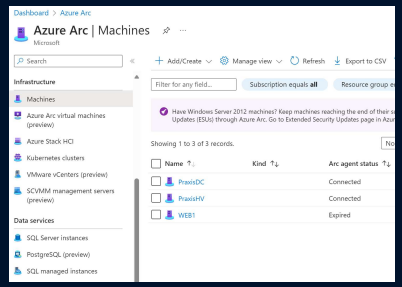
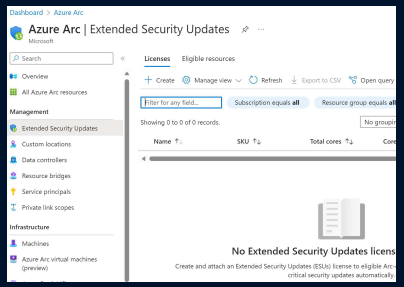
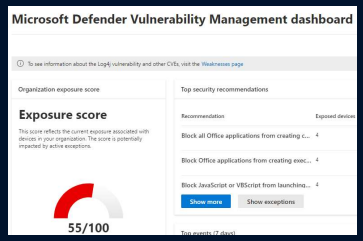
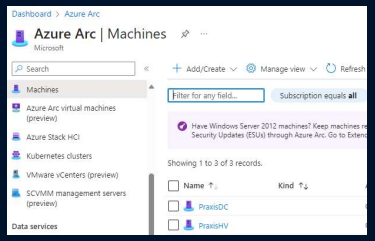
Multicloud Servermanagement with Azure Arc

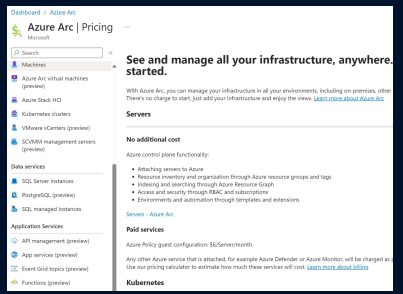
by Gregor Reimling











About “Gregor Reimling”

Azure Meetup BONN

www.azurebonn.de.de

Focus

Azure Governance, Security and IaaS

From

Cologne, Germany

My Blog

https://www.reimling.eu

Certifications

Cloud Security Architect, MVP for MS Azure

Hobbies

Family, Community, Worldtraveler

Contact

@GregorReimling

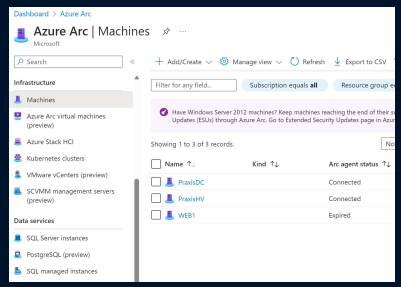
Gregor Reimling

Cloud Inspires Podcast

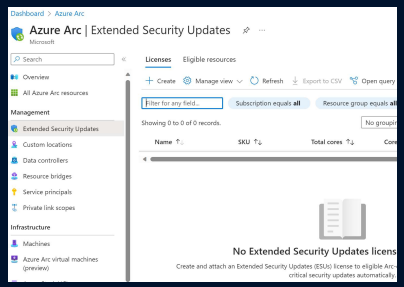
Stories and people behind Cloud Transformation

