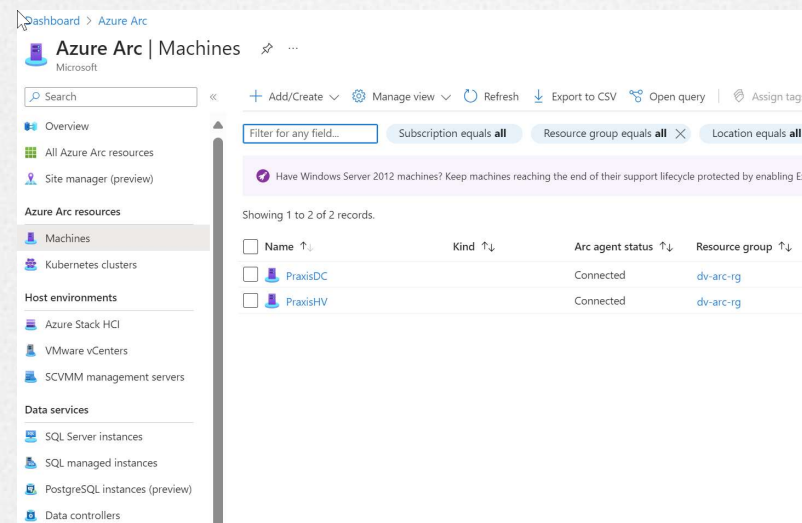


Verwalten und sichern der Hybrid Cloud mit Azure Arc



Gregor Reimling – Cloud (Security) Architect

www.reimling.eu | [@GregorReimling](https://twitter.com/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

