Microsoft

# Azure Log Analytics

# Workshop

Michael Petersen, Microsoft Cloud Solution Architect

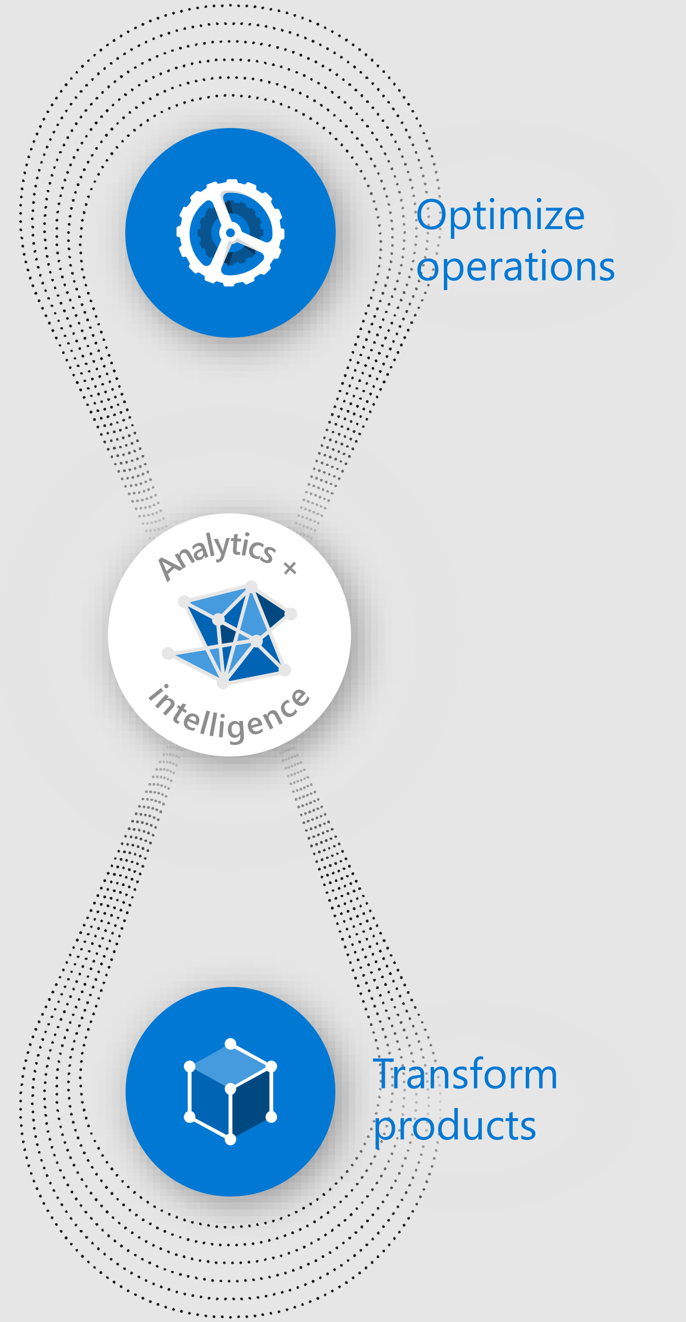
# In this workshop

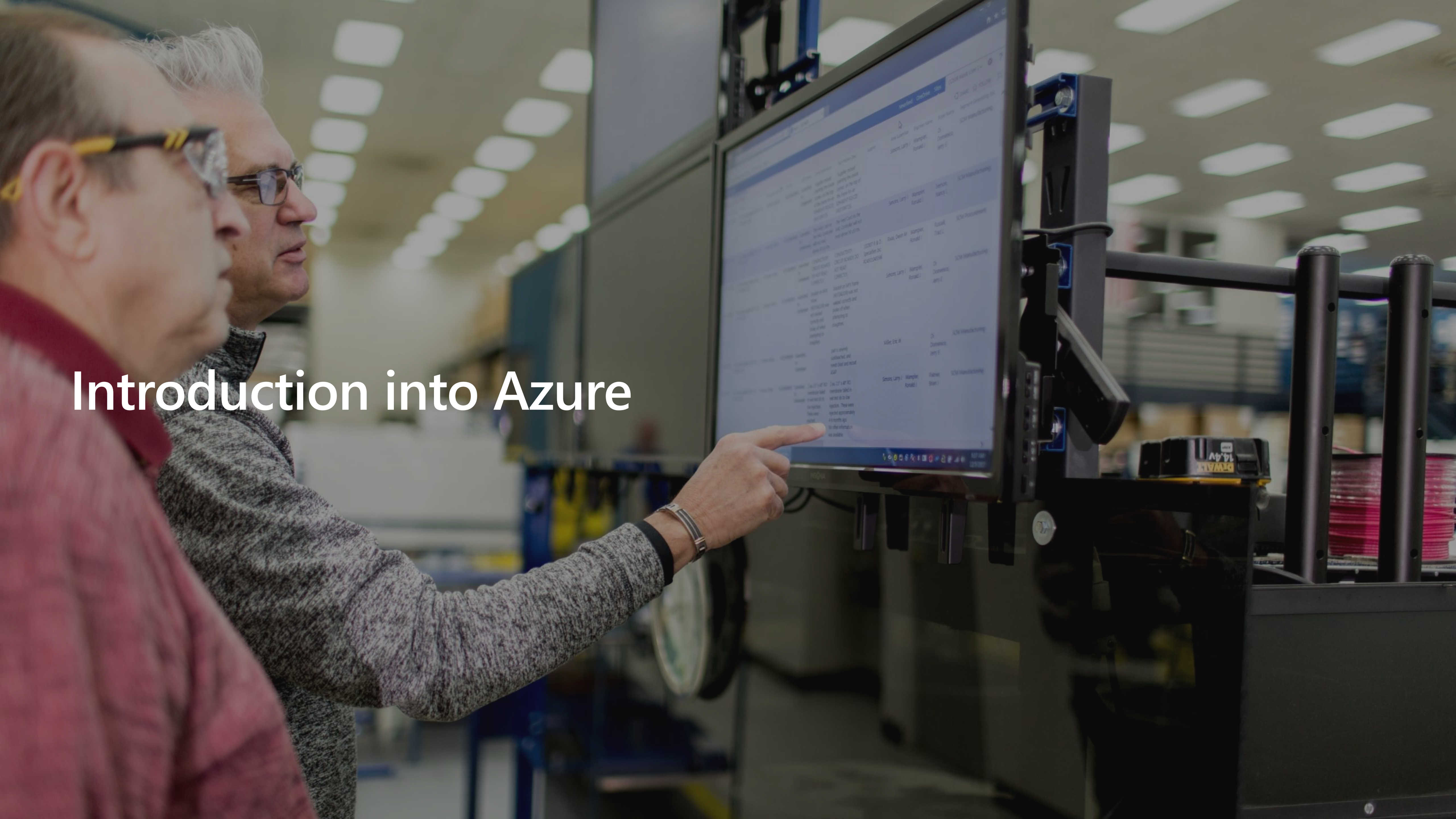
1. **Introduction into Azure**

2. **Azure Monitor**
   Logs & Metrics,
   Insights
   Network Watcher

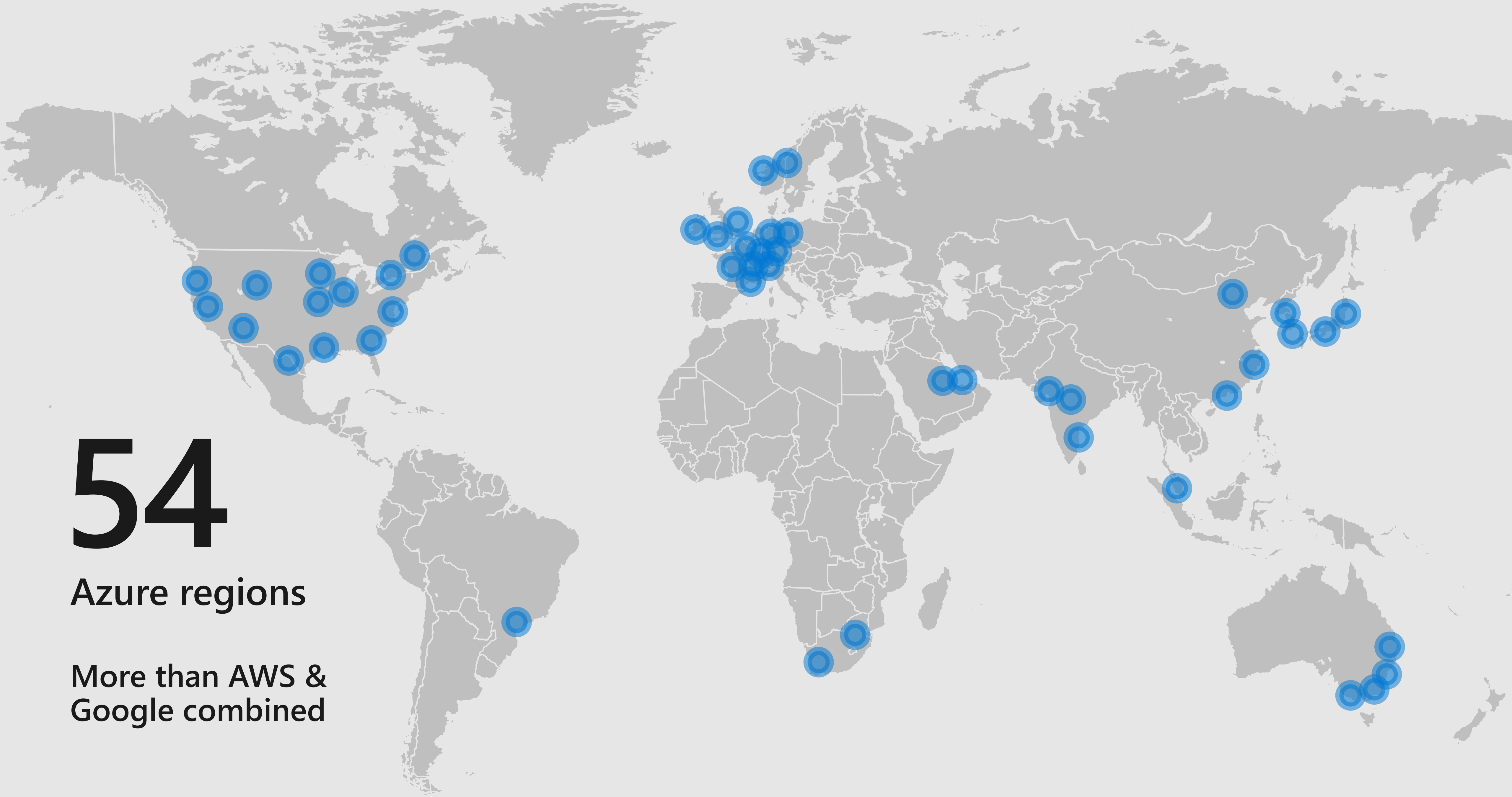
3. **Log Analytics**
   Alerts & Actions Groups
   Kusto Query Language
   How to use Tiles, Views, and Parts

4. **Log Analytics End-to-End Solution**
   What is a Solution?
   Import data into a Workspace
   Queries and Dashboards
   How to integrate external Systems
