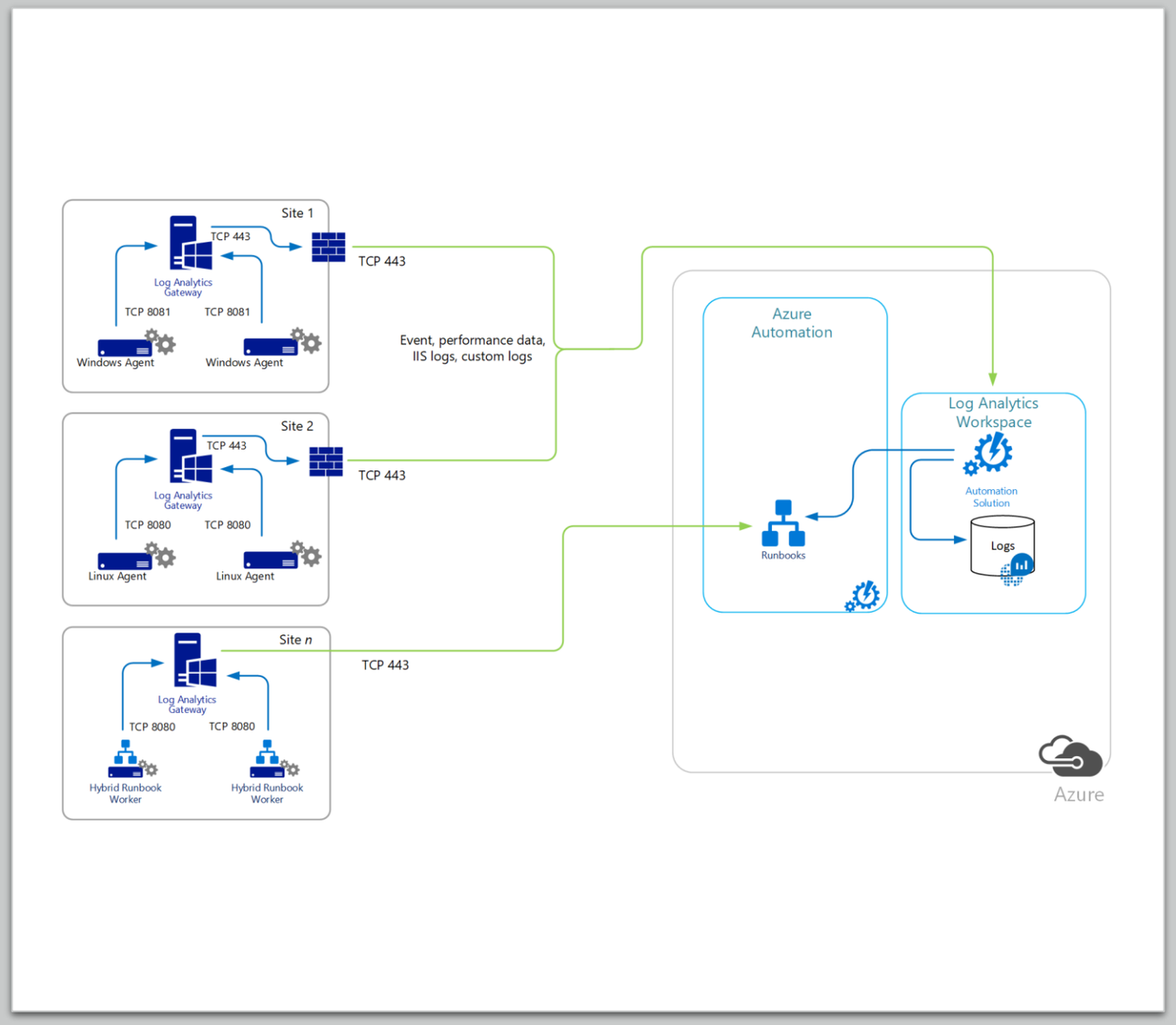
Azure Monitor Logs data security

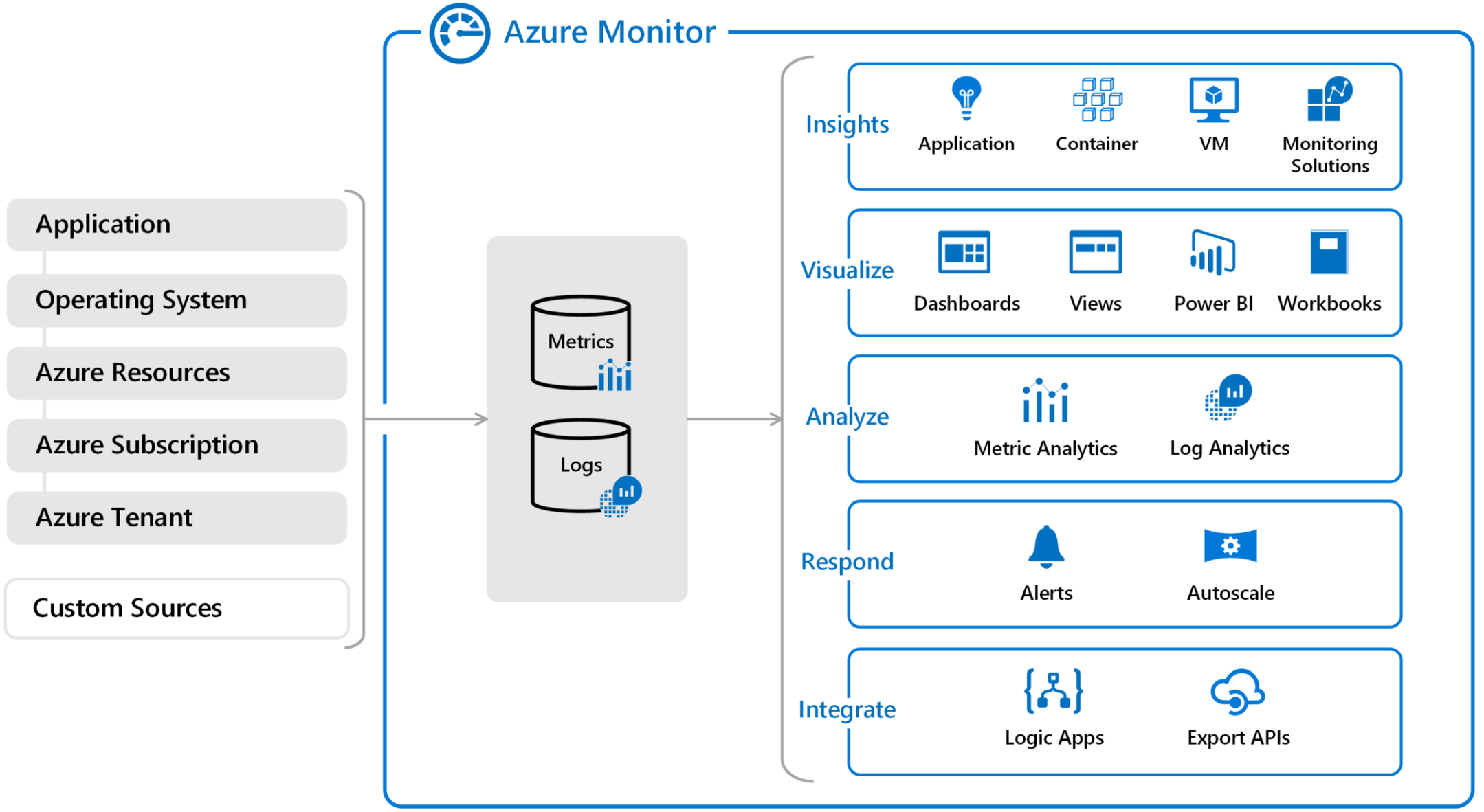
How log data is collected, processed, and secured by Azure Monitor.

Azure Monitor meets the following Certifications and attestations:

- ISO/IEC 27001
- ISO/IEC 27018:2014
- ISO 22301
- Payment Card Industry (PCI Compliant) Data Security Standard (PCI DSS) by the PCI Security Standards Council.
- Service Organization Controls (SOC) 1 Type 1 and SOC 2 Type 1 compliant
- HIPAA and HITECH
- Windows Common Engineering Criteria
- Microsoft Trustworthy Computing

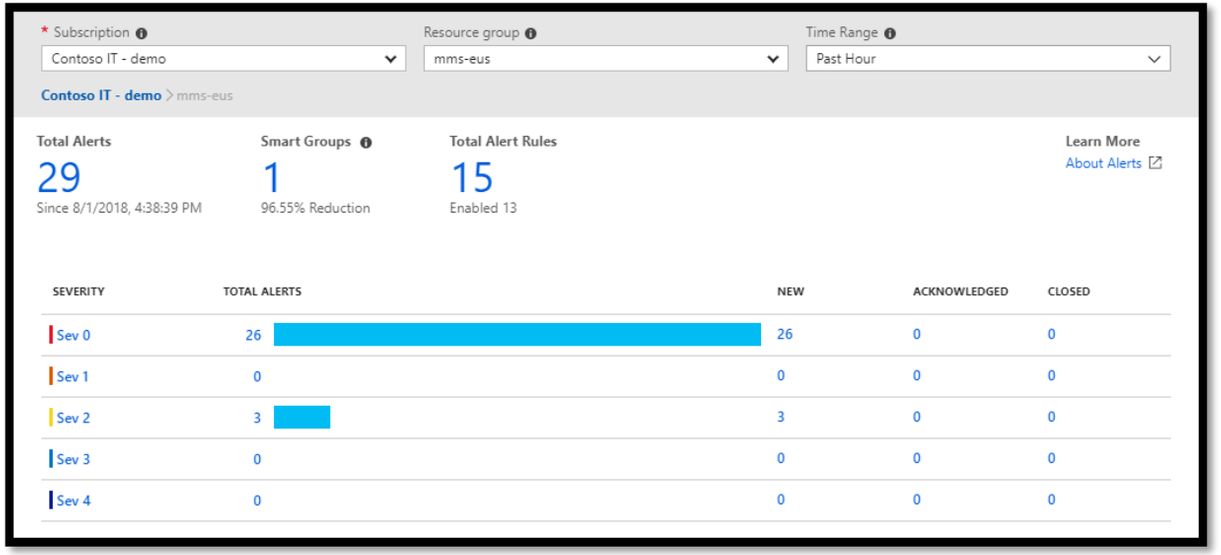
Source # https://docs.microsoft.com/en-us/azure/azure-monitor/logs/data-security#certifications-and-attestations



