



10 coole Features im Azure Monitor, die ihr (vielleicht) noch nicht kanntet

Haiko Hertes, Azure Architect & Principal Consultant, Microsoft Azure MVP

20.06.2023



- Seit 2019 bei SoftwareOne
- Principal Consultant & Architect
- Azure Consulting Team
- Microsoft MVP, YouTuber,
Blogger, Conference Speaker
- Familievater, Offizier d.R.,
Holzwurm



www.hertes.net



about.me/haiko.hertes



twitter.com/HHertes



youtube.com/c/HaikoHertes

Haiko Hertes
Cloud Architect / Principal Consultant
software one

01

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	HVSERV17	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

02

Basic Logs

Basic Logs

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](#).

i 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](#).)

i 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

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

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

Category	Analytics	Basic
Ingestion	Regular ingestion cost. (WEU: 2.816€/GB)	Reduced ingestion cost. (WEU: 0.613€/GB)
Log queries	Full query capabilities No extra cost.	Basic query capabilities. Pay-per-use. (WEU: 0.007€/GB scanned)
Retention	Configure retention from 30 days to two years.	Retention fixed at 8 days. 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

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

The screenshot shows a search interface with a query editor at the top containing the text: 1 MonitoringAgent_CL | summarize count() by _ResourceId. Below the editor is a results pane. A red error message box is displayed, stating: 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 r

The screenshot shows a window titled "Running search job" with a progress bar indicating "00:12". Below the title, it says "The results will appear soon in a table named 'Perf_SRCH'". There are three blue dots above the progress bar.

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 can project-away columns)

Also, the syntax for the transformation query is limited as of now (i.e. no „summarize“)

<input type="checkbox"/> InsightsMetrics	Azure table	Analytics	Workspace default (90 days)	Manage table
<input type="checkbox"/> KubeEvents	Azure table	Analytics	Workspace default (90 days)	Create transformation
<input type="checkbox"/> KubeHealth	Azure table	Analytics	Workspace default (90 days)	Edit schema
<input type="checkbox"/> KubeMonAgentEvents	Azure table	Analytics	Workspace default (90 days)	
<input type="checkbox"/>				

[General availability: Azure Monitor Logs, custom log API and ingestion-time transformations | Azure updates | Microsoft Azure](#)

