Microsoft

Introduction to Azure Monitor and Log Analytics

John Deardurff

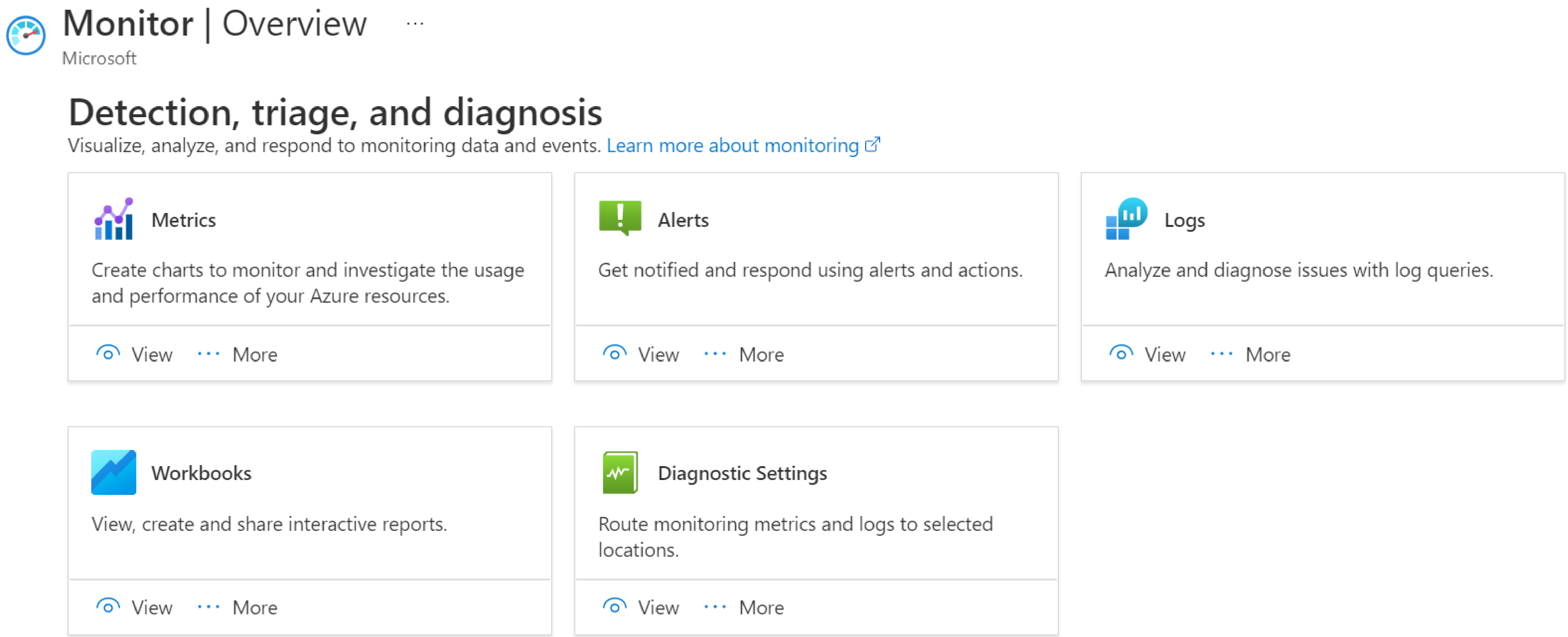
What does this session cover?

- What is Azure Monitor?
- Azure Monitor Metrics
- Azure Monitor Alerts
- Azure Monitor Logs
- Demonstration

Microsoft

Azure Monitor Metrics and Alerts

Azure Monitor



Monitor | Overview ...

Microsoft

Detection, triage, and diagnosis

Visualize, analyze, and respond to monitoring data and events. Learn more about monitoring

Metrics

Create charts to monitor and investigate the usage and performance of your Azure resources.

View ··· More

Alerts

Get notified and respond using alerts and actions.

View ··· More

Logs

Analyze and diagnose issues with log queries.

View ··· More

Workbooks

View, create and share interactive reports.

View ··· More

Diagnostic Settings

Route monitoring metrics and logs to selected locations.