www.cloudinspires.me.me

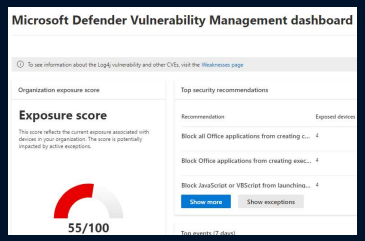
Agenda



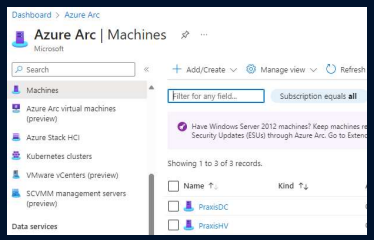
Overview about Azure Arc



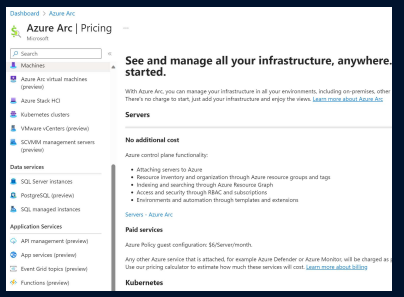
Server Management



Azure Automanage Machine Configuration

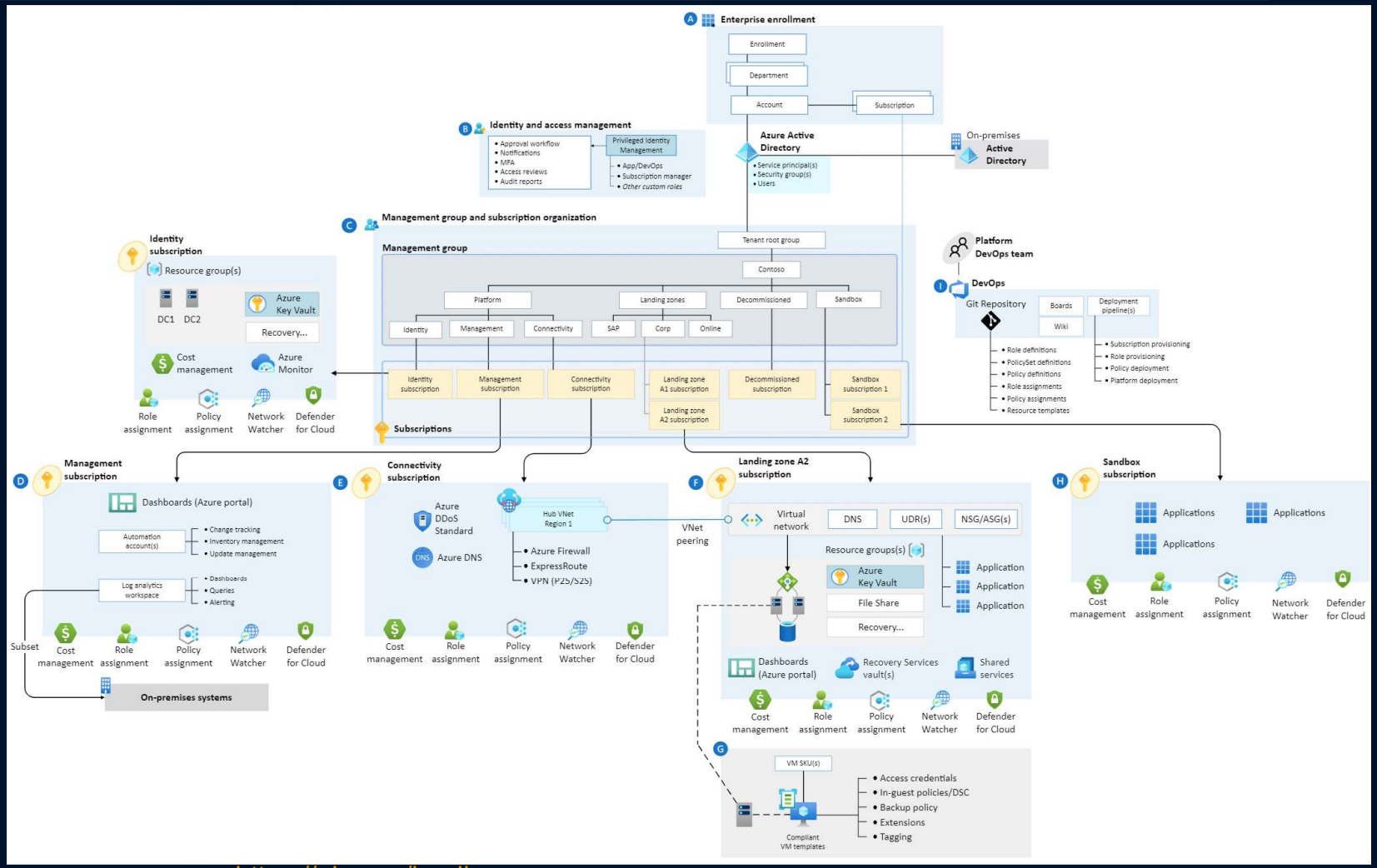


Update Management Center



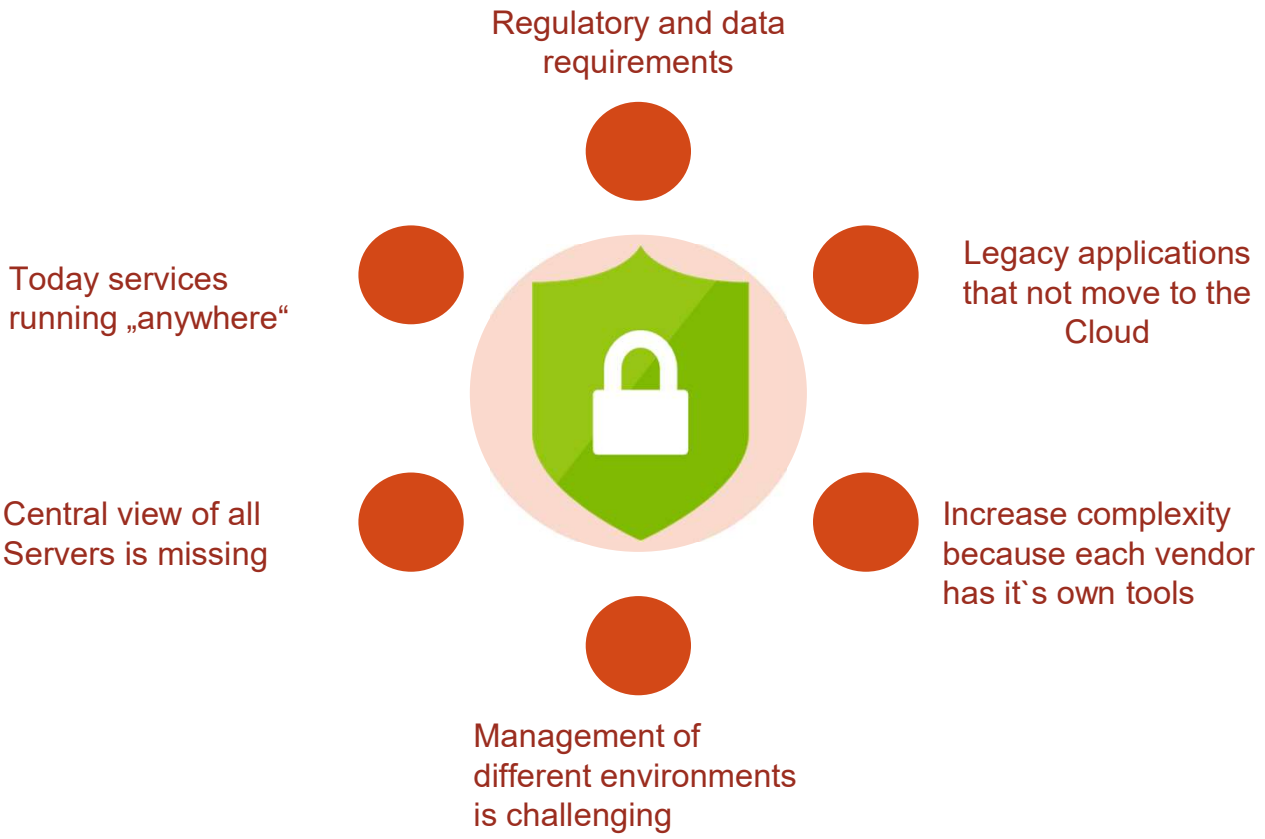
Defender for Server

Enterprise Scale

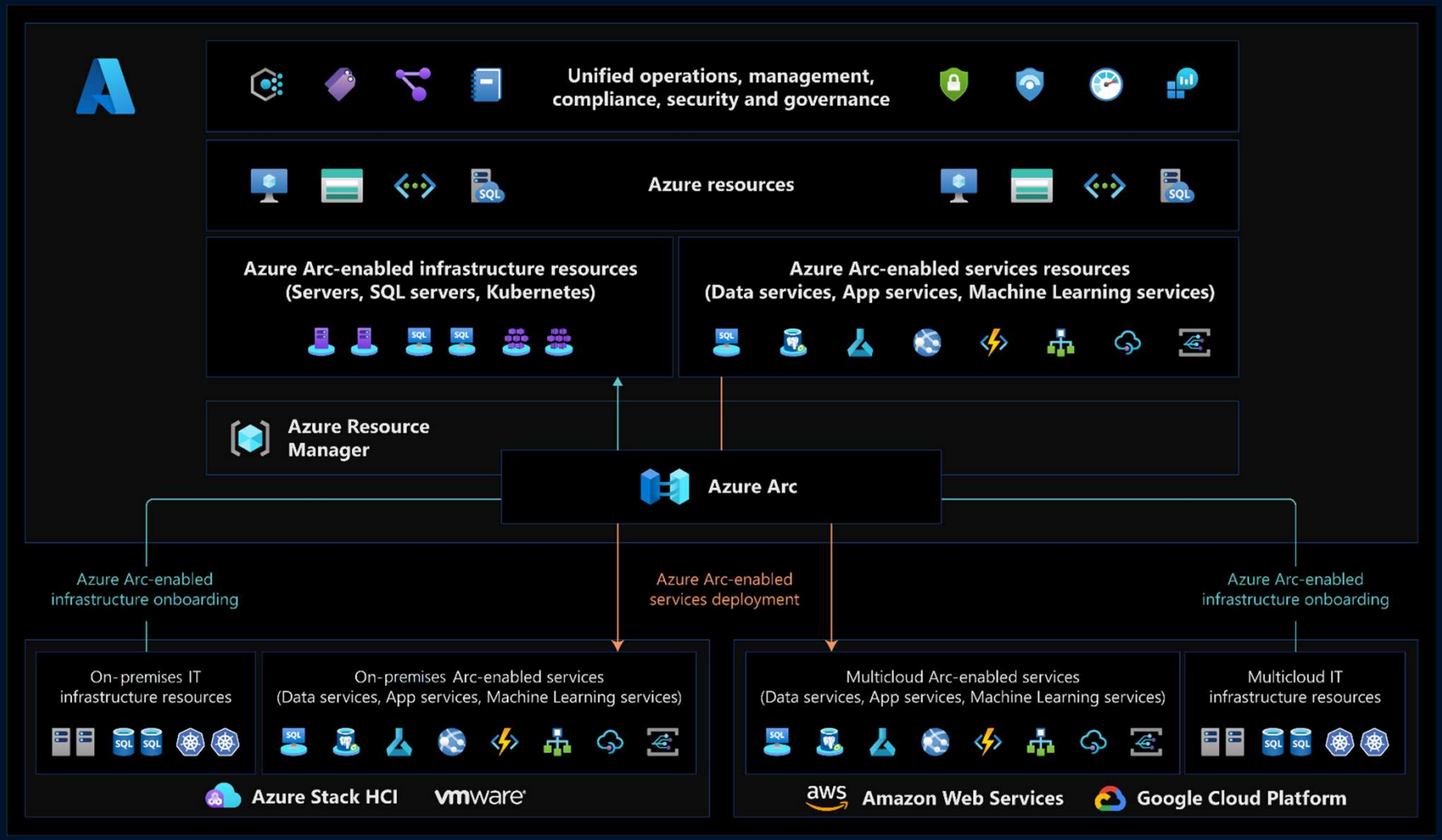


https://aka.ms/landingzones

Reasons for Hybrid Infrastructures



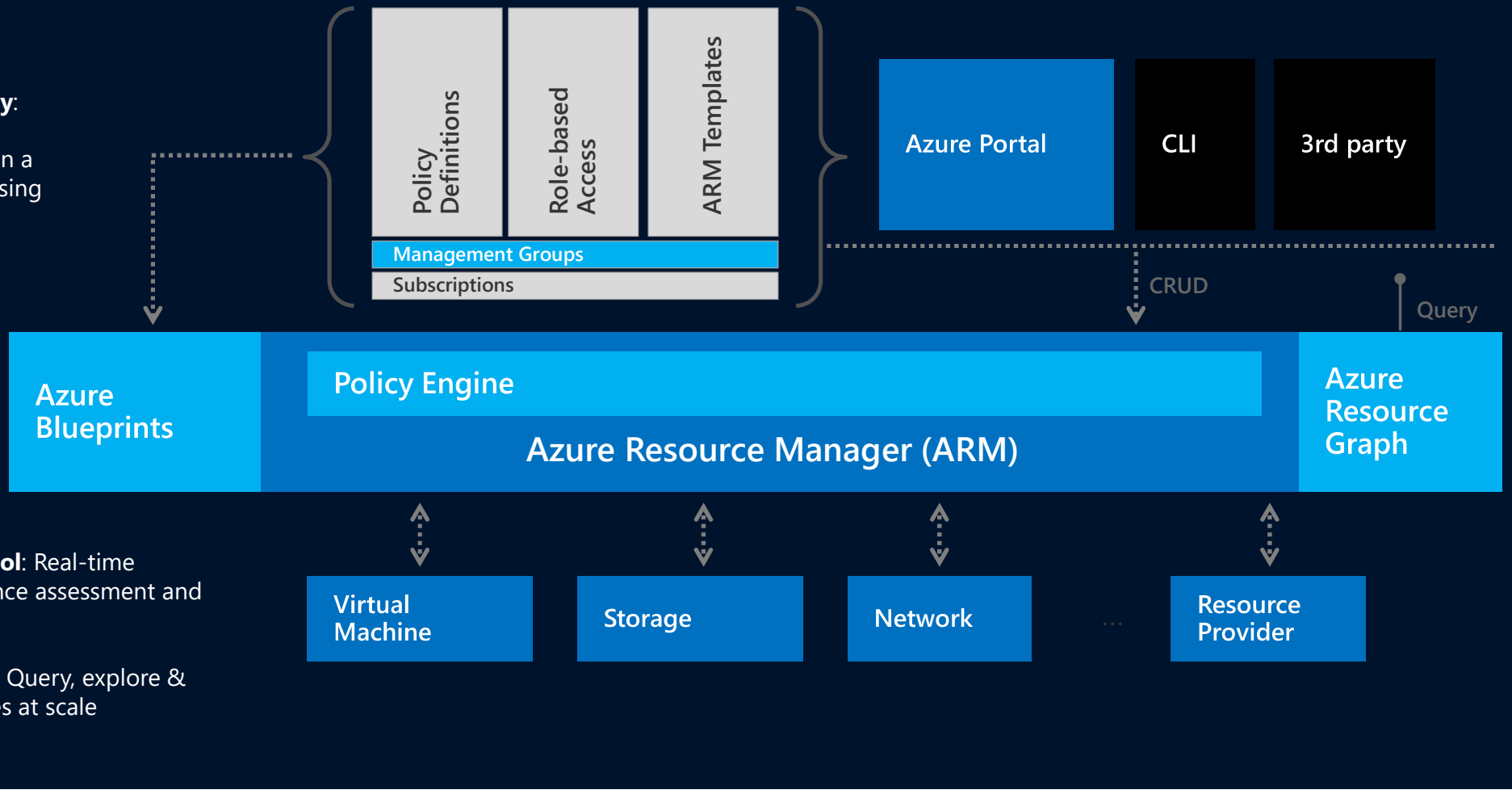
