

Hybrid- and Multi- Cloud Server Management with Azure Arc

by Gregor Reimling

1

Gregor Reimling

Cloud Consultant @ adesso SE

Cloud and Datacenter, Governance

Azure Infrastructure (Governance, IaaS, Security)

info@reimling.eu

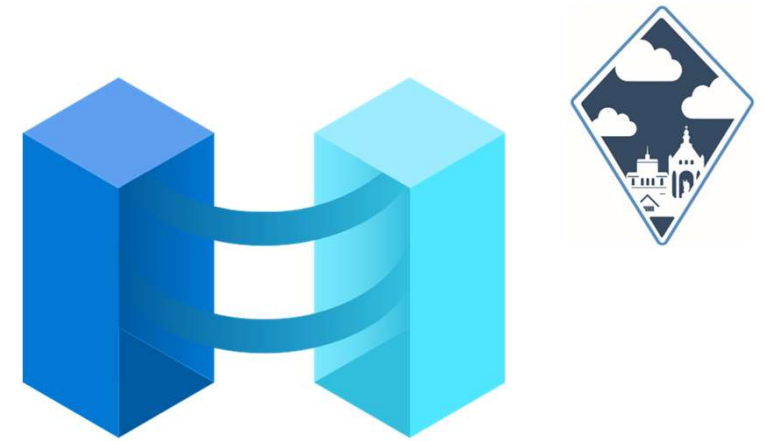
@GregorReimling | @AzureBonn

www.reimling.eu | www.neutralien.com



Agenda

- Overview of Azure Arc
- Connecting
- Arc Machine Agent
- Security
- Automanage
- Update Management (Center)
- Conclusion





Thanks to the Sponsors

Platinum Sponsors



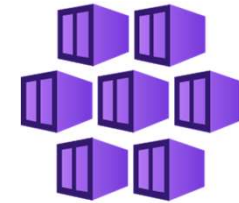
Gold Sponsors



Silver Sponsors



Customer environments





Reasons for Hybrid growing

- Regulatory and data requirements
- Legacy applications that not move to the Cloud
- Increase complexity because each vendor has it`s own tools
- Management of different environments is challenging
- Central view of all Servers is missing
- Today services running „anywhere“

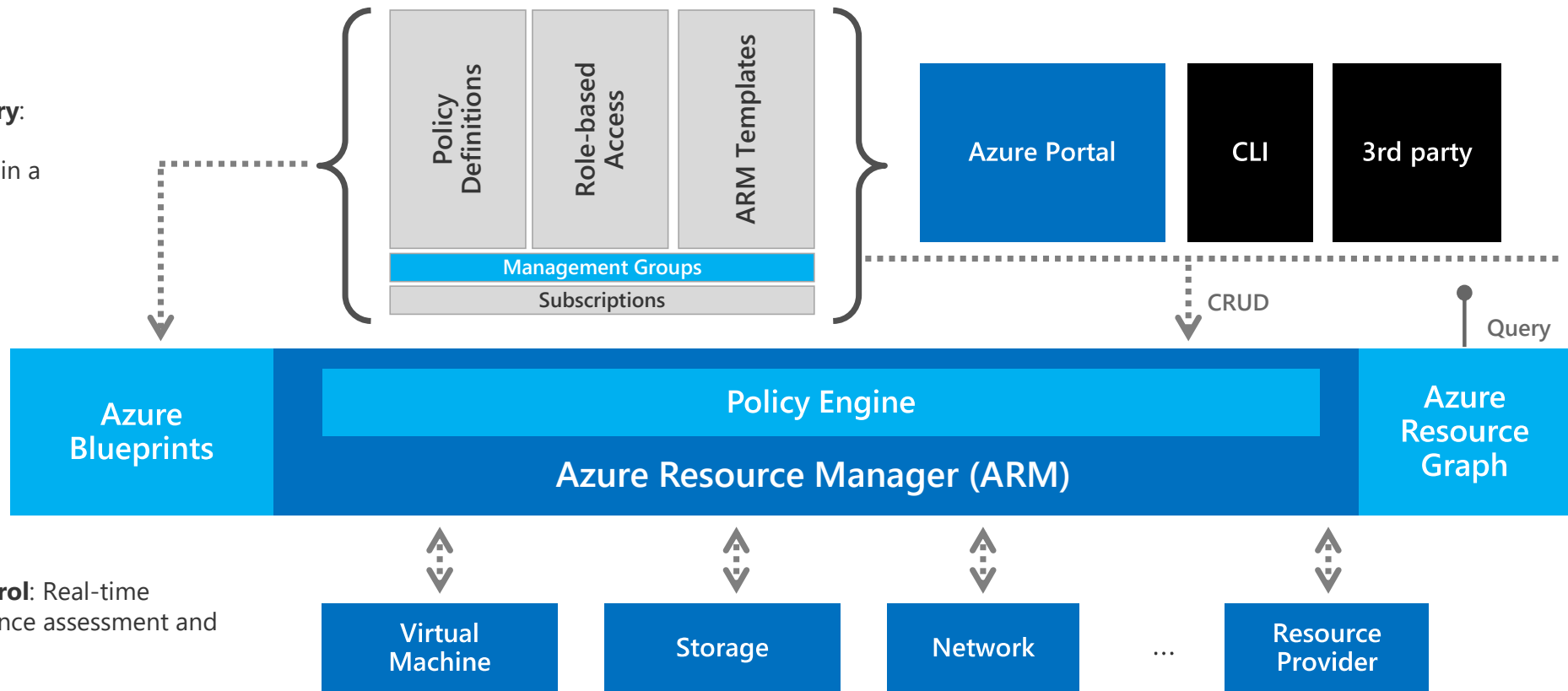
Azure Governance Architecture

providing control over the cloud environment, without sacrificing developer agility



