SoftwareONE

EMPOWERING COMPANIES TO TRANSFORM

Using Azure Log Analytics to get performance usage and save costs on SQL in Azure

Haiko Hertes

HERTES.NET
knowledge - experience - insights

E = M C²

Microsoft® MVP 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

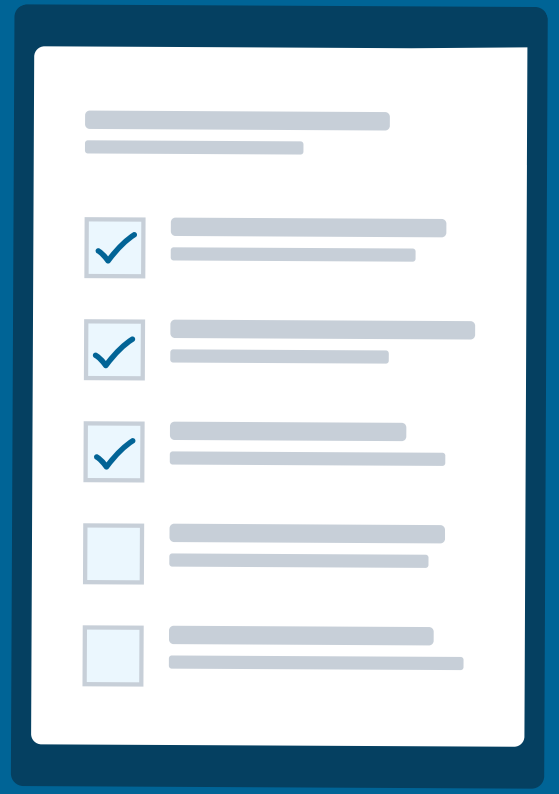
AGENDA

01 Azure Monitor Overview

