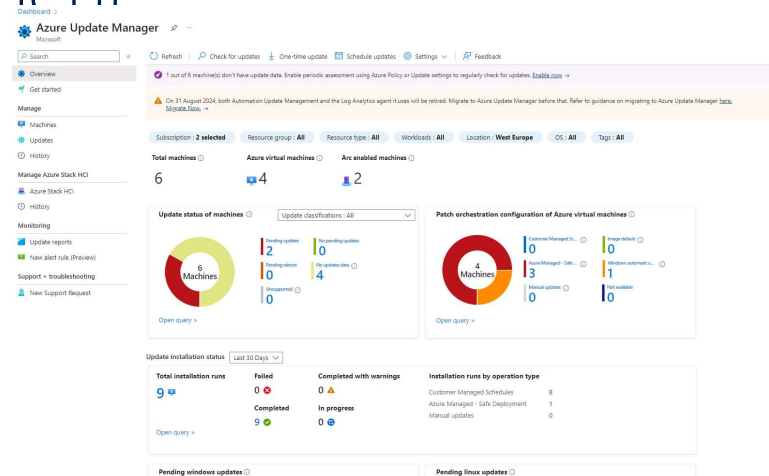




Azure Update Manager

Die neue Zentrale fürs Update Management



Gregor Reimling – Cloud (Security) Architect
www.reimling.eu | @GregorReimling



About "Gregor Reimling"



