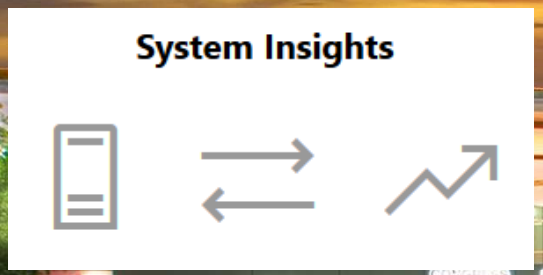
Windows Server Insights mit Log Analytics



Gregor Reimling | Azure MVP

About me

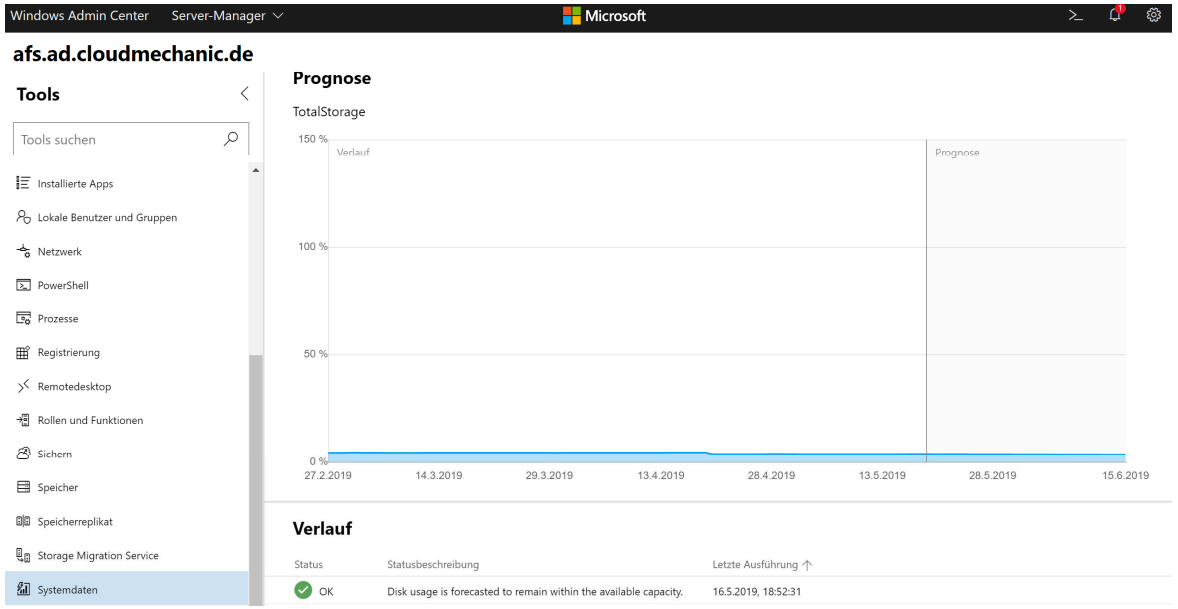
- Gregor Reimling
  - Cloud Architekt – Fokus Azure
  - Orga AzureBonn Meetup (www.azurebonn.de)
  - Microsoft MVP for Azure
  - Tätig bei sepago® GmbH Köln
- Kontakt:
  - Mail: Gregor.Reimling@sepago.de
  - Twitter: @GregorReimling
  - Blog: https://www.reimling.eu

Azure Meetup BONN

Microsoft® MVP Most Valuable Professional

Agenda

- Generally
- Windows Server Insights
- Azure Monitor (Log Analytics)
- Conclusion



@GregorReimling

powered by Rachfahl IT-Solutions
CLOUD & DATACENTER CONFERENCE Germany

Windows Server System Insights

- Available since Windows Server 2019
- Physical or virtual
- Hypervisor agnostic
- Cloud agnostic
- Easy to activate
- Integrated in Windows Admin Center

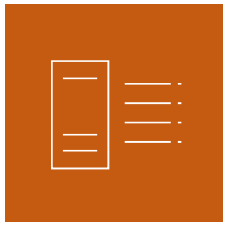
Feststellen der Ressourcenauslastung

1. **Gather the data**
2. **Store the data**
3. **Visualize the data**
4. **Forecast usage**
5. **Maintain pipeline**

@GregorReimling

System Insights

High-accuracy, predictive capabilities for Windows Server 2019



Predictions analyze system data, such as performance counters and ETW events.

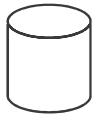
Transform reactive emergencies of the past to **proactive management experiences**

