FINLAND
AZURE
USER
GROUP

Monitoring Real-Life Azure Applications

Karl Ots, Zure Ltd

Jyväskylä 28.5.2019
@ Adafy

Karl Ots

Chief Consulting Officer

karl.ots@zure.com

- Cloud & cybersecurity expert
- Organizer of FAUG and #GlobalAzure
- Patented inventor
- Working on Azure since 2011
- Helped to secure 100+ Azure applications, from startups to Fortune 500 enterprises
- zure.ly/karl

MVP Microsoft® Most Valuable Professional

CISSP® Microsoft CERTIFIED Trainer

ZURE

@fincooper

Azure Monitoring scene

FINLAND
AZURE
USER
GROUP

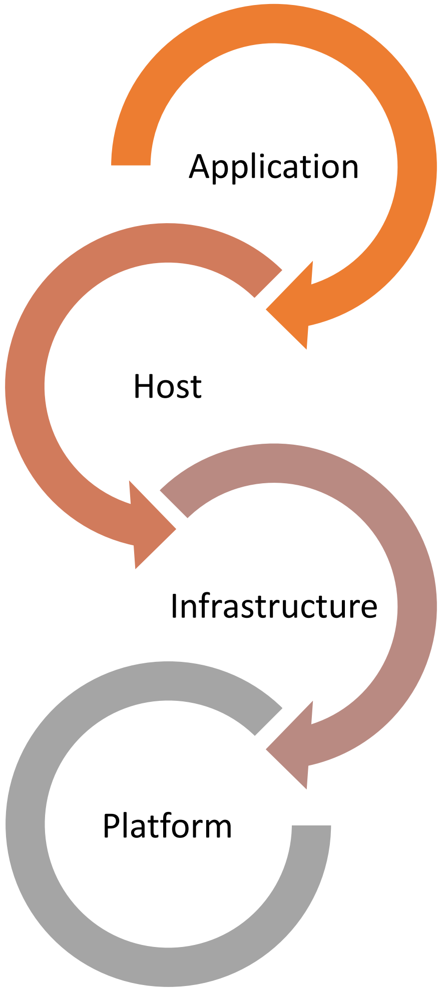
- Application Insights
- Azure Monitor
- Azure Health
- ARM Activity Logs
- System Center Operations Manager
- Operations Management Suite
- Log Analytics
- Network Watcher
- Application Gateway / WAF
- Secure DevOps Kit for Azure (AzSK)
- Security Center

Recent Branding changes

- Azure Monitor = Application Insights + Log Analytics + more
- Operations Management Suite (OMS) was a bundling of the following Azure management services for licensing purposes:
  - Application Insights
  - Azure Automation
  - Azure Backup
  - Log Analytics
  - Site Recovery
- Kusto -> Data Explorer Query Language

Azure Monitoring

FINLAND
AZURE
USER
GROUP



- Application Insights
- Web Application Firewalls
- Vulnerability Scanners

- Microsoft Monitoring Agent
- Service Map and other Log Analytics Solution Packs
- Azure Security Center