Focus

Azure Governance, Security and IaaS

From

Cologne, Germany

My Blog

<https://www.reimling.eu>



Certifications

Cloud Security Architect, MVP for MS Azure and Security

Hobbies

Family, Community, Worldtraveler

Contact



@GregorReimling

@CloudInspires



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



CLOUD IDENTITY SUMMIT '24

Save the date!
Thu, September 5th, 2024

Community Event by

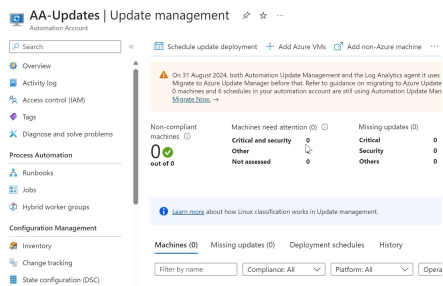


www.identitysummit.cloud

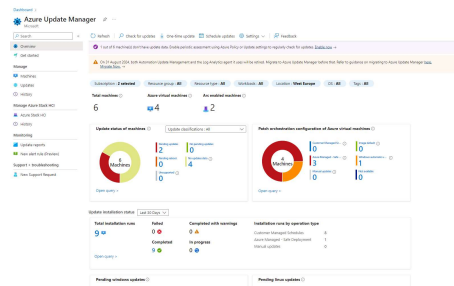


Agenda

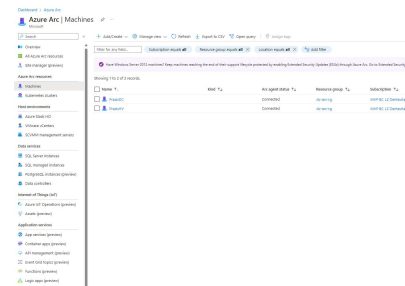
Automation Update



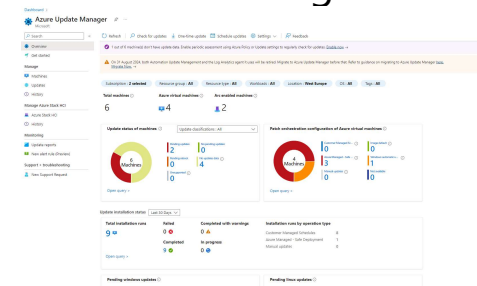
Update Manager



Hotpatching

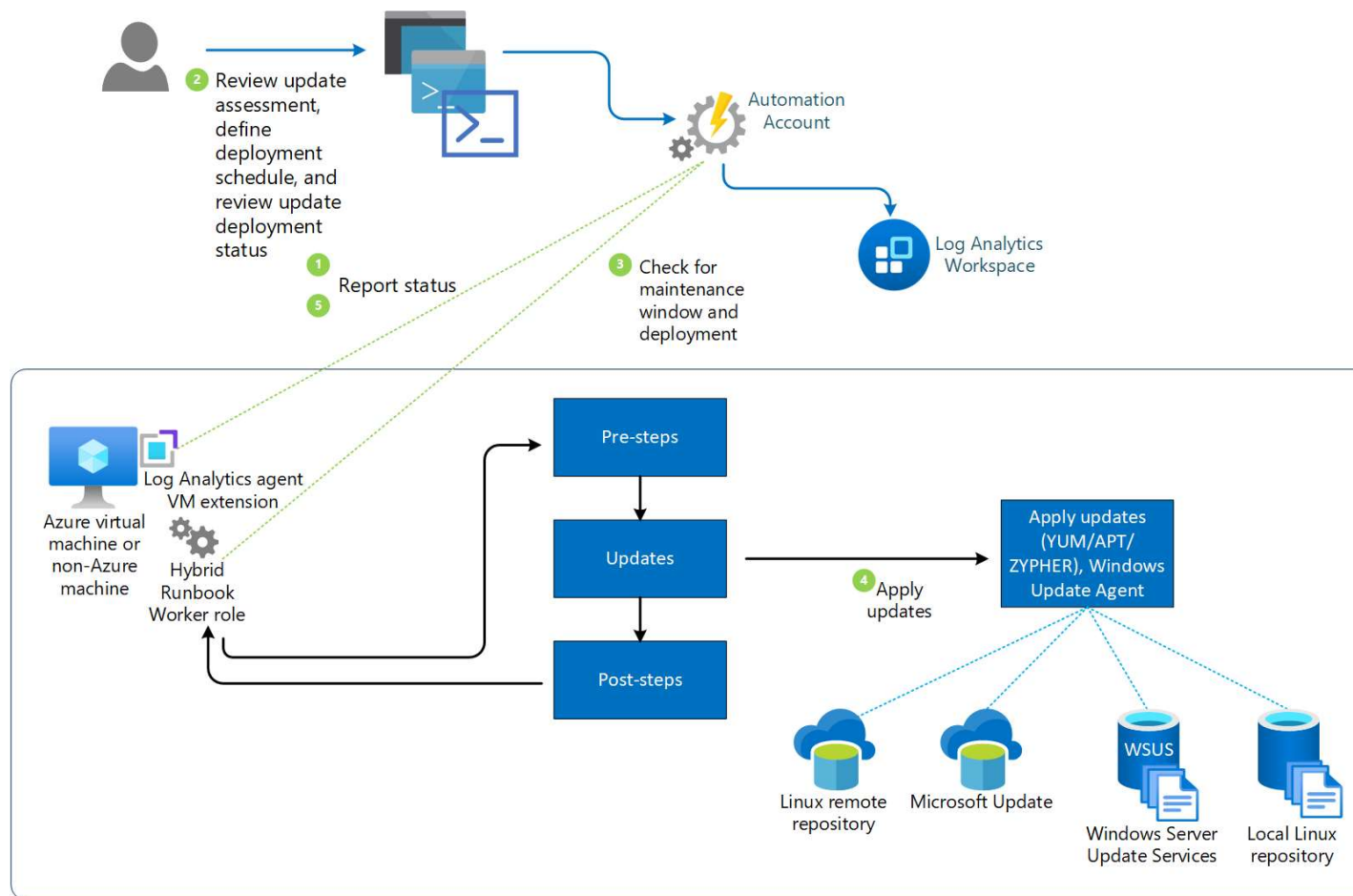


Best Practices & Pricing





Azure Automation Update Management (v1)





Warum Update Manager

GA seit
September 2023



V2 ist komplett Neuentwickelt

Keine Abhängigkeiten zu MMA und Azure Automation
Komplett neue Architektur, dadurch



Vollständiger Support mit Azure Policy



Integration in Enterprise Scale



Server Sichtbarkeit in Azure gewährleistet



Warum Azure Update Manager?



