

# Azure Automanage

## Dein VM Service Provider



by Gregor Reimling





# Gregor Reimling

Cloud Consultant @ adesso SE

Cloud and Datacenter, Governance

Azure Infrastructure (Governance, IaaS, Security)

info@reimling.eu

@GregorReimling | @AzureBonn

www.reimling.eu | [www.neutralien.com](http://www.neutralien.com)

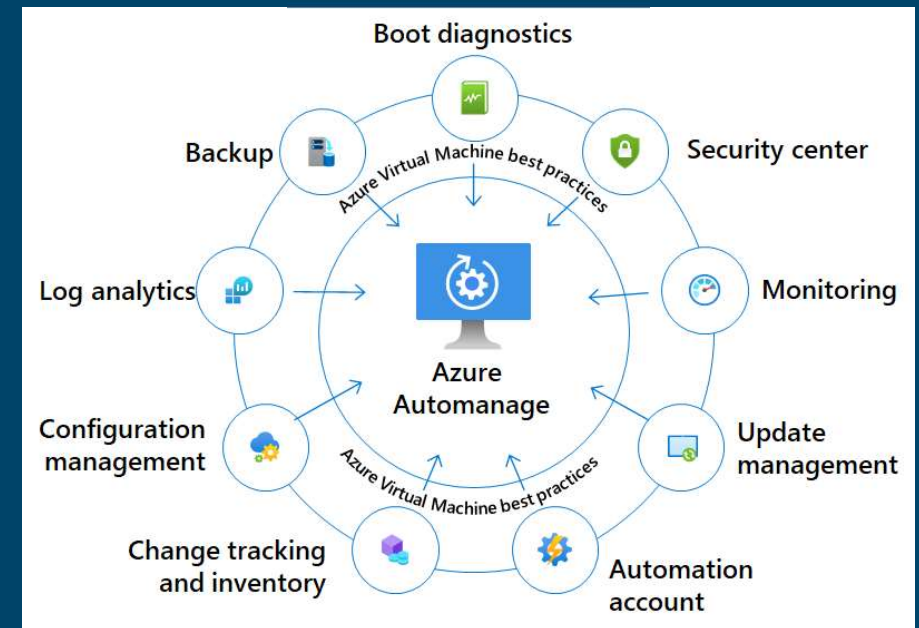


[www.cloudinspires.me](http://www.cloudinspires.me)



# Azure Automanage - Agenda

- Überblick
- Enthaltene Services
- Deployment
- Live Einblicke
- Best Practices
- Zusammenfassung