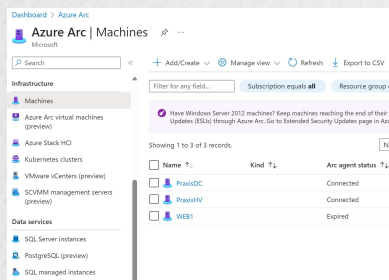
Save the date!
Thu, September 5th, 2024

Community Event by

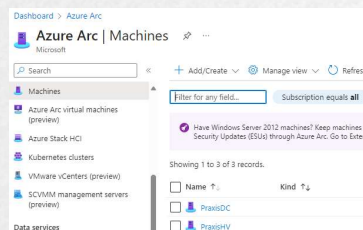


www.identitysummit.cloud

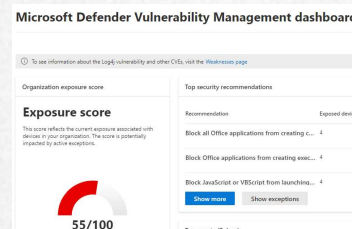
Agenda



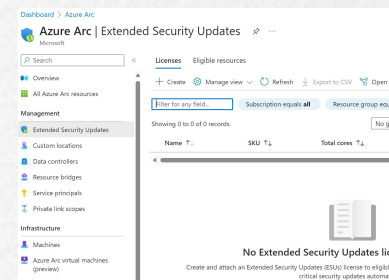
Overview about
Azure Arc



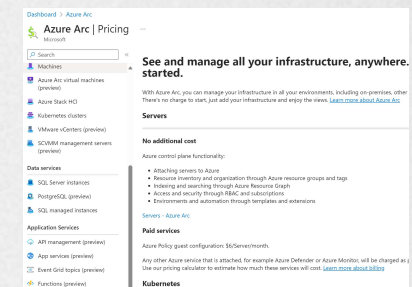
Server
Management



Azure Automachine
Machine Configuration

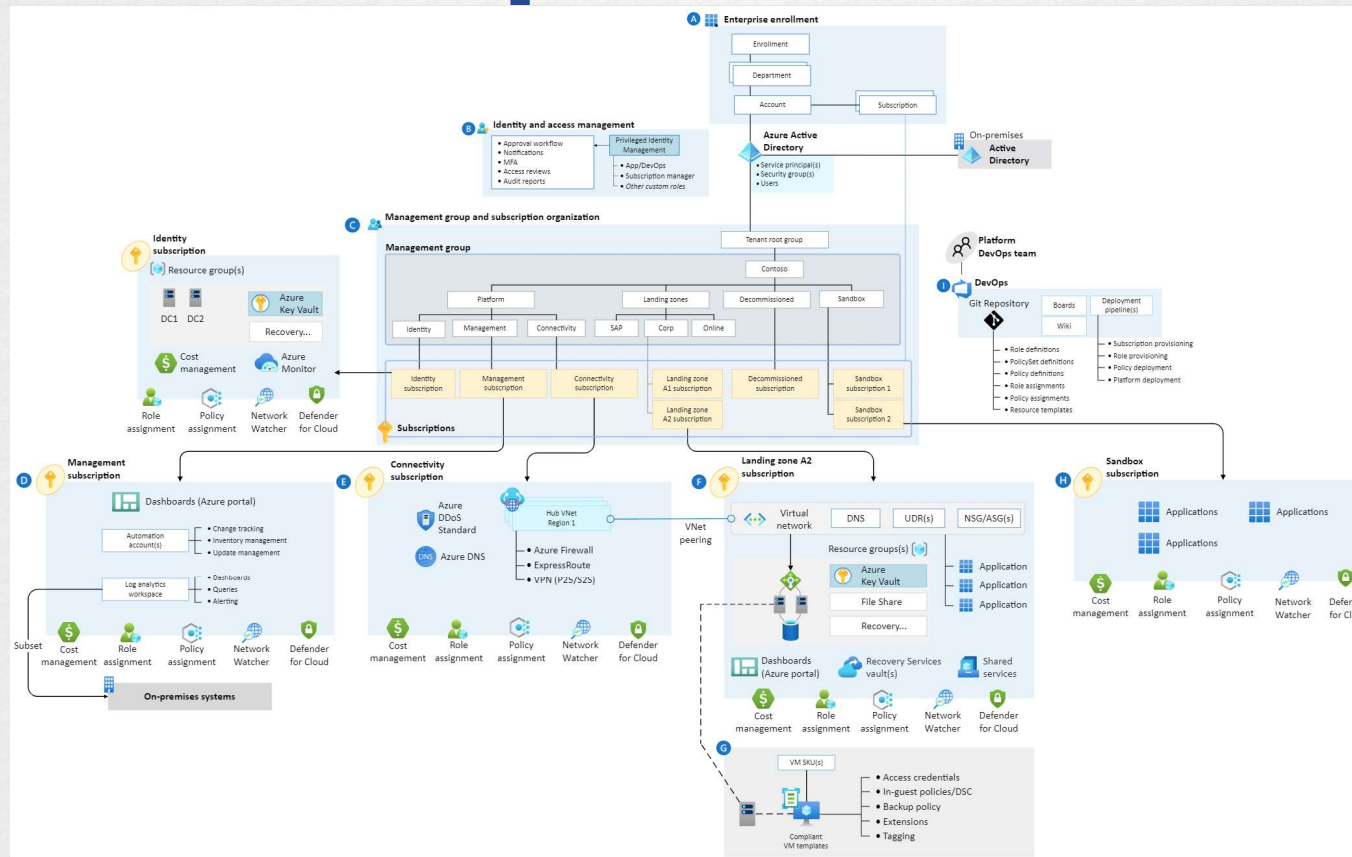


Update
Management Center

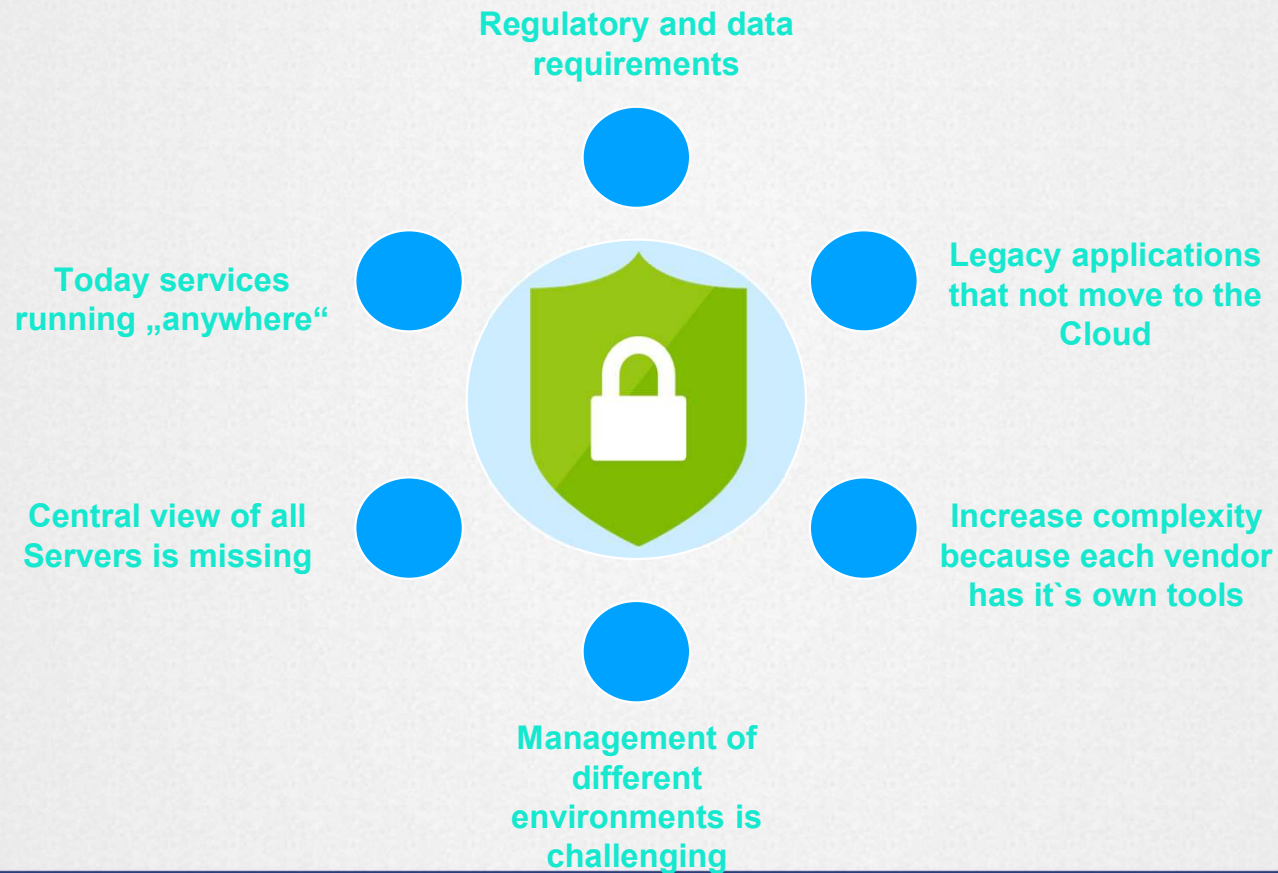


Defender for
Server

Enterprise Scale



Reasons for Hybrid Infrastructures





Unified operations, management,
compliance, security and governance



Azure resources



Azure Arc-enabled infrastructure resources
(Servers, SQL servers, Kubernetes)



Azure Arc-enabled services resources
(Data services, App services, Machine Learning services)



Azure Resource
Manager



Azure Arc

Azure Arc-enabled
infrastructure onboarding

Azure Arc-enabled
services deployment

Azure Arc-enabled
infrastructure onboarding

On-premises IT
infrastructure resources



On-premises Arc-enabled services
(Data services, App services, Machine Learning services)



Azure Stack HCI vmware

Multicloud Arc-enabled services
(Data services, App services, Machine Learning services)