1. Environment Factory:

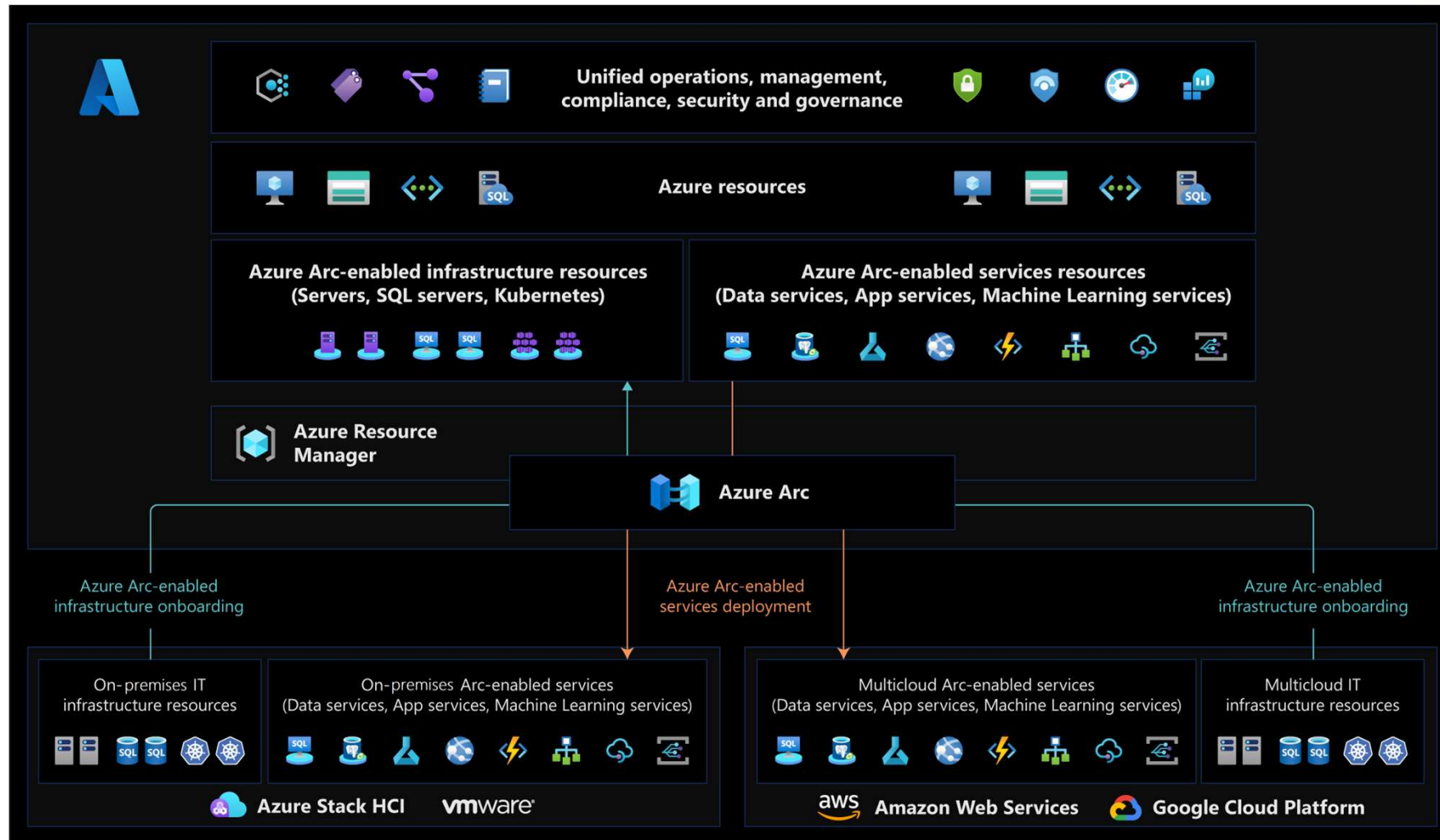
Deploy and update cloud environments in a repeatable manner using composable artifacts