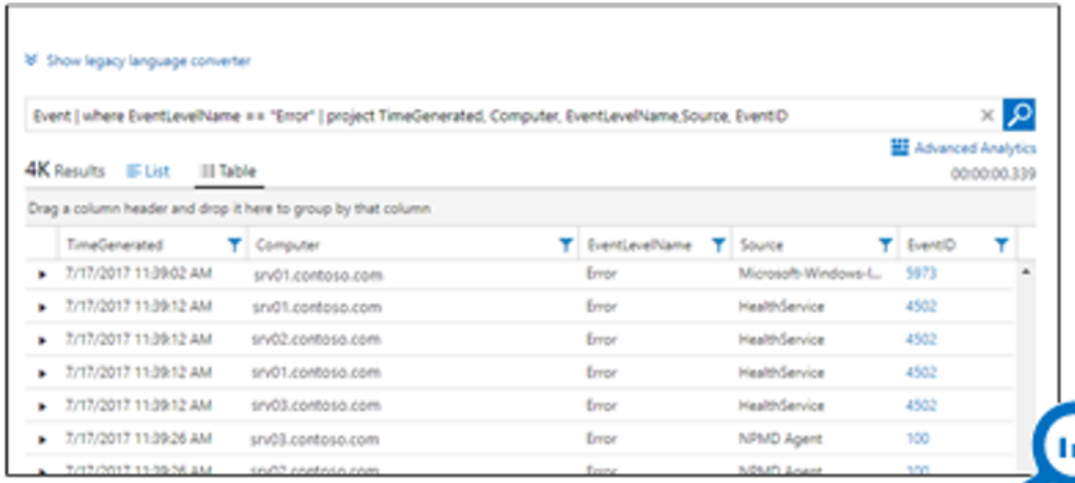

Azure Monitor
Application
Operating System
Azure Resources
Azure Subscription
Azure Tenant
Custom Sources
Metrics
Logs
Insights
Application
Container
VM
Monitoring Solutions
Visualize
Dashboards
Views
Power BI
Workbooks
Analyze
Metric Analytics
Log Analytics
Respond
Alerts
Autoscale
Integrate
Logic Apps
Export APIs

Alert

- **Metrics rules** – Real-time alerting on numeric values
- **Log rules** – Complex logic across data from multiple sources
- Email/SMS/Push/Voice