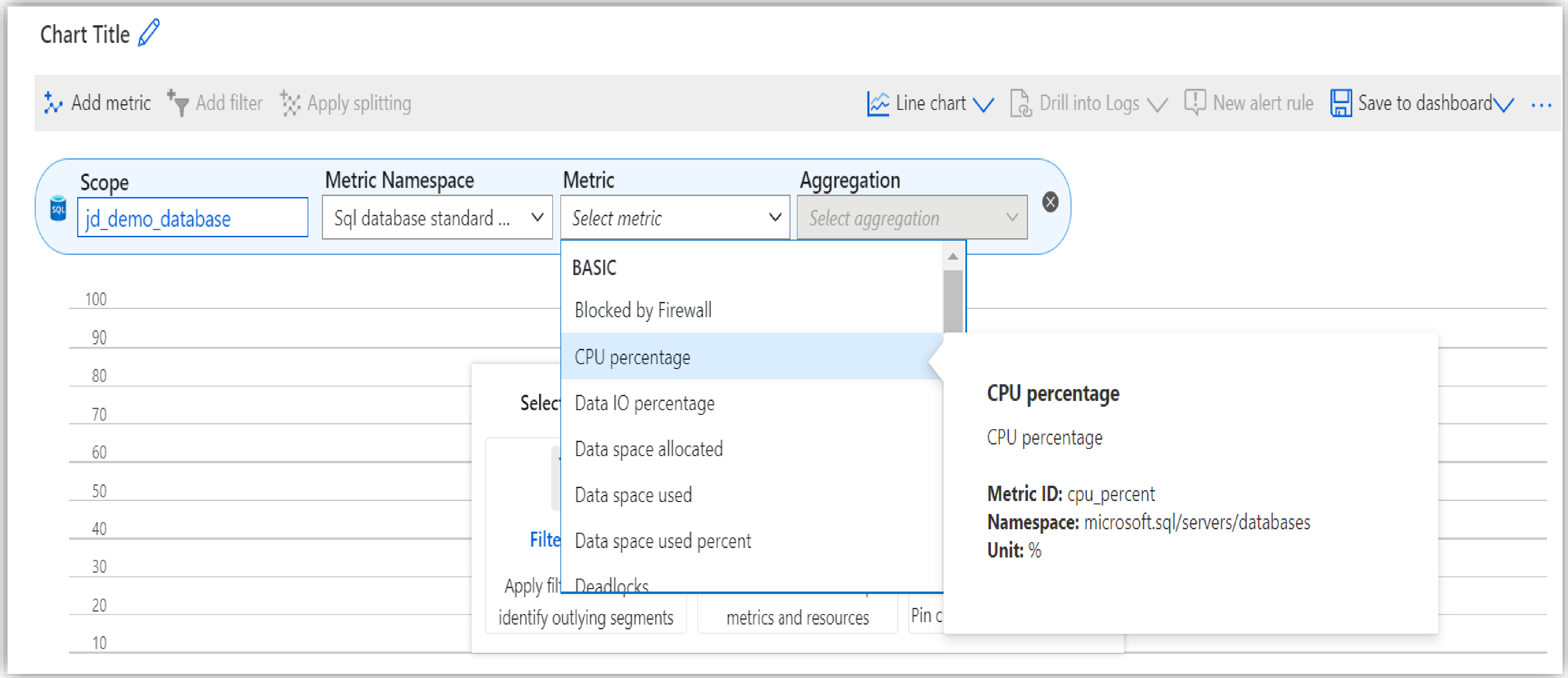
View ··· More

Azure Monitor Metrics

Azure Monitor Metrics stores numeric data in a time-series database, which makes this data more lightweight than Azure Monitor Logs and capable of supporting near real-time scenarios making them particularly useful for alerting and fast detection of issues

- Low-Latency
- Retention – 90 days
- Cost – Free

Azure Monitor Metrics



Scope: jd_demo_database

Metric Namespace: Sql database standard ...