Log Analytics
Workspace



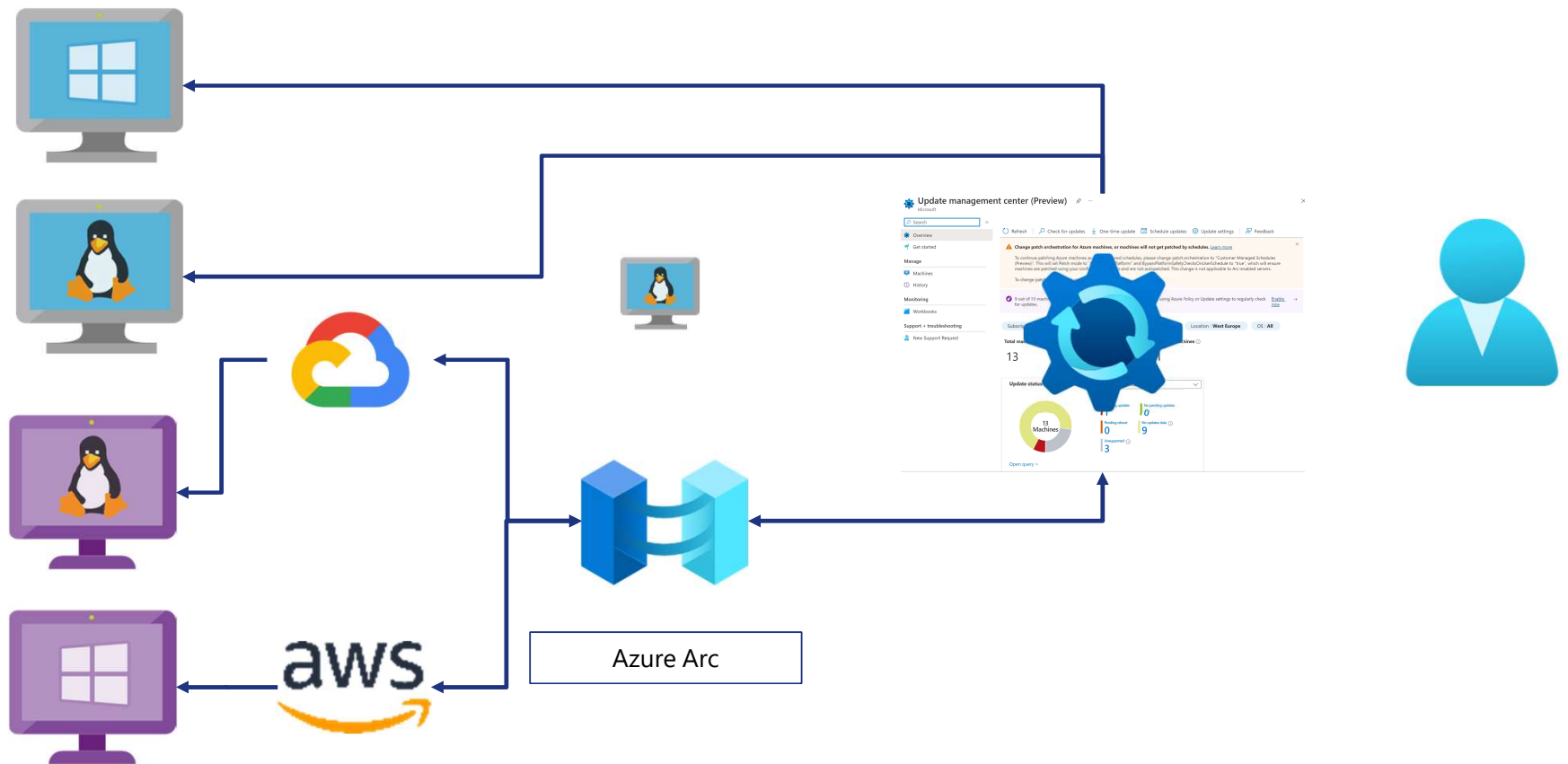
Automation Account

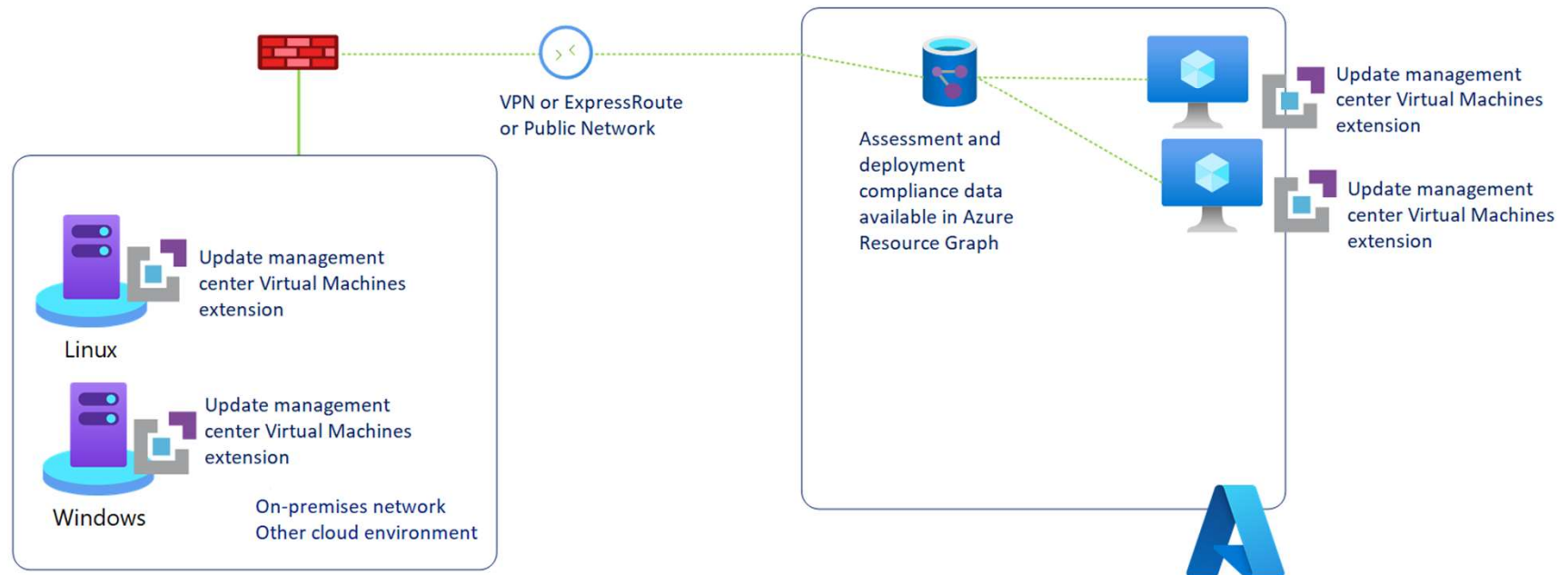
- Derzeitiges Update Management basiert auf Log Analytics Agent (MMA)
- MMA ist zum 31.08.2024 abgekündigt

Azure Log Analytics-Agent (auch bezeichnet als Microsoft Monitoring Agent, MMA), wird im **August 2024 außer Dienst gestellt**. Die Azure Automation Update Management-Lösung basiert auf diesem Agenten und es kann zu Problemen kommen, sobald der Agent außer Betrieb genommen wird, da er nicht mit dem Azure Monitoring Agent (AMA) zusammenarbeitet. ...



