# SoftwareONE

EMPOWERING COMPANIES TO TRANSFORM

## Azure Monitor – News & Updates

Haiko Hertes

softwareONE

HERTES.NET knowledge - experience - insights

E = M Cᵀ

MVP Microsoft® Most Valuable Professional

- Seit 2019 bei SoftwareONE
- Principal Consultant & Architect im Azure Consulting Team
- Vorher IT-Leiter im Mittelstand
- Microsoft MVP und Speaker in diversen Communities

www.hertes.net

about.me/haiko.hertes

twitter.com/HHertes

youtube.com/c/HaikoHertes

# Haiko Hertes

**Cloud Architect / Principal Consultant**

softwareONE

# AGENDA

**01** Manage Log Analytics Tables in Azure Portal

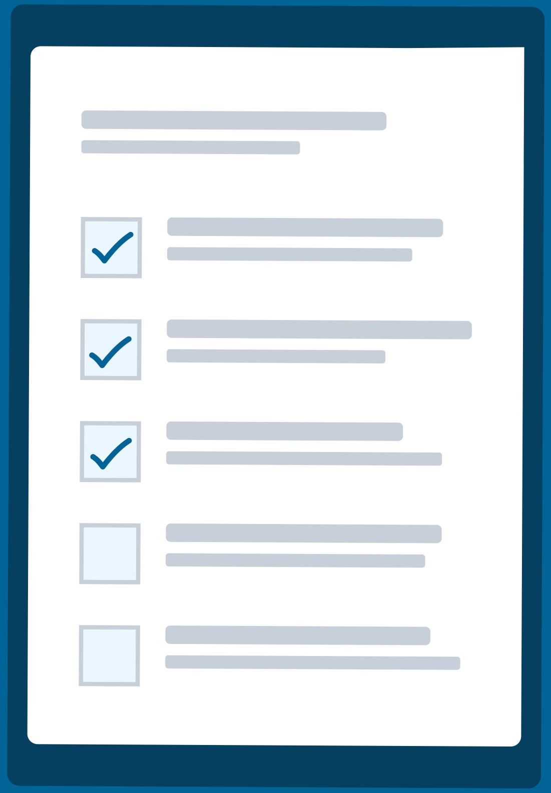
**02** Basic Logs + Data Retention Management

**03** Ingestion-time Log transformations

**04** Azure Monitor Agent changes

**05** Predictive Autoscale

**06** Change Analysis / Tracking

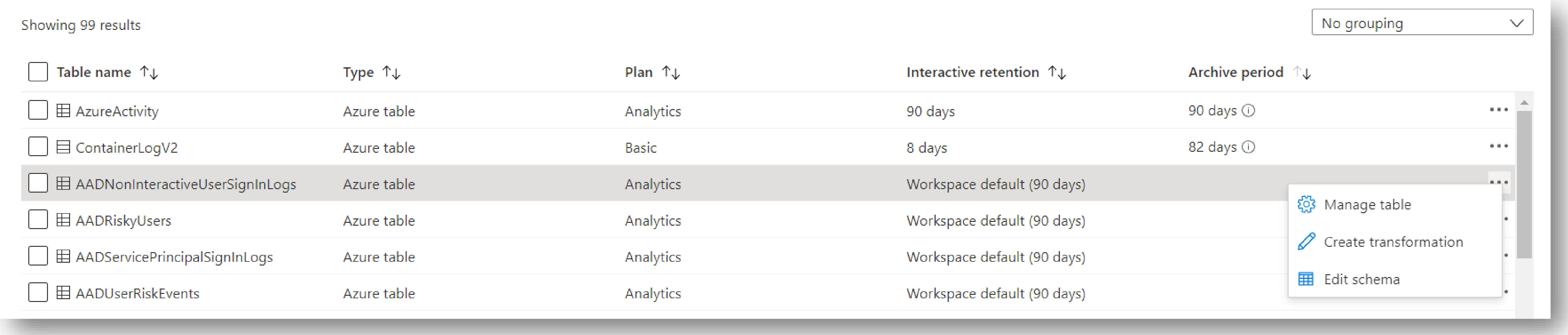


01

# Manage tables in Portal

# Manage Log Analytics Tables in Azure Portal

- You can now manage Log Analytics Tables directly via the Portal
  - View list of existing tables (inluding properties)
  - Change some details (next topics ;))
  - Create or delete a table
  - Manage table schema /