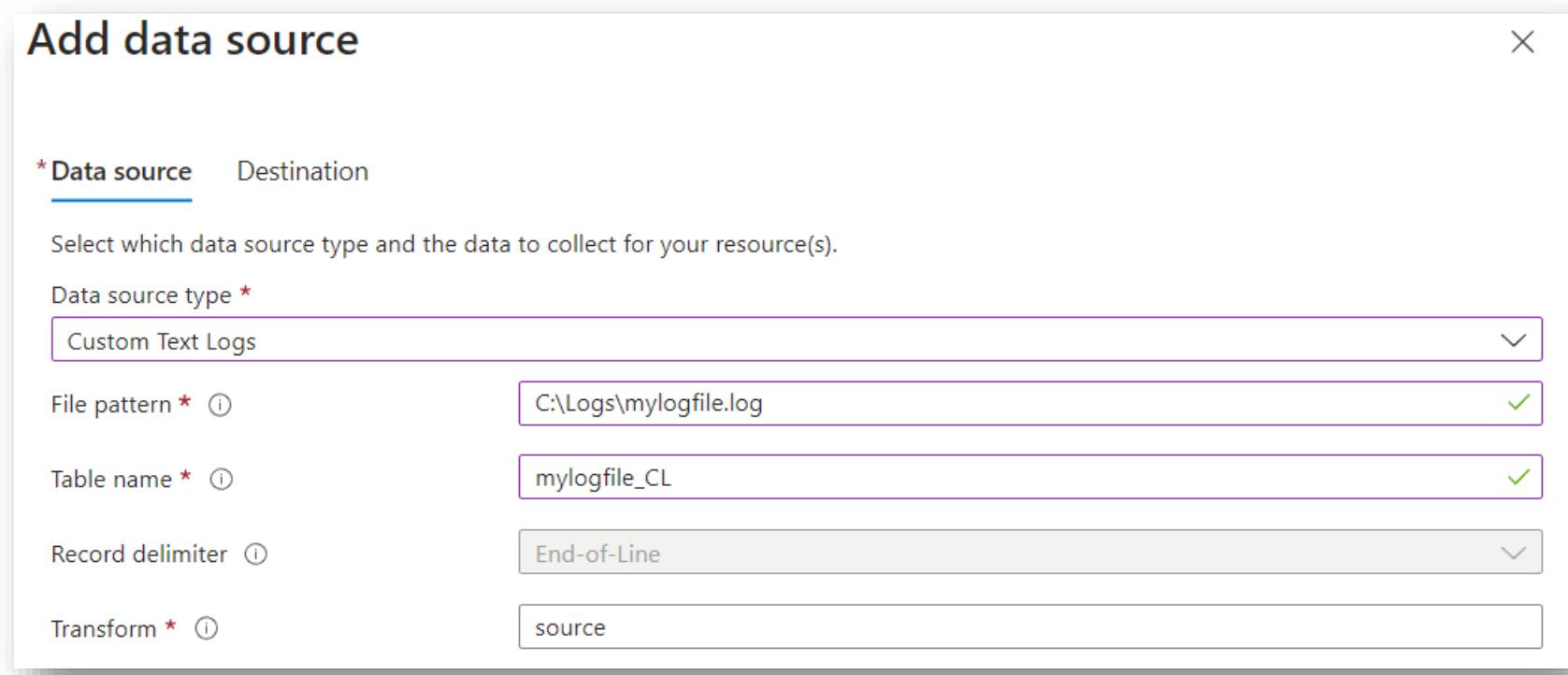


04

Text-based Logfiles with AMA

Text-based Logfiles with AMA

- Uses AMA on Linux and Windows
- Needs DCR amd DCE
- Custom Table as destination, needs to be created manually