02 Diagnostic Settings

03 Log Analytics

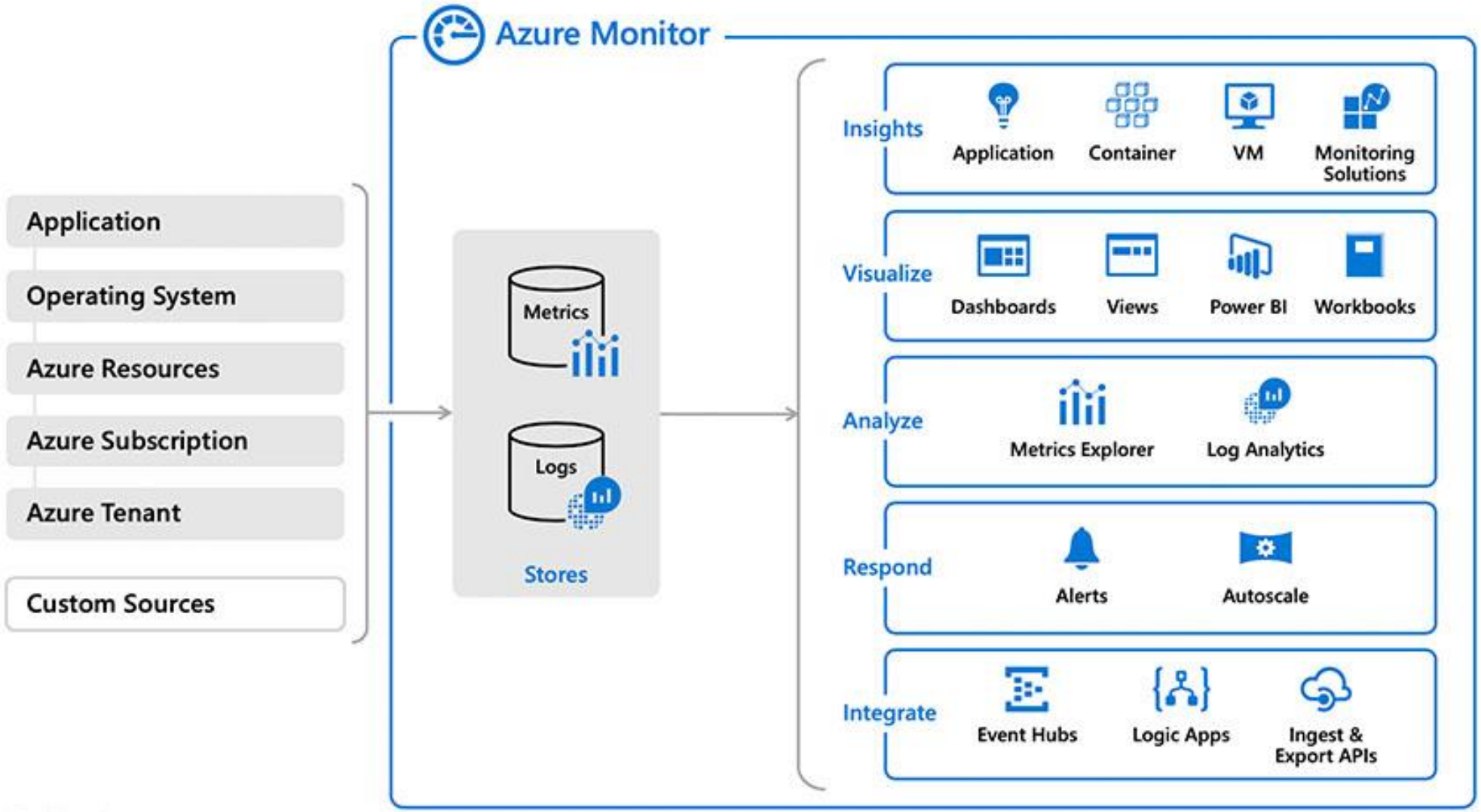
04 Live-Demo



01

Azure Monitor Overview

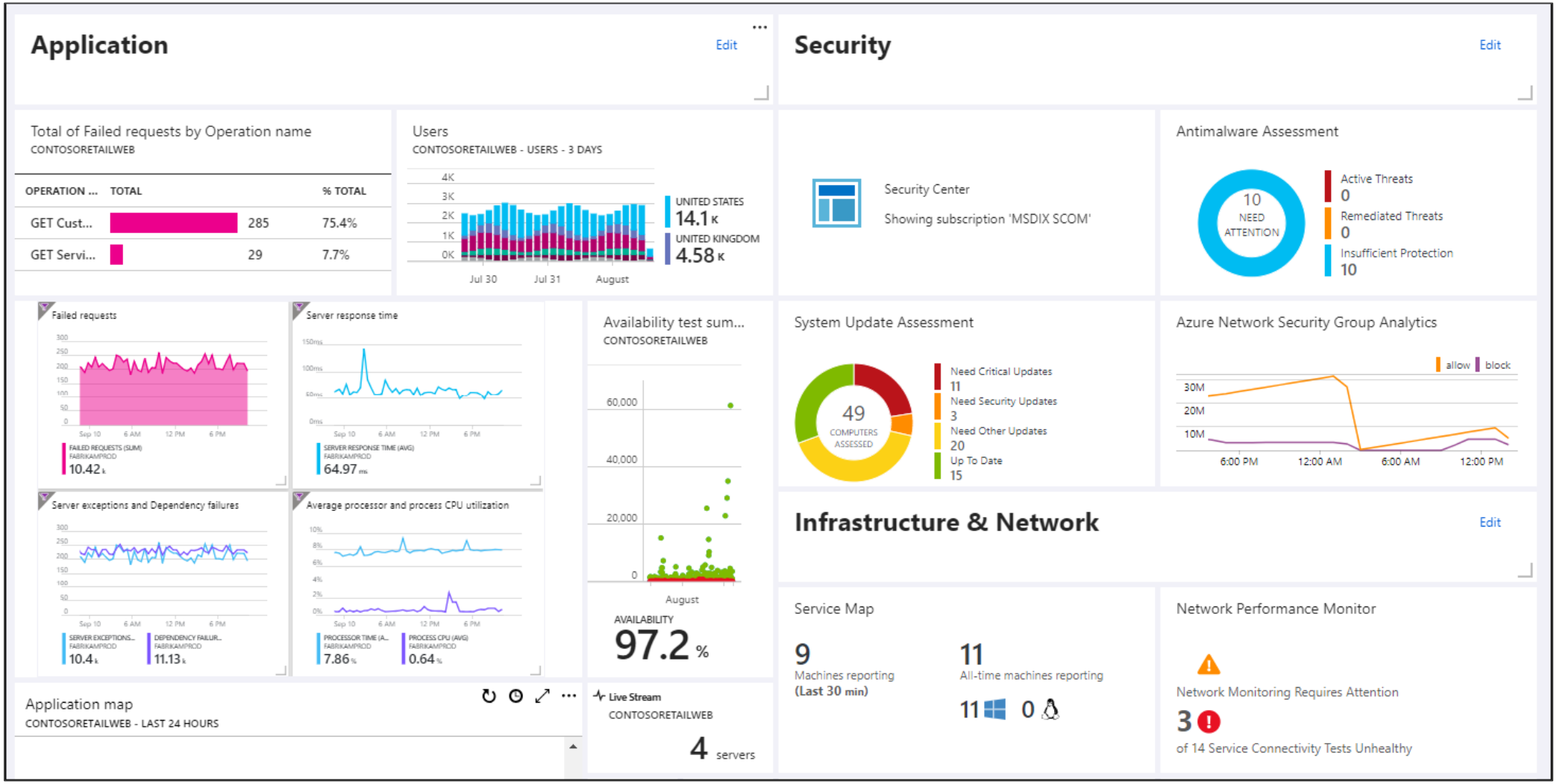
Azure Monitor



Azure Monitor overview - Azure Monitor | Microsoft Docs

Azure status history | Microsoft Azure

Azure Monitor



softwareONE

[Azure Monitor overview - Azure Monitor | Microsoft Docs]