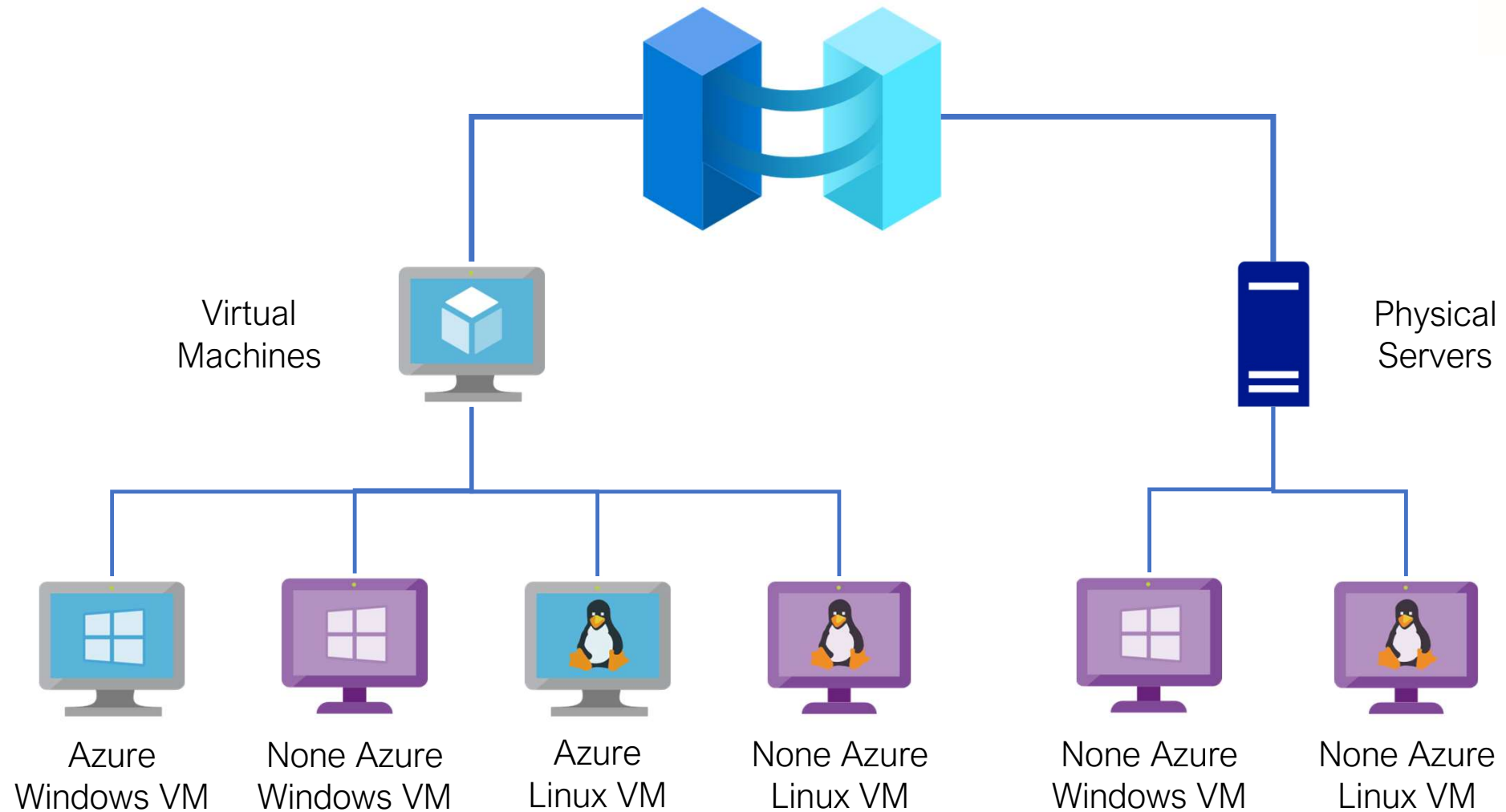
2. Policy-based Control: Real-time enforcement, compliance assessment and remediation at scale

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

Azure Arc



This session





Supported Environments and OS

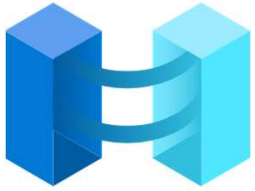
- Environments
 - VMware (including Azure VMware)
 - Azure Stack HCI
 - GCP, AWS, etc.
- Operating Systems
 - Windows Server 2008 R2 SP1 and higher (including Core)
 - Windows IoT Enterprise
 - Ubuntu 16.04, 18.04, 20.04 and 22.04
 - Debian 10 and 11 | CentOS Linux 7 and 8 | Rocky Linux 8
 - SLES 12 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 Resource Admin
- Resource Providers
 - Microsoft.HybridCompute
 - Microsoft.GuestConfiguration
 - Microsoft.HybridConnectivity
- Outbound via TCP 443 (Proxy server is supported)
- Private Link support