   Solution Install and Uninstall





# Introduction into Azure



# 54

## Azure regions

More than AWS &
Google combined

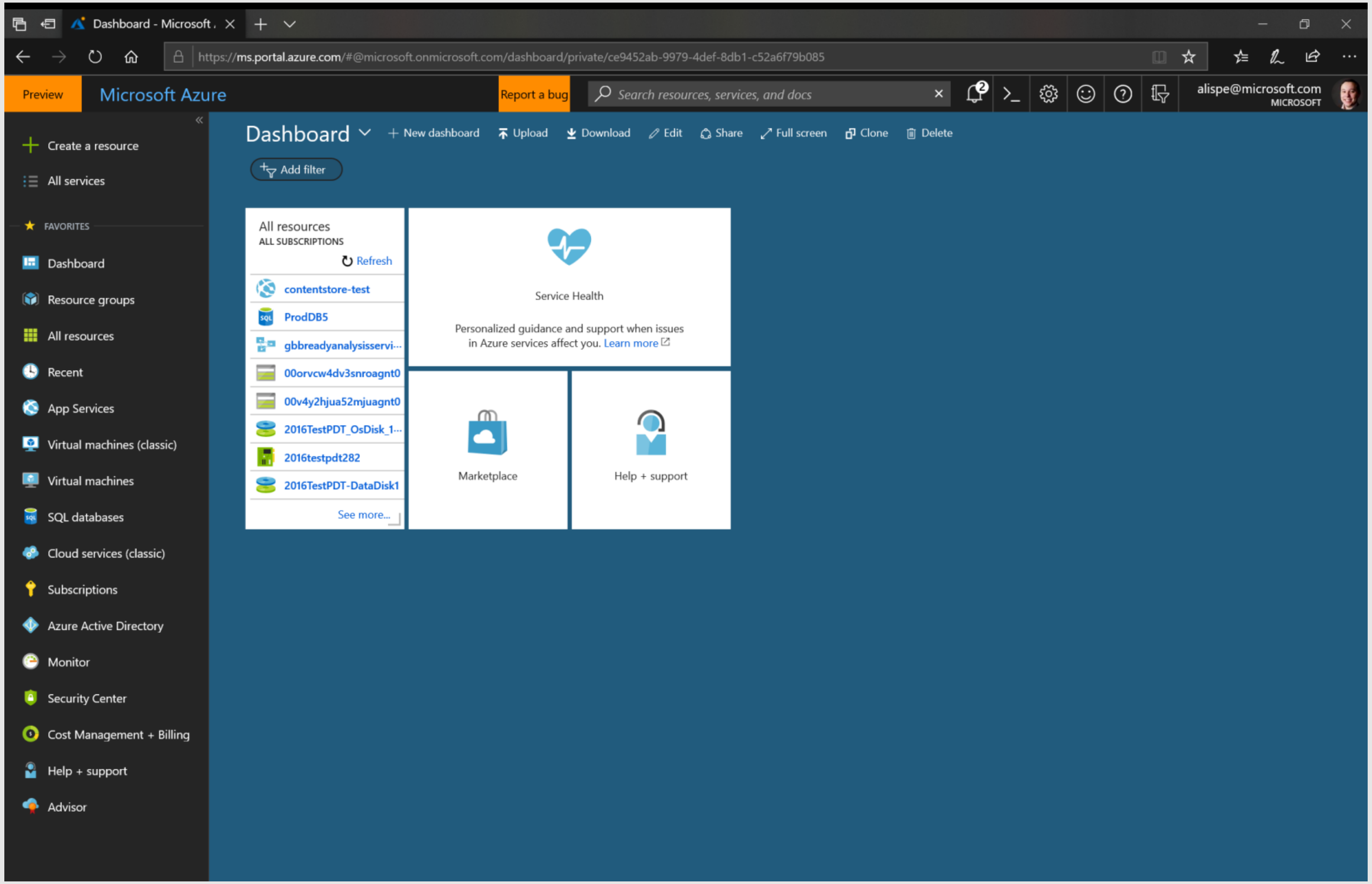
# Azure Portal – https://portal.azure.com

## Recommendations

Create multiple portal dashboards by key roles, (e.g., operations, finance, development), key projects, and key service KPIs

Customize portal to specific needs

Share portal dashboards in teams



https://ms.portal.azure.com/#@microsoft.onmicrosoft.com/dashboard/private/ce9452ab-9979-4def-8db1-c52a6f79b085

Personalized guidance and support when issues in Azure services affect you. Learn more