Natively in Windows Server 2019

Node-Local Functionality

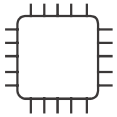
@GregorReimling

Out of the Box Forecasts

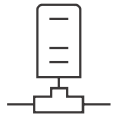


VOLUME

TOTAL STORAGE



CPU



NETWORKING

Forecasting models

Forecast using daily data, collected for a year

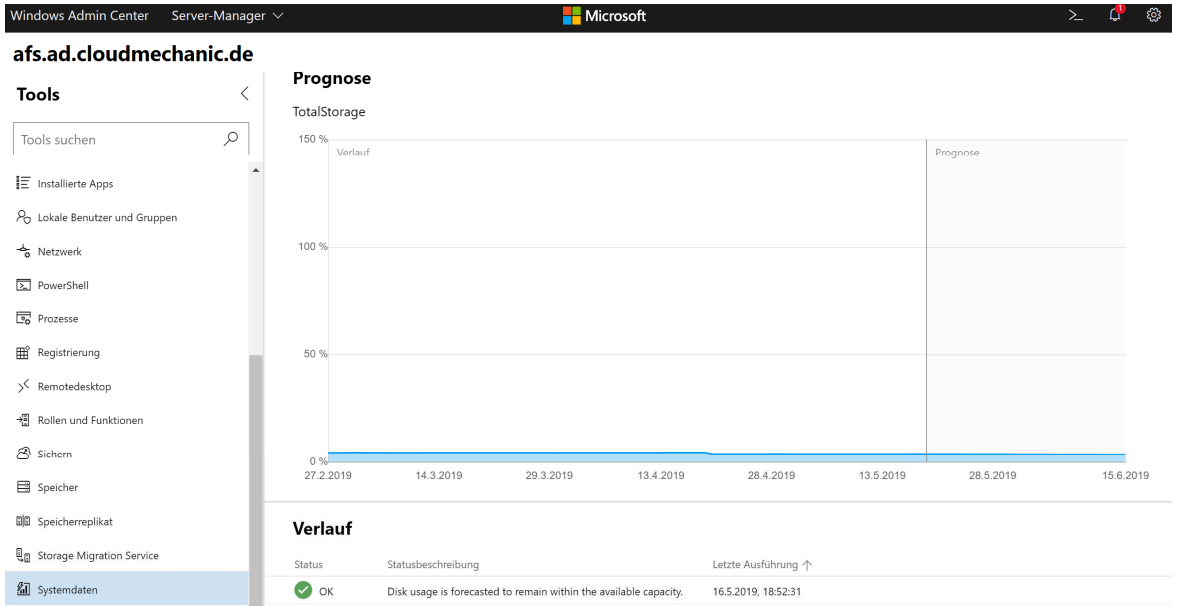
Estimated data footprint = ~5MB

(CPU + # Volumes + # Net. Adapters + # Disks) * 250KB

Trained locally using an auto-regressive model

Agenda

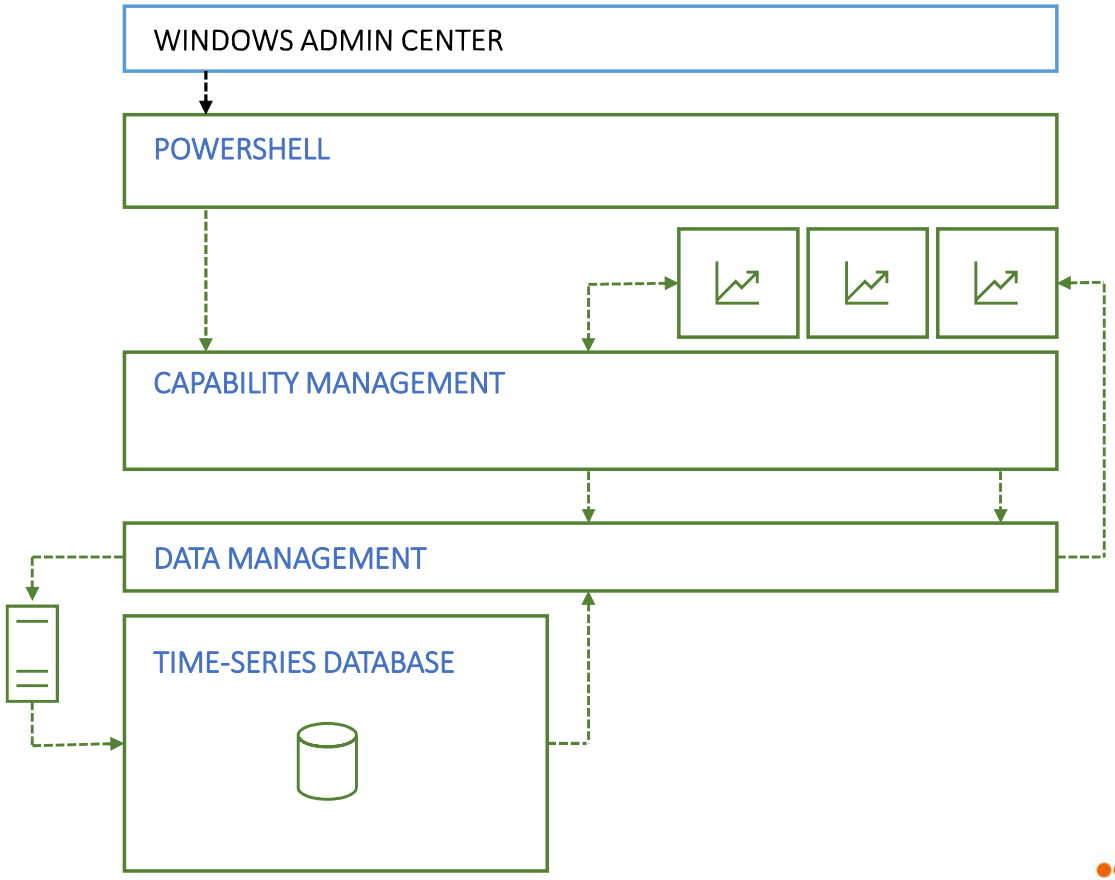
- Generally
- Windows Server Insights
- Azure Monitor (Log Analytics)
- Conclusion



@GregorReimling

powered by Rachfahl IT-Solutions
CLOUD & DATACENTER CONFERENCE Germany

System Insights architecture



System Insights Architecture

Capability Name	Data source(s)	Filtering logic
Volume consumption	Volume size	Max daily usage
Total storage consumption	Sum of volume, sum of disk sizes	Max daily usage
CPU capacity	% processor time	Max 2-hour average per day
Networking capacity	Bytes Total/sec	Max. 2-hour average per day