Showing 99 results

No grouping

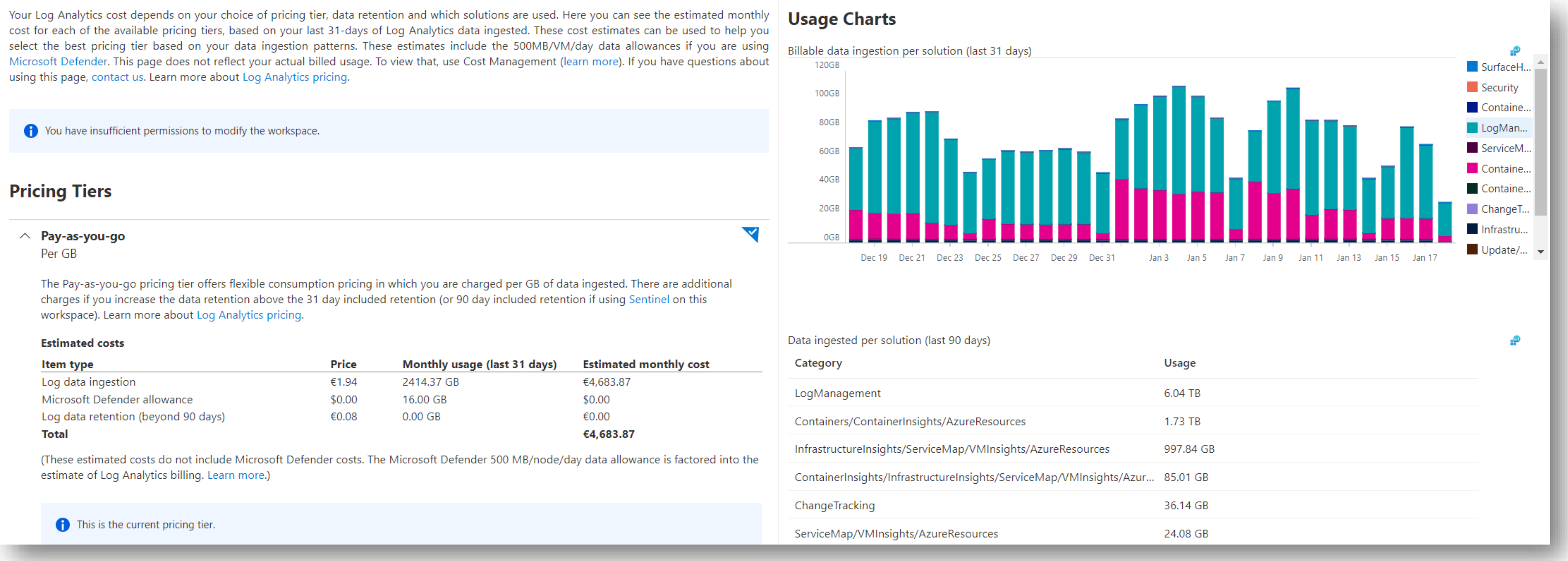
| □ Table name ↑↓ | Type ↑↓ | Plan ↑↓ | Interactive retention ↑↓ | Archive period ↑↓ |
|---|---|---|---|---|
| □ AzureActivity | Azure table | Analytics | 90 days | 90 days ⓘ |
| □ ContainerLogV2 | Azure table | Basic | 8 days | 82 days ⓘ |
| □ AADNonInteractiveUserSignInLogs | Azure table | Analytics | Workspace default (90 days) | |
| □ AADRiskyUsers | Azure table | Analytics | Workspace default (90 days) | |
| □ AADServicePrincipalSignInLogs | Azure table | Analytics | Workspace default (90 days) | |
| □ AADUserRiskEvents | Azure table | Analytics | Workspace default (90 days) | |

[General availability: Manage your Log Analytics Tables in Azure Portal | Azure updates | Microsoft Azure]

## 02

# Basic Logs & Data Retention

# Basic Logs & Data Retention



Your Log Analytics cost depends on your choice of pricing tier, data retention and which solutions are used. Here you can see the estimated monthly cost for each of the available pricing tiers, based on your last 31-days of Log Analytics data ingested. These cost estimates can be used to help you select the best pricing tier based on your data ingestion patterns. These estimates include the 500MB/VM/day data allowances if you are using Microsoft Defender. This page does not reflect your actual billed usage. To view that, use Cost Management (learn more). If you have questions about using this page, contact us. Learn more about Log Analytics pricing.

You have insufficient permissions to modify the workspace.