# Azure Cloud Shell – https://shell.azure.com

## Hints

Choose shell environment via URL path

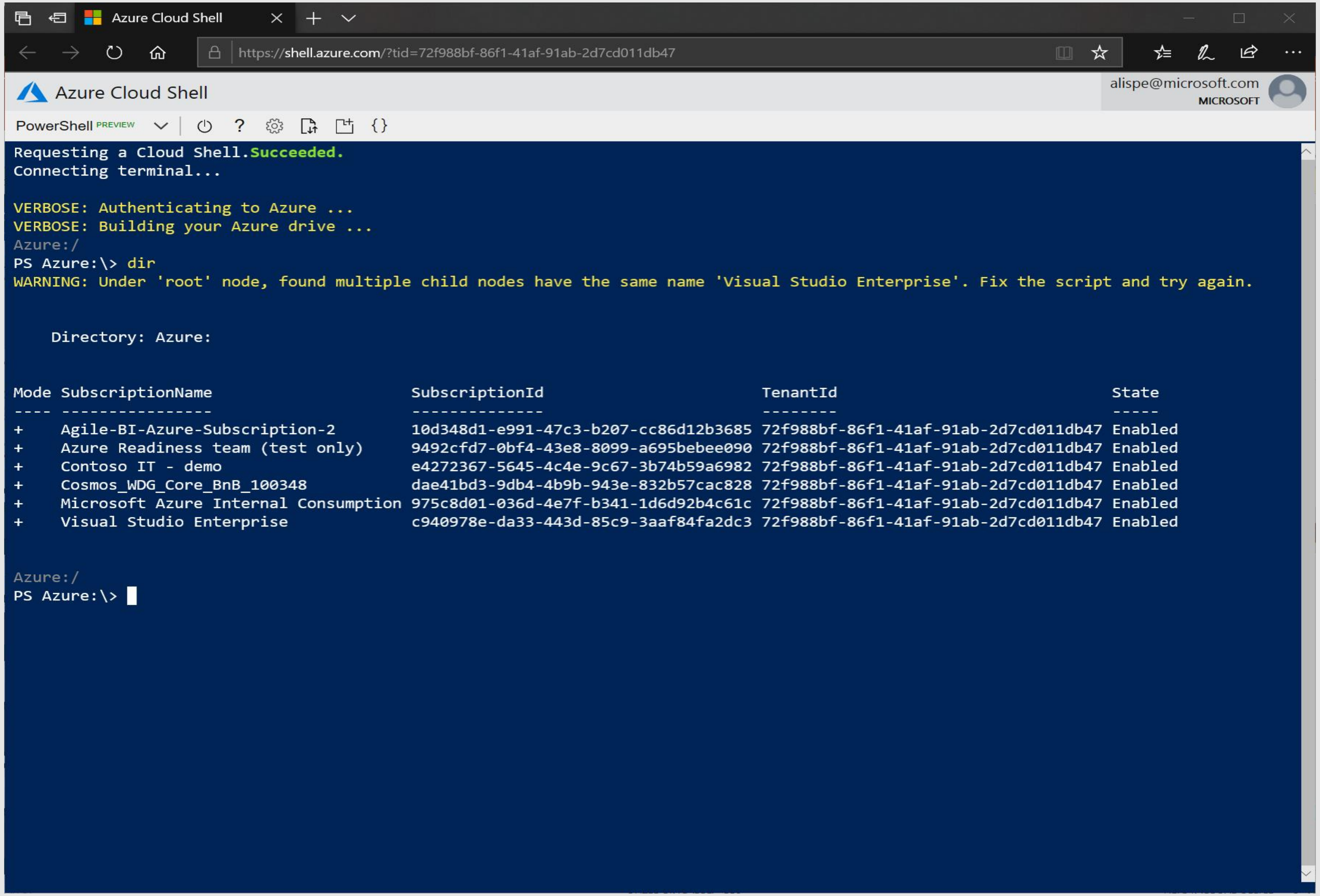
- /powershell
- /bash

Latest tools installed (e.g. kubectl, terraform, Az modules)

Rely on Az modules and migrate away from AzureRM modules

Cloud shell always runs on Linux and is executed within Docker containers

Migrate away from Windows PowerShell to PowerShell Core

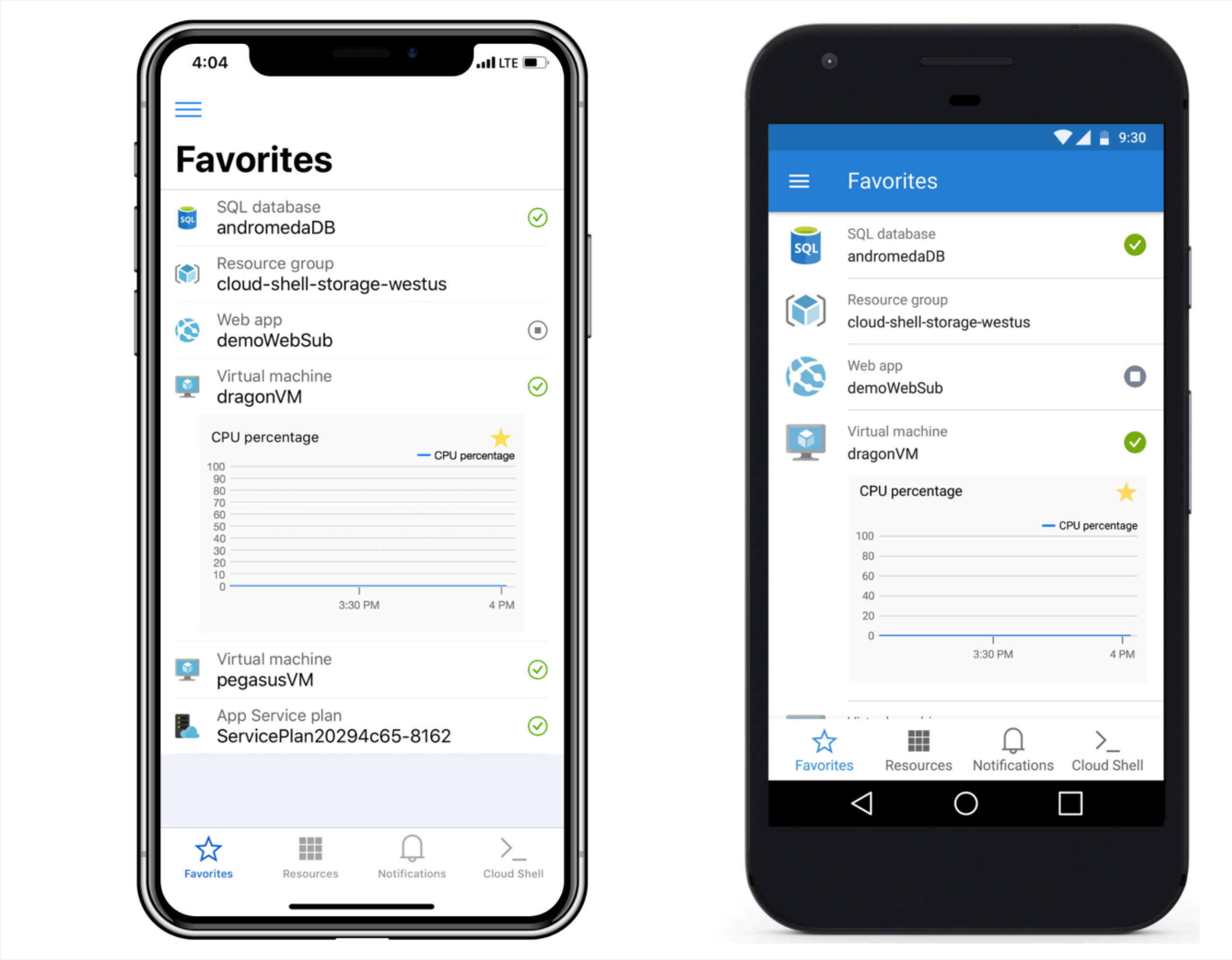


```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
Azure:/
PS Azure:\> dir
WARNING: Under 'root' node, found multiple child nodes have the same name 'Visual Studio Enterprise'. Fix the script and try again.


    Directory: Azure:


Mode SubscriptionName                     SubscriptionId                       TenantId                             State
---- ----------------                     --------------                       --------                             -----
+    Agile-BI-Azure-Subscription-2        10d348d1-e991-47c3-b207-cc86d12b3685 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled
+    Azure Readiness team (test only)     9492cfd7-0bf4-43e8-8099-a695bebee090 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled
+    Contoso IT - demo                    e4272367-5645-4c4e-9c67-3b74b59a6982 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled
+    Cosmos_WDG_Core_BnB_100348           dae41bd3-9db4-4b9b-943e-832b57cac828 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled
+    Microsoft Azure Internal Consumption 975c8d01-036d-4e7f-b341-1d6d92b4c61c 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled
+    Visual Studio Enterprise             c940978e-da33-443d-85c9-3aaf84fa2dc3 72f988bf-86f1-41af-91ab-2d7cd011db47 Enabled


Azure:/
PS Azure:\>
```

# Azure Mobile App

**Stay connected to your Azure resources – anytime, anywhere**

- Monitor the health and status of your Azure resources on the go
- Get quick access to your favorite resources
- Get notifications and alerts about important health issues
- Quickly diagnose and fix issues from your mobile device
- Run Azure Cloud Shell scripts (PowerShell or Bash) from the app
- Control access to resources using Role Based Access Control
- Available on iOS and Android