# Warum Azure Automanage?

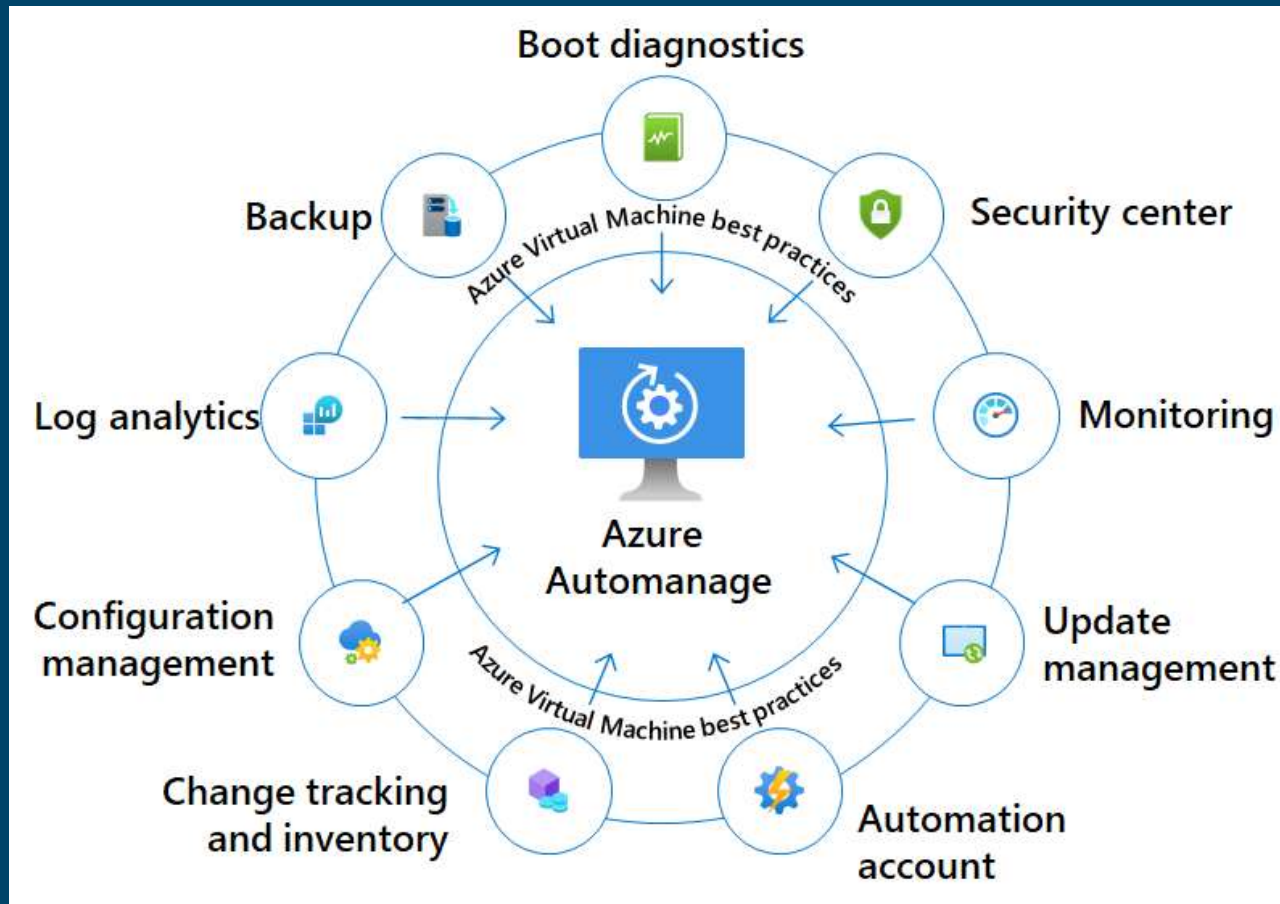
- Azure VMs sind immer noch die häufigsten Services in Tenants
- Vielfältige Einstellungsmöglichkeiten
  - Zeitaufwendig und Fehleranfällig
  - Häufig different und nicht einheitlich
- Jede VM erfordert wiederkehrende, wichtige Tätigkeiten
  - Monitoring & Tracking
  - Security
  - Update Management
  - Backup
- MS hat dies mittlerweile im Cloud Adoption Framework hinterlegt



# Dein Service Provider

- Bringt Automatisiert Best Practices Konfiguration für alle VMs in den Tenant
- Über Azure Arc auf alle VMs
- Vollständig Anpassbar über Benutzerdefinierte Profile
- Für Windows und Linux VMs
- Kostenfrei verfügbar

# Azure Automanage – Überblick



# Voraussetzungen

- Supported Windows Versions
  - Windows Server 2012 R2 and above
  - Windows Server 2022 Azure edition \*
  - Windows 10
- Supported Linux Distributions
  - CentOS 7.3+ & 8
  - RHEL 7.4+ & 8
  - Ubuntu 16.04; 18.04 and 20.04
  - SLES 12
- Supported Regions
  - West and North Europe
  - Central- East- and West US (2)
  - South- and West Central US
  - Canada Central
  - UK South



# Aktivierung

- Automanage Resource Provider registrieren
- Contributor Rechte auf Subscription/Ressourcengruppe
- Aktuell noch keine vordefinierte Azure Automanage Rolle vorhanden
- Bringt zwei Default Profile mit
  - Production
  - Dev / Test
- Spezifische Profile möglich
- Automanage Services und Standardkonfiguration im Profil enthalten