- Azure Monitor
- Secure DevOps kit for Azure (AzSK)
- Network Watcher

- Activity Logs
- Azure Monitor
- Azure Health

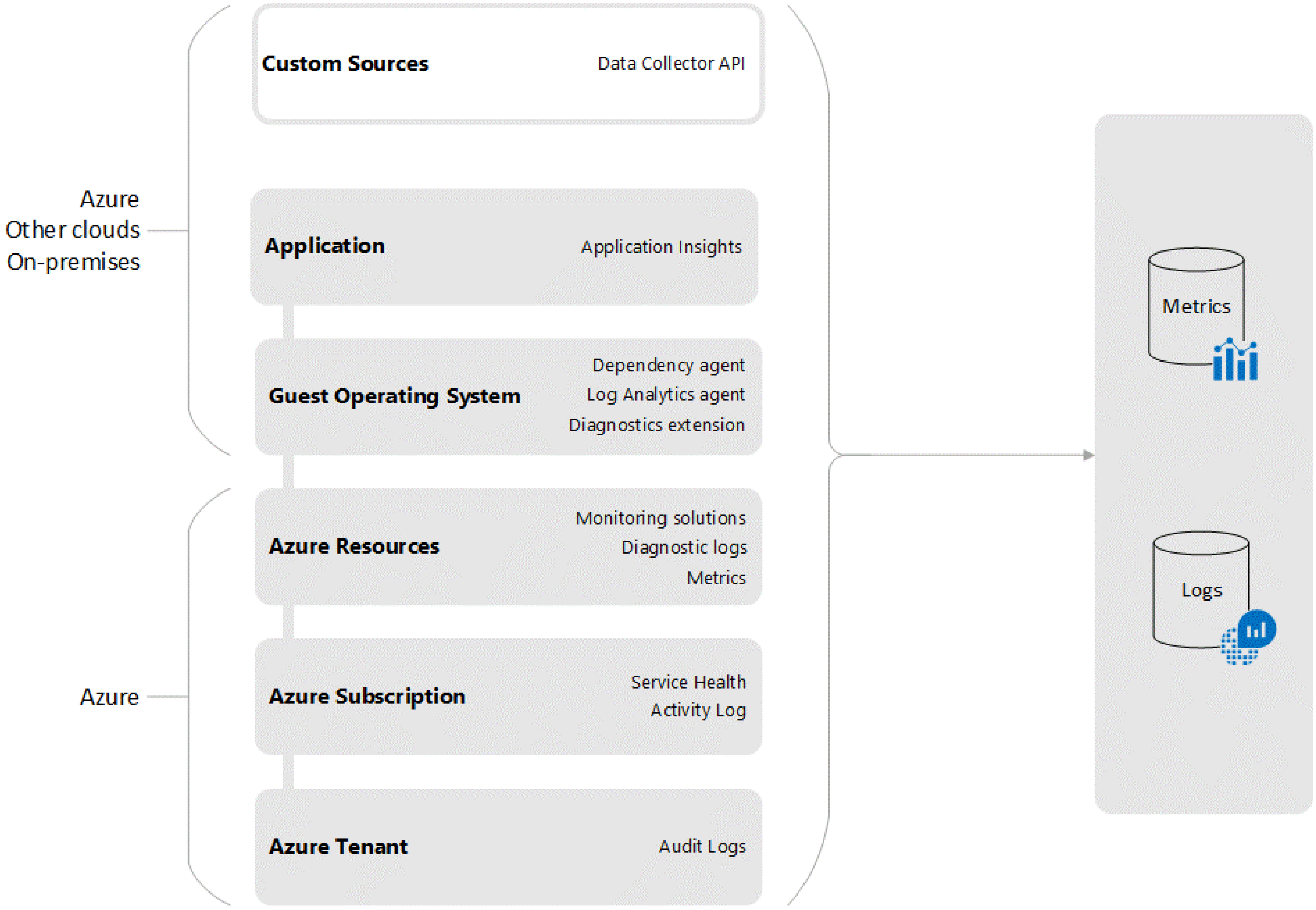
Azure Activity Logs

- Monitors Azure Platform level operations:
  - What operations were taken on the resources in your subscription
  - HTTP Operations on your Resource Providers
  - Who initiated the operation
- Default retention time is only 90 days!

Azure Monitor

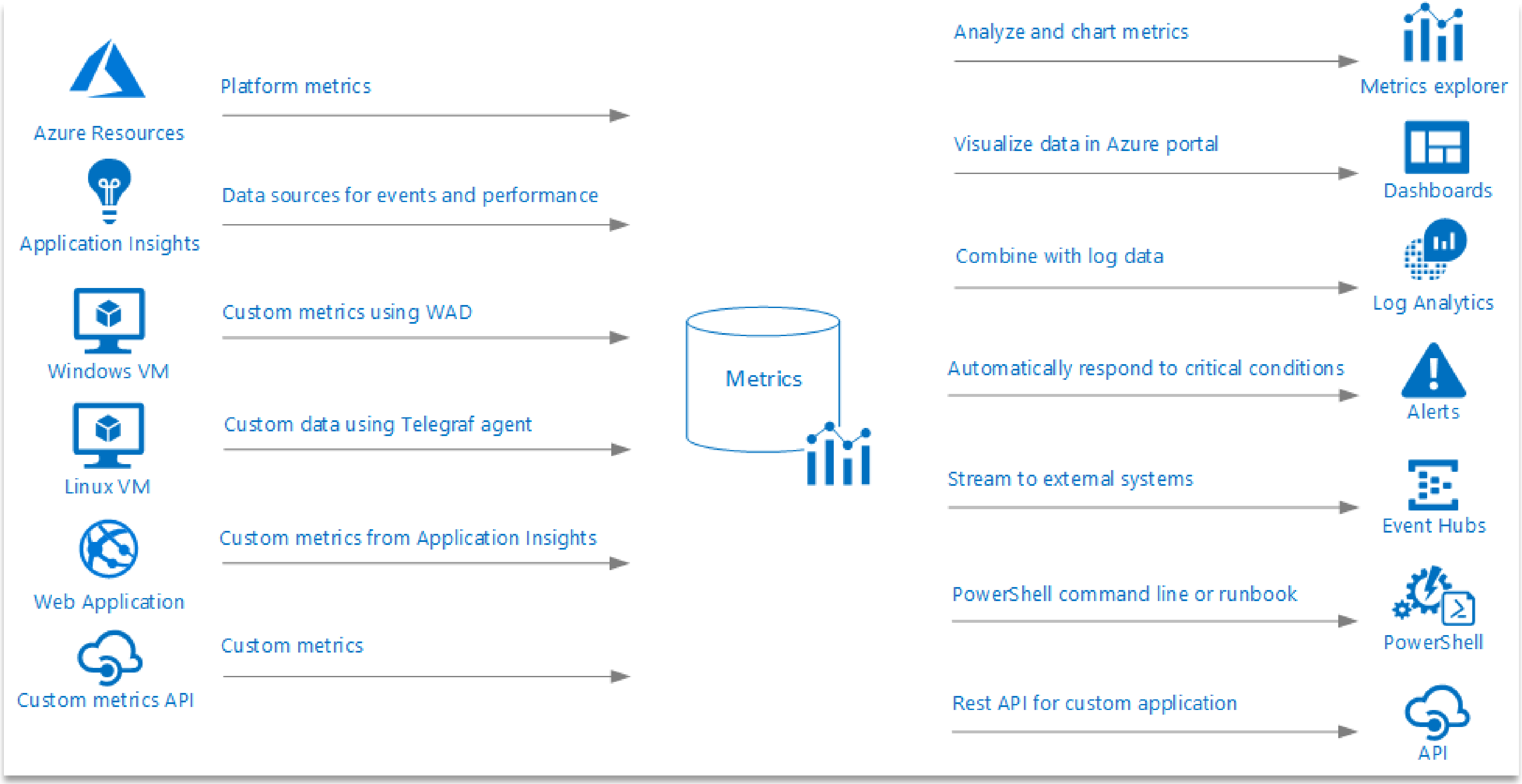
FINLAND AZURE USER GROUP

- Metrics and Logs
- Built-In monitoring support for all Azure resources
- Out-of-the-box Metrics, such as:
    - Total active connections on Azure DB for MySQL
    - Number of throttling errors for IoT Hub
    - Number of dead lettered messages in Service Bus
- Exposed as an API