Connecting Azure Arc

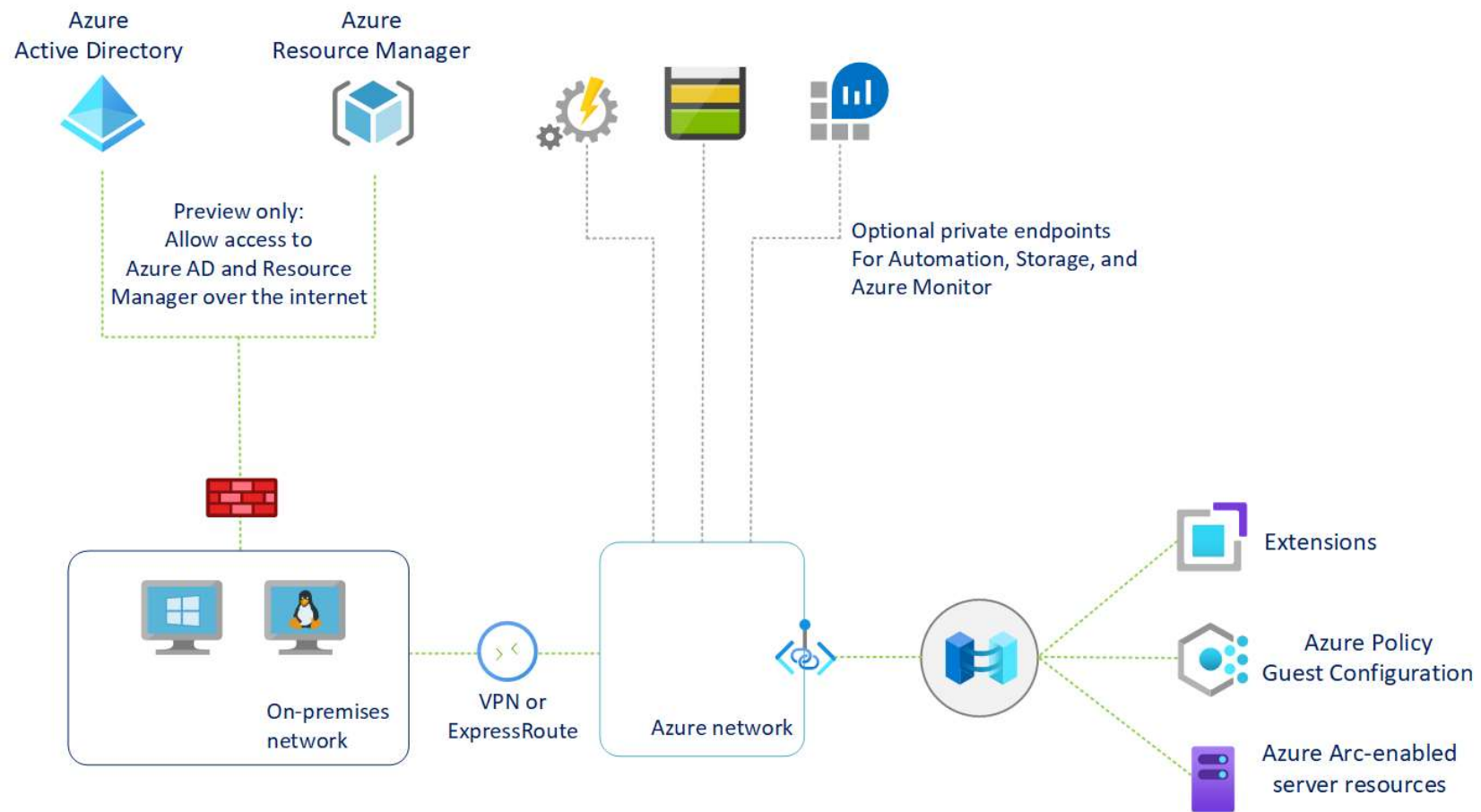
Connecting VMs



```
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- -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="$env:CORREL
ATION_ID";authType="$env:AUTH_TYPE";messageType=$_.FullyQualifiedErrorId;message="$_";};
    Invoke-WebRequest -UseBasicParsing -Uri "https://gbl.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."
```

Private Link



[Use Azure Private Link to securely connect servers to Azure Arc - Azure Arc | Microsoft Learn](#)

