



Log Analytics Overview

Maxim Sergeev

Sr. Premier Field Engineer



Azure Monitor for VMs - Preview



Challenges in VM Monitoring



Hard to...

- Figure out what and how to Monitor
- Disambiguate the issues in the VM, caused due to its usage or Azure itself
- Troubleshoot how guest-level resource constraints impacts workloads/apps
- Identify VM hotspots at scale based on resource utilization
- Determine whether how back-end dependencies are affecting clients
- Determine health and availability of Azure VMs across Resource Groups

"The scenario I am imagining is in an Ops room, with a large screen, where we can see at a glance on multiple graphs how all VM's are performing in terms of CPU, Mem, Disk, Network etc.?"

"We had a process that was putting everything at a standstill – we had high latency due to a poorly scheduled process that was taking up bandwidth. Show me all the processes running on the servers, and show how much they're trying to transmit."

"It's too difficult to wire together all the diagnostics for memory. I can always RDP into boxes, but I want to see it automatically."

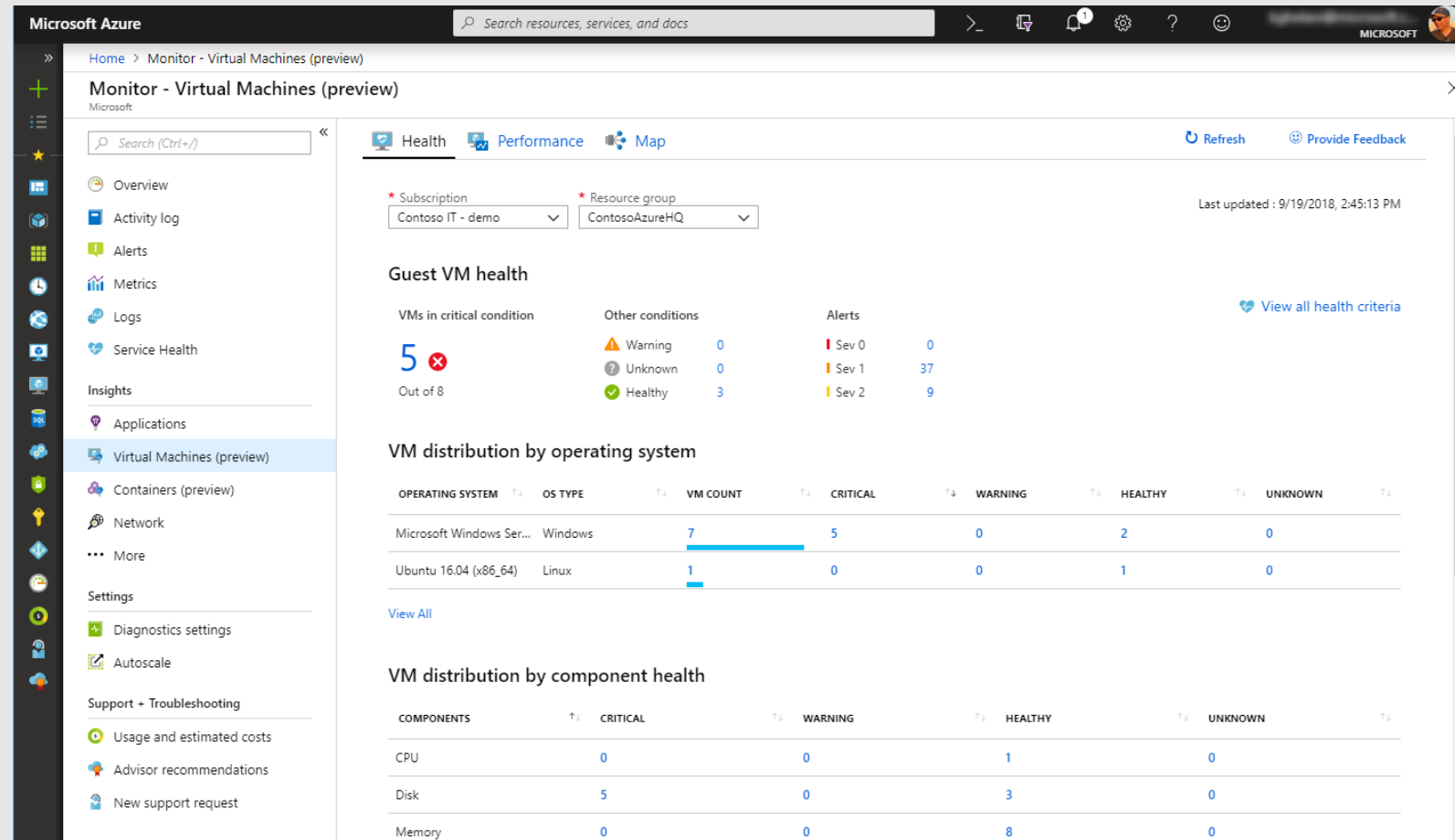
"I need to know how VMs from my customers communicate."

Azure Monitor for VMs



Health Diagnostics

- ➔ Pre-defined health monitors to jump-start VM monitoring
- ➔ Near real-time monitoring of core VM components (CPU, Memory,..)
- ➔ Health diagnostics, that helps to localize the issue fast
- ➔ KB articles on common causes and resolution
- ➔ Customizable alerting thresholds on health monitors

