

Monitor Windows Server Using Azure Services



Tim Warner

Microsoft Azure Solutions Architect

@TechTrainerTim TechTrainerTim.com



Overview



**Monitor Azure Virtual Machines by using
Azure Diagnostics extension**

Deploy Log Analytics agents

Collect performance counters to Azure

Create alerts

**Monitor Azure Virtual Machines
performance by using VM insights**



Windows Server 2022: Monitor and Troubleshoot Server Environments

Monitor Windows Server Using Local Tools

Monitor Windows Server Using Azure Services

Troubleshoot Windows Server Hybrid Networking

Troubleshoot Windows Server VM Deployment Failures

Troubleshoot Windows Server VM Connection Issues

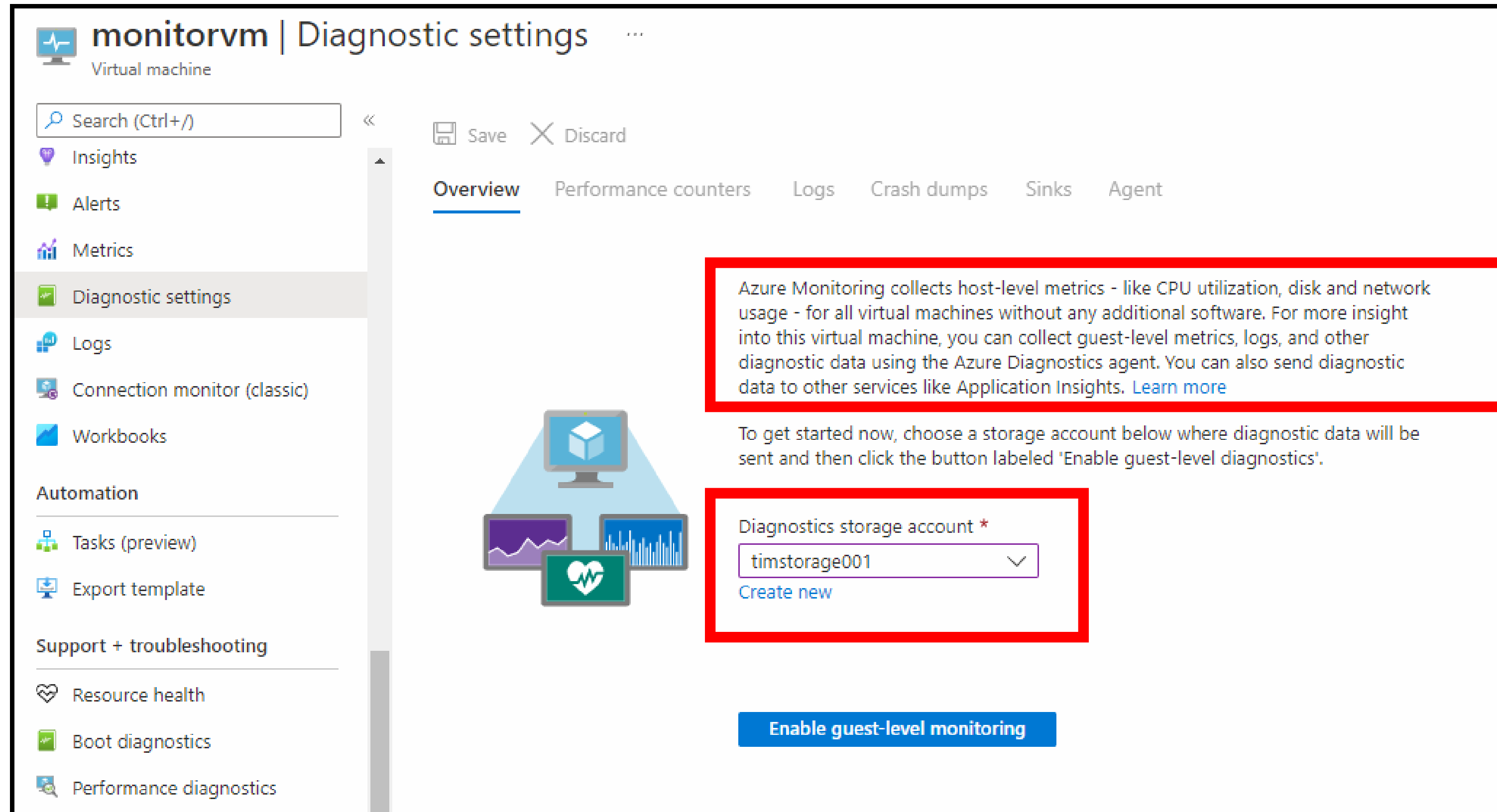
Troubleshoot Active Directory



Azure VM Diagnostics Extension



Azure Diagnostics Extension



The screenshot shows the 'monitorvm | Diagnostic settings' page for a virtual machine. The left sidebar contains navigation links: Insights, Alerts, Metrics, Diagnostic settings (highlighted), Logs, Connection monitor (classic), Workbooks, Automation (Tasks (preview), Export template), and Support + troubleshooting (Resource health, Boot diagnostics, Performance diagnostics). The main content area has tabs for Overview, Performance counters, Logs, Crash dumps, Sinks, and Agent. The Overview tab is active, displaying a diagram of a VM connected to monitoring components. A red box highlights a text block explaining that Azure Monitoring collects host-level metrics (CPU, disk, network) for all VMs without additional software, and that guest-level metrics can be collected using the Azure Diagnostics agent. Another red box highlights a dropdown menu for 'Diagnostics storage account' with 'timstorage001' selected and a 'Create new' link. A blue button labeled 'Enable guest-level monitoring' is at the bottom.

monitorvm | Diagnostic settings ...
Virtual machine

Search (Ctrl+ /)

Save Discard

Overview Performance counters Logs Crash dumps Sinks Agent

Azure Monitoring collects host-level metrics - like CPU utilization, disk and network usage - for all virtual machines without any additional software. For more insight into this virtual machine, you can collect guest-level metrics, logs, and other diagnostic data using the Azure Diagnostics agent. You can also send diagnostic data to other services like Application Insights. [Learn more](#)

To get started now, choose a storage account below where diagnostic data will be sent and then click the button labeled 'Enable guest-level diagnostics'.