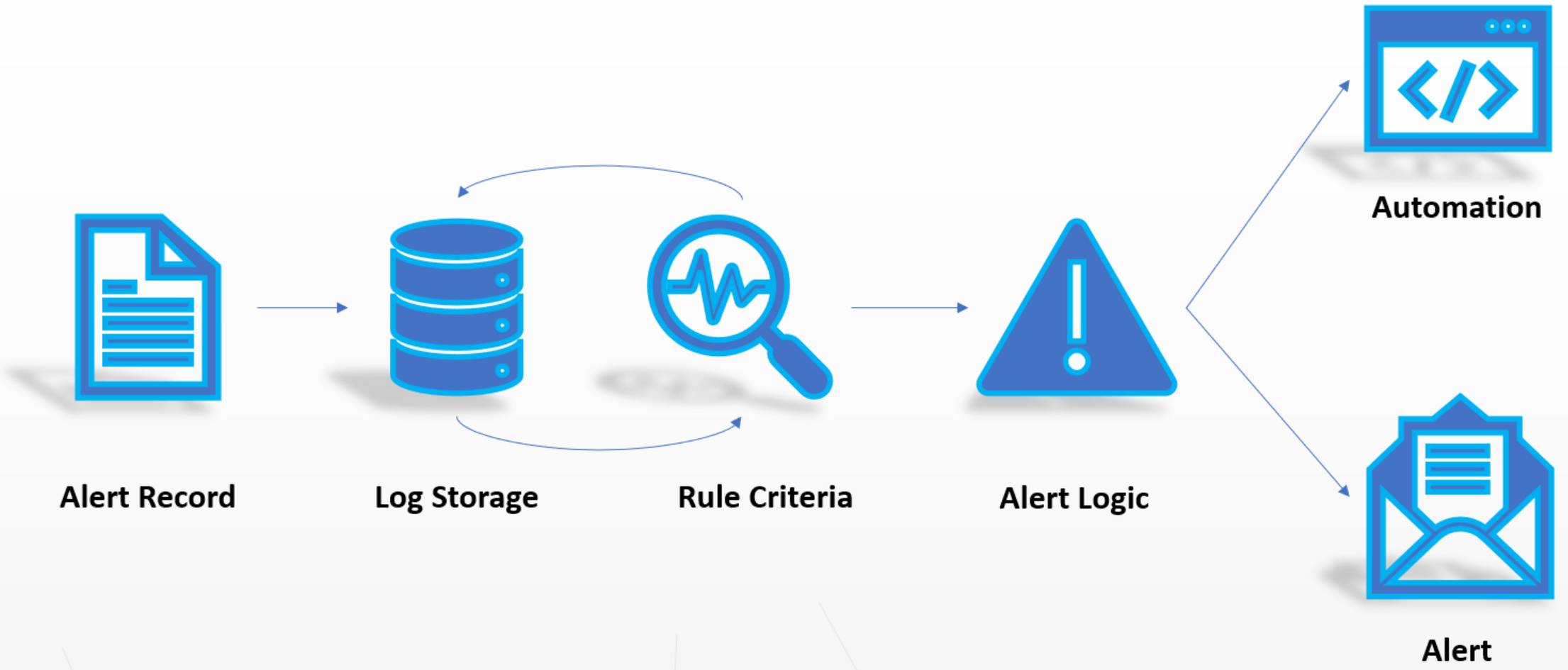


Metrics Explorer



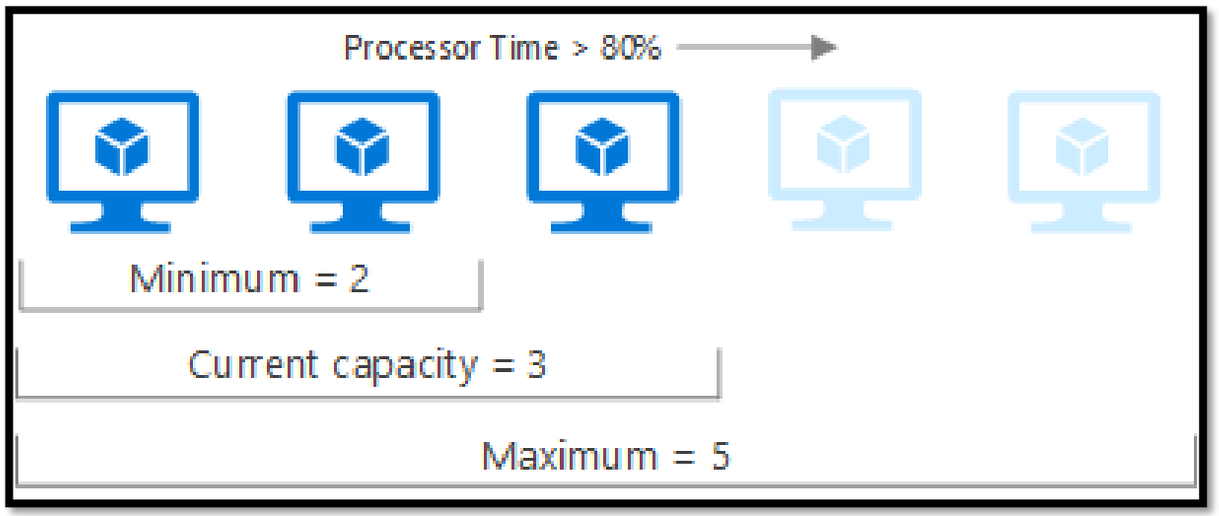
Log Analytics

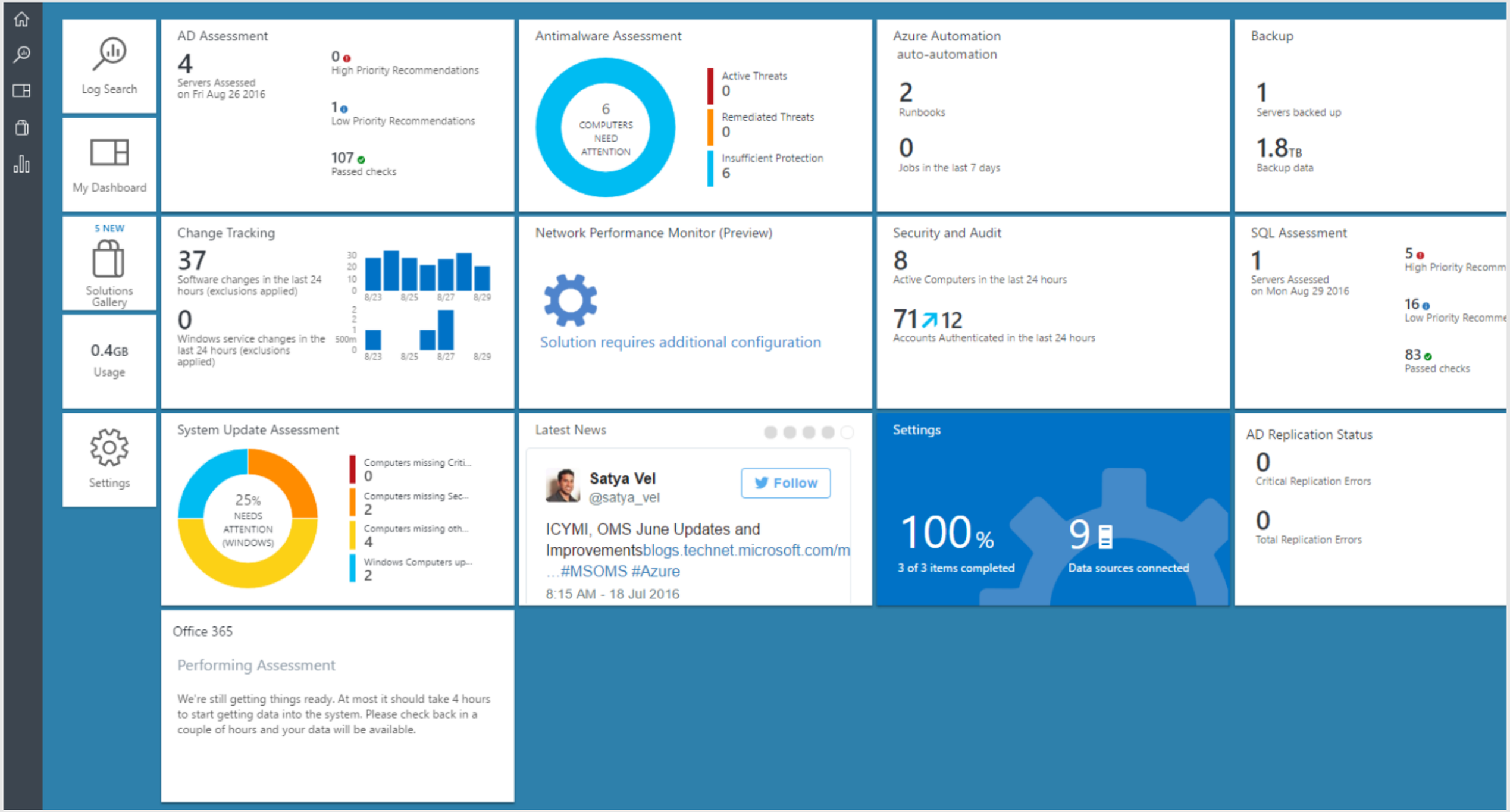
Metrics vs. Logs


Automation
Alert Record
Log Storage
Rule Criteria
Alert Logic
Alert

Automation

- Azure Functions
- Logic Apps
- Webhooks
- ITSM
- Automation Runbook




Log Search
My Dashboard
5 NEW
Solutions Gallery
0.4GB
Usage
Settings
AD Assessment
4
Servers Assessed
on Fri Aug 26 2016
0
High Priority Recommendations
1
Low Priority Recommendations
107
Passed checks
Antimalware Assessment
6
COMPUTERS NEED ATTENTION
Active Threats
0
Remediated Threats
0
Insufficient Protection
6
Azure Automation
auto-automation
2
Runbooks
0
Jobs in the last 7 days
Backup
1
Servers backed up
1.8TB
Backup data
Change Tracking
37
Software changes in the last 24 hours (exclusions applied)
0
Windows service changes in the last 24 hours (exclusions applied)
30
20
10
0
8/23
8/25
8/27
8/29
2
2
1
500m
0
8/23
8/25
8/27
8/29
Network Performance Monitor (Preview)
Solution requires additional configuration
Security and Audit
8
Active Computers in the last 24 hours
71 12
Accounts Authenticated in the last 24 hours
SQL Assessment
1
Servers Assessed
on Mon Aug 29 2016
5
High Priority Recomm
16
Low Priority Recomme
83
Passed checks
System Update Assessment
25%
NEEDS ATTENTION (WINDOWS)
Computers missing Criti...
0
Computers missing Sec...
2
Computers missing oth...
4
Windows Computers up...
2
Latest News
Satya Vel
@satya_vel
Follow
ICYMI, OMS June Updates and Improvementsblogs.technet.microsoft.com/m
...#MSOMS #Azure
8:15 AM - 18 Jul 2016
Settings
100%
3 of 3 items completed
9
Data sources connected
AD Replication Status
0
Critical Replication Errors
0
Total Replication Errors
Office 365
Performing Assessment
We're still getting things ready. At most it should take 4 hours to start getting data into the system. Please check back in a couple of hours and your data will be available.

Overview

Log Search

My Dashboard

Solutions Gallery

2.7GB
Servers and Usage

AD Assessment

4
Servers Assessed

3
High Priority Recommendations

6
Low Priority Recommendations

72
Passed Checks

Malware Assessment

1
Servers with Active Threats

38
Servers with Inadequate Protection

Capacity Planning

23.6 %
Available Cores

62.3 %
Available Memory

42.5 %
Available Storage

Backup

ITPRodBackup

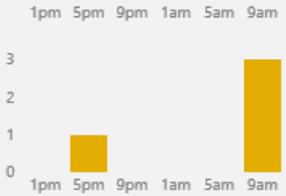
13
Servers backed up

3 TB
Backup data

Alert Management

0
Active critical alerts in the last 24 hours

4
Active warning alerts in the last 24 hours



Automation

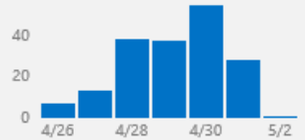
ITAutomation

9
Runbooks

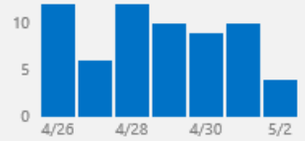
15
Jobs in the last 7 days

Change Tracking

20
Software changes in the last 24 hours



6
Windows service changes in the last 24 hours (excludes Status)

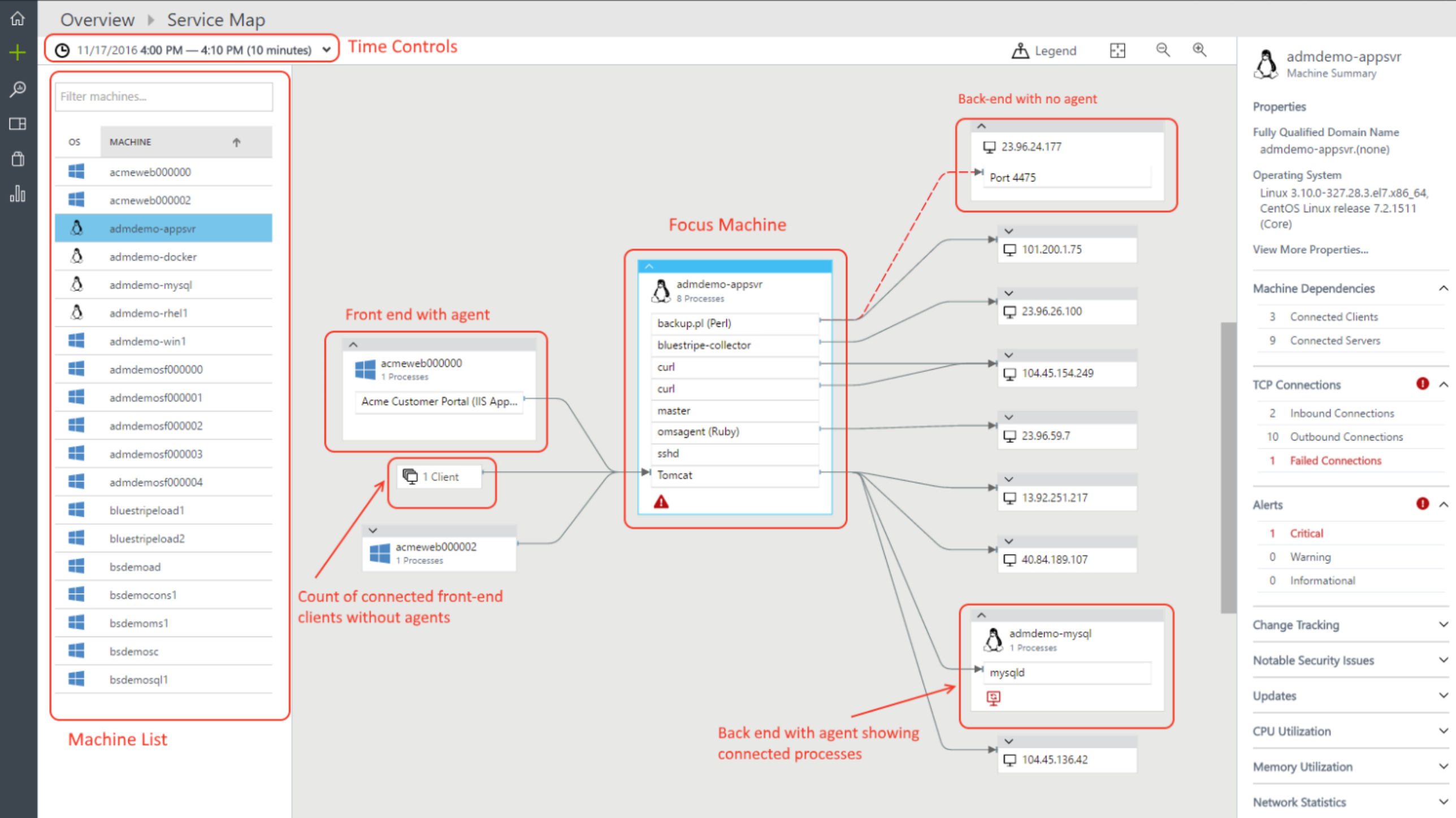


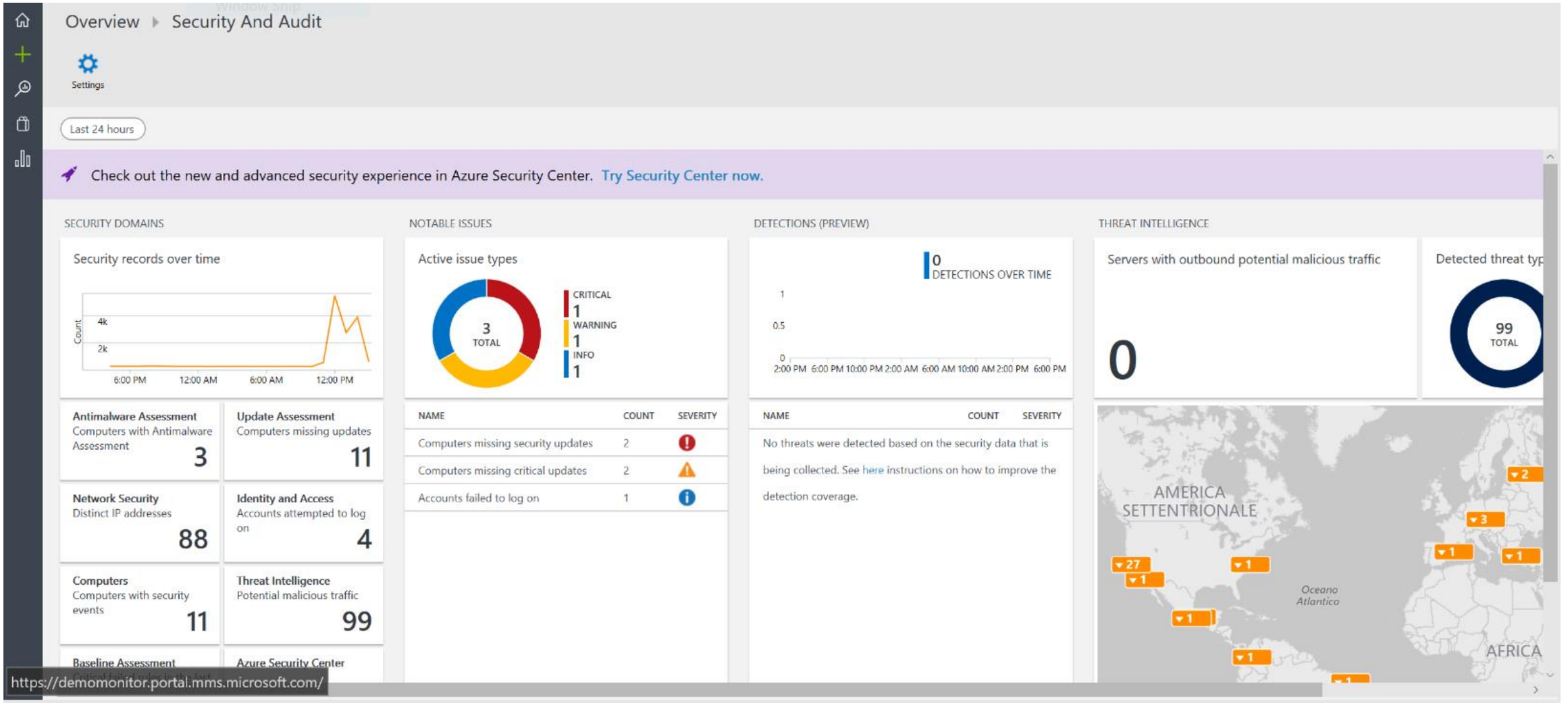
Security and Audit

95 ↘ 1
Active Computers in the last 24 hours

64 ↗ 1
Accounts Authenticated in the last 24 hours

Feedback


Overview
Service Map
11/17/2016 4:00 PM — 4:10 PM (10 minutes)
Time Controls
Legend
Filter machines...
OS
MACHINE
acmeweb000000
acmeweb000002
admdemo-appsvr
admdemo-docker
admdemo-mysql
admdemo-rhel1
admdemo-win1
admdemosf000000
admdemosf000001
admdemosf000002
admdemosf000003
admdemosf000004
bluestripeload1
bluestripeload2
bsdemoad
bsdemocons1
bsdemoms1
bsdemosc
bsdemosql1
Machine List
Back-end with no agent
23.96.24.177
Port 4475
Focus Machine
admdemo-appsvr
8 Processes
backup.pl (Perl)
bluestripe-collector
curl
curl
master
omsagent (Ruby)
sshd
Tomcat
101.200.1.75
23.96.26.100
104.45.154.249
23.96.59.7
13.92.251.217
40.84.189.107
Front end with agent
acmeweb000000
1 Processes
Acme Customer Portal (IIS App...
1 Client
acmeweb000002
1 Processes
Count of connected front-end clients without agents
admdemo-mysql
1 Processes
mysqld
Back end with agent showing connected processes
104.45.136.42
admdemo-appsvr
Machine Summary
Properties
Fully Qualified Domain Name
admdemo-appsvr.(none)
Operating System
Linux 3.10.0-327.28.3.el7.x86_64, CentOS Linux release 7.2.1511 (Core)
View More Properties...
Machine Dependencies
3 Connected Clients
9 Connected Servers
TCP Connections
2 Inbound Connections
10 Outbound Connections
1 Failed Connections
Alerts
1 Critical
0 Warning
0 Informational
Change Tracking
Notable Security Issues
Updates
CPU Utilization
Memory Utilization
Network Statistics