Prediction status	Event ID	Status description
OK	151	The forecast does not exceed the available capacity
Warning	148	The forecast exceeds the available capacity in the next 30 days
Critical	150	The forecast exceeds the available capacity in the next 7 days
Error	149	The capability ran into an unexpected error
None	132	There isn't enough data to make a prediction

Managing capabilities

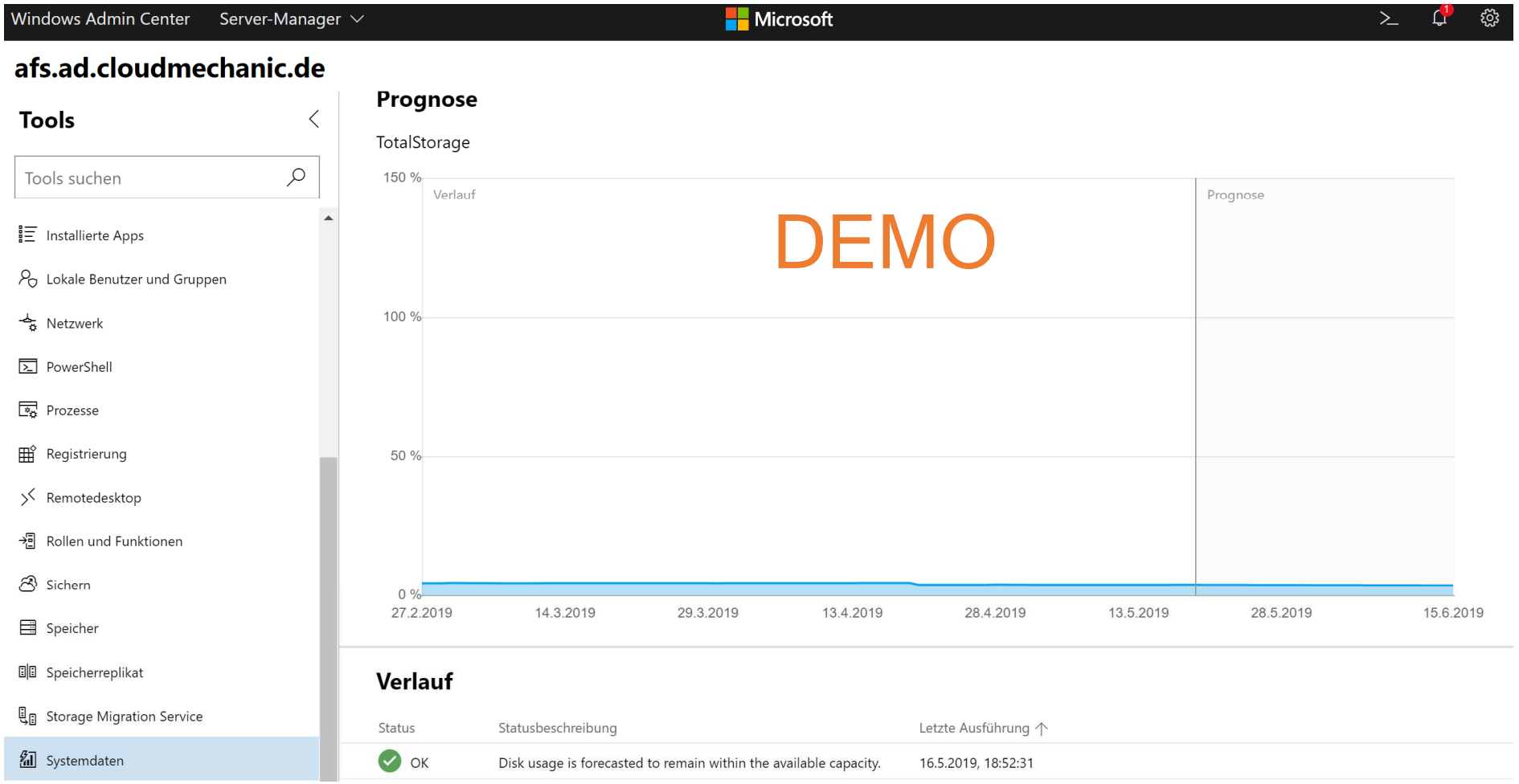
- All results will store in a JSON File
- View all available Capabilitys
  - Get-InsightsCapability
- Enable and Disable Capabilitys
  - En(Dis-)able-InsightsCapability -Name „CPU capacity forec…“
- Invoke-InsightsCapability – Name …
- Get-InsightsCapabilityResult parse JSON File

Creating remediation actions

- Sample remediation actions include running
  - Disk cleanup
  - Running dedup
  - Live migrate VM
  - ….
- Create own scripts that run, when forecast reach warning level
  - Set-InsightsCapabilityAction -Name "CPU capacity forecasting" -Type Warning -Action "C:\Users\Public\WarningScript.ps1" -ActionCredential $Cred
- View all self defined action scripts
  - Get-InsightsCapability | Get-InsightsCapabilityAction

Adding and developing new capabilities

- Add new predective capabilities
- Any new capability can integrate in System Insights
- New capabilities specify any performance counter or system event
- There are many data sources to collect
- To develop there is a System Insights NuGet package available
- Take a look at the API documentation for classes & interfaces
- There are also a System Insights start sample available

