nicX edition

May 31 – June 2, Oslo Spektrum

10th anniversary

Unified Operations and Management of your cross-premises server fleet with **Azure Arc**

David Pazdera

Cloud Solution Architect, Microsoft

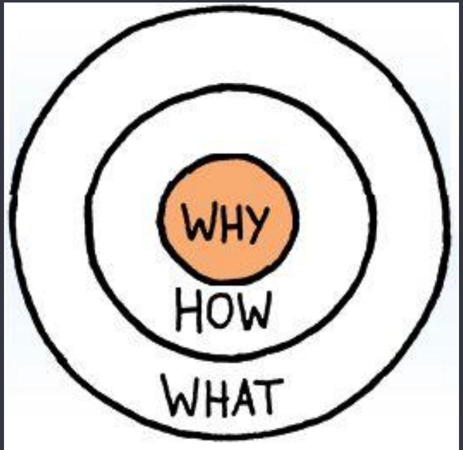
@pazdedav

Start with WHY

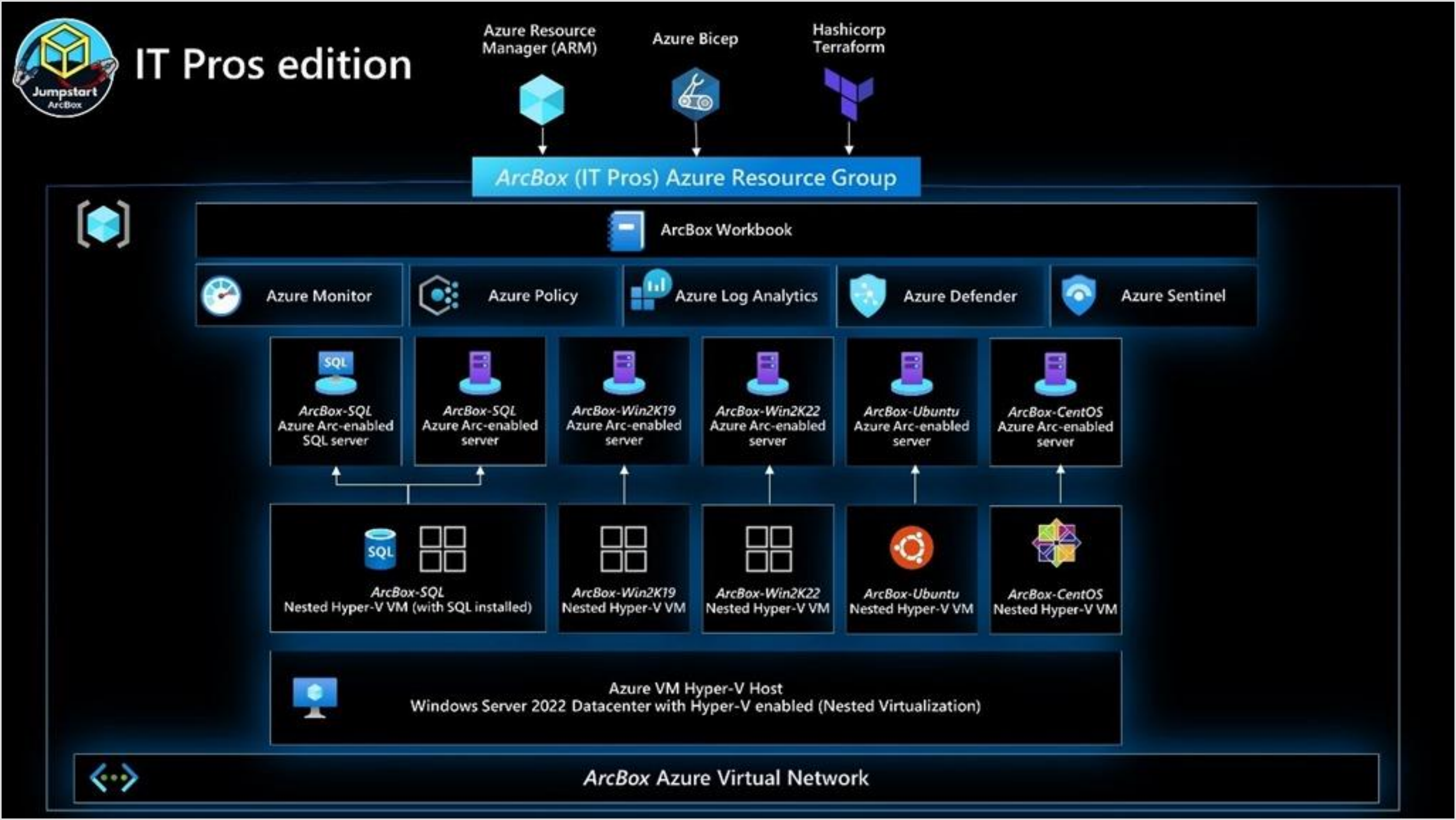
Start with Why

- Are you using **Azure Governance and Management services** in production? *Do you like the experience?*
- Are you responsible for **managing heterogeneous infrastructure** spanning Azure, on-premises, multicloud, and edge?

- What pain points are you trying to solve?
- What objectives and requirements do you have?
- Do you have a clear (PoC) project scope?



Jumpstart ArcBox 2.0 – IT Pros edition


Jumpstart
ArcBox
IT Pros edition
Azure Resource Manager (ARM)
Azure Bicep
Hashicorp Terraform
ArcBox (IT Pros) Azure Resource Group
ArcBox Workbook
Azure Monitor
Azure Policy
Azure Log Analytics
Azure Defender
Azure Sentinel
SQL
ArcBox-SQL Azure Arc-enabled SQL server
ArcBox-SQL Azure Arc-enabled server
ArcBox-Win2K19 Azure Arc-enabled server
ArcBox-Win2K22 Azure Arc-enabled server
ArcBox-Ubuntu Azure Arc-enabled server
ArcBox-CentOS Azure Arc-enabled server
SQL
ArcBox-SQL Nested Hyper-V VM (with SQL installed)
ArcBox-Win2K19 Nested Hyper-V VM
ArcBox-Win2K22 Nested Hyper-V VM
ArcBox-Ubuntu Nested Hyper-V VM
ArcBox-CentOS Nested Hyper-V VM
Azure VM Hyper-V Host
Windows Server 2022 Datacenter with Hyper-V enabled (Nested Virtualization)
ArcBox Azure Virtual Network

aka.ms/AzureArcJumpstart

Unified Operations domains

Govern & organize

- Policy guest configuration
- Resource tagging
- Resource Graph

Monitor & observe

- Log Analytics
- VM Insights
- Workbooks

Configure & automate

- Azure Automation: Update Management, Change Tracking & Inventory, Hybrid Runbooks
- Custom scripts
- Azure Automanage