## Pricing Tiers

**Pay-as-you-go**

Per GB

The Pay-as-you-go pricing tier offers flexible consumption pricing in which you are charged per GB of data ingested. There are additional charges if you increase the data retention above the 31 day included retention (or 90 day included retention if using Sentinel on this workspace). Learn more about Log Analytics pricing.

**Estimated costs**

| Item type | Price | Monthly usage (last 31 days) | Estimated monthly cost |
|---|---|---|---|
| Log data ingestion | €1.94 | 2414.37 GB | €4,683.87 |
| Microsoft Defender allowance | $0.00 | 16.00 GB | $0.00 |
| Log data retention (beyond 90 days) | €0.08 | 0.00 GB | €0.00 |
| **Total** | | | **€4,683.87** |

(These estimated costs do not include Microsoft Defender costs. The Microsoft Defender 500 MB/node/day data allowance is factored into the estimate of Log Analytics billing. Learn more.)

This is the current pricing tier.

## Usage Charts

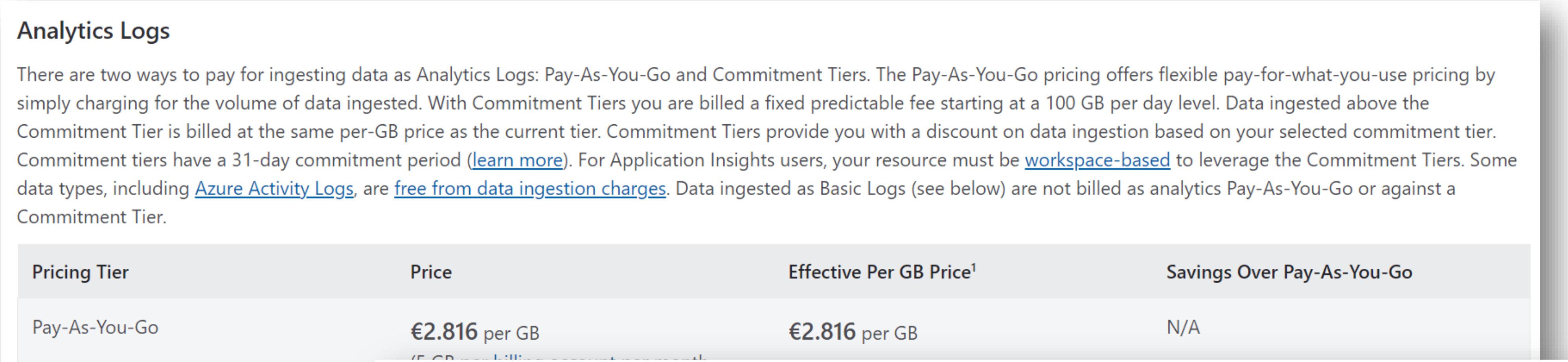
Billable data ingestion per solution (last 31 days)

Data ingested per solution (last 90 days)

| Category | Usage |
|---|---|
| LogManagement | 6.04 TB |
| Containers/ContainerInsights/AzureResources | 1.73 TB |
| InfrastructureInsights/ServiceMap/VMInsights/AzureResources | 997.84 GB |
| ContainerInsights/InfrastructureInsights/ServiceMap/VMInsights/Azur... | 85.01 GB |
| ChangeTracking | 36.14 GB |
| ServiceMap/VMInsights/AzureResources | 24.08 GB |