Azure Arc


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)
Multicloud Arc-enabled services (Data services, App services, Machine Learning services)
Multicloud IT infrastructure resources
Azure Stack HCI
vmware
aws
Amazon Web Services
Google Cloud Platform

Azure Governance Architecture

providing control over the cloud environment, without sacrificing developer agility

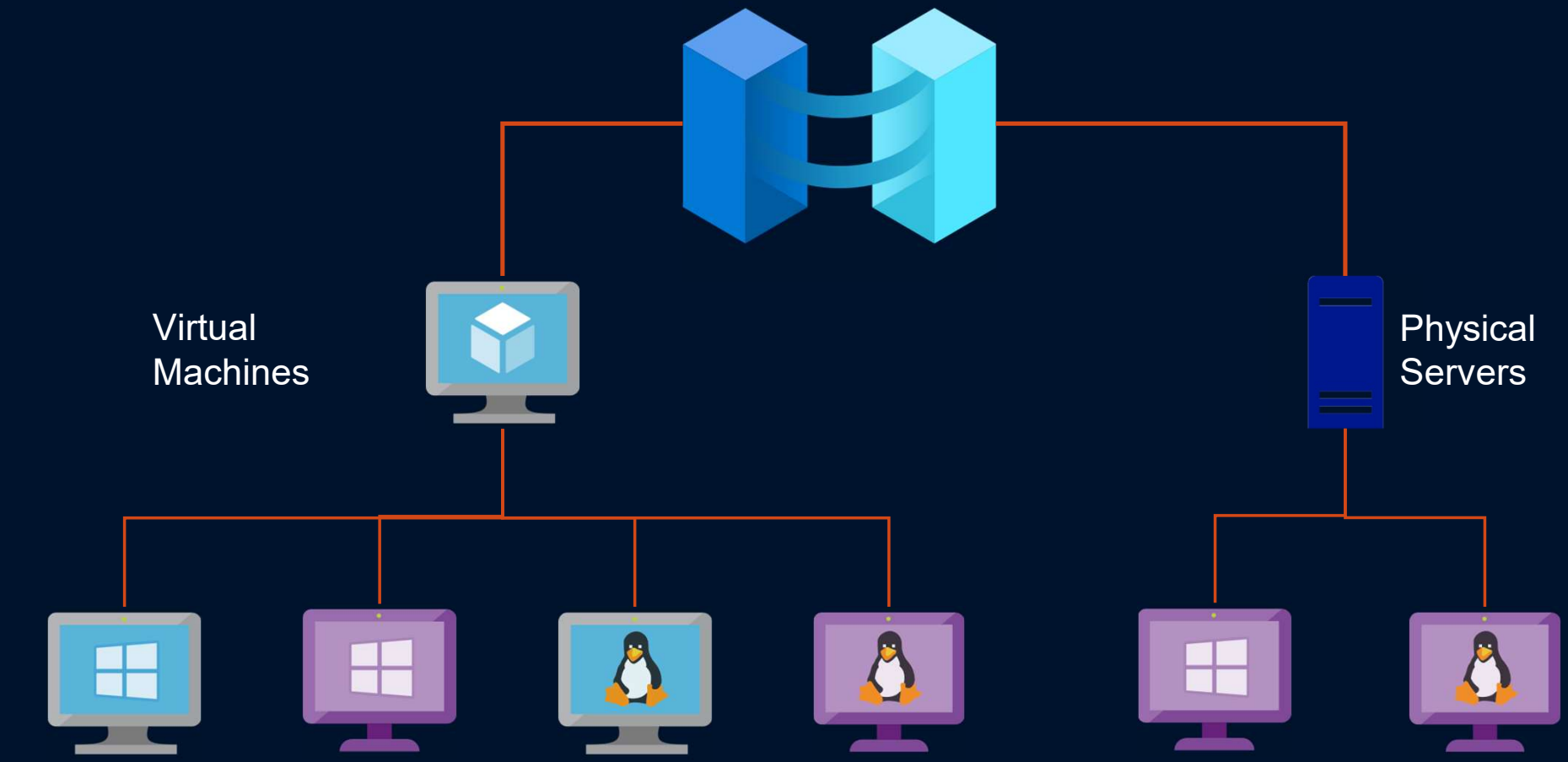
1. Environment Factory: Deploy and update cloud environments in a repeatable manner using composable artifacts