Favorites

SQL database
andromedaDB

Resource group
cloud-shell-storage-westus

Web app
demoWebSub

Virtual machine
dragonVM

Virtual machine
pegasusVM

App Service plan
ServicePlan20294c65-8162

# Azure Monitor

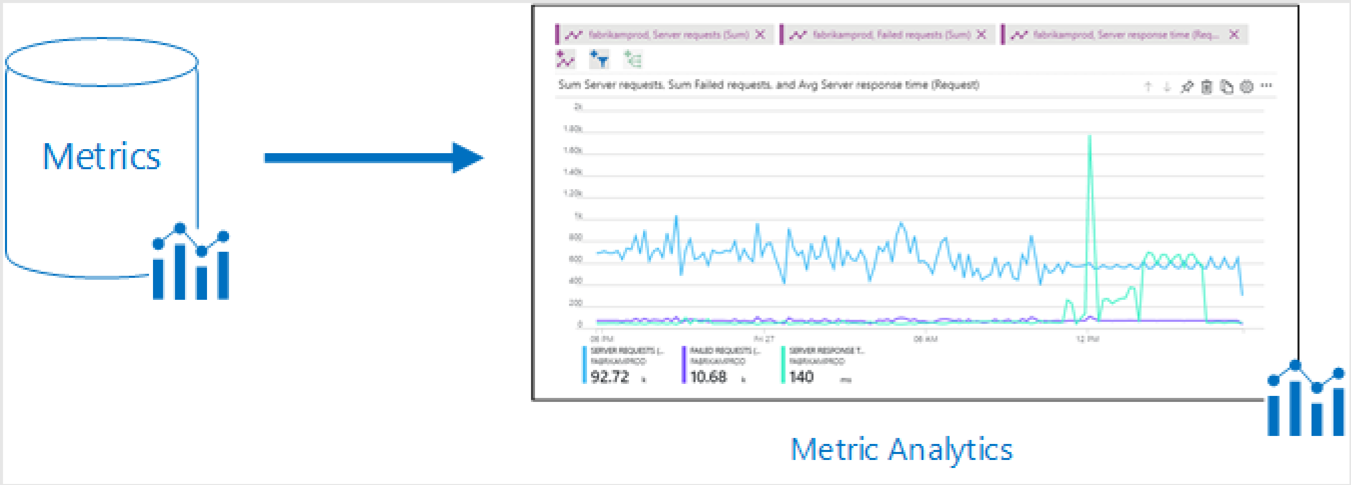
# Azure Monitor

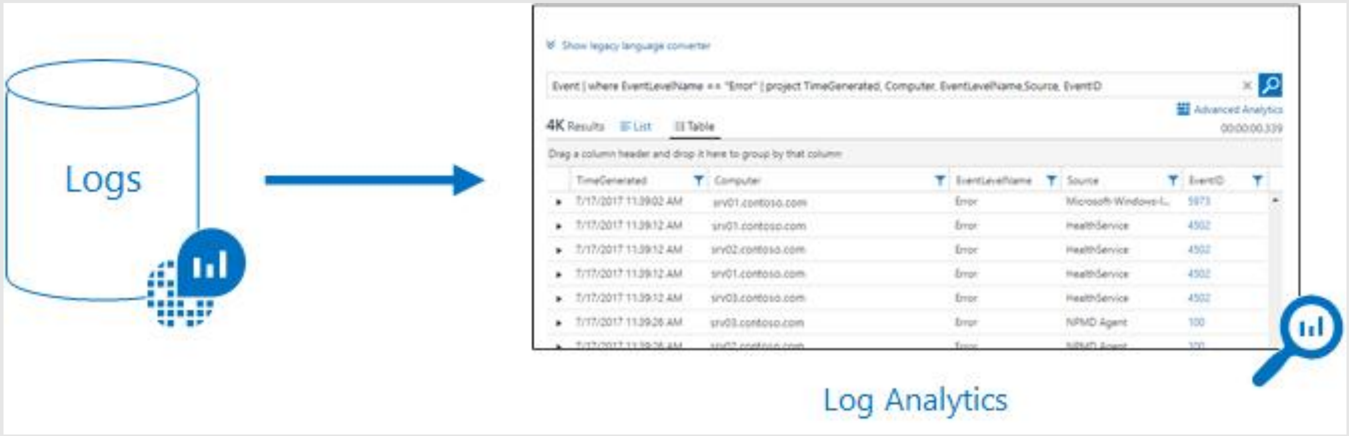
## Metrics and Logs

- All data collected by Azure Monitor fits into one of two fundamental types, metrics and logs.

- Metrics are numerical values that describe some aspect of a system at a particular point in time.

- Logs contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs.





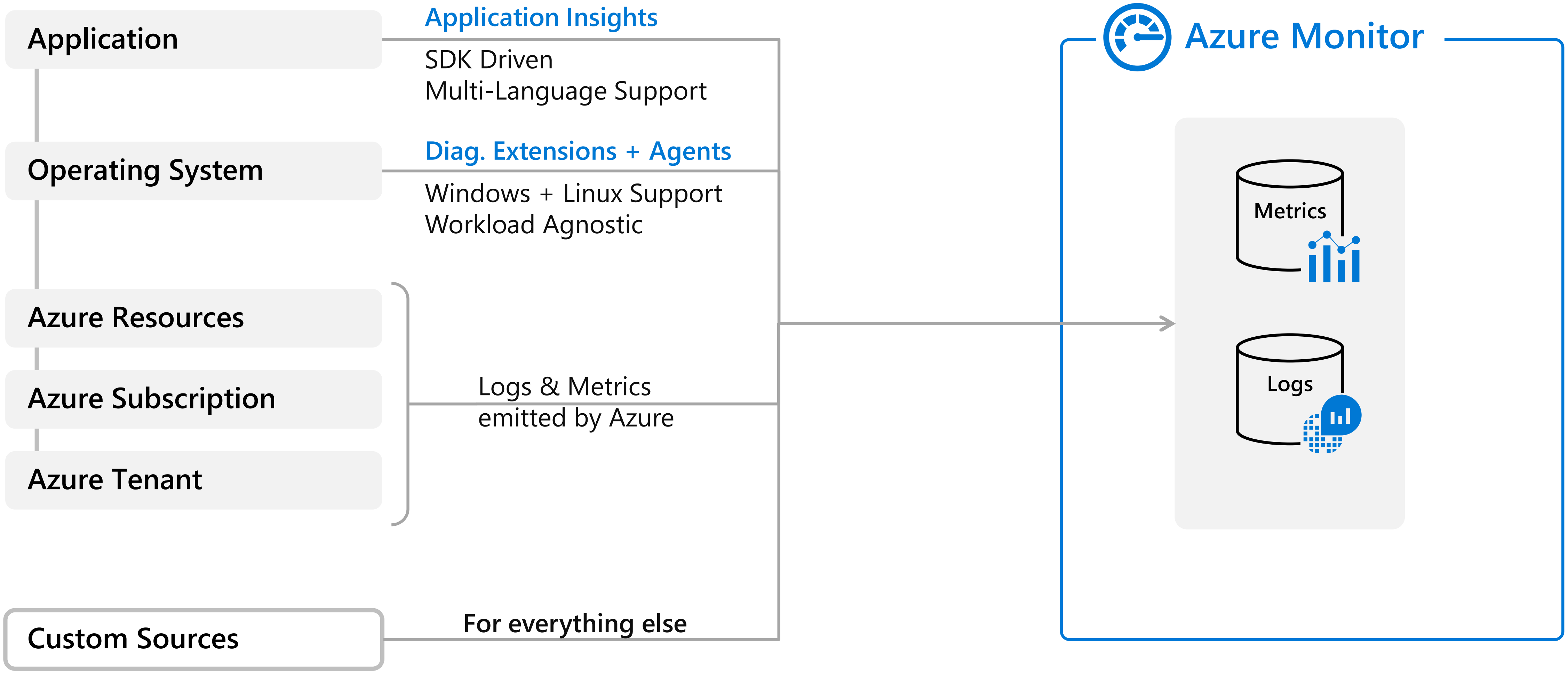
```
Event | where EventLevelName == "Error" | project TimeGenerated, Computer, EventLevelName,Source, EventID
```

