

Azure VM Best Practices

by Gregor Reimling

Gregor Reimling



Cloud Consultant



Cloud and Datacenter, Governance



Azure Infrastructure (Governance, IaaS, Security)



info@reimling.eu



@GregorReimling | @AzureBonn



www.reimling.eu | www.neutralien.com








www.AzureBonn.de

Agenda

- Azure VM Überblick
- Best Practices
- Empfehlungen
- Zusammenfassung



				
Governance <small>NEW</small>	Security	Resiliency	Monitoring	Automate
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

Azure VM Components



Warum Azure VM Best Practices?

- Fehlende Guidelines und Governance in der Cloud Nutzung
- Häufig keine Unterscheidung zwischen Entwicklungs- und Produktiv- Umgebung
- Kaum Automatisierung
- Vernachlässigte Sicherheit
- Kostenbewusstsein für Cloud Nutzung wenig ausgeprägt

Korrektes Azure VM Sizing



- Azure VM Size sollte sich an realen Anwendungsperformance orientieren
- Monitoring vorhandener Workloads, um genaue Performance Daten zu ermitteln
- Regelmäßige Prüfung der Performance Entwicklung, um Anpassungen vorzunehmen
- Regelmäßiger Blick auf Azure Tools wie Advisor und Security Center



[Azure VM Comparison \(azureprice.net\)](https://azureprice.net)

Auto Start and Stop for VMs

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

Azure VM Laufzeit > 500h pro Monat = RIS



Wahl der korrekten Disk Größe und SKU



Standard HDD



Standard SSD



Premium SSD



Ultra SSD

Single disk max value

	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

Wahl der korrekten Disk Größe und SKU

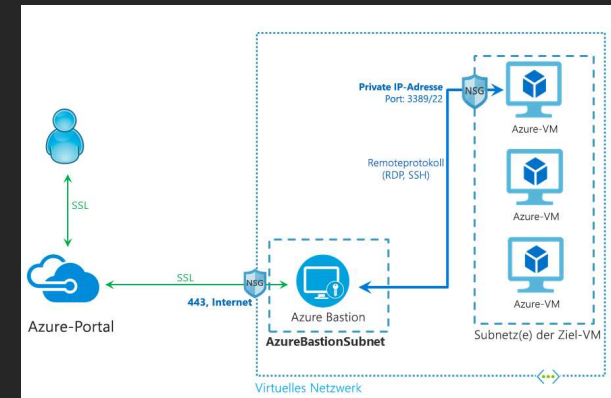


- Kosten für Azure Disks fallen immer an – auch wenn die VM ausgeschaltet (deallocated) ist
- Azure (Managed) Disks Kosten basieren auf Performance und reservierter Größe
- Performance lässt sich jederzeit anpassen
- Für VMs die nur selten genutzt werden, lohnt es sich die SKU auf Standard HDD zu setzen