Diagnostics storage account *

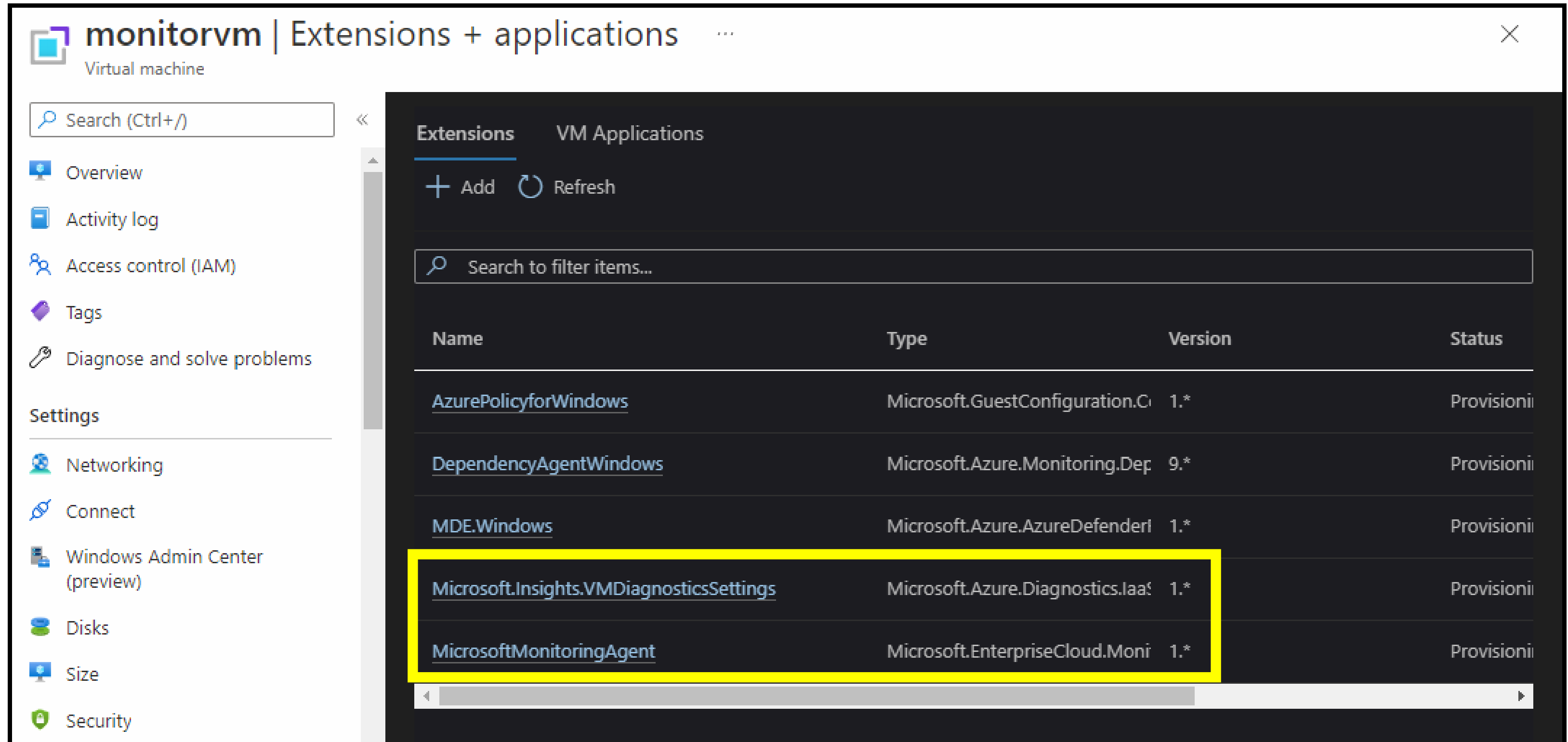
timstorage001

Create new

Enable guest-level monitoring



Azure Diagnostics Extension



monitorvm | Extensions + applications

Virtual machine

Search (Ctrl+ /)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Windows Admin Center (preview)
- Disks
- Size
- Security

Extensions VM Applications

+ Add ↻ Refresh

Search to filter items...

Name	Type	Version	Status
AzurePolicyforWindows	Microsoft.GuestConfiguration.C	1.*	Provisioni
DependencyAgentWindows	Microsoft.Azure.Monitoring.Dep	9.*	Provisioni
MDE.Windows	Microsoft.Azure.AzureDefenderI	1.*	Provisioni
Microsoft.Insights.VMDiagnosticsSettings	Microsoft.Azure.Diagnostics.Iaa	1.*	Provisioni
MicrosoftMonitoringAgent	Microsoft.EnterpriseCloud.Moni	1.*	Provisioni



Azure Diagnostics Extension

monitorvm | Diagnostic settings

Virtual machine

Search (Ctrl+ /)

monitoring

Insights

Alerts

Metrics

Diagnostic settings

Logs

Connection monitor (classic)

Workbooks

Automation

Tasks (preview)

Export template

Support + troubleshooting

Resource health

Boot diagnostics

Performance diagnostics

Reset password

Redeploy + reapply

Save Discard

Overview Performance counters Logs Crash dumps Sinks Agent

Choose **Basic** to enable the collection of performance counters. Choose **Custom** if you want more control over which performance counters are collected.