Overview ▸ Security And Audit
Settings
Last 24 hours
Check out the new and advanced security experience in Azure Security Center. Try Security Center now.
SECURITY DOMAINS
Security records over time
Count
4k
2k
6:00 PM
12:00 AM
6:00 AM
12:00 PM
Antimalware Assessment
Computers with Antimalware Assessment
3
Update Assessment
Computers missing updates
11
Network Security
Distinct IP addresses
88
Identity and Access
Accounts attempted to log on
4
Computers
Computers with security events
11
Threat Intelligence
Potential malicious traffic
99
Baseline Assessment
Azure Security Center
NOTABLE ISSUES
Active issue types
3
TOTAL
CRITICAL
1
WARNING
1
INFO
1
NAME
COUNT
SEVERITY
Computers missing security updates
2
Computers missing critical updates
2
Accounts failed to log on
1
DETECTIONS (PREVIEW)
0
DETECTIONS OVER TIME
1
0.5
0
2:00 PM
6:00 PM
10:00 PM
2:00 AM
6:00 AM
10:00 AM
2:00 PM
6:00 PM
NAME
COUNT
SEVERITY
No threats were detected based on the security data that is being collected. See here instructions on how to improve the detection coverage.
THREAT INTELLIGENCE
Servers with outbound potential malicious traffic
0
Detected threat typ
99
TOTAL
AMERICA SETTENTRIONALE
Oceano Atlantico
AFRICA
2
3
1
1
27
1
1
1
1
https://demomonitor.portal.mms.microsoft.com/

Overview ▸ Update Management

ASSESSED COMPUTERS

Windows Computers

NEED CRITICAL UPDATES 2
NEED SECURITY UPDATES 0
NEED OTHER UPDATES 1
UP TO DATE 0

COMPUTER	CRITICAL	SECURITY	OTHER
monitorwinvm	1	1	3
monitorwinvm2	1	1	2
mediaproxy	0	0	2

Linux Computers

NEED CRITICAL UPDATES 2
NEED SECURITY UPDATES 1
NEED OTHER UPDATES 5
UP TO DATE 0

COMPUTER	CRITICAL	SECURITY	OTHER
monitorlinuxvm2	6	21	303
giuliocentos	4	12	240
monitorlinuxvm1	0	3	135
aks-agentpool-12019904-0	0	0	57
aks-agentpool-12019904-1	0	0	57
aks-agentpool-12019904-2	0	0	57
aks-agentpool-50015563-0	0	0	25
aks-agentpool-50015563-1	0	0	25

MISSING UPDATES

Windows Updates

CRITICAL UPDATES 1
SECURITY UPDATES 1
OTHER UPDATES 5

CLASSIFICATION	NUMBER OF UPDATES
Critical Updates	1
Security Updates	1
Definition Updates	3
Update Rollups	1
Updates	1

Linux Updates

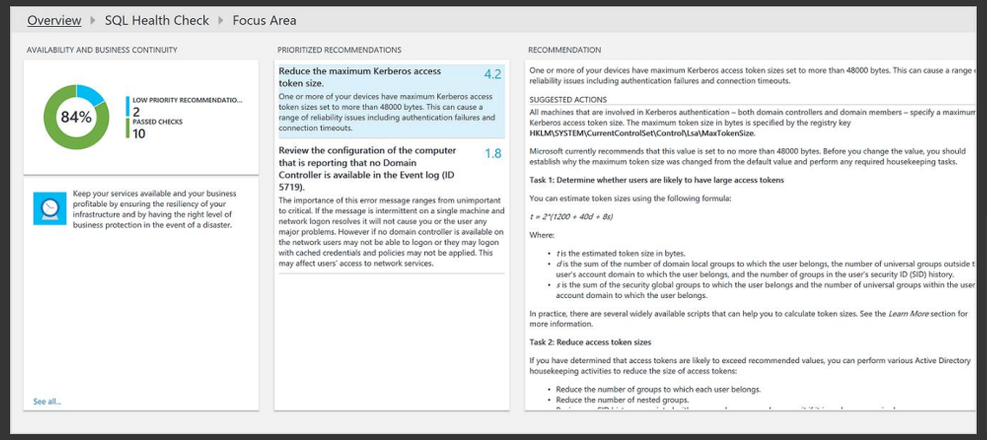
CRITICAL UPDATES 6
SECURITY UPDATES 24
OTHER UPDATES 442

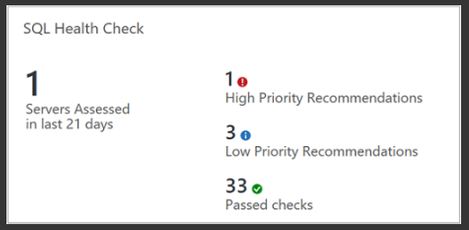
CLASSIFICATION	NUMBER OF UPDATES
Critical Updates	6
Security Updates	24
Others	442