00:00:00.339

Drag a column header and drop it here to group by that column

| TimeGenerated | Computer | EventLevelName | Source | EventID |
|---|---|---|---|---|
| 7/17/2017 11:39:02 AM | srv01.contoso.com | Error | Microsoft-Windows-L... | 5973 |
| 7/17/2017 11:39:12 AM | srv01.contoso.com | Error | HealthService | 4502 |
| 7/17/2017 11:39:12 AM | srv02.contoso.com | Error | HealthService | 4502 |
| 7/17/2017 11:39:12 AM | srv01.contoso.com | Error | HealthService | 4502 |
| 7/17/2017 11:39:12 AM | srv03.contoso.com | Error | HealthService | 4502 |
| 7/17/2017 11:39:26 AM | srv03.contoso.com | Error | NPMD Agent | 100 |
| 7/17/2017 11:39:26 AM | srv02.contoso.com | Error | NPMD Agent | 100 |

# Azure Monitor Metrics & Logs



Application

Application Insights

SDK Driven
Multi-Language Support

Operating System

Diag. Extensions + Agents

Windows + Linux Support
Workload Agnostic

Azure Resources

Azure Subscription

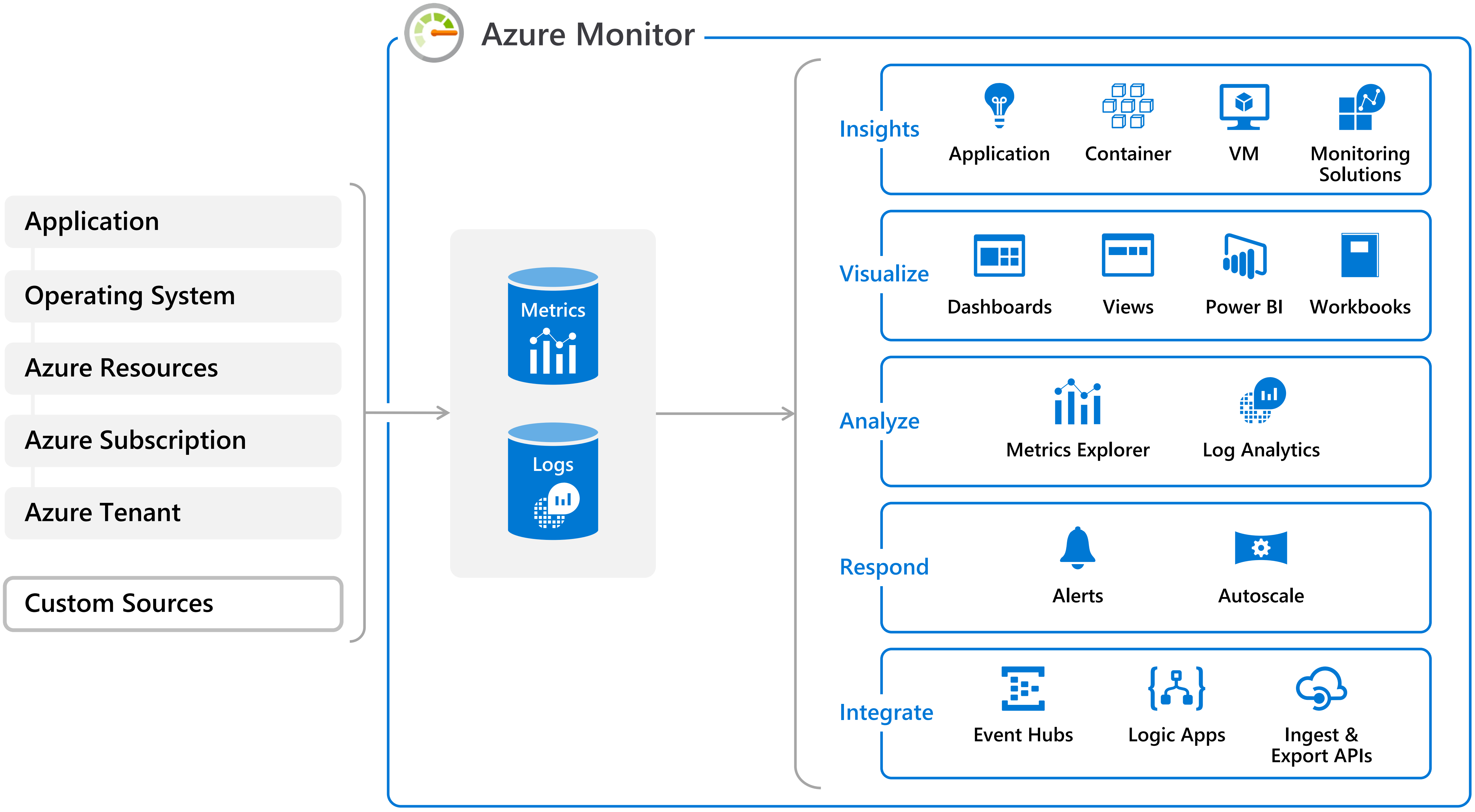
Azure Tenant

Logs & Metrics
emitted by Azure

Custom Sources

For everything else

Azure Monitor


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
Metrics Explorer
Log Analytics
Respond
Alerts
Autoscale
Integrate
Event Hubs
Logic Apps
Ingest & Export APIs

# Azure Monitor

## Data Collection

- Application monitoring data: Data about the performance and functionality of the code you have written, regardless of its OS platform and cloud environment.
- Guest OS monitoring data: Data about the operating system on which your application is running. This could be running in Azure, another cloud like AWS, or on-premises.
- Azure resource monitoring data: Data about the operation of an Azure resource.
- Azure subscription monitoring data: Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
- Azure tenant monitoring data: Data about the operation of tenant-level Azure services, such as Azure Active Directory.

## Custom Sources

- Azure Monitor can collect log data from any REST client using the Data Collector API and Metric API. This allows you to create custom monitoring scenarios and extend monitoring to resources that don't expose telemetry through other sources.
    - Log Analytics Collector API
    - Metrics REST API

# Azure Monitor

### Insights

- Azure Monitor includes several features and tools that provide valuable insights into your applications and other resources that they depend on. Monitoring solutions and features such as VM Insights, Application Insights, and Container Insights provide deep insights into different aspects of your application and specific Azure services.

### Responding to Events

- Alerts in Azure Monitor proactively notify you of critical conditions and potentially attempt to take corrective action. Alert rules based on metrics provide near real time alerting based on numeric values, while rules based on logs allow for complex logic across data from multiple sources.
- Alert rules in Azure Monitor use action groups, which contain unique sets of recipients and actions that can be shared across multiple rules. Based on your requirements, action groups can perform such actions as using webhooks to have alerts start external actions or to integrate with your ITSM tools.

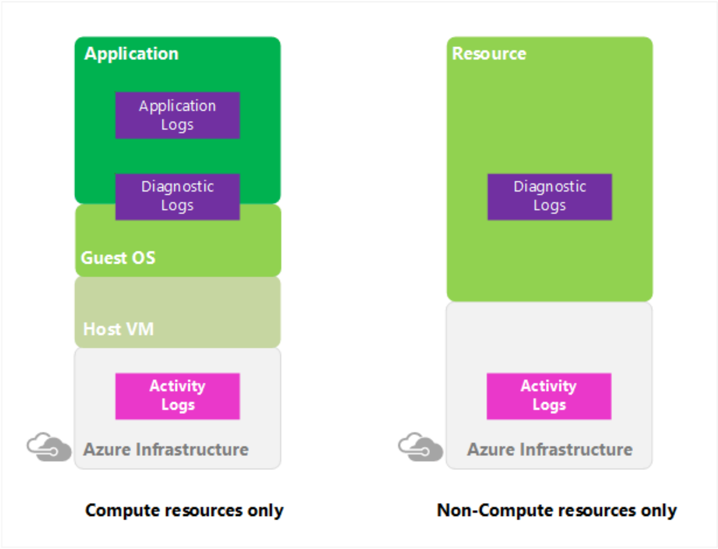
### Integrate and Export

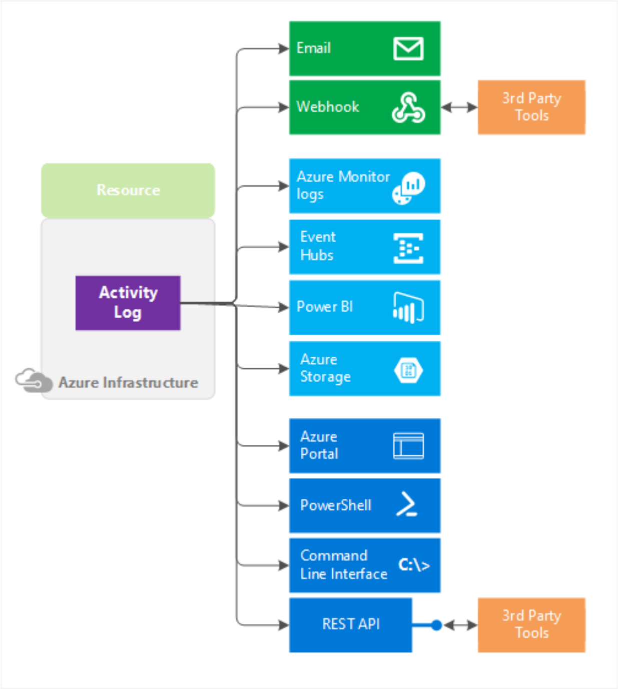
- Other Azure services work with Azure Monitor to provide integration capabilities like Event Hub and Logic Apps as well as Azure Monitor APIs.