# Basic Logs & Data Retention

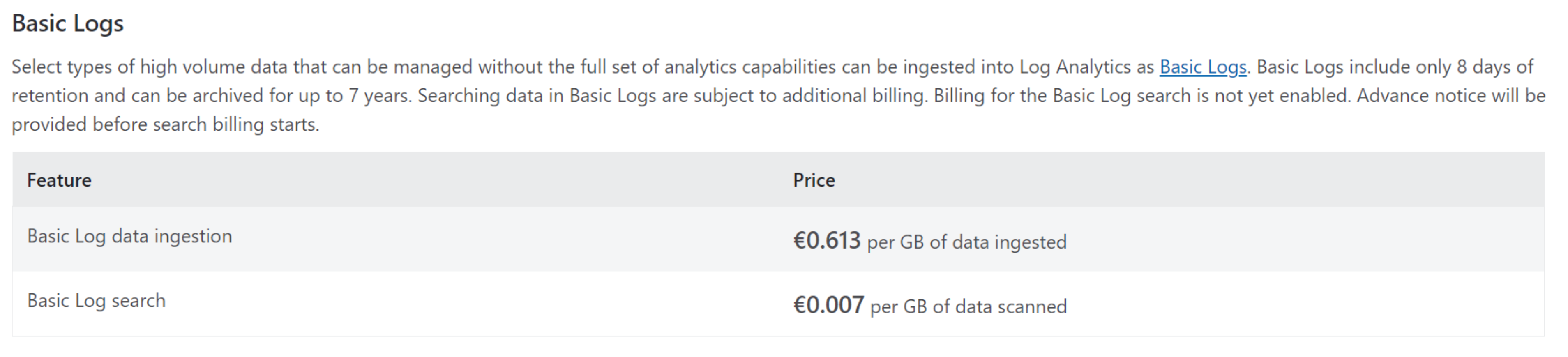
- Basic Logs allow to keep „noisy“ data on a cheaper tier (for max. 8 days)
- New option next to the old log type now called „Analytics Logs“
- Does NOT support all types of queries
- Ingestion is cheaper, but searching within Log data has a price tag instead



### Analytics Logs

There are two ways to pay for ingesting data as Analytics Logs: Pay-As-You-Go and Commitment Tiers. The Pay-As-You-Go pricing offers flexible pay-for-what-you-use pricing by simply charging for the volume of data ingested. With Commitment Tiers you are billed a fixed predictable fee starting at a 100 GB per day level. Data ingested above the Commitment Tier is billed at the same per-GB price as the current tier. Commitment Tiers provide you with a discount on data ingestion based on your selected commitment tier. Commitment tiers have a 31-day commitment period (learn more). For Application Insights users, your resource must be workspace-based to leverage the Commitment Tiers. Some data types, including Azure Activity Logs, are free from data ingestion charges. Data ingested as Basic Logs (see below) are not billed as analytics Pay-As-You-Go or against a Commitment Tier.

| Pricing Tier | Price | Effective Per GB Price[1] | Savings Over Pay-As-You-Go |
|---|---|---|---|
| Pay-As-You-Go | **€2.816** per GB | **€2.816** per GB | N/A |



### Basic Logs

Select types of high volume data that can be managed without the full set of analytics capabilities can be ingested into Log Analytics as Basic Logs. Basic Logs include only 8 days of retention and can be archived for up to 7 years. Searching data in Basic Logs are subject to additional billing. Billing for the Basic Log search is not yet enabled. Advance notice will be provided before search billing starts.

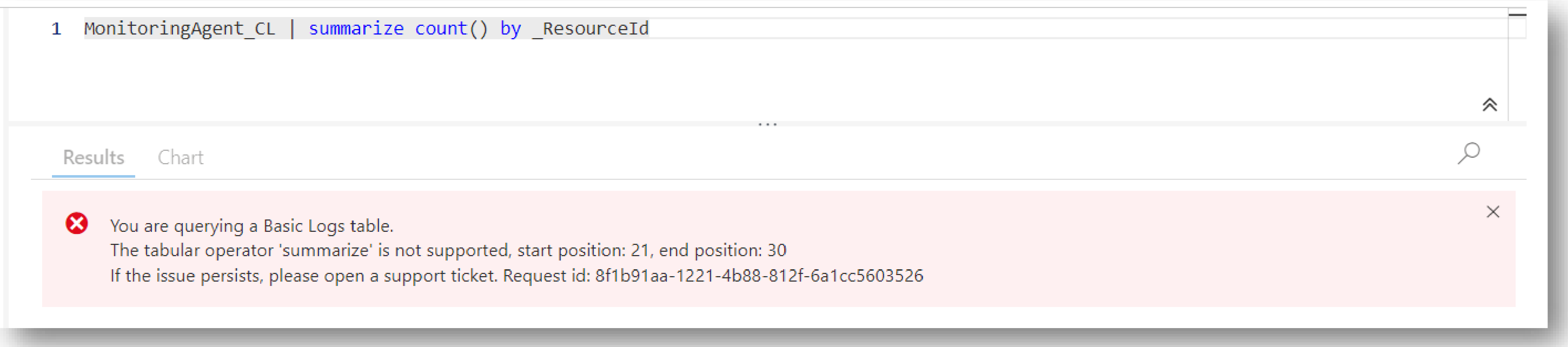
| Feature | Price |
|---|---|
| Basic Log data ingestion | **€0.613** per GB of data ingested |
| Basic Log search | **€0.007** per GB of data scanned |