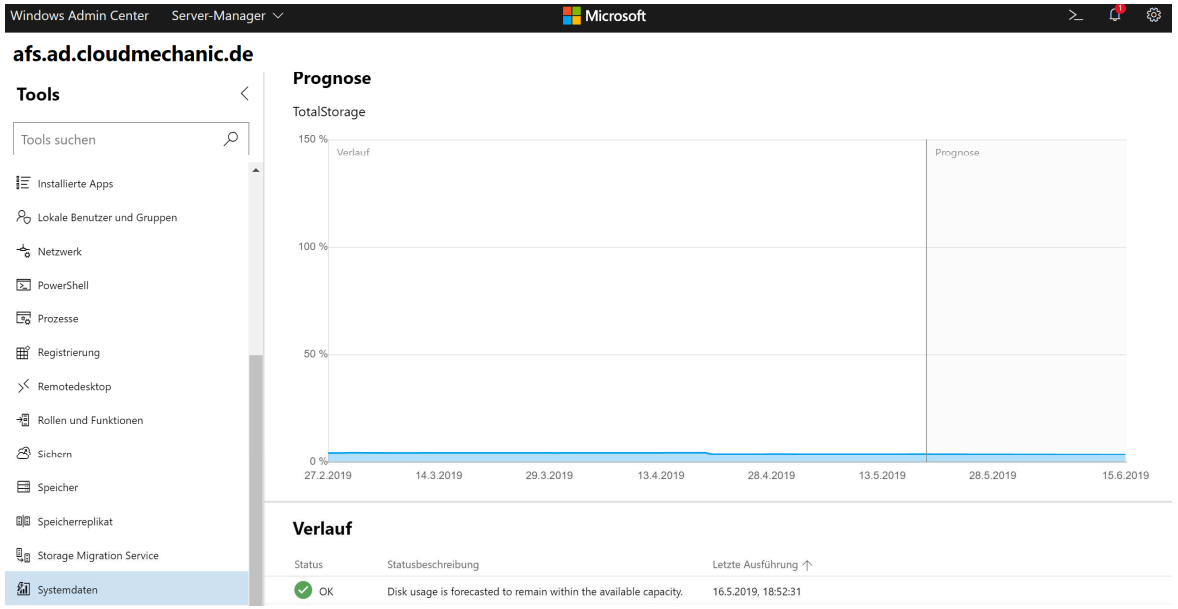


@GregorReimling

powered by Rachfahl IT-Solutions
CLOUD & DATACENTER CONFERENCE Germany

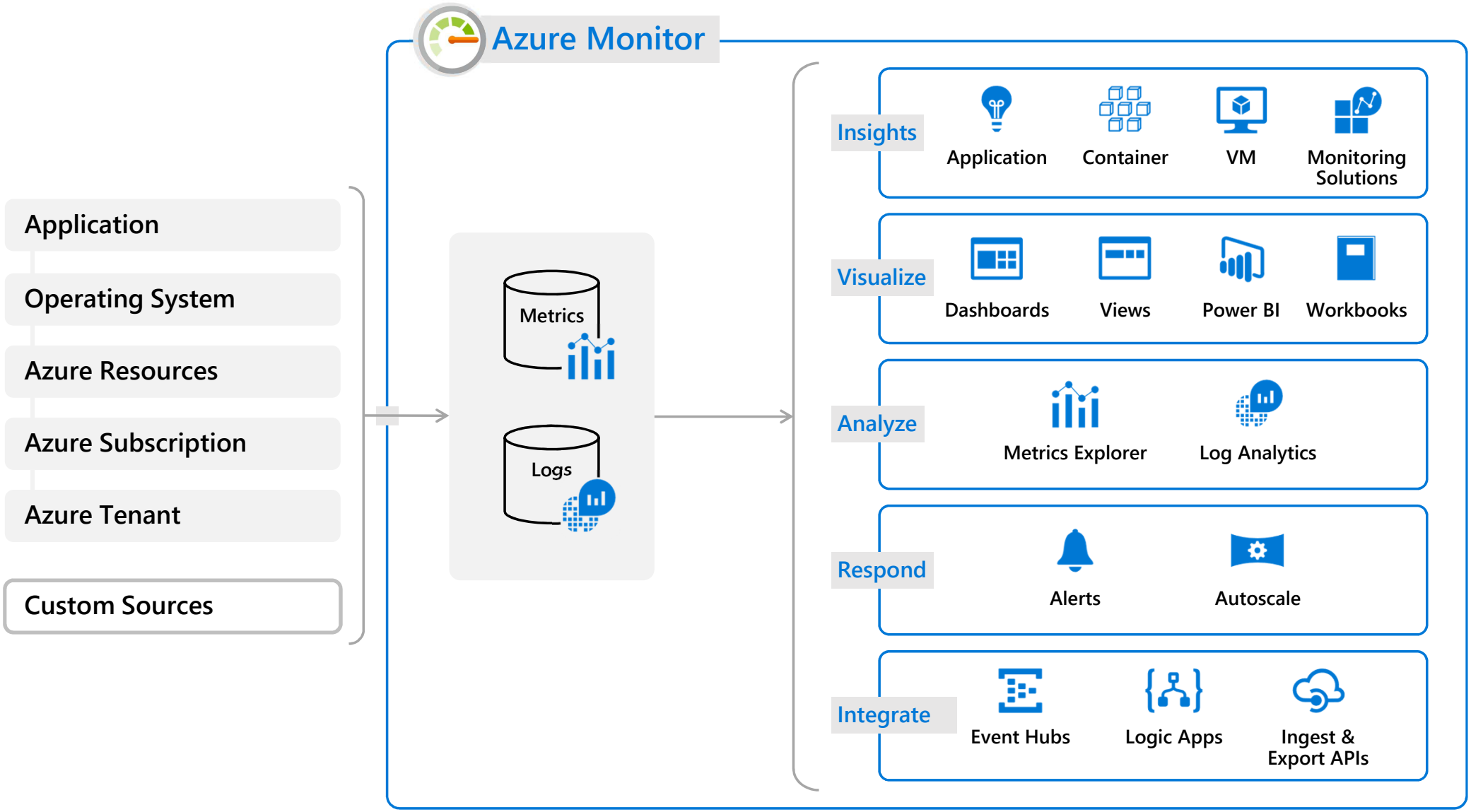
Agenda

- Generally
- Windows Server Insights
- Azure Monitor (Log Analytics)
- Conclusion