Azure Architecture

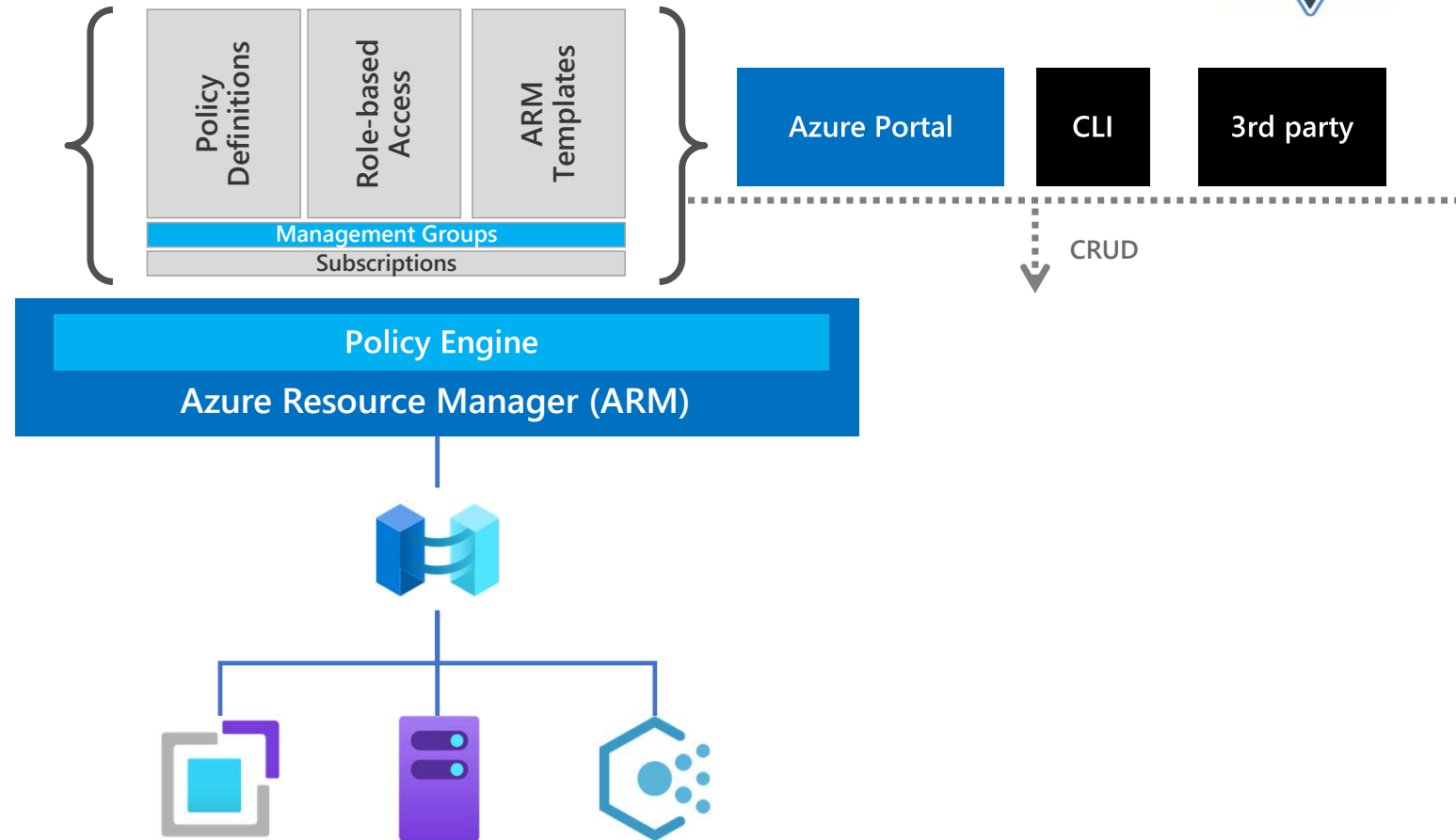
providing control over the cloud environment, without sacrificing developer agility

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

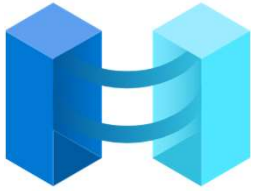
3. Resource Visibility: Query, explore & analyze cloud resources at scale





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



Azure Policy Guest Configuration

Renamed to

Azure Automanage Machine Configuration

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

Azure Policy



- Turn on built-in policies or build custom ones for all resource types
- Real-time policy evaluation and enforcement
- Periodic & on-demand compliance evaluation
- VM In-Guest Policy (**NEW**)

Enforcement & Compliance



- Apply policies to a Management Group with control across your entire organization
- Apply multiple policies and & aggregate policy states with policy initiative
- Exclusion Scope

Apply policies at scale



- Real time remediation
- Remediation on existing resources (**NEW**)

Remediation

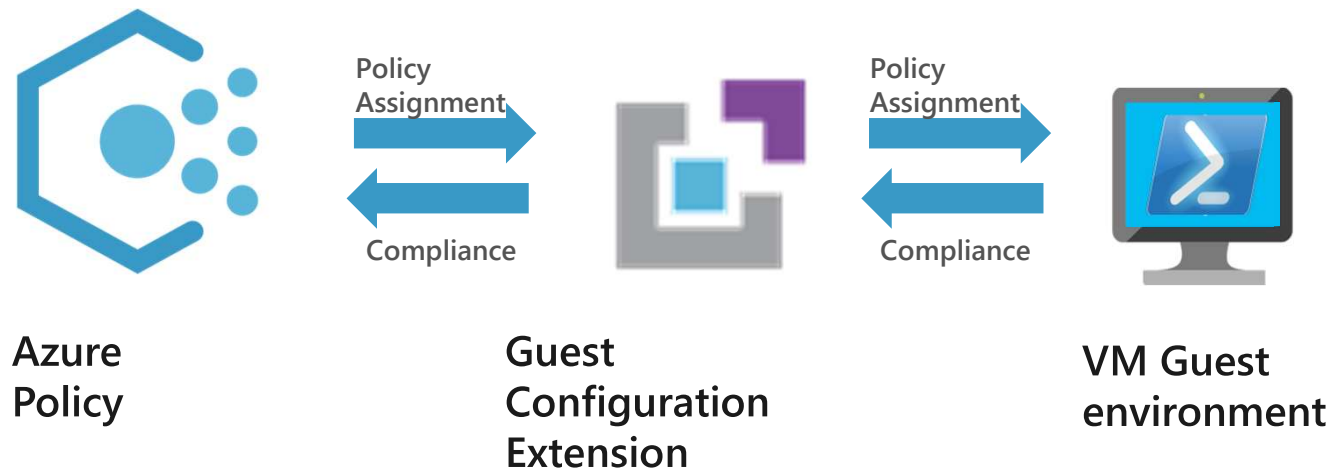


Azure Automanage Machine Configuration



- 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

How VM guest policy works





Dashboard >

Guest Assignments

Build Clouds

[+](#) Create [⚙](#) Manage view [v](#) [↺](#) Refresh [↓](#) Export to CSV [🔗](#) Open query | [🏷](#) Assign tags [🗑](#) Delete

