

Microsoft Azure Administrator: Monitor Resources with Azure Monitor

CONFIGURING MICROSOFT AZURE RESOURCE MONITORING



Tim Warner

AUTHOR EVANGELIST, PLURALSIGHT

@TechTrainerTim TechTrainerTim.com



Overview



Configure diagnostic settings

Configure and interpret metrics

- Analyze metrics across subscriptions















Analyze alerts across subscriptions

Implement a Log Analytics workspace

Configure Application Insights



Exercise Files



What do you want to learn?

Timothy
timothywarner316@gmail.com

Troubleshooting with Microsoft Azure Network Watcher

by Tim Warner

Microsoft now gives you packet-level access to your Windows Server and Linux virtual machines (VMs) running in Azure. You'll learn how to use Network Watcher to troubleshoot network security groups (NSGs), perform packet captures, and much more.

[Resume Course](#) [Bookmark](#) [Add to Channel](#)

Table of contents

Description

Transcript

Exercise files

Discussion


Learning Check

Recommended

These exercise files are intended to provide you with the assets you need to create a video-based hands-on experience. With the exercise files, you can follow along with the author and re-create the same solution on your computer. We find this to be even more effective than written lab exercises.

[Download exercise files](#)

Course author

**Tim Warner**

Timothy Warner is a Microsoft Most Valuable Professional (MVP) in Cloud and Datacenter Management who is based in Nashville, TN.

Course info

Level	Intermediate
Rating	★★★★★
My rating	★★★★★
Duration	2h 12m
Released	31 Oct 2017

Share course

[f](#) [t](#) [g+](#) [in](#)



Exercise Files

The screenshot displays a Windows desktop environment with three overlapping windows:

- File Explorer (Left):** Shows the 'Downloads' folder. A list of folders is visible, with '02' selected. The status bar at the bottom indicates '0 / 5 object(s) selected'.
- Text Editor (Center):** A Notepad window titled 'microsoft-azure-ad-privileged-identity-management-configuring-m4-links.txt'. It contains a list of 22 numbered items, each consisting of a title and a URL. The status bar at the bottom shows 'Spaces: 4 UTF-8 CRLF Plain Text'.
- File Download Window (Right):** A small window showing a file named '02\demos\' with a size of 1,298 bytes and a package size of 359 bytes.

The text editor content is as follows:

```
1 Module 4: Organize and Perform Azure AD PIM Access Reviews
2
3 Microsoft Azure
4 https://azure.microsoft.com/en-us/
5
6 Azure Documentation
7 https://docs.microsoft.com/en-us/azure/
8
9 Azure AD Privileged Identity Management (PIM) documentation | Microsoft Docs
10 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/
11
12 Identity Governance - Azure Active Directory | Microsoft Docs
13 https://docs.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview
14
15 Create an access review of Azure resource roles in PIM - Azure Active Directory | Microsoft Docs
16 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-start-access-review
17
18 Review access to Azure AD roles in PIM - Azure Active Directory | Microsoft Docs
19 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-perform-security-review
20
21 View audit history for Azure AD roles in PIM - Azure Active Directory | Microsoft Docs
22 https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-use-audit-log
```



Microsoft Azure Administrator

Objective
Domain

Exam AZ-104: Microsoft Azure Administrator – Skills Measured

Monitor and back up Azure resources (10-15%)

Functional Group

Objective

Monitor resources by using Azure Monitor

- configure and interpret metrics
 - analyze metrics across subscriptions
- configure Log Analytics
 - implement a Log Analytics workspace
 - configure diagnostic settings
- query and analyze logs
 - create a query
 - save a query to the dashboard
 - interpret graphs
- set up alerts and actions
 - create and test alerts
 - create action groups
 - view alerts in Azure Monitor
 - analyze alerts across subscriptions
- configure Application Insights
- NOT: Network monitoring