Azure (Enterprise) | Resource providers

Register Unregister Refresh Feedback

automanage

Provider	Status
Microsoft.Automanage	NotRegistered

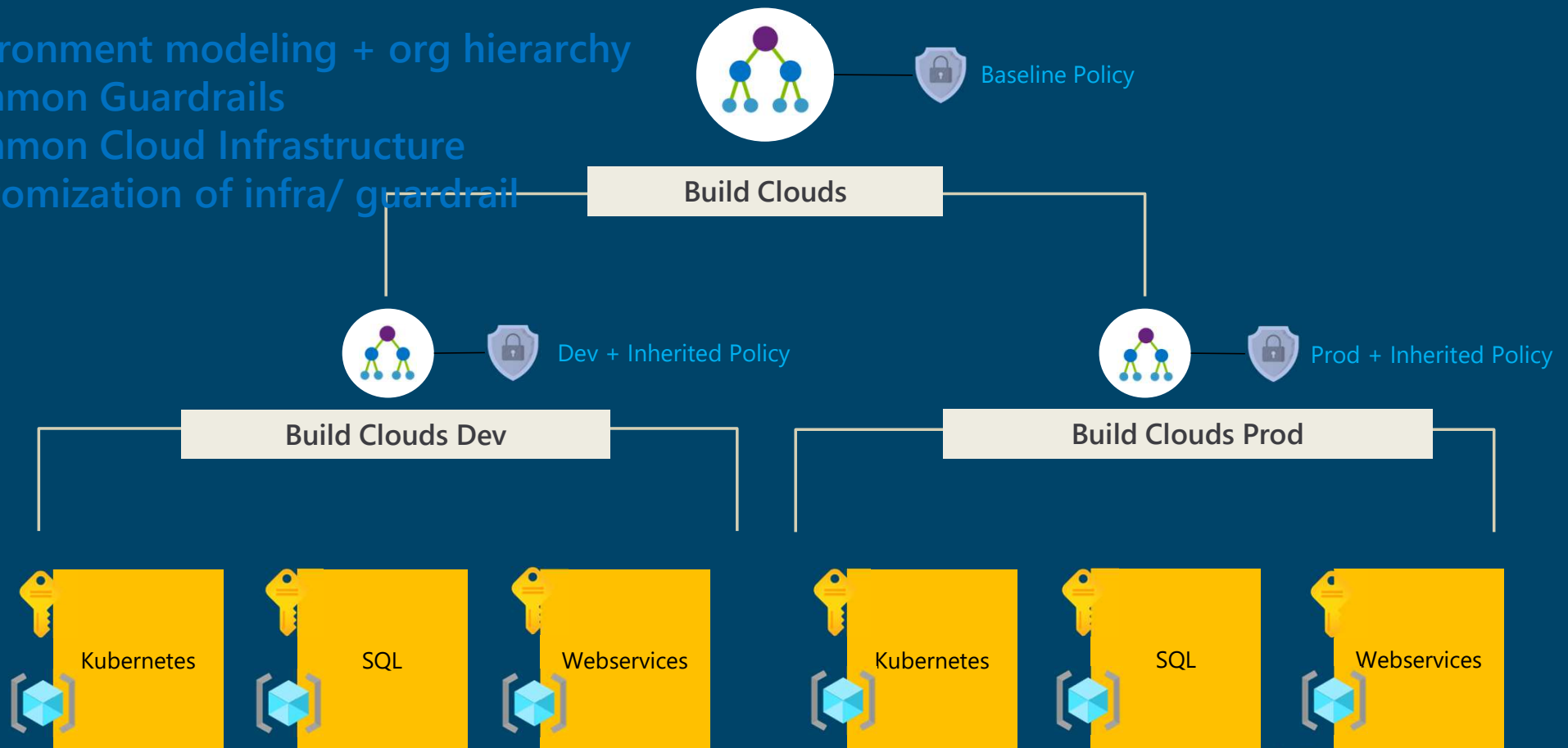
✓ Automanage Resource Provider Registration Succeeded

Microsoft.Automanage resource provider registered for 1 subscription(s).