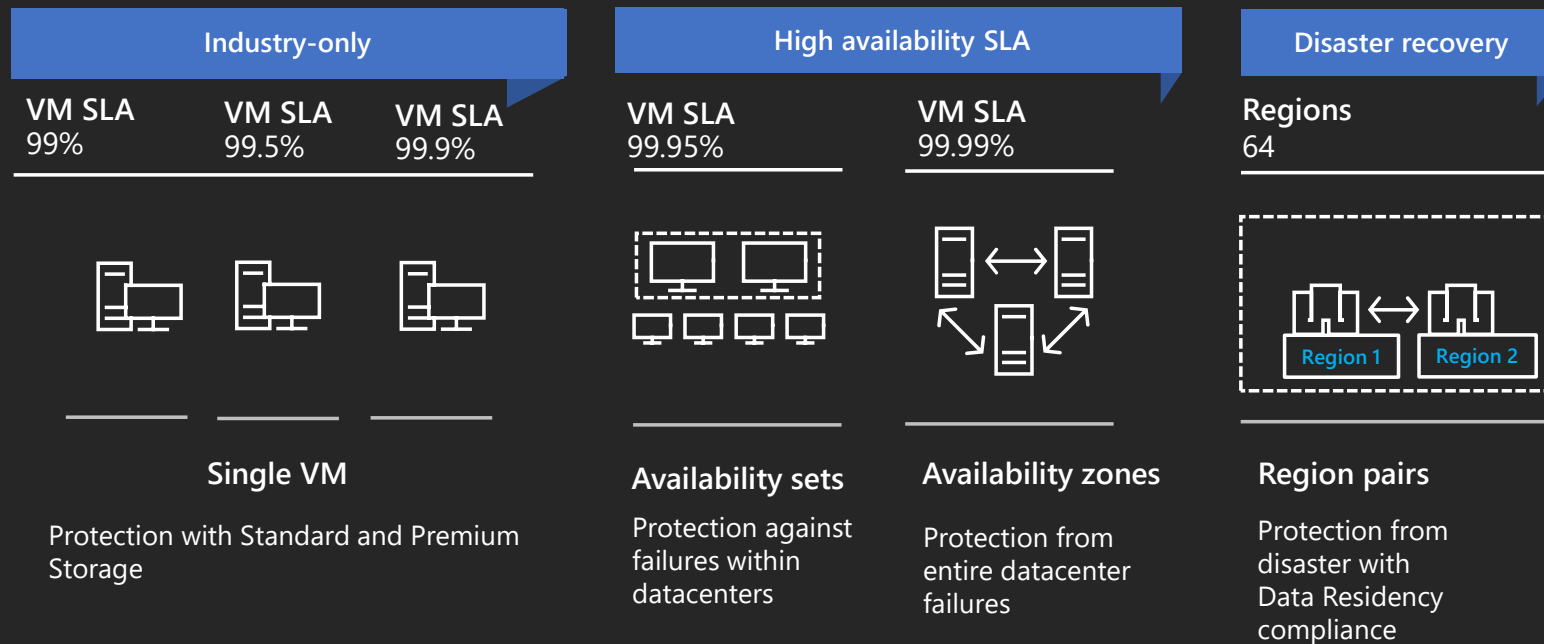
Azure VMs nicht über das Internet verwalten



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



SLA & Hochverfügbarkeit



Öffentliche IP Adressen an Load Balancer



- Azure VMs mit Public IPs sollten immer hinter einem Load Balancer gesetzt werden
- Sichert VM ggü. Internet ab
- Scan zeigt nur den Load Balancer – keine Infos über OS, Patch Stand, etc.
- Load Balancer ermöglicht hohe Flexibilität



Azure VMs in Azure Monitor integrieren



- Log Analytics Workspace als zentrales Monitoring Element
- Microsoft Monitoring Agent Standardmäßig auf jeder VM
- Per Azure Policy automatisierbar
- Ermöglicht weitere Services
 - Azure Update Management
 - Azure Security Center Recommendations
 - Guest Health features

Guest Health Features



- Frei verfügbar über Azure Monitor
- VM min. Windows Server 2012 oder Ubuntu 16.04/18.04 LTS
- Aktiviert Monitoring von
 - CPU Auslastung
 - Freier Speicherplatz
 - Arbeitsspeicher und Auslastung
 - Dateisystem
 - Etc.



[Guest health feature in Azure Monitor for virtual machines](#) | [Azure Blog and Updates](#) | [Microsoft Azure](#)

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

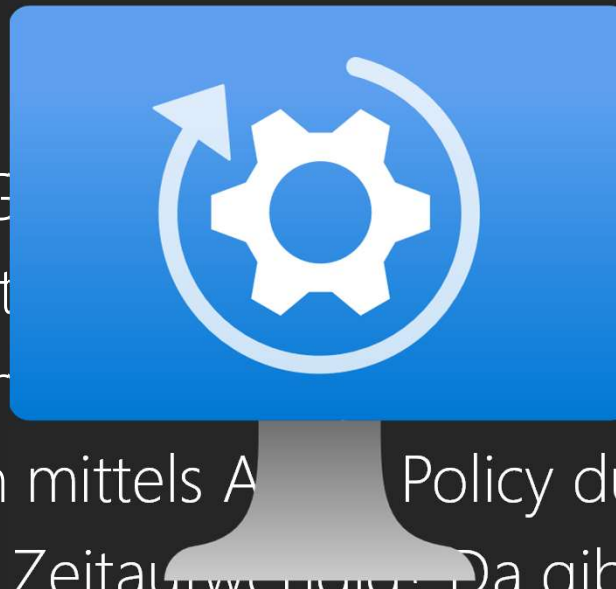
Azure Security Center (Defender)