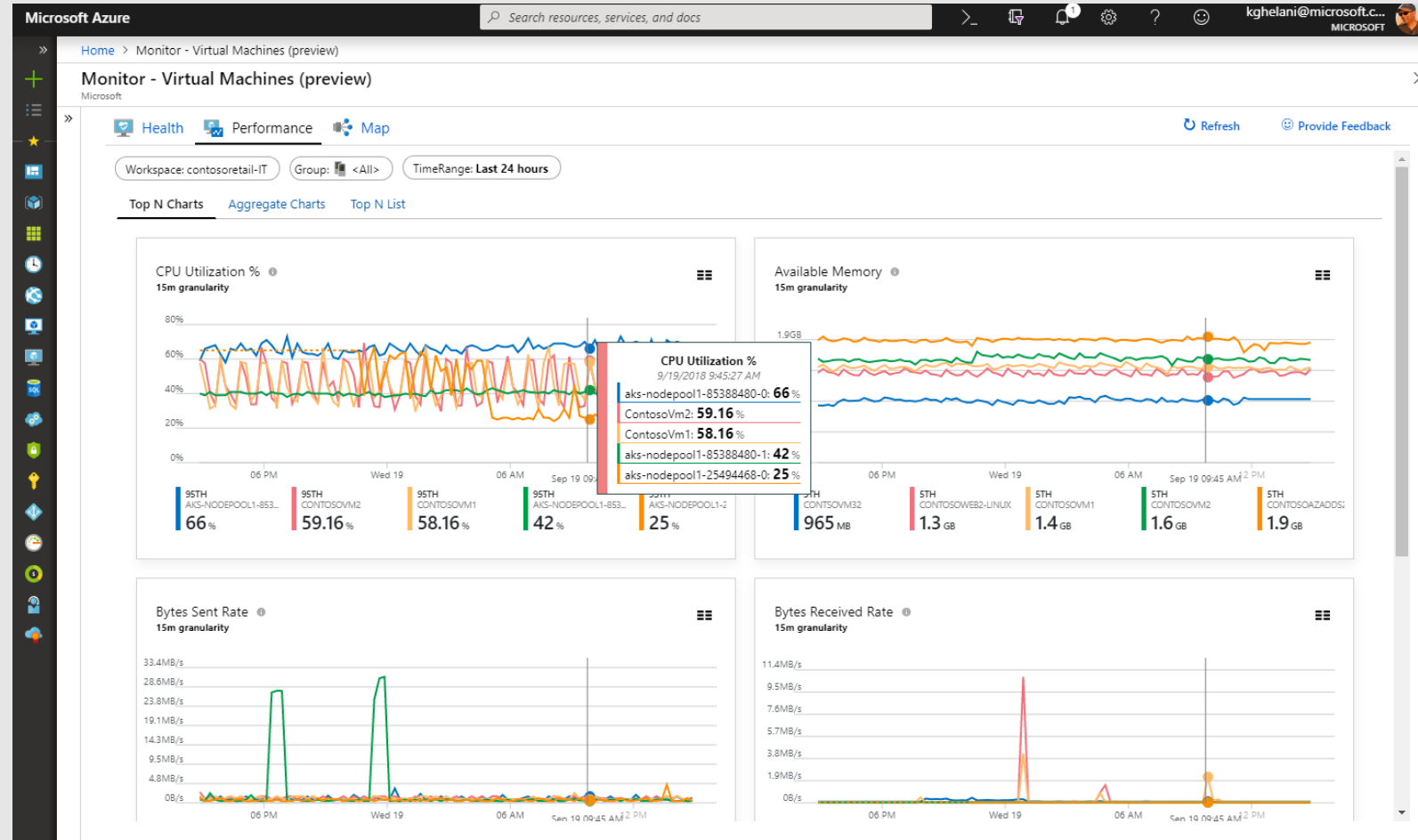


Azure Monitor for VMs



Performance

- ➔ Aggregation of VM metrics across thousands of VMs
- ➔ Top N performance views identify resource constrained VMs @ scale
- ➔ Drill through performance diagnostics for root cause analysis
- ➔ Drill through to advanced analytics on VM logs
- ➔ Built in views for key performance indicators

