SQL KONFERENZ 2025

Niko Neugebauer

Azure SQL Observability



Niko Neugebauer

- Product Manager at Microsoft working on Azure SQL
- Spent over 20 years helping customers building solutions on OLTP & OLAP.
- Organized the first international SQL Saturday. Started data community in Portugal.



Niko.Neugebauer@microsoft.com

/in/nikoneugebauer/

@NikoNeugebauer

www.nikoport.com

Session Agenda

- Observability in Azure SQL and it sources
- Monitoring Azure SQL
- Security side



Microsoft

Azure SQL

Azure SQL

The family of SQL cloud databases



SQL Server on Azure Virtual Machines



Azure SQL Managed Instance



Azure SQL Database

Migration

Best for: *Migrating ("lift and shift") 3rd party apps* to customer-managed Azure virtual machines.

Best for: *Migrating custom apps at-scale* to a Microsoft-managed, SQL Server-compatible instance.

Innovation

Best for: *Developing highly-scalable, AI-ready applications* with SQL's reliability and security at commercial open-source database costs.



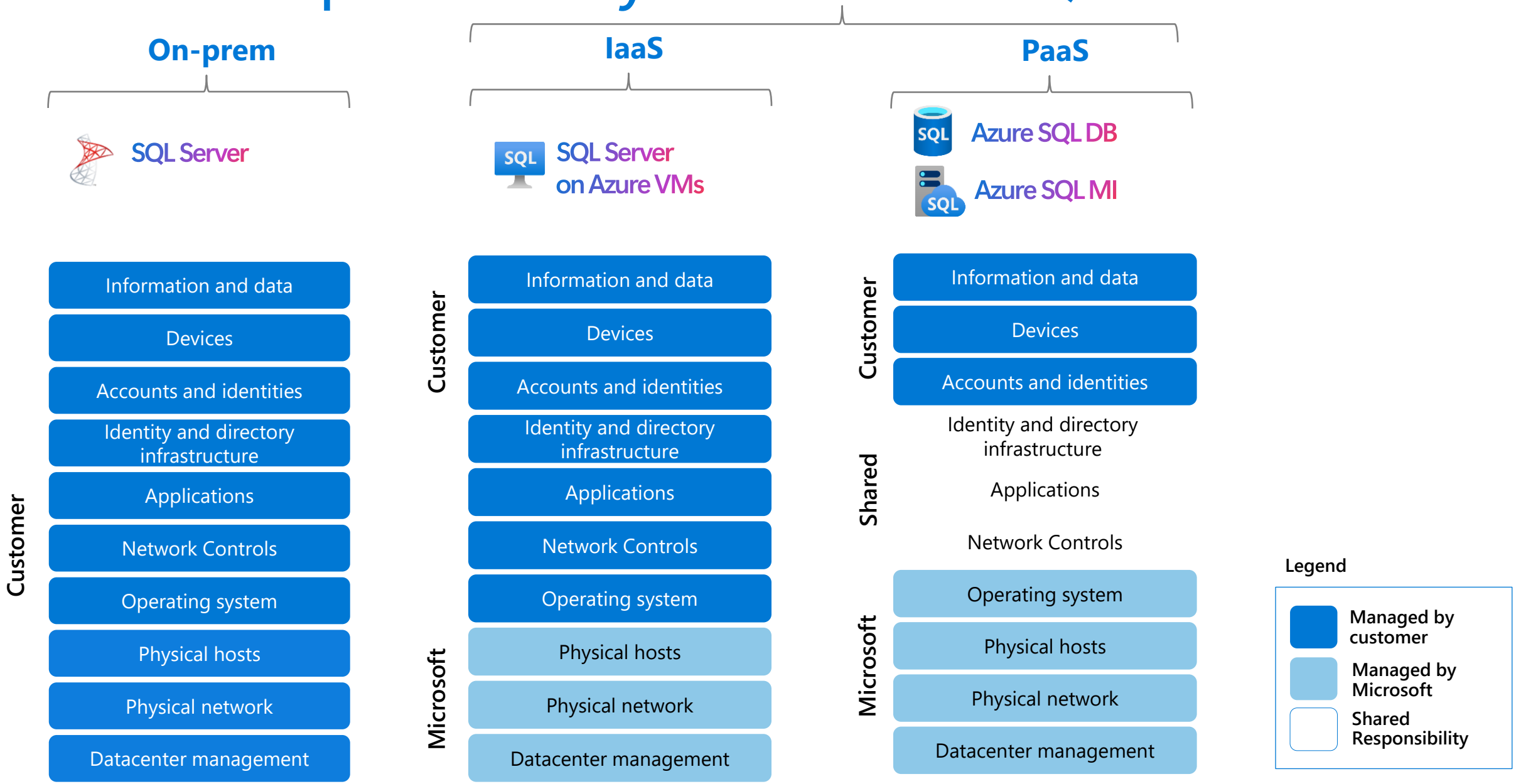
Azure SQL enabled by Azure Arc

Run Azure SQL on premises and in multicloud environments

Your first step on the journey to Azure.

Azure is the cloud that knows SQL Server best

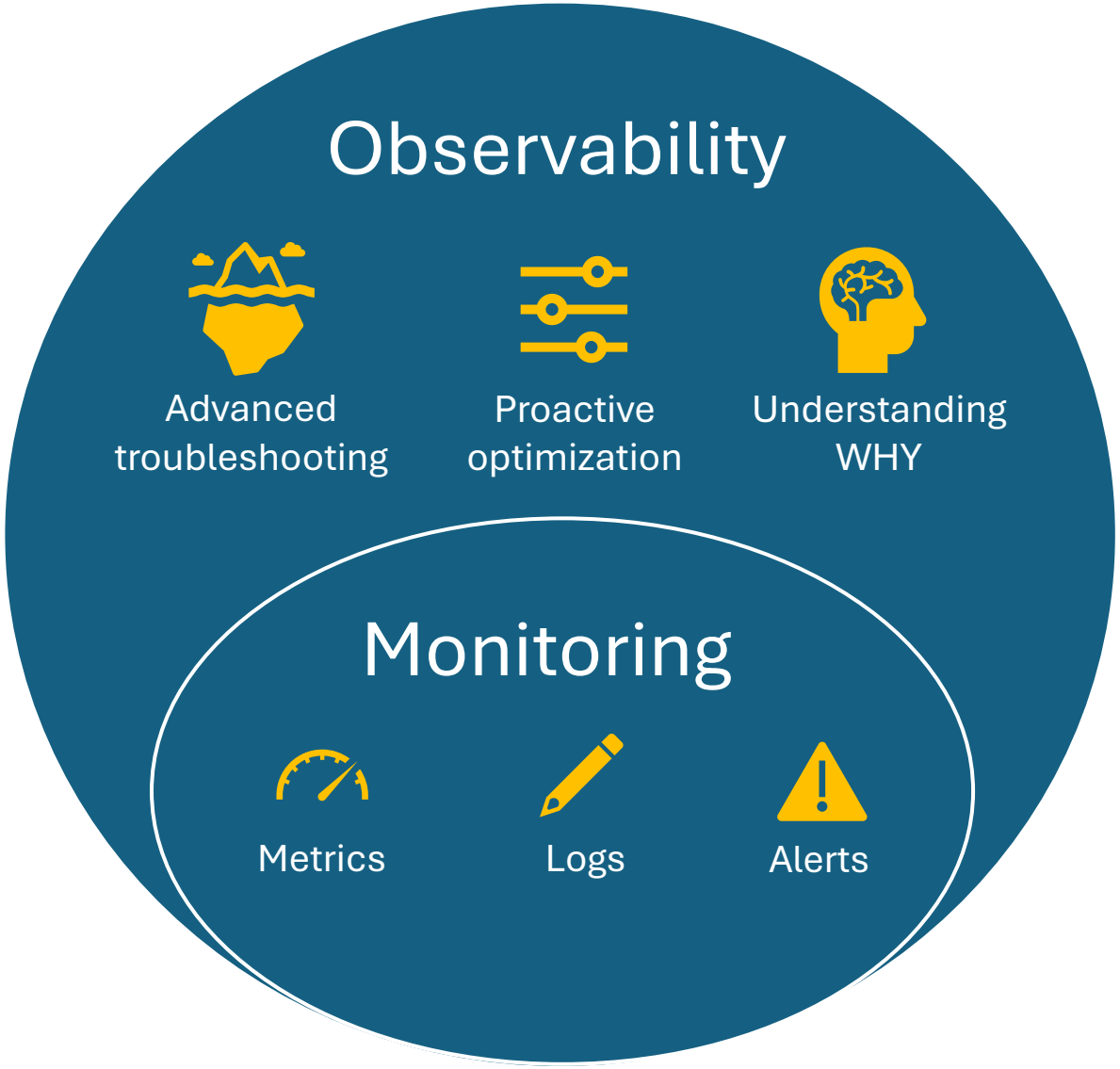
Shared responsibility on Azure SQL



Microsoft

Observability

Monitoring and Observability



Monitoring is a key part of the Observability, providing it with the metrics, logs & traces – describing the current state of the observed system.

Traditional monitoring focuses on predefined metrics and logs to track the performance and availability of systems.
It is more suited for simpler systems, where parameters are well-known, and performance is well-understood.
Tools like Database Watcher or some 3rd party tools are important for observability in terms of presenting the service health and service state data and creating alerts to act upon.

Observability provides a more comprehensive view of system behavior by integrating various data sources and analyzing them.
It is better suited for the multi-system environment with more potential unknowns and dynamic changes of the system elements.
It goes beyond traditional monitoring by offering advanced capabilities.

Observability Opportunities

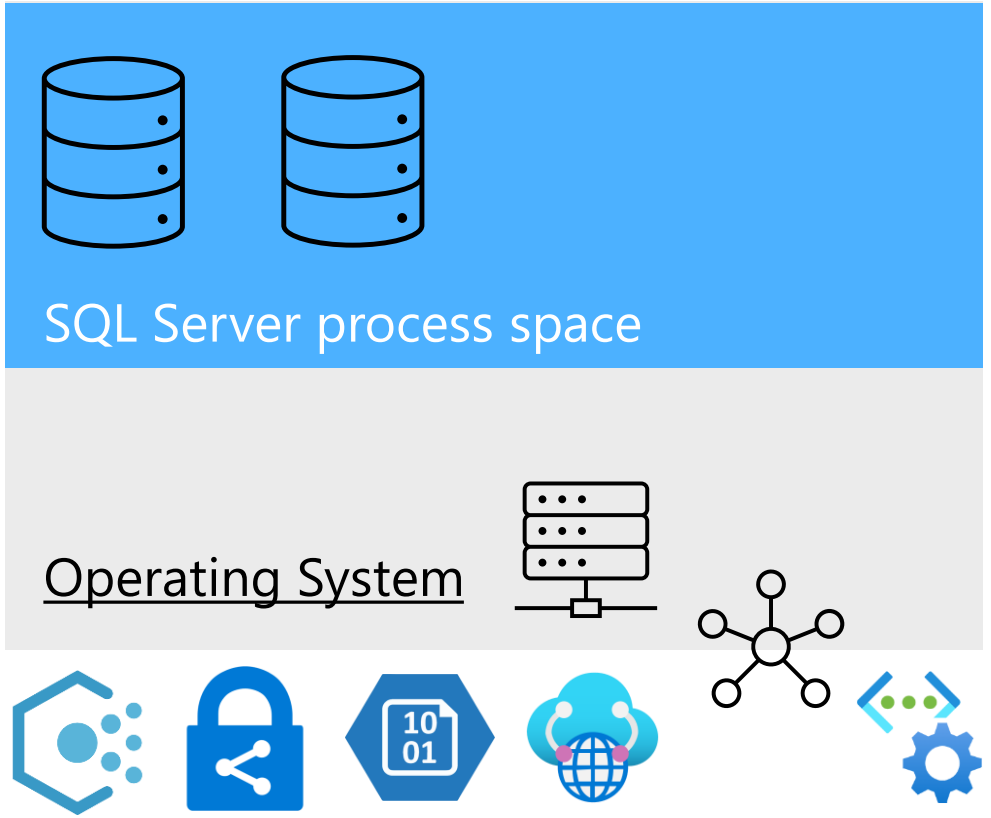
- Single version of truth viewed through the single pane of glass
- Availability of all information needed to determine the state of the system
- Data available to both humans and automated processes
- Value provided to every role and level of expertise, from DBA to non-technical
- Provide intelligence on the problem identification from the information collected
- Execute corrective action based on the collected and analyzed information