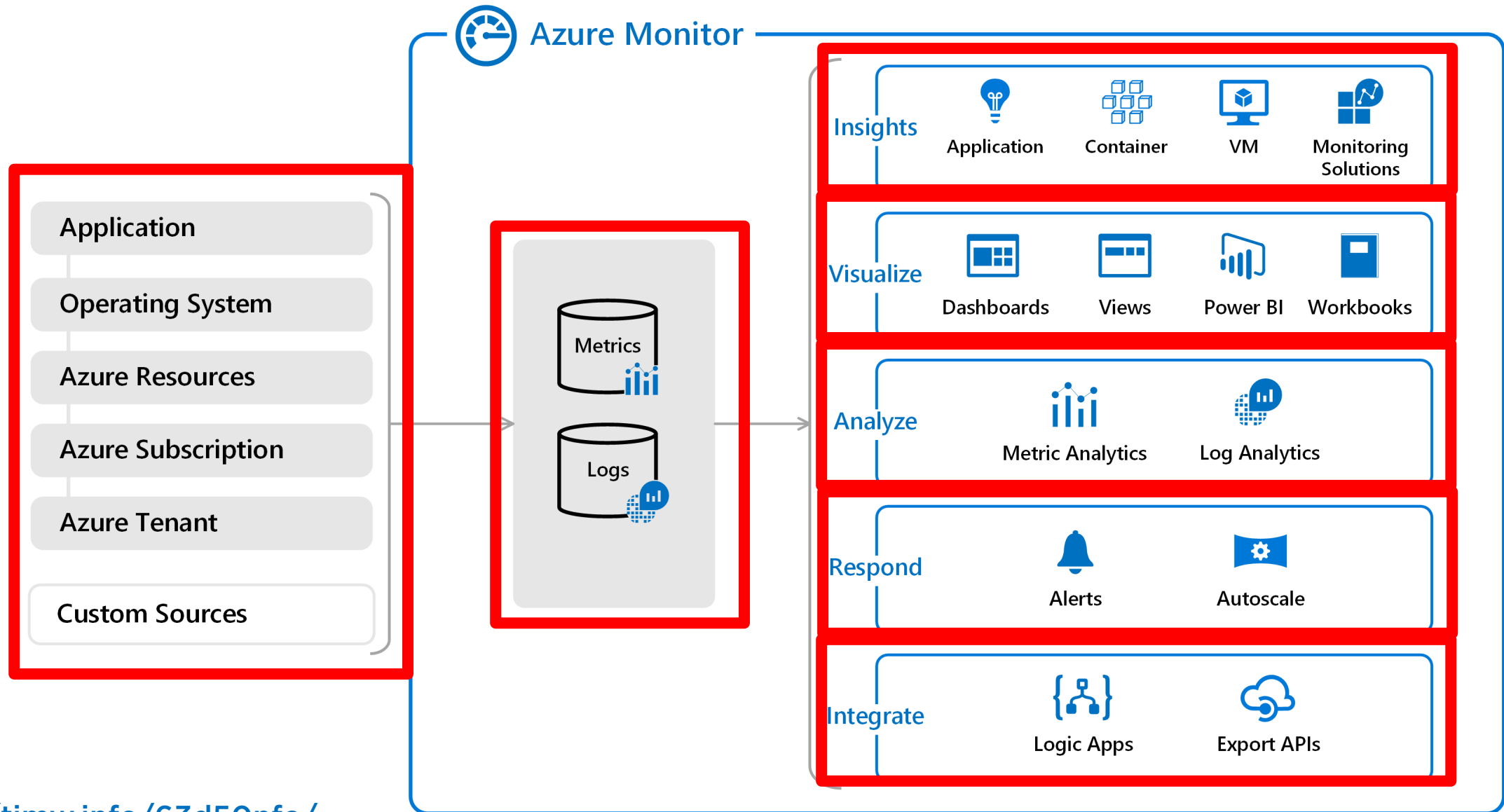
Skills



Diagnostic Settings



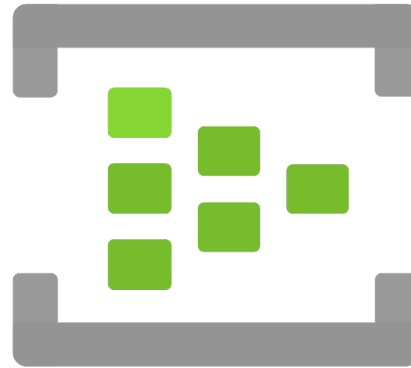
Azure Monitor Data Sources



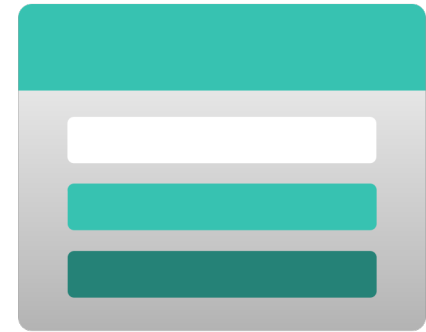
Diagnostic Settings - Logs and Metrics



Log Analytics
workspace



Event Hub



Storage account



Enable Diagnostics - Azure PowerShell

```
Set-AzDiagnosticSetting -Name KeyVault-Diagnostics `
  -ResourceId /subscriptions/.../Microsoft.KeyVault/vaults/mykeyvault `
  -Category AuditEvent -MetricCategory AllMetrics -Enabled $true `
  -StorageAccountId /.../Microsoft.Storage/storageAccounts/mystorageaccount `
  -WorkspaceId /.../workspaces/myworkspace `
  -EventHubAuthorizationRuleId /.../RootManageSharedAccessKey
```