Subscription equals **all**

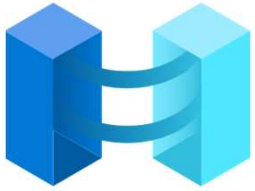
Resource group equals **all** [×](#)

Location equals **all** [×](#)

[+🔍](#) Add filter

No grouping

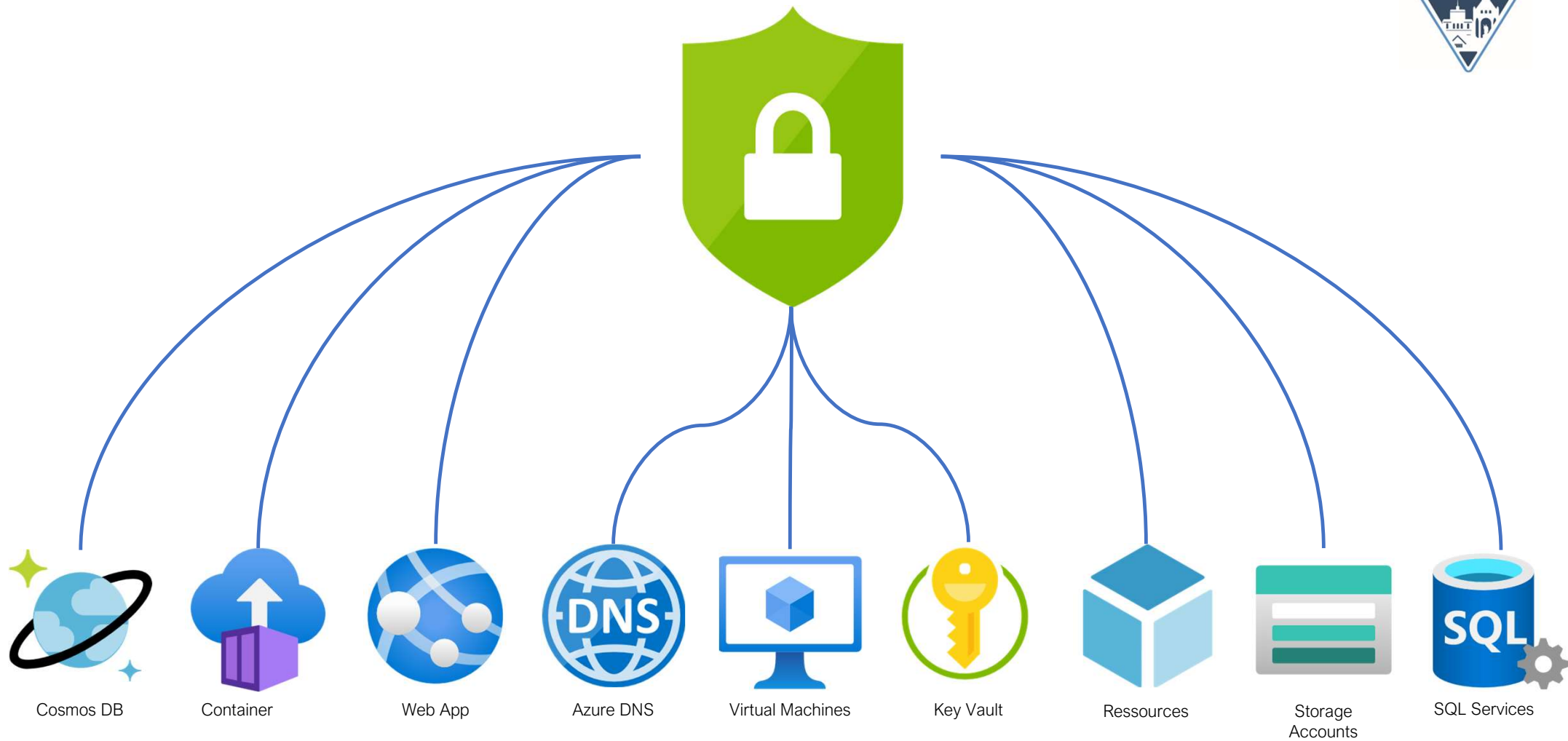
<input type="checkbox"/> Name ↑↓	Machine ↑↓	Type ↑↓	Status ↑↓	Resource
<input type="checkbox"/> AuditSecureProtocol (W...	WEB1	Microsoft.HybridCompute	NonCompliant	arc_rg
<input type="checkbox"/> AzureWindowsBaseline ...	WEB1	Microsoft.HybridCompute	NonCompliant	arc_rg
<input type="checkbox"/> WindowsDefenderExplo...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



Defender for Cloud



Microsoft Defender for Cloud



Microsoft Defender for Cloud



A service to strengthen your security posture



Available in two Tiers – ASC Basic and Azure Defender



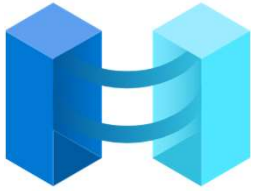
Basic -> Free – Activated by default for all subscriptions