Microsoft

Monitoring & Observing

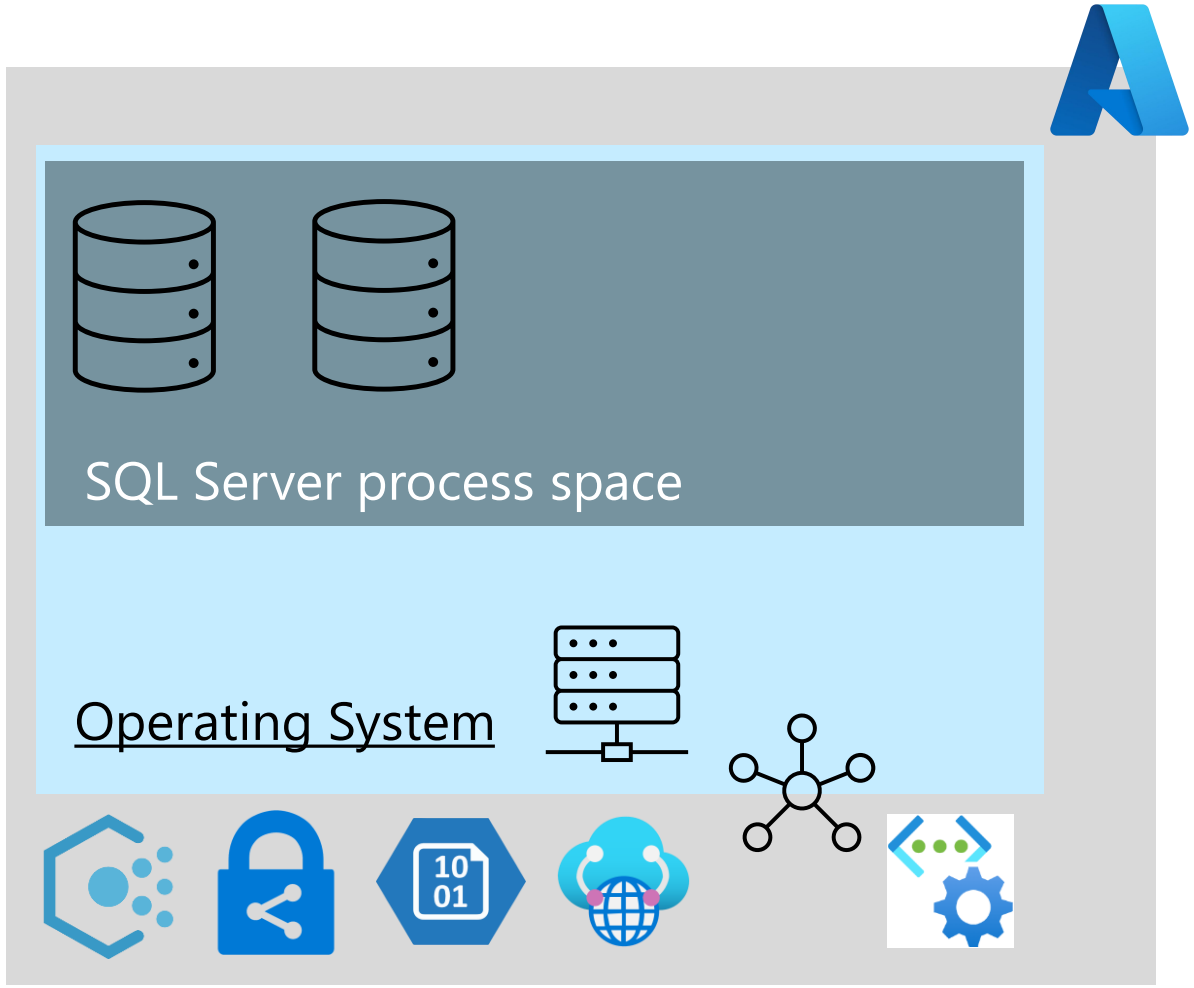
SQL Server on-premises & Azure

- Azure SQL PaaS consists out of the main 3 parts: **SQL Server engine** + **O/S** + **Azure Platform**
- Tightly integrated with other Azure services (Authentication, Storage, Automation…)
- Delivered under an SLA
- Exposes details of the user & system actions in different interfaces

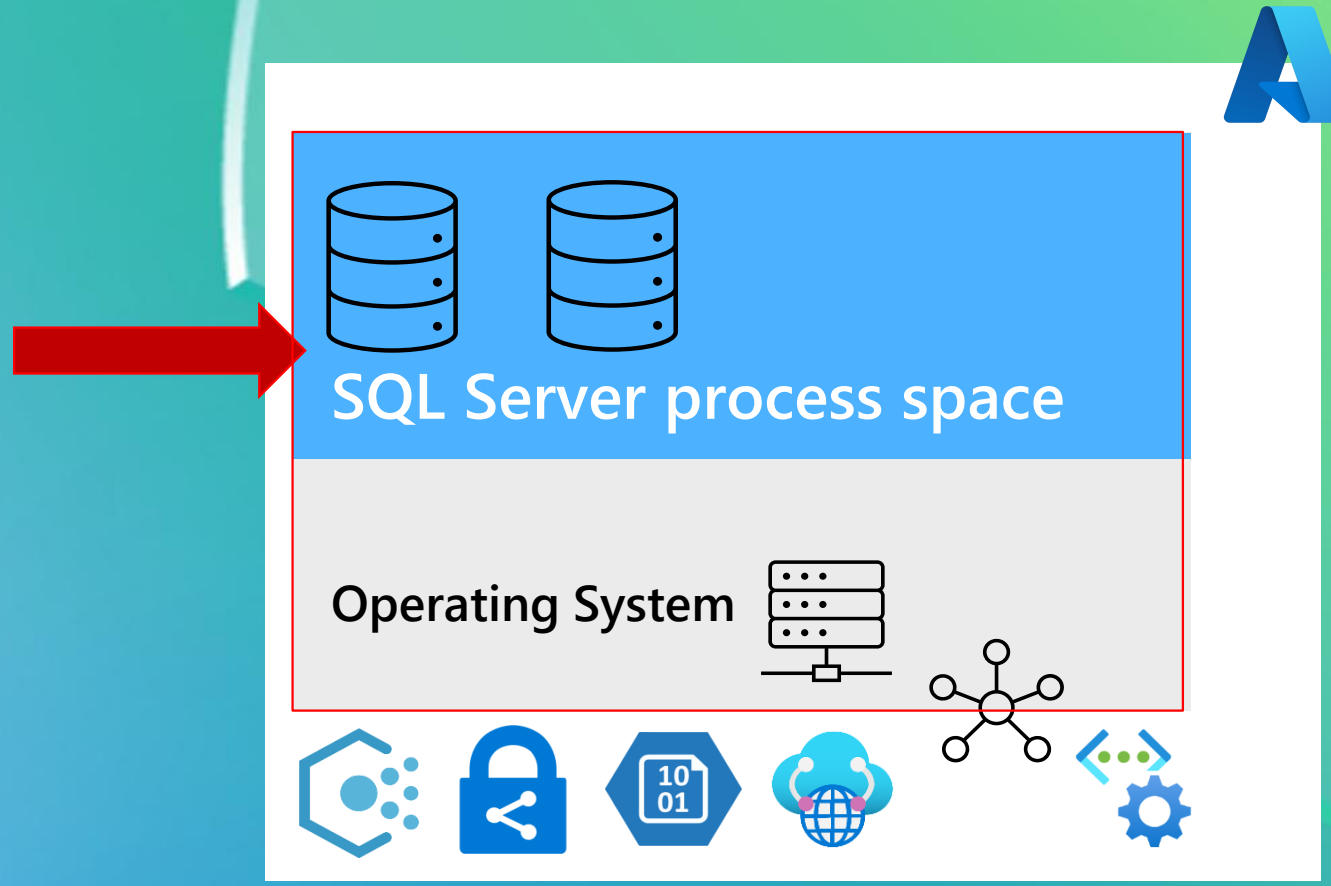


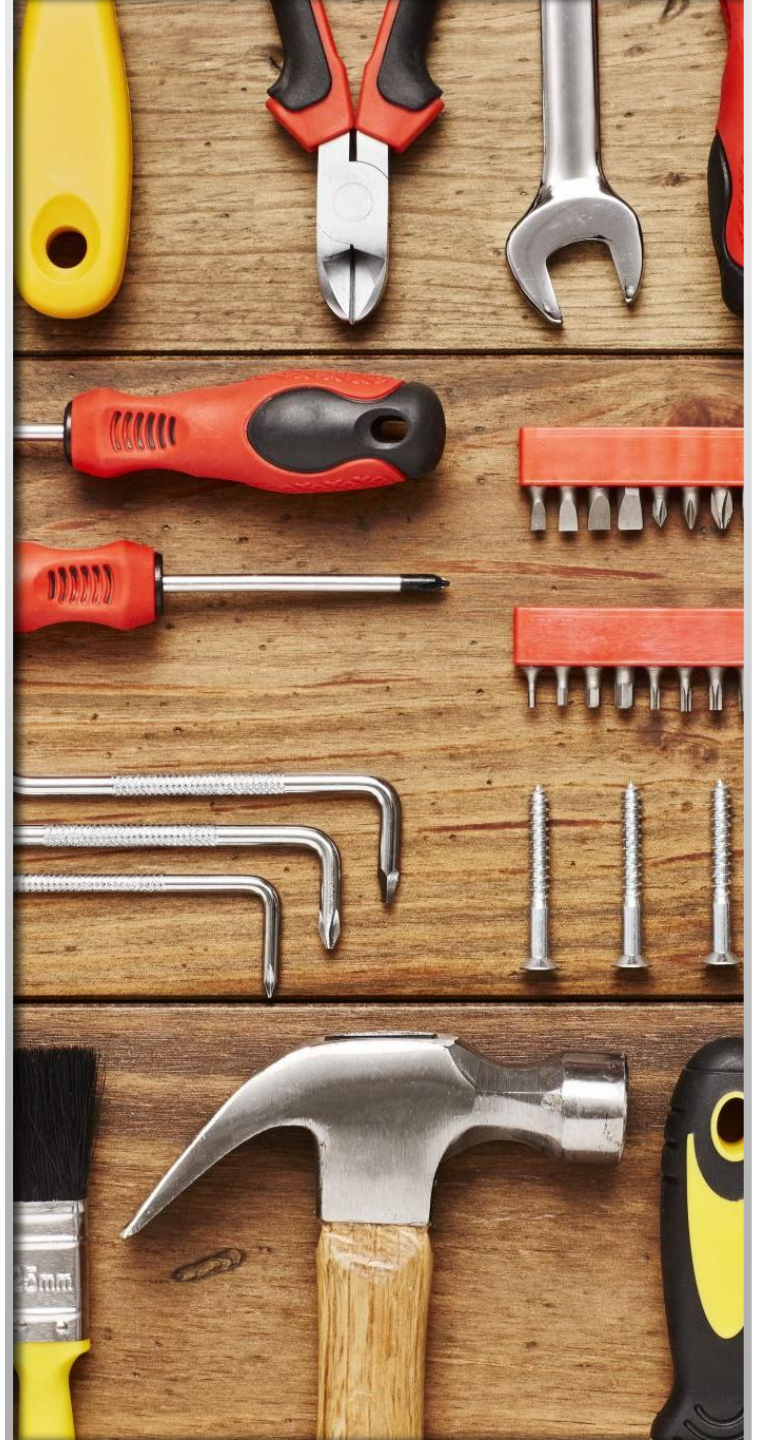
Azure SQL PaaS monitoring parts

- Azure SQL PaaS consists out of the main 3 parts: **SQL Server engine** + **O/S** + **Azure Platform**
- Tightly integrated with other Azure services (Authentication, Storage, Automation…)
- Delivered under an SLA
- Exposes details of the user & system actions in different interfaces



SQL Server process Observability





Some of the SQL Server observability sources

SQL SERVER
ERROR LOG

SQL AGENT
ERROR LOG

DATABASE MAIL
ERROR LOG

SQL SERVER FAILOVER CLUSTER
DIAGNOSTIC LOG

DMVs

EXTENDED EVENTS

WINDOWS
EVENT VIEWER

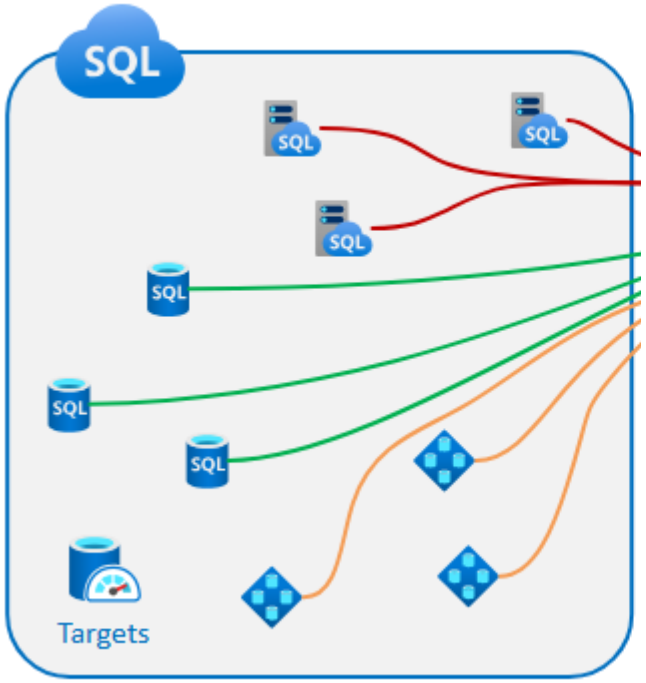
AND MORE!