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

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

This session



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

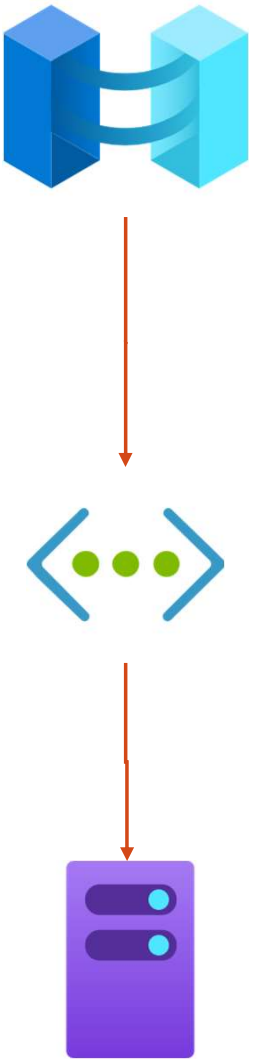
Linux

- 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

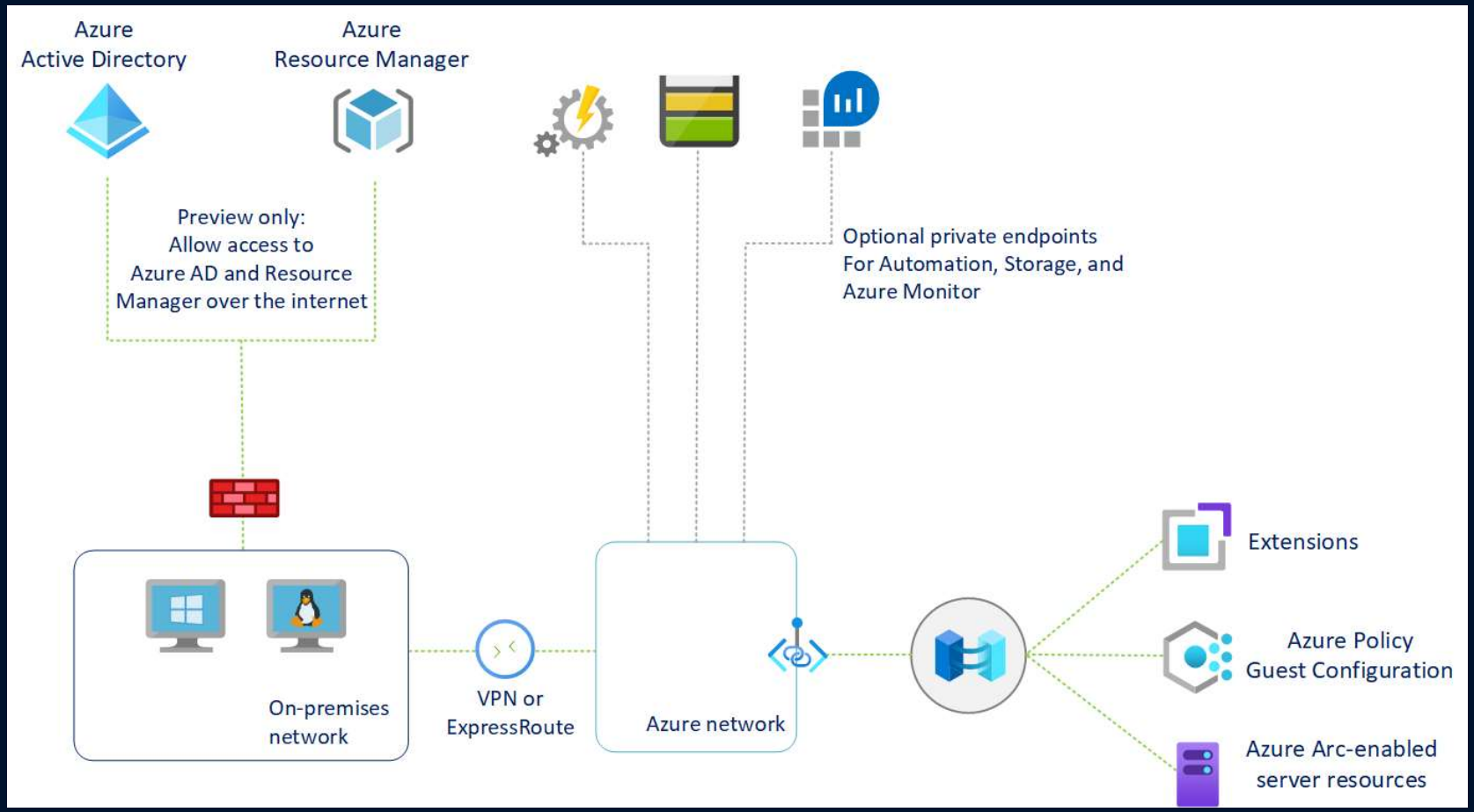
Prerequisites

- 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

Connecting to Azure Arc



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="$env:CORRE
LATION_ID";authType="$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."
```

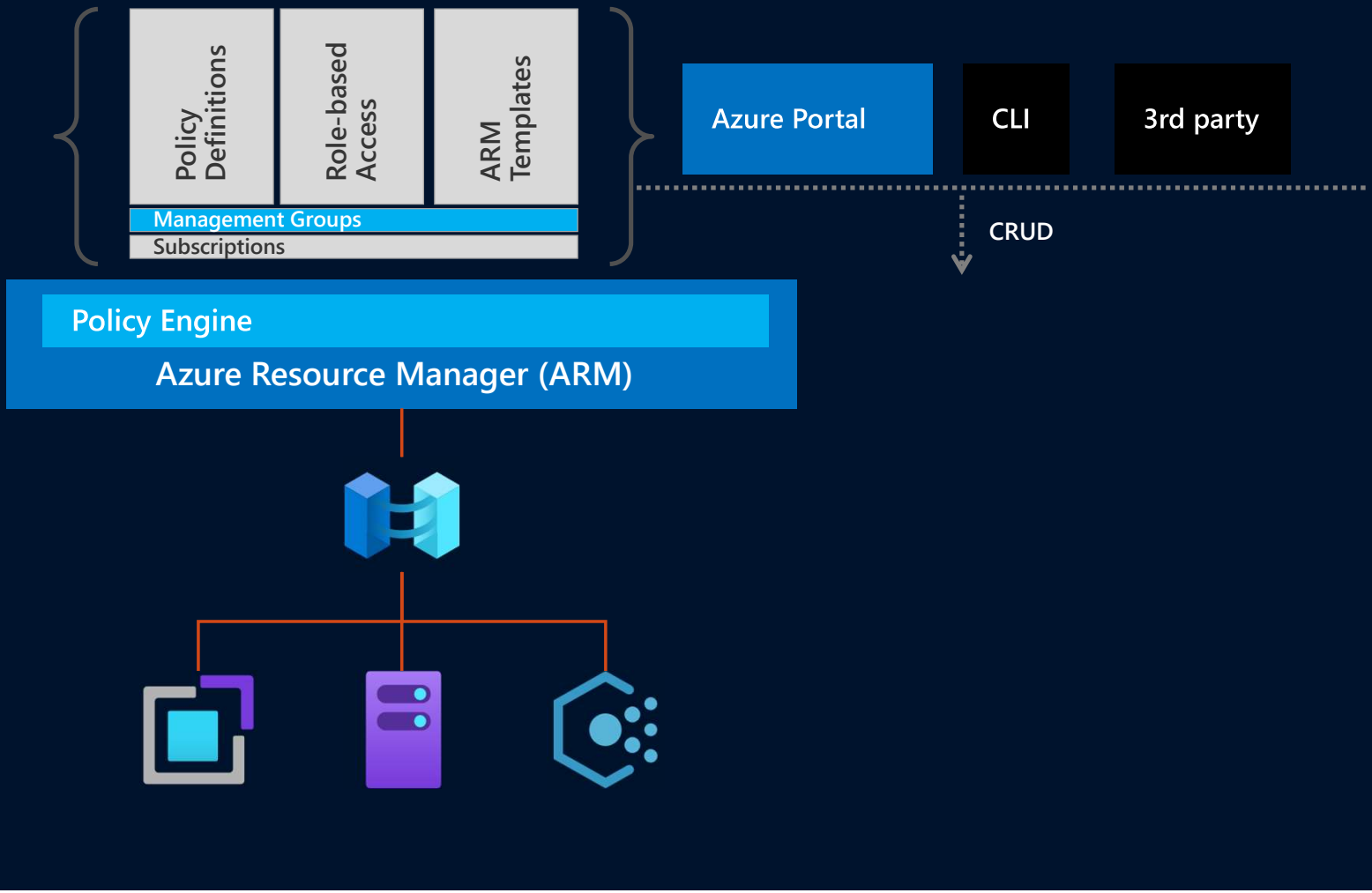
Azure Architecture

providing control over the cloud environment, without sacrificing developer agility

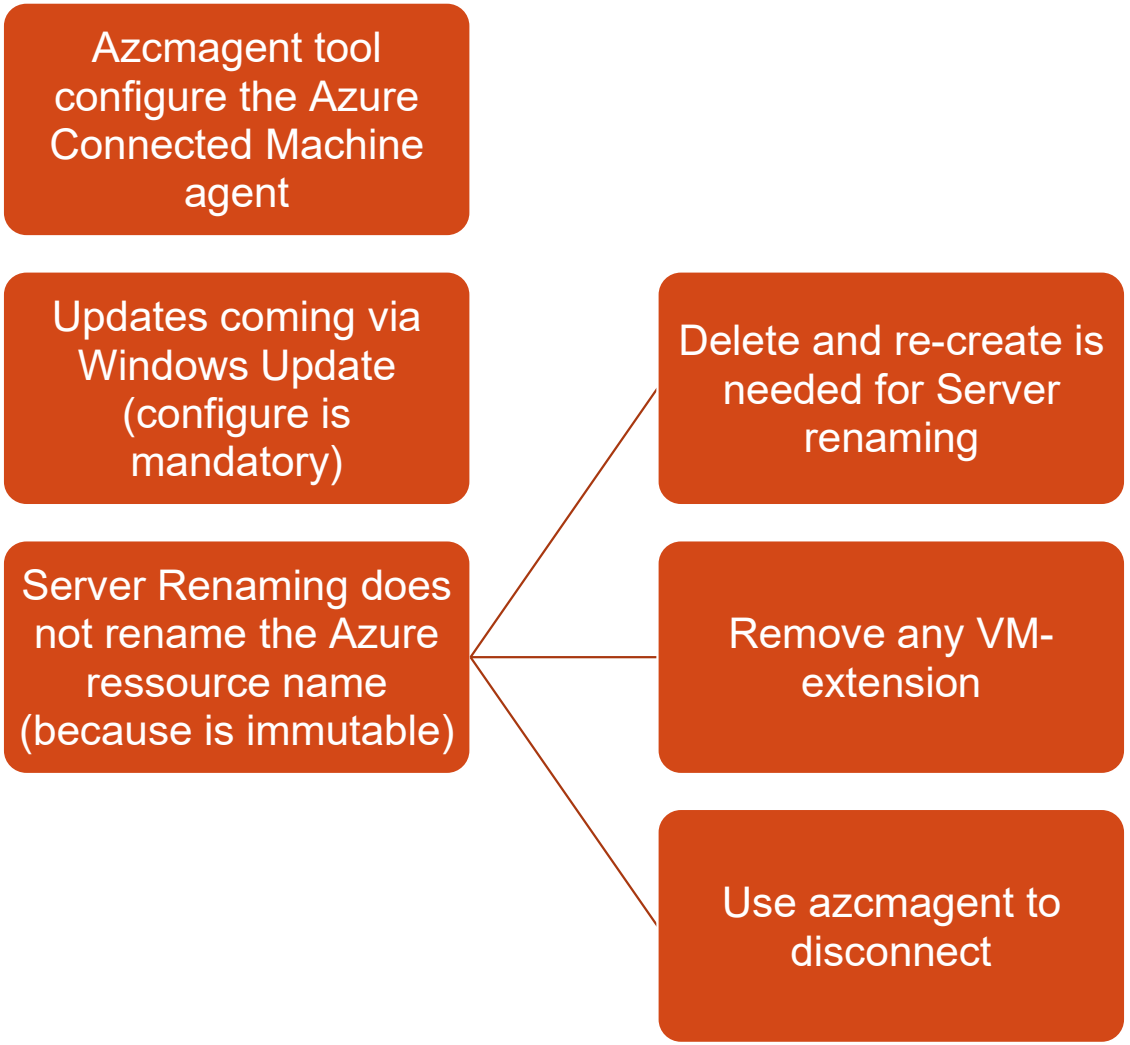
1. **Environment Factory**: Deploy and update cloud environments in a repeatable manner using composable artifacts