Based on an security score – scope based



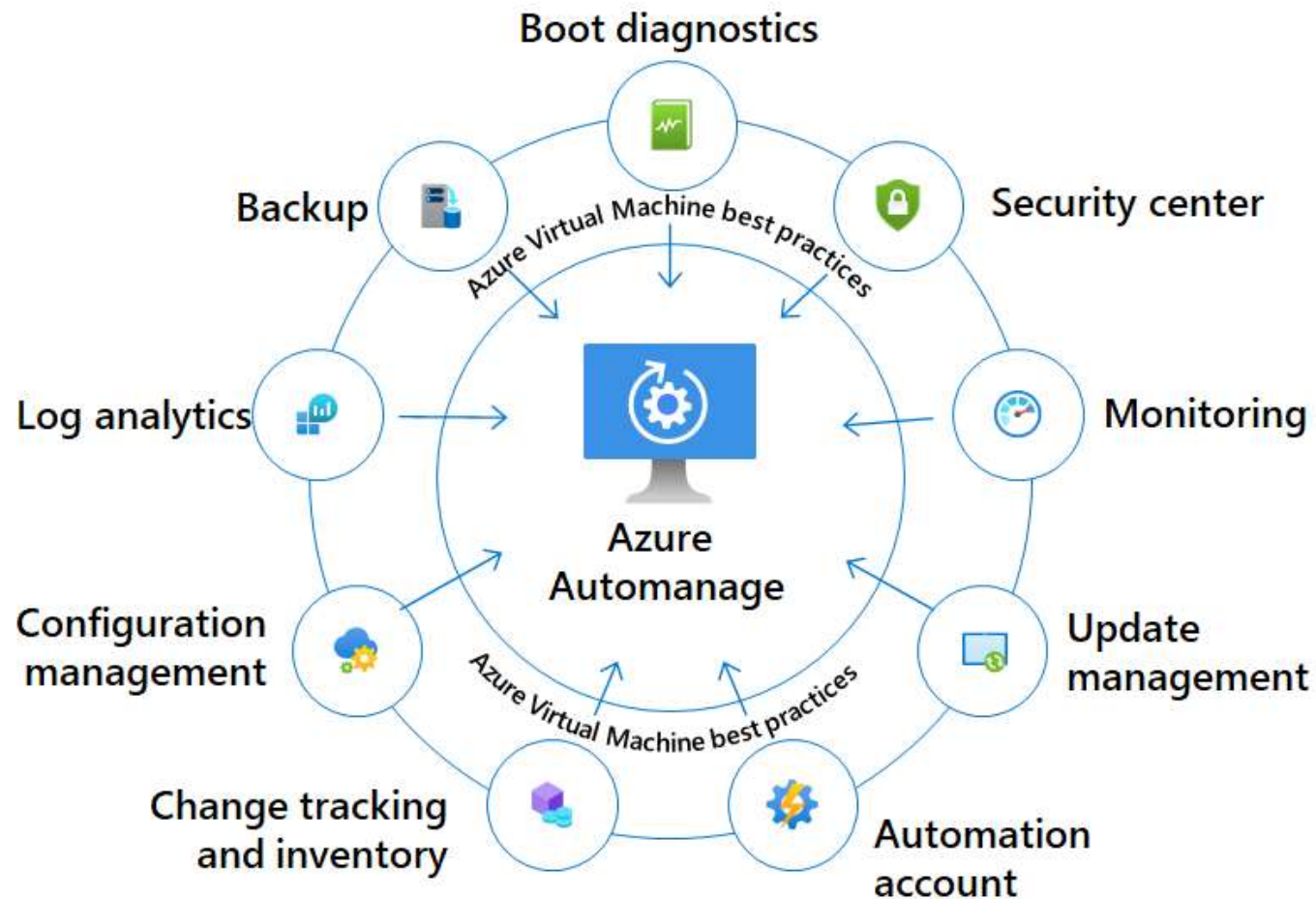
Available for all workloads (Server, Container, SQL, IoT and many more)



Azure Automanage



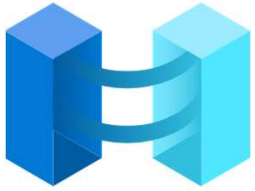
Azure Automanage – Your VM Service provider





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



Update Management Center




[Dashboard](#) >

Update management center (Preview) ...