Azure Monitor Metrics

FINLAND
AZURE
USER
GROUP



Azure Resources — Platform metrics

Application Insights — Data sources for events and performance

Windows VM — Custom metrics using WAD

Linux VM — Custom data using Telegraf agent

Web Application — Custom metrics from Application Insights

Custom metrics API — Custom metrics

Metrics

Analyze and chart metrics — Metrics explorer

Visualize data in Azure portal — Dashboards

Combine with log data — Log Analytics

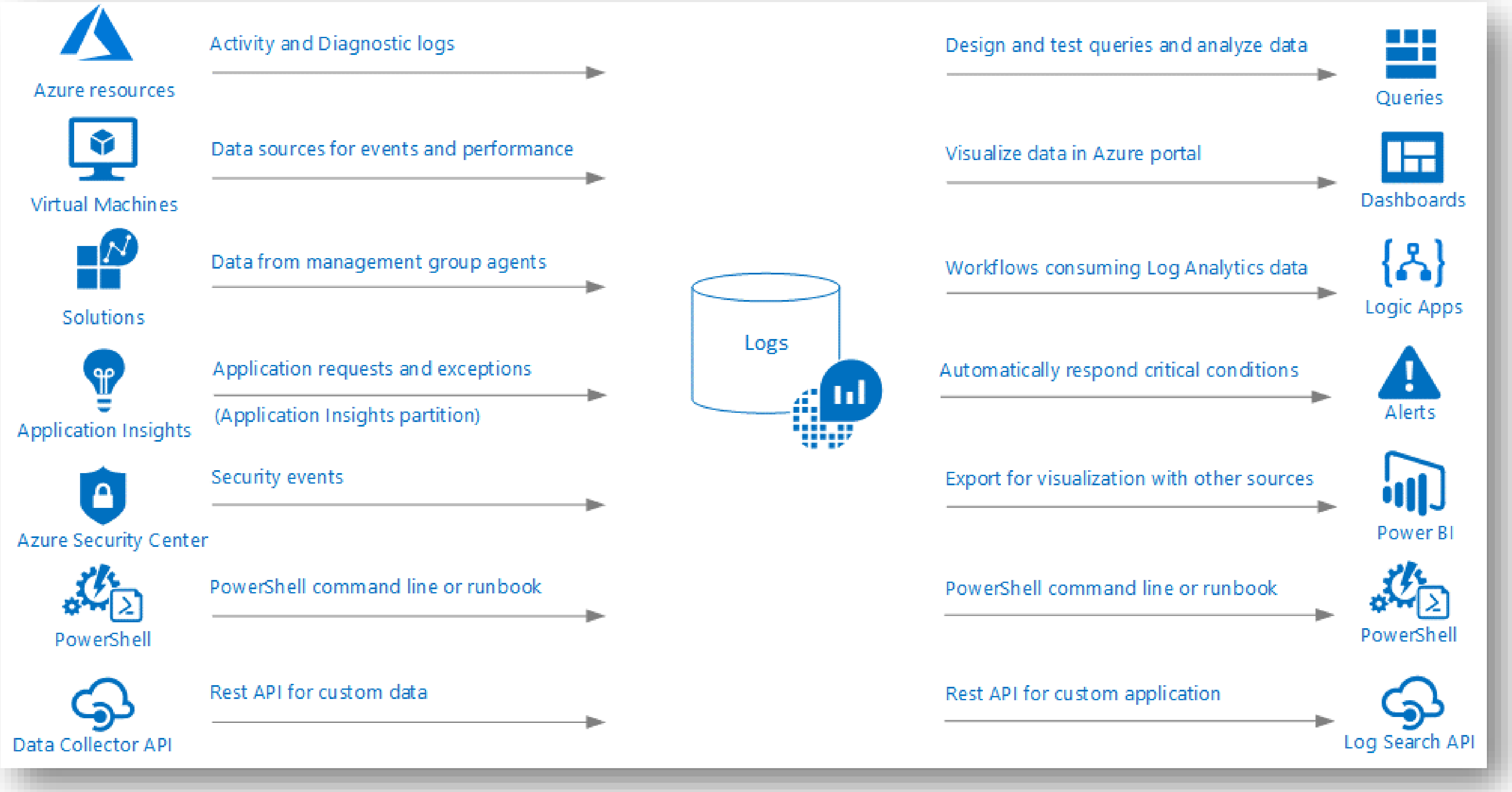
Automatically respond to critical conditions — Alerts

Stream to external systems — Event Hubs

PowerShell command line or runbook — PowerShell

Rest API for custom application — API

Azure Monitor Metrics are available for 90 days!



Azure resources — Activity and Diagnostic logs

Virtual Machines — Data sources for events and performance

Solutions — Data from management group agents

Application Insights — Application requests and exceptions (Application Insights partition)

Azure Security Center — Security events

PowerShell — PowerShell command line or runbook

Data Collector API — Rest API for custom data

Logs

Design and test queries and analyze data — Queries

Visualize data in Azure portal — Dashboards

Workflows consuming Log Analytics data — Logic Apps

Automatically respond critical conditions — Alerts

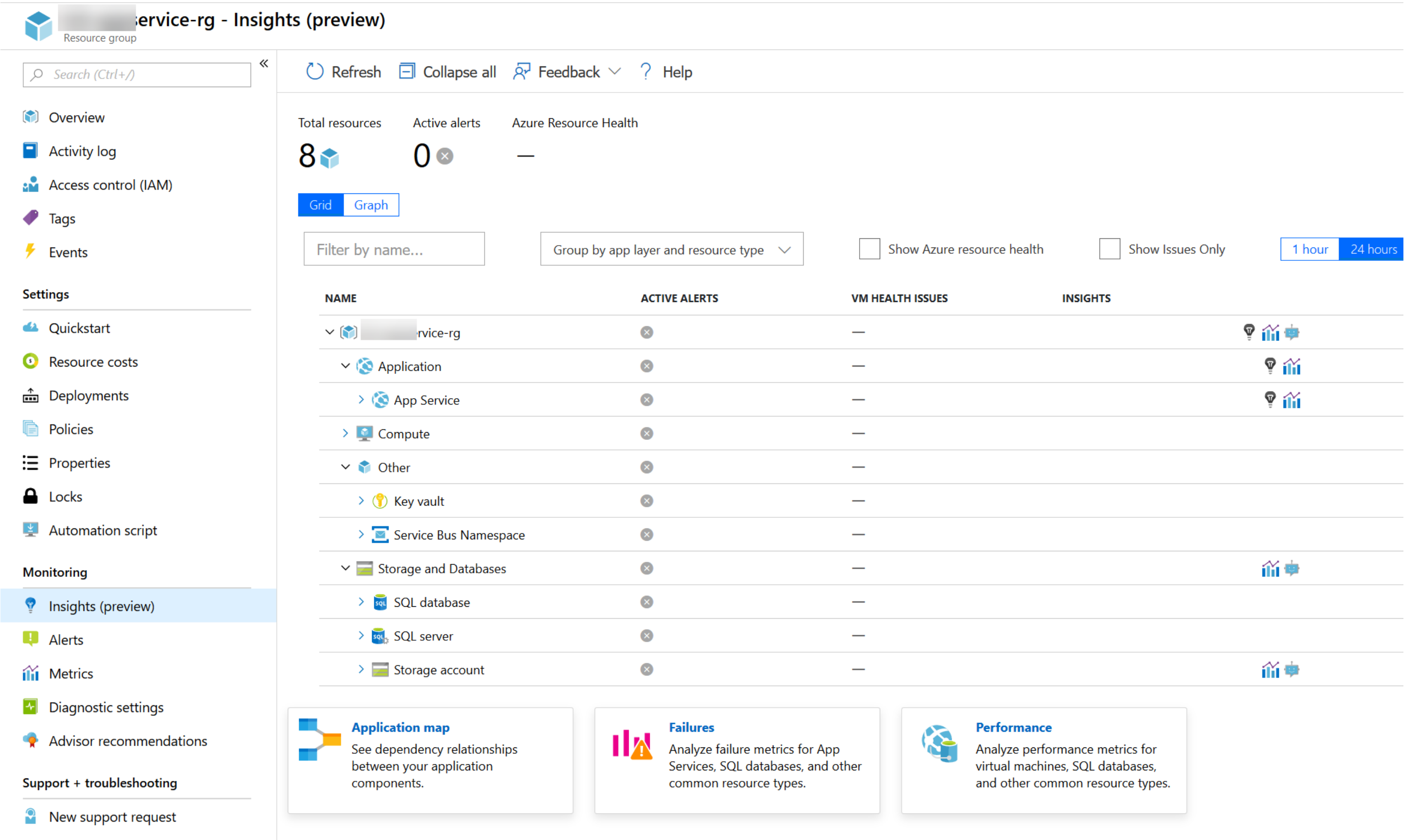
Export for visualization with other sources — Power BI