# Basic Logs & Data Retention

| Category | Analytics | Basic |
|---|---|---|
| **Ingestion** | Regular ingestion cost.<br>(WEU: 2.816€/GB) | Reduced ingestion cost.<br>(WEU: 0.613€/GB) |
| **Log queries** | Full query capabilities<br>No extra cost. | Basic query capabilities.<br>Pay-per-use.<br>(WEU: 0.007€/GB scanned) |
| **Retention** | Configure retention from 30 days to two years. | Retention fixed at 8 days.<br>When you change an existing table's plan to Basic logs, Azure archives data that's more than eight days old but still within the table's original retention period. |
| **Alerts** | Supported. | Not supported. |

# Basic Logs & Data Retention

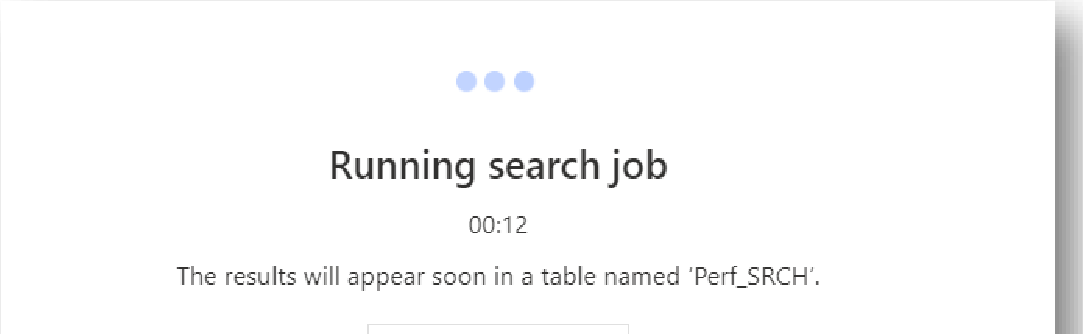
- Query on Basic Logs =~ Search Jobs
- Search Jobs would allow log queries that would otherwise run into timeout (10min)
- Basic Log queries and Search Jobs have the same limitations



```
MonitoringAgent_CL | summarize count() by _ResourceId
```

You are querying a Basic Logs table.
The tabular operator 'summarize' is not supported, start position: 21, end position: 30
If the issue persists, please open a support ticket. Request id: 8f1b91aa-1221-4b88-812f-6a1cc5603526