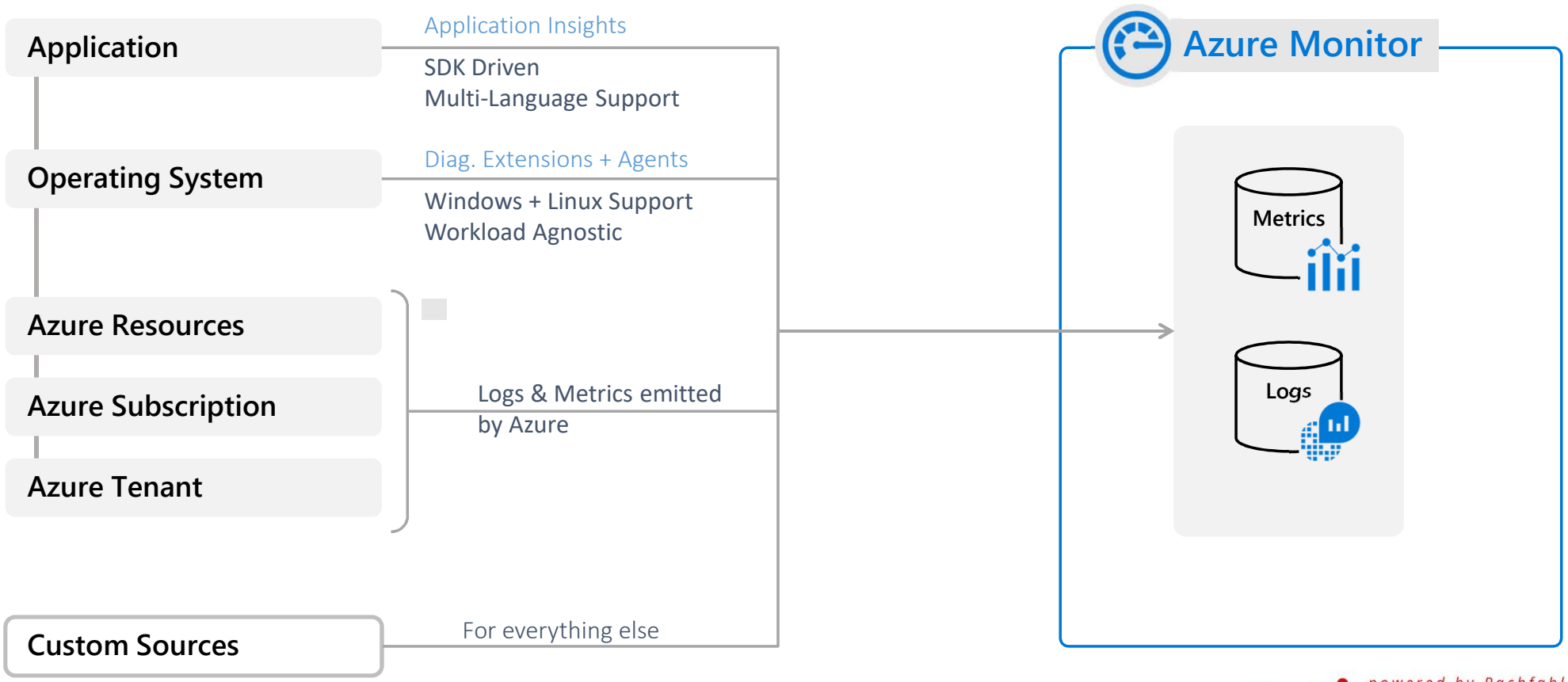


@GregorReimling

powered by Rachfahl IT-Solutions
CLOUD & DATACENTER CONFERENCE Germany

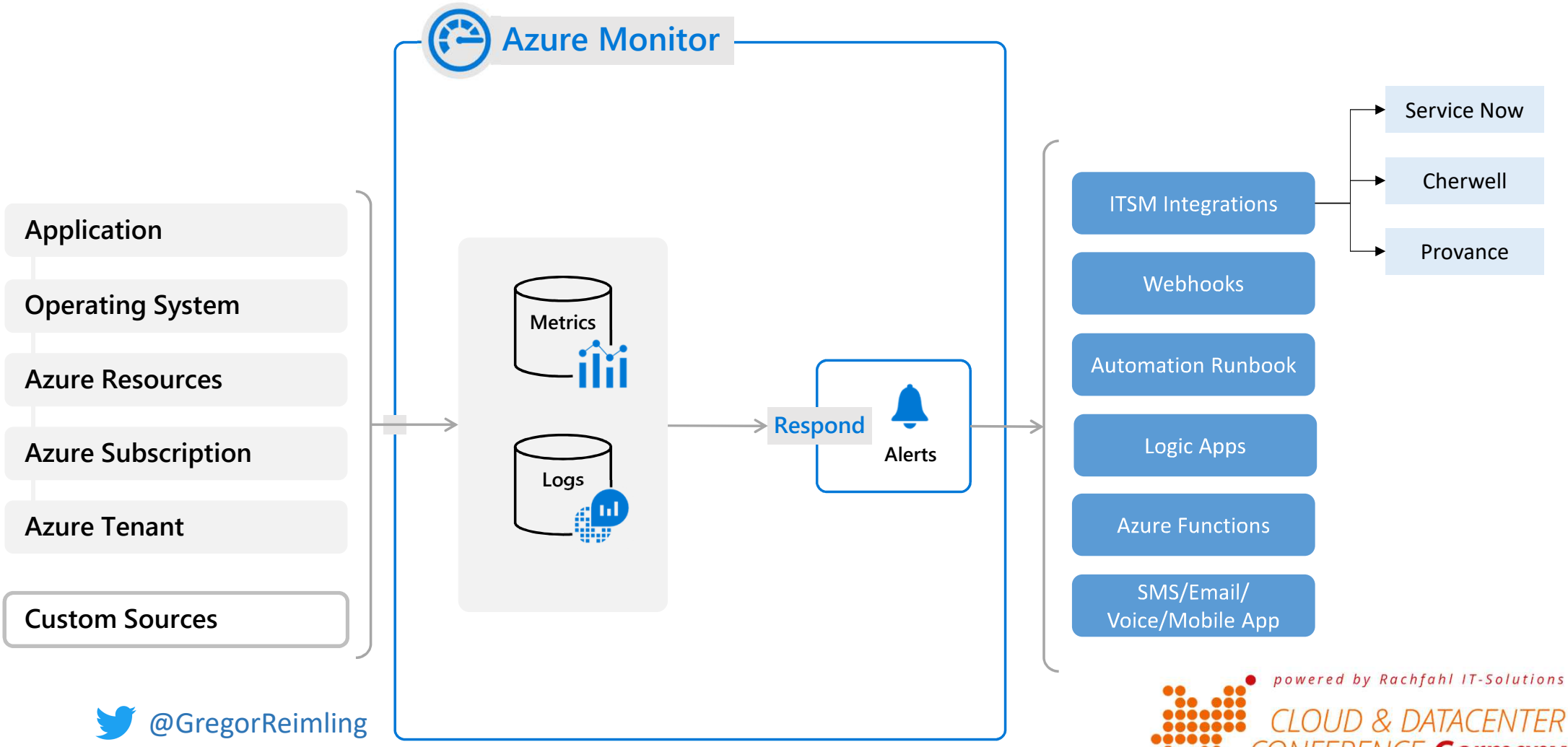

Azure Monitor
Application
Operating System
Azure Resources
Azure Subscription
Azure Tenant
Custom Sources
Metrics
Logs
Insights
Application
Container
VM
Monitoring Solutions
Visualize
Dashboards
Views
Power BI
Workbooks
Analyze
Metrics Explorer
Log Analytics
Respond
Alerts
Autoscale
Integrate
Event Hubs
Logic Apps
Ingest & Export APIs