Metric: Select metric

Aggregation: Select aggregation

CPU percentage

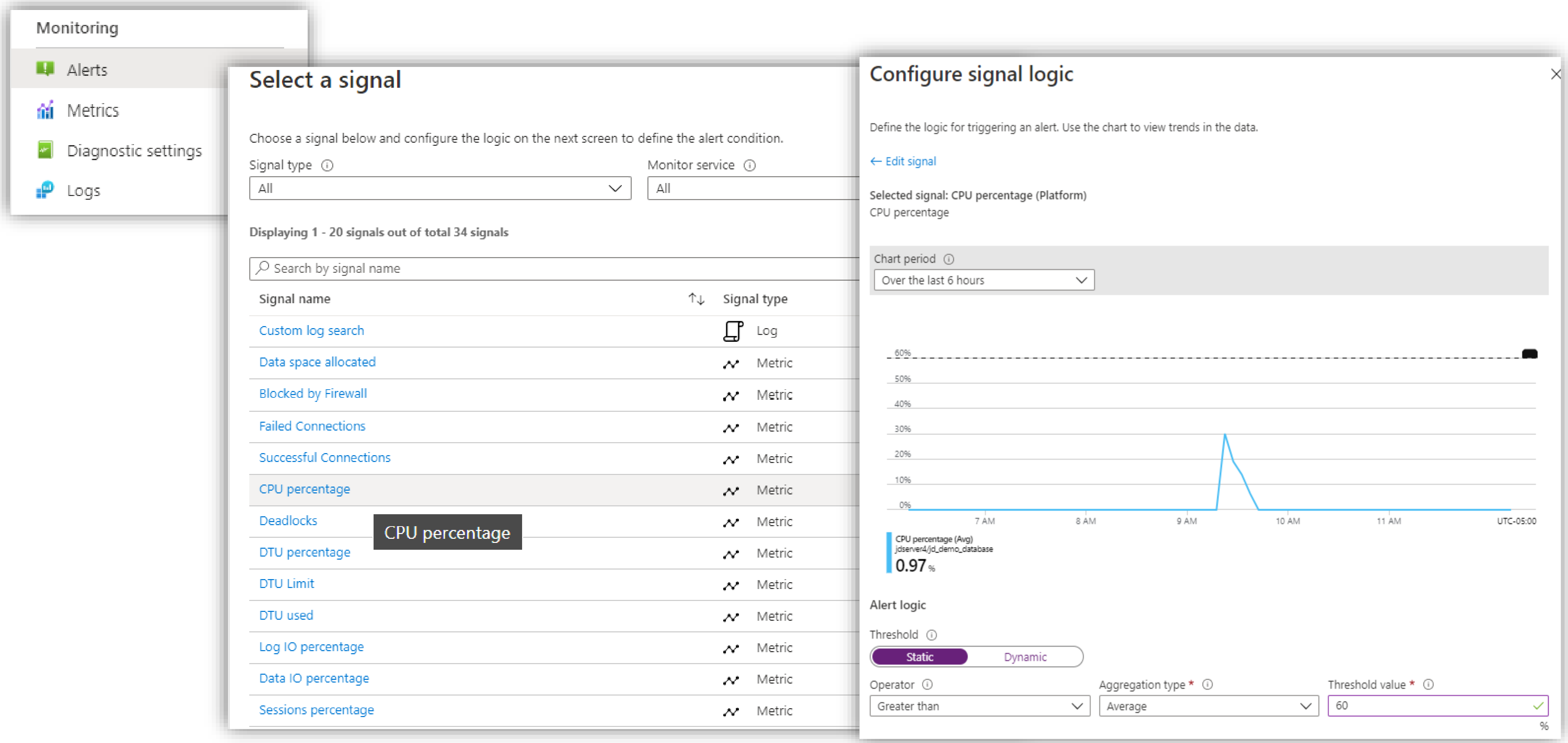
CPU percentage

Metric ID: cpu_percent
Namespace: microsoft.sql/servers/databases
Unit: %

Azure Monitor Metrics

Metric Name	Aggregation Type	Minimum Alert Time Window
CPU percentage	Average	5 minutes
Data IO percentage	Average	5 minutes
Log IO percentage	Average	5 minutes
DTU percentage	Average	5 minutes
Total database size	Maximum	30 minutes
Successful Connections	Total	10 minutes
Failed Connections	Total	10 minutes
Blocked by Firewall	Total	10 minutes
Deadlocks	Total	10 minutes
Database size percentage	Maximum	30 minutes
In-Memory OLTP storage percent(Preview)	Average	5 minutes
Workers percentage	Average	5 minutes
Sessions percent	Average	5 minutes
DTU limit	Average	5 minutes
DTU used	Average	5 minutes

Azure Monitor Alerts - Conditions



Select a signal

Choose a signal below and configure the logic on the next screen to define the alert condition.

Signal type: All

Monitor service: All

Displaying 1 - 20 signals out of total 34 signals

Search by signal name

Signal name	Signal type
Custom log search	Log
Data space allocated	Metric
Blocked by Firewall	Metric
Failed Connections	Metric
Successful Connections	Metric
CPU percentage	Metric
Deadlocks	Metric
DTU percentage	Metric
DTU Limit	Metric
DTU used	Metric
Log IO percentage	Metric
Data IO percentage	Metric
Sessions percentage	Metric

CPU percentage

Configure signal logic

Define the logic for triggering an alert. Use the chart to view trends in the data.