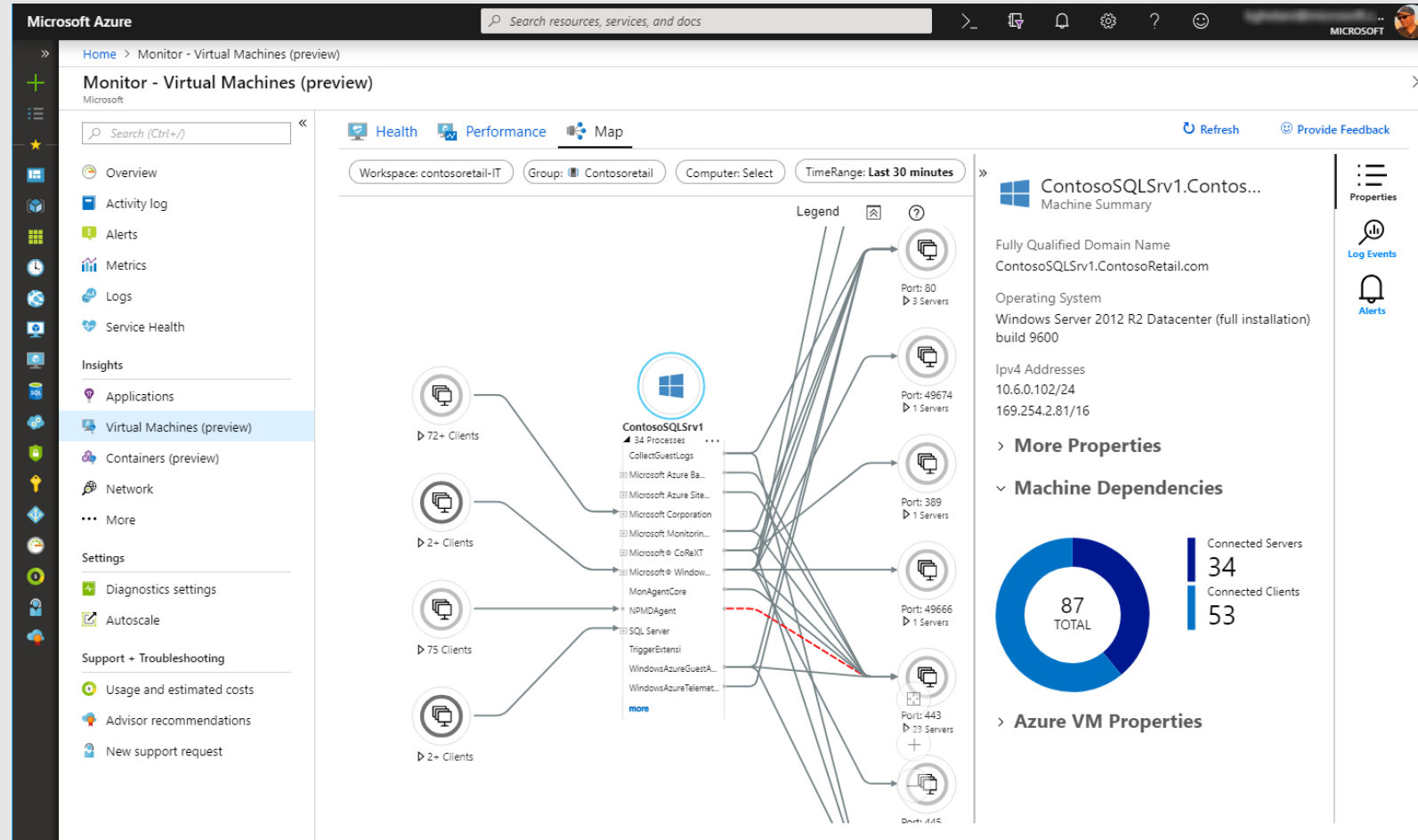


Azure Monitor for VMs



Maps

- ➔ Visualize VMs and process interaction for resource groups, VM scale sets and subscriptions
- ➔ Identify surprise dependencies and connection failures
- ➔ Live connection metrics between processes and VMs identifying spikes in network traffic
- ➔ Drill through dependent VMs to Alerts and Logs



Azure Monitor for VMs



On boarding

- ➔ Built-in monitoring policy to on board Azure VMs @ scale
- ➔ Policy supports existing VMs and new VMs created
- ➔ Remediation policy to on board VMs falling out of compliance

The screenshot shows the Azure portal interface for the 'Enable Azure Monitor for VMs - ContosoAd' policy. The page includes a search bar at the top, a left-hand navigation pane, and a main content area. The main content area displays the policy details, including the name, description, and definition. Below this, there is a section for 'Selected Scopes' showing '1 selected subscription'. A summary section shows the compliance state: 'Non-compliant' (2 out of 6), 'Non-compliant policies' (2), and 'Non-compliant resources' (2). It also shows 'Events (last 7 days)' with counts for Audit (2), Append (0), Deny (0), and Deploy (41). The bottom section is a table of non-compliant resources.

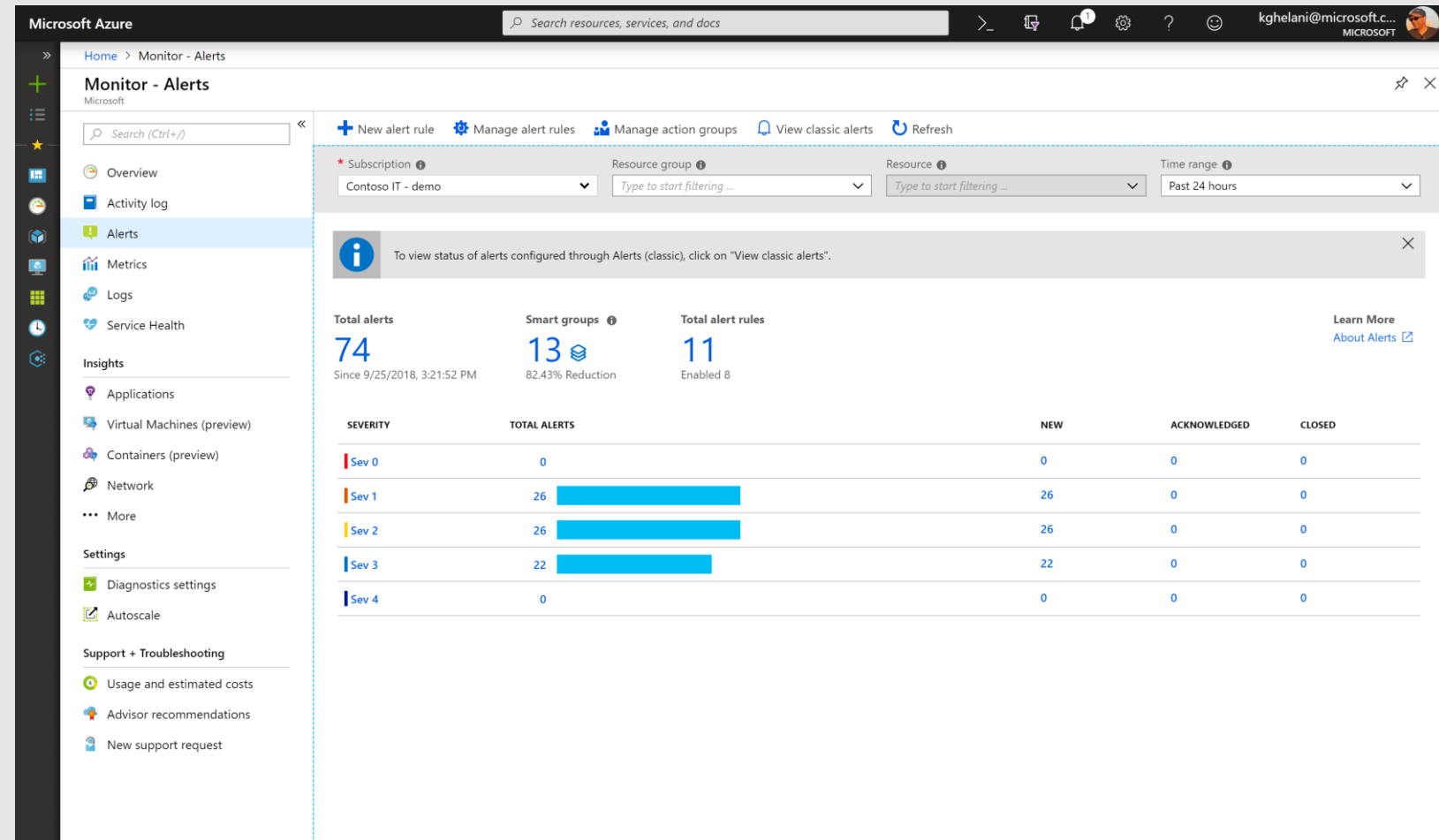
NAME	EFFECT TYPE	COMPLIANCE	NON-COMPLIANT RESOURCES
Audit Dependency Agent Deployment - VM Image (OS) unlisted ...	AuditIfNotExists	Non-compliant	1
Deploy Log Analytics Agent for Windows VMs - Preview	DeployIfNotExists	Non-compliant	1
Audit Log Analytics Agent Deployment - VM Image (OS) unlisted...	AuditIfNotExists	Compliant	0
Deploy Dependency Agent for Linux VMs - Preview	DeployIfNotExists	Compliant	0
Deploy Dependency Agent for Windows VMs - Preview	DeployIfNotExists	Compliant	0
Deploy Log Analytics Agent for Linux VMs - Preview	DeployIfNotExists	Compliant	0