# Management Groups

Environment modeling + org hierarchy  
Common Guardrails  
Common Cloud Infrastructure  
Customization of infra/ guardrail



# Windows vs. Linux

Service	Windows VMs	Linux VMs	WS Azure Edition
Machine Insights Monitoring	X	X	X
Backup	X	X	
MS Defender for Cloud	X	X	X
Update Management	X	X	X
Change Tracking & Inventory	X Audit & Remediate	X Audit only	X Audit & Remediate
Guest configuration	X	X	X
Boot diagnostics	X	X	X
Azure Automation Account	X	X	X
Log Analytics Workspace	X	X	X
MS Antimalware	X		X
Windows Admin Center	X		X
Hotpatch			X
SMB over QUIC			X
Extended Network for Azure			X

# JSON

```
{
  "id": "/subscriptions/sub-id/resourceGroups/automanage_rg/providers/Microsoft.Automanage/configurationProfiles/Azure-MLG-Best-Practices",
  "name": „Automanage Profilname“,
  "type": "Microsoft.Automanage/configurationProfiles",
  "location": "westeurope",
  "properties": {
    "configuration": {
      "Antimalware/Enable": true,
      "Antimalware/Exclusions/Paths": "",
      "Antimalware/Exclusions/Extensions": "",
      "Antimalware/Exclusions/Processes": "",
      "Antimalware/EnableRealTimeProtection": true,
      "Antimalware/RunScheduledScan": true,
      "Antimalware/ScanType": "Quick",
      "Antimalware/ScanDay": 6,
      "Antimalware/ScanTimeInMinutes": 120,
      "Backup/Enable": true,
      "Backup/PolicyName": "dailyBackupPolicy",
      "Backup/TimeZone": "W. Europe Standard Time",
      "Backup/InstantRpRetentionRangeInDays": 2,
      "Backup/SchedulePolicy/ScheduleRunFrequency": "Daily",
      "Backup/SchedulePolicy/ScheduleRunTimes": [
        "2022-06-27T01:00:00Z"
      ],
      "WindowsAdminCenter/Enable": false,
      "VMInsights/Enable": true,
      "AzureSecurityCenter/Enable": true,
      "UpdateManagement/Enable": true,
      "ChangeTrackingAndInventory/Enable": true,
      "GuestConfiguration/Enable": true,
      "AutomationAccount/Enable": true,
      "LogAnalytics/Enable": true,
      "BootDiagnostics/Enable": true
    }
  },
  "systemData": {
    "createdAt": "2022-06-27T12:34:18.8446552+00:00",
    "createdBy": "gregor@reimling.eu",
    "createdByType": "User",
    "lastModifiedAt": "2022-06-27T12:34:18.8446552+00:00",
    "lastModifiedBy": "gregor@reimling.eu",
    "lastModifiedByType": "User"
  }
}
```



# Guest Configuration

- Installiert Security Baselines für Windows und Linux
- Konfiguriert im Audit-Only Mode
- Non-Compliant Geräte werden angezeigt aber nicht zurück gesetzt
- Zurücksetzen durch erweiterte Konfiguration möglich

```
{  
  "code": "BadRequest",  
  "message": "Exception occurred while trying to get VM information  
from the compute API. Exception: GuestConfiguration failed to get the compute information of t  
he VM. Please ensure Microsoft.GuestConfiguration is registered RP inside the subscription.",
```



# Service Überblick

- MS Defender for Cloud
  - Bindet VM in MS Defender for Cloud (Free Tier) ein
- Azure Boot Diagnostics
  - Ermöglicht Analyse von fehlgeschlagenen hochfahren von Azure VMs
  - Erstellt Storage Account für Ablage der Daten
- Azure Backup
  - Aktiviert Azure Backup
  - Nur im vordefinierten Produktions-Profil aktiviert
  - Zeitpunkt und Aufbewahrung bei Anlage auszuwählen



# WS (vNext) Datacenter Azure Edition

- Preview über Azure Marketplace verfügbar
- Enthält jährlichen Releaseryhtmus
- Release Updates kommen über Windows Update
- WSAE Preview im Frühjahr
- Finales Update im Herbst