← Edit signal

Selected signal: CPU percentage (Platform)
CPU percentage

Chart period: Over the last 6 hours

Alert logic

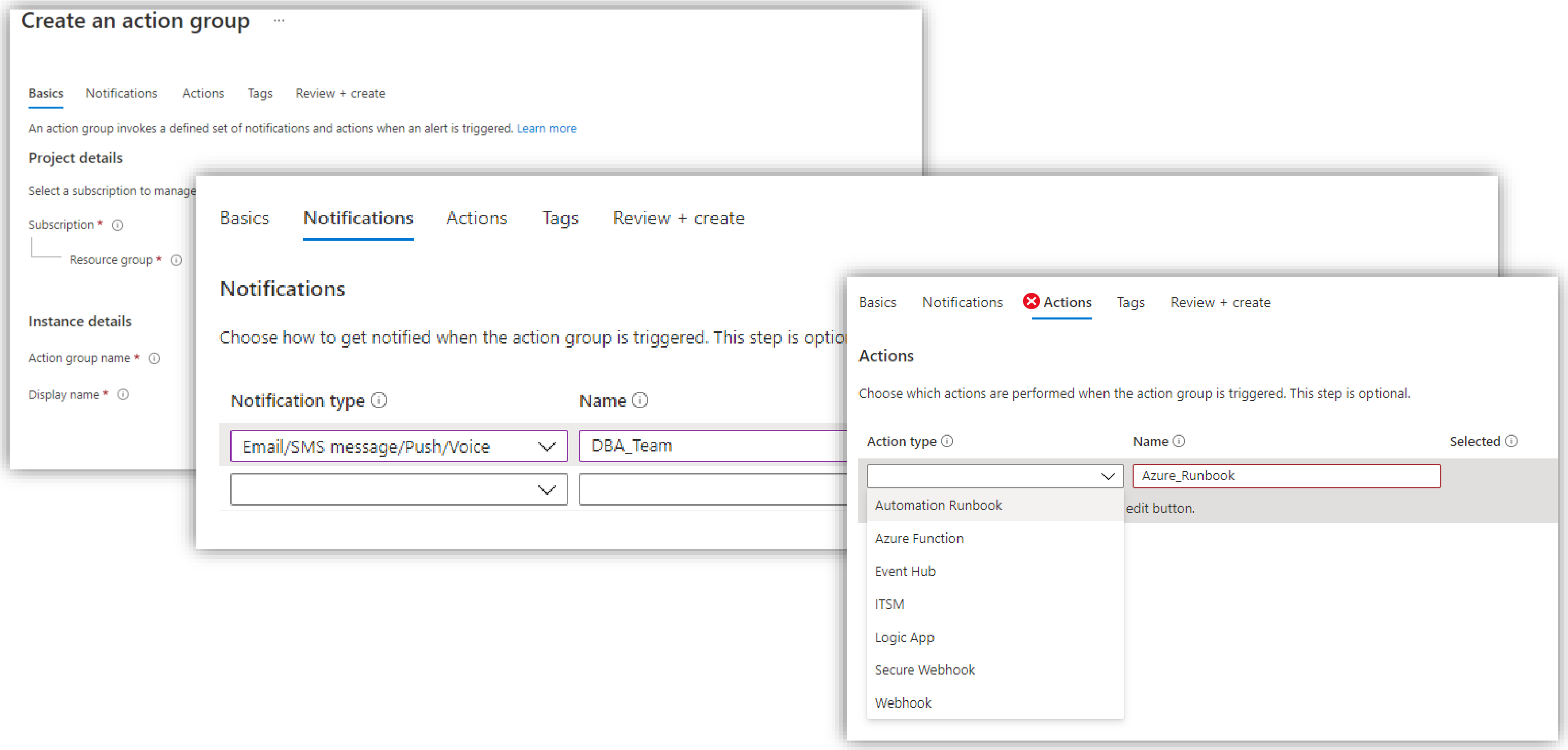
Threshold: [✓ Static] Dynamic

Operator: Greater than

Aggregation type *: Average

Threshold value *: 60 %

Azure Monitor Alerts – Action Groups



An action group invokes a defined set of notifications and actions when an alert is triggered. Learn more

Project details

Select a subscription to manage

Subscription *

Resource group *

Instance details

Action group name *

Display name *

Notifications

Choose how to get notified when the action group is triggered. This step is optio

Notification type: Email/SMS message/Push/Voice

Name: DBA_Team

Actions

Choose which actions are performed when the action group is triggered. This step is optional.

Action type

Name: Azure_Runbook

Selected

edit button.

Azure Dashboards

Customizable

Pin:

- Resources
- Metrics
- Log analytics charts
- Text boxes

Private or shared

Back-up or copy

- Download JSON – save for backup purposes
- Replace references from one server/database to the other
- Upload as new dashboard

Demonstration Time

Azure Log Analytics

What is Log Analytics?

Append-only log data

Queried using Kusto Query Language (KQL)