Support Matrix und Azure Arc





Update management center Virtual Machines extension makes API calls to/from Windows Update Agent or Linux Package manager to check for update(s) or deploy update(s).



Vorteile

Native Integration ohne MMA oder Azure Automation Abhängigkeit

Integration in Azure Policy

Vollständiger RBAC Support

Support für Automatic Guest Patching

Support für **Hotpatching**



Keyfacts

Alle Assessment und Update Status Infos werden an UMA übermittelt



Assessment Daten stehen für 7 Tage bereit



Update Installationsstatus für 30 Tage



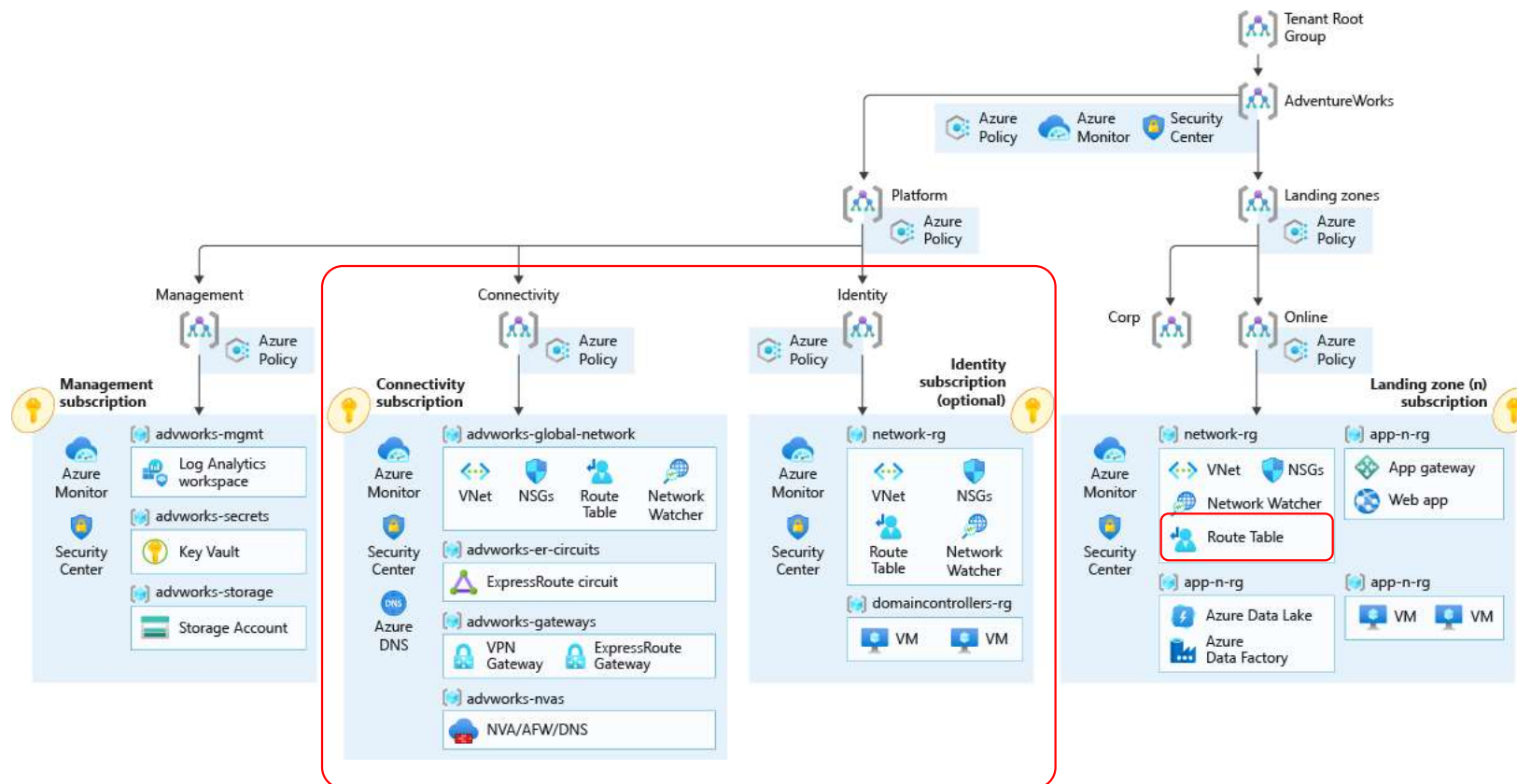
Unterstützung der lokalen Settings

- WSUS oder MS Update



Enterprise-Scale Reference Implementation

Foundation with Advanced Connectivity (Enterprise)