Azure Monitor Alerts



Just got better

- ➔ One Alert Mgmt experience
- ➔ Configure Alerts at Scale
Multi-resource alerting
- ➔ Unified Alert lifecycle Management
- ➔ Smart grouping to reduce noise
- ➔ Dynamic threshold base Alerting



Demo

Azure Monitor for VMs

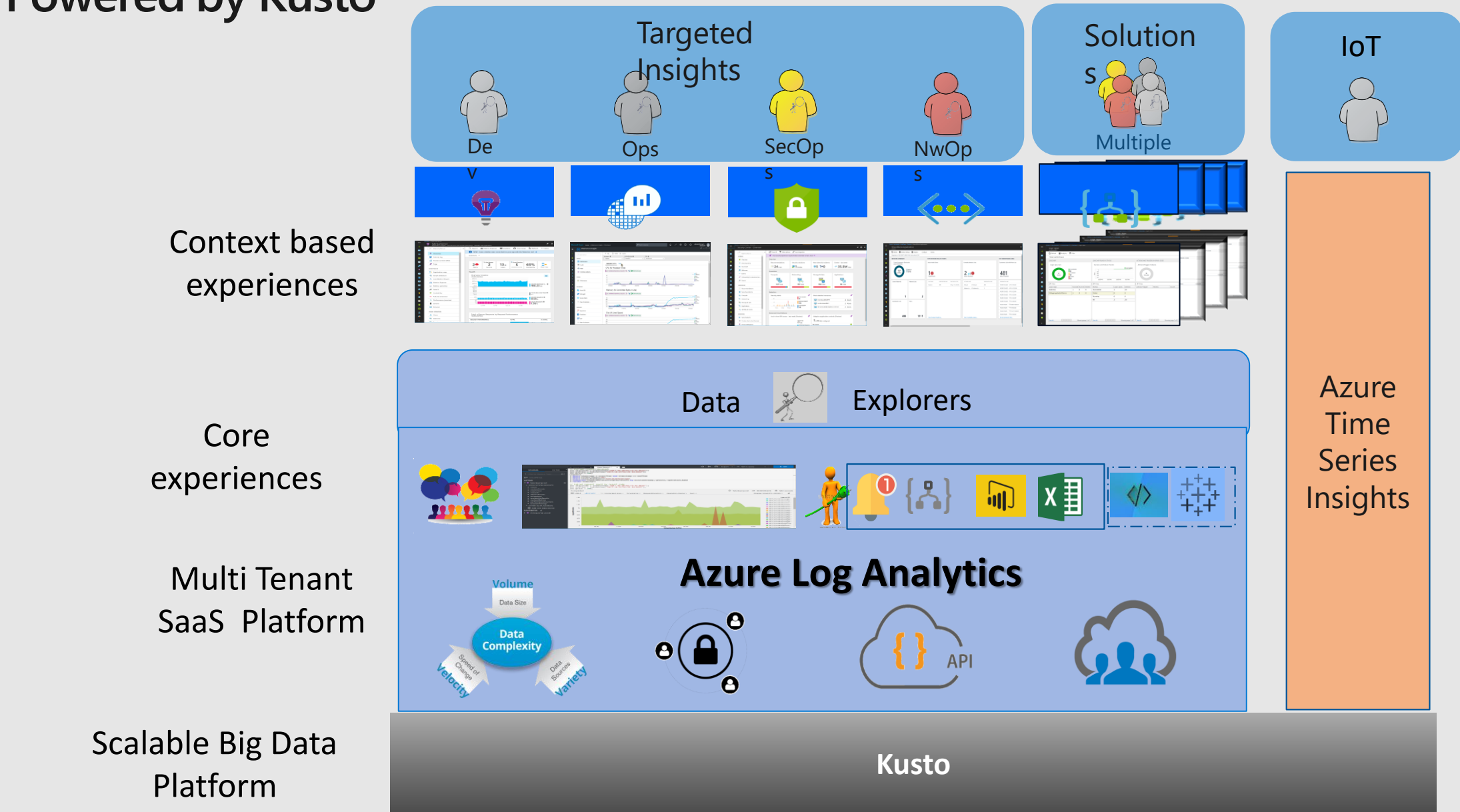


Azure Monitor Logs (aka Log Analytics)



