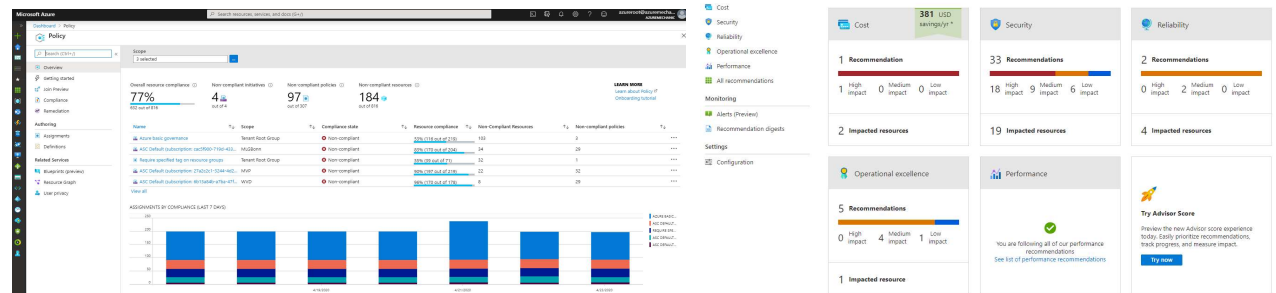
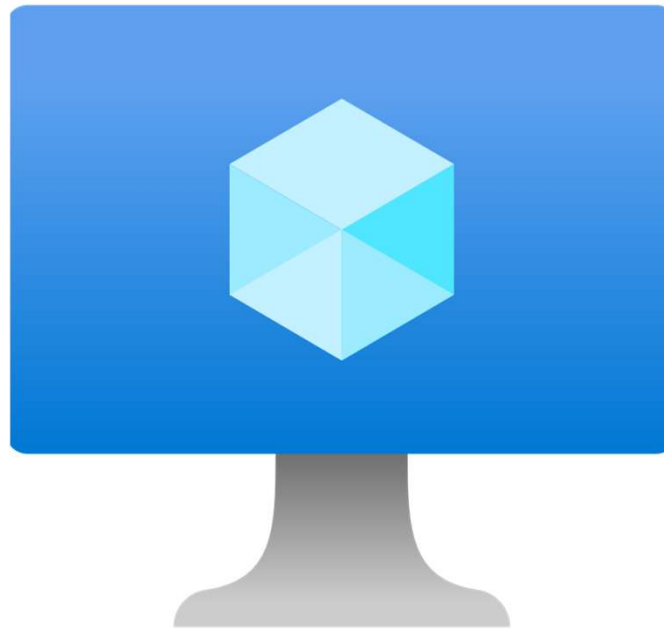


Azure VM Best Practices

by Gregor Reimling



About "Gregor Reimling"



Focus

Azure Governance, Security and IaaS

From

Cologne, Germany

My Blog

<https://www.Reimling.eu>



Certifications

MVP for Azure & Security, Cloud Architect

Hobbies

Family, Community, Worldtraveler

Contact



@GregorReimling

@CloudInspires



[cloudinspires](https://cloudinspires.com)



CLOUD IDENTITY SUMMIT '23

Thu, September 7th, 2023

Deep-Dive and Q&A sessions on #AzureAD
Hybrid Event in Koblenz, Germany
www.identitysummit.cloud

Community event by



Follow us on Twitter:
[@identitysummit](https://twitter.com/identitysummit)

Agenda

- Azure VM Überblick
- Best Practices
- Empfehlungen
- Zusammenfassung



Proactively apply policies and optimize cloud spend



Industry leading Security with Advanced Threat Protection



High availability and protection for VMs, apps and data



Deep operational insights with rich intelligence



Powerful scripting, configuration and update management



Warum Azure VM Best Practices?