aws Amazon Web Services Google Cloud Platform

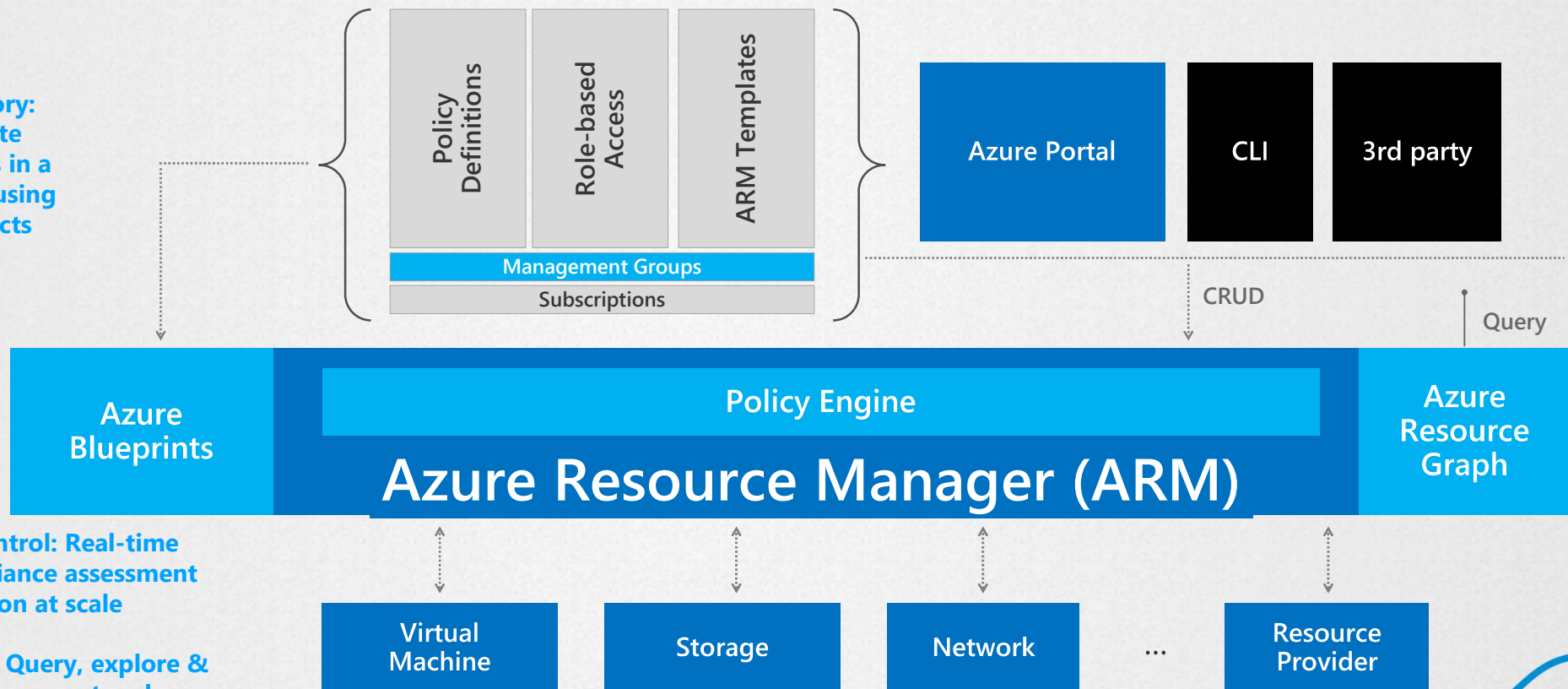
Multicloud IT
infrastructure resources



Azure Governance Architecture

providing control over the cloud environment, without sacrificing developer agility

1. Environment Factory:
Deploy and update
cloud environments in a
repeatable manner using
composable artifacts



2. Policy-based Control: Real-time
enforcement, compliance assessment
and remediation at scale

3. Resource Visibility: Query, explore &
analyze cloud resources at scale

Supported Environments and OS



Environments

- VMware (including Azure VMware)
- Azure Stack HCI
- GCP, AWS, etc.



Windows

- Windows Server 2008 R2 SP1 and higher (including Core)
- Windows IoT Enterprise



Linux

- Ubuntu 16.04, 18.04, 20.04 and 22.04
- Debian 10 and 11
- CentOS Linux 7 and 8
- Rocky Linux 8
- SLES 12 and 15
- RHEL 7 and 8
- Amazon Linux 2
- Oracle Linux 7 and 8

Prerequisites

NET Framework 4.6

Windows PowerShell 4 (included in WS2012R2 and higher)

Azure RBAC

- **Onboarding: Azure Connected Machine Onboarding**
- **Read, Modify, Delete: Azure Connected Machine Ressource Admin**