PowerShell command line or runbook — PowerShell

Rest API for custom application — Log Search API

Azure Monitor: Resource Group Insights

FINLAND
AZURE
USER
GROUP



[redacted]ervice-rg - Insights (preview)
Resource group

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Events

Settings

- Quickstart
- Resource costs
- Deployments
- Policies
- Properties
- Locks
- Automation script

Monitoring

- Insights (preview)
- Alerts
- Metrics
- Diagnostic settings
- Advisor recommendations

Support + troubleshooting

- New support request

Total resources	Active alerts	Azure Resource Health
8	0 ⊗	—

Group by app layer and resource type

□ Show Azure resource health

□ Show Issues Only

1 hour | 24 hours

NAME	ACTIVE ALERTS	VM HEALTH ISSUES	INSIGHTS
[redacted]rvice-rg	⊗	—	
Application	⊗	—	
App Service	⊗	—	
Compute	⊗	—	
Other	⊗	—	
Key vault	⊗	—	
Service Bus Namespace	⊗	—	
Storage and Databases	⊗	—	
SQL database	⊗	—	
SQL server	⊗	—	
Storage account	⊗	—	

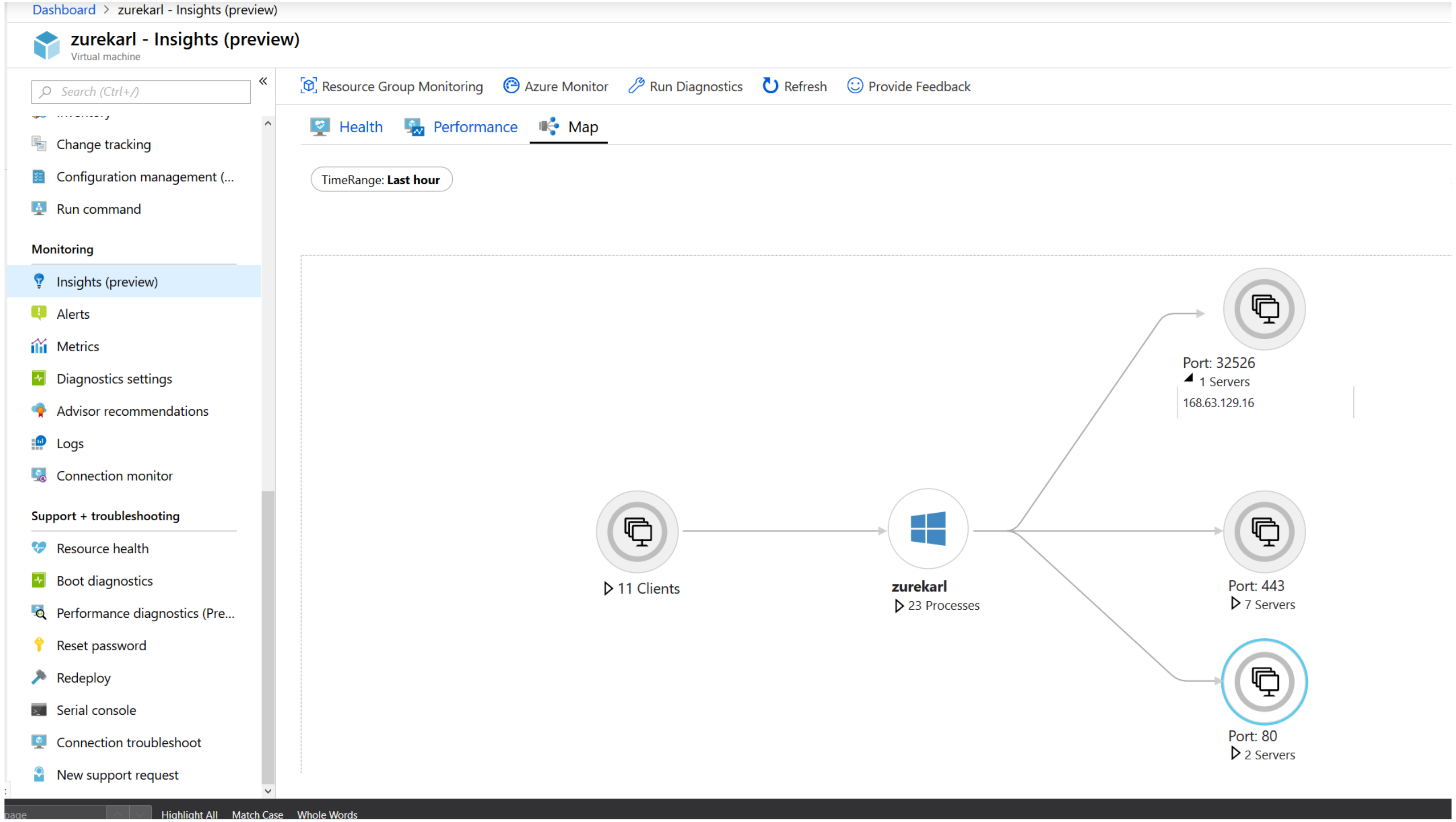
Application map
See dependency relationships between your application components.