- When running a Search Job, result is then saved into a new table



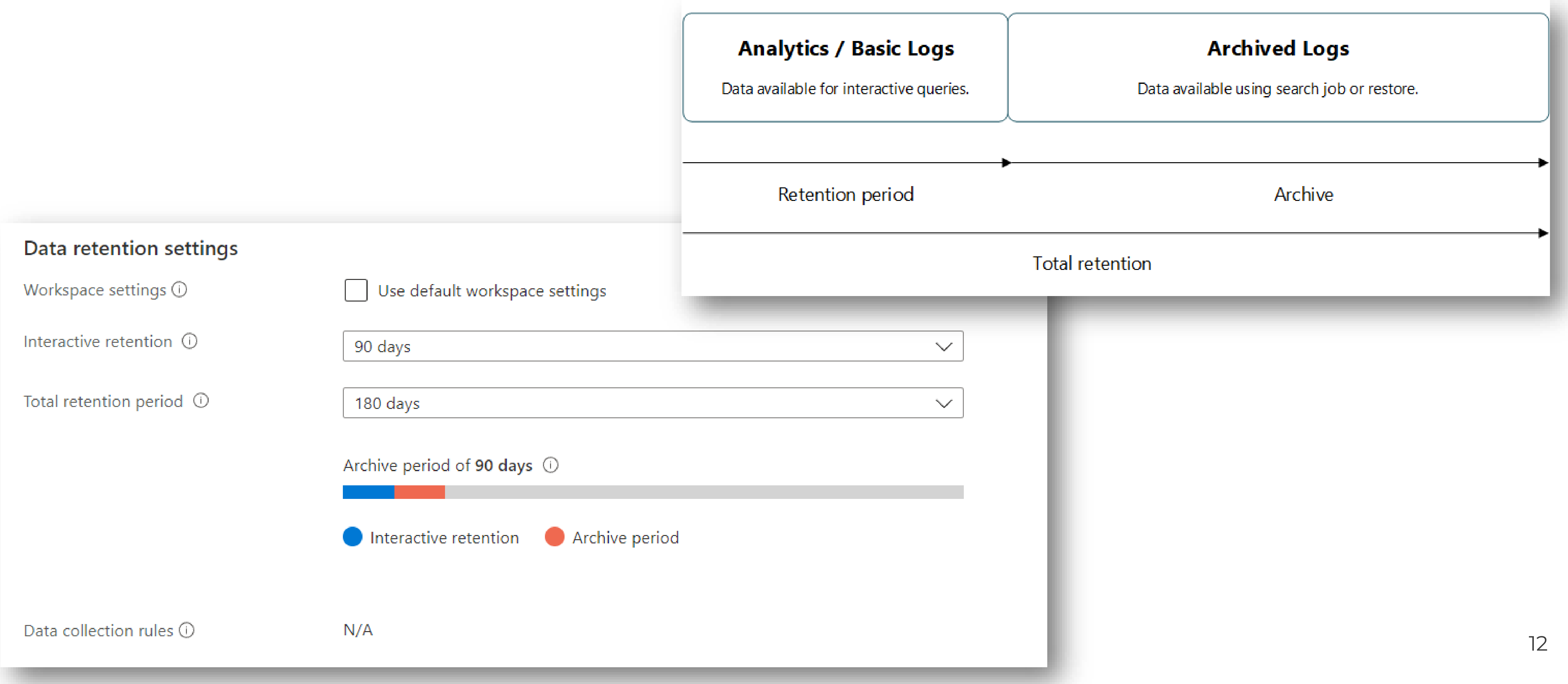
Running search job

00:12

The results will appear soon in a table named 'Perf_SRCH'.

# Basic Logs & Data Retention

- Another new option is to move log data to Archive tier to save on retention cost
- Data on archive cannot be read directly – need to get „rehydrated“ or using search jobs



**Analytics / Basic Logs**

Data available for interactive queries.

**Archived Logs**

Data available using search job or restore.

**Data retention settings**

Workspace settings ⓘ □ Use default workspace settings

Interactive retention ⓘ 90 days

Total retention period ⓘ 180 days

Archive period of **90 days** ⓘ

● Interactive retention ● Archive period

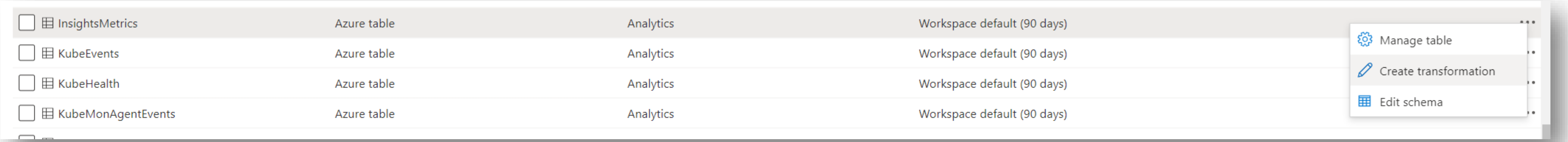
Data collection rules ⓘ N/A

03

# Ingestion-Time Transformation

# Ingestion-time Log transformations

- Usually, you cannot control, which data is sent to a log analytics workspace in detail
- You might get columns that you don‘t need – but need to pay for
- A transformation is using KQL and a data collection rule to alter the data that is saved in Log Analytics (i.e. you coul project-away columns)
- Also, the syntax for the transformation query is limited as of now (i.e. no „summarize“)



| | | | |
|---|---|---|---|
| □ InsightsMetrics | Azure table | Analytics | Workspace default (90 days) |
| □ KubeEvents | Azure table | Analytics | Workspace default (90 days) |
| □ KubeHealth | Azure table | Analytics | Workspace default (90 days) |
| □ KubeMonAgentEvents | Azure table | Analytics | Workspace default (90 days) |

General availability: Azure Monitor Logs, custom log API and ingestion-time transformations | Azure updates | Microsoft Azure

# 04

# Azure Monitor Agent

# Azure Monitor Agent

- Text Logs / IIS Logs
- Support for Windows Client OS through MSI Installer (not for Servers!)
- Agent Migration Tools / DCR config generator