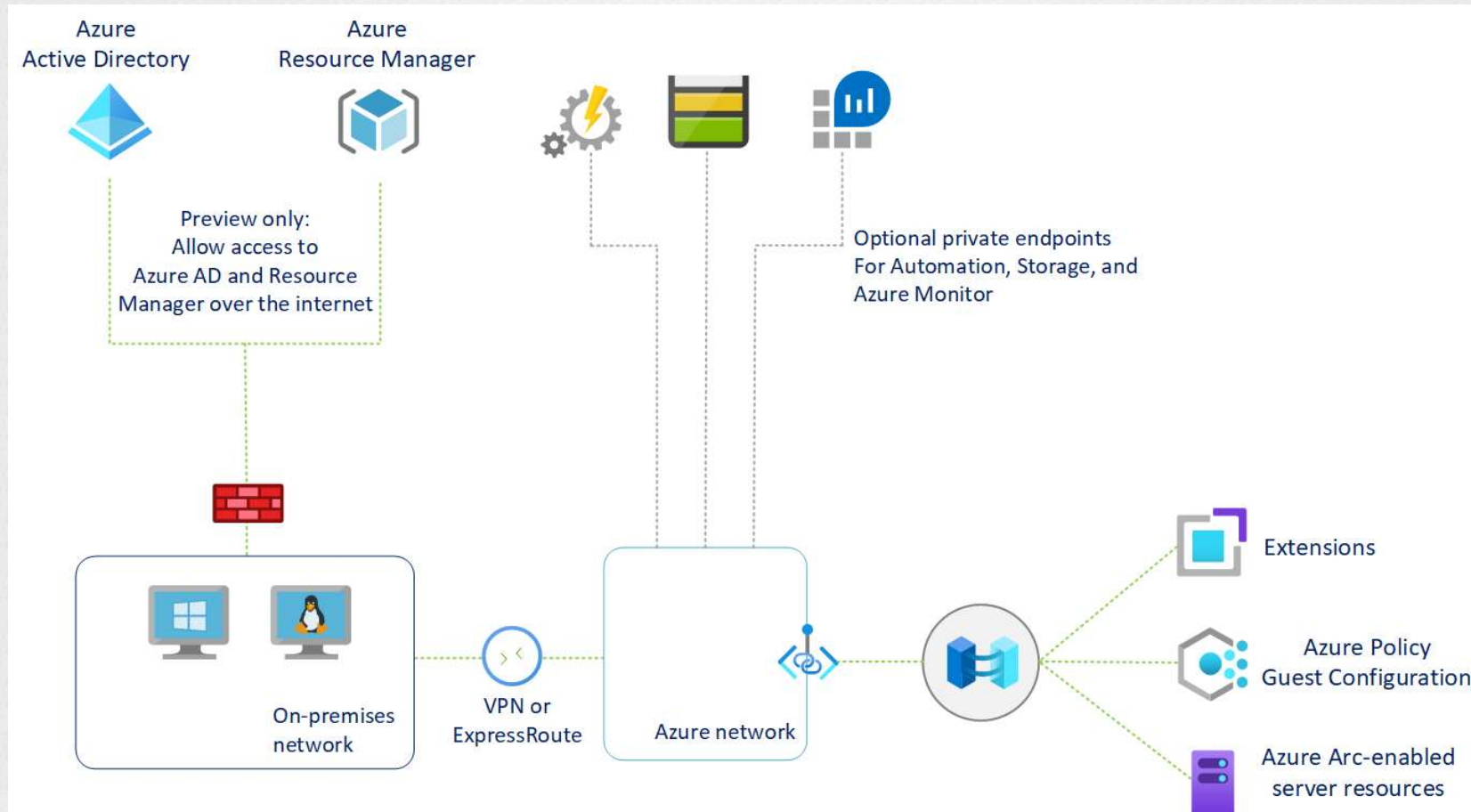
Resource Providers

- **Microsoft.HybridCompute**
- **Microsoft.GuestConfiguration**
- **Microsoft.HybridConnectivity**

Outbound via TCP 443 (Proxy server is supported)

Private Link support

Private Link



Use Azure Private Link to securely connect servers to Azure Arc - Azure Arc | Microsoft Learn



Connecting VMs

```
PS C:\Users\Administrator> try {
    $env:SUBSCRIPTION_ID = "009c17ca--4905999fba2d";
    $env:RESOURCE_GROUP = "arc_rg";
    $env:TENANT_ID = "e4f80c4f--3141bca1ced3";
    $env:LOCATION = "westeurope";
    $env:AUTH_TYPE = "token";
    $env:CORRELATION_ID = "95256887-01a2-4c82-948e-e457830cda97";
    $env:CLOUD = "AzureCloud";
    [Net.ServicePointManager]::SecurityProtocol = [Net.ServicePointManager]::SecurityProtocol -bor 3072;
    # Download the installation package
    Invoke-WebRequest -UseBasicParsing -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile "$env:TEMP\install_windows_azcmagent.ps1";
    # Install the hybrid agent
    & "$env:TEMP\install_windows_azcmagent.ps1";
    if ($LASTEXITCODE -ne 0) { exit 1; }
    # Run connect command
    & "$env:ProgramW6432\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group "$env:RESOURCE_GROUP" --tenant-id "$env:TENANT_ID" --location "$env:LOCATION" --subscription-id
"$env:SUBSCRIPTION_ID" --cloud "$env:CLOUD" --tags "Datacenter=Ohligs,City=Solingen,StateOrDistrict=NRW,CountryOrRegion=Germany,Service=Arc,Environment=Prod" --correlation-id
"$env:CORRELATION_ID";}
catch {$logBody =
@{subscriptionId="$env:SUBSCRIPTION_ID";resourceGroup="$env:RESOURCE_GROUP";tenantId="$env:TENANT_ID";location="$env:LOCATION";correlationId="$env:CORRELATION_ID";authType="$env:AUTH_TYPE";me
ssageType=$_.FullyQualifiedErrorId;message="$_";};
    Invoke-WebRequest -UseBasicParsing -Uri "https://gb1.his.arc.azure.com/log" -Method "PUT" -Body ($logBody | ConvertTo-Json) | out-null;
    Write-Host -ForegroundColor red $_.Exception;}
VERBOSE: Installing Azure Connected Machine Agent
VERBOSE: .NET Framework version: 4.6.1586
VERBOSE: Downloading agent package from https://aka.ms/AzureConnectedMachineAgent to C:\Users\ADMINI~1\AppData\Local\Temp\AzureConnectedMachineAgent.msi
VERBOSE: Installing agent package

Installation of azcmagent completed successfully
time="2022-11-11T22:16:46+01:00" level=info msg="The computer is connected in Azure. This may take a few minutes."
time="2022-11-11T22:17:59+01:00" level=info msg="Log in using the pop-up browser to authenticate yourself."
```