- SQL-Like language

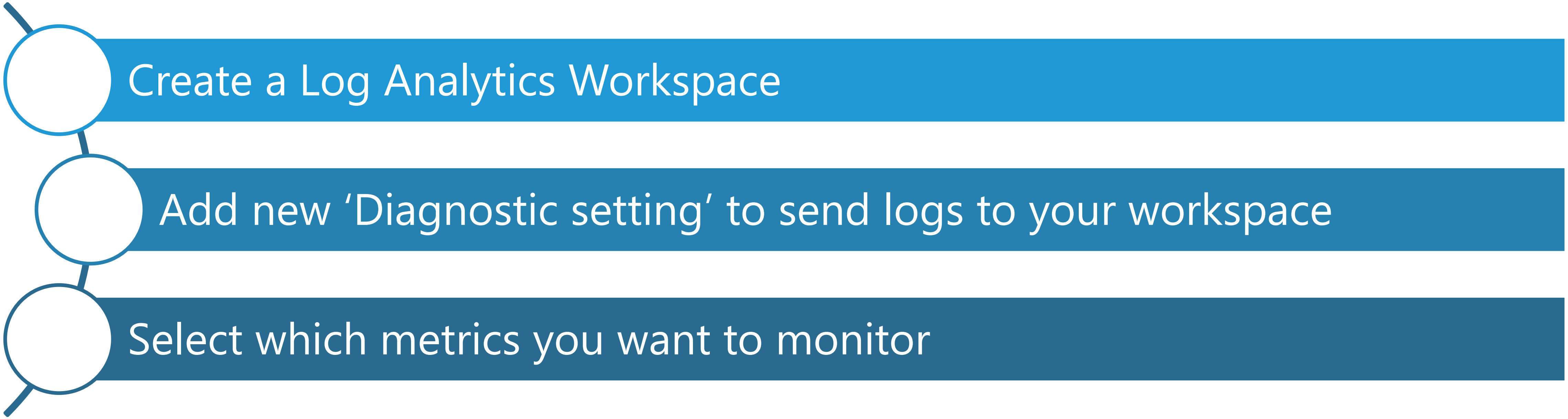
Cost

- Pay-by-ingestion
- Minimize cost by only pulling over needed metrics

Latency

- 10-15 minutes max latency

Enabling Log Analytics

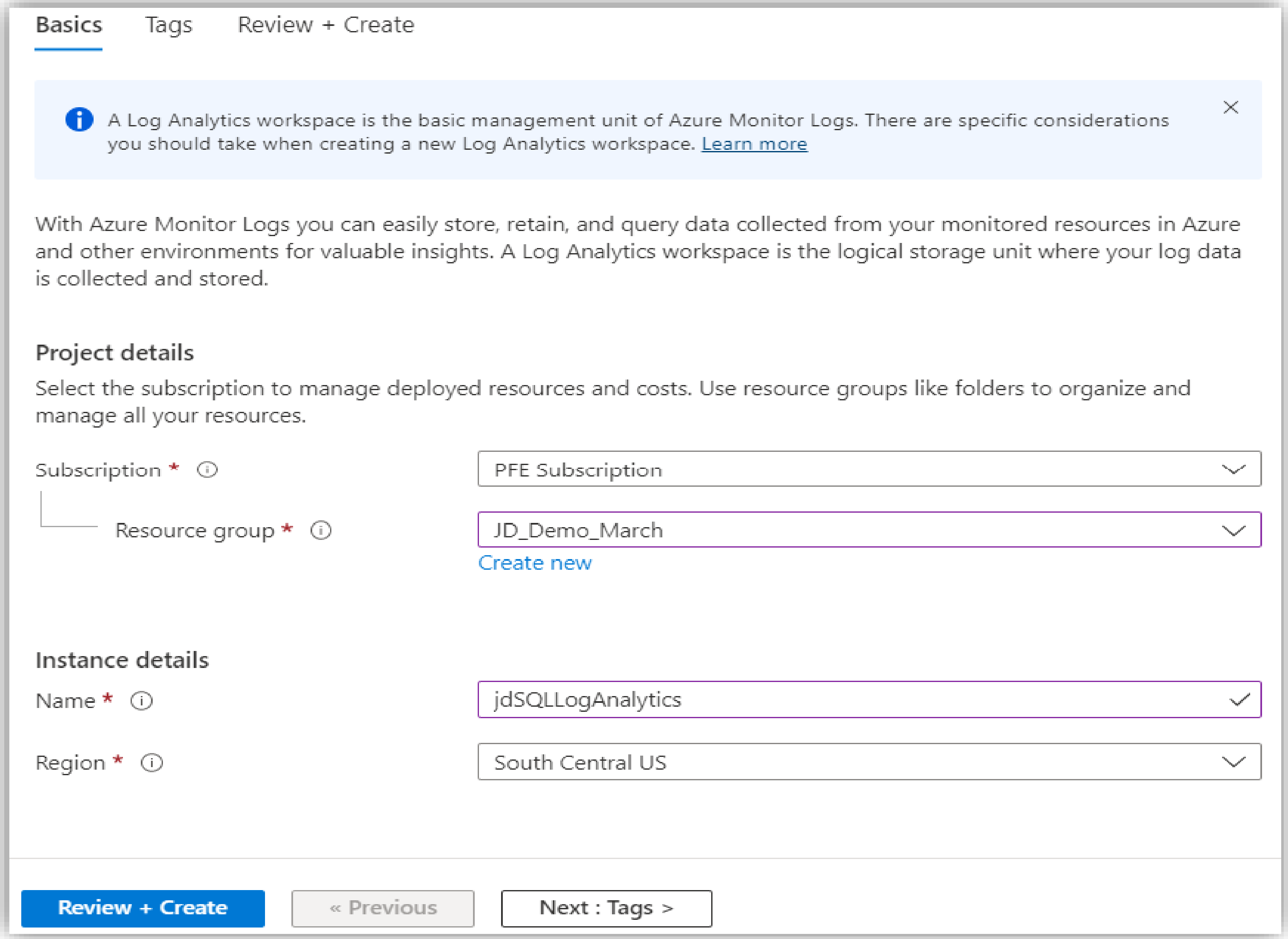


Create a Log Analytics Workspace

Add new ‘Diagnostic setting’ to send logs to your workspace

Select which metrics you want to monitor

Create Log Analytics Workspace



A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : PFE Subscription

Resource group * : JD_Demo_March

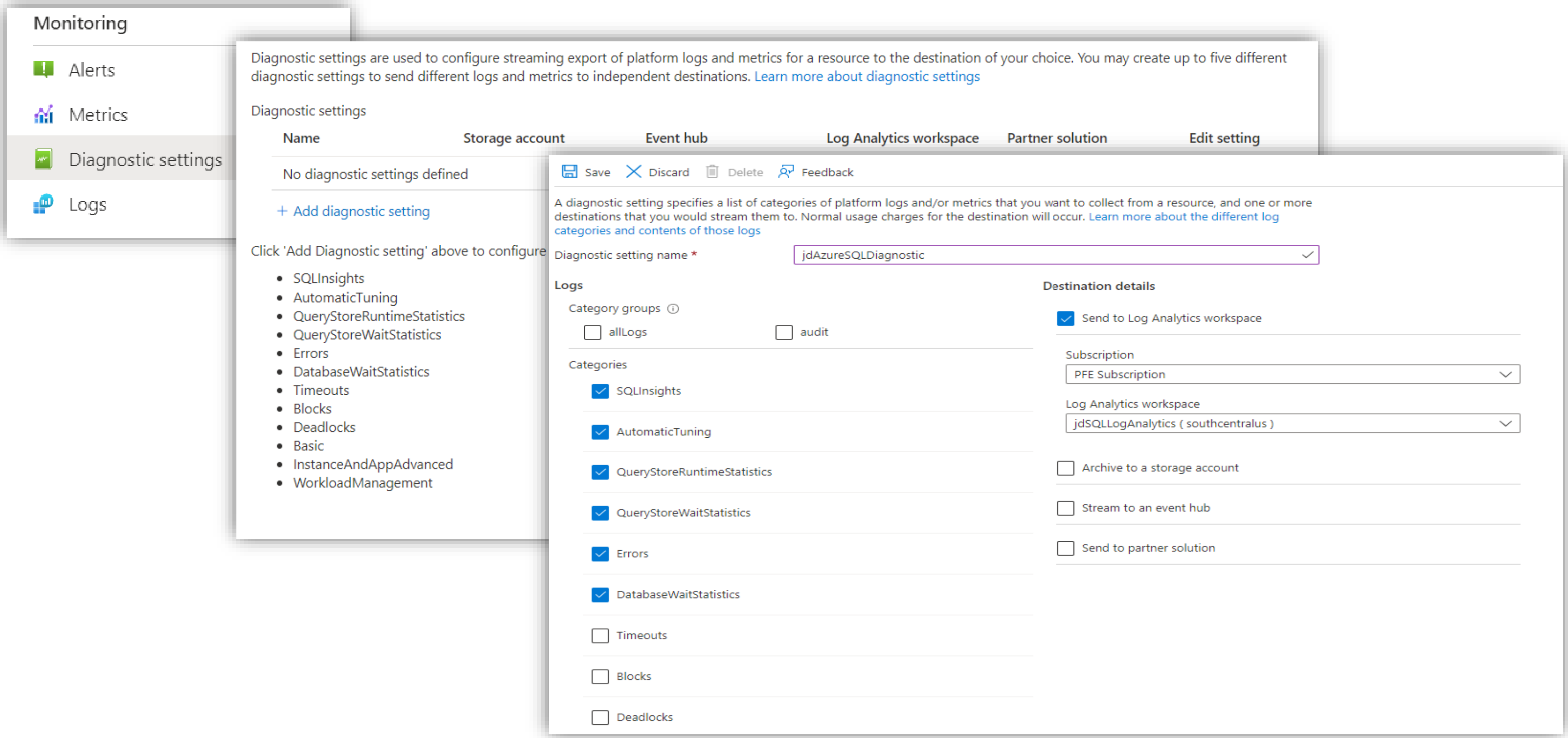
Create new

Instance details

Name * : jdSQLLogAnalytics

Region * : South Central US

Configure Diagnostic Settings



Monitoring

- Alerts
- Metrics
- Diagnostic settings
- Logs

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings

Diagnostic settings

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
No diagnostic settings defined					

+ Add diagnostic setting

Click 'Add Diagnostic setting' above to configure

- SQLInsights
- AutomaticTuning
- QueryStoreRuntimeStatistics
- QueryStoreWaitStatistics
- Errors
- DatabaseWaitStatistics
- Timeouts
- Blocks
- Deadlocks
- Basic
- InstanceAndAppAdvanced
- WorkloadManagement

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. Learn more about the different log categories and contents of those logs