SQL Server observability sources availability

Feature			
DMVs	**Yes**	**Yes**	**Yes**
Common Error logs	**Yes**	**Yes** (does not survive restart)	❌ Not supported
Failover cluster logs	**Yes**	❌ Not supported	❌ Not supported
Windows Server error logs	**Yes**	❌ Not supported	❌ Not supported
Windows event viewer	**Yes**	❌ Not supported	❌ Not supported
Performance counters	**Yes**	**Yes** (with limitations)	**Yes** (with limitations)
Extended events	**Yes**	**Yes** (with limitations)	**Yes** (with limitations)
DBCC	**Yes**	**Yes** (with limitations)	**Yes** (with limitations)
WMI	**Yes**	❌ Not supported	❌ Not supported
Default trace	**Yes**	**Yes**	❌ Not supported
Profiler	**Yes**	**Yes**	**Yes**
Query Store	**Yes**	**Yes**	**Yes**

Monitoring SQL Server process

Database Watcher



Hotspots and outliers across the estate

- CPU, Data IO, Log IO, workers
- Requests, waits
- IOPS, throughput, latency
- Connectivity probes

Top queries across the estate

- Rank by any Query Store metric
- Filter by server, database, query hash, query text

Common SQL perf metrics in one place

- CPU, Data IO, Log IO, workers
- Requests and waits over time
- Perf counters: query processing, memory, replicas, etc.

Query activity and session statistics

- Current and historical
- Blocking chains
- Session wait stats

Table and index metadata

- Schema details
- Index usage
- Index suggestions

Backup and SQL Agent job history

- Job state
- Job history
- Backup history and statistics

Properties and configuration

- Detect configuration drift
- Find misconfigured servers and databases

Database Watcher

Monitor all Azure SQL DB and Azure SQL Managed Instance workloads



Managed monitoring



Current and historical data



Configurable



Near real time latency



Dashboards in Azure portal

This wasn't easy in Azure SQL before...

Hotspots and outliers across the estate

- CPU, Data IO, Log IO, workers
- Requests, waits
- IOPS, throughput, latency
- Connectivity probes

Top queries across the estate

- Rank by any Query Store metric
- Filter by server, database, query hash, query text

Common SQL perf metrics in one place

- CPU, Data IO, Log IO, workers
- Requests and waits over time
- Perf counters: query processing, memory, replicas, etc.

Query activity and session statistics

- Current and historical
- Blocking chains
- Session wait stats

Table and index metadata

- Schema details
- Index usage
- Index suggestions

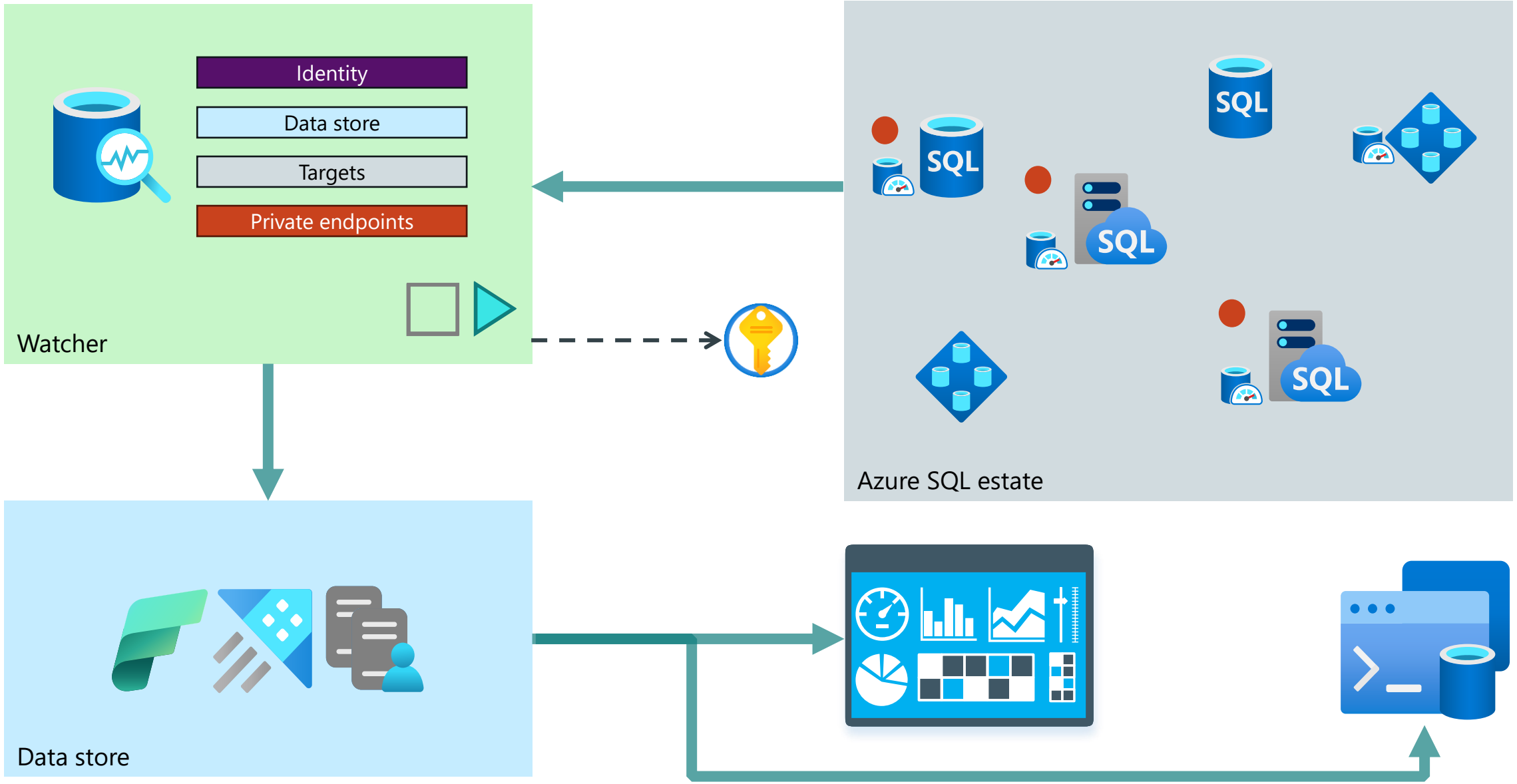
Backup and SQL Agent job history

- Job state
- Job history
- Backup history and statistics

Properties and configuration

- Detect configuration drift
- Find misconfigured servers and databases

How Database Watcher works



dbw-demo-1 | Dashboards

Database watcher

Search

Overview
Activity log
Access control (IAM)
Resource visualizer
Favorites
Monitoring
Dashboards
Configuration
Identity
Managed private endpoints
SQL targets
Data store
Automation

Auto refresh: Off

Data store

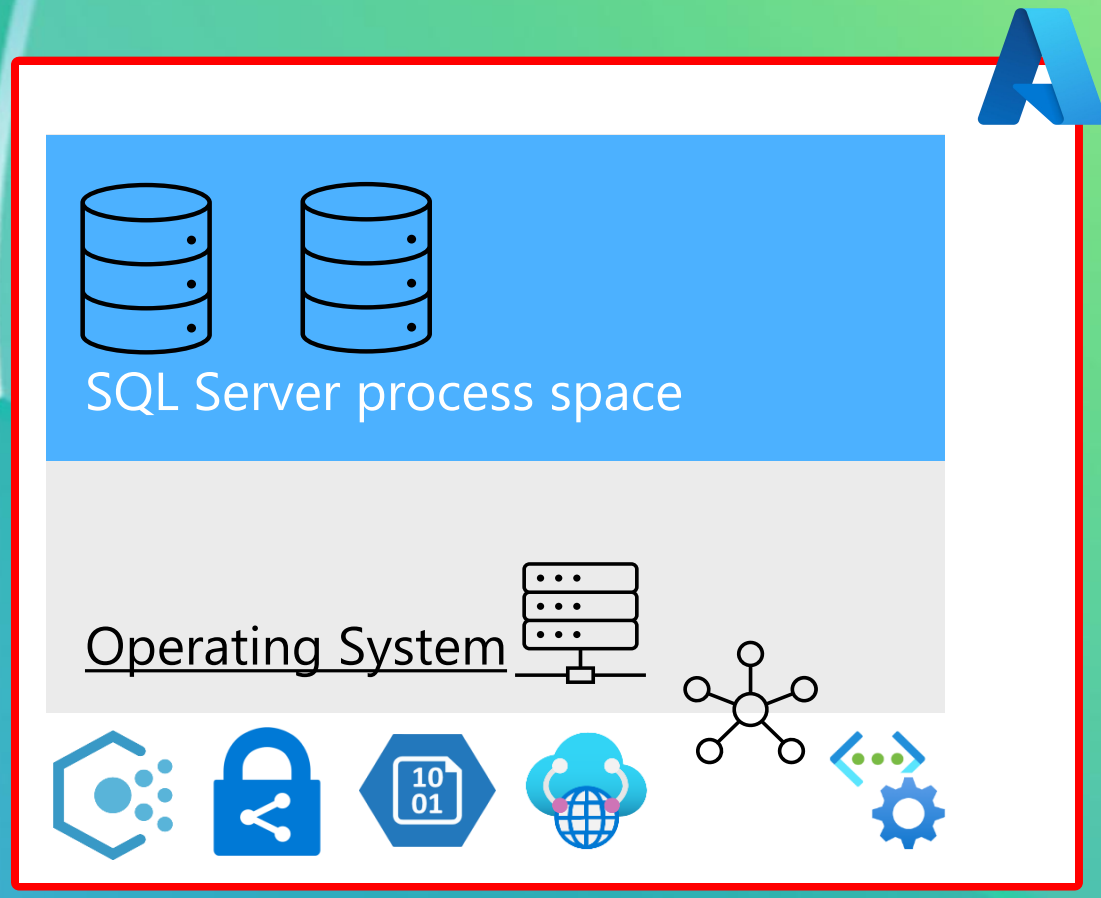
Azure SQL databases
13

Azure SQL elastic pools
2

Azure SQL managed instances
3

Learn more

Azure Platform Observability







Azure SQL platform observability sources

- Azure Metrics
- Azure Service Health (generic & personalized)
- Resource Health
- Activity Log
- Azure Diagnostic Logs
- Azure Log Analytics
- Azure Advisor
- Microsoft Entra logs & reports

Azure Metrics in Azure Portal

- Built-in monitoring of basic telemetry (CPU, storage, IOPS)
- Sampling frequency: 1 minute
- Alerts through Azure Alerting
- Does not consume DB resource for monitoring

Pros:

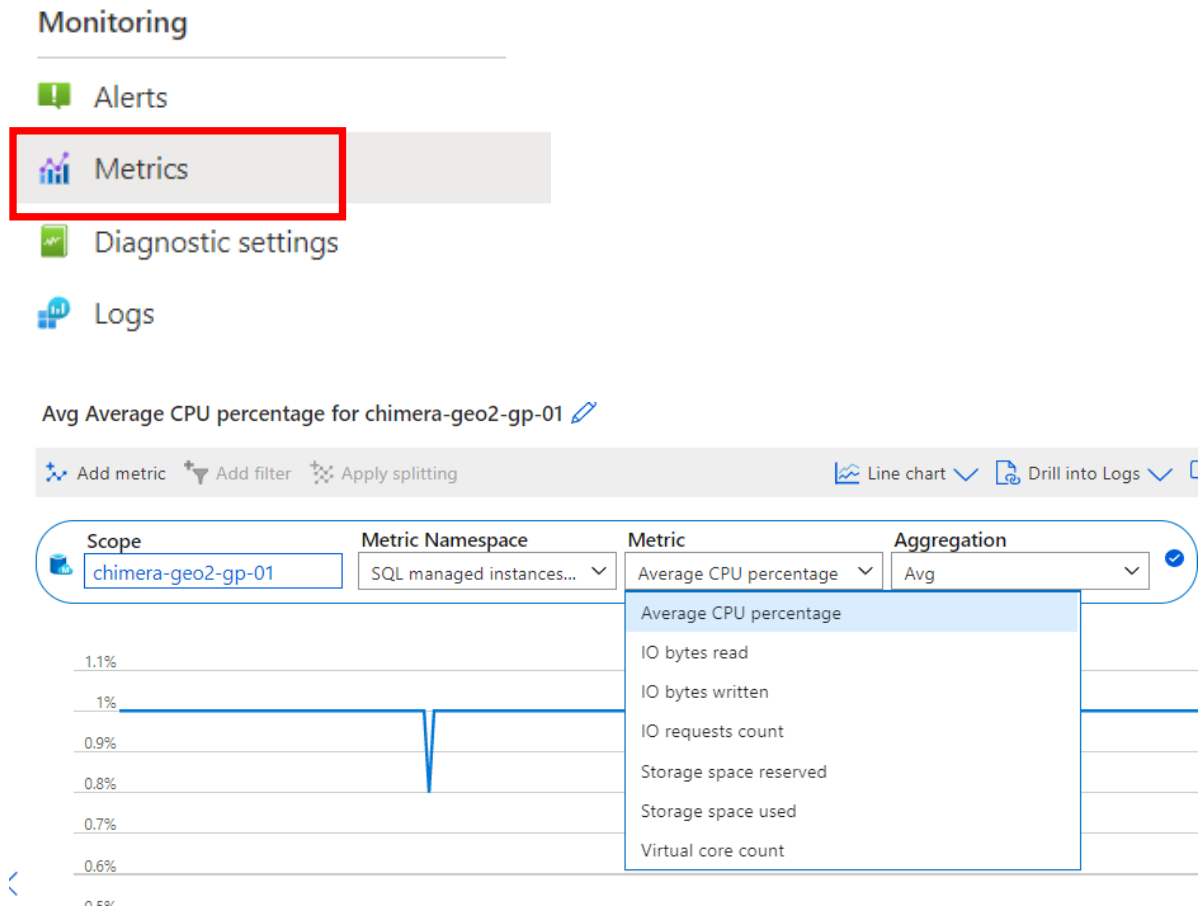
- Easy to use

Cons:

- No multi-resource alerts (e.g. you cannot have 1 alert for many resources

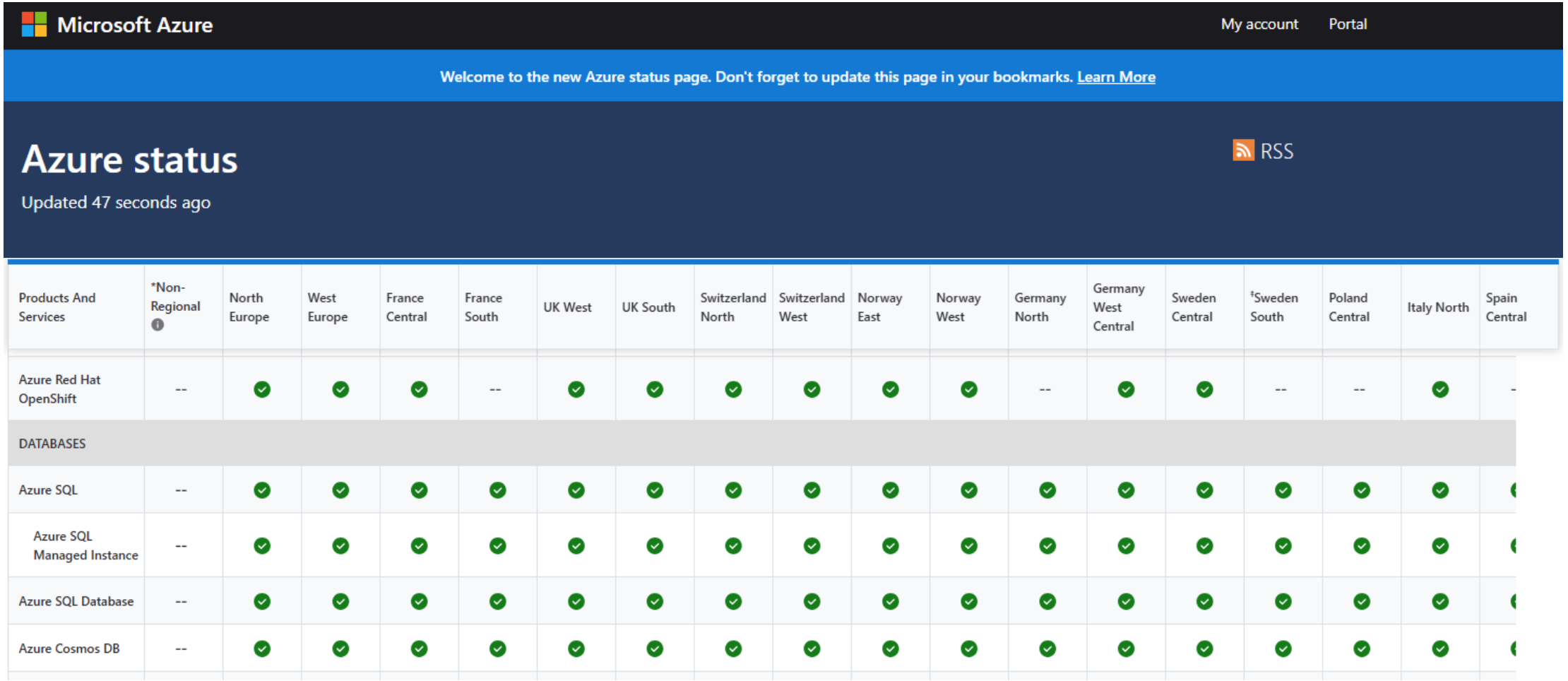
Costs:

- Charged per single alert per month, see Azure Monitor pricing for details



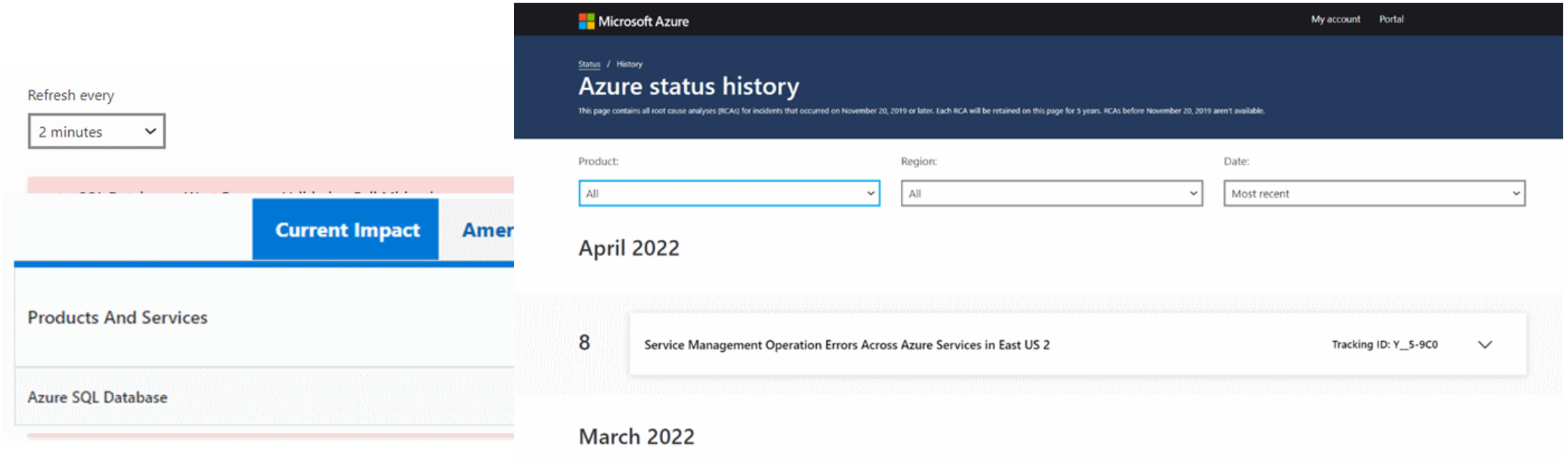
Azure Service Health - generic

https://azure.status.microsoft/en-us/status



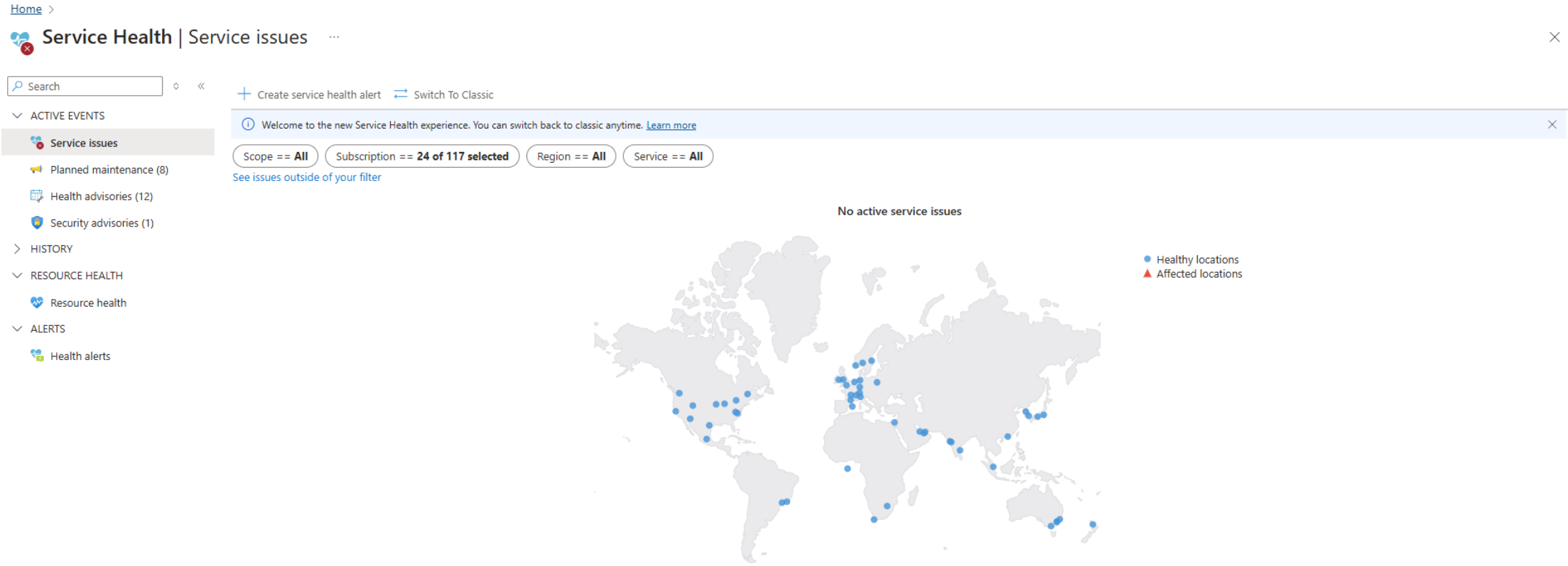
Products And Services	*Non-Regional	North Europe	West Europe	France Central	France South	UK West	UK South	Switzerland North	Switzerland West	Norway East	Norway West	Germany North	Germany West Central	Sweden Central	‡Sweden South	Poland Central	Italy North	Spain Central
Azure Red Hat OpenShift	--	✓	✓	✓	--	✓	✓	✓	✓	✓	✓	--	✓	✓	--	--	✓	-
DATABASES																		
Azure SQL	--	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure SQL Managed Instance	--	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure SQL Database	--	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Azure Cosmos DB	--	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Azure Service Health – generic