Failures
Analyze failure metrics for App Services, SQL databases, and other common resource types.

Performance
Analyze performance metrics for virtual machines, SQL databases, and other common resource types.

Azure Monitor: Virtual Machine Insights

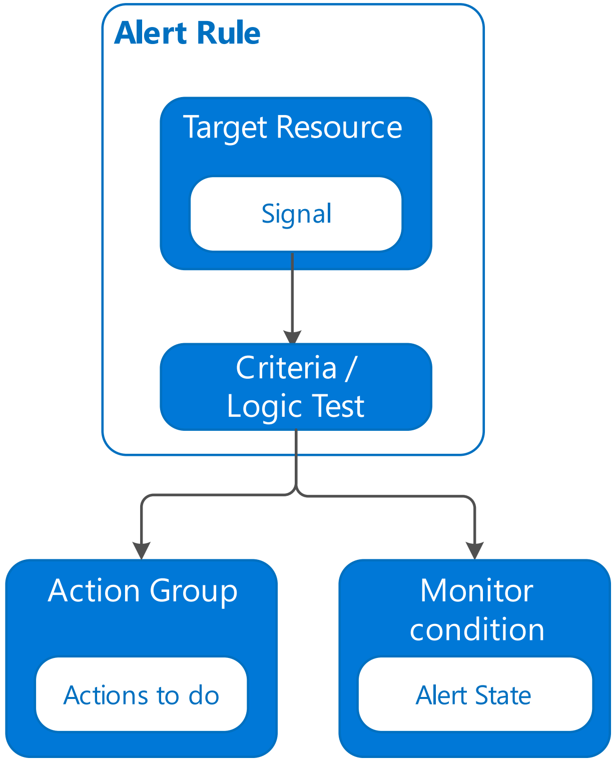
FINLAND
AZURE
USER
GROUP



Azure Monitor: Alerts

FINLAND
AZURE
USER
GROUP

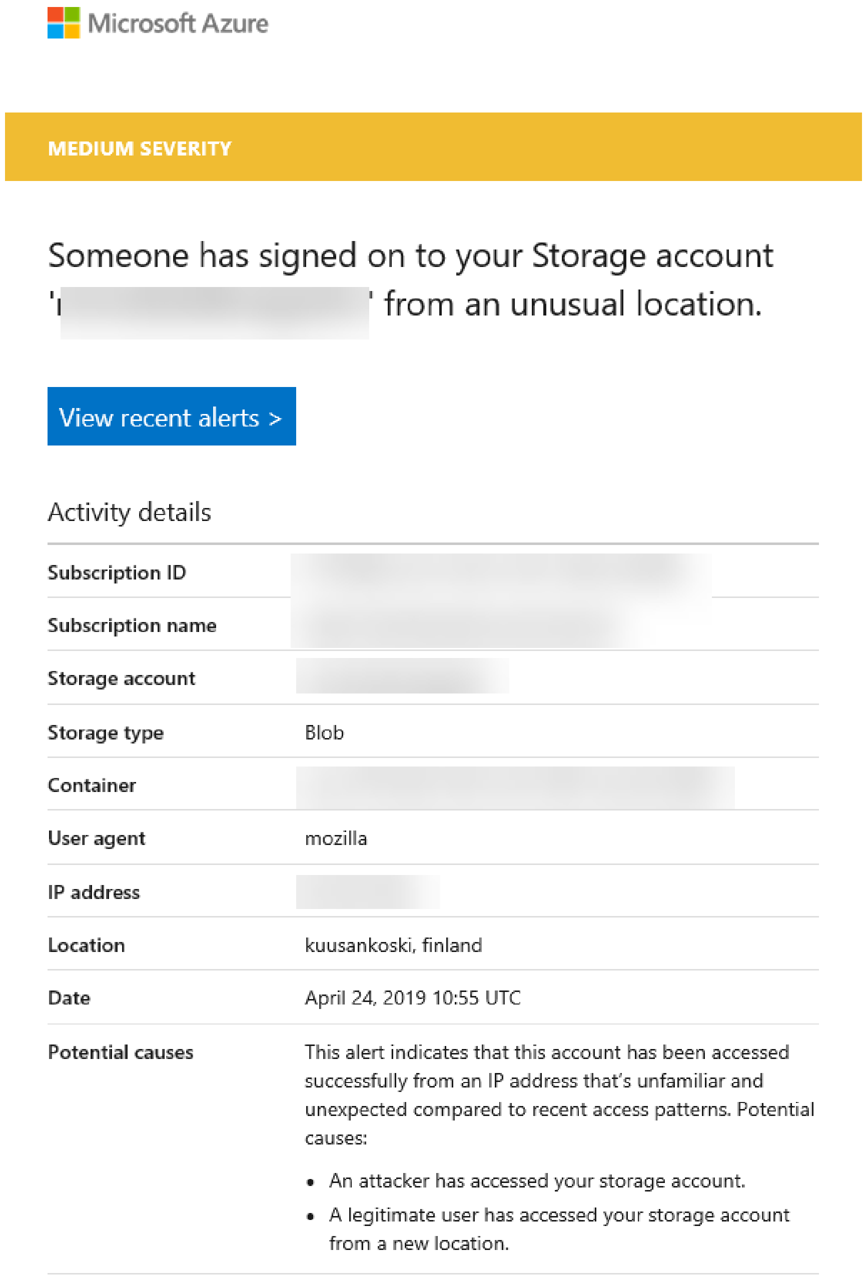
- You can create native alerts from:
  - Monitor Metric values
  - Monitor Log search queries
  - Activity Log events
  - Health of the underlying Azure platform
  - Tests for web site availability



Storage Advanced Threat Protection

- Access from unusual location
- Application Anomaly
- Anonymous access
- Data Exfiltration
- Unexpected delete
- Upload Azure Cloud Service package
- Access permission change
- Access Inspection
- Data Exploration