Fehlende Richtlinien und/oder Cloud Governance in der Cloud Nutzung

Häufig keine Unterscheidung zwischen Entwicklung und Produktion

Geringe Automatisierung

Vernachlässigte Sicherheit

Geringes Kostenbewusstsein für Cloud Services

Azure VM Sizing

Die Größe von Azure VM sollte auf der tatsächlichen Anwendungsleistung basieren

Überwachung bestehender Arbeitsbelastungen zur Ermittlung genauer Leistungsdaten

Regelmäßige Überprüfung der Leistungsentwicklung, um Anpassungen vornehmen zu können

Regelmäßiger Blick auf Azure-Tools wie Advisor und Security Center



Auto Start and Stop for VMs





- Azure VMs Größen werden nach CPU/RAM Nutzung auf stündlicher Basis berechnet
- Wichtig ist VMs aufzuteilen nach Business Hours und 7/24 Nutzung
- Auto Start- und Stop VM Funktion vereinheitlichen und verpflichten



Wahl der korrekten Disk Größe und SKU

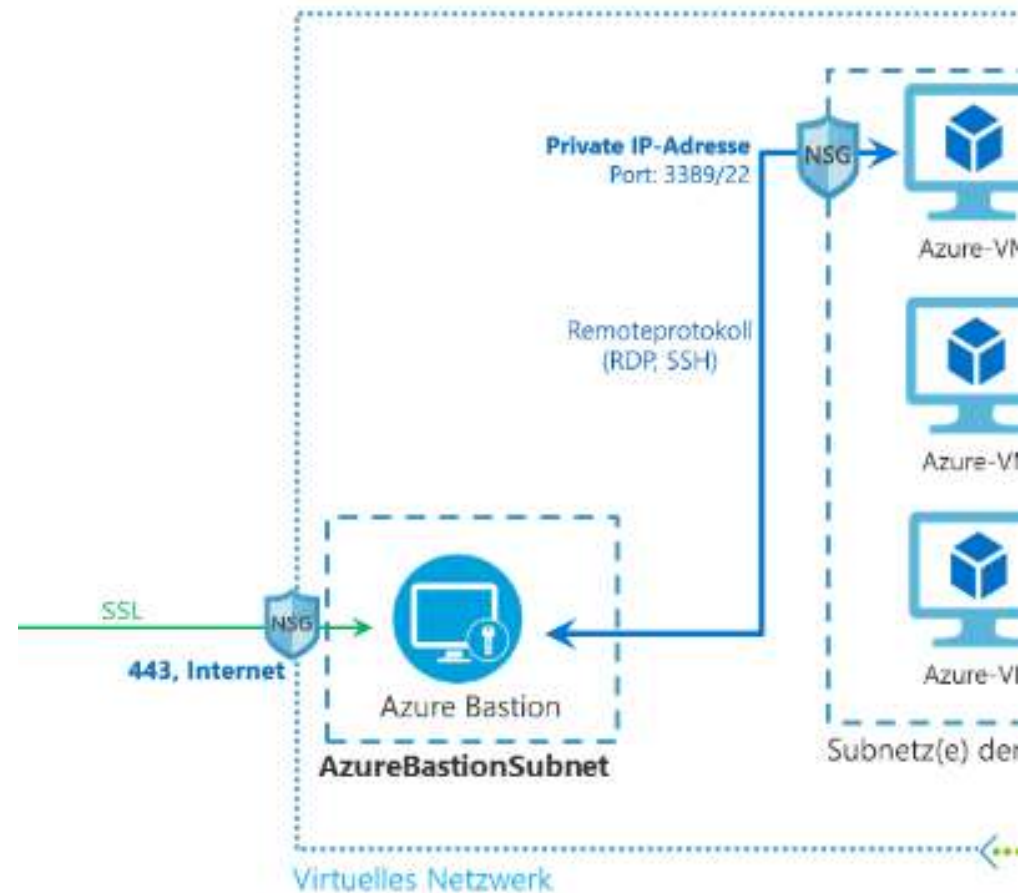


Single disk max value

				
	Standard HDD	Standard SSD	Premium SSD	Ultra SSD
	Low-cost storage	Consistent performance	High performance	Sub-millisecond latency
SIZE	32TiB	32TiB	32TiB	64TiB
IOPS	2,000	2,000	20,000	80,000 – 160,000
BANDWIDTH	500 MBps	500 MBps	750 MBps	2,000 MBps