Microsoft

<<

 Overview

 Getting started

Manage

 Machines

 History

Monitoring

 Workbooks

Support + troubleshooting

 New Support Request

Subscription : **MLGBonn**

Resource group : **All**

Resource type : **All**

Location : **All**

Total machines ⓘ

10

Azure virtual machines ⓘ

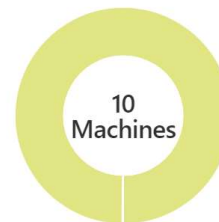
 7

Arc enabled machines ⓘ

 3

Update status of machines ⓘ

Update classifications : All



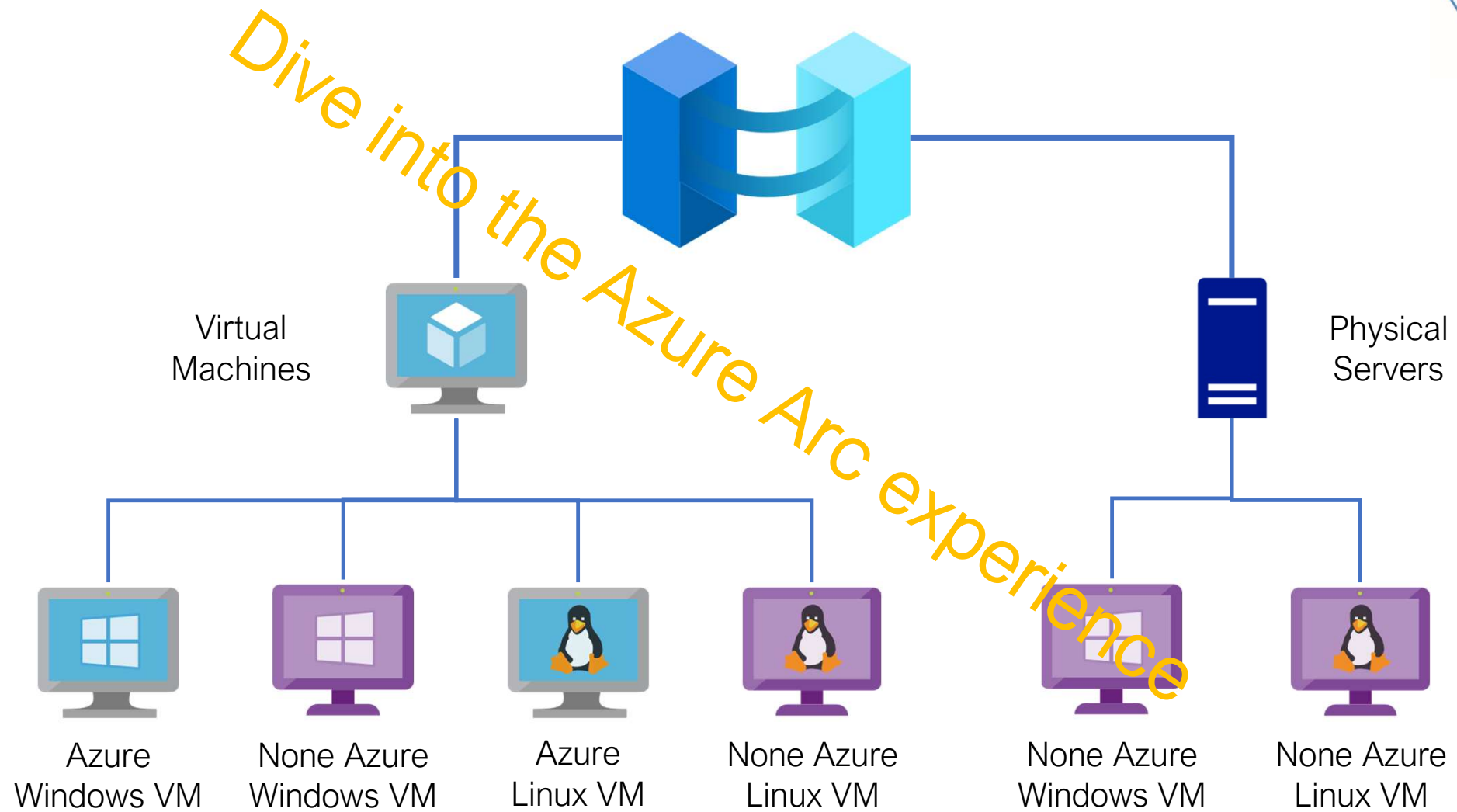
[Open query >](#)

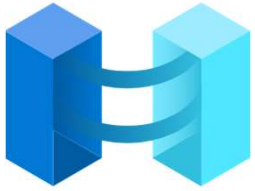
Patch orchestration configuration of Azure virtual machines ⓘ



[Open query >](#)







How To Start



Azure Arc Jumpstart

Overview

- [Jumpstart Scenarios](#)
- [Jumpstart ArcBox](#)
- [Jumpstart HCIBox](#)
- [Jumpstart Release Notes](#)
- [Scenario Write-up Guidelines](#)
- [Jumpstart FAQ](#)
- [Open-Source Commitment](#)
- [Code of Conduct](#)
- [Contributing](#)
- [Security](#)

Overview

Azure Arc Jumpstart [↗](#)

The Azure Arc Jumpstart is designed to provide a “zero to hero” experience so you can start working with Azure Arc right away!

The Jumpstart provides step-by-step guides for independent Azure Arc scenarios that incorporate as much automation as possible, detailed screenshots and code samples, and a rich and comprehensive experience while getting started with the Azure Arc platform.

Our goal is for you to have a working Azure Arc environment spun-up in no time so you can focus on the core values of the platform, regardless of where your infrastructure may be, either on-premises or in the cloud.



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



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](#)

About "Gregor Reimling"

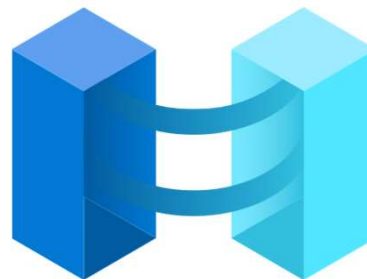


Thank You



Blog

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



Contact



- @GregorReimling
- @CloudInspires