FINLAND
AZURE
USER
GROUP

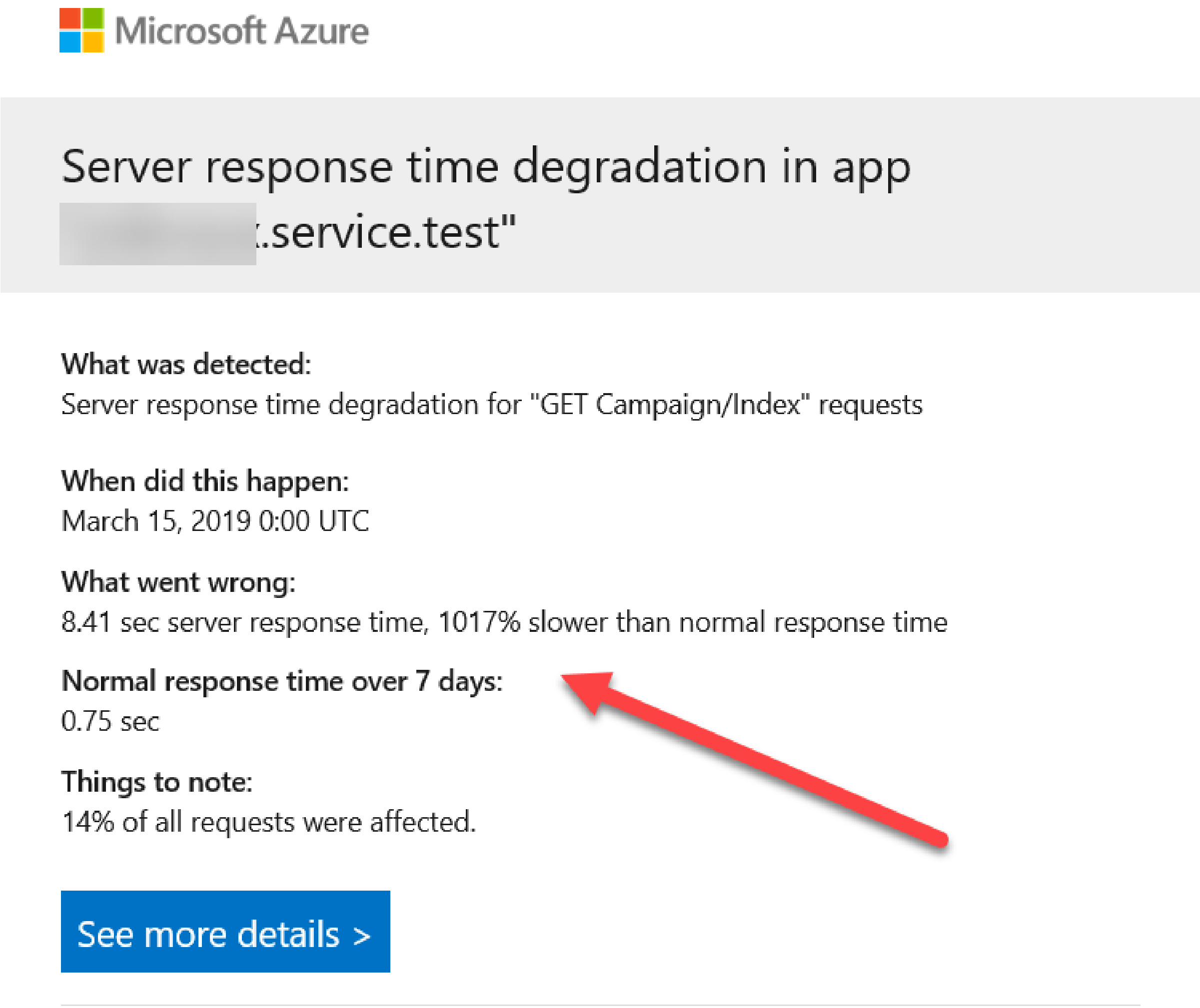


MEDIUM SEVERITY

Someone has signed on to your Storage account '[redacted]' from an unusual location.

Activity details

Subscription ID	[redacted]
Subscription name	[redacted]
Storage account	[redacted]
Storage type	Blob
Container	[redacted]
User agent	mozilla
IP address	[redacted]
Location	kuusankoski, finland
Date	April 24, 2019 10:55 UTC
Potential causes	This alert indicates that this account has been accessed successfully from an IP address that's unfamiliar and unexpected compared to recent access patterns. Potential causes: • An attacker has accessed your storage account. • A legitimate user has accessed your storage account from a new location.



Microsoft Azure

Server response time degradation in app [redacted].service.test"