Azure VMs nicht über das Internet verwalten

- RDP/SSH gehören nicht an eine öffentliche IP Adresse
- Zur Verwaltung von VMs gibt es verschiedene Optionen
 - Azure Bastion – Voll verwalteter Jump Host
 - JIT (Just-in-Time-access) Workflow zur Freigabe des SSH/RDP Ports
 - VPN-Verbindung



Update Management

- Jede Azure VM gehört ins Update Management
- Azure Update Management und/oder WSUS
- Definition von Update Policies nach Workloads
- Per Policy Update Management erzwingbar
- Windows Server Richtlinien auch bei Azure Update Management sinnvoll



Microsoft Defender for Cloud (ASC)

- Microsoft Defender for Cloud Free ist frei verfügbar für alle Workloads
- Empfehlungen und Best Practices nach MS Guidelines
- ASC Defender bietet verbesserte Sicherheit
 - Mindestens für Produktive Workloads aktivieren
 - Integriert Vulnerability management
 - Integriert MS Threat protection (keine extra Lizenz notwendig)



Defender for Servers Plans



	Plan 1	Plan 2
Unified View	✓	✓
Automatic MDE provisioning	✓	✓
MS Threat and Vulnerability management	✓	✓
Security Policy and Regulatory Compliance		✓
Integrated Vulnerability by Qualys		✓
Log Analytics 500MB free data ingestion per day		✓
Threat detection		✓
Adaptive application control		✓
File integrity monitoring		✓
Just-in-Time VM access		✓
Adaptive Network hardening		✓
Docker host hardening		✓
Fileless attack detection		✓
Price	5\$ per Server	15\$ per Server

Defender for CSPM Pricing



GA since end of March



Billing starts on Aug 1 2023



Billable workloads will be VMs, Storage Accounts, OSS DBs, & SQL PaaS & Servers on VMs



Price \$5 per **billable** resource/month

Defender for CSPM features

Security recommendations to fix misconfigurations

[Asset inventory](#)

[Secure score](#)

[Data exporting](#)

[Workflow automation](#)