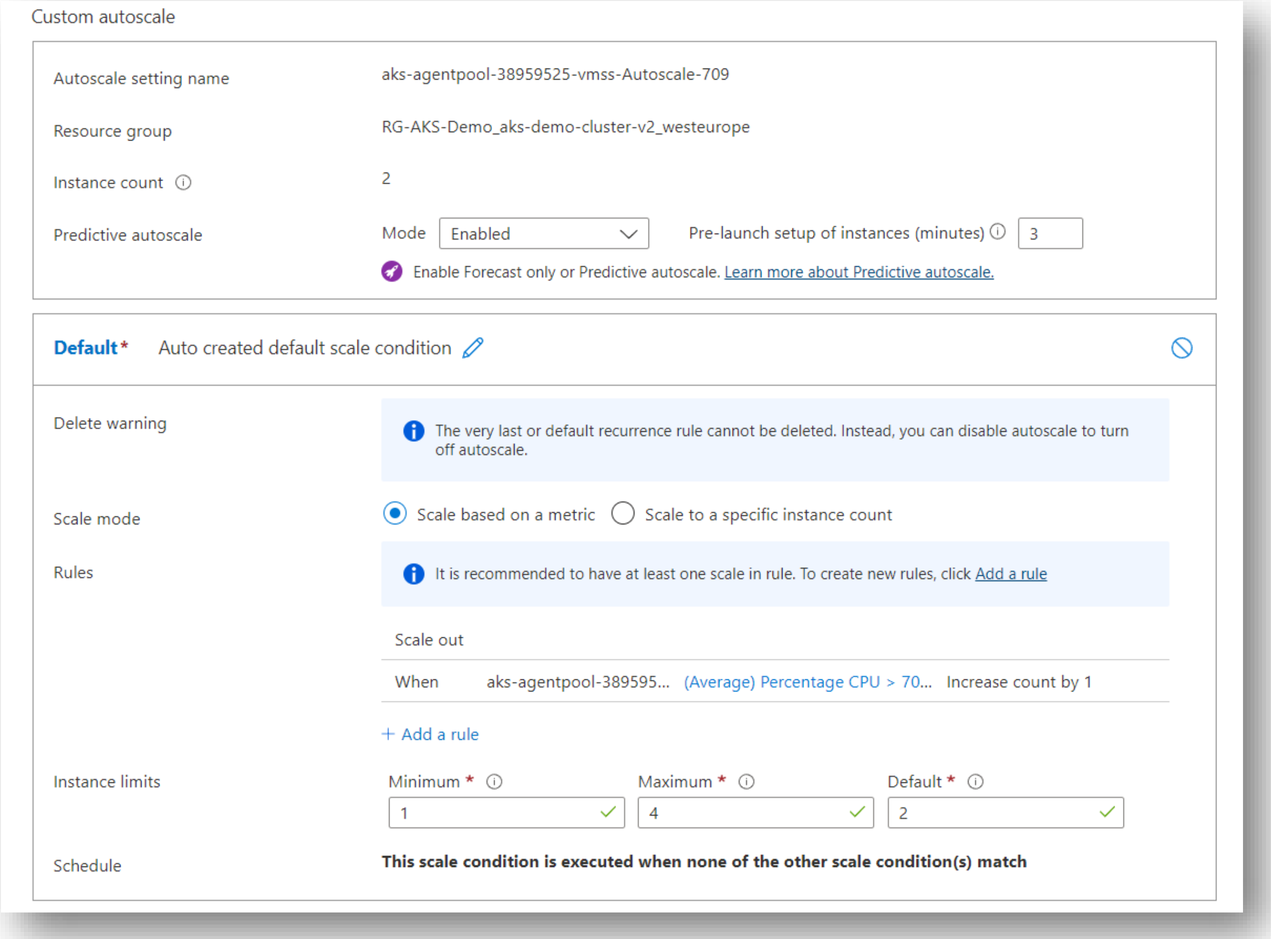
General availability: Azure Monitor agent custom and IIS logs | Azure updates | Microsoft Azure

# 05

# Predictive Autoscale

# Predictive Autoscale

- Scaling a system when it is already under load is often useless – more capacity is available when load already decreases
- Load balancing for VMSS allows using usage data now to predict high load and scale in advance
- Only works on „Percentage CPU“ now



Custom autoscale

Autoscale setting name: aks-agentpool-38959525-vmss-Autoscale-709

Resource group: RG-AKS-Demo_aks-demo-cluster-v2_westeurope

Instance count ⓘ: 2

Predictive autoscale: Mode: Enabled; Pre-launch setup of instances (minutes) ⓘ: 3

Enable Forecast only or Predictive autoscale. Learn more about Predictive autoscale.