Azure Service Health - personalized

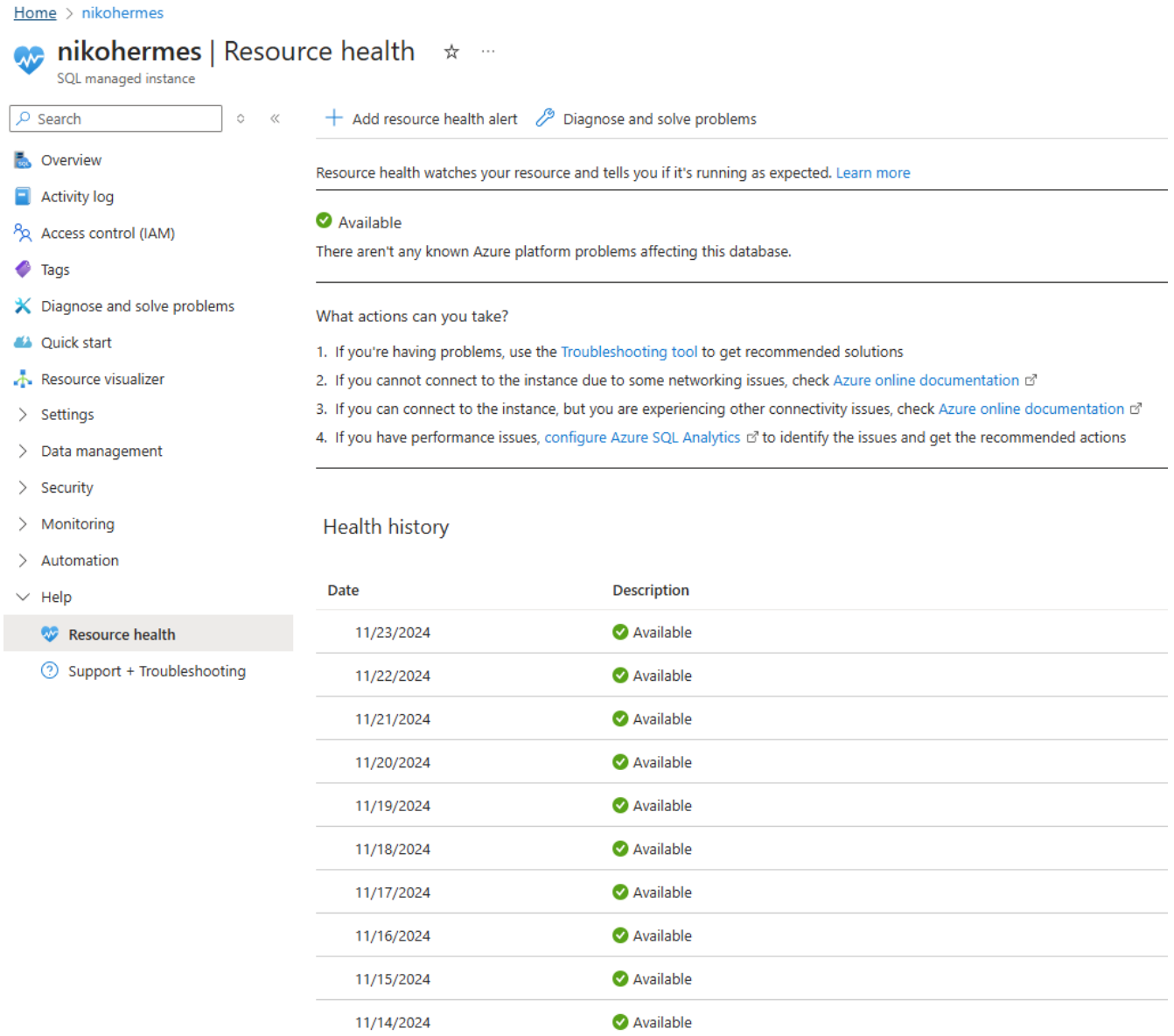
https://aka.ms/azureservicehealth



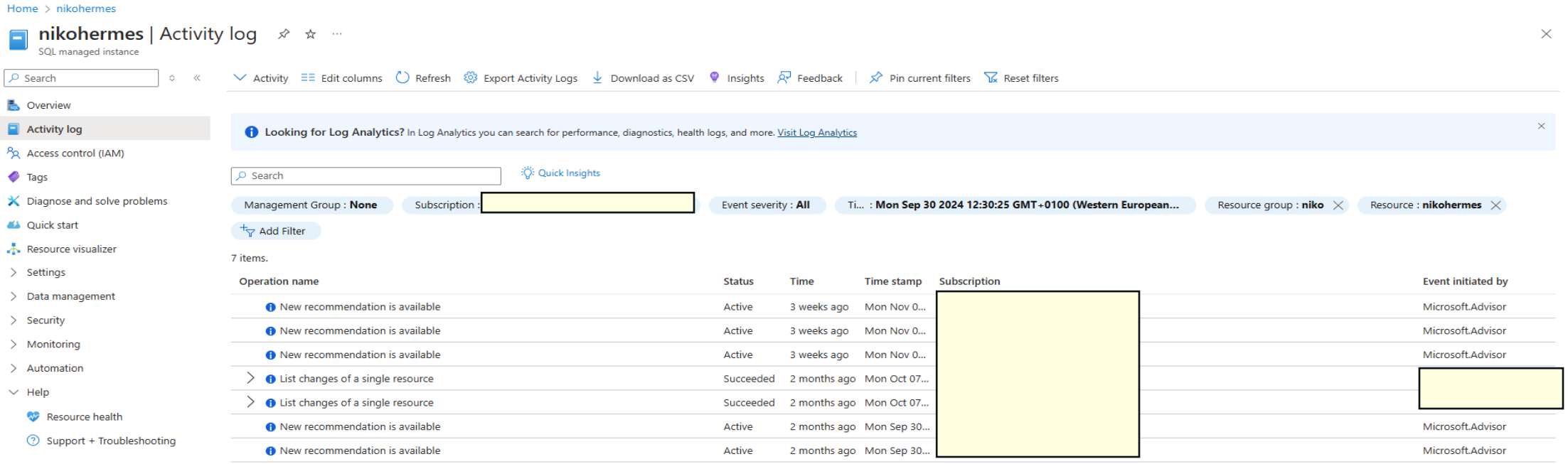
Resource Health

This is an individual resource representation of the Service Health.

- Lists the detailed health events for the selected resource.
- Allows an easy setup of resource health alert
- Provides with a basic troubleshooting



Activity Log

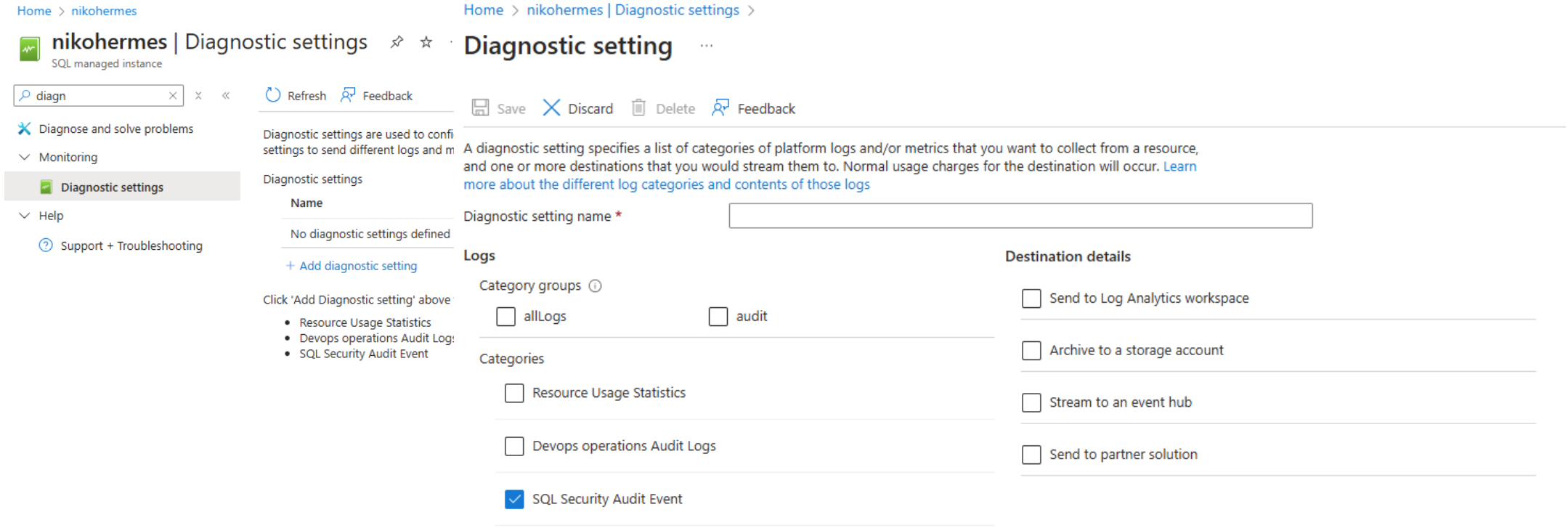


The **Azure Monitor activity log** is a platform log in Azure that provides insight into subscription-level and resource-level events. The activity log includes information like when a resource is modified, or a resource status is changed (for example - started/stopped).

Service health notifications are published by the Azure infrastructure into the Azure activity log.

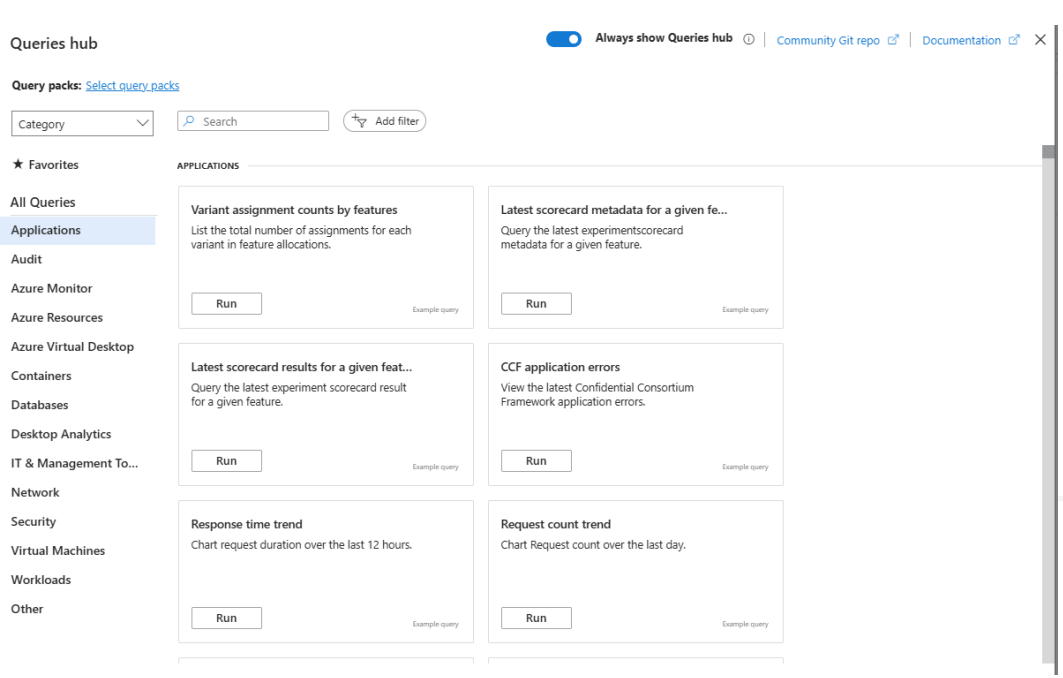
The notifications contain information about the resources under your subscription. Given the possibly large volume of information stored in the activity log, there's a separate user interface to make it easier to view and set up alerts on service health notifications.

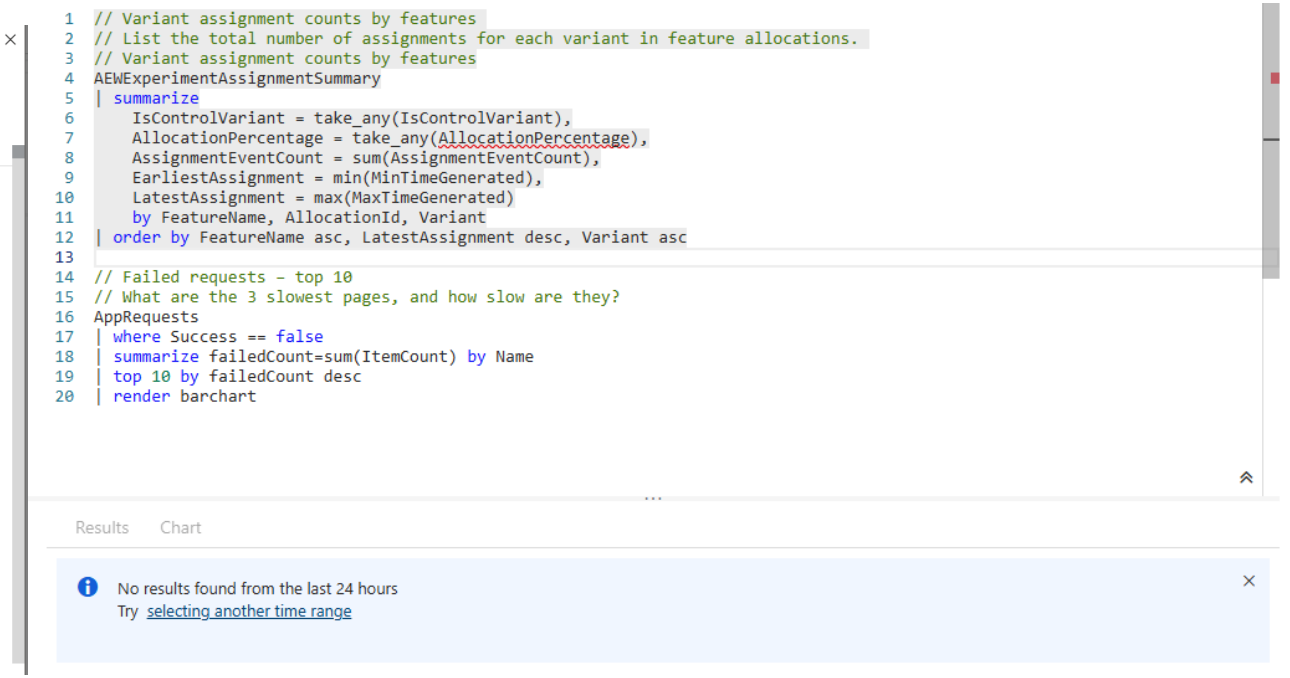
Azure Diagnostic Logs



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.

Azure Log Analytics





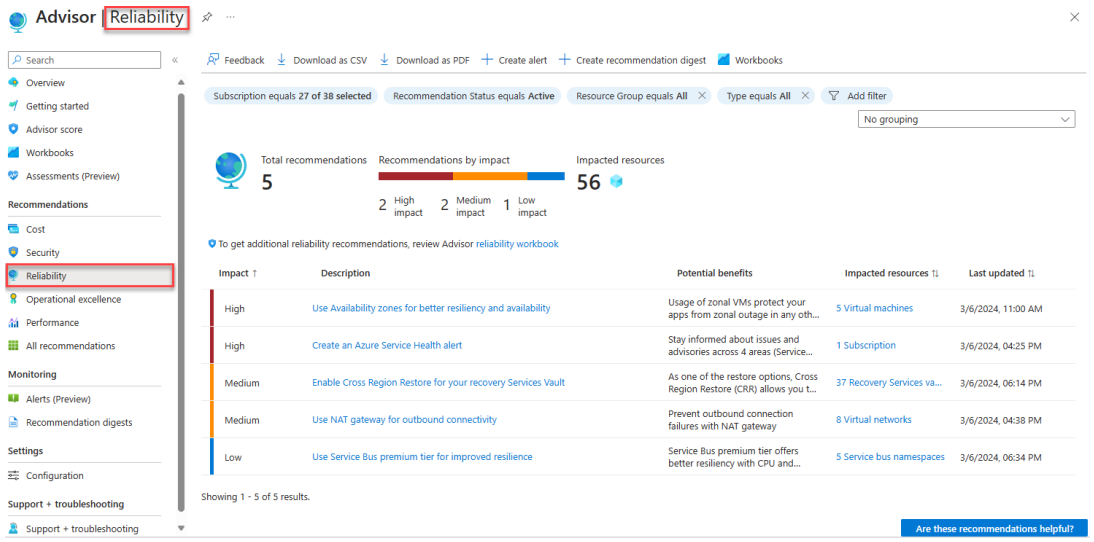
Log Analytics is a tool in the Azure portal that's used to edit and run log queries against data in the Azure Monitor Logs store.