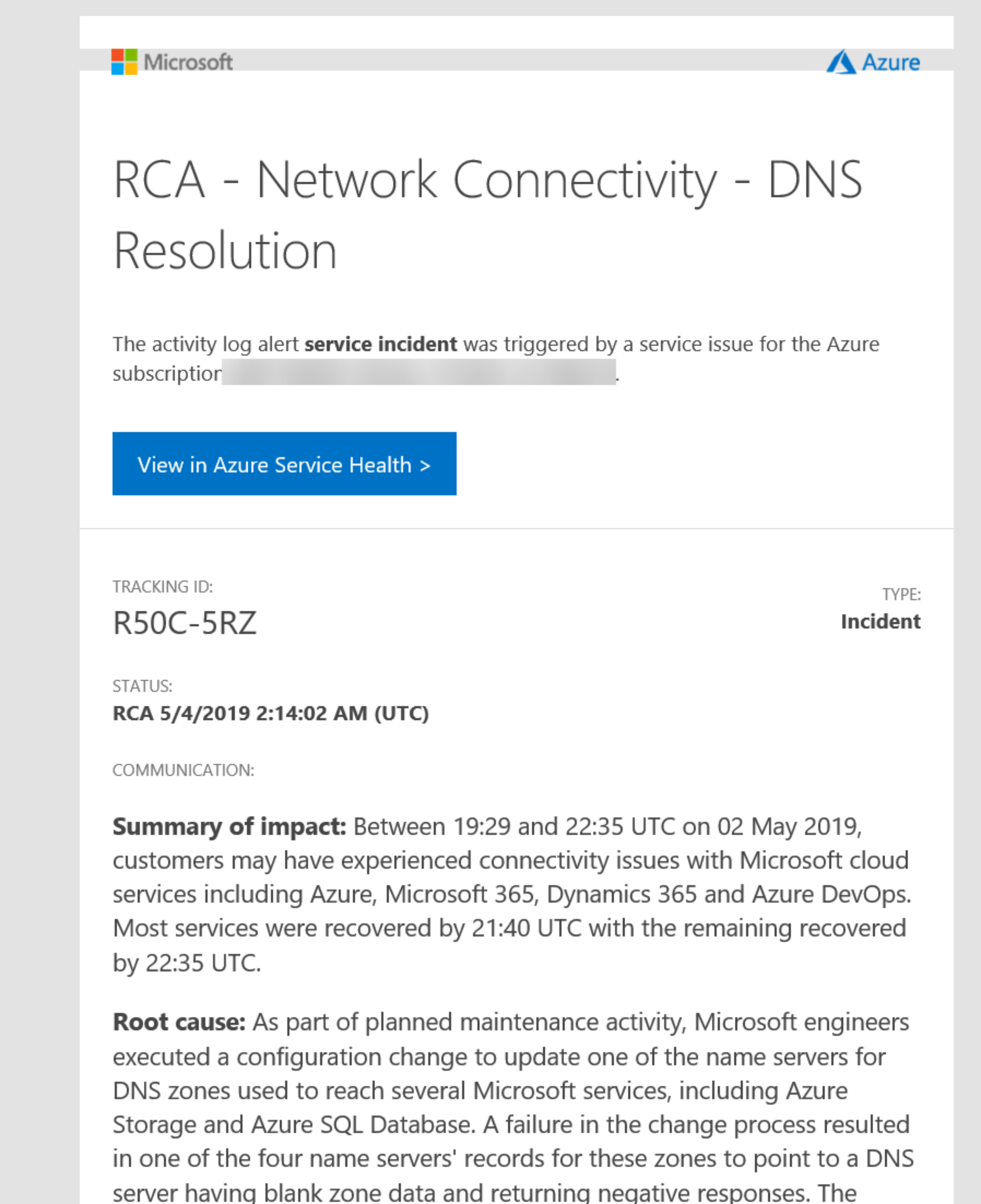
What was detected:
Server response time degradation for "GET Campaign/Index" requests

When did this happen:
March 15, 2019 0:00 UTC

What went wrong:
8.41 sec server response time, 1017% slower than normal response time

Normal response time over 7 days:
0.75 sec

Things to note:
14% of all requests were affected.



RCA - Network Connectivity - DNS Resolution

The activity log alert **service incident** was triggered by a service issue for the Azure subscription [redacted].

TRACKING ID:
R50C-5RZ

TYPE:
Incident

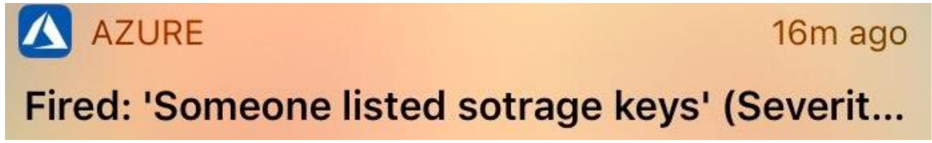
STATUS:
RCA 5/4/2019 2:14:02 AM (UTC)

COMMUNICATION:

Summary of impact: Between 19:29 and 22:35 UTC on 02 May 2019, customers may have experienced connectivity issues with Microsoft cloud services including Azure, Microsoft 365, Dynamics 365 and Azure DevOps. Most services were recovered by 21:40 UTC with the remaining recovered by 22:35 UTC.

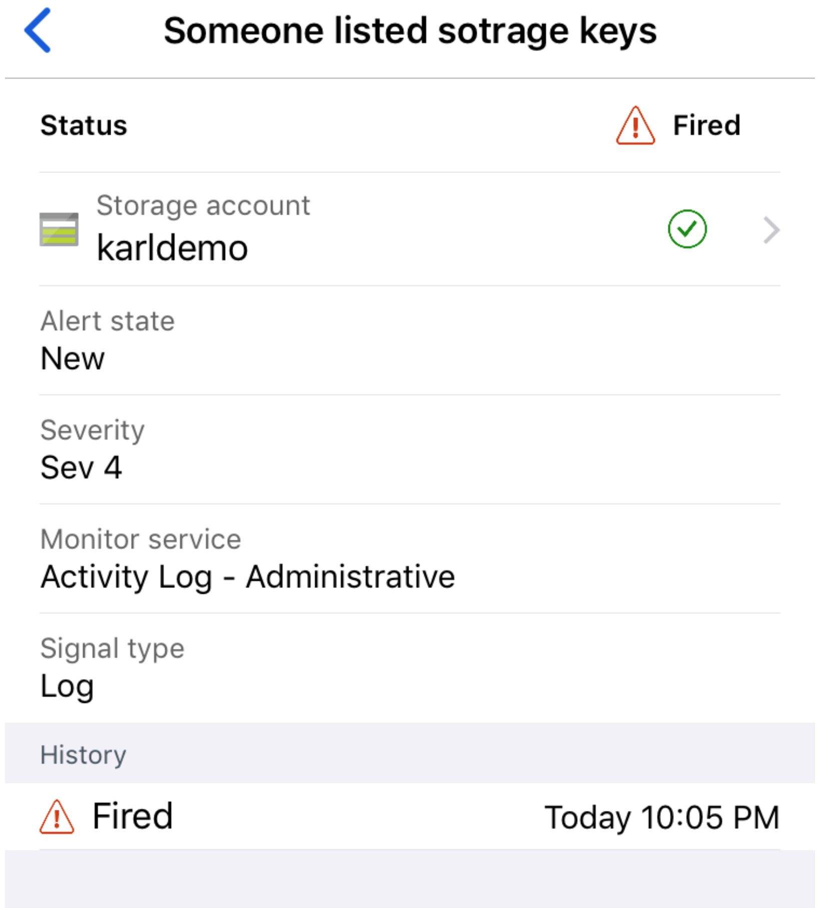
Root cause: As part of planned maintenance activity, Microsoft engineers executed a configuration change to update one of the name servers for DNS zones used to reach several Microsoft services, including Azure Storage and Azure SQL Database. A failure in the change process resulted in one of the four name servers' records for these zones to point to a DNS server having blank zone data and returning negative responses. The

FINLAND
AZURE
USER
GROUP



AZURE 16m ago

Fired: 'Someone listed sotrage keys' (Severit...