Source: [GitHub-Repo "Azure/Enterprise-Scale"](#) - Deploy Enterprise-Scale with hub and spoke architecture



Unterstützte Funktionen



Linux

Ubuntu Server 16.04 LTS | 18.04 LTS | 20.04 LTS

RHEL 7.2-7.9 | 8-8_6

OpenLogic CentOS | SUSE



Windows

2008R2 SP1 – 2022



Extended Security Updates (ESU)



Support for alle Marketplace Images

Kein Automatisches VM-Gastpatching



Support für Benutzerdefinierte Images

[Azure Update Manager support matrix | Microsoft Learn](#)



(Nicht) Unterstützte Betriebssysteme

Keine Windows
Client
Betriebssysteme -
> Intune

Keine Support für CIS
Images

**Azure Guest Patching Service -
Image Support Request**



Voraussetzungen



Microsoft.Maintenance resource provider



Azure VM oder Azure Arc-enabled server agent



Update Management Manager extension (WindowsPatchExtension)



Aktueller Azure VM Agent



Windows Update Dienst ist aktiviert



On-demand Azure Arc for Servers guest patching preview



Patch Orchestration

Azure Managed – Safe Deployment

- Supported for Linux und Windows
- Modus ermöglicht automatisches VM-Gastpatchen
- Assessment während der Installation und speicherung und Azure Resource Graph
- Unterstützt Patches nach Verfügbarkeit

Customer Managed Schedules

- Nur für Windows VMs
- Unterstützt keine Patches nach Verfügbarkeit
- Standard-Modus wenn nichts anderes konfiguriert ist

Windows automatic updates

- Einstellung der Windows VM werden hier übernommen (Registry-/GPO-settings)

Manual updates

- Nur für Windows VMs
- Unterstützt keine Patches nach Verfügbarkeit
 - Modus sollte für benutzerdefinierte Patchlösungen verwendet werden

ImageDefault

- Nur für virtuelle Linux VMs
- Standard-Modus wenn nichts anderes konfiguriert ist für Linux
- Unterstützt keine Patches nach Verfügbarkeit



Automatic OS image upgrade

Nur für Virtual Machine Scale Sets

Wendet im Batchverfahren immer das neueste, veröffentlichte Image auf VMSS an

Ersetzt vorhandene OS-Disk durch die aktualisierte



Azure Managed – Safe Deployment patching für Azure VMs



Kritische und Sicherheitsupdates werden automatisch heruntergeladen und angewendet



Patches werden außerhalb der Spitzenzeiten für IaaS-VMs in der VM-Zeitzone angewendet



Patches werden immer für VMSS Flex angewendet



Patchorchestrierung wird von Azure verwaltet und Patches werden nach den verfügbarkeitsbasierten Prinzipien angewendet



VM-Integrität wird anhand von Integritätssignalen der Plattform ermittelt und überwacht, um Patchfehler zu erkennen



Die Anwendungsintegrität kann über die Application Health-Erweiterung überwacht werden.



Funktioniert für alle VM-Größen – allerdings kein Support für Benutzerdefinierte Images



Notwendige (aktivierte) Features

Azure VM Agent für Windows oder Linux (Linux min. V. 2.2.53.1)

InGuestAutoPatchVM Extension

C:\Packages\Plugins\Microsoft.CPlat.Core.WindowsPatchExtension<version>



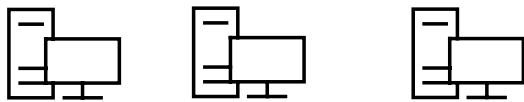
Patch Modus Verfügbarkeitsupdates

Industry-only

VM SLA
99%

VM SLA
99.5%

VM SLA
99.9%



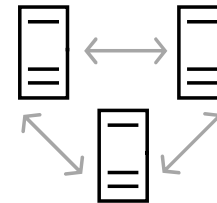
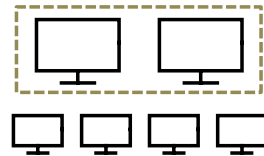
Single VM

Protection with **Standard and** Premium Storage

High availability SLA

VM SLA
99.95%

VM SLA
99.99%



Availability sets

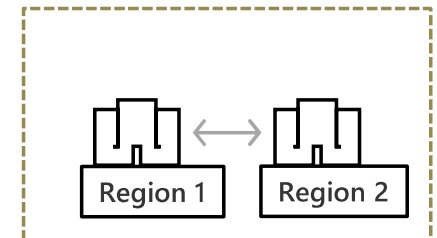
Protection against failures within datacenters