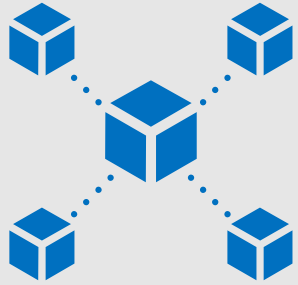
Azure Log Analytics

Powered by Kusto



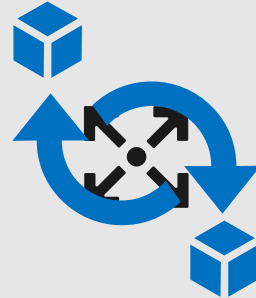
Simple and unified experience

Expand your enterprise management with a consistent experience



Single platform for overall management

- Single pane of control
- Unified experience



Leverage existing management platform

- Integrate with existing systems
- Connect with isolated resources





Access anywhere with a consistent user experience

- Control from anywhere
- Consistent user interface



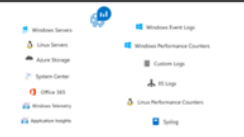
Azure Log Analytics Ecosystem

Ingestion




Microsoft Monitoring Agent

Azure Extensions
Data Collector APIs
Linux





Exploration



Microsoft Azure Portal
Advanced Analytics Portal



Azure Monitor
Service Map

Export & Correlation



Application Insights
Connector

Power BI



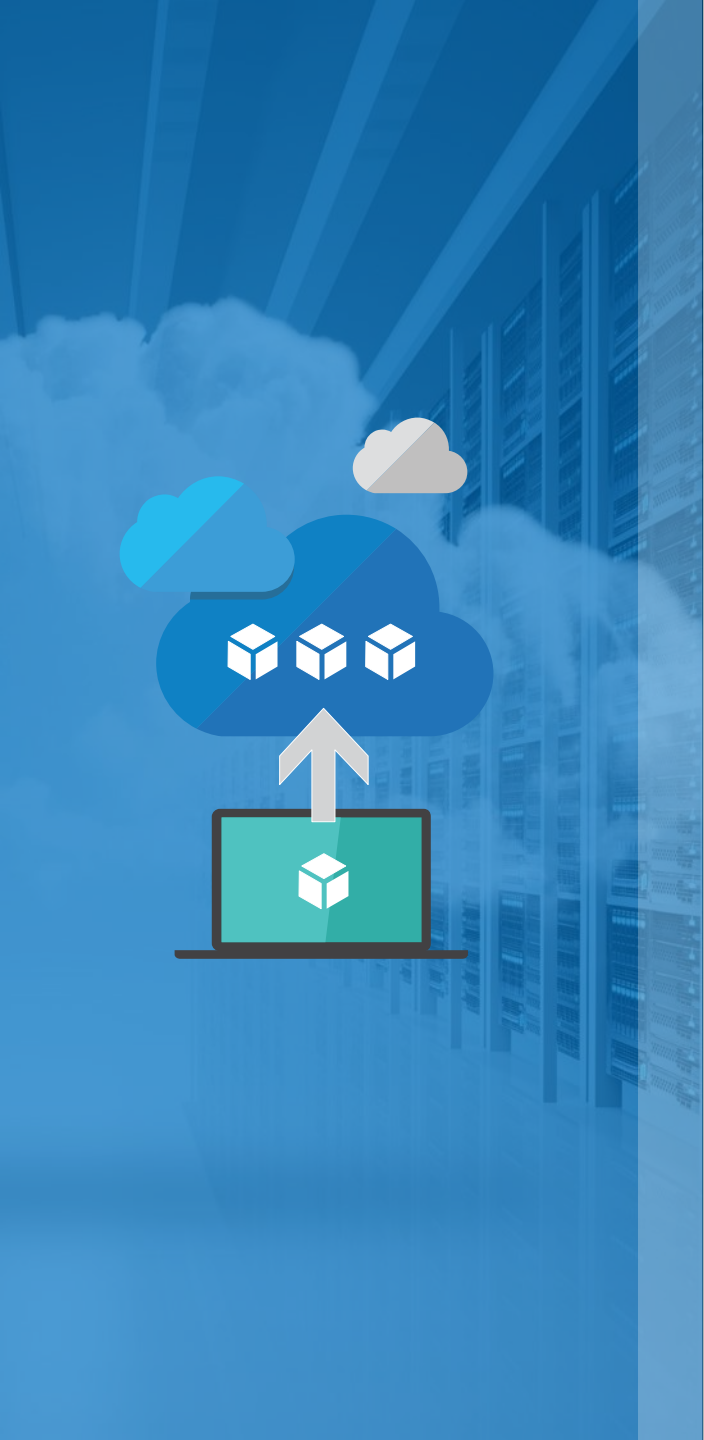
Blob storage

Microsoft Flow

Data Access REST APIs

Solutions

Security & Audit	Wire Data	Upgrade Compliance	HD Insights	VMWare
Antimalware	Network Performance	Upgrade Readiness	SQL Assessment	Azure App Gateway
Azure Activity Logs	Monitoring	Device Health	AD Assessment	Azure NSG Analytics
Update Management	Office 365	Service Map	SQL Assessment Plus	Key Vault Analytics
Azure Automation	Azure SQL Analytics	Alert Management	Exchange Assessment	MORE....
Change Tracking	Azure Containers	Capacity Management	SP Assessment	