Someone listed sotrage keys

Status ⚠ Fired

Storage account
karldemo ✓

Alert state
New

Severity
Sev 4

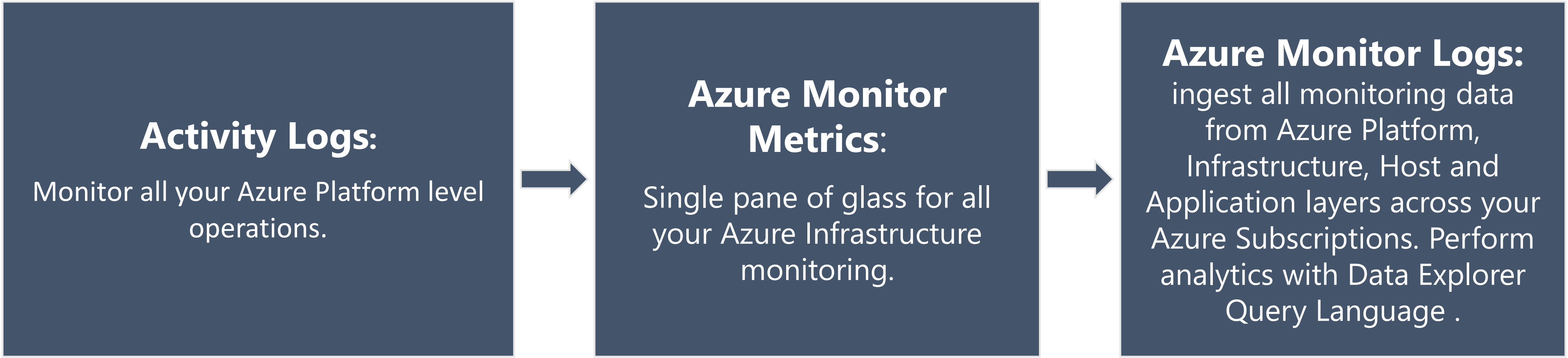
Monitor service
Activity Log - Administrative

Signal type
Log

History

⚠ Fired Today 10:05 PM

Putting it all together



Activity Logs:

Monitor all your Azure Platform level operations.

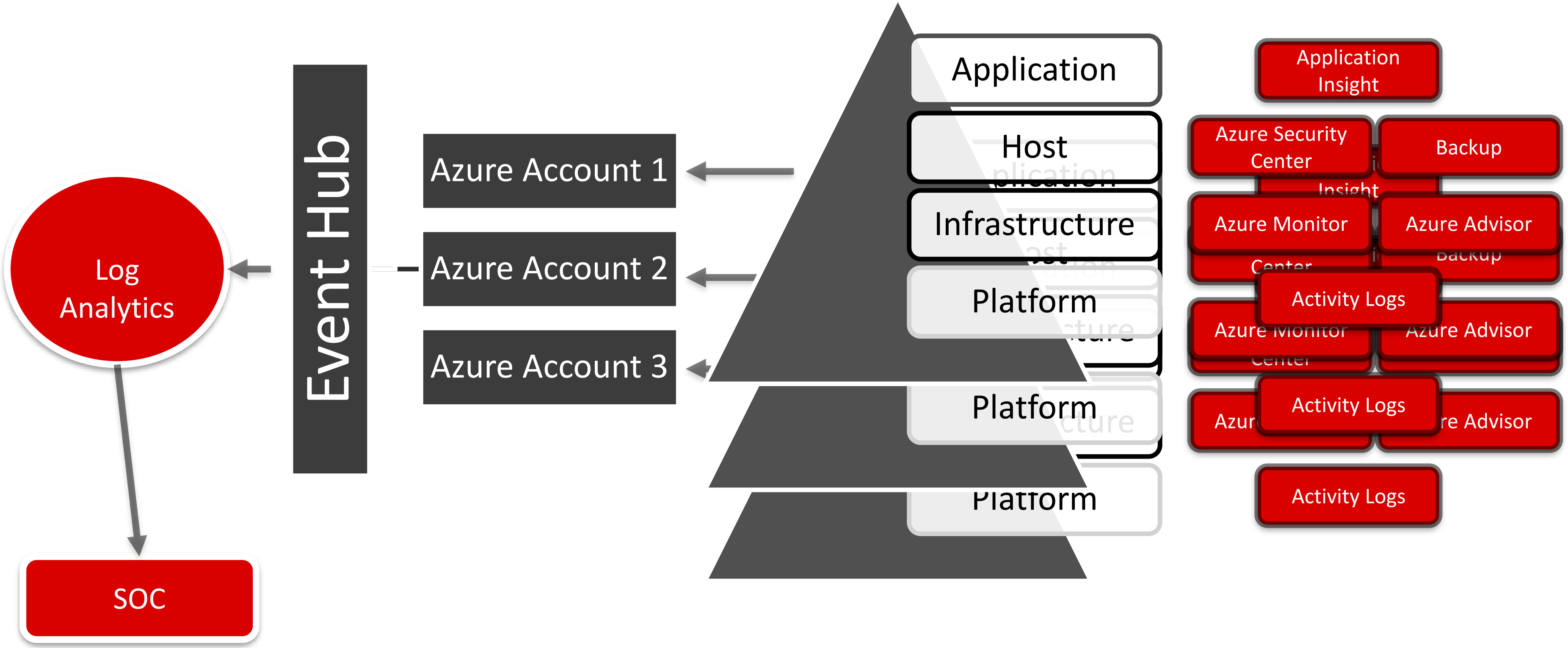
Azure Monitor Metrics:

Single pane of glass for all your Azure Infrastructure monitoring.

Azure Monitor Logs:
ingest all monitoring data from Azure Platform, Infrastructure, Host and Application layers across your Azure Subscriptions. Perform analytics with Data Explorer Query Language .

Collecting Azure logs in the enterprise

FINLAND AZURE USER GROUP



Materials

FINLAND
AZURE
USER
GROUP

- Data Explorer Query Language course
  - aka.ms/KQLPluralsight
- Azure Monitor
  - aka.ms/MonitoringDocs
- Tutorials, videos and more
  - aka.ms/AzMonOverview
- These slides
  - zure.ly/karl-slides