Wiring it all up



@GregorReimling

Integrate your alerts into a partner system



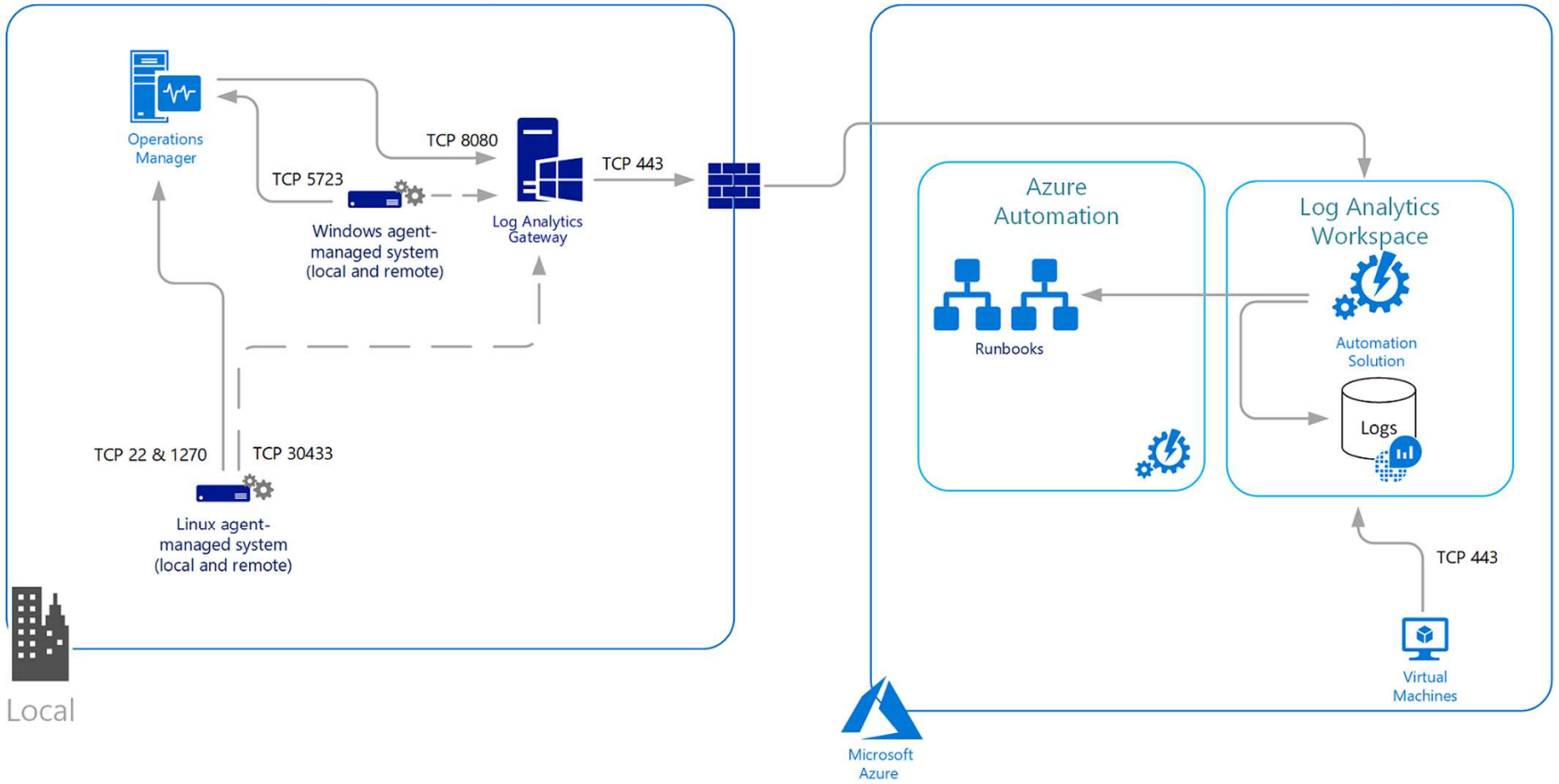
@GregorReimling

Log Analytics Agent

- Log Analytics-Agent for Windows or Linux
  - (Microsoft Monitoring Agent)
  - Also known as SCOM Agent
  - 32-Bit and 64-Bit version available
- Min. Windows Server 2008 R2 or Windows 7 SP1
- Min. Ubuntu 14.04 LTS, CentOS 6, Debian 8, …
- Dependency agent (Part of Service Map)

```
AzureGeek-MMASetup-AMD64.exe /C:"setup.exe /qn ADD_OPINSIGHTS_WORKSPACE=1
OPINSIGHTS_WORKSPACE_ID=b069                    -f2          3098
OPINSIGHTS_WORKSPACE_KEY=hr                      2V+                                  4LP5IuZgY/j
OcxenFpX91hZuKln2yQ== AcceptEndUserLicenseAgreement=1"
InstallDependencyAgentforServiceMap-Windows.exe /s
```