None Basic Custom

Configure the performance counters to collect, and how often they should be sampled:

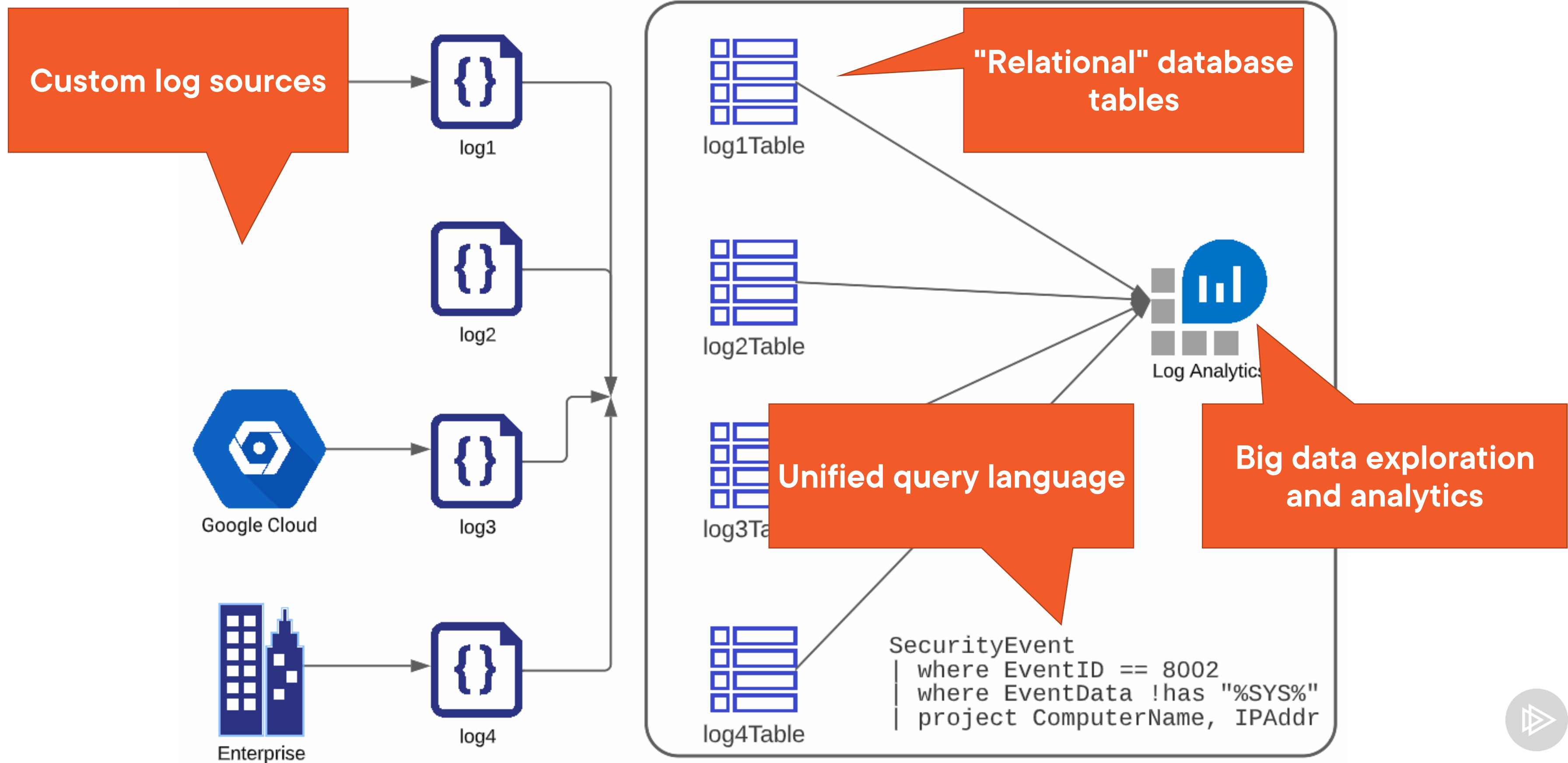
Performance counter	Sample rate (seconds)	Unit
<input checked="" type="checkbox"/> \Processor Information(_Total)\% Processor Time	60	Percent
<input checked="" type="checkbox"/> \Processor Information(_Total)\% Privileged Time	60	Percent
<input checked="" type="checkbox"/> \Processor Information(_Total)\% User Time	60	Percent
<input checked="" type="checkbox"/> \Processor Information(_Total)\Processor Frequency	60	Count
<input checked="" type="checkbox"/> \System\Processes	60	Count
<input checked="" type="checkbox"/> \Process(_Total)\Thread Count	60	Count
<input checked="" type="checkbox"/> \Process(_Total)\Handle Count	60	Count
<input checked="" type="checkbox"/> \System\System Up Time	60	Count
<input checked="" type="checkbox"/> \System\Context Switches/sec	60	CountPerSecond
<input checked="" type="checkbox"/> \System\Processor Queue Length	60	Count