**Default*** Auto created default scale condition

Delete warning: The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode: ● Scale based on a metric ○ Scale to a specific instance count

Rules: It is recommended to have at least one scale in rule. To create new rules, click Add a rule

Scale out

When aks-agentpool-389595... (Average) Percentage CPU > 70... Increase count by 1

+ Add a rule

Instance limits: Minimum * ⓘ 1 ✓ Maximum * ⓘ 4 ✓ Default * ⓘ 2 ✓

Schedule: **This scale condition is executed when none of the other scale condition(s) match**

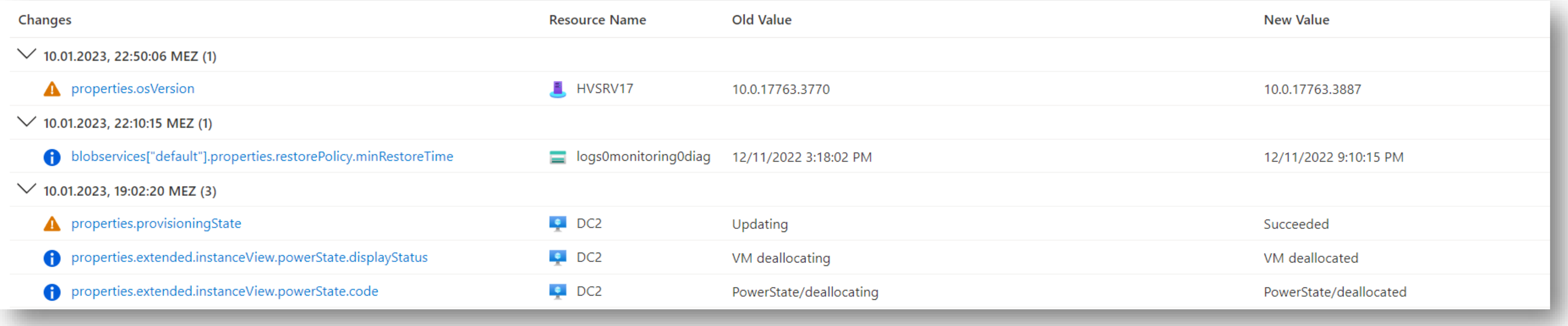
General availability: Azure Monitor predictive autoscale for Azure Virtual Machine Scale Sets | Azure updates | Microsoft Azure

# 06

# Change Analysis

# Change Analysis / Tracking

- GA since August 2022
- Built on top of Azure Resource Graph
- Stores resource and application configuration changes
- Has RBAC on top
- Allows to better find reasons for outages / issues



| Changes | Resource Name | Old Value | New Value |
|---|---|---|---|
| 10.01.2023, 22:50:06 MEZ (1) | | | |
| ⚠ properties.osVersion | HVSRV17 | 10.0.17763.3770 | 10.0.17763.3887 |
| 10.01.2023, 22:10:15 MEZ (1) | | | |
| ℹ blobservices["default"].properties.restorePolicy.minRestoreTime | logs0monitoring0diag | 12/11/2022 3:18:02 PM | 12/11/2022 9:10:15 PM |
| 10.01.2023, 19:02:20 MEZ (3) | | | |
| ⚠ properties.provisioningState | DC2 | Updating | Succeeded |
| ℹ properties.extended.instanceView.powerState.displayStatus | DC2 | VM deallocating | VM deallocated |
| ℹ properties.extended.instanceView.powerState.code | DC2 | PowerState/deallocating | PowerState/deallocated |

# 07

# And much more…

# Smaller Changes

- Action Groups can be saved within Germany if needed (data-protection reasons) (Generally available: Action groups can now be saved and processed within Europe | Azure updates | Microsoft Azure)
- Azure Monitor Agent supports ARM64-based VMs now
- SCOM managed instance (Preview)
- Anomalie detection with KQL machine learning capabilities
- Azure Monitor Workspace (Preview)

# Current Previews

- Container insights support for AKS hybrid clusters (Public Preview: Container insights support for AKS hybrid clusters | Azure updates | Microsoft Azure)
- Azure Monitor managed service for Prometheus (Public preview: Azure Monitor managed service for Prometheus | Azure updates | Microsoft Azure)
- Ampere Altra ARM-based VMs support (Public preview: Monitoring for Ampere Altra Arm–based VMs and AKS clusters | Azure updates | Microsoft Azure)

# Questions?

# Haiko Hertes

Haiko.Hertes@SoftwareONE.com