Data Types

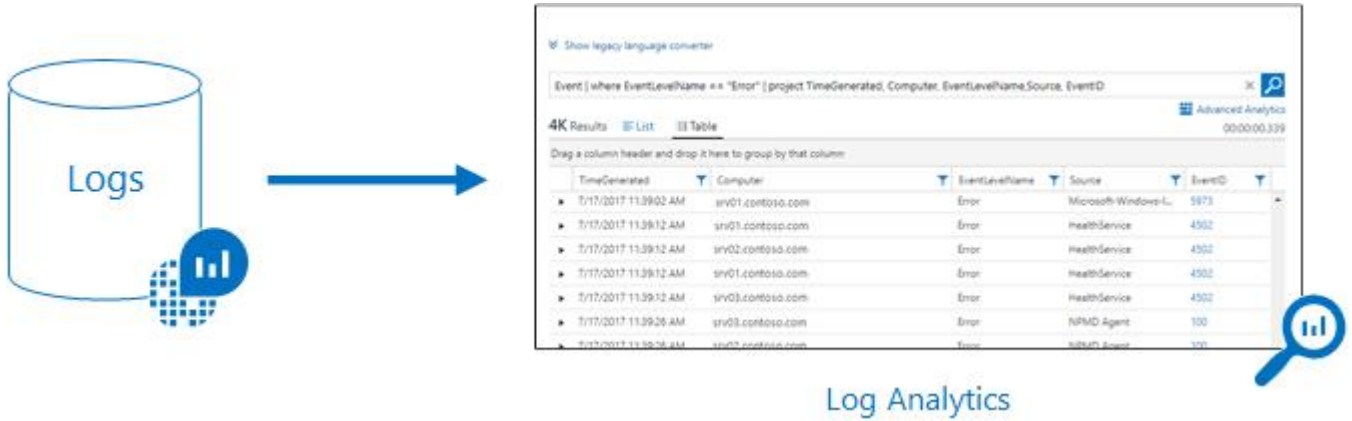
- Metrics
  - Numerical values that describe some aspect of a system at a particular point in time
  - CPU / Disk / Network …
- Logs
  - different kinds of data organized into records with different sets of properties for each type
  - Activity Log, AAD Audit Logs, Resource Logs
- (Insights)
  - Application Insights
  - Container Insights
  - VM Insights

Azure Monitor overview - Azure Monitor | Microsoft Docs

Data Types

[Metrics in Azure Monitor - Azure Monitor | Microsoft Docs]

[Overview of Azure platform logs - Azure Monitor | Microsoft Docs]



Data Generation

- Azure Platform itself – out of the box
  - Metrics
  - Activity / Audit Logs
  - More or less realtime…
- Agent
  - Agent in Azure Platform hostet VMs
  - Agent in on-premises VMs
  - Agent in other Cloud Provider VMs
  - several types of agents for different used cases

Azure Monitor overview - Azure Monitor | Microsoft Docs

Data retention

Azure Monitor - Metrics	30 Days / Docs: 93 days
Application Insights	90 Days
Resource Logs	90 Days
Activity Logs	90 Days
AAD Logs	Other table

- Autogenerated data has short retention / lifetime
- Timerange varies on datatype
- After that, data will be „gone“
- Typical retention time:

How long does Azure AD store the data?

Activity reports

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Audit logs	7 days	30 days	30 days
Sign-ins	7 days	30 days	30 days
Azure AD MFA usage	30 days	30 days	30 days

You can retain the audit and sign-in activity data for longer than the default retention period outlined above by routing it to an Azure storage account using Azure Monitor. For more information, see Archive Azure AD logs to an Azure storage account.

Security signals

Report	Azure AD Free	Azure AD Premium P1	Azure AD Premium P2
Users at risk	7 days	30 days	90 days
Risky sign-ins	7 days	30 days	90 days

Persisting of data

- Diagnostic Settings
  - export of
    - platform logs and
    - metrics
  - for a resource to the destination of your choice
  - up to five different diagnostic settings
    - to send different logs and metrics to independent destinations
- Diagnostic Settings Destination
  - Log Analytics Workspace
  - Storage Account
  - Event Hub
  - Partner Solution

Create diagnostic settings to send platform logs and metrics to different destinations - Azure Monitor | Microsoft Docs