Availability zones

Protection from entire datacenter failures

Disaster recovery

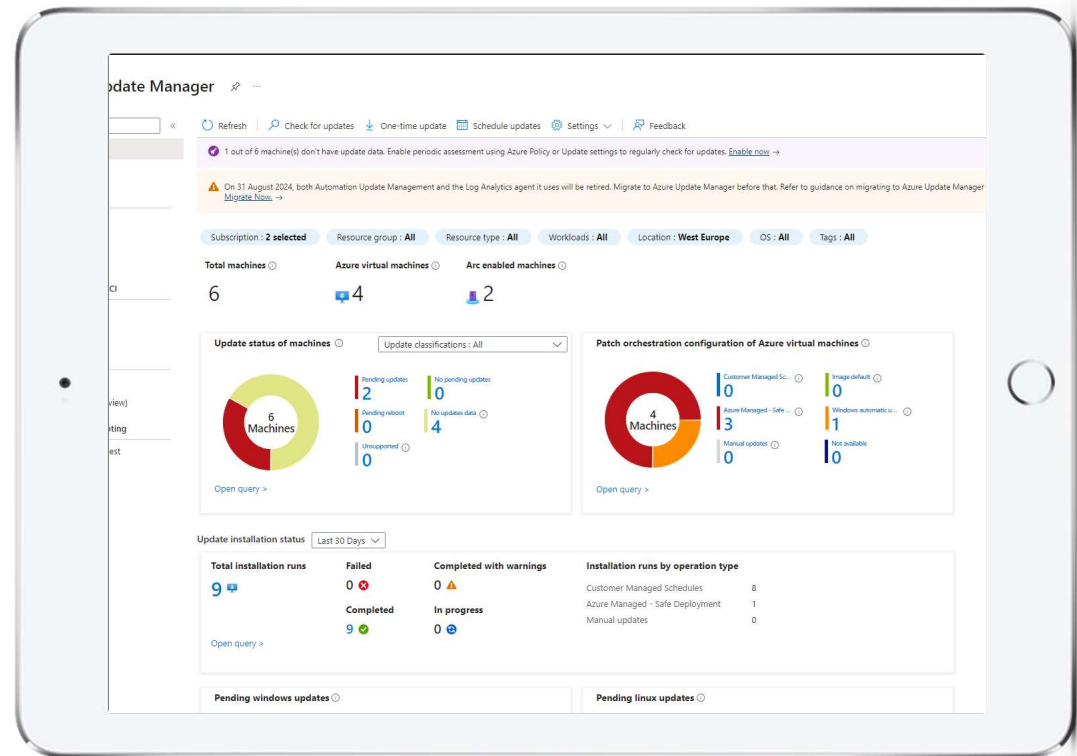
Regions
54



Region pairs

Protection from disaster with Data Residency compliance

Demo + Azure Update Manager





Hotpatch



WS 2022 Datacenter: Azure Edition Server Core

Azure = GA

Azure Stack HCI = GA

Hotpatch im Standard aktiviert



WS 2022 Datacenter: Azure Edition mit Desktop

Azure = GA

Azure Stack HCI = GA



Hotpatching for Azure Arc

Support for Windows Server 2025 (Standard and Enterprise ist angekündigt)

Niedrigere Server OS – unbekannt

Wird in der Preview kommen

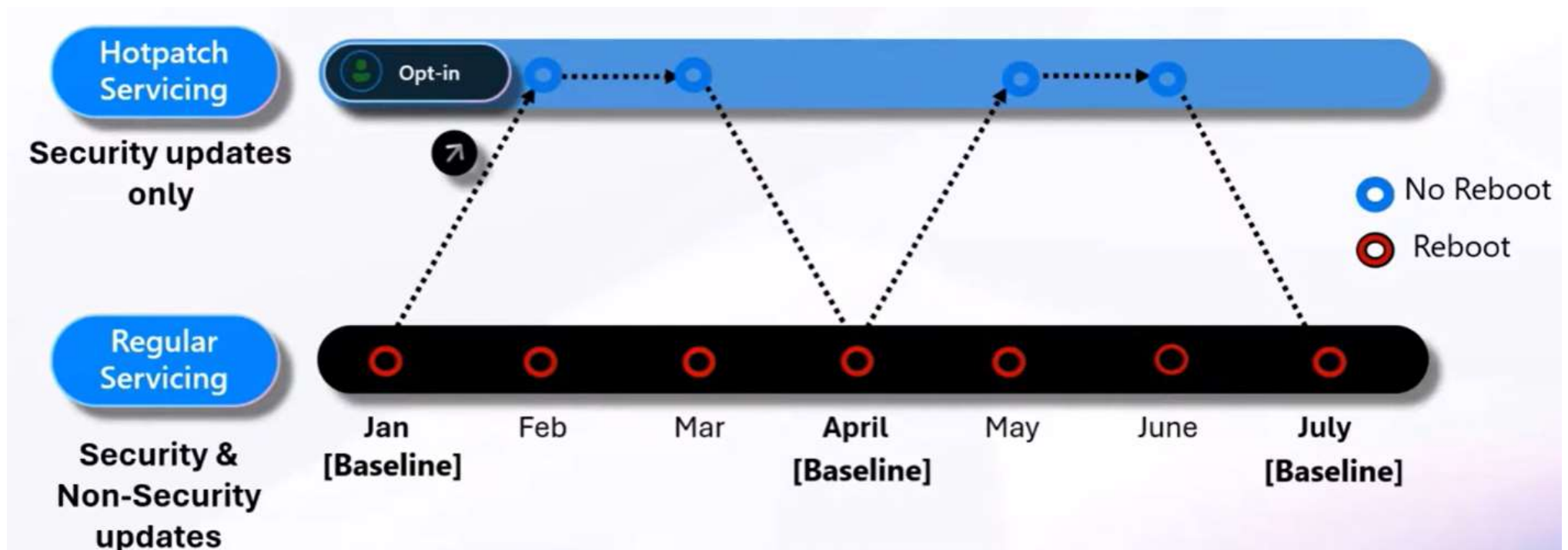
[Hotpatch für Windows Server: Azure Edition | Microsoft Learn](#)