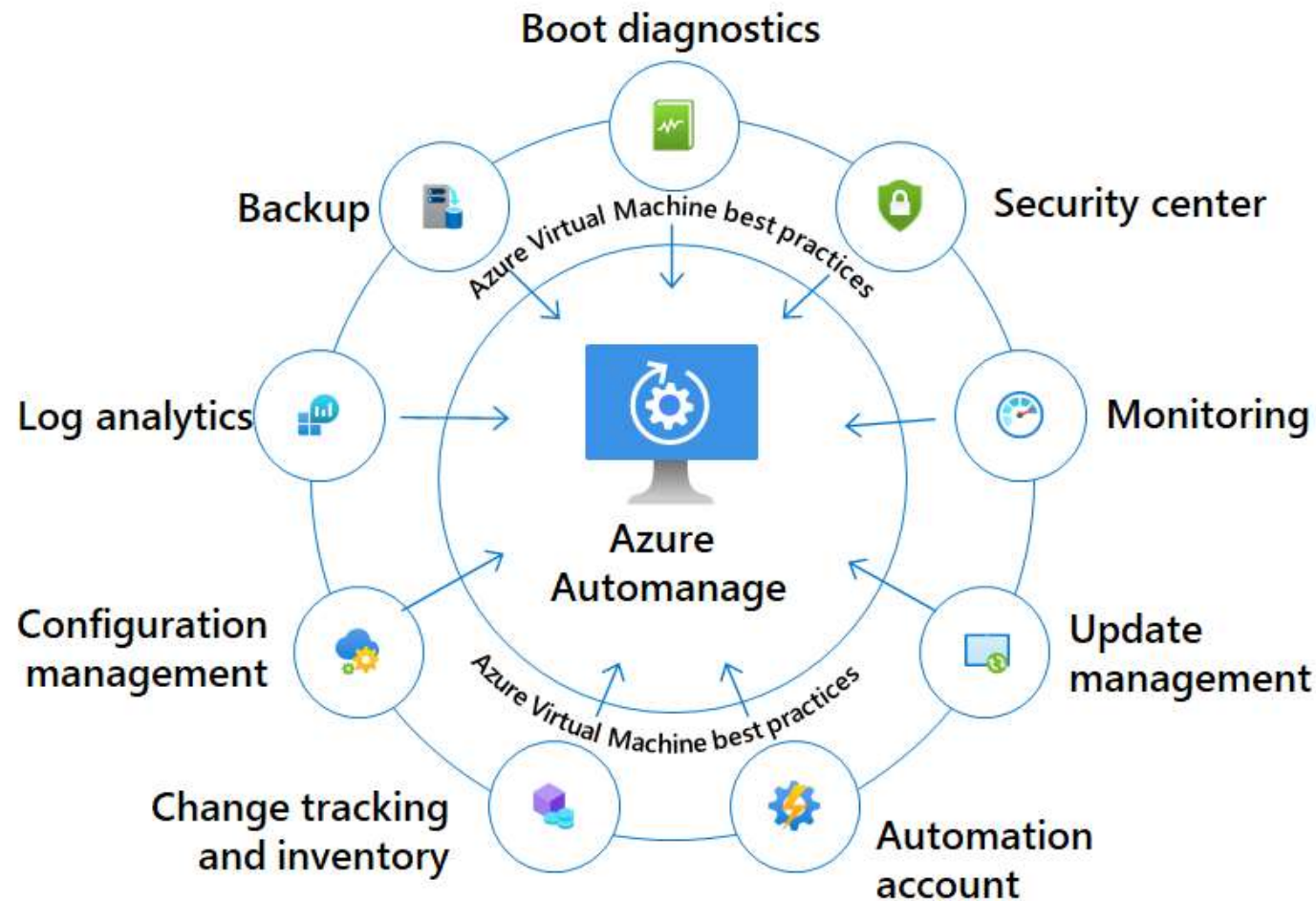
- ASC Basic ist frei verfügbar für alle Workloads
- Empfehlungen und Best Practices nach MS Guidelines
- ASC Defender bietet verbesserte Sicherheit
 - Mindestens für Produktive Workloads aktivieren
 - Integriert Vulnerability management
 - Integriert MS Threat protection (keine extra Lizenz notwendig)