Azure Virtual Machine Agents



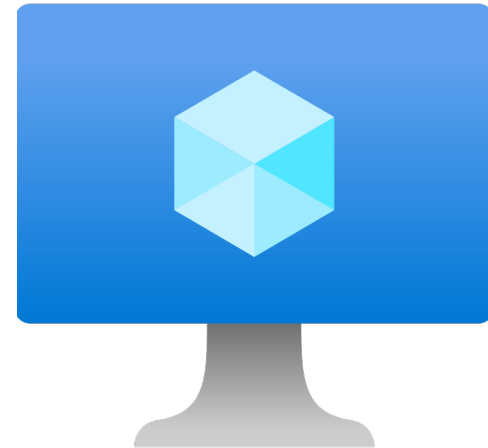
VM Diagnostics extension



Log Analytics agent



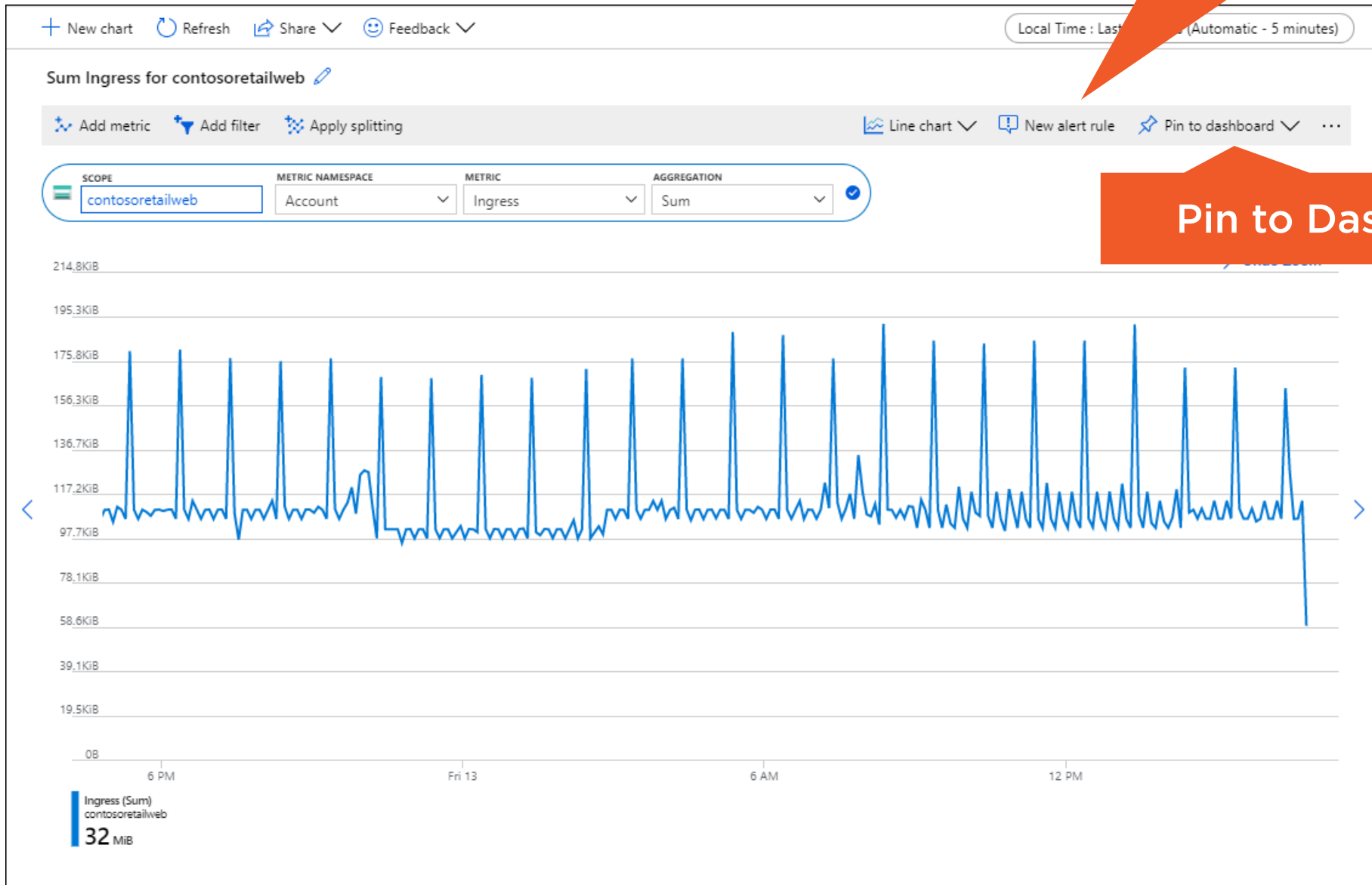
Dependency agent



Metrics Explorer

Raise alerts

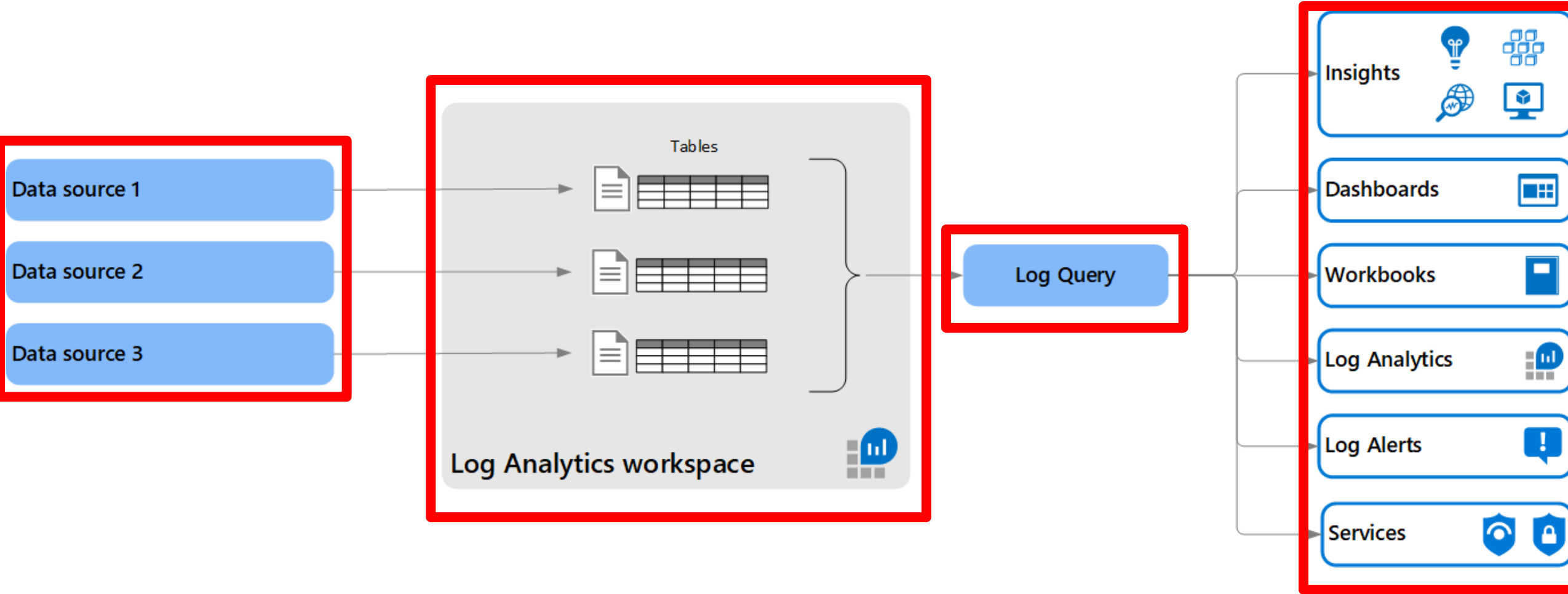
Pin to Dashboard



Log Analytics



Azure Log Analytics (Azure Monitor Logs)



Kusto Query Language (KQL)

```
let StartTime = now()-5d;
```

```
let EndTime = now()-4d; //comment
```

```
Perf
```

```
| where CounterName == "% Processor Time"
```

```
| where TimeGenerated > StartTime and TimeGenerated < EndTime
```

```
| project TimeGenerated, Computer, cpu=CounterValue
```

```
| join kind= inner (
```

```
    Perf
```

```
        | where CounterName == "% Used Memory"
```

```
        | where TimeGenerated > StartTime and TimeGenerated < EndTime
```

```
        | project TimeGenerated , Computer, mem=CounterValue
```

```
) on TimeGenerated, Computer
```

```
| summarize avgCpu=avg(cpu), maxMem=max(mem) by TimeGenerated bin=30m
```