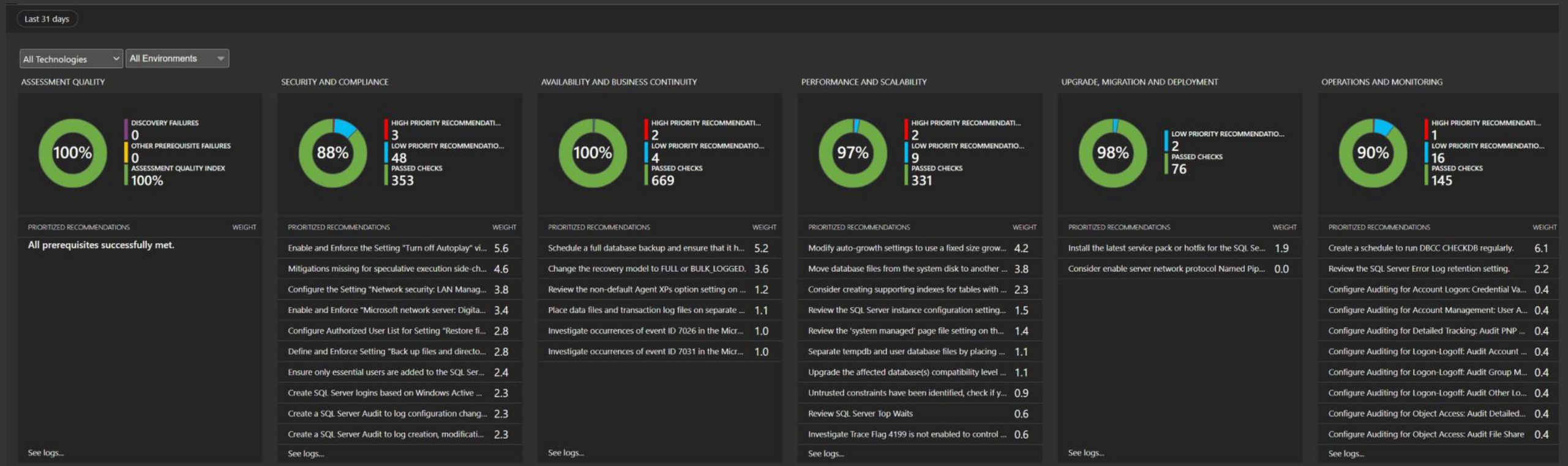
UPDATE DEPLOYMENT

MANAGE UPI

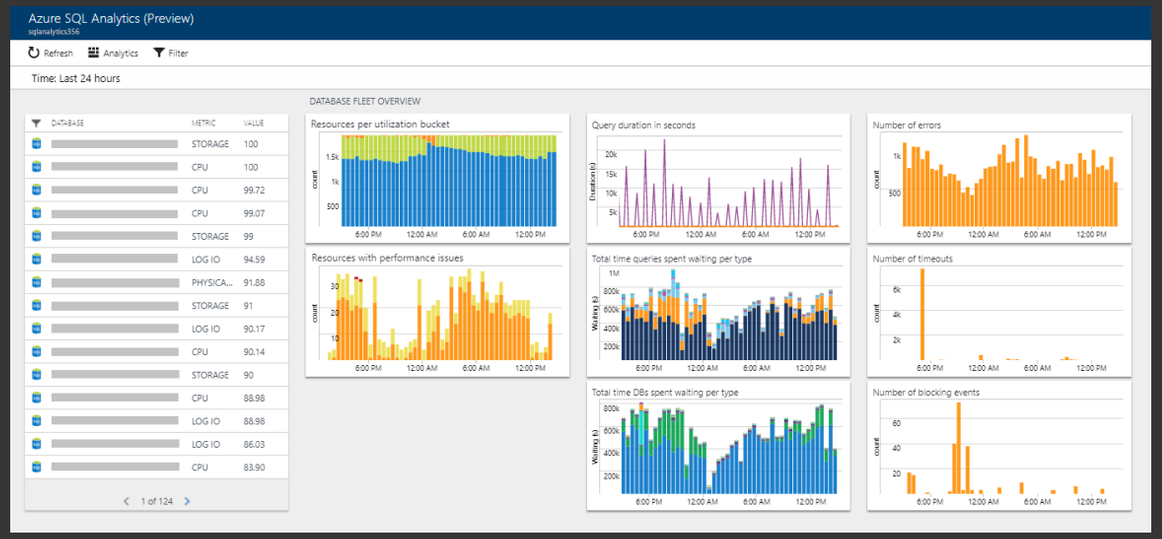
SQL Server Monitoring

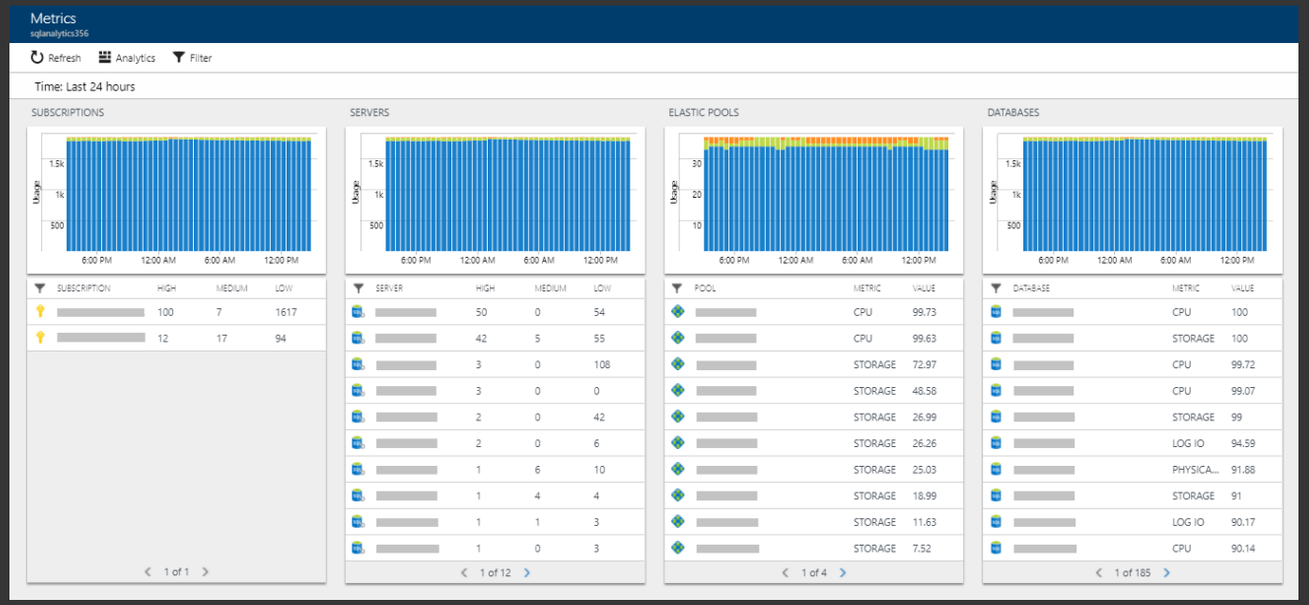




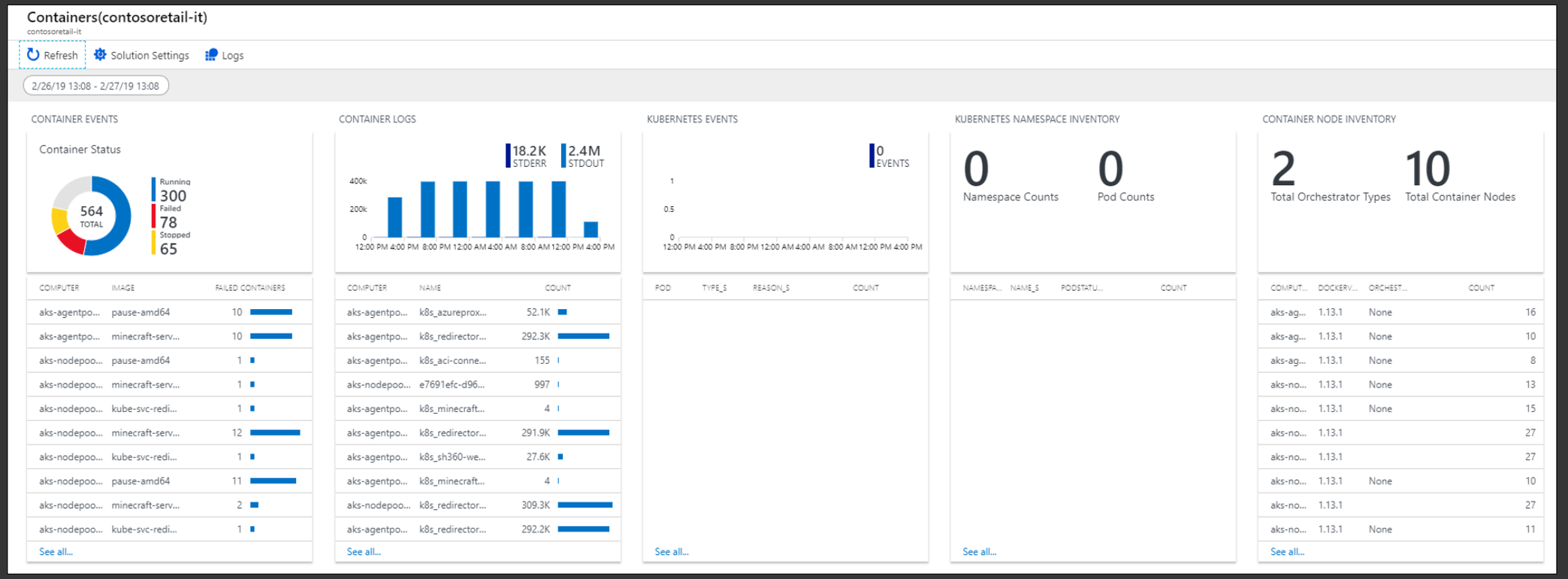


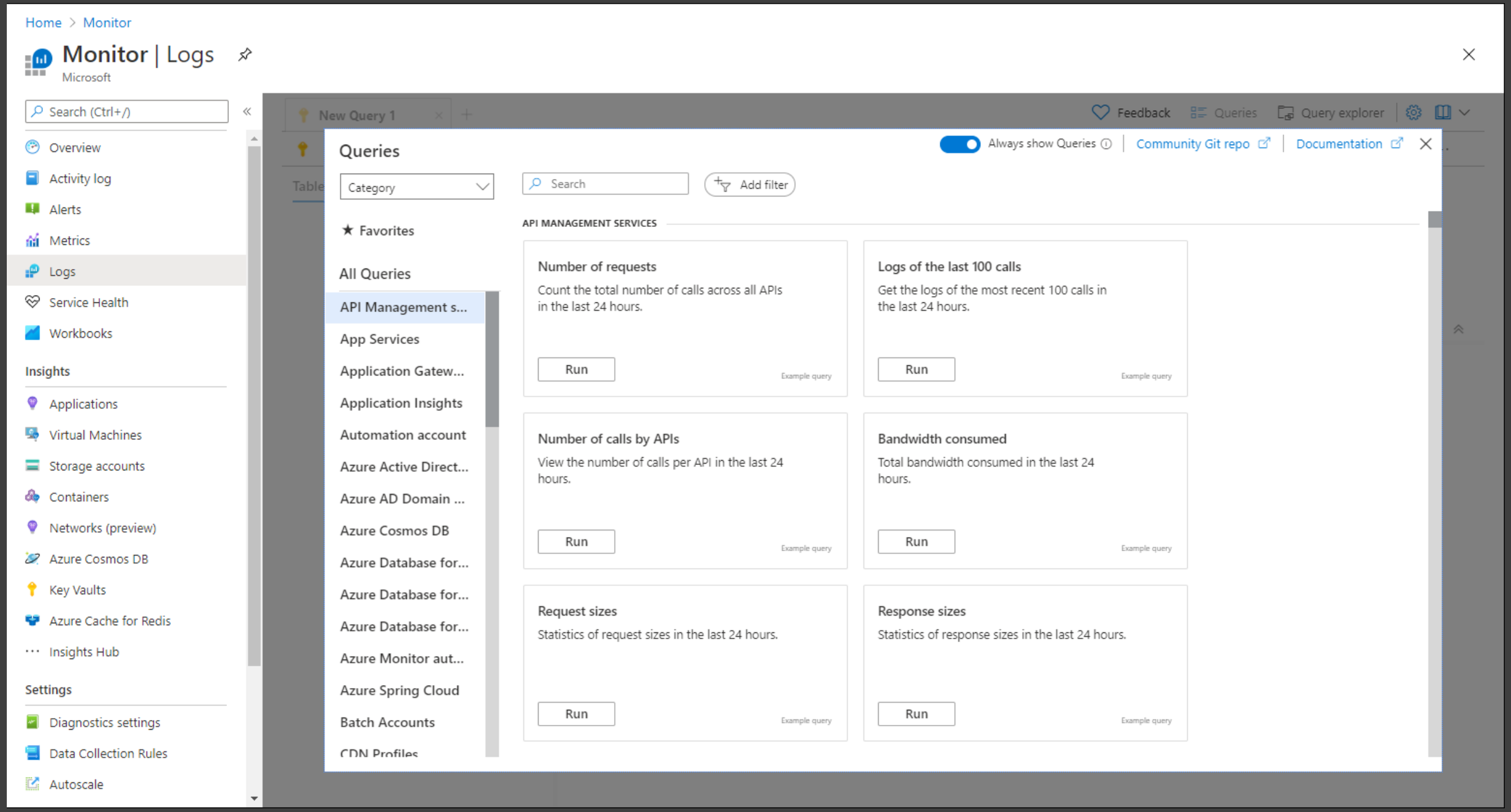
Azure SQL Monitoring





Dockers and Containers




Home > Monitor
Monitor | Logs
Microsoft
Search (Ctrl+/)
Overview
Activity log
Alerts
Metrics
Logs
Service Health
Workbooks
Insights
Applications
Virtual Machines
Storage accounts
Containers
Networks (preview)
Azure Cosmos DB
Key Vaults
Azure Cache for Redis
Insights Hub
Settings
Diagnostics settings
Data Collection Rules
Autoscale
New Query 1
Feedback
Queries
Query explorer
Queries
Always show Queries
Community Git repo
Documentation
Category
Search
Add filter
★ Favorites
All Queries
API Management s...
App Services
Application Gatew...
Application Insights
Automation account
Azure Active Direct...
Azure AD Domain ...
Azure Cosmos DB
Azure Database for...
Azure Database for...
Azure Database for...
Azure Monitor aut...
Azure Spring Cloud
Batch Accounts
CDN Profiles
API MANAGEMENT SERVICES
Number of requests
Count the total number of calls across all APIs in the last 24 hours.
Run
Example query
Logs of the last 100 calls
Get the logs of the most recent 100 calls in the last 24 hours.
Run
Example query
Number of calls by APIs
View the number of calls per API in the last 24 hours.
Run
Example query
Bandwidth consumed
Total bandwidth consumed in the last 24 hours.
Run
Example query
Request sizes
Statistics of request sizes in the last 24 hours.
Run
Example query
Response sizes
Statistics of response sizes in the last 24 hours.
Run
Example query