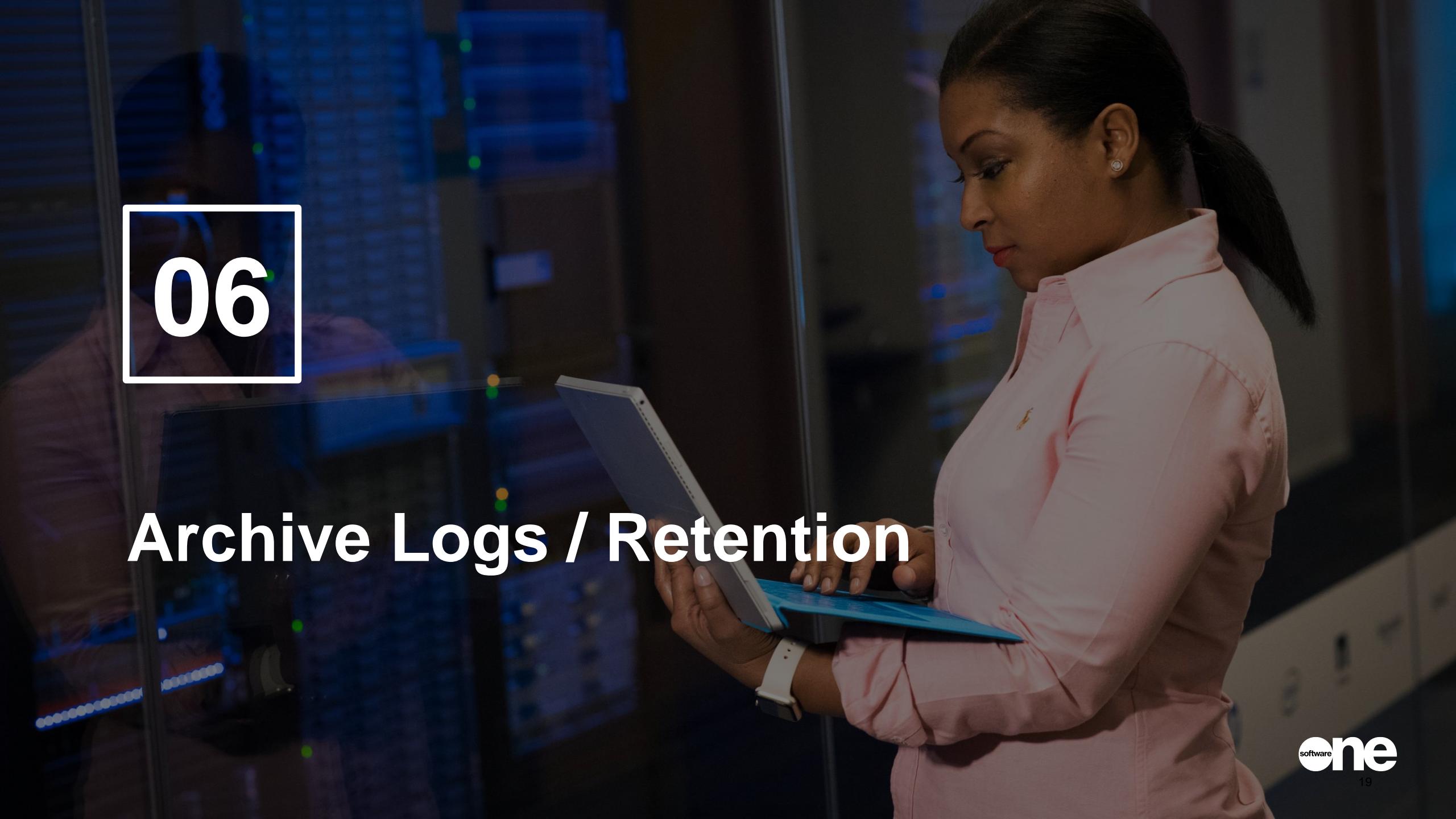
05

Built-in Policies for Diagnostic Settings

Built-in policies to enable Diagnostic Settings at Scale

The screenshot shows the Azure Policy Definitions blade. On the left, there's a navigation menu with links like Overview, Getting started, Compliance, Remediation, and Events. Below that is an Authoring section with three tabs: Definitions (selected), Assignments, and Exemptions. The main area has a search bar and filters for Scope (3 selected), Definition type (All definition types), Category (1 categories), and a search term (diag). A note says: "The export to GitHub experience has been deprecated due to scalability issues. We are looking to introduce a similar experience using SDK in our documentation." The table lists 14 built-in policy definitions:

Name	Definition location	Policies	Type	Definition type	Category
Deploy Diagnostic Settings for Batch Account to Event Hub			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Batch Account to Log Analytics workspace			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Data Lake Analytics to Event Hub			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Data Lake Analytics to Log Analytics workspace			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Data Lake Storage Gen1 to Event Hub			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Data Lake Storage Gen1 to Log Analytics workspace			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Event Hub to Event Hub			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Event Hub to Log Analytics workspace			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Key Vault to Log Analytics workspace			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Logic Apps to Event Hub			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Logic Apps to Log Analytics workspace			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Network Security Groups			Builtin	Policy	Monitoring
Deploy Diagnostic Settings for Search Services to Event Hub			Builtin	Policy	Monitoring



06

Archive Logs / Retention

Archive 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

The screenshot shows the 'Data retention settings' section of a software interface. At the top, there are two boxes: 'Analytics / Basic Logs' (Data available for interactive queries) and 'Archived Logs' (Data available using search job or restore). A horizontal arrow points from the left towards the right, labeled 'Retention period' above it and 'Archive' below it. Below this, another horizontal arrow points further to the right, labeled 'Total retention'. On the left, under 'Data retention settings', there are three dropdown menus: 'Workspace settings' (with an 'Use default workspace settings' checkbox), 'Interactive retention' (set to 90 days), and 'Total retention period' (set to 180 days). Below these is a legend: 'Archive period of 90 days' with a blue bar (labeled 'Interactive retention') and a red bar (labeled 'Archive period'). At the bottom, 'Data collection rules' is listed as 'N/A'.

Setting	Value
Workspace settings	<input type="checkbox"/> Use default workspace settings
Interactive retention	90 days
Total retention period	180 days
Archive period of 90 days	Interactive retention (blue bar), Archive period (red bar)
Data collection rules	N/A

A close-up photograph of a person with dark skin and short hair, wearing a white lab coat. They are looking down at a red compound light microscope, focusing on the eyepiece. The background is blurred, showing some greenery and laboratory equipment.

07

Search Jobs

Search Jobs

- Usual log queries will timeout after 10 minutes
- When searching large volumes or using complex operations, timeout is reached very quick
- Running a query as search job will allow queries to run for up to 24 hours
- The result will written into a new (custom) table

The screenshot shows the Microsoft Power BI desktop application. At the top, there's a ribbon with 'Feedback', 'Queries', 'Format query', and other options. Below the ribbon, the main area has tabs for 'Tables', 'Queries', and 'Functions'. A search bar is at the bottom left. In the center, there's a search bar with the placeholder 'Type your query...'. A modal dialog box is open in the foreground, titled 'Search job'. It contains the text: 'Run a search query in the background. Results will appear in the table as they arrive.' Below this, there's a link 'Learn more about search jobs and pricing'. A text input field is labeled 'New table name' with the value 'Enter table name _SRCH'. At the bottom of the dialog is a blue button labeled 'Run a search job'.