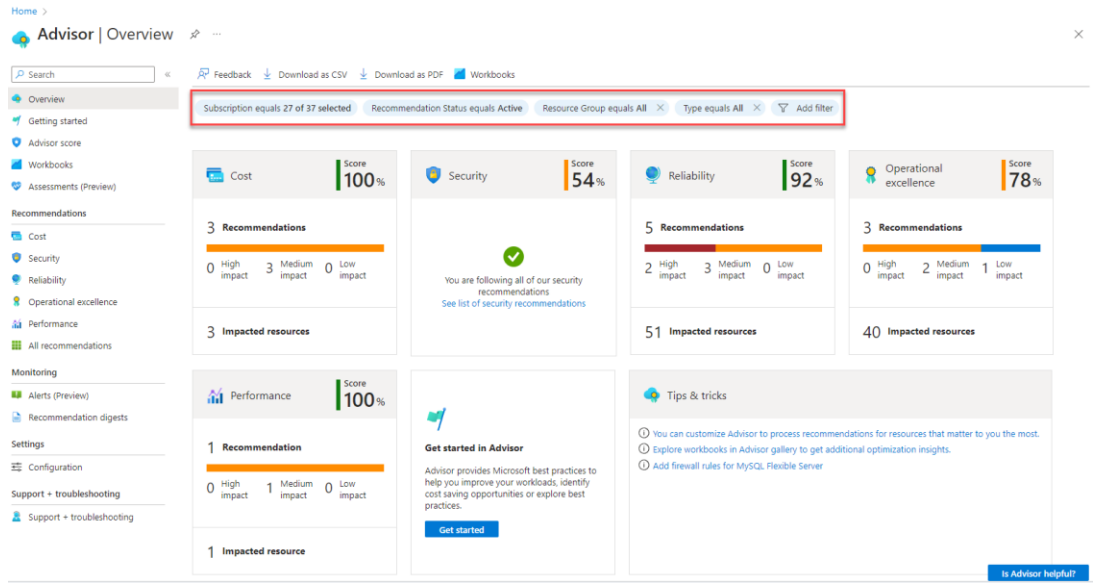
By using **KQL (Kusto Query Language)** customer can easily execute analysis of the collected observability information.

Azure Advisor

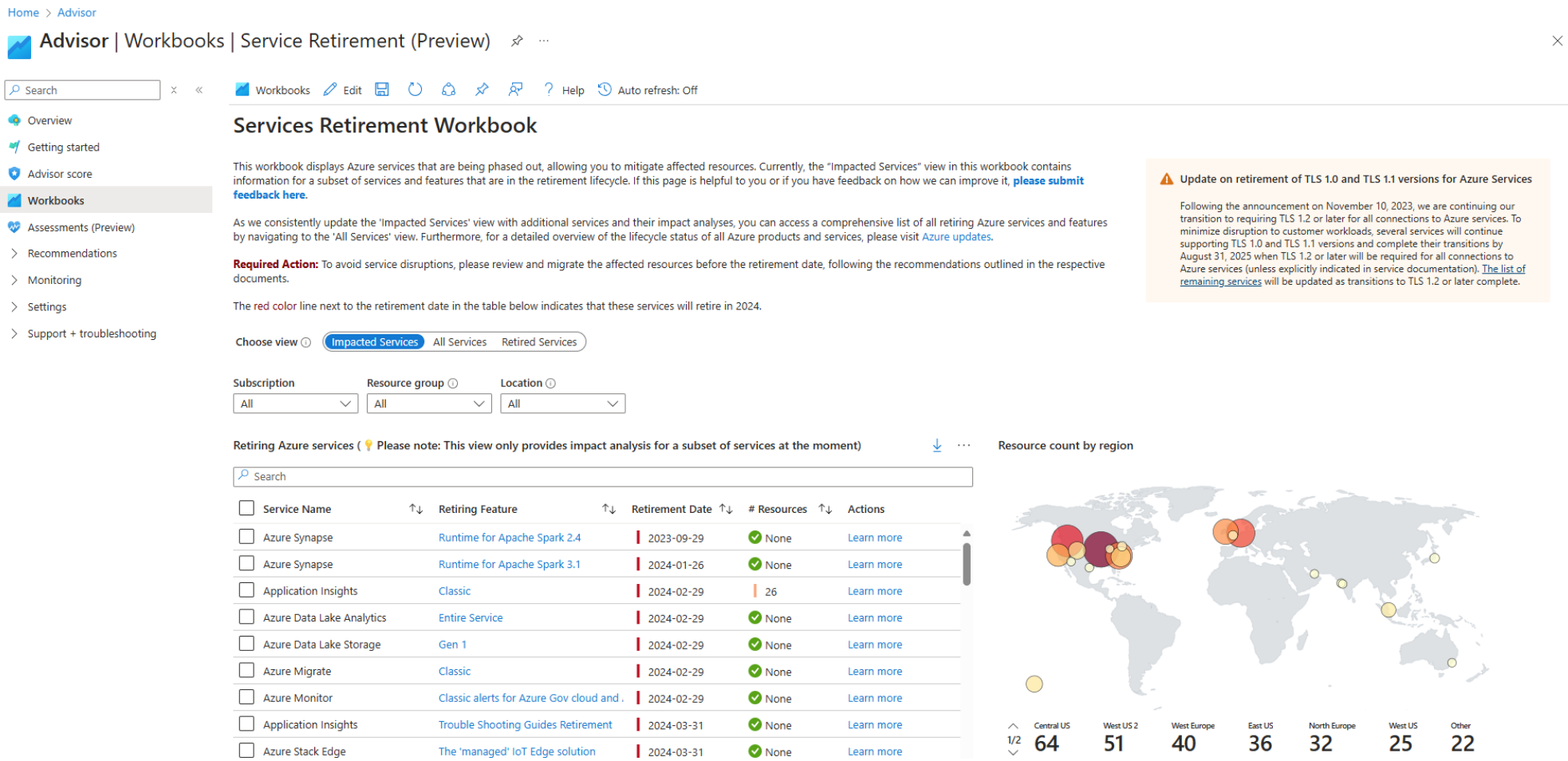
Advisor is a digital cloud assistant that helps you follow best practices to optimize your Azure deployments

- **Reliability**: To ensure and improve the continuity of your business-critical applications.
- **Security**: To detect threats and vulnerabilities that might lead to security breaches.
- **Performance**: To improve the speed of your applications.
- **Cost**: To optimize and reduce your overall Azure spending
- **Operational excellence**: To help you achieve process and workflow efficiency, resource manageability, and deployment best practices.





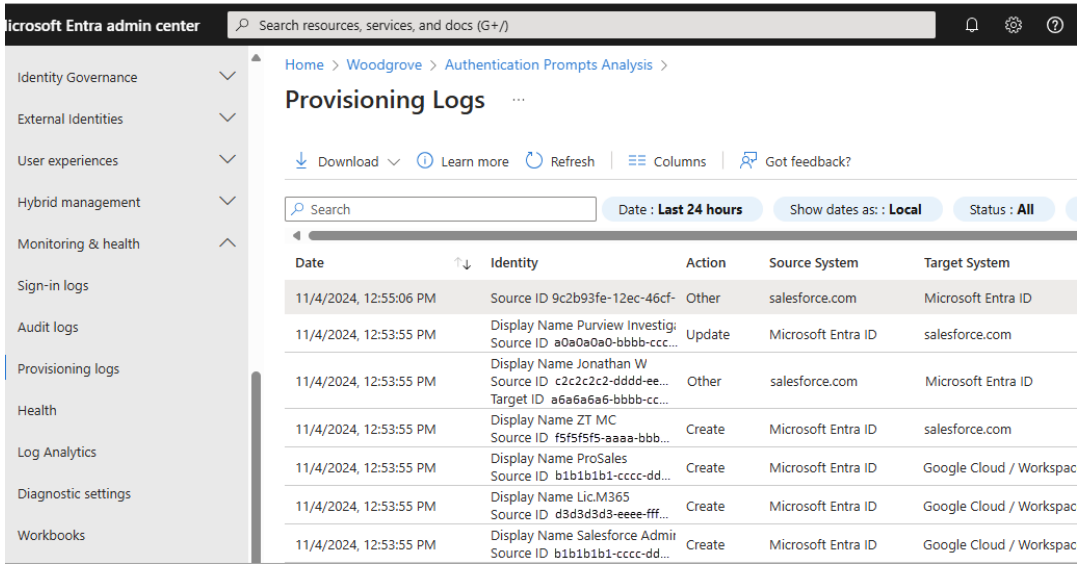
Azure Advisor workbooks

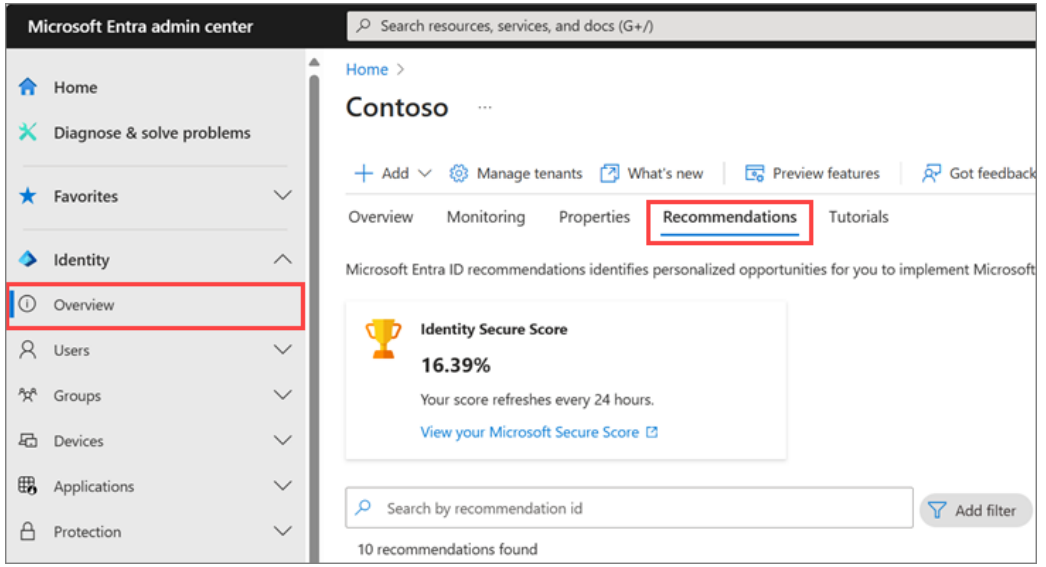


Microsoft Entra logs & reports

- **Audit Logs** (compliance, access promotion, password resets, etc)
- **Sign-in Logs** (who, when and what have been accessed, includes pattern recognition)
- **Provisioning Logs** (identity details about resource provisioning and reconfiguration)

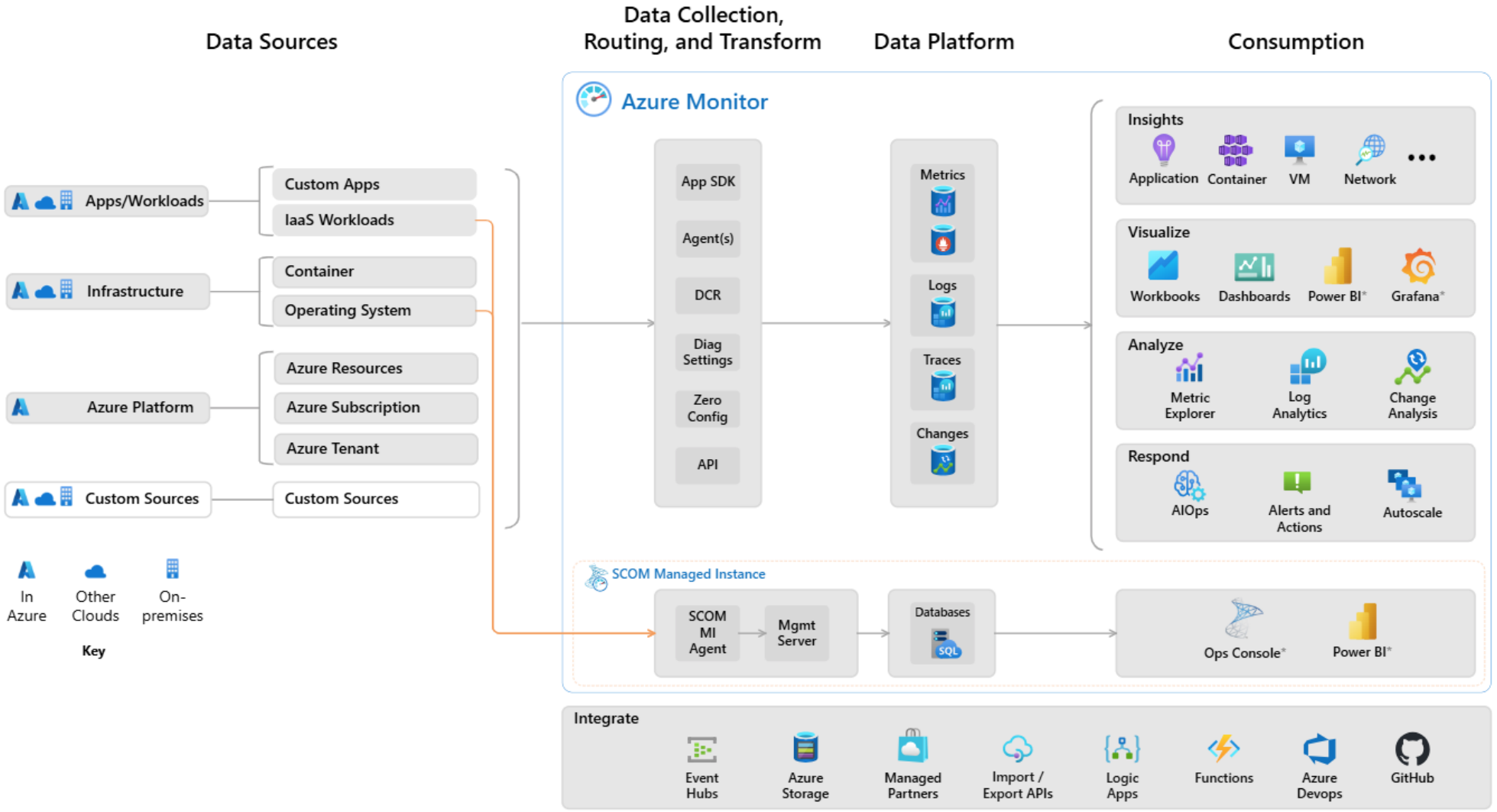
- **Identity Protection**
- **Application activities**
- **Entra Workbooks**
- **Microsoft Entra Recommendations**
- **Microsoft Entra Health**