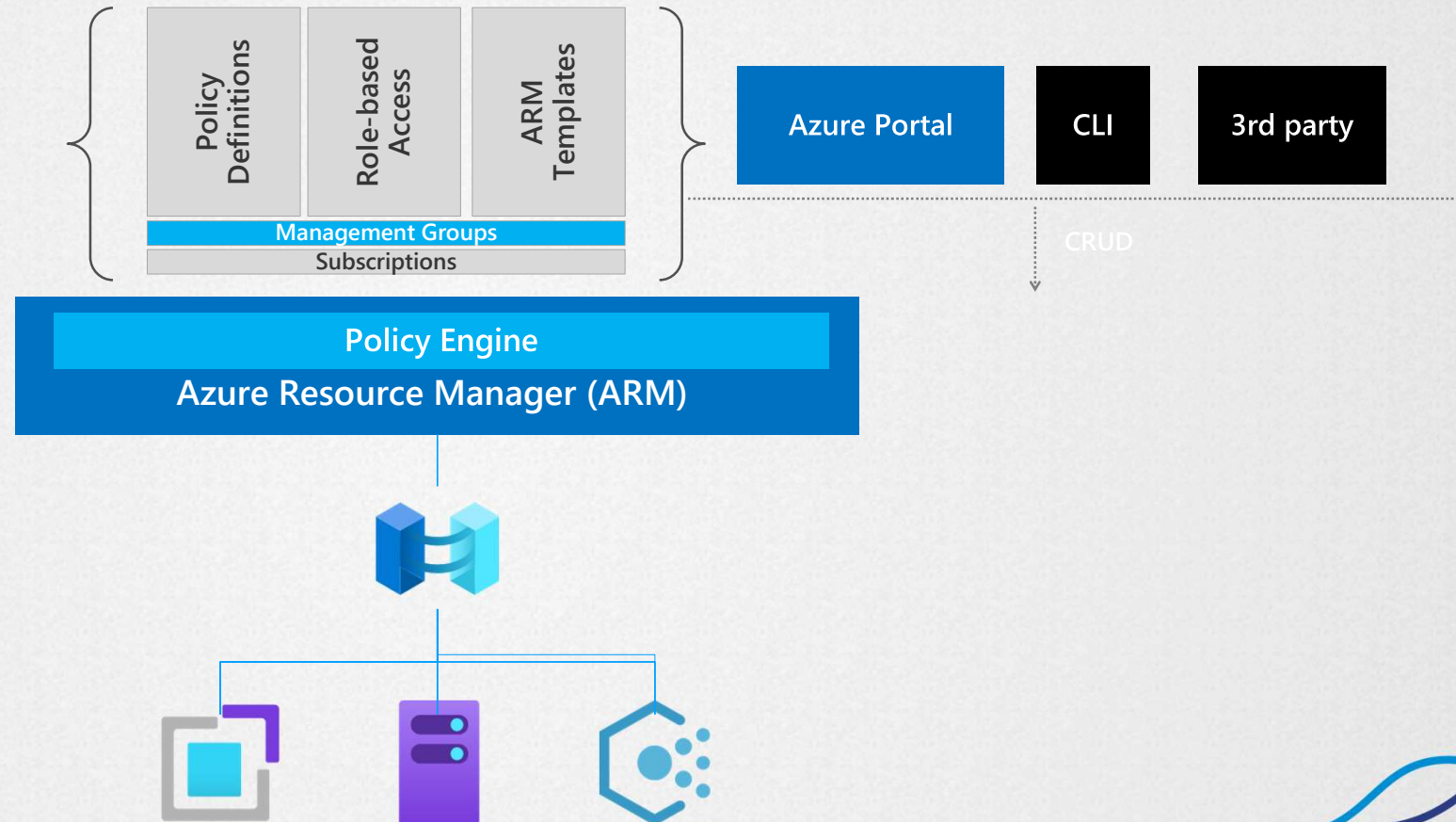
Azure Architecture

providing control over the cloud environment, without sacrificing developer agility

1. Environment Factory:
Deploy and update
cloud environments in a
repeatable manner using
composable artifacts

2. Policy-based Control: Real-time
enforcement, compliance assessment
and remediation at scale

3. Resource Visibility: Query, explore &
analyze cloud resources at scale



Connected Machine Agent



Azcmagent tool configure the Azure Connected Machine agent



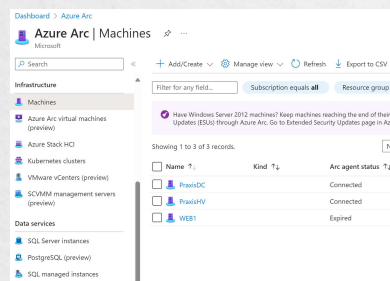
Updates coming via Windows Update (configure is mandatory)



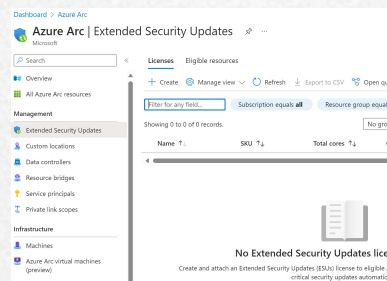
Server Renaming does not rename the Azure resource name (because is immutable)

Delete and re-create is needed for Server renaming
Remove any VM-extension
Use azcmagent to disconnect

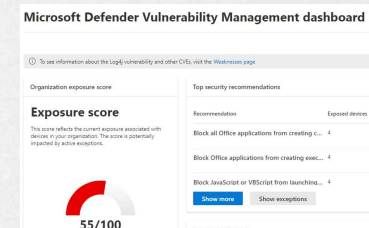
Demo Azure Arc



Overview about
Azure Arc



Server
Management



Azure Automate
Machine Configuration



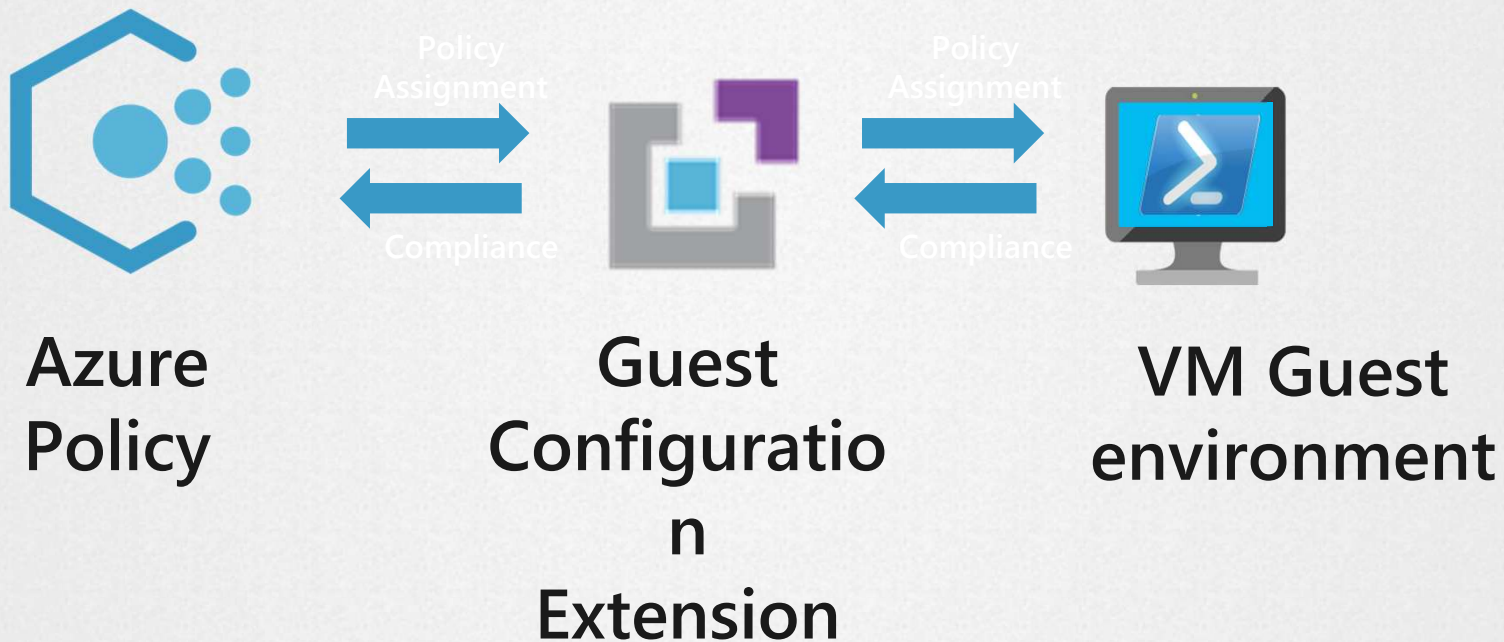
Azure Policy Guest Configuration

Renamed to

Azure Automanage Machine Configuration

Coming soon: guest configuration renames to machine
configuration - Microsoft Community Hub