Log Analytics Agent



Log Analytics Architecture



Log Analytics Agent

Naming confusion

- OMS Agent
- Microsoft Monitoring Agent (MMA)
- Log Analytics Agent
- Azure Monitor Agent (AMA)

Scope

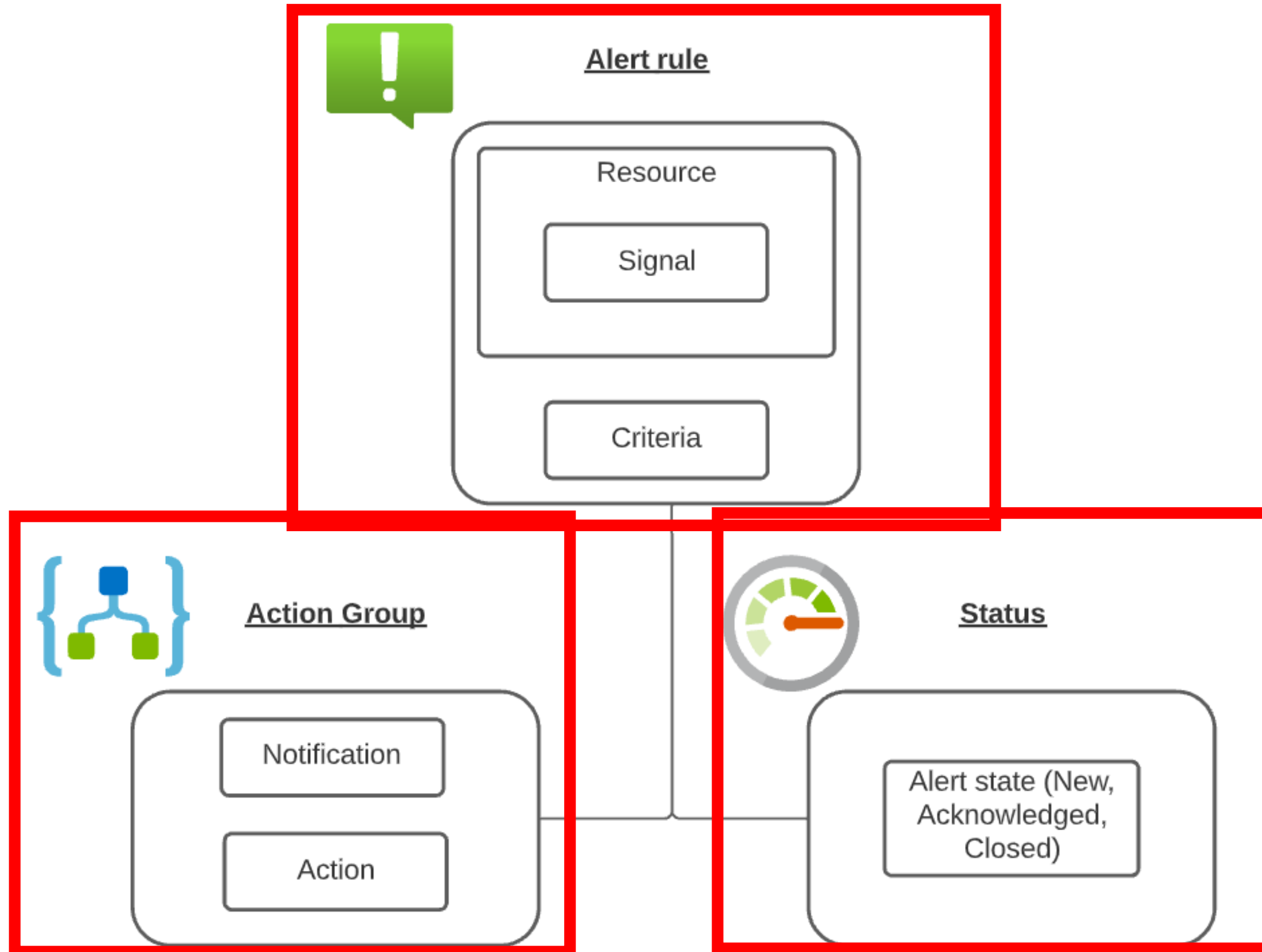
- Azure VMs (Windows and Linux)
- VMs in other clouds
- Physical and virtual machines on-premises