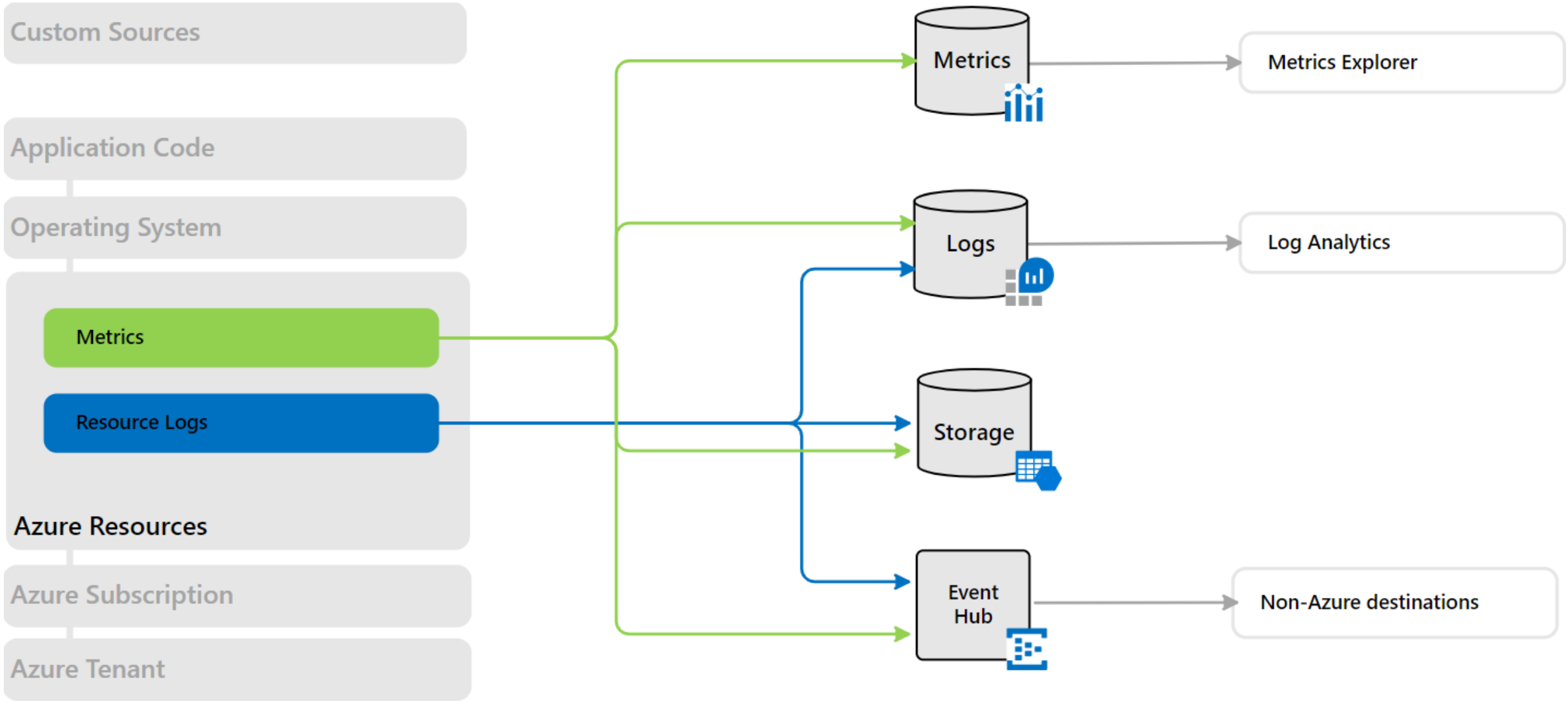
Demo

Azure Monitor / Metrics for Azure SQL DB

softwareONE


02
Diagnostics Settings

Diagnostic Settings



Diagnostic Settings

- PaaS Services allow to set Diagnostic Settings
- Using them, zou can persist Log and Metrics to Log Analztics, Storage Accounts and other Sinks

- A VM has an extended Diagnostic Settings view
- Here you can enable and configure guest level monitoring
- This allows collecting more data, i.e. sending Memory consumption to Azure Monitor

- Sending data to an storage account could be challenging when searching for certain information

03

Log Analytics

Log Analytics Workspace

- correlate resource log data with other monitoring data
- consolidate log entries from multiple Azure sources
- use log queries to perform complex analysis
- gain deep insights on log data.
- use log alerts with complex alerting logic
- uses KQL (Kusto Query Language) for queries

Overview of Log Analytics in Azure Monitor - Azure Monitor | Microsoft Docs

Pricing / Data Retention / Daily Cap

- Log Analytics pricing is based on two facts
  - Data ingestion
    - Pay-as-you-go or Capacity Reservation
  - Data retention
    - 31 days are free of charge

Monitoring usage and estimated costs in Azure Monitor - Azure Monitor | Microsoft Docs

04

Live Demo

Zeit für Fragen

Haiko Hertes

Haiko.Hertes@SoftwareONE.com