How VM guest policy works



Guest Assignments





[Dashboard](#) >

Guest Assignments

Build Clouds

[+](#) Create [⚙️](#) Manage view [↺](#) [🔄](#) Refresh [↓](#) Export to CSV [🔗](#) Open query | [🏷️](#) Assign tags [🗑️](#) DeleteSubscription equals **all**Resource group equals **all** [×](#)Location equals **all** [×](#)[+](#) Add filter

No grouping

<input type="checkbox"/> Name ↑↓	Machine ↑↓	Type ↑↓	Status ↑↓	Resource
<input type="checkbox"/>  AuditSecureProtocol (W...	WEB1	Microsoft.HybridCompute	NonCompliant	arc_rg
<input type="checkbox"/>  AzureWindowsBaseline ...	WEB1	Microsoft.HybridCompute	NonCompliant	arc_rg
<input type="checkbox"/>  WindowsDefenderExplo...	WEB1	Microsoft.HybridCompute	Compliant	arc_rg
<input type="checkbox"/>  WindowsLogAnalyticsA...	WEB1	Microsoft.HybridCompute	Compliant	arc_rg

Azure Automanage Machine

Guest configuration extend
Azure Policy to Server

Perform audit and
configuration inside Server

Need Resource Provider
Microsoft.GuestConfiguration

Checks for changes every 5
minutes

Installs security baselines for
Windows and Linux

Configured in audit-only
mode

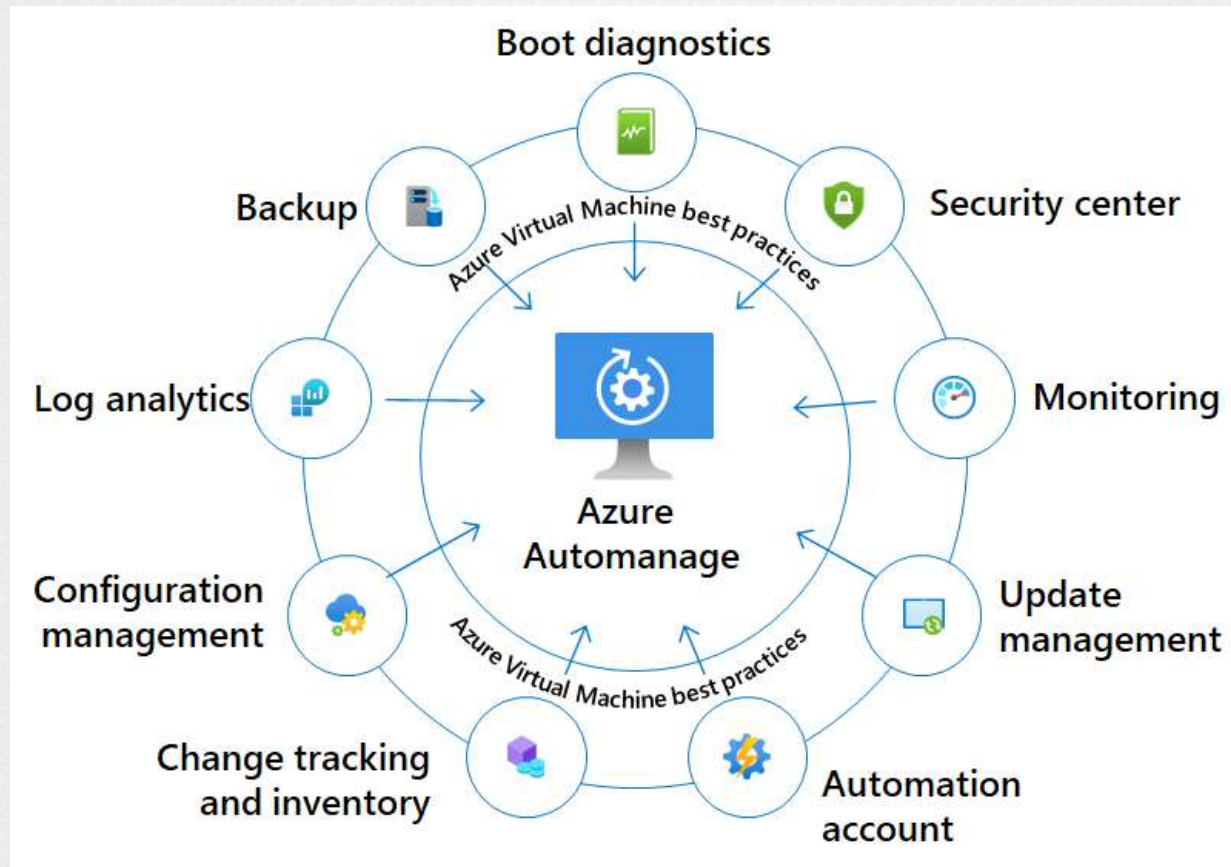
Non-compliant devices are
displayed but not reset

Reset possible through
advanced configuration



Azure Automanage

Azure Automanage – Your VM Service provider





Azure Automanage



Automates best practices configuration for all VMs



Access to all VMs via Azure Arc (Multicloud enabled)



Fully customizable via user-defined profiles



For Windows and Linux VMs



Available free of charge





Azure Update Manager



Warum Azure Update Manager?



Log Analytics
Workspace



Automation Account

- Current update management is based on Log Analytics Agent (MMA)
- MMA is deprecated as of 31.08.2024

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. ...

Why Azure Update Center v2?