Search Jobs

- Could also be used to retrieve records from archived logs and basic logs (as an alternative to restore the archived logs or query basic logs directly)
- Search jobs are charged!
- But there is also some **limitations**:
 - Limited set of KQL statements / operations
 - You can only query one table at a time
 - The time range is limited to one year
 - Results are limited to 1 Mio records
 - Concurrent execution of max. 5 search jobs per workspace
 - Max. 100 search result tables per workspace
 - Max. 100 search job executions per day

08

Granular RBAC on Table-level

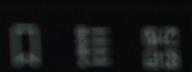
Table Level Read Access

- Although, in theory other roles would work here as well, you usually only grant Read access to a certain table
- Needs custom role and some API usage:
- Details:
- [Manage access to Log Analytics workspaces](#)
[Azure Monitor | Microsoft Learn](#)

```
{  
  "requests": [  
    {  
      "content": {  
        "Id": "<GUID_1>",  
        "Properties": {  
          "PrincipalId": "<user_object_ID>",  
          "PrincipalType": "User",  
          "RoleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/acdd72a7-  
3385-48ef-bd42-f606fba81ae7",  
          "Scope":  
            "/subscriptions/<subscription_ID>/resourceGroups/<resource_group_name>/providers/Microso  
t.OperationalInsights/workspaces/<workspace_name>/Tables/<table_name>",  
          "Condition": null,  
          "ConditionVersion": null  
        }  
      },  
      "httpMethod": "PUT",  
      "name": "<GUID_2>",  
      "requestHeaderDetails": {  
        "commandName": "Microsoft_Azure_AD."  
      },  
      "url":  
        "/subscriptions/<subscription_ID>/resourceGroups/<resource_group_name>/providers/Microso  
t.OperationalInsights/workspaces/<workspace_name>/Tables/<table_name>/providers/Microso  
ft.Authorization/roleAssignments/<GUID_1>?api-version=2020-04-01-preview"  
    }  
  ]  
}
```

09

Duplicate Alert Rule



Total Deaths

4.720

Total Recovered

68.324

RUSSIA

3.056 deaths
Hubei China

827 deaths
Italy

429 deaths
Iran

66 deaths
Korea, South

55 deaths
Spain

48 deaths
France France

31 deaths
Washington US

22 deaths
Henan China

16 deaths
Japan

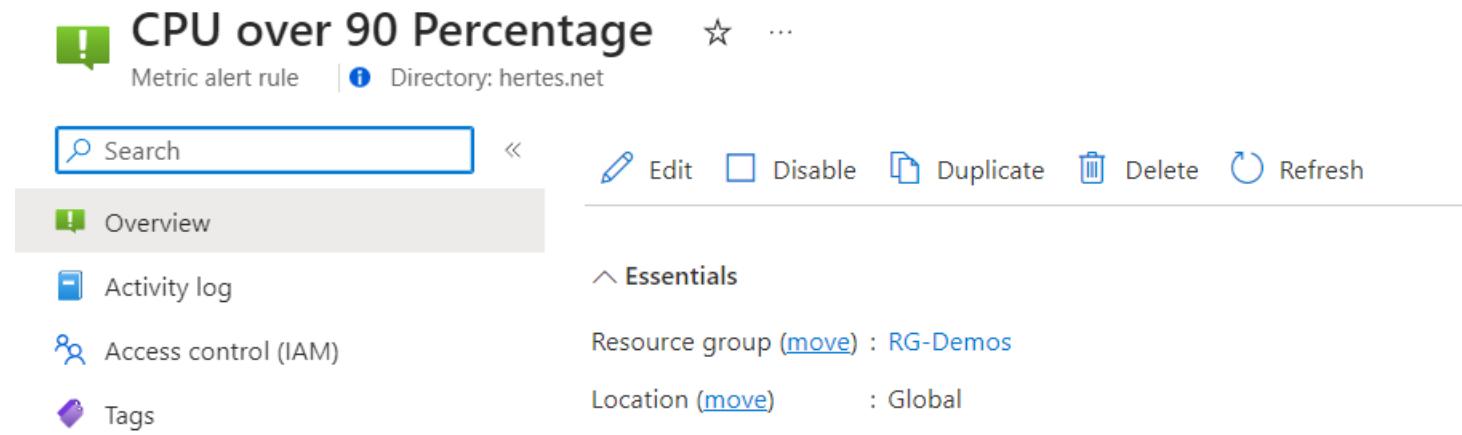
13 deaths
Heilongjiang China

8 deaths
Jiangsu China

one
software

Duplicating Alert Rules

- Creating Alert Rules can sometimes be time-consuming
- Creating many Alert Rules even more...
- New option to duplicate an existing Alert Rule creates a new Rule with the old Rules settings pre-filled, but all of the m could still be changed