Diagnostic setting name * jdAzureSQLDiagnostic

Logs

Category groups

□ allLogs □ audit

Categories

☑ SQLInsights

☑ AutomaticTuning

☑ QueryStoreRuntimeStatistics

☑ QueryStoreWaitStatistics

☑ Errors

☑ DatabaseWaitStatistics

□ Timeouts

□ Blocks

□ Deadlocks

Destination details

☑ Send to Log Analytics workspace

Subscription: PFE Subscription

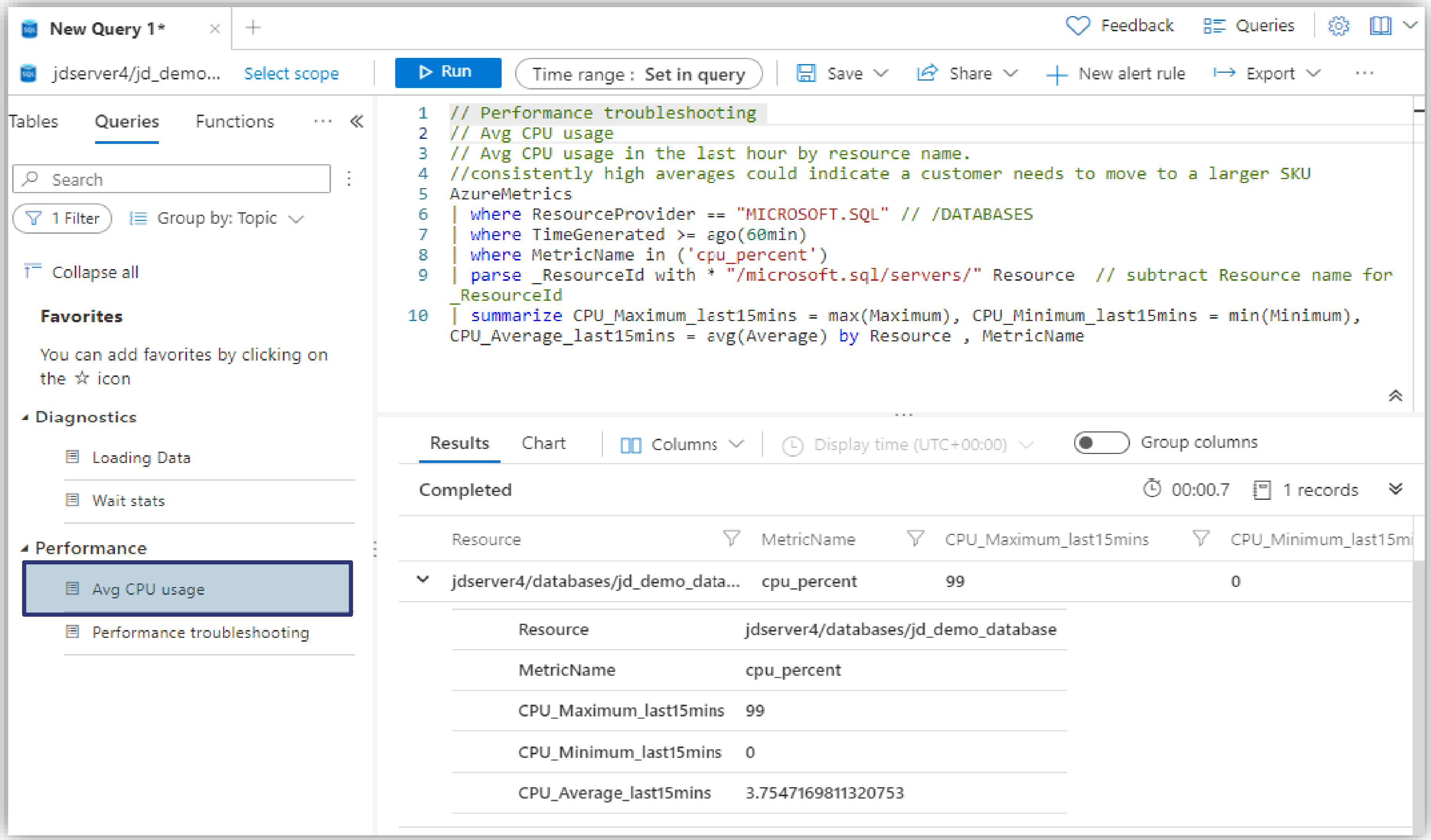
Log Analytics workspace: jdSQLLogAnalytics (southcentralus)

□ Archive to a storage account

□ Stream to an event hub

□ Send to partner solution

Querying Log Analytics (Avg CPU Usage)



```
// Performance troubleshooting
// Avg CPU usage
// Avg CPU usage in the last hour by resource name.
//consistently high averages could indicate a customer needs to move to a larger SKU
AzureMetrics
| where ResourceProvider == "MICROSOFT.SQL" // /DATABASES
| where TimeGenerated >= ago(60min)
| where MetricName in ('cpu_percent')
| parse _ResourceId with * "/microsoft.sql/servers/" Resource  // subtract Resource name for _ResourceId
| summarize CPU_Maximum_last15mins = max(Maximum), CPU_Minimum_last15mins = min(Minimum), CPU_Average_last15mins = avg(Average) by Resource , MetricName
```