IT Service Management Connector

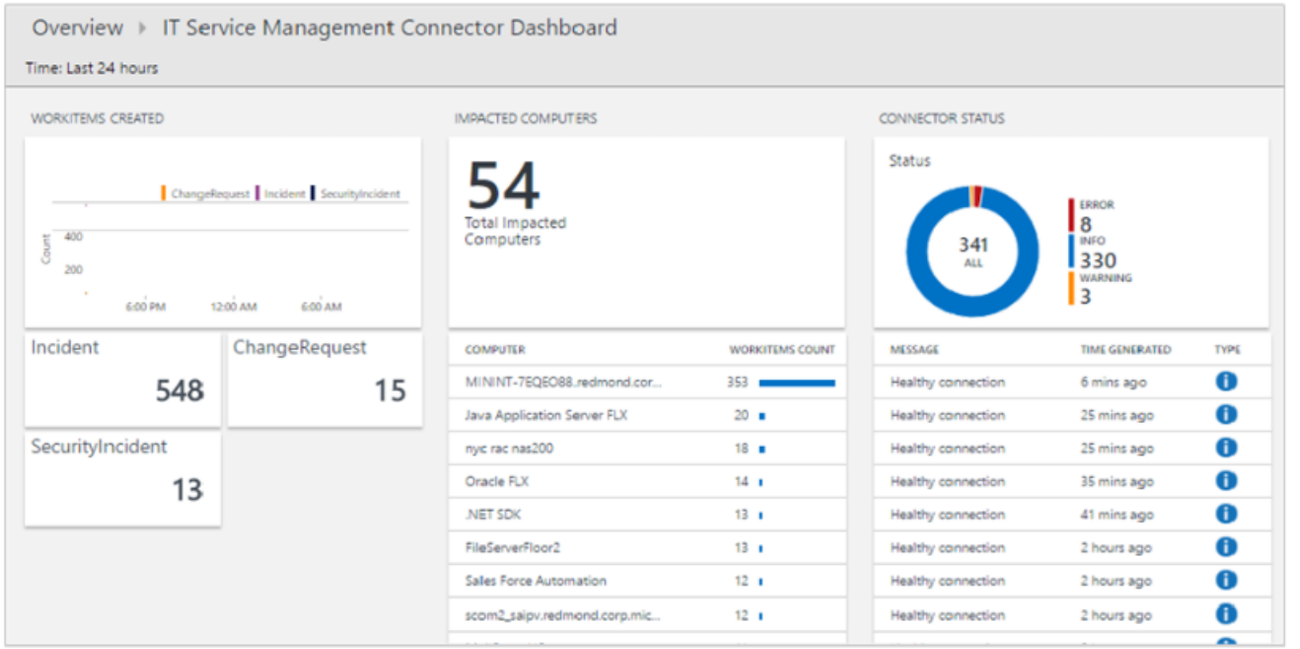
- The IT Service Management Connector integrates your **existing IT Service Management (ITSM) products** and services with OMS Log Analytics.

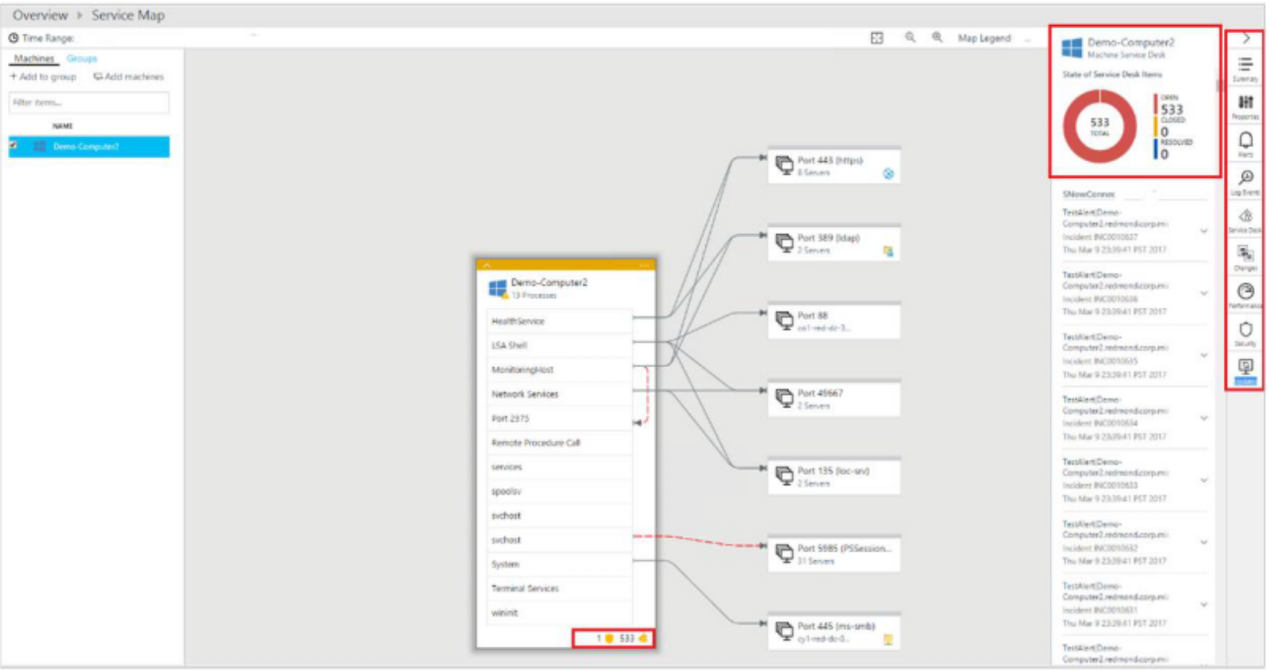
- The solution has **bidirectional integration** with ITSM products/services:
  - it provides the OMS users an option to create incidents, alerts, or events in ITSM solution.
  - it imports data such as incidents, and change requests from ITSM solution into OMS Log Analytics.

- Supported ITSM products:
  - **System Center Service Manager** (SCSM)
  - **ServiceNow**
  - **Provance**
  - **Cherwell**