# Monitor – Walkthrough

## Walkthroughs

1. Activity Logs
   - PUT, POST, DELETE on any subscription resource, no GETs
   - Operations on the resource: "control plane", Activity Logs
   - Operations of the resource: "data plane", Diagnostic Logs
   - Stored for 90 days, read only
   - Activity Logs Overview, Export Activity Log with Log Profiles
2. Diagnostics Settings
   - Collect diagnostics logs from any resource
3. Metric Alerts, Alert Rules, Action Groups
   - Create CPU alert for VM
4. Metrics
   - Create CPU and IOPS/s charts for VM
5. Service Health
   - Service Issues, Planned Maintenance, Health Advisories, Health History, Resource Health, Health Alerts

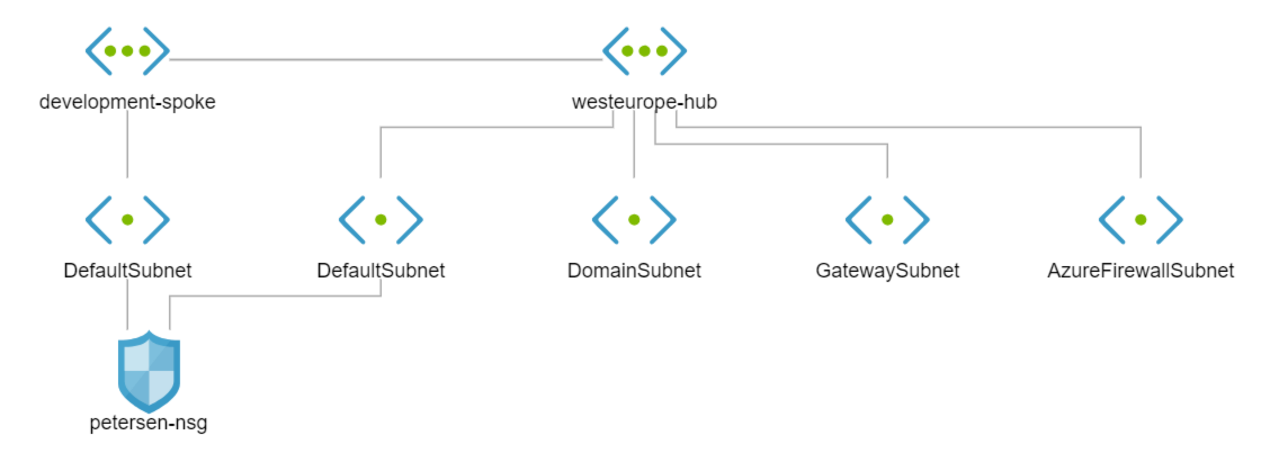


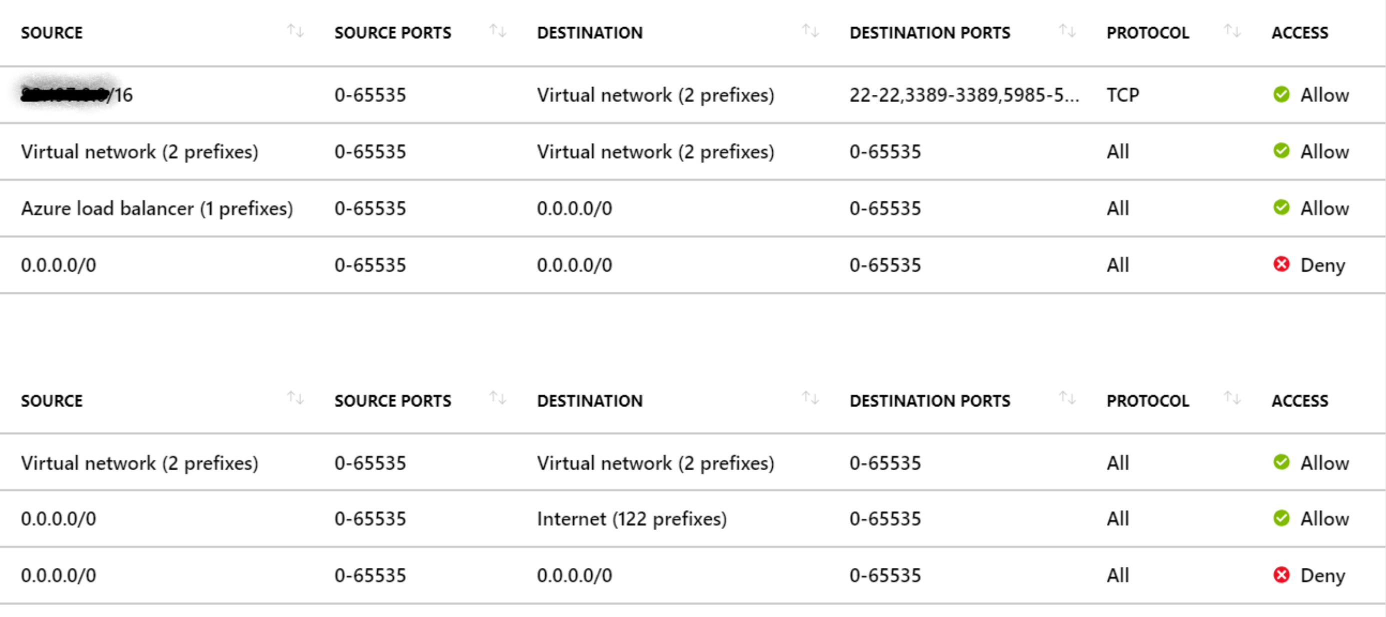


# Network Watcher – Walkthrough

**Walkthroughs**

1. Network Watcher
   - Topology
   - Connection Monitor (e.g. Web -> SQL)
   - IP Flow Verify
   - Next Hop
   - Effective Security Rules
   - Packet Capture





| SOURCE | SOURCE PORTS | DESTINATION | DESTINATION PORTS | PROTOCOL | ACCESS |
|---|---|---|---|---|---|
| [redacted]/16 | 0-65535 | Virtual network (2 prefixes) | 22-22,3389-3389,5985-5... | TCP | ✓ Allow |
| Virtual network (2 prefixes) | 0-65535 | Virtual network (2 prefixes) | 0-65535 | All | ✓ Allow |
| Azure load balancer (1 prefixes) | 0-65535 | 0.0.0.0/0 | 0-65535 | All | ✓ Allow |
| 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | All | ✗ Deny |