[Hotpatching: Improving server security and productivity | Windows Server Summit 2024](#)





Hotpatching





Best Practices eigene Zeitpläne



Erfordert: Customer Managed Schedules

Select filter by

Resource groups

No items selected

Resource types

All items selected

Locations

No items selected

OS types

All items selected

Tags

No tags selected



Zeitpläne erstellen für Dynamic Scopes



Dynamic Scopes filtern auf
Basis verschiedener Kriterien

Best Practices: Resource Type,
Location und Tags



Wissenswertes



Aktivierung automatischer VM-Gastupdates auf einer VM kann > 3h dauern



Bewertung und Installation außerhalb der Spitzenzeit



Patches werden außerhalb der Spitzenzeit innerhalb des Wartungsfensters installiert

Betrifft auch kritische Updates



Side Note



Azure Update Manager

Microsoft

Refresh | Check for updates | One-time update | Schedule updates | Settings | Feedback

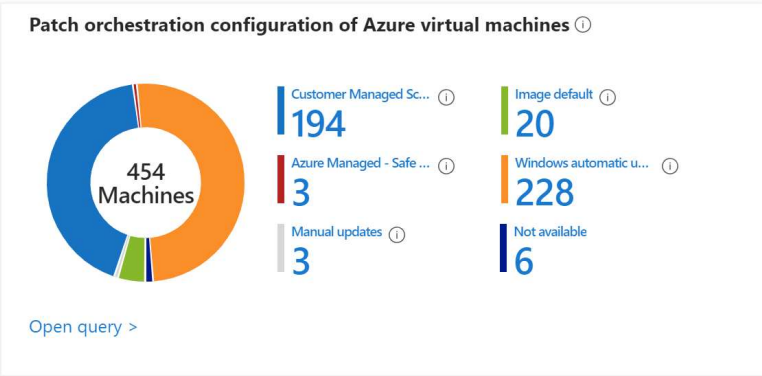
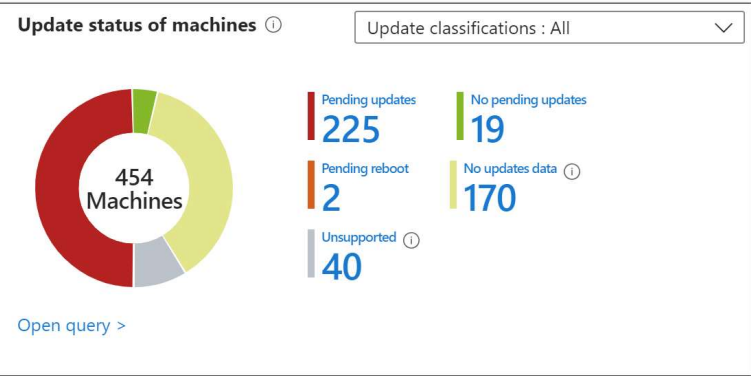
151 out of 454 machine(s) don't have update data. Enable periodic assessment using Azure Policy or Update settings to regularly check for updates. [Enable now](#) →

On 31 August 2024, both Automation Update Management and the Log Analytics agent it uses will be retired. Migrate to Azure Update Manager before that. Refer to guidance on migrating to Azure Update Manager [here](#). [Migrate Now](#). →

Subscription : 59 selected | Resource group : All | Resource type : All | Workloads : All | Location : All | OS : All | Tags : All