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

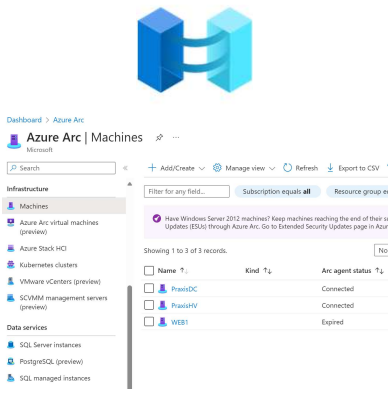
3. **Resource Visibility**: Query, explore & analyze cloud resources at scale



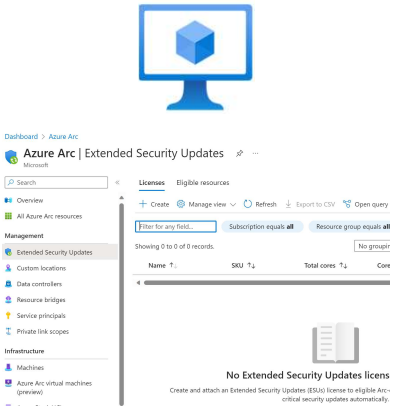
Connected Machine Agent



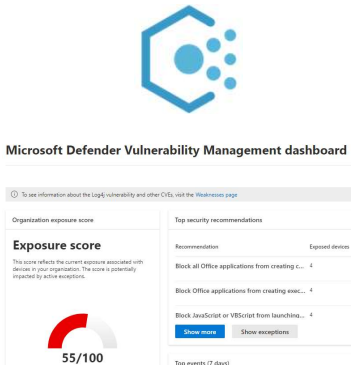
Demo Azure Arc



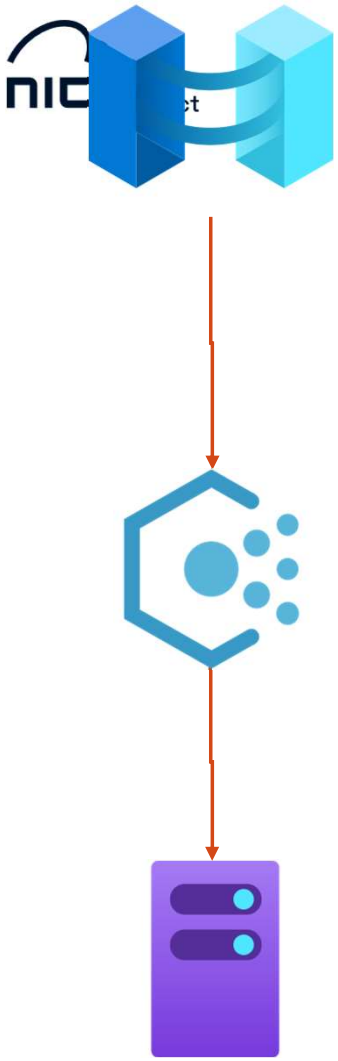
Overview about Azure Arc



Server Management



Azure Automanage Machine Configuration



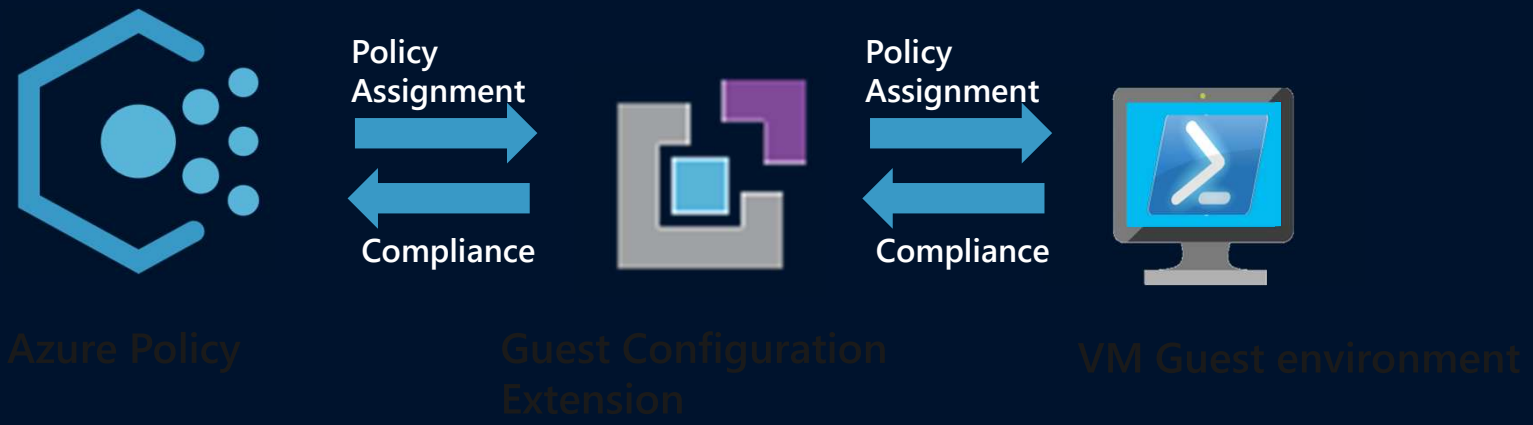
Azure Policy Guest Configuration

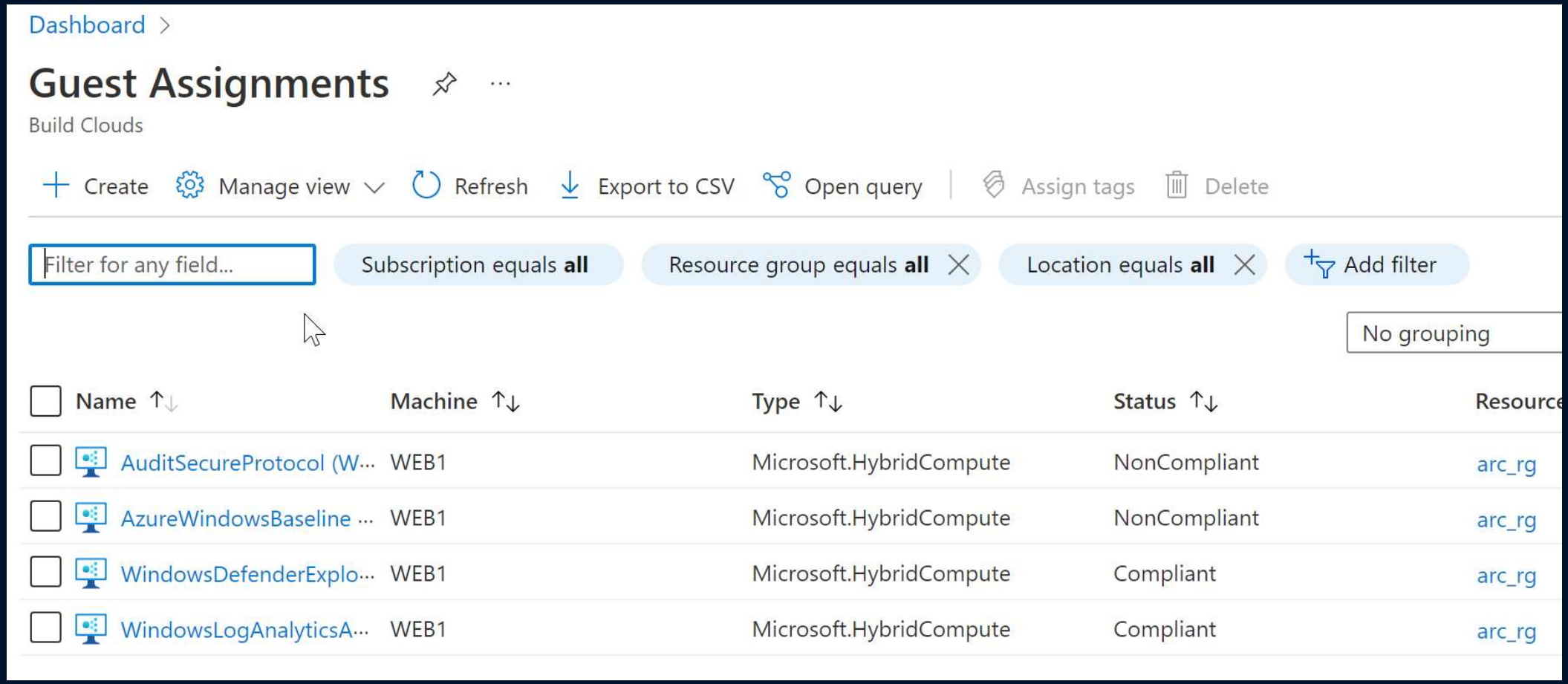
Renamed to

Azure Automanage Machine Configuration

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

How VM guest policy works



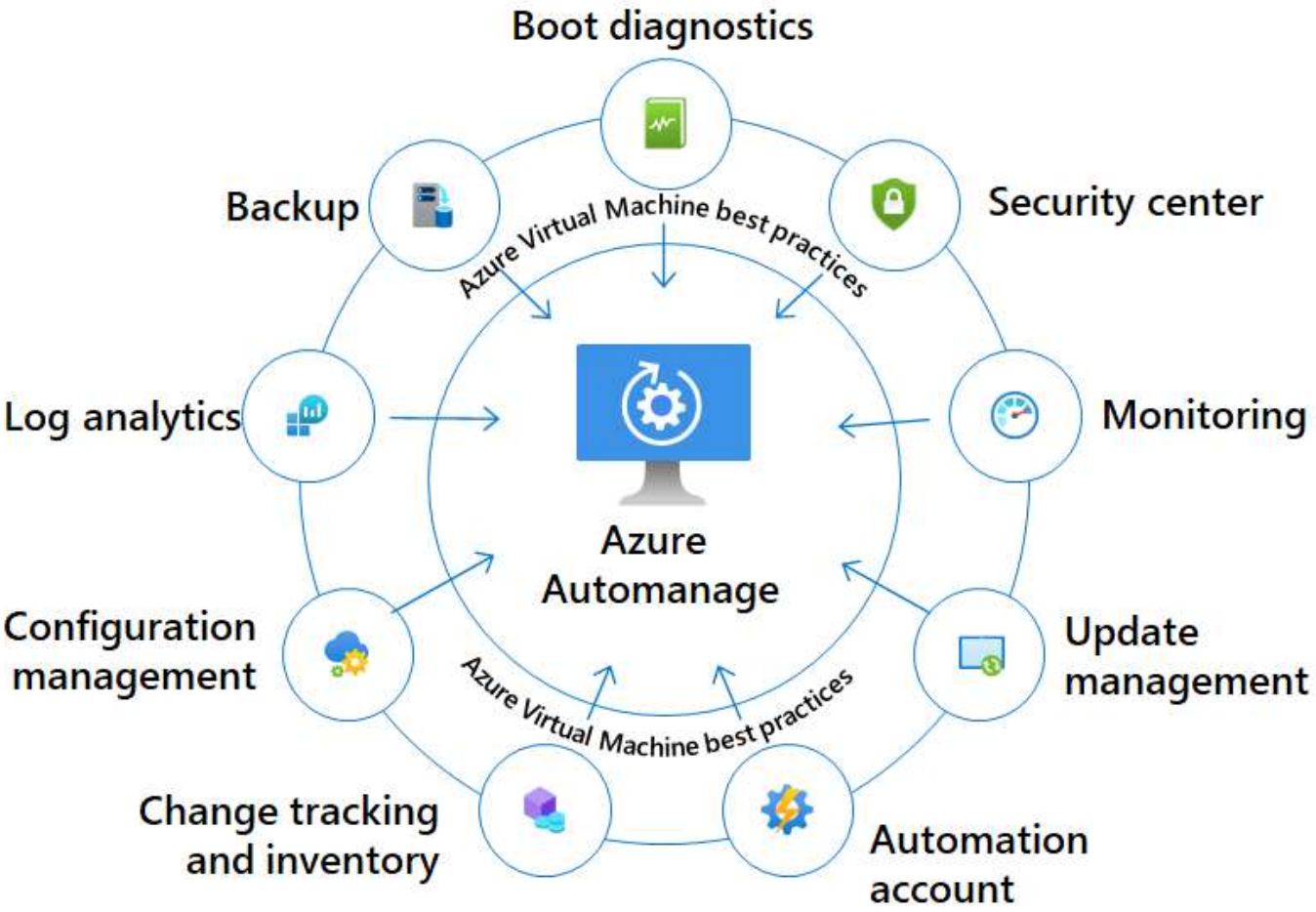

Dashboard
Guest Assignments
Build Clouds
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Delete
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
No grouping