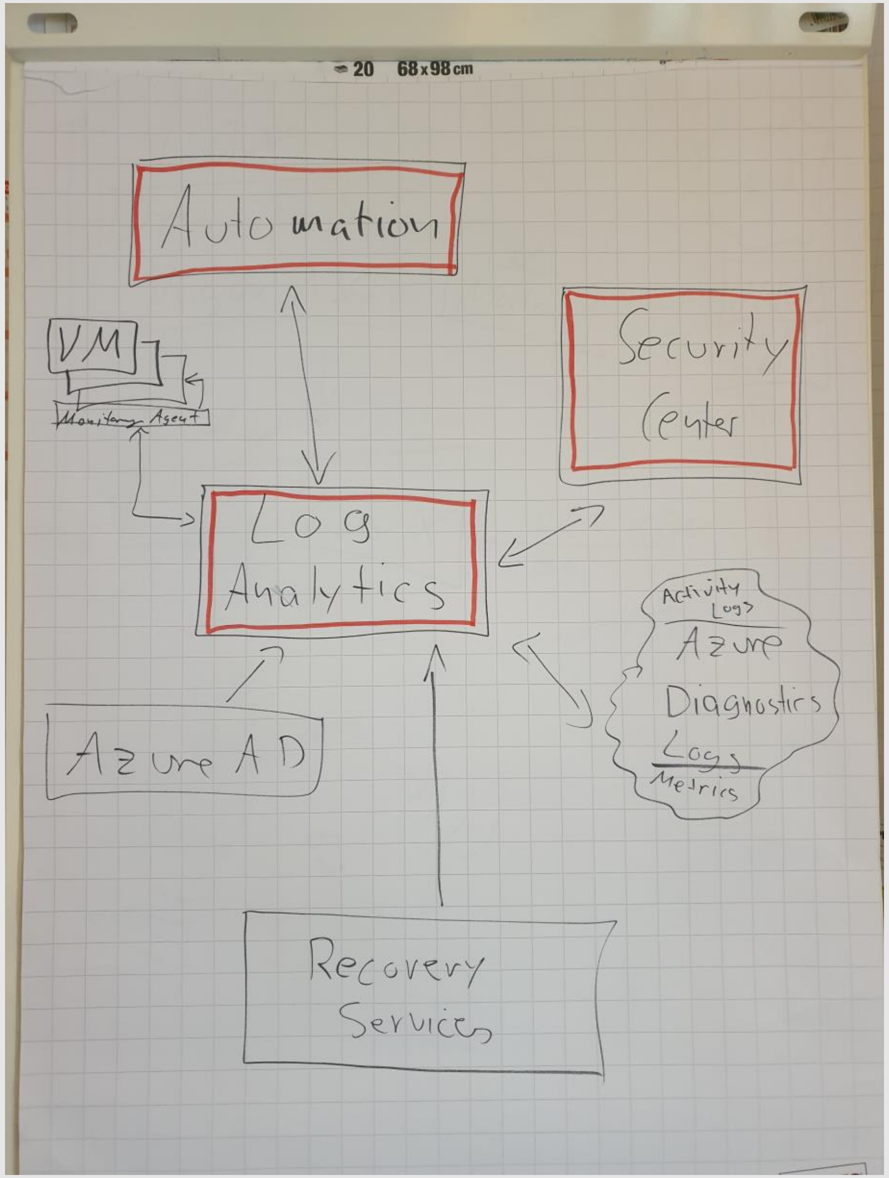
| SOURCE | SOURCE PORTS | DESTINATION | DESTINATION PORTS | PROTOCOL | ACCESS |
|---|---|---|---|---|---|
| Virtual network (2 prefixes) | 0-65535 | Virtual network (2 prefixes) | 0-65535 | All | ✓ Allow |
| 0.0.0.0/0 | 0-65535 | Internet (122 prefixes) | 0-65535 | All | ✓ Allow |
| 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | All | ✗ Deny |

# Log Analytics

# Log Analytics – Walkthrough

**Walkthroughs**

1. Log Analytics
   - Workspace Data Sources
   - Advanced Settings
   - Monitoring Solutions
   - Automation Account
2. Log Alerts & Action Groups
   - Alert on Log Analytics Data
   - Heartbeat | take 1 -> New Alert Rule
3. Automation
   - Inventory
   - Update Management
   - Hybrid Worker Groups
   - Process Automation (Runbooks/Jobs)
   - Runbook Logging
   - Source Control



# Kusto Query Language – Walkthrough

Azure Log Analytics for DBS.txt

## Walkthroughs

1. Kusto Query Language
   - Get started with Queries in Log Analytics
   - More advanced Queries with Log Analytics
   - Kusto Query Language (KQL) Reference

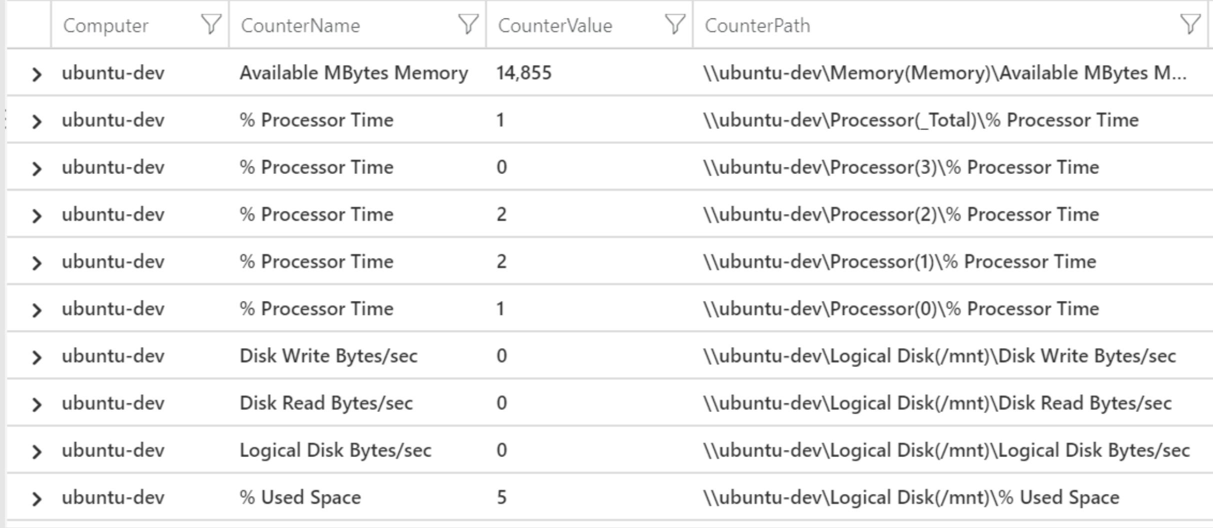
Azure Log Analytics

Azure Application Insights

Windows Defender Advanced Threat Protection

Azure Security Center

2. Log Analytics – Logs Query Window
   - Query Windows: Perf | take 10
   - Schema, Filter
   - Drag ObjectName for „Group By“ + Delete
   - Filter ObjectName for „Processor“ + Clear
   - Select Columns (see on right side)
   - Each Query has unique ID and can be shared
   - Save, Copy, Export, Pin to Dashboard
   - Help, Settings, Samples Queries, Query Explorer



| | Computer | CounterName | CounterValue | CounterPath |
|---|---|---|---|---|
| > | ubuntu-dev | Available MBytes Memory | 14,855 | \\ubuntu-dev\Memory(Memory)\Available MBytes M... |
| > | ubuntu-dev | % Processor Time | 1 | \\ubuntu-dev\Processor(_Total)\% Processor Time |
| > | ubuntu-dev | % Processor Time | 0 | \\ubuntu-dev\Processor(3)\% Processor Time |
| > | ubuntu-dev | % Processor Time | 2 | \\ubuntu-dev\Processor(2)\% Processor Time |
| > | ubuntu-dev | % Processor Time | 2 | \\ubuntu-dev\Processor(1)\% Processor Time |
| > | ubuntu-dev | % Processor Time | 1 | \\ubuntu-dev\Processor(0)\% Processor Time |
| > | ubuntu-dev | Disk Write Bytes/sec | 0 | \\ubuntu-dev\Logical Disk(/mnt)\Disk Write Bytes/sec |
| > | ubuntu-dev | Disk Read Bytes/sec | 0 | \\ubuntu-dev\Logical Disk(/mnt)\Disk Read Bytes/sec |
| > | ubuntu-dev | Logical Disk Bytes/sec | 0 | \\ubuntu-dev\Logical Disk(/mnt)\Logical Disk Bytes/sec |
| > | ubuntu-dev | % Used Space | 5 | \\ubuntu-dev\Logical Disk(/mnt)\% Used Space |

# View Designer – Walkthrough

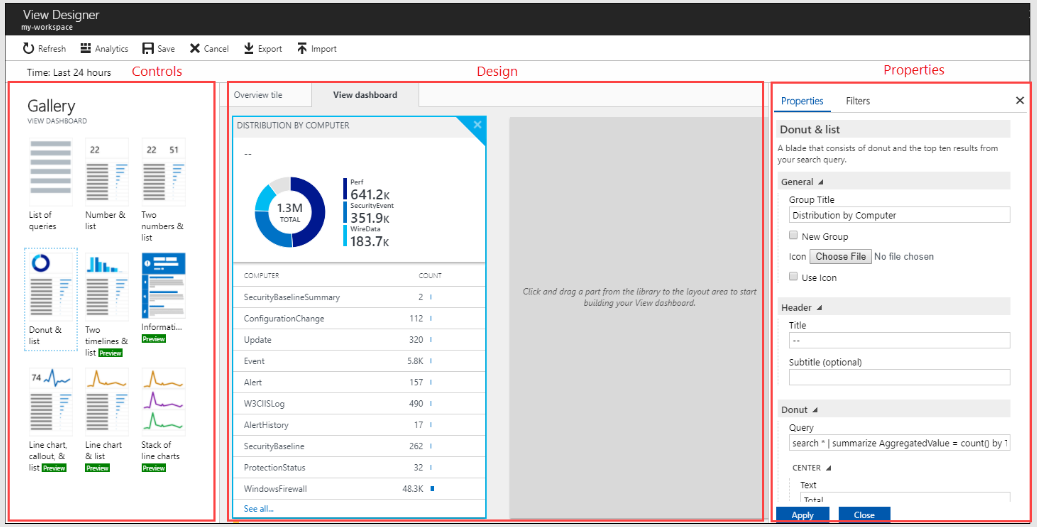
## Walkthroughs

1. Tiles, Views, and Parts
   - Work with View Designer
   - Create a Tile
   - Create a Visualization Part based on a Query
   - Create Filters