Monitoring Azure Platform

Azure Monitor

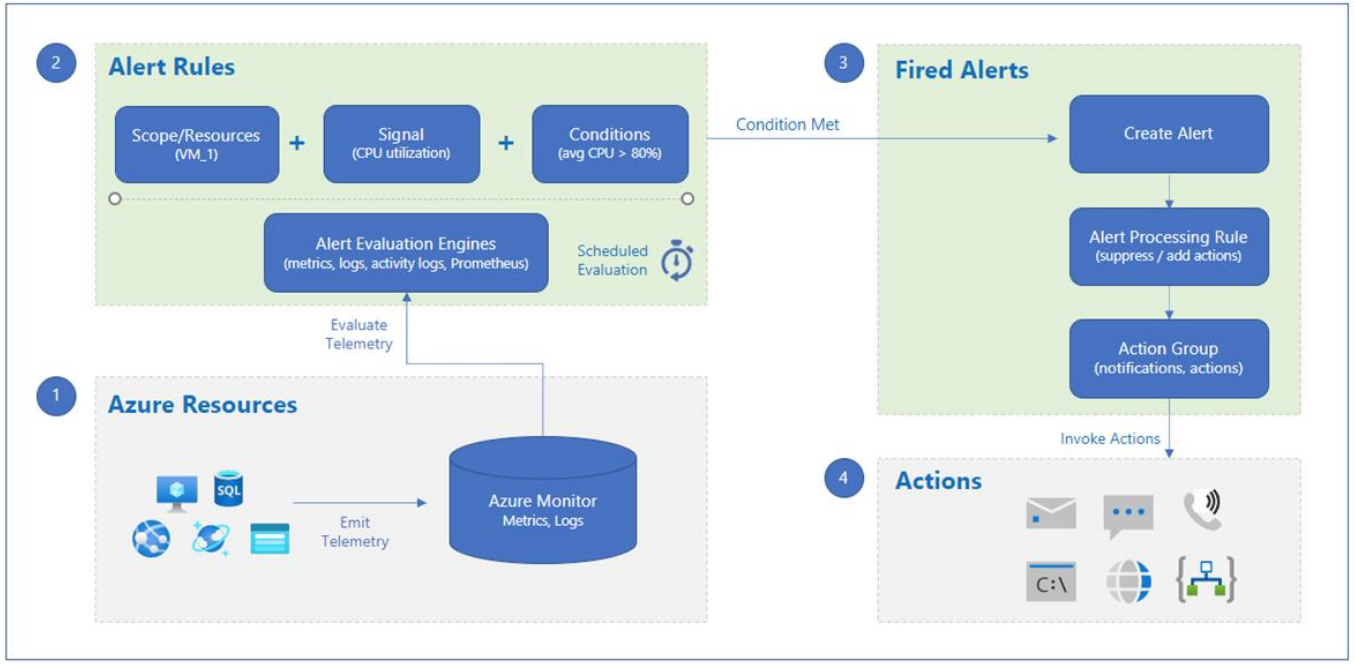


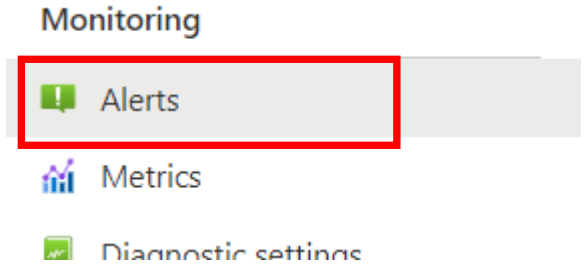
Azure Monitor: pillars of Observability & data storage

Pillar of Observability/ Data Store	Description
Azure Monitor Metrics	Metrics are numerical values that describe an aspect of a system at a particular point in time. Azure Monitor Metrics is a time-series database, optimized for analyzing time-stamped data. Azure Monitor collects metrics at regular intervals. Metrics are identified with a timestamp, a name, a value, and one or more defining labels. They can be aggregated using algorithms, compared to other metrics, and analyzed for trends over time. It supports native Azure Monitor metrics and Prometheus metrics.
Azure Monitor Logs	Logs are recorded system events. Logs can contain different types of data, be structured or free-form text, and they contain a timestamp. Azure Monitor stores structured and unstructured log data of all types in Azure Monitor Logs. You can route data to Log Analytics workspaces for querying and analysis.
Traces	Distributed tracing allows you to see the path of a request as it travels through different services and components. Azure Monitor gets distributed trace data from instrumented applications. The trace data is stored in a separate workspace in Azure Monitor Logs.
Changes	Changes are a series of events in your application and resources. They're tracked and stored when you use the Change Analysis (classic) service, which uses Azure Resource Graph as its store. Change Analysis (classic) helps you understand which changes, such as deploying updated code, may have caused issues in your systems.

Azure Alerting

- Built-in platform alerting for
  - Azure Monitor & other services (Metrics, Logs, Service Health & others)
- Supports only Azure platform pipeline (not DMVs or XEvents)
- Delivery of alerting through
  - Notification: Email, SSMS message, Voice
  - Actions: Runbook, Azure Function, Event Hub, ITSM, Logic App, Web hooks
- Cost
  - Per alert per month
  - See Azure monitor for pricing





Security monitoring on Azure SQL

Value proposition of Microsoft Defender for SQL



Discover and mitigate potential database vulnerabilities



Advanced threat protection



Alerts you to anomalous activities that might be an indication of a threat to your databases.

Vulnerability Assessment

Get visibility

- Discover sensitive data and potential security holes

Remediate

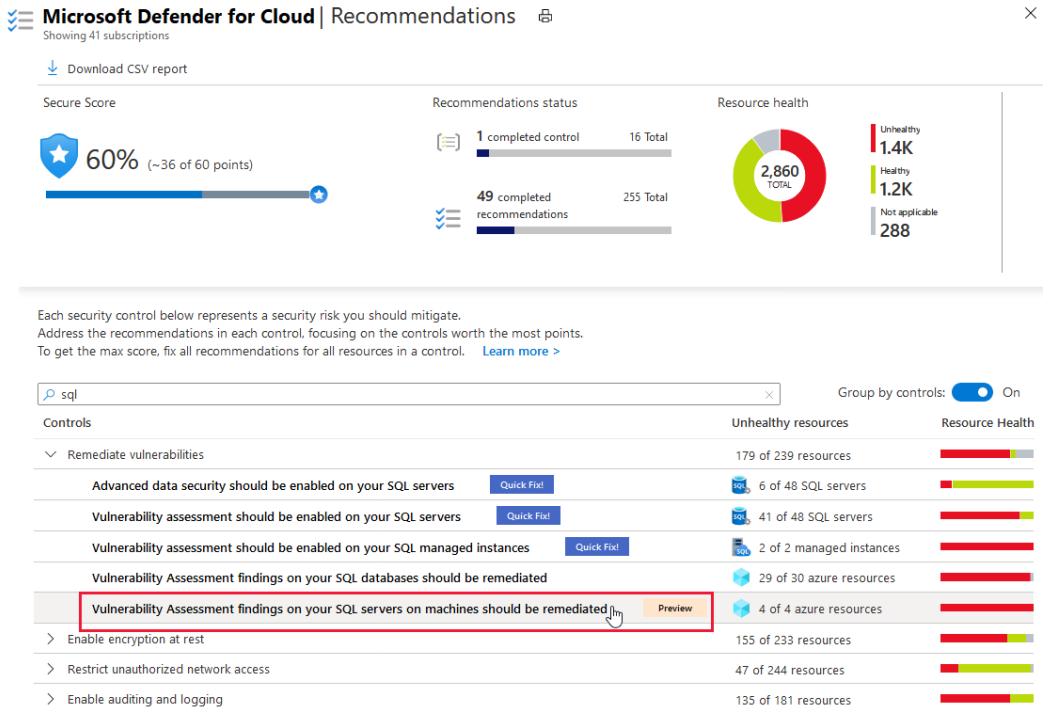
- Actionable remediation and security hardening steps

Customize

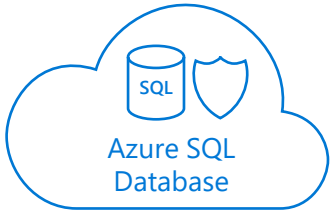
- Baseline policy tuned to your environment, allowing you to focus on deviations