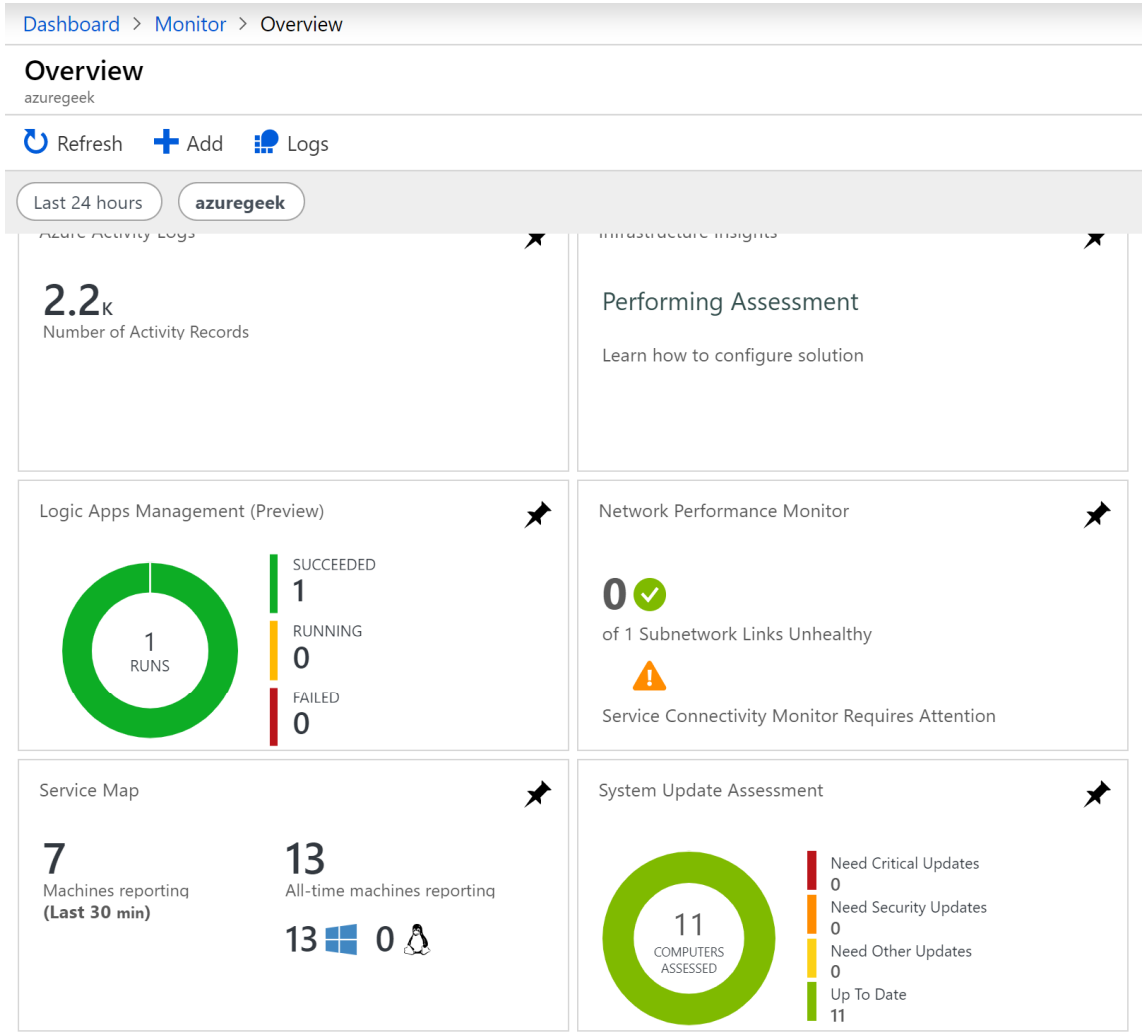
Log Analytics Agent



Azure Monitor

- Easy activate for Azure VMs (extension based)
- Agent for Windows Server and Linux VMs available
- Agent is the same like SCOM agent
- Easy to set up
- Low price
  - Data Ingestion
    - First 5GB per Loganlytics free for every month
    - 2,52€ per additional GB per month
  - Data Retention
    - No charge for every GB in the first 31 days
    - 0,11€ per additional GB per month
- Many possibilities for alarms

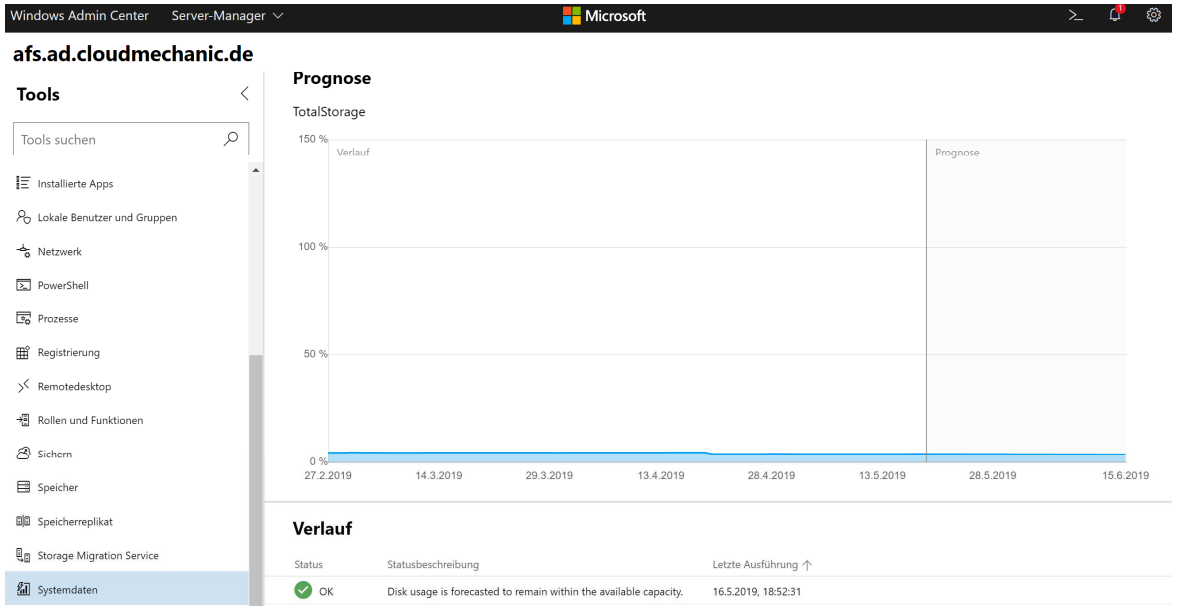
DEMO



@GregorReimling

Agenda

- Generally
- Windows Server Insights
- Azure Monitor (Log Analytics)
- Conclusion



@GregorReimling

powered by Rachfahl IT-Solutions
CLOUD & DATACENTER CONFERENCE Germany

System Insights & Azure Monitor Conclusion

- System Insights
  - Easy to activate ☺
  - Need less CPU performance and storage ☺
  - Only single node solution 😐
  - Limited forecast extensions available 😐
  - No Out-of-the-Box Integration in SCOM or Azure Monitor ☹
- Azure Monitor
  - Easy to setup and price cheap ☺
  - On-Prem Agent with good OS Support ☺
  - Start a little bit complex 😐

Outlook

- More extensions will be come
- Extensions from 3-rd Party companies are in planning
- Group based view needed
- Easy integration in Azure Monitor or 3rd party tools would be great

Links

- System Insights - Microsoft DOCs
- System Insights - Add capabilities
- System Insights – API
- System Insights – Sample capabilities
- Azure Monitor – Microsoft DOCs
- Azure Monitor – Action Groups
- Azure Monitor Blog by Stefan Roth
- Azure Monitor – Price Overview

Zeit für Fragen

http://www.jobinterviewtools.com/blog/wp-content/uploads/2010/01/dreamstimemedium_19473030-300x300.jpg

@GregorReimling

Danke an unsere Partner!

Platinum Sponsor

Gold Sponsoren

Danke an unsere Partner!

Gold Sponsoren

Silber Sponsoren

Vielen Dank für eure Aufmerksamkeit

Gregor Reimling | Azure MVP

powered by Rachfahl IT-Solutions

CLOUD & DATACENTER CONFERENCE Germany

Azure Meetup BONN