Total machines | Azure virtual machines | Arc enabled machines

454 | 454 | 0



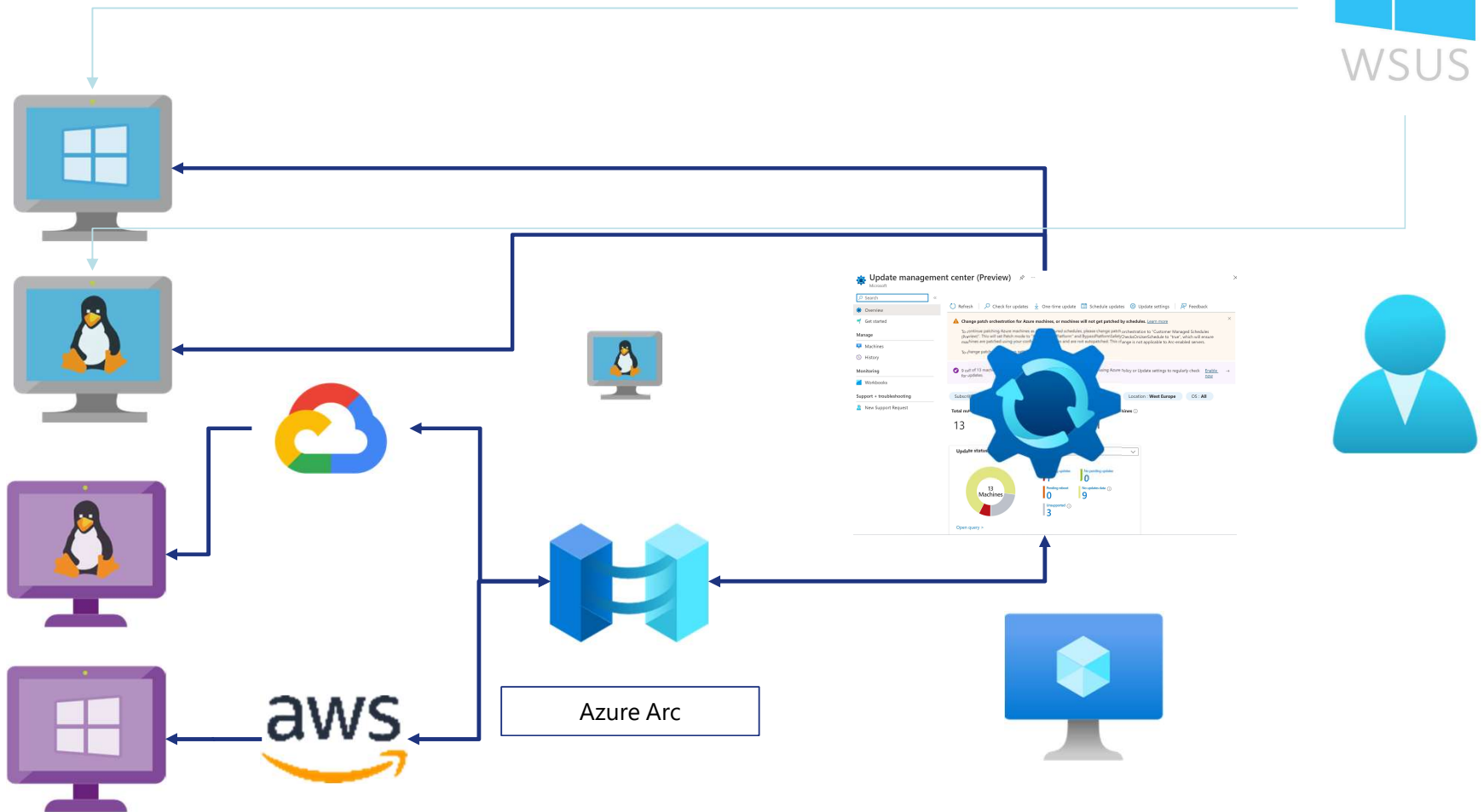
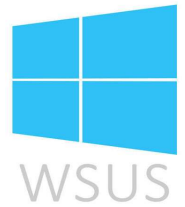
Update installation status | Last 30 Days

Total installation runs | Failed | Completed with warnings | Installation runs by operation type










UMA und WSUS





Preisübersicht

	Service	Price
	Azure	Free
	Extended Security Updates (ESUs) via Arc	Free
	Defender for Server P2 via Arc	Free
	Azure Stack HCI clusters	Free
	Azure Arc	5\$ (4,62€)
	Other enabled Defender Plans via Arc	0,16\$ per Day (5\$ per Month)



Zusammenfassung

- Da MMA abgekündigt ist, muss mit der Evaluierung von UMA begonnen werden 😊
- Migrationstool von Automation Update zu UMA nun vorhanden 😊
- Dies gilt für Azure und für Hybride Umgebungen ;)
- Integration in Azure Arc war dringend erforderlich 😊
- Support für Windows Clients aktuell unsicher 😐
- Installations Force Parameter nicht vorhanden 😞



Links

- [Automatic VM Guest Patching for Azure VMs](#)
- [What's new in Azure Update Manager](#)
- [The new Azure Update Manager is GA Part 1](#)
- [Guidance to move virtual machines from Automation Update Management to Azure Update Manager](#)
- [Automatic VM Guest Patching for Azure VMs](#)
- [Hotpatch for Windows Server Azure Edition](#)
- [Azure Update Manager support matrix](#)
- [Troubleshoot known issues with UMC \(preview\)](#)



Vielen Dank an unsere Sponsoren!

Platinum



Mainzer
Datenfabrik



Gold



Silber



reinheimer_systemlösungen^e





Bitte gebt uns euer Feedback!

- Feedback geben und Geschenk mitnehmen

■ Vielen Dank!

<https://www.reimling.eu>



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



@GregorReimling