Name
Machine
Type
Status
Resource
AuditSecureProtocol (W...
WEB1
Microsoft.HybridCompute
NonCompliant
arc_rg
AzureWindowsBaseline ...
WEB1
Microsoft.HybridCompute
NonCompliant
arc_rg
WindowsDefenderExplo...
WEB1
Microsoft.HybridCompute
Compliant
arc_rg
WindowsLogAnalyticsA...
WEB1
Microsoft.HybridCompute
Compliant
arc_rg

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

Azure Automanage

Azure Automanage – Your VM Service provider



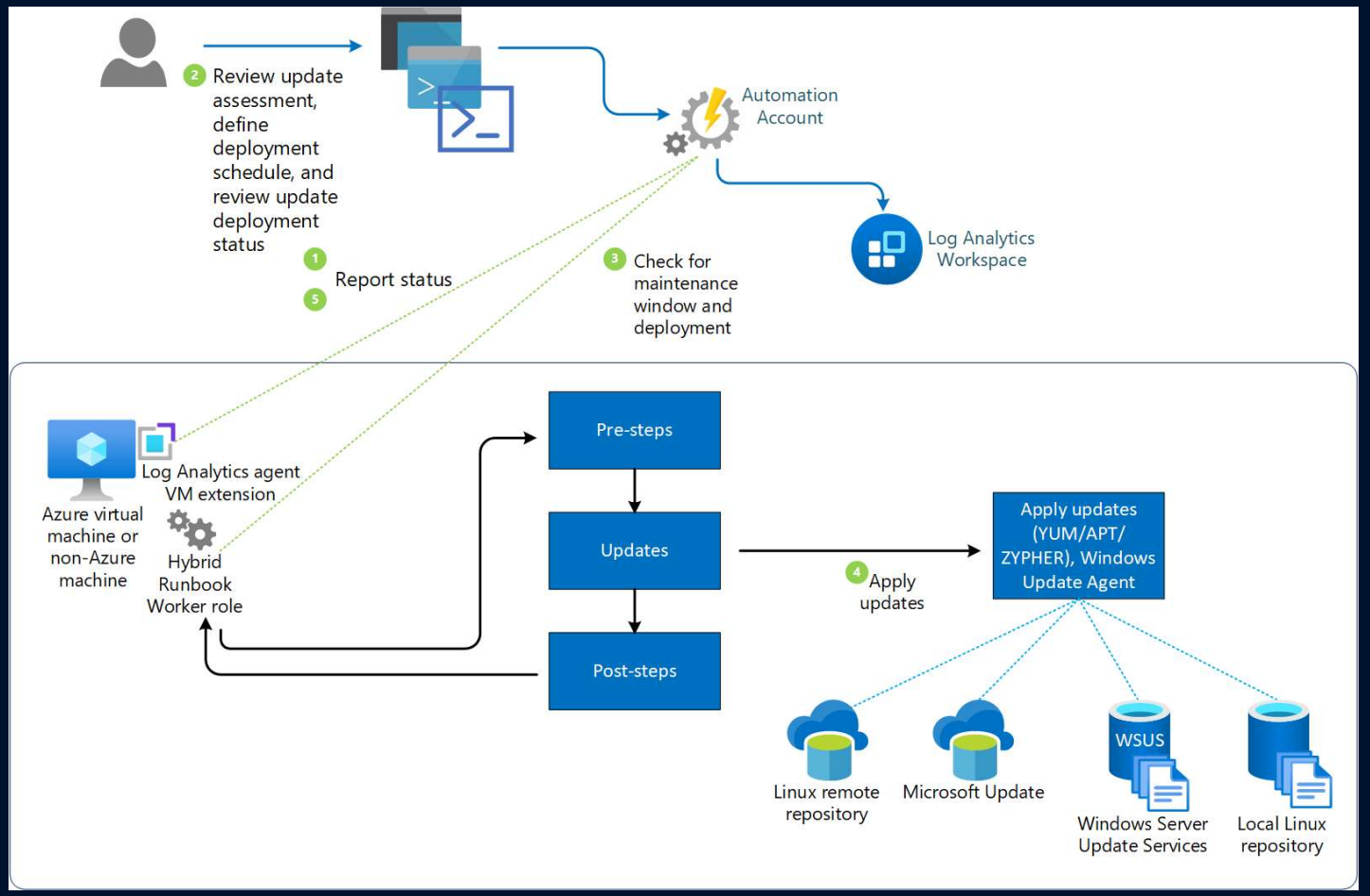
Azure Automanage

- 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

nic Cloud Connect

Azure Update Center

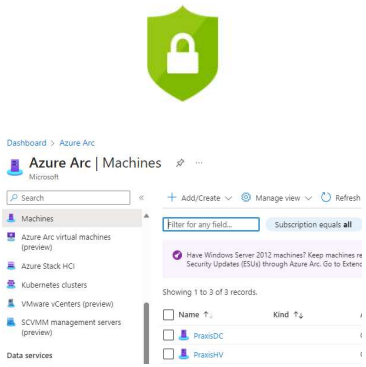
Azure Automation Update Management (v1)



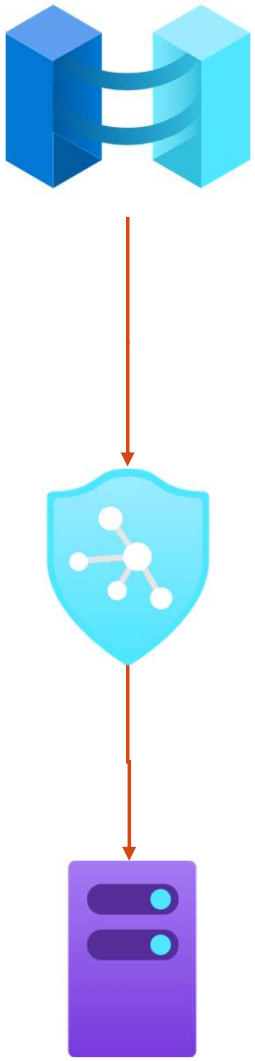
Why Azure Update Center v2?

- 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 charged by 5$ per Server/month beginning of January (only for Arc Machines)