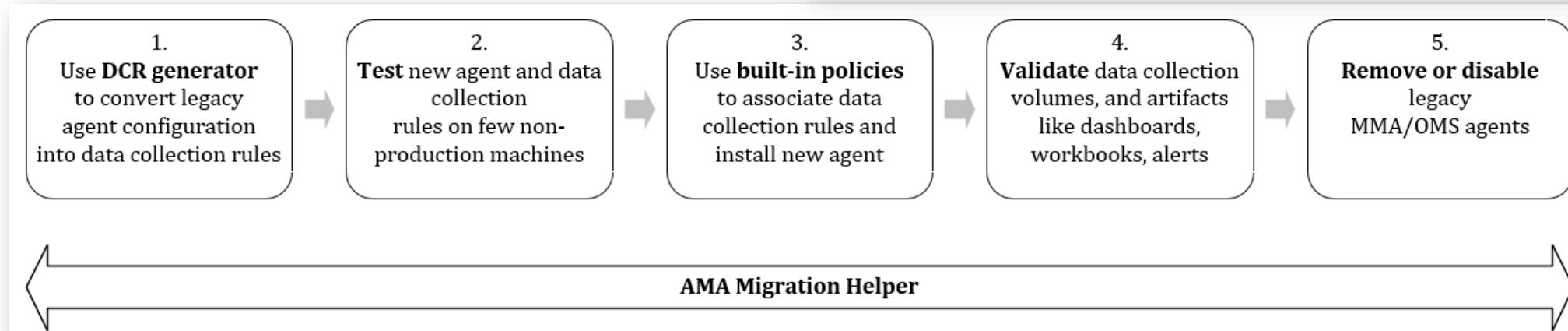
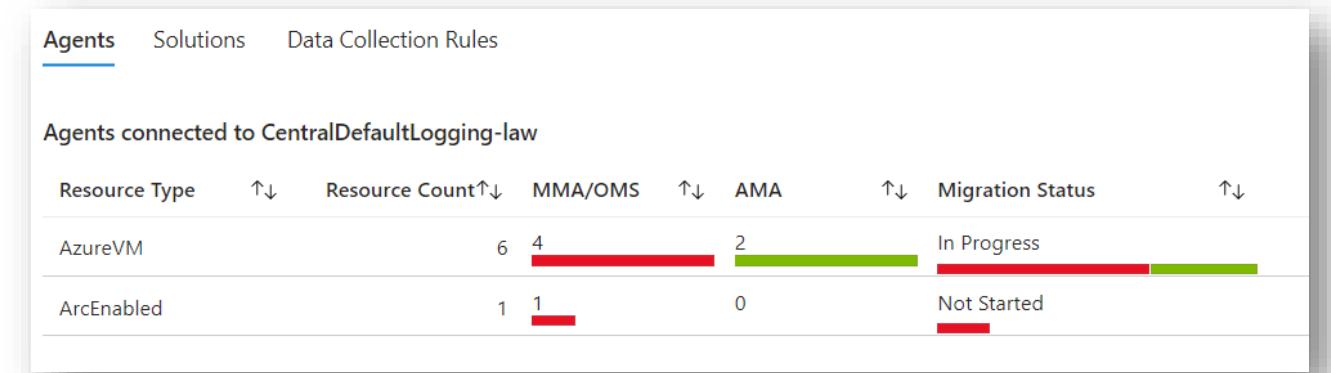
10

AMA Migration Tools



AMA Migration Tools

- Log Analytics Agent / Microsoft Monitoring Agent / Legacy Agent deprecates August 2024
- Migrating complex scenarios from MMA to AMA could be very time-consuming
- Microsoft provides tools (PowerShell Script, Workbook) to create DCRs from Log Analytics configurations and show systems that still need migration



Ihr wollt einige der coolen Speaker hier (und weitere) bald wieder hören? Kommt zum SysAdminDay nach Leipzig!

Fr., 28.07.2023

SoftwareOne
Niederlassung
Leipzig

14:00 – 21:00

www.sysadminday.it

Thank You!



Disclaimer

This publication contains proprietary information that is protected by copyright. SoftwareOne reserves all rights thereto.

SoftwareOne shall not be liable for possible errors in this document. Liability for damages directly and indirectly associated with the supply or use of this document is excluded as far as legally permissible.

The information presented herein is intended exclusively as a guide offered by SoftwareOne. The publisher's product use rights, agreement terms and conditions and other definitions prevail over the information provided herein. The content must not be copied, reproduced, passed to third parties or used for any other purposes without written permission of SoftwareOne

Copyright © 2023 by SoftwareOne. All Rights Reserved. SoftwareOne is a registered trademark of SoftwareOne. All other trademarks, service marks or trade names appearing herein are the property of their respective owners.