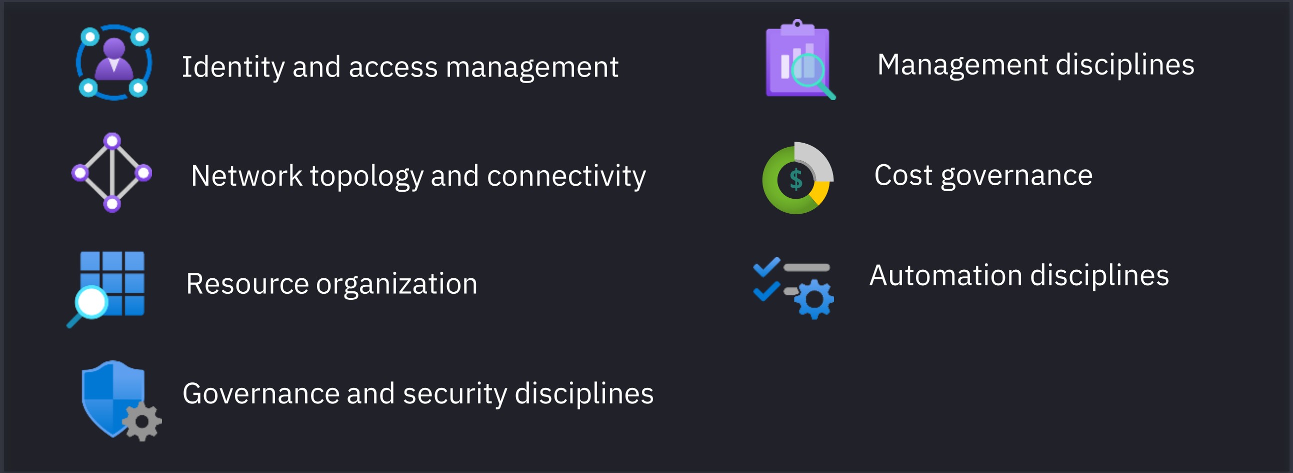
Protect & secure

- Defender
- Key Vault
- Sentinel
- Managed Identity
- Azure RBAC

Design and prepare a landing zone

Architecture guidance

- Minimum **prerequisites**
  - Provider registration, permissions, supported OS++
- Azure Arc **landing zone accelerator** for hybrid and multicloud
  - Extension of Azure Landing Zone
  - Seven ‘Critical Design Areas’



Identity and access management

Network topology and connectivity

Resource organization

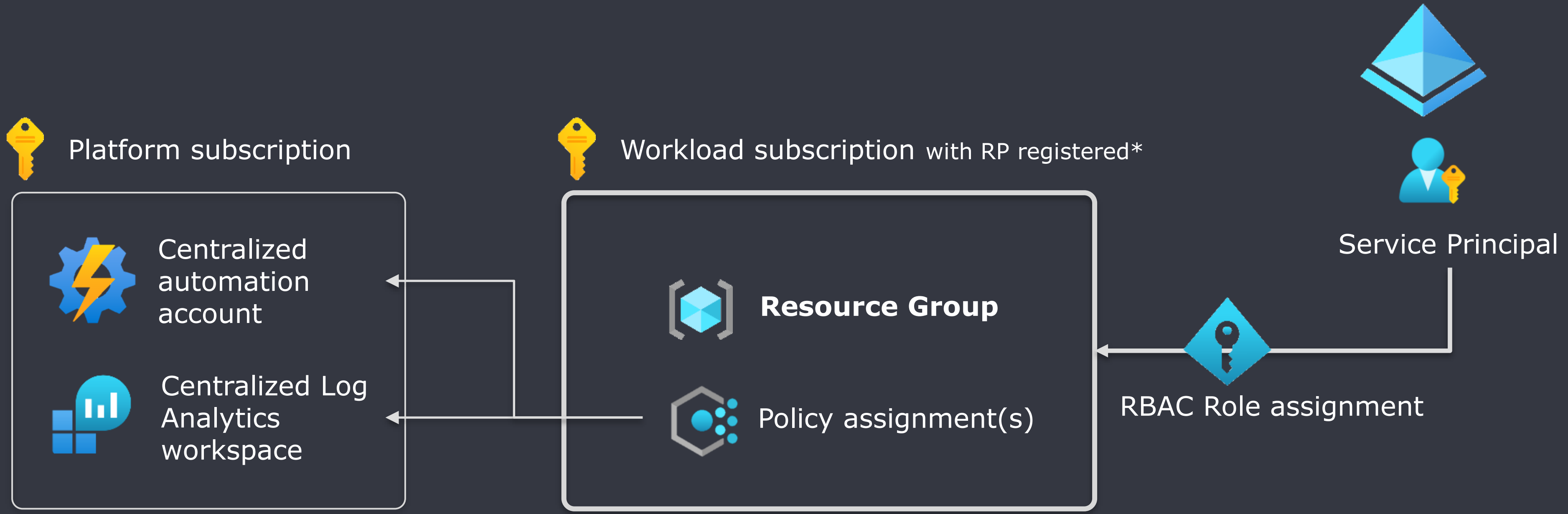
Governance and security disciplines

Management disciplines

Cost governance

Automation disciplines

Landing zone example



Platform subscription

Centralized automation account

Centralized Log Analytics workspace

Workload subscription with RP registered*

Resource Group

Policy assignment(s)