Azure Administration.omsview

2. Create Dashboards in the Azure Portal
   - [Create and share dashboards of Log Analytics data](#) based on a query in Logs

```
Perf
| where Computer in (AzureAdministration__ComputerGroup)
| where ObjectName == "Processor" and CounterName == "% Processor Time"
| summarize AverageUtilization = avg(CounterValue) by Computer, Time = bin(TimeGenerated, 1h)
| order by Time asc
| render barchart with (kind = unstacked, title = "Processor Utilization")
```



| COMPUTER | COUNT |
|---|---|
| SecurityBaselineSummary | 2 |
| ConfigurationChange | 112 |
| Update | 320 |
| Event | 5.8K |
| Alert | 157 |
| W3CIISLog | 490 |
| AlertHistory | 17 |
| SecurityBaseline | 262 |
| ProtectionStatus | 32 |
| WindowsFirewall | 48.3K |

See all...

Group Title: Distribution by Computer

□ New Group

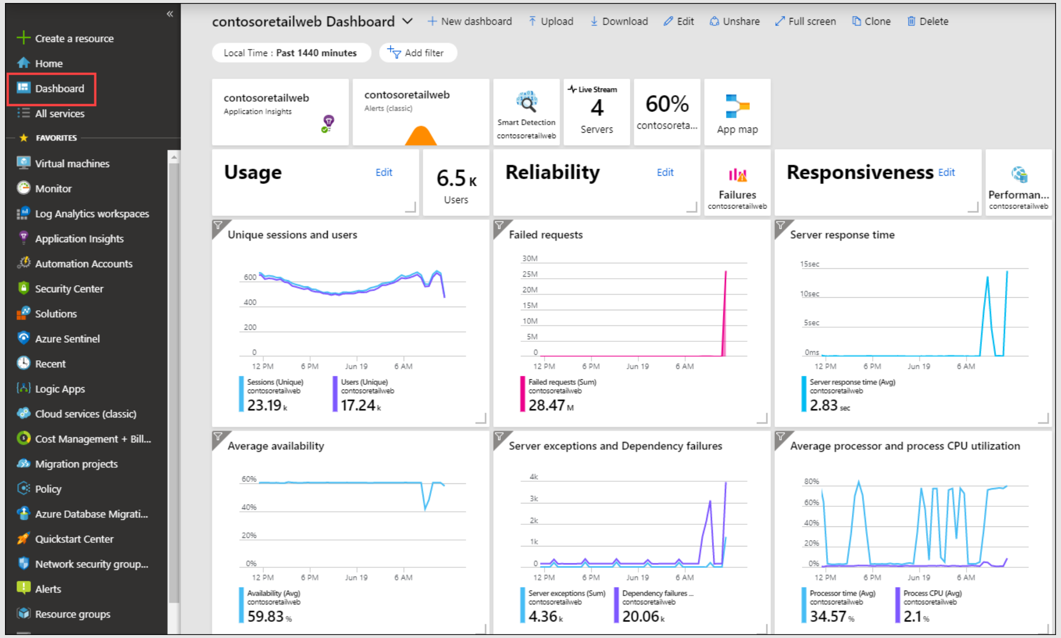
Icon: Choose File No file chosen

□ Use Icon

Title: --

Subtitle (optional)

Query: search * | summarize AggregatedValue = count() by T

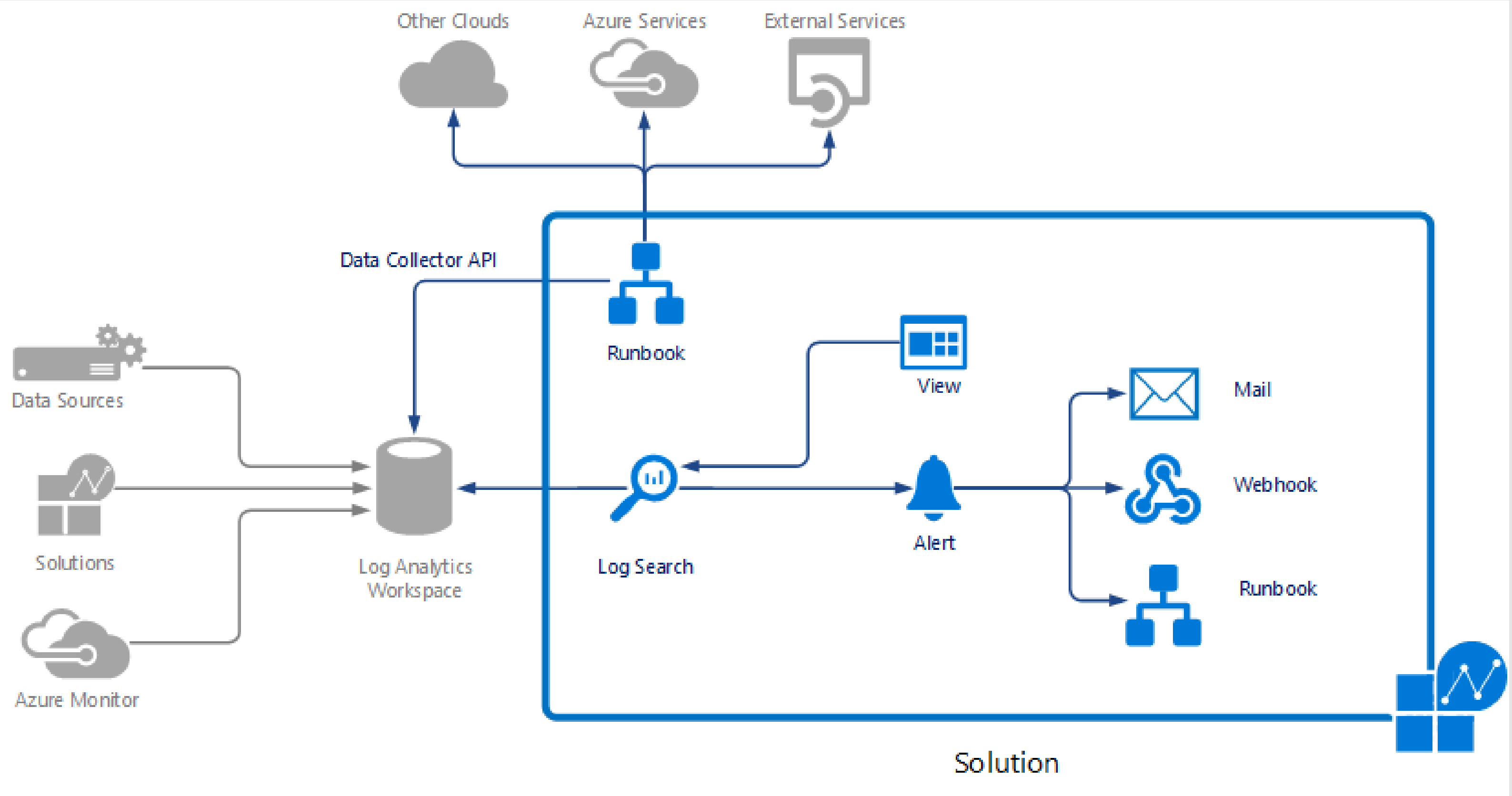


# Log Analytics End-to-End Solution

# Log Analytics – End-To-End Solution

**Guide based on Visual Studio**

1. Empty Solution
    - No contained resources
2. Automation Solution
    - Complex template with referenced and contained solution resources
3. Views Solution
    - Simple template that deploys a view as contained solution resource
4. Collector Solution
    - Template contains runbook for custom data ingestion with the [Data Collector API]
    - Read [Best Practices for Monitoring Solutions]



# Microsoft Azure

Productive + Hybrid + Intelligent + Trusted