Demo Azure Update Manager

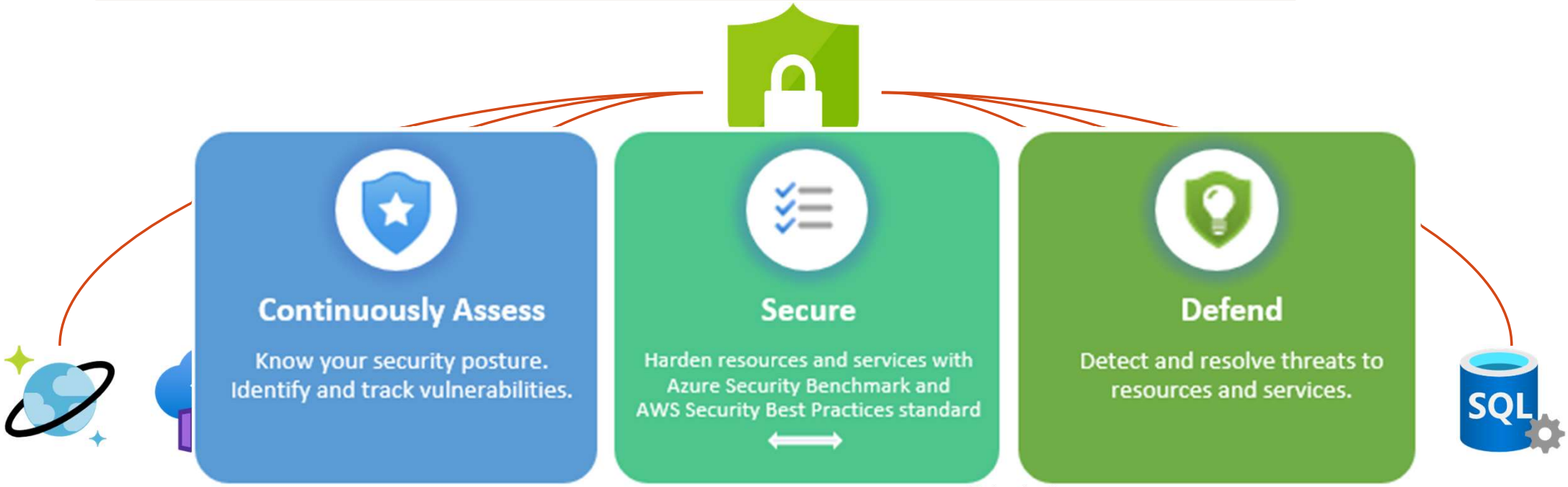


Azure Update Manager



Defender for Cloud

Microsoft Defender for Cloud



Defender for Azure Cosmos DB

Defender for Containers

Defender for App Service

Defender for DNS

Defender for CSPM

Defender for Servers

Defender for Key Vault

Defender for Resource Manager

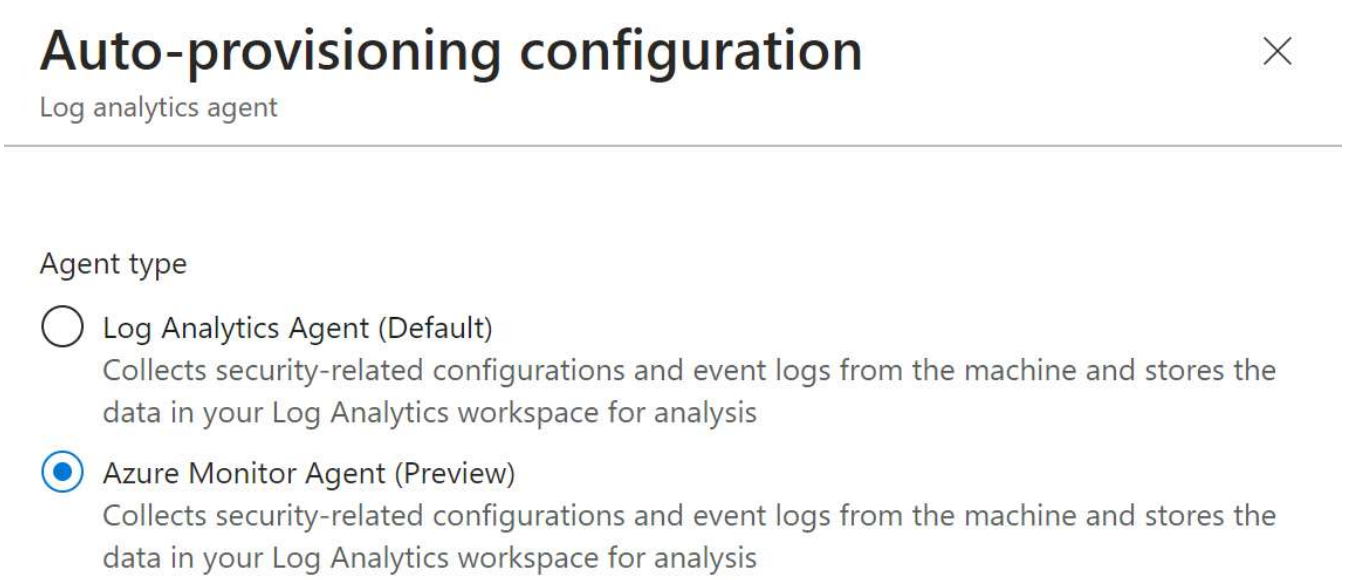
Defender for Storage

Defender for SQL

Activation of Defender for Servers

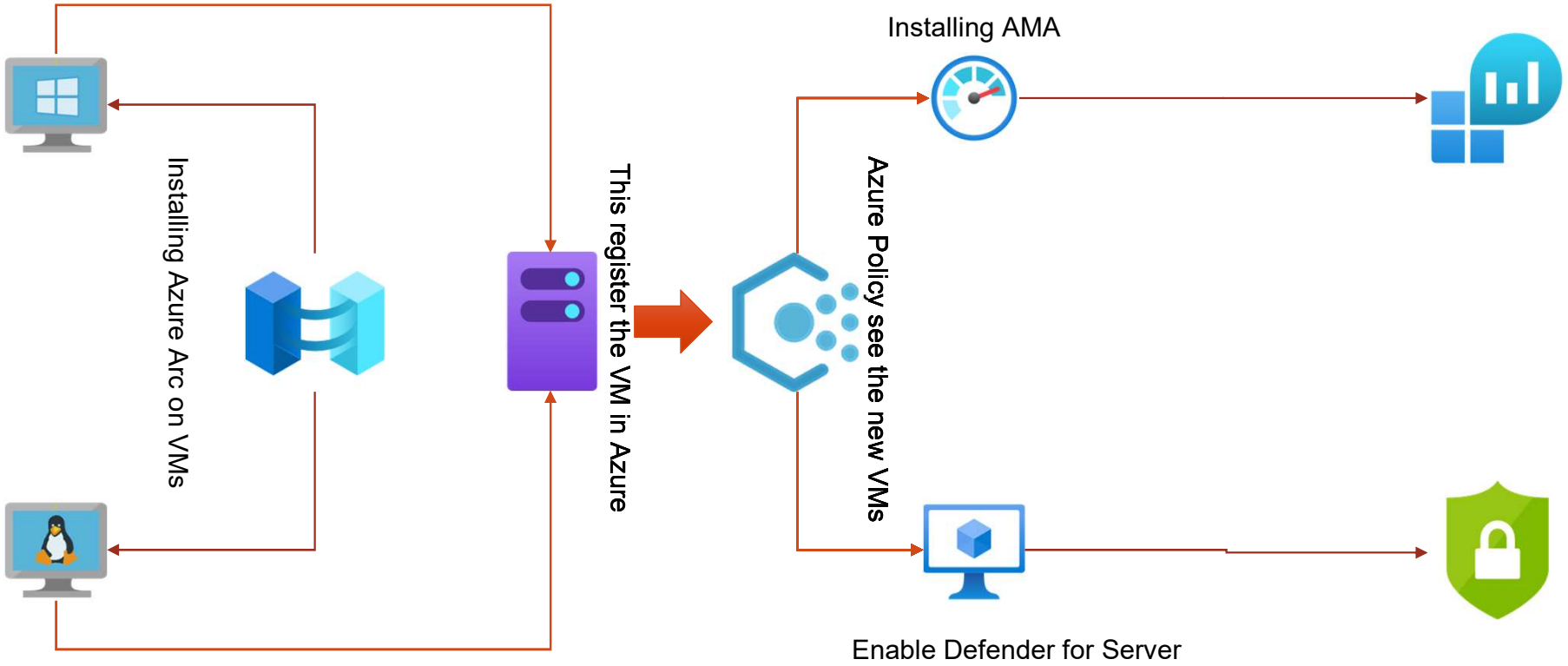
- Defender for Servers plan 1 must be enabled on subscription level
- Defender for Servers plan 2 must be enabled on subscription and **Workspace** level
- Mixing of the plans only possible with different subscription
- License cost for plan 2 is incurred for each machine connected to the Workspace where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

Auto-provisioning configuration