UNIFIED EXPERIENCE

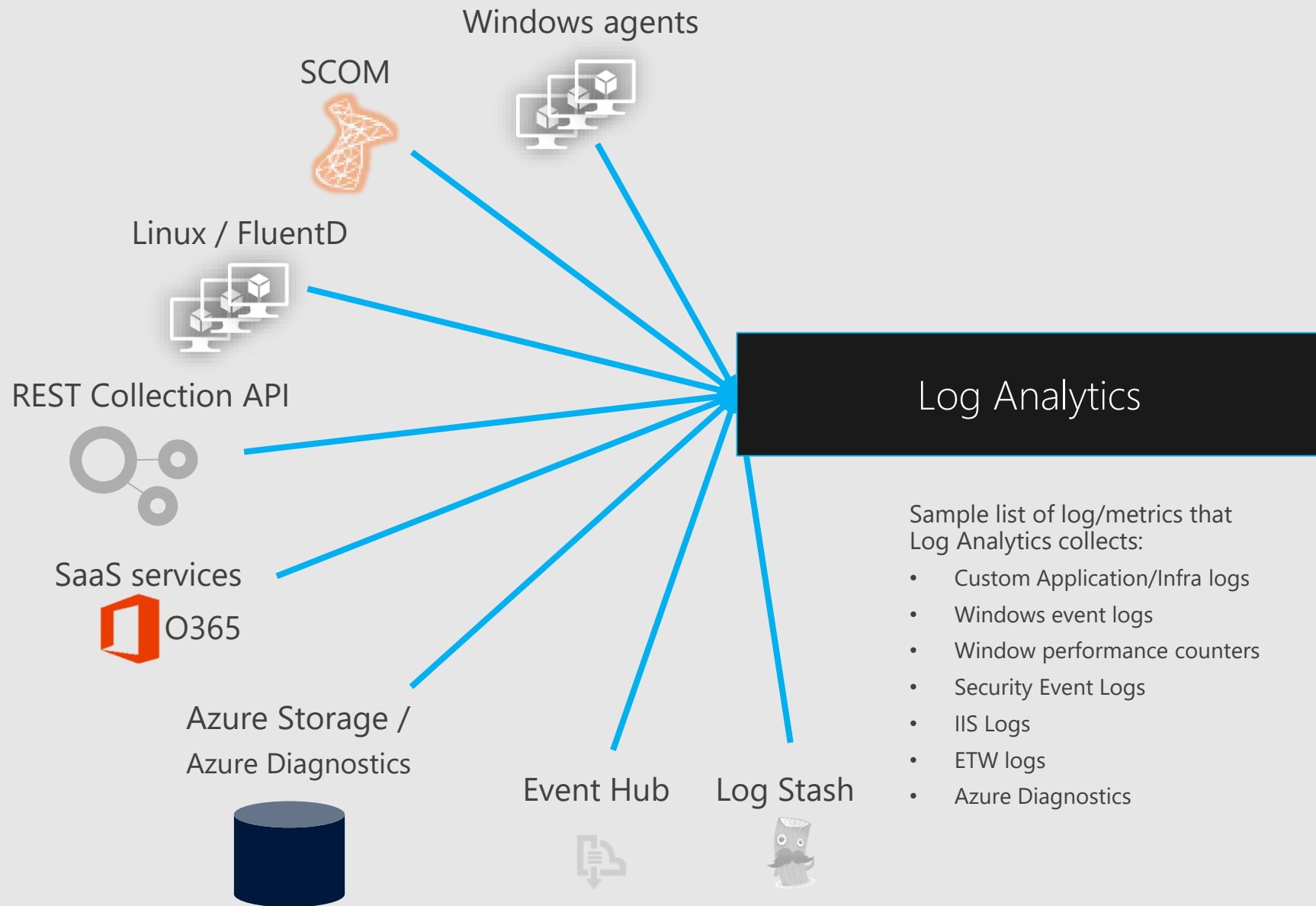
COLLECT AND INDEX DATA

SEARCH AND INVESTIGATE

CORRELATE AND ANALYZE

VISUALIZE AND REPORT

MONITOR AND ALERT

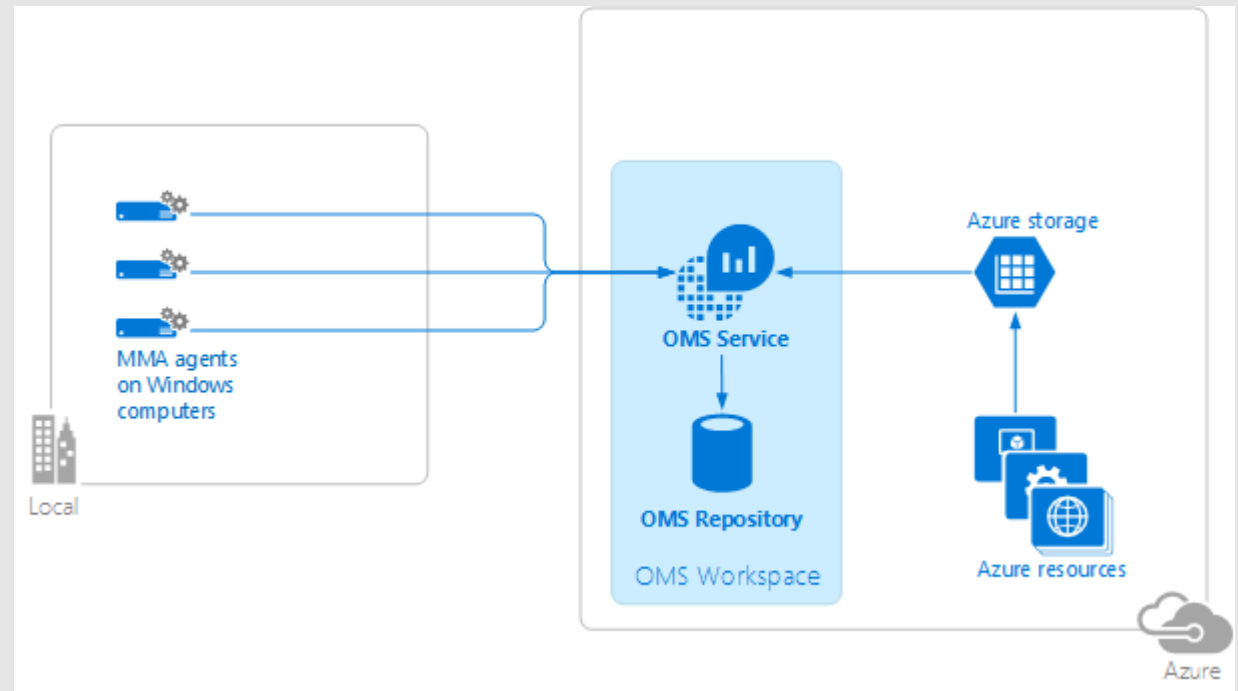


Windows agents



Log Analytics

Connect to Windows computers in your on-premises infrastructure directly to OMS workspaces by using a customized version of the Microsoft Monitoring Agent (MMA).