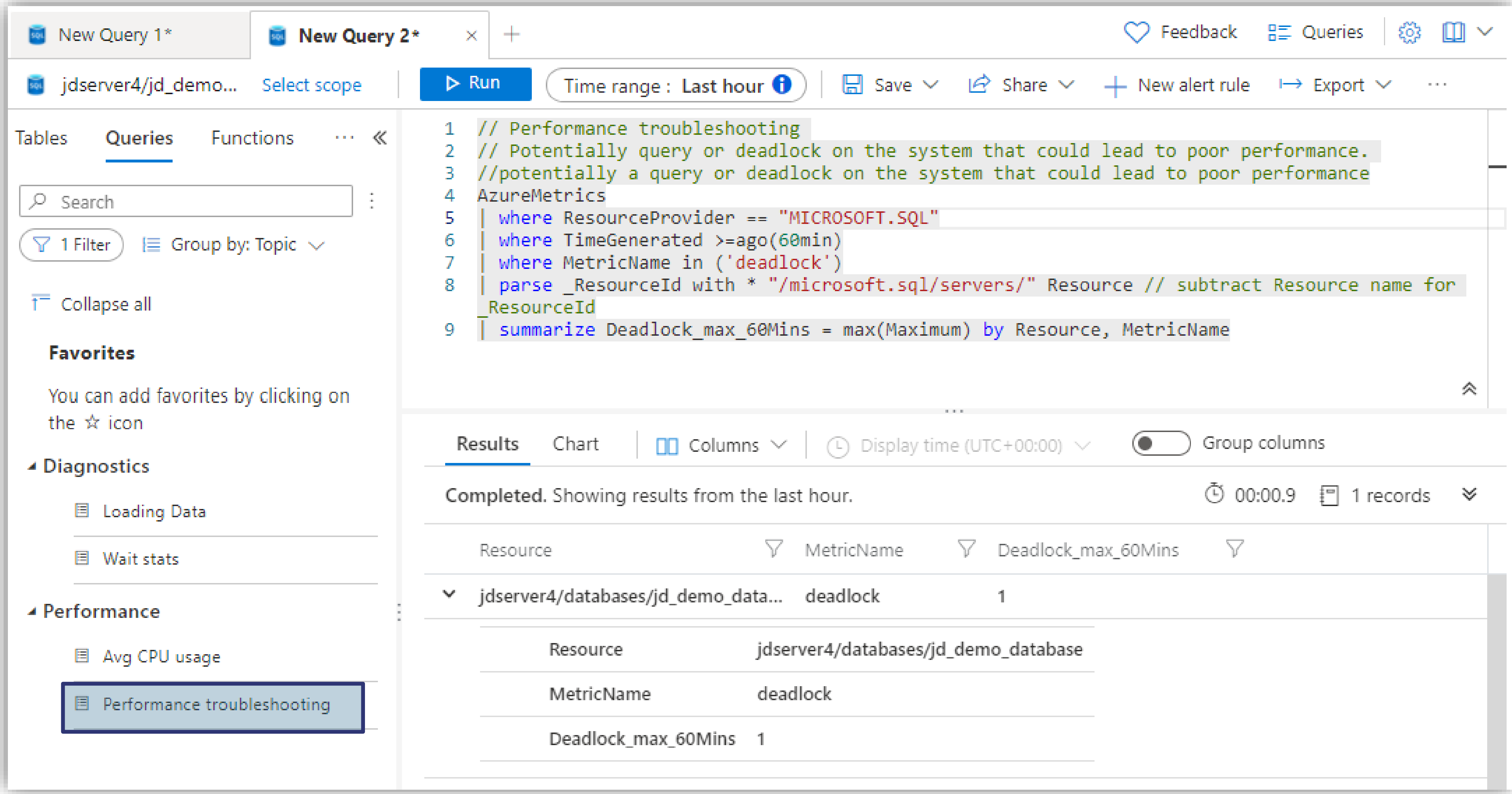
Completed

00:00.7 1 records

Resource	MetricName	CPU_Maximum_last15mins	CPU_Minimum_last15mi
jdserver4/databases/jd_demo_data...	cpu_percent	99	0

Resource	jdserver4/databases/jd_demo_database
MetricName	cpu_percent
CPU_Maximum_last15mins	99
CPU_Minimum_last15mins	0
CPU_Average_last15mins	3.7547169811320753

Querying Log Analytics (Deadlocks)



Time range : Last hour

```
// Performance troubleshooting
// Potentially query or deadlock on the system that could lead to poor performance.
//potentially a query or deadlock on the system that could lead to poor performance
AzureMetrics
| where ResourceProvider == "MICROSOFT.SQL"
| where TimeGenerated >=ago(60min)
| where MetricName in ('deadlock')
| parse _ResourceId with * "/microsoft.sql/servers/" Resource // subtract Resource name for _ResourceId
| summarize Deadlock_max_60Mins = max(Maximum) by Resource, MetricName
```

Completed. Showing results from the last hour.

00:00.9   1 records

Resource	MetricName	Deadlock_max_60Mins
jdserver4/databases/jd_demo_data...	deadlock	1

Resource	jdserver4/databases/jd_demo_database
MetricName	deadlock
Deadlock_max_60Mins	1

Demonstration Time

Questions?