Zusammenfassung

- Für Azure VM sind Guidelines möglich
- Guidelines möglichst frühzeitig festlegen
- Guidelines in Governance umsetzen
- Guidelines technisch mittels Azure Policy durchsetzen
- Zu kompliziert oder Zeitaufwendig: Da gibt es auch was ☺



Azure Automanage

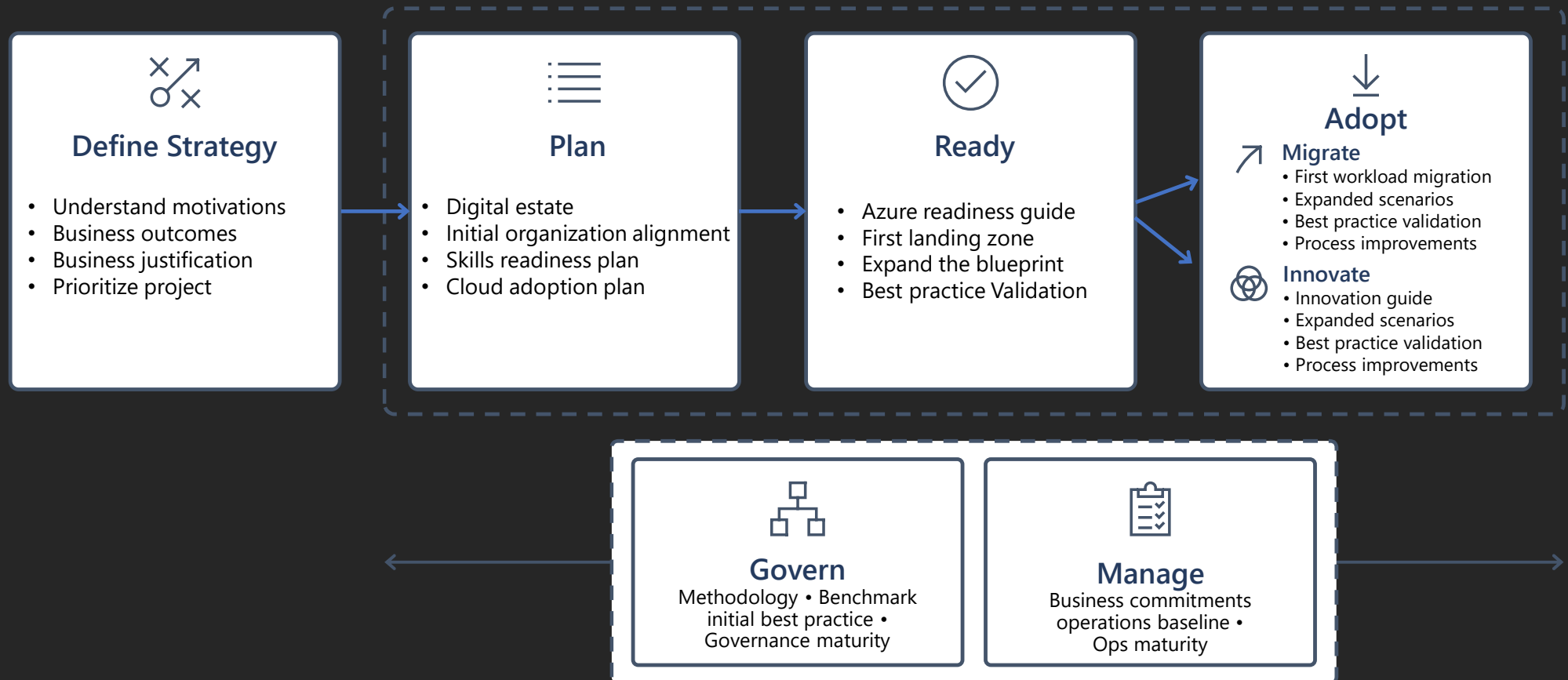


Links





- [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>
- Training: <https://aka.ms/ascninja>
- ASC Lab: <https://aka.ms/aslabs>

Microsoft Cloud Adoption Framework for Azure



Vielen Dank!
Spätere Fragen -> Twitter😊

 @GregorReimling | @AzureBonn
 www.reimling.eu | www.azurebonn.de