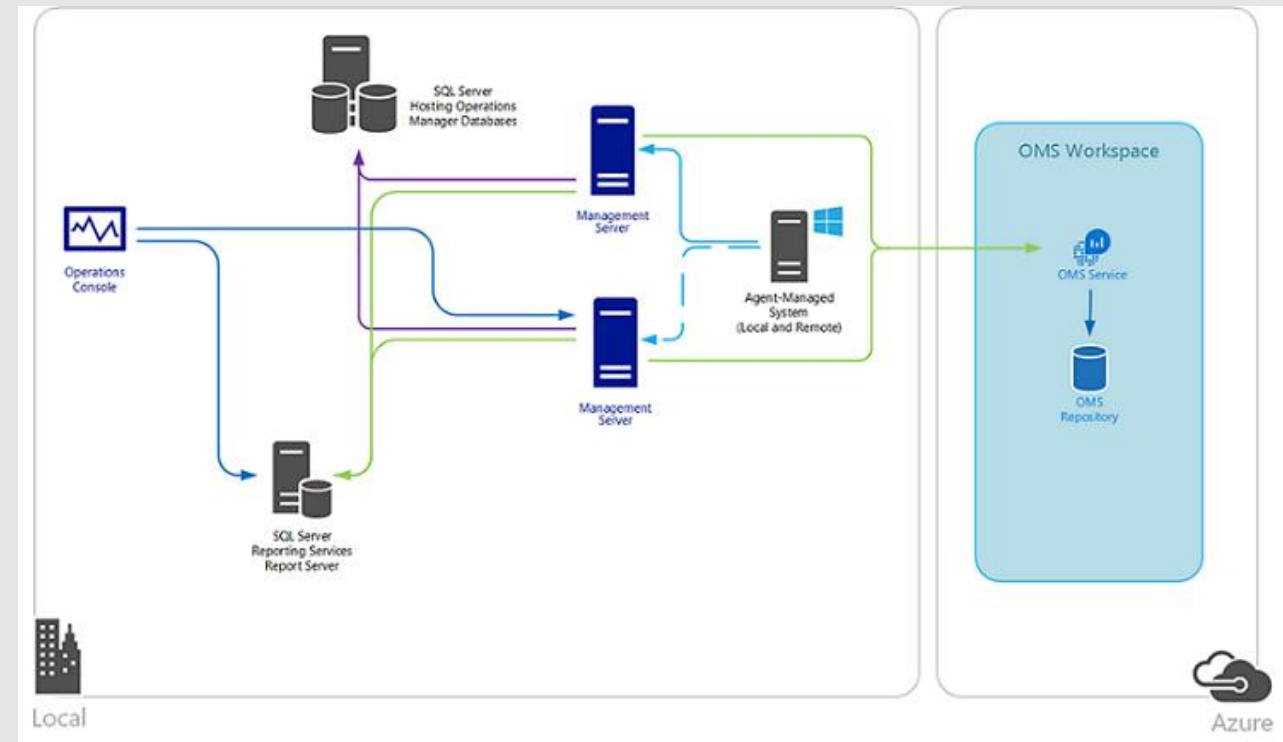
SCOM



Log Analytics

Integrate Operations Manager with your OMS workspace to:

- Continue monitoring the health of your IT services with Operations Manager
- Maintain integration with your ITSM solutions supporting incident and problem management
- Manage the lifecycle of agents deployed to on-premises and public cloud IaaS virtual machines that you monitor with Operations Manager





UNIFIED EXPERIENCE

COLLECT AND INDEX DATA

SEARCH AND INVESTIGATE

CORRELATE AND ANALYZE

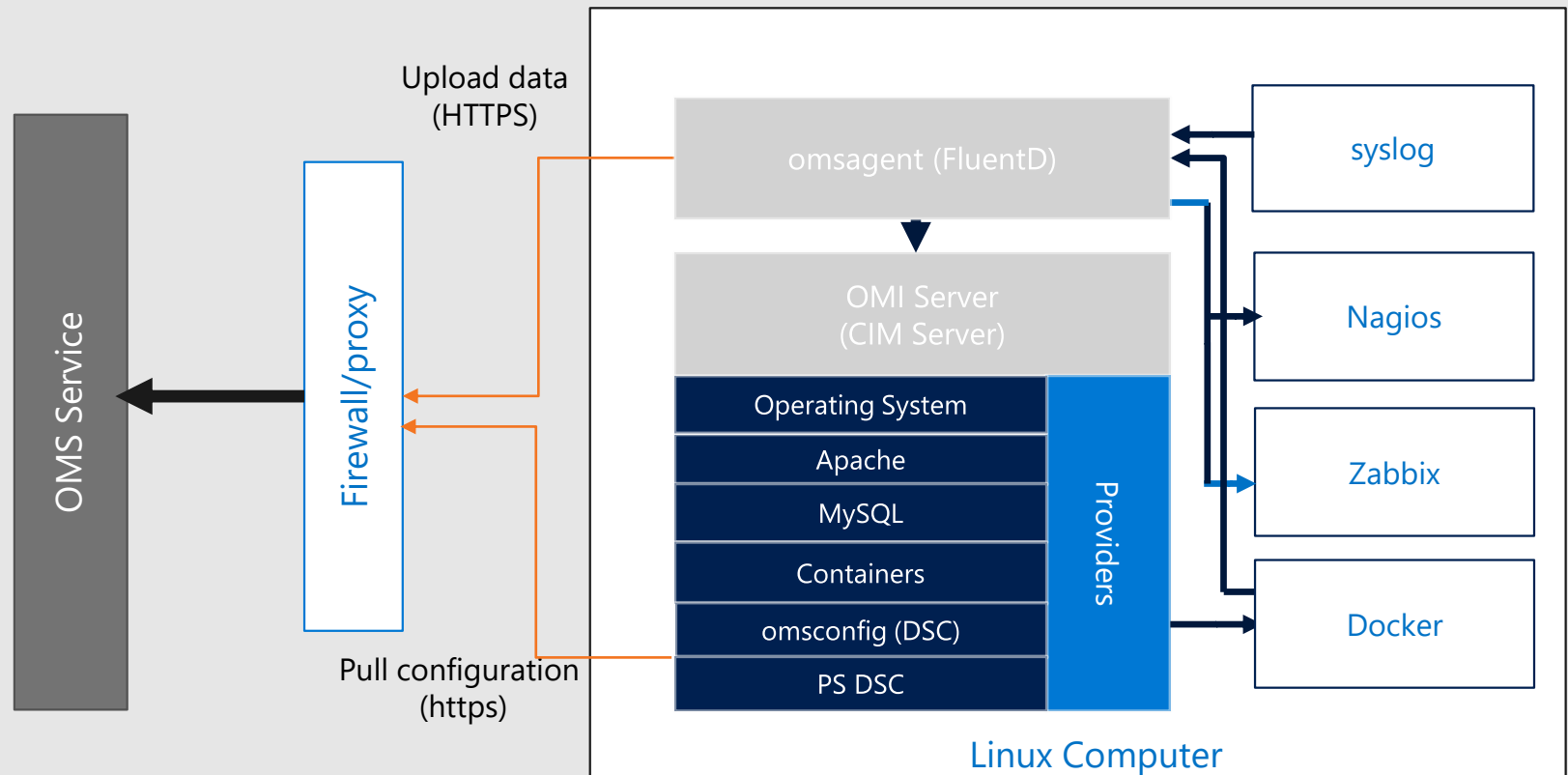
VISUALIZE AND REPORT

MONITOR AND ALERT

Linux / FluentD



Collect and act on data generated from Linux computers. Adding data collected from Linux to Log Analytics allows you to manage Linux systems and container solutions like Docker regardless of where your computers are located—virtually anywhere.