Report

- Pass internal or external audits to facilitate compliance



Azure SQL Managed Instance



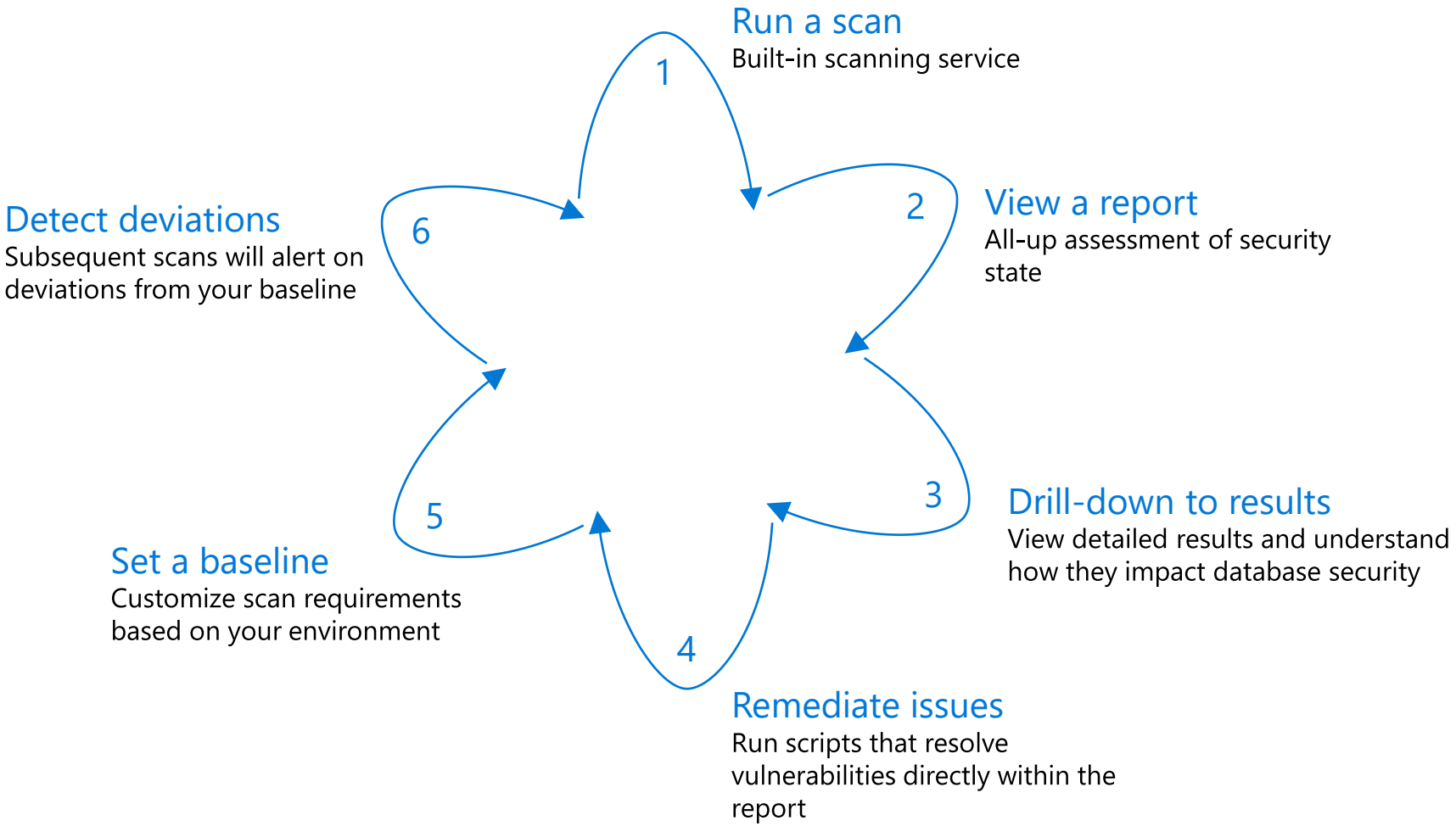
Vulnerability Assessment

Identifies, tracks, and resolves SQL security vulnerabilities



Developer/DBA

Vulnerability Assessment



SQL advanced threat protection

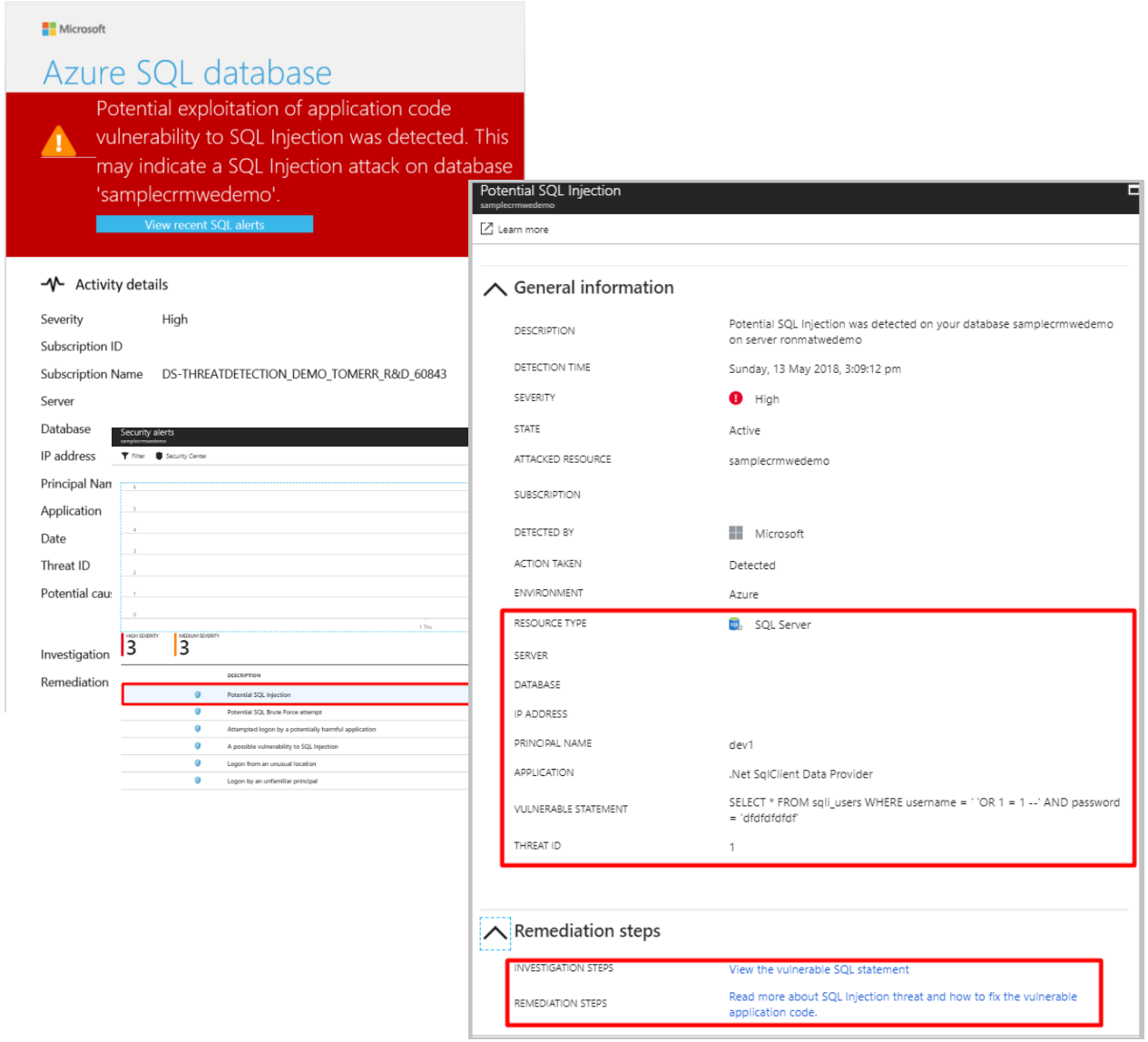
Receive an alert

- Suspicious database activities
- Potential vulnerabilities
- SQL injection attacks
- Anomalous database access and queries patterns

Details of suspicious activity

- Recommend action on how to investigate and mitigate the threat

Recommended to enable auditing



Microsoft Azure

Microsoft Purview

For Azure SQL DBAs



Discover and govern Azure SQL in Microsoft Purview

When you're scanning Azure SQL Database, Microsoft Purview supports extracting technical metadata from these sources:

- Server
- Database
- Schemas
- Tables, including columns
- Views, including columns (with lineage extraction enabled, as part of scanning)
- Stored procedures (with lineage extraction enabled)
- Stored procedure runs (with lineage extraction enabled)

Azure SQL Database

Metadata Extraction	Full Scan	Incremental Scan	Scoped Scan	Classification	Labeling	Access Policy	Lineage	Data Sharing	Live view
Yes	Yes	Yes	Yes	Yes	Yes	Yes (preview)	Yes (preview)	No	Yes

Azure SQL Managed Instance

Metadata Extraction	Full Scan	Incremental Scan	Scoped Scan	Classification	Labeling	Access Policy	Lineage	Data Sharing	Live view
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Limited**	No	No

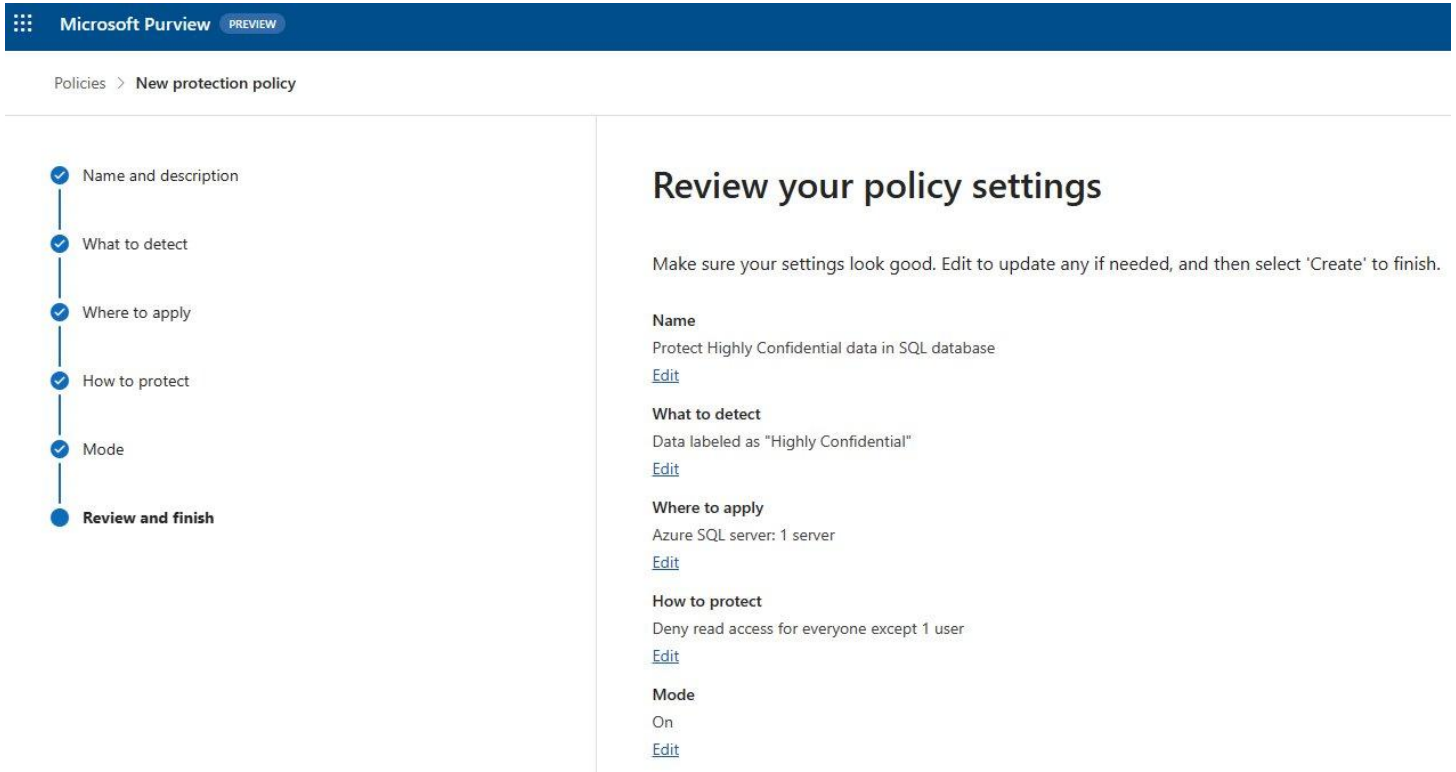
Label-based access control using Purview policies *(preview)*

Provision protection policies in Purview to restrict access to sensitive data in Azure SQL

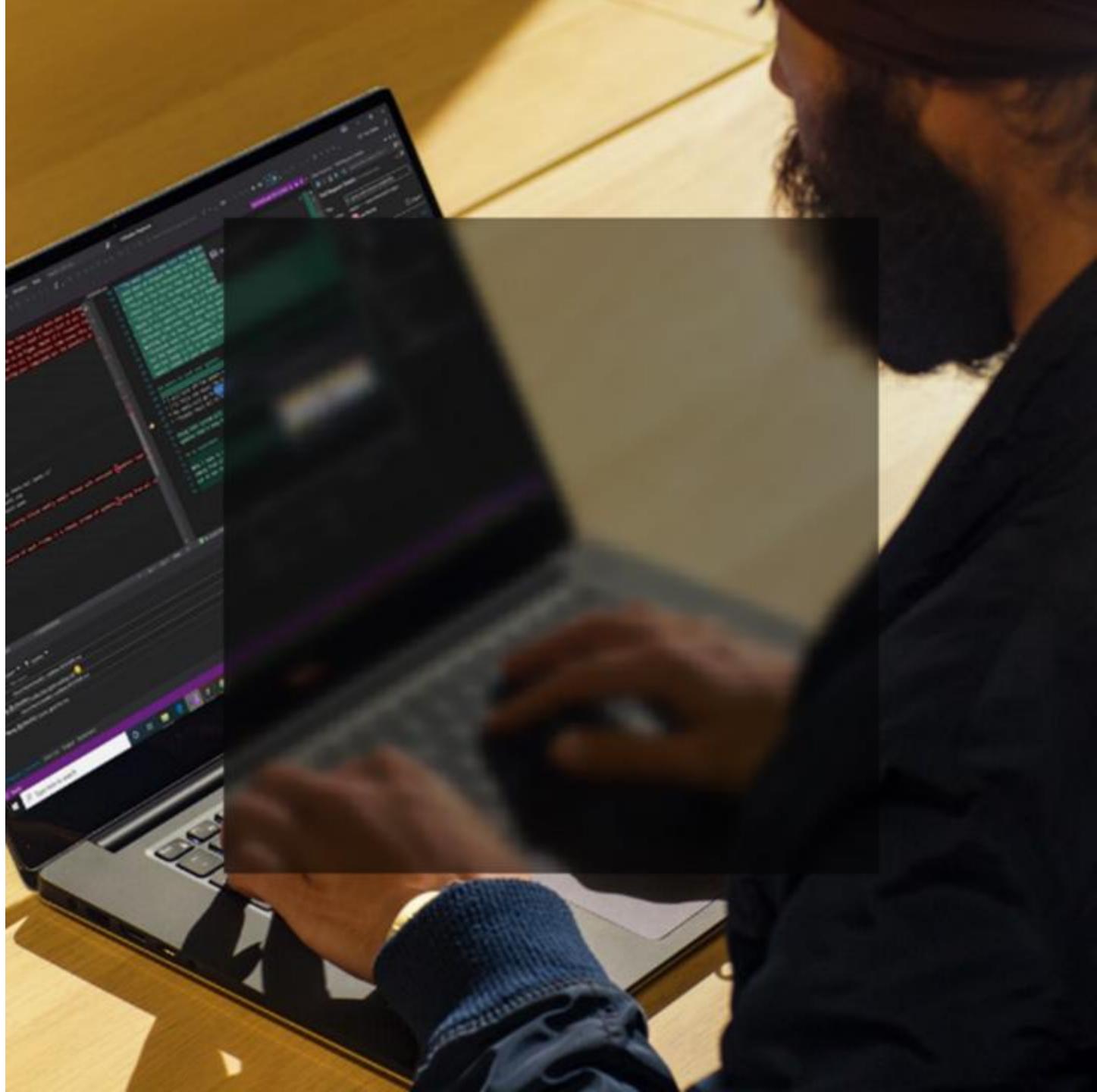
Enterprise admins can authorize data access for a particular sensitivity label to specific users/groups

Access control is automatically imposed whenever sensitive information is accessed by users

Getting started with the preview: https://aka.ms/sql-purview-protection-preview-docs



To be successful, What do you need from Azure SQL Observability?



Experience Azure SQL for free

Azure SQL Managed Instance

aka.ms/freesqlMI

What's included



- **1 instance** per Azure subscription
- **4 or 8 vCores** of GP compute
- **750 vCore hours** per month
- **64 GB data** storage
- **64 GB backup** storage

Use it for 12 months



Use this free offer to support your migration proof of concepts for **12 months.**

You're in control



- Optimize your monthly available vCore hours by **stopping** and **starting** the instance when necessary.

Azure SQL Database

aka.ms/SQLfreeoffer

What's included



- **1 Azure SQL Database** per Azure subscription
- **100,000 vCore seconds** per month.
- **32 GB data** storage
- **32 GB backup** storage

No time limits



- Apply this free offer for the **life** of your **subscription**.

Need more? No problem.



- Stick with the default **auto-pause** option or continue usage for additional charges.