Deployment

- ARM/Bicep template
- Manually
- SCCM
- Azure Policy
- Arc-enabled server



Azure Alert Object Model



Action Group Options

**Email/SMS
notification**

Push notification

**Automation
runbook**

Function/Logic app

ITSM ticket

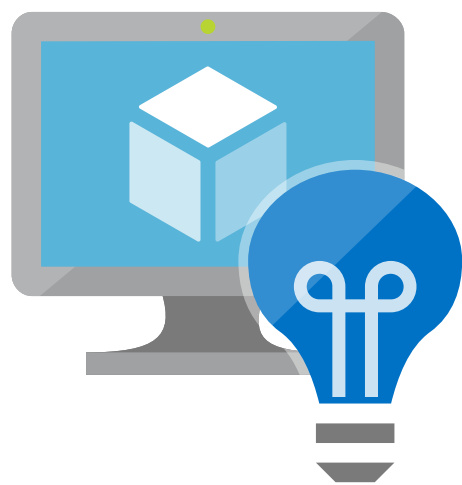
HTTP(S) webhook



Azure Monitor VM Insights



Azure Monitor VM Insights



Insights: Curated monitoring views for specific Azure resources

Workbook model

Requires Log Analytics workspace

Reports on Windows and Linux machines in a hybrid-, multi-cloud environment

- Guest health extension available for Azure VMs only as of summer 2022



Azure Monitor Workbooks

Monitor | Workbooks | Key Metrics

Microsoft

Search (Ctrl+ /)

Overview

Activity log

Alerts

Metrics

Logs

Service Health

Workbooks

Insights

Applications

Virtual Machines

Storage accounts

Containers

Networks

SQL (preview)

Azure Cosmos DB

Workbooks Edit Save Refresh Add Favorite Smile Help Auto refresh: Off

Subscription

Virtual Machines

Time Range

Microsoft Azure Sponsorship

2 selected

Last hour

2 / 2

Virtual machines

Overview

Key metrics

Regions

Resource health

Search

Subscription

Percentage CPU...

Percentage CPU Timeline

Disk Read Bytes ...

Disk Write Bytes.

Microsoft Azure Sponsorship (2)

monitorvm

2.7%

85.2MiB

246.2MiB

tim-vm-01



Demo



1

Log Analytics onboarding

Manual

Arc

KQL

Log search alert

VM Insights

Onboarding



Summary



Learning KQL is not optional

- Microsoft cert exams
- Your career

Workbooks can greatly shorten your learning curve

Lead: Our team needs to monitor Azure virtual networks, but they aren't yet strong on networking



Up Next:

Troubleshoot Windows Server Hybrid
Networking