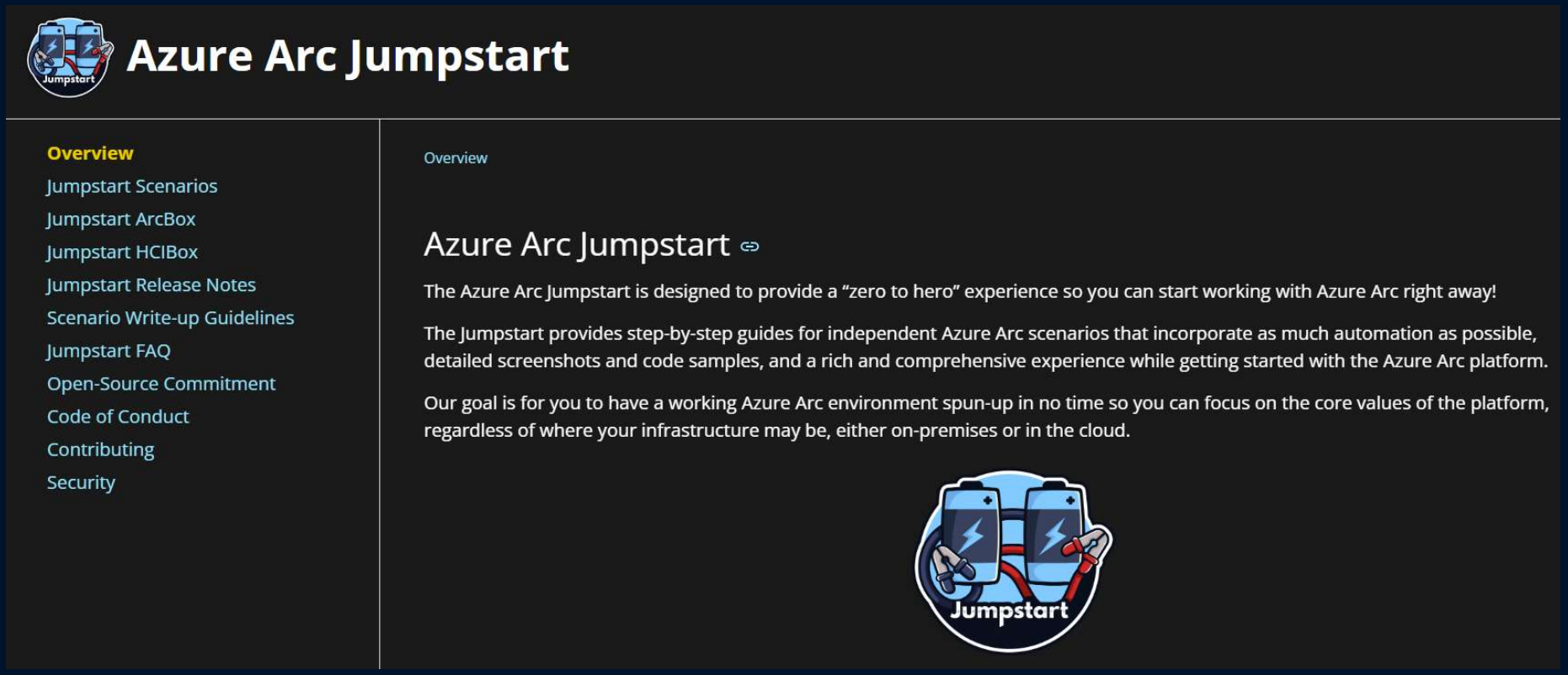
- Switch from MMA to AMA does not uninstall the MMA-agent
  - Duplicate agents results in doubled events or recommendations and appear twice in Defender
- Monitoring workbook – AMA migration tracker workbook

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



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

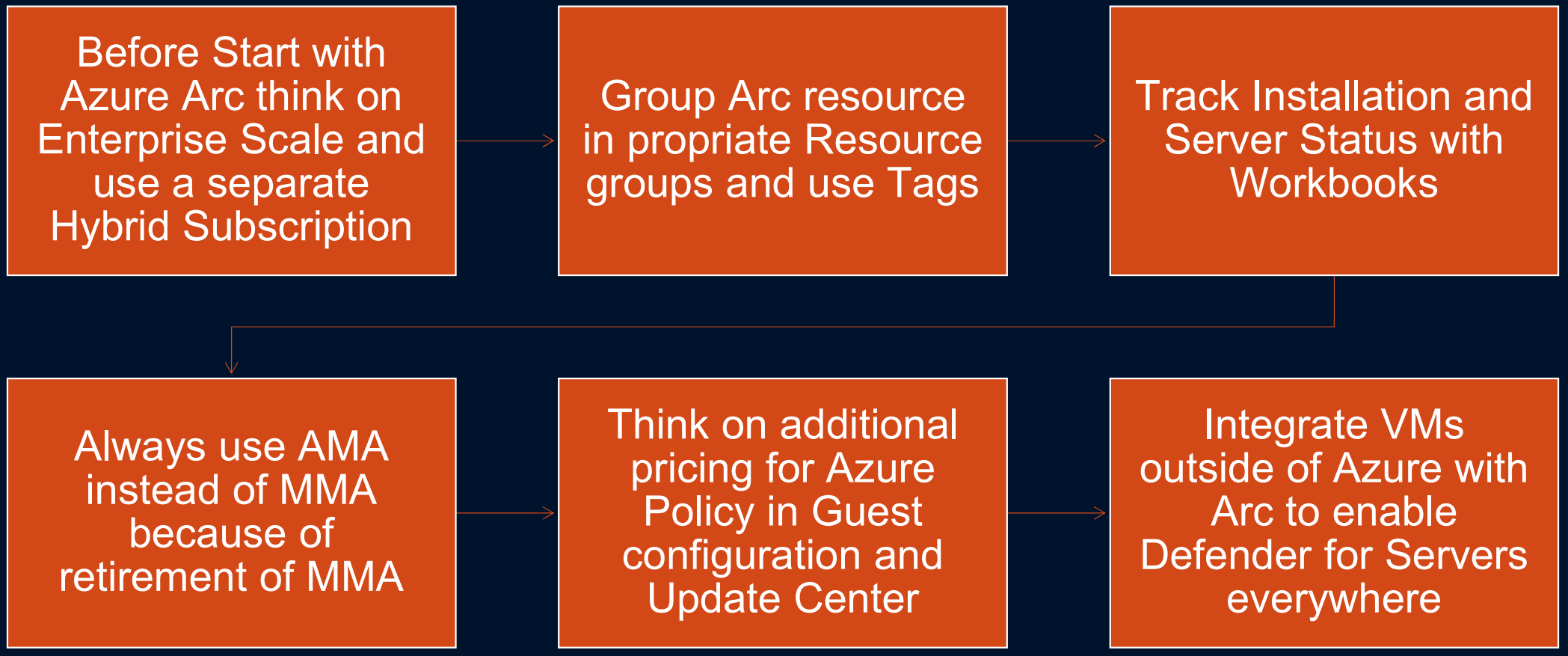
likamrat Lior Kamrat

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

Summary and Best Practices



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

Azure Arc – Person of Interests

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

Thank You

Azure Meetup BONN

www.azurebonn.de

Cloud Inspires Podcast

Stories and people behind Cloud Transformation

www.cloudinspires.me

Blog

- https://www.Reimling.eu

Contact

- @GregorReimling
- Gregor Reimling