V2 is complete new

No dependencies to MMA or Azure Automation



Fully support for Azure Policy



Integration in Enterprise Scale



Server visibility in Azure guaranteed



Update Manager will be charged by 5\$ per Server/month beginning of January (only for Arc Machines)



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
- 

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](#)

Preisübersicht

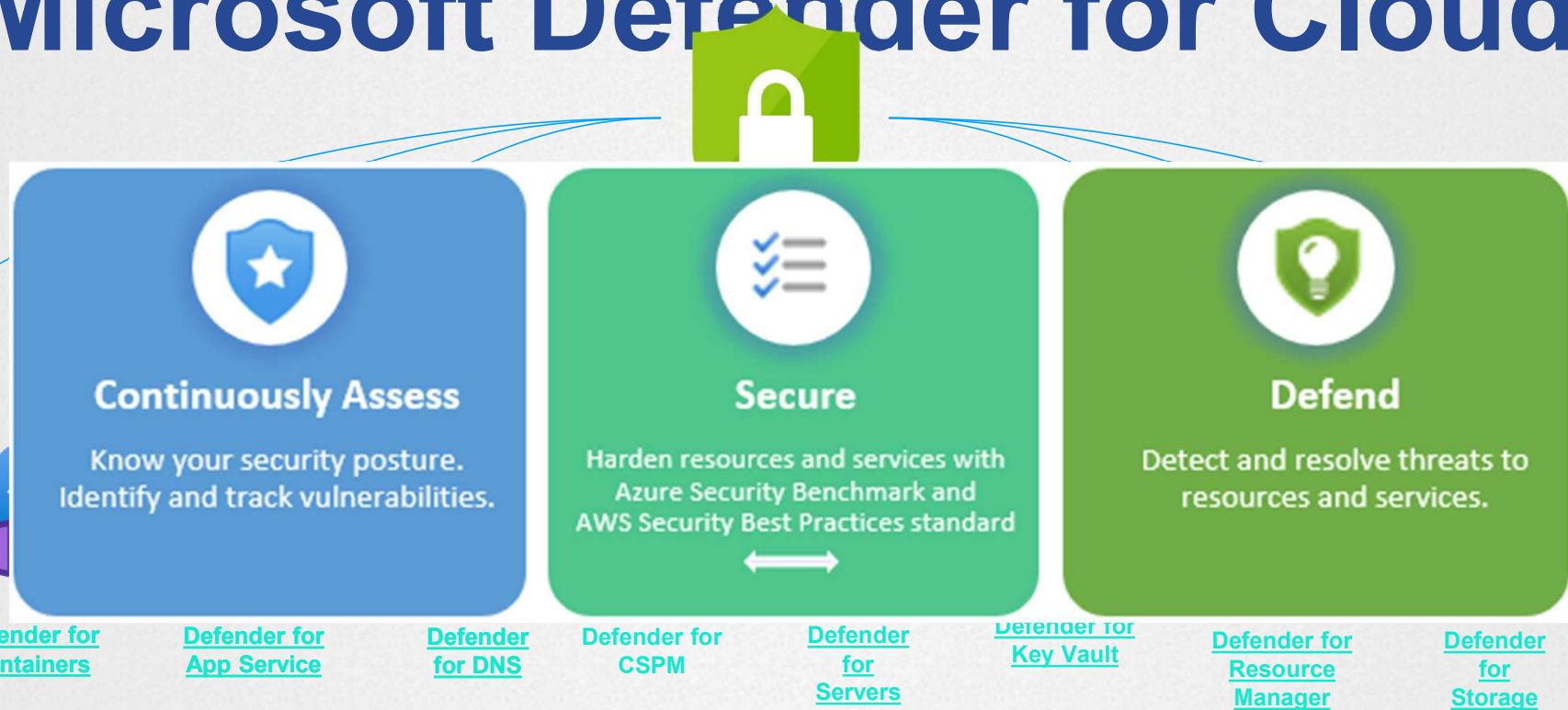
Service	Price
Azure	Free
Extended Security Updates (ESUs) via Arc	Free
Defender for Server P2 via Arc	Free
Azure Stack HCI clusters	Free
Azure Arc	5\$ (4,62€)
Other enabled Defender Plans via Arc	0,16\$ per Day (5\$ per Month)





Defender for Cloud

Microsoft Defender for Cloud



Activation of Defender for Servers

- Defender for Servers plan 1 must be enabled on subscription level
- Defender for Servers plan 2 must be enabled on subscription and **Workspace** level
- Mixing of the plans only possible with different subscription
- License cost for plan 2 is incurred for each machine connected to the Workspace where plan 2 is activated



Auto-provisioning configuration

Auto-provisioning configuration

Log analytics agent

Agent type

☐ Log Analytics Agent (Default)
Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis

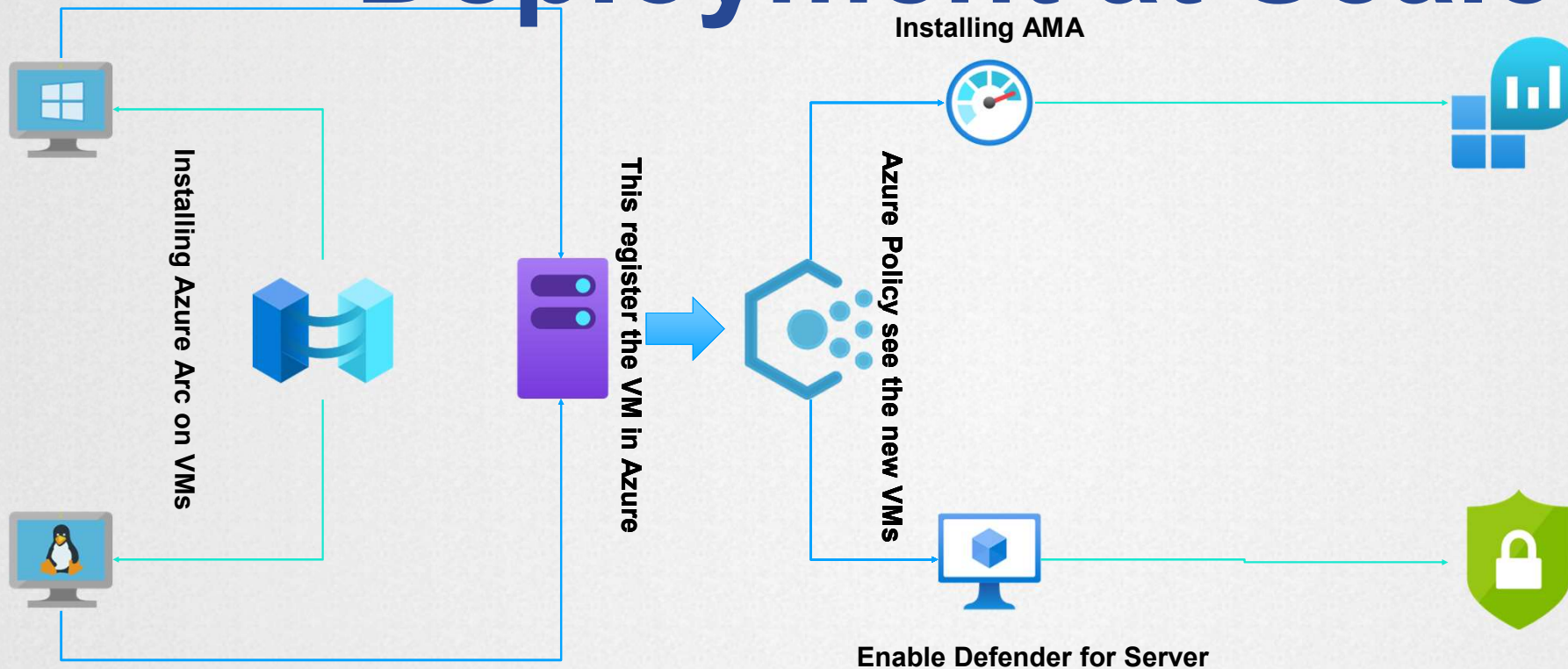
☒ Azure Monitor Agent (Preview)
Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis

- **Switch from MMA to AMA does not uninstall the MMA-agent**
- **Duplicate agents results in doubled events or recommendations and appear twice in Defender**
 - **Monitoring workbook – AMA migration tracker workbook**

Defender for Server

	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

Deployment at Scale

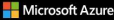


- Deploy Microsoft Defender for Endpoint agent on Windows virtual machines
- Deploy Microsoft Defender for Endpoint agent on Windows Azure Arc machines
- Deploy Microsoft Defender for Endpoint agent on Linux hybrid machines
- Deploy Microsoft Defender for Endpoint agent on Linux virtual machines



How To Start



 Arc Jumpstart Getting started ▾ Community ▾ Resources ▾ Adaptive cloud Search 🔍 Release notes 📄 GitHub 🐙

Jumpstart

Scenarios

Want to explore multiple environments and see the full breadth of Jumpstart? Get automated zero-to-hero scenarios for Arc-enabled servers, Arc-enabled Kubernetes, and more.

[Browse scenarios >](#)

Jumpstart

Agora

Explore cloud-to-edge scenarios designed for specific industry needs. Get a full-stack deployment with dedicated guides to walk you through the process—plus the end-to-end user experience.

[Browse industry solutions >](#)

Jumpstart

ArcBox

Get a complete Azure Arc environment in just one click. Explore all the major capabilities of Azure Arc in a virtual, hybrid sandbox—all you need is an Azure subscription to get started.

[View ArcBox capabilities >](#)

Jumpstart

HCIBox

Want to try Azure Stack HCI? This is the tool for you. Get a dedicated Azure Stack HCI sandbox in one click—all you need is an Azure subscription to get started.

[View HCIBox capabilities >](#)

Jumpstart

Drops

No matter how big or small the contribution, create a Drops to help others explore, discover, and leverage development artifacts. You can also find quick deployment guides, useful code snippets, and more.

[Browse development artifacts >](#)

Overview | Azure Arc Jumpstart

How to start

Microsoft Azure Arc Community Monthly Meetup

Overview

Once a month, the various Azure Hybrid Cloud product groups at Microsoft will hold a call to showcase new features, talk through important topics and engage in a Q&A regarding Azure Arc. The foundational goals of the call are highlighted below:

- Provide the Azure Arc community with product updates
- Host a short talk and/or demo on Azure Hybrid Cloud technologies and products technologies
- Collect feedback from the community on issues, blockers, use cases, and questions related to Azure Hybrid Cloud technologies and products

Contributors 3



likamrat Lior Kamrat



microsoftopensource Microsoft Open ...



csand-msft Chris Sanders

Azure Arc Community Monthly Meetup

[GitHub - microsoft/azure_arc_community](https://github.com/microsoft/azure_arc_community): Public repository for hosting the Azure Arc Community content

Summary and Best Practices

Before Start with
Azure Arc think on
Enterprise Scale and
use a separate
Hybrid Subscription

Group Arc resource
in propriate
Resource groups
and use Tags

Track Installation and
Server Status with
Workbooks

Always use AMA
instead of MMA
because of
retirement of MMA

Think on additional
pricing for Azure
Policy in Guest
configuration and
Update Center

Integrate VMs
outside of Azure with
Arc to enable
Defender for Servers
everywhere

Links

- [Introduction to Azure Arc - Training | Microsoft Learn](#)
- [Managing the Azure Arc-enabled servers agent - Azure Arc | Microsoft Learn](#)
- [Overview of the Azure Connected Machine agent - Azure Arc | Microsoft Learn](#)
- [Archive for What's new with Azure Arc-enabled servers agent - Azure Arc | Microsoft Learn](#)
- [GitHub - microsoft/azure_arc_community: Public repository for hosting the Azure Arc Community content](#)
- [Azure Automanage | Microsoft Learn](#)
- [Update management center \(preview\) overview | Microsoft Learn](#)
- [Microsoft Cybersecurity Reference Architectures - Security documentation | Microsoft Learn](#)
- [Join Our Security Community - Microsoft Tech Community](#)



Lior Kamrat

Principal Product Manager -
Azure Arc Platform

[Lior Kamrat | LinkedIn](#)



Thomas Maurer

Senior PM and Chief Evangelist
Azure Hybrid at Microsoft

[Thomas Maurer | LinkedIn](#)

Danke an unsere Sponsoren

PLATINUM SPONSOR

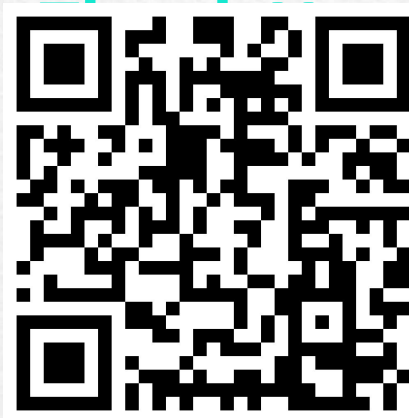


WE LIVE IT



GOLD SPONSOR





Blog

- <https://www.Reimling.eu>

Contact



- @GregorReimling
- Gregor Reimling