Variable

Comment

Table

Clause

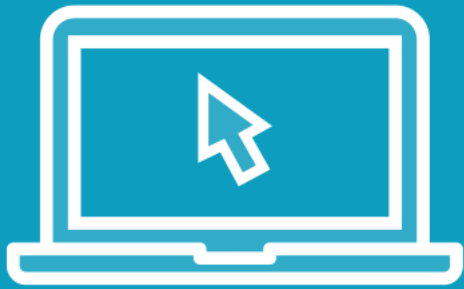
Join

Calculations

Table/chart output



Demo



1

Enable diagnostics

View metrics

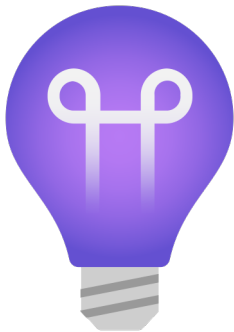
Review alerts



Application Insights



Application Insights



Application Performance Management (APM) service

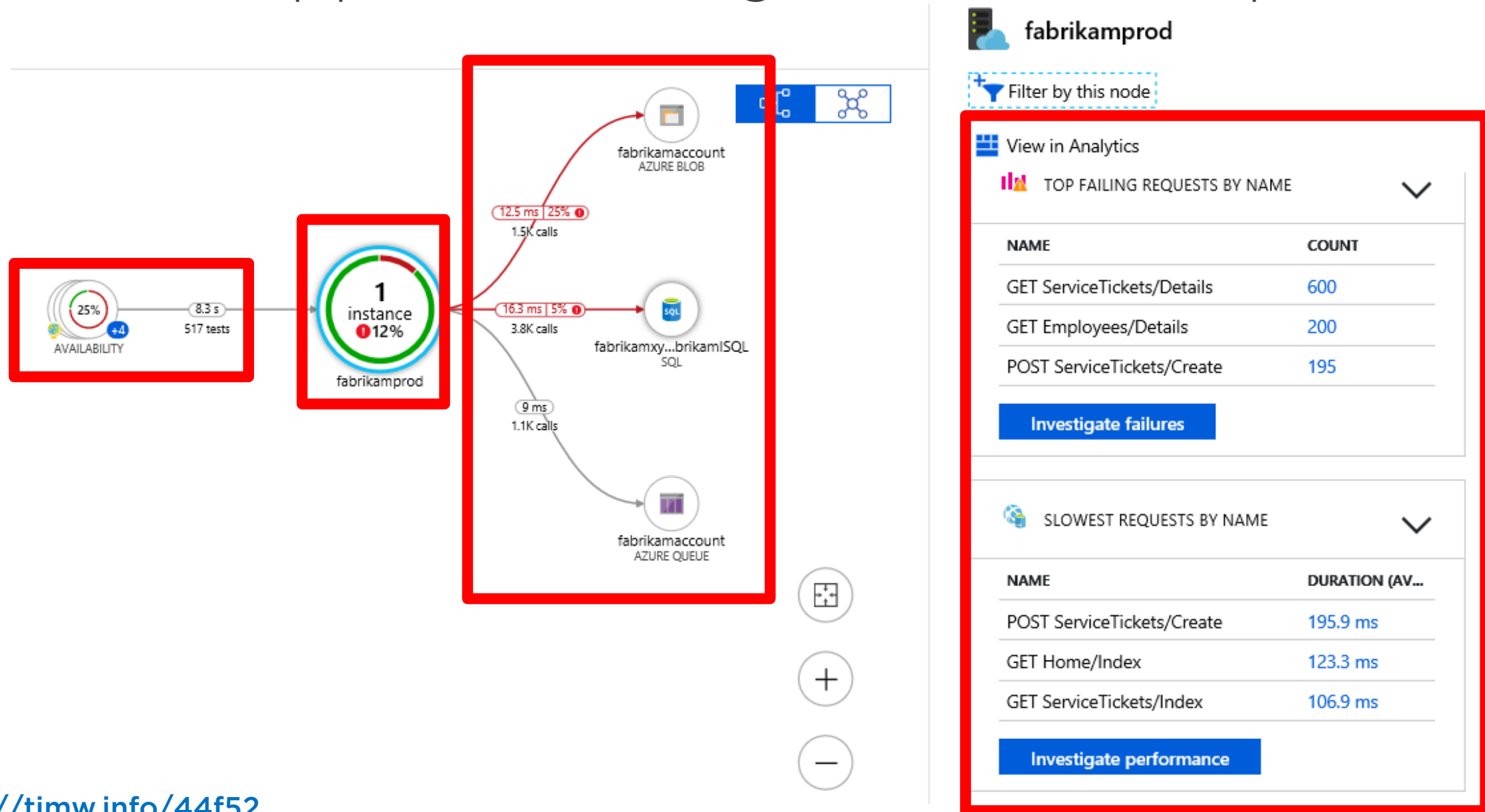
Visualize application performance

- Host telemetry
- Dependencies
- User behavior
- Performance anomalies

Web tests with synthetic transactions



Application Insights Service Map



Demo



2

Enable App Insights

- Visual Studio
- Portal



Summary



Spend time leveling up your KQL skills

- Log Analytics is the future of Azure monitoring

Send your custom log data into your Log Analytics workspace

Use Azure Monitor alerting to automate notification and remediation

Next module: Monitoring and Reporting on Microsoft Azure Resources