# Windows Server Azure Edition

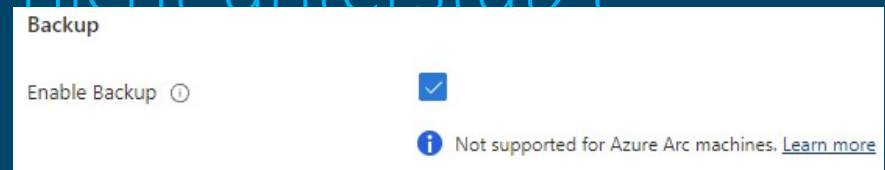
- SMB over QUIC
  - Pakete werden immer mit TLS 1.3 verschlüsselt
  - Erfordert WS 2022 Azure Edition, Win 11, WAC & PKI
  - Automanage überwacht und warnt vor Ablauf der Zertifikate
- Azure Extended Network
  - Ermöglicht Beibehaltung der lokalen IP-Adressen in Azure

Session von Manfred Helber für weitere Infos

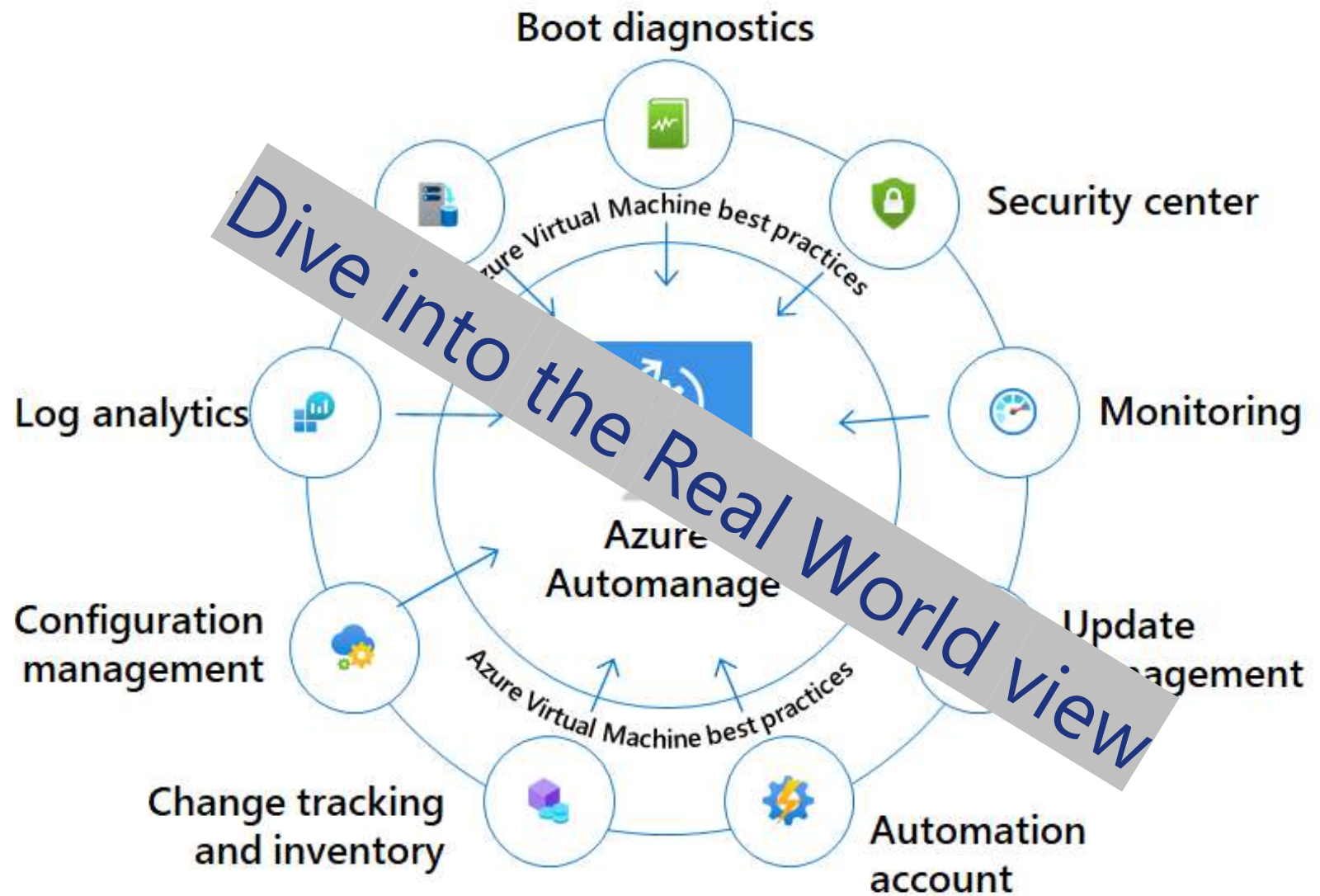


# Azure Arc

- Arc ermöglicht die Anwendung der Azure ARM Control Plane auf Services außerhalb von Azure
- Für VMs, Container, Datenservices und mehr
- Bei VMs Installation von einem Agent
- Arc integrierte VMs werden durch Automanage unterstützt
- Azure Backup ist leider aktuell nicht unterstützt







Dive into the Real World view



# Kosten

- Preview -> Automanage kostenlos
- Kosten fallen für die genutzten Services an
  - Backup
  - Log Analytics Nutzung
  - Storage
  - etc.



# Wissenswertes

- Landing Zone Design sinnvoll
- Azure Automanage via Azure Policy auf bestimmte
  - Management Groups
  - Subscriptions aktivieren
- Angabe vorgegebener Services aktuell nur über ARM möglich 😊



# Wissenswertes

- Profile lassen sich nachträglich nicht bearbeiten ☹
- Verhalten von deaktivierten Azure Automanage VMs
  - VM- und deren Dienst- konfiguration, die aufgenommen wurden, ändert sich nicht
  - Sämtliche Gebühren, die durch die Dienste anfallen, fallen weiterhin an