Tools for remediation

Microsoft Cloud Security Benchmark

Governance

Regulatory compliance

Cloud security explorer

Attack path analysis

Agentless scanning for machines

Agentless discovery for Kubernetes

Data aware security posture

MMA ist abgekündigt



Log Analytics agent (MMA) ist abgekündigt Aug 2024

AMA wird als Nachfolger an die Stelle treten

Allerdings ist es abhängig von der Lösung die verwendet wird

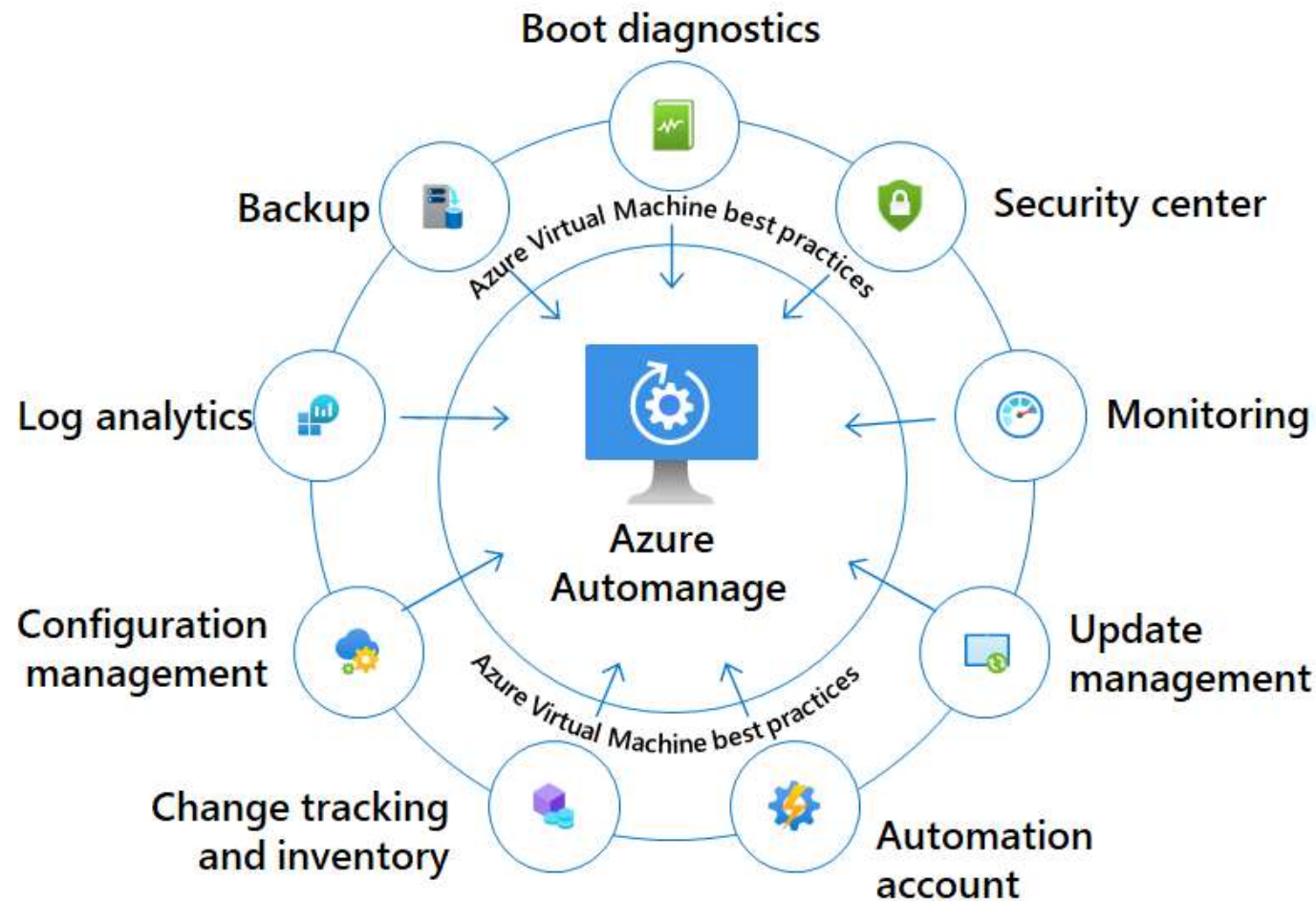
[We're retiring the Log Analytics agent in Azure Monitor on 31 August 2024 | Azure updates | Microsoft Azure](#)

Zusammenfassung

- Für Azure VM sind Guidelines enorm wichtig
- Guidelines möglichst vor Cloud Nutzung festlegen
- Guidelines in Governance Konzept hinterlegen
- Guidelines technisch mittels Azure Policy durchsetzen
- Zu kompliziert oder Zeitaufwendig? Da gibt es auch was 😊



Azure Automanage





Links

- [Azure VM Best Practices – Reimling.eu](#)
- [Guest health feature in Azure Monitor for virtual machines](#)
- [Azure Update Management overview](#)
- [Azure VM Comparisation](#)
- [Manage Azure resources and monitor costs by creating automation tasks \(preview\)](#)
- [Preview: Azure Automanage for virtual machines](#)
- <https://techcommunity.microsoft.com/t5/azure-security-center/weekly-secure-score-progress-report/ba-p/2159354>
- <https://github.com/Azure/Azure-Security-Center/tree/master/Secure%20Score/SecureScoreOverTimeReport>
- Microsoft Defender for Cloud - strategy and plan towards Log Analytics Agent (MMA) deprecation
- Training: <https://aka.ms/ascninja>
- ASC Lab: <https://aka.ms/aslabs>



CLOUD IDENTITY SUMMIT '23

Thu, September 7th, 2023

Deep-Dive and Q&A sessions on #AzureAD
Hybrid Event in Koblenz, Germany
www.identitysummit.cloud

Community event by



Follow us on Twitter:
[@identitysummit](https://twitter.com/identitysummit)

Thank you



Focus

Azure Governance, Security and IaaS

From

Cologne, Germany

My Blog

<https://www.Reimling.eu>



[cloudinspires](https://cloudinspires.com)

Certifications

Cloud Security Architect, MVP for MS Azure

Hobbies

Family, Community, Worldtraveler

Contact



@GregorReimling

@CloudInspires