UNIFIED EXPERIENCE

COLLECT AND INDEX DATA

SEARCH AND INVESTIGATE

CORRELATE AND ANALYZE

VISUALIZE AND REPORT

MONITOR AND ALERT

Linux / FluentD



Log Analytics

Supported Linux platform



6.X 32/64-bit

7.X 32/64-bit

8.X 32/64-bit



5.X 32/64-bit

6.X 32/64-bit

7.X 64-bit



2013.09 – 2015.09



5.X 32/64-bit

6.X 32/64-bit

7.X 64-bit



12.X 32/64-bit

14.X 32/64-bit

15.X 32/64-bit

16.X 32/64-bit



alpha
beta
stable



10.X 32/64-bit

11.X 32/64-bit

12.X 64-bit

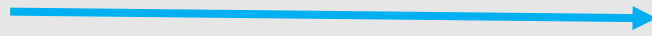
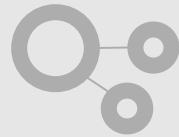


5.X 32/64-bit

6.X 32/64-bit

7.X 64-bit

REST Collection API



Log Analytics

Leverage REST collection API to ingest custom data to Operations Management Suite

Post json document to HTTPS endpoint

Ensure json is flattened and not nested

```
$json = @"  
[ { "slot_ID"           : 12345,  
  "ID"                 : "5cdad72f-c848-4df0-8aaa-ffe033e75d57",  
  "availability_Value" : 100,  
  "measurement_Name"  : "last_one_hour",  
  "duration"           : 3600,  
  "ExecutionTime"     : "2016-05-12T20:00:00.625Z"  
},  
{ ... } ]  
"@
```

Authenticated using workspace key to hash content

API

[Log Search API](#)

[Alert API](#)

Powershell

[Log Analytics cmdlets](#)

Nouns

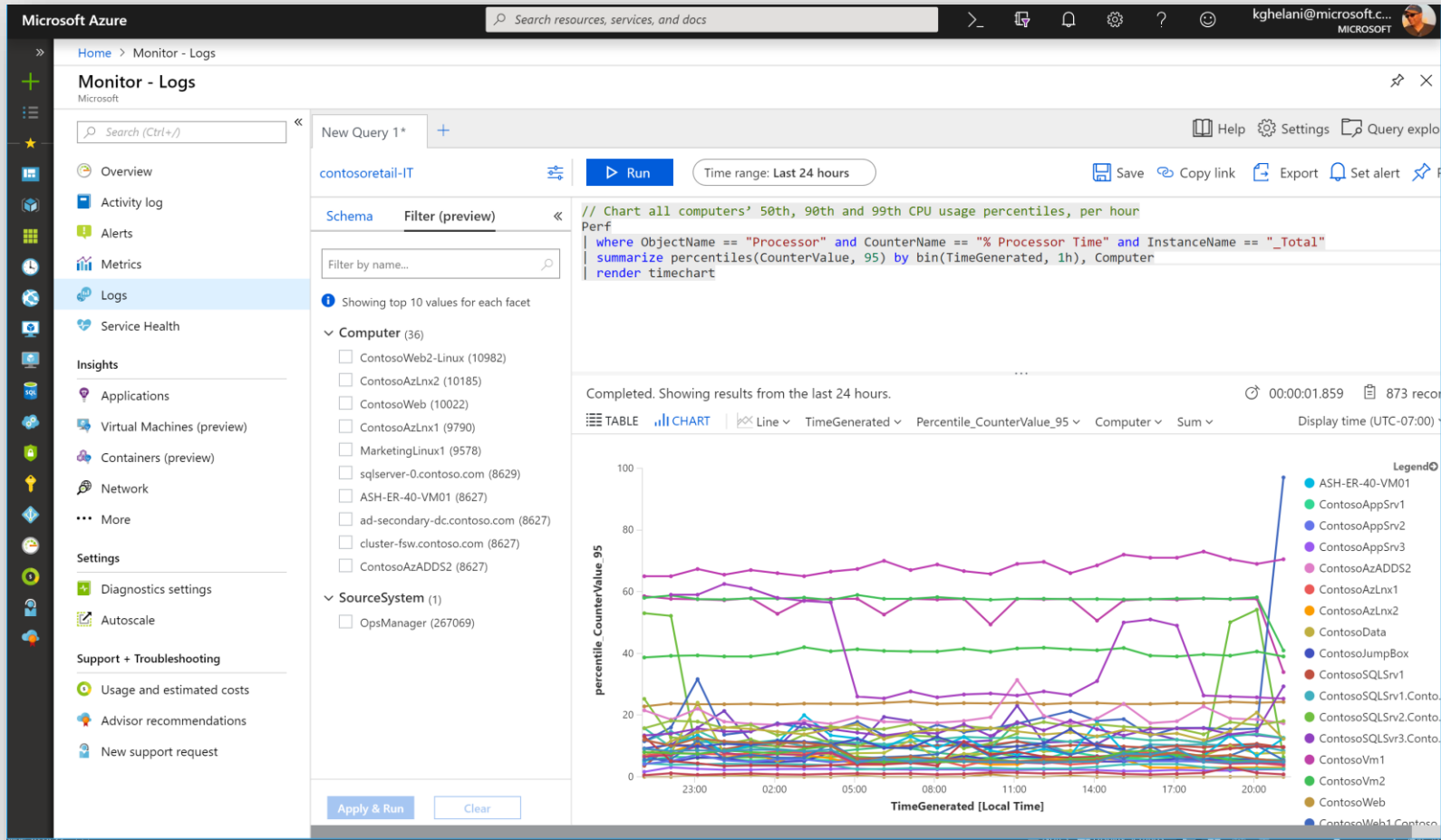
- ComputerGroup
- IntelligencePacks (solutions)
- LinkTargets
- SavedSearch
- SavedSearchResults
- StorageInsights
- Workspace
- WorkspaceManagementGroups
- WorkspaceSharedKeys
- WorkspaceUsage

Azure Monitor Logs



Log Analytics

- Log Analytics advanced query experience now in Azure Portal
- RBAC per type
- Run analytics queries for investigations, statistics, and root cause + trend analysis
- Utilize ML algorithms for clustering and anomaly detection
- Training: <http://aka.ms/kqlpluralsight>



Azure Monitor Logs

Log Analytics Demo



Recap



Azure Monitor for VMs

Monitor VMs @ Scale

Identify & isolate host-level or guest-level health problems

Visualize service dependencies & connection failures in Maps

On board VMs at Scale using PowerShell and/or Azure Policy

Azure Monitor Logs

Log Analytics advanced query experience now in Azure Portal

Utilize ML algorithms for clustering and anomaly detection

RBAC per type

<http://aka.ms/kqlpluralsight>