servicenow PROVANCE Cherwell Microsoft® System Center Service Manager

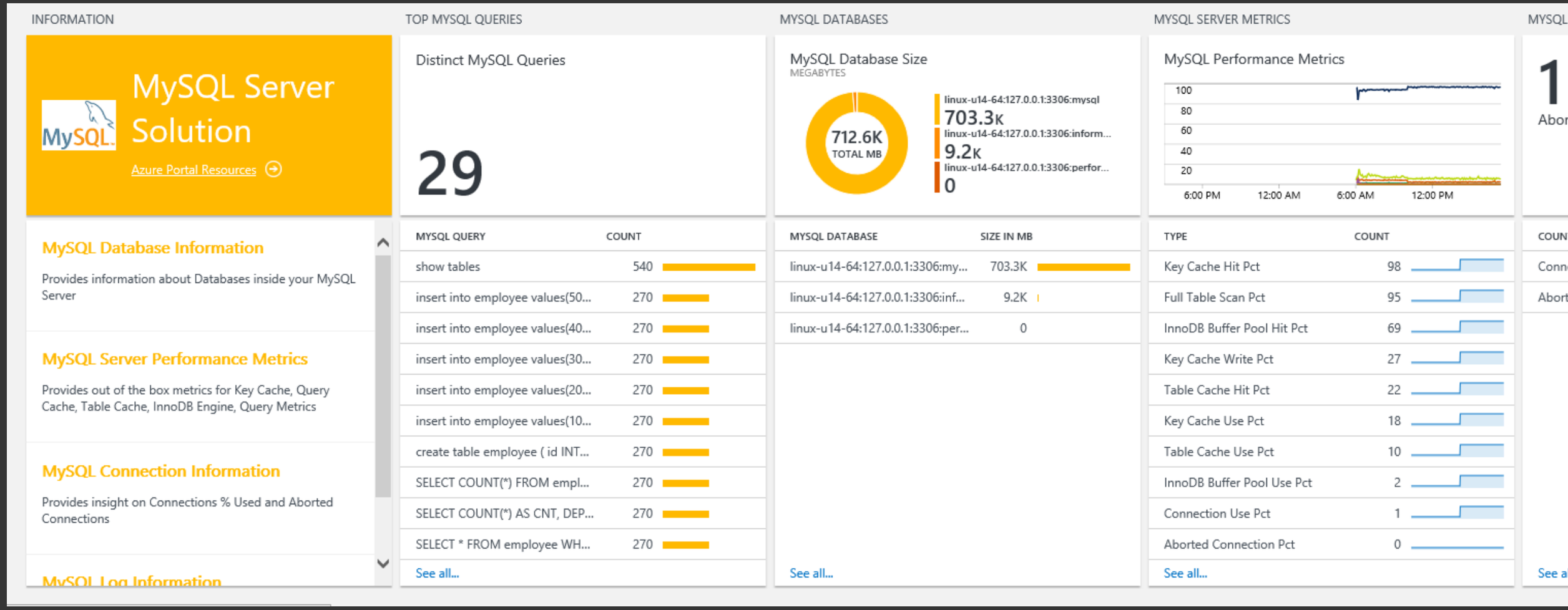
Integrate ITSM with other OMS solutions





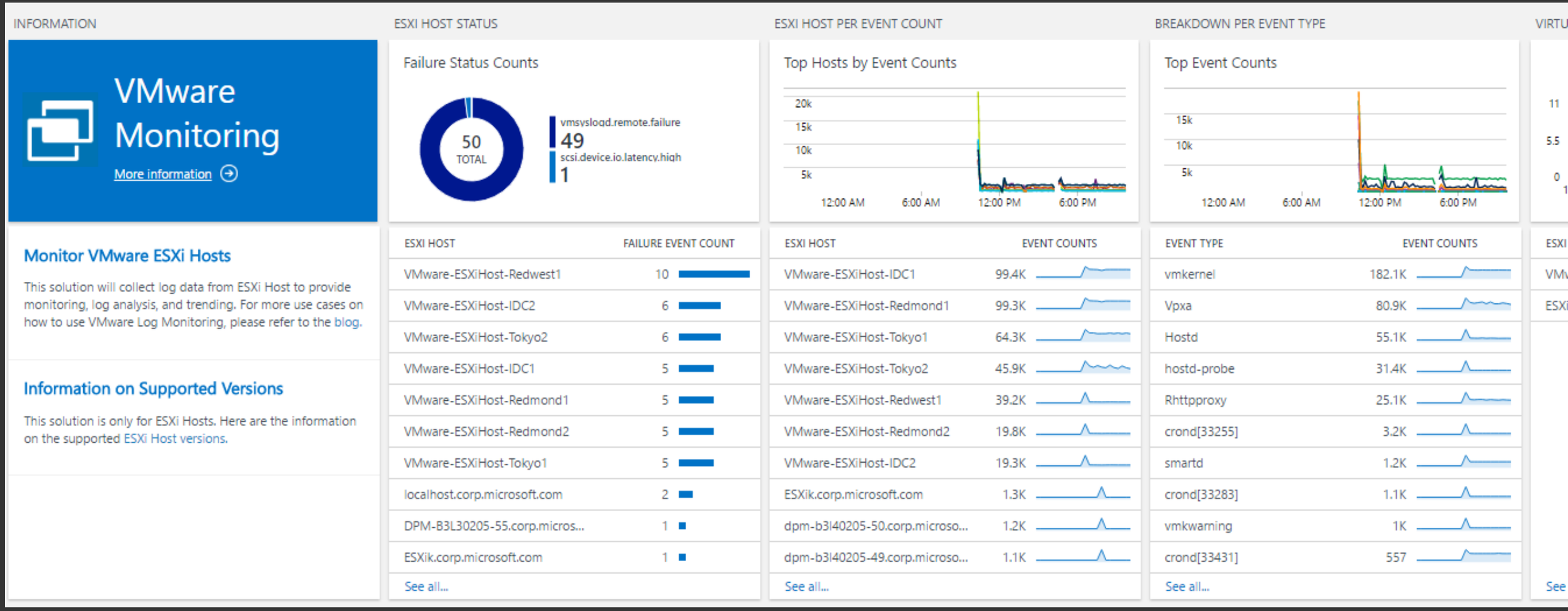
MySQL Server Monitoring

Microsoft



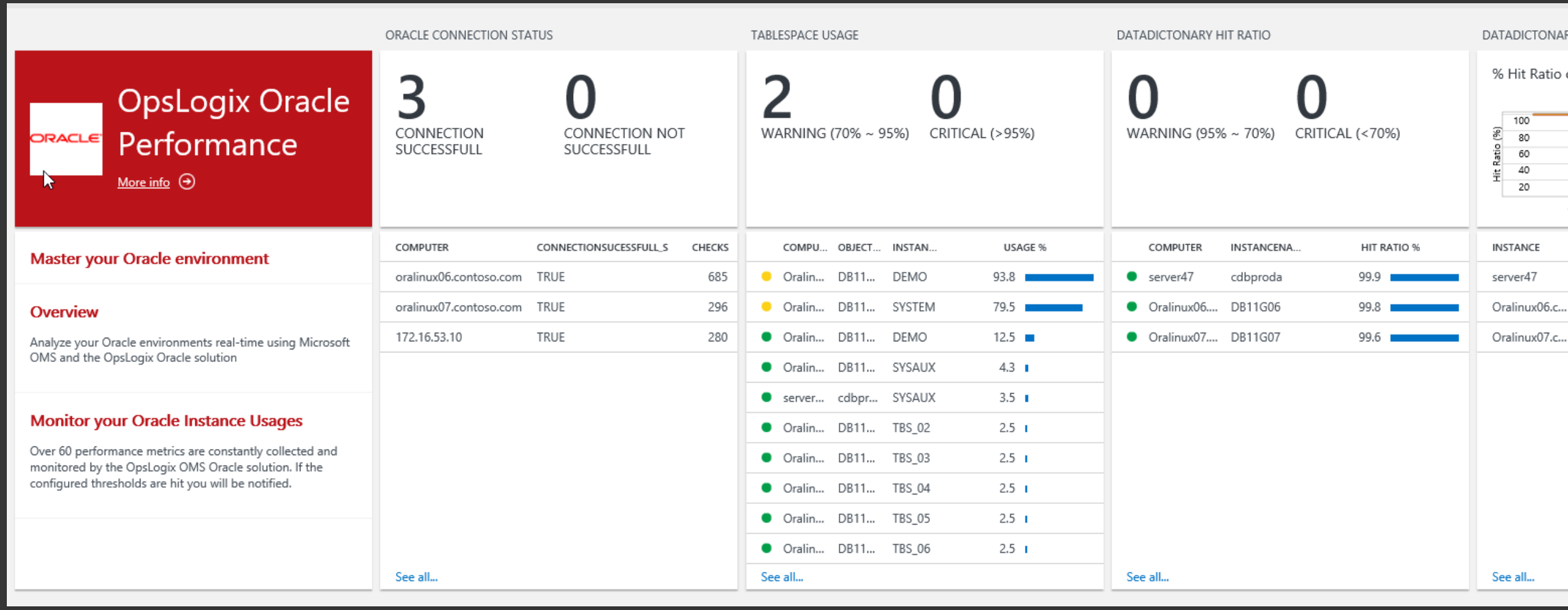
VMware Monitoring

Microsoft



Oracle Performance

(ops) logix



Oracle Auditing

(ops) logix

OpsLogix Oracle Auditing

More info

Master your Oracle environment

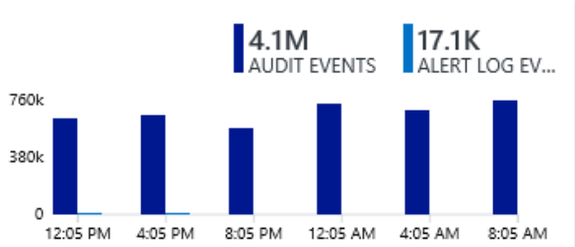
Overview

Analyze your Oracle environments real-time using Microsoft OMS and the OpsLogix Oracle monitoring solution

Oracle Auditing

Get grip on what's happening within your Oracle databases. This Solution will collect activity so you can see any time any action. This is ideal for ISO or SOX compliancy auditing.

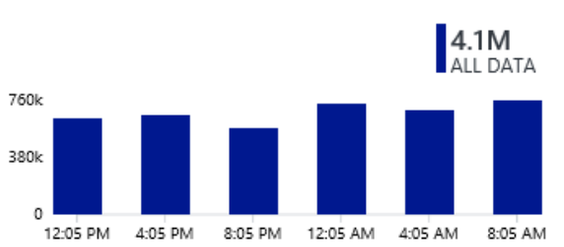
TOTAL AUDIT EVENTS DISTRIBUTION BY ORACLE INSTANCES



ORACLE INSTA...	INSTANCE_NAM...	COUNT
Oralinux07.c...	DB11G07	3M
Oralinux06.c...	DB11G06	1M
server47	cdbproda	2.2K

See all...

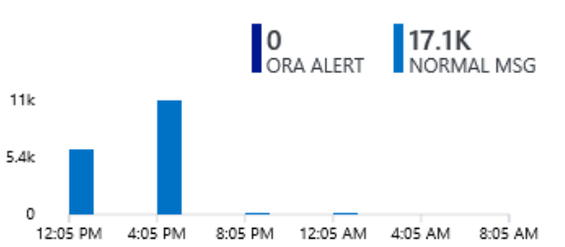
TOTAL ORACLE AUDIT EVENTS BY ORACLE INSTANCE



INSTANCE	INSTANCE_NAM...	COUNT
Oralinux07.c...	DB11G07	3M
Oralinux06.c...	DB11G06	1M
server47	cdbproda	2.2K

See all...

TOTAL ORACLE ALERT LOG EVENTS BY ALERT ID



ORA NU...	INSTANC...	ORAMSG...	COUNT
server47	cdbproda	0	16.9K
Oralinu...	DB11G07	0	149
Oralinu...	DB11G06	0	81

See all...

TOP FAILE

0

Failed L

USER N...
server47

See all...

Nutanix Monitoring

COMTRADE

COMTRADE SOFTWARE

Nutanix Enterprise Clouds

More info

Overview

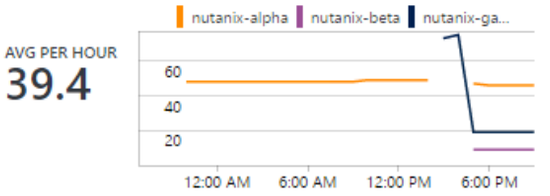
Nutanix Enterprise Clouds solution from Comtrade Software provides you monitoring and log analytics for Nutanix Enterprise Clouds

COMTRADE SOFTWARE

RUNNING VMS PER CLUSTER

Total Running VMS over time

VM STATUS IS ON



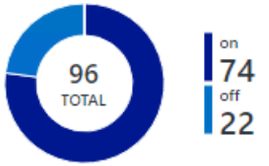
CLUSTER NAME	# VMS
nutanix-alpha	46
nutanix-gamma	19
nutanix-beta	9

See all...

TOTAL VMS PER CLUSTER

Total VMS

ALL CLUSTERS

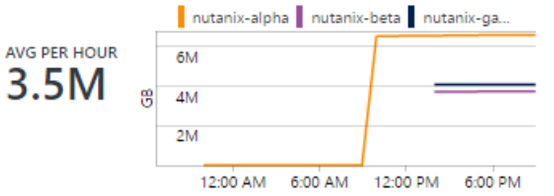


CLUSTER NAME	# VMS
nutanix-alpha	57
nutanix-gamma	27
nutanix-beta	12

See all...

MEMORY SIZE AND USAGE

Memory usage over time



CLUSTER NAME	TOTAL ME...
nutanix-alpha	7.2
nutanix-gamma	6.1
nutanix-beta	4.3

See all...

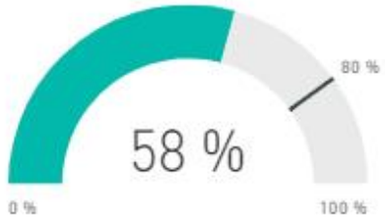
IT Operations

Resource usage and availability

Server
- DBServer-1
- DBServer-2
- DBServer-3
- DBServer-4
- WebApp-1
- WebApp-2
- WebApp-3
- WebApp-4
- WebApp-5