  - Überwachung des Automanage-Datendriffs wird sofort beendet
- Aktuell kein Support für VMs in Skalierungsgruppen ☹
- Automanage ausschließlich für VMs ☺



# Wissenswertes

- Automanage integriert VMs in Azure Backup
  - VMs mit aktivierter Azure Disk Encryption (ADE) benötigen besondere Anpassungen
- Fehlermeldung -> „Upgrade erforderlich“?
  - Automanage hat eine neue API
  - Zum Wechsel Automanage deaktivieren und wieder aktivieren
  - 2020-06-30-preview -> 2021-04-30-preview oder höher



# Ausblick

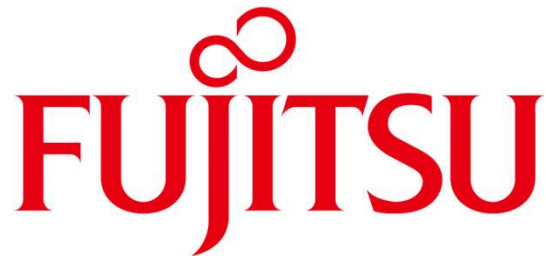
- GA noch unbekannt
- Tagging fehlt noch komplett
- Ermöglichen eigener Guest Policies
- Antimalware auf Azure Arc
- Besseres Customizing der Backend Services



# Vielen Dank an unsere Sponsoren!

---

## Platinum



CREATING COMPUTERS.



---

## Gold



## Silver






# Links



- [Reimling.eu – Azure VM Best Practices](#)
- [Reimling.eu – Azure HA and Latency](#)
- [Azure Automanage MS Landing Page](#)
- [MS Docs – Azure Automange Documentation](#)
- [MS Docs – Azure Automanage Best Practices](#)
- [MS Docs – Windows Server Hotpatch](#)
- [MS Docs – Azure Automanage for Azure Arc VMs](#)
- [MS Docs – Automanage, Azure Backup und ADE](#)
- [MS Docs – Overview of Azure Server Management Services](#)





Questions?  
Please reach me via  
Blog/Linkedin/Twitter 😊

😊 Feedback 😊

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