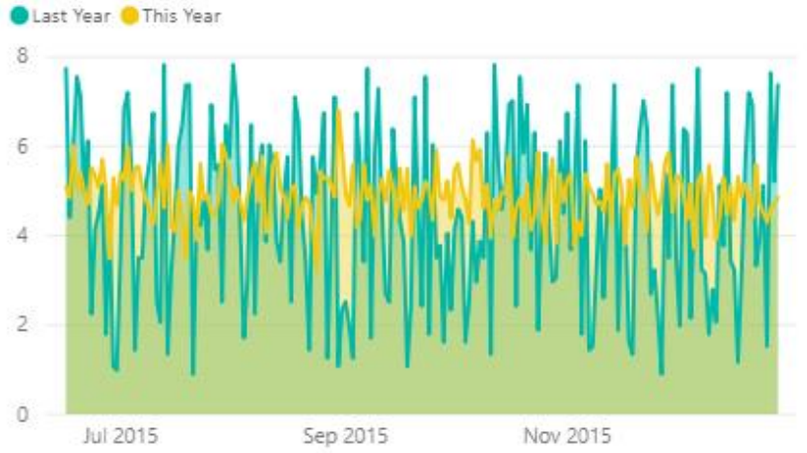
CPU utilization

Memory utilization



Disk utilization

CPU utilization by year



Total DBs

275

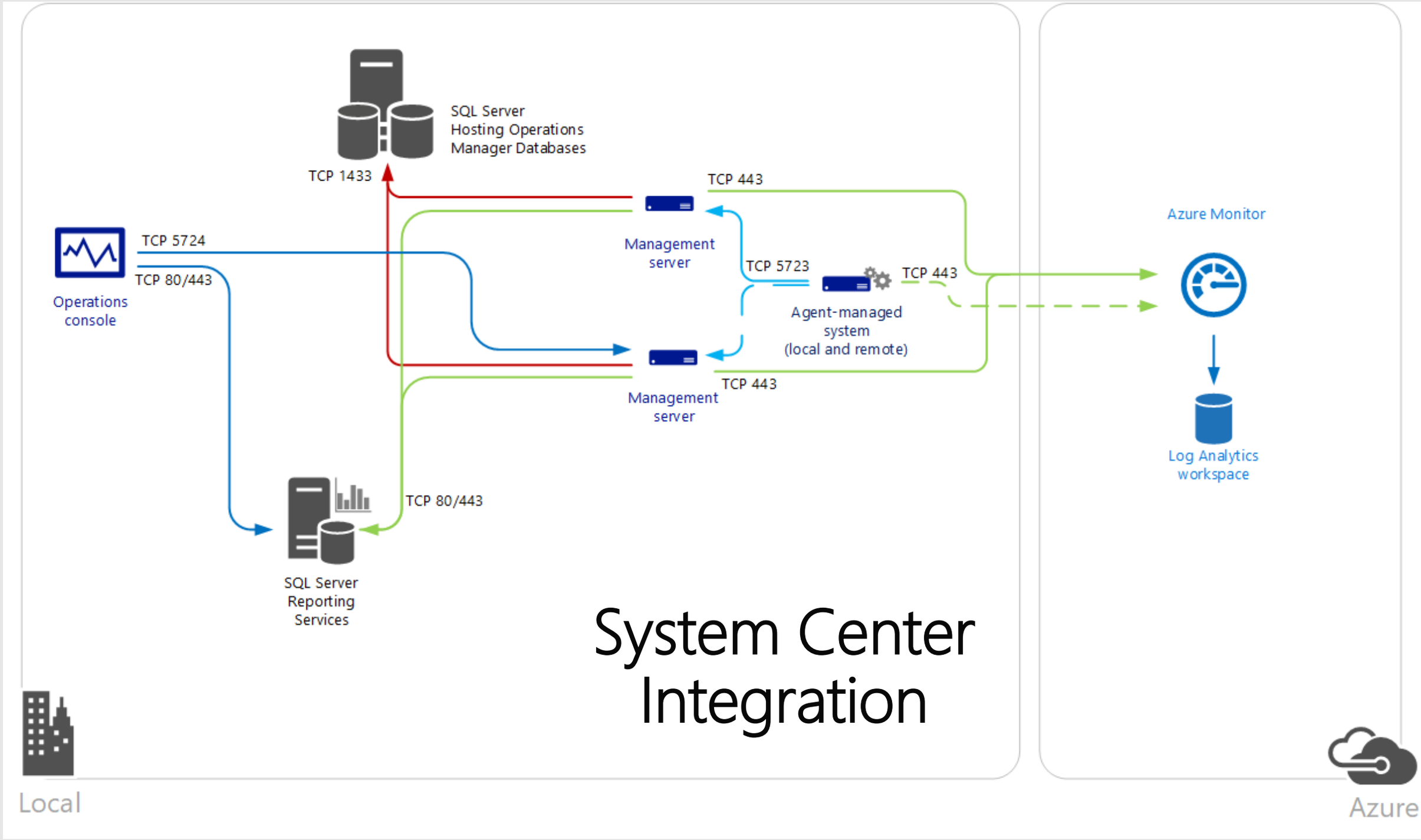
Database Backups

271	3	346782
Backups Run	Backups Failed	Backup Size (GB)

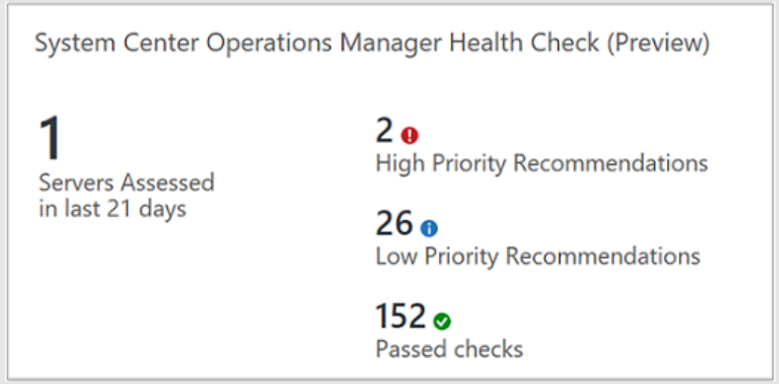
Usage Type
- Data Activity
- Data Size
- User Conne...

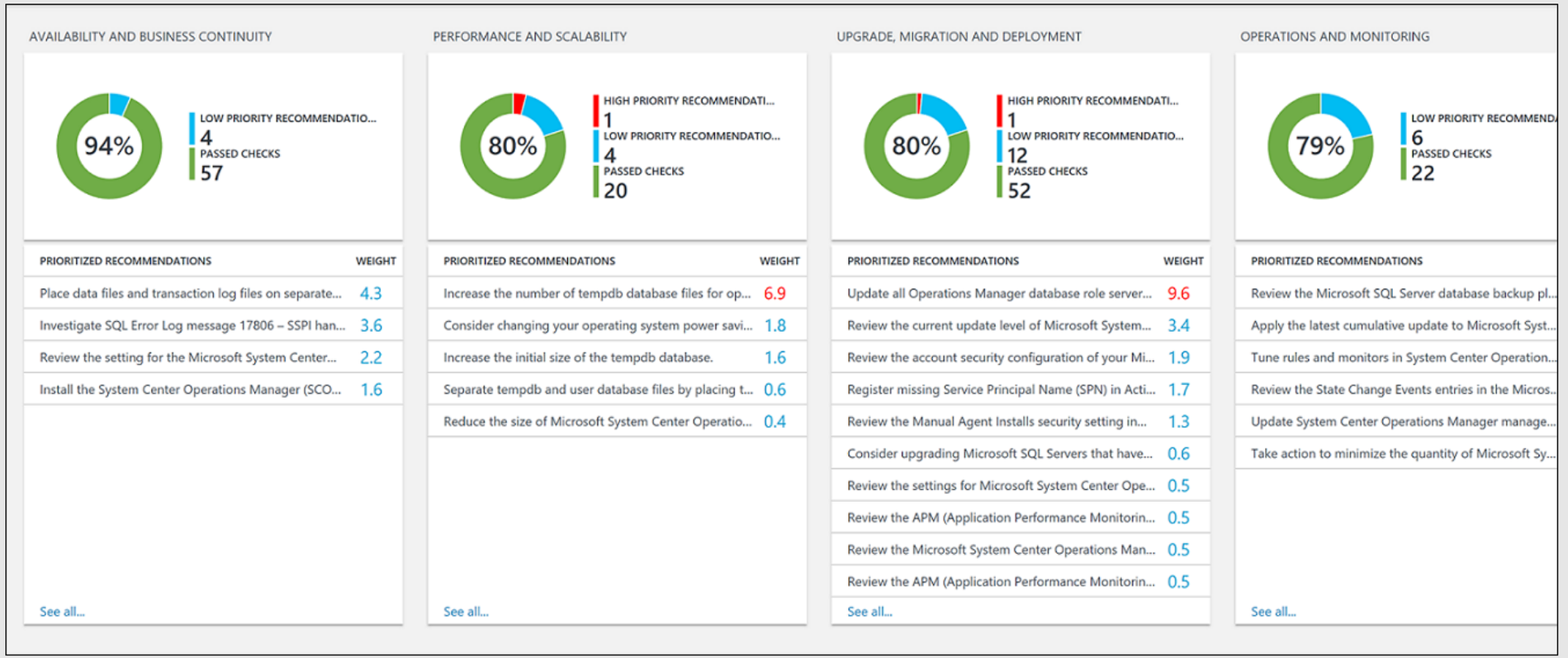
Usage by type and region

Network usage by location


SQL Server
Hosting Operations
Manager Databases
TCP 1433
TCP 443
Management
server
TCP 5724
TCP 80/443
Operations
console
TCP 5723
TCP 443
Agent-managed
system
(local and remote)
Azure Monitor
TCP 443
Management
server
Log Analytics
workspace
TCP 80/443
SQL Server
Reporting
Services
System Center
Integration
Local
Azure

System Center Assessment





Azure Monitor Pricing

Log Data Ingestion

Log Analytics and **Application Insights** charge for data they ingest. There are two ways to pay for ingesting data: Pay-As-You-Go and Commitment Tiers. The Pay-As-You-Go pricing offers flexible pay-for-what-you-use pricing by simply charging for the volume of data ingested. With Commitment Tiers you are billed a fixed predictable fee starting at a 100 GB per day level. Data ingested above the Commitment Tier is billed at the same per-GB price as the current tier. Commitment Tiers provide you a discount on data ingestion based on your selected commitment tier. Commitment tiers have a 31-day commitment period (learn more). For Application Insights users, your resource must be workspace-based to leverage the Commitment Tiers. Some data types, including Azure Activity Logs, are free from data ingestion charges.

Pricing Tier	Price	Effective Per GB Price[1]	Savings Over Pay-As-You-Go
Pay-As-You-Go	**$2.76** per GB (5 GB per billing account per month included)	**$2.76** per GB	N/A
100 GB per day	**$235.20** per day	**$2.36** per GB	15%
200 GB per day	**$441.60** per day	**$2.21** per GB	20%
300 GB per day	**$648** per day	**$2.16** per GB	22%
400 GB per day	**$844.80** per day	**$2.12** per GB	23%
500 GB per day	**$1,038** per day	**$2.08** per GB	25%
1,000 GB per day	**$2,040** per day	**$2.04** per GB	26%
2,000 GB per day	**$3,984** per day	**$2.00** per GB	28%

Log Data Retention

Data ingested into your **Log Analytics** workspace can be retained at no charge for up to first 31 days (or 90 days if Azure Sentinel is enabled on the workspace). Data ingested into either classic or workspace-based **Application Insights** is retained for 90 days without any charge.

Data retained beyond these no-charge periods will be charged for each GB of data retained for a month (pro-rated daily).

Feature	Days of Included Retention	Price
Data Retention	31 days (or 90 days if Sentinel is enabled), and 90 days for Application Insights data	**$0.12** per GB per month

Log Data Export

Log Analytics Data Export offers continuous streaming export of logs from your Log Analytics workspace to destinations such as Azure Storage and Event Hub. You are billed per GB of data exported from the Log Analytics Workspace. Exporting data via Diagnostic Settings is covered below in the Platform Logs section of this page.

Billing for the Log Analytics Data Export feature is not yet enabled. Advance notice will be provided before billing starts.

Feature	Price
Log Analytics Data Export	**$0.12** per GB[1]

[1]The size of data exported by Log Analytics Data Export is the number of bytes in the exported JSON formatted data. 1 GB = 10^9 bytes.

Web Tests

Application Insights has URL Ping tests and Multi-step web tests which enable you to verify the availability of your application.

Feature	Price

Notifications

Notifications are sent based on when an Alert rule triggers. You are billed based on the type and number of notifications you choose to send.

Feature	Free units included	Price
ITSM connector create or update event	1,000 events per month	$5/1,000 events
Emails	1,000 emails per month	$2/100,000 emails
Push notification (to Azure Mobile App)	1,000 notifications per month	$2/100,000 notifications
Secure web hooks	1 secure web hook	$6/1,000,000 secure web hooks
Web hooks	100,000 web hooks per month	$0.60/1,000,000 web hooks

We Look Forward to Partnering With You…

A Cloud 9, Mohamed Naguib Axis,
North Investors Area, New Cairo, Egypt.

P +2 02 25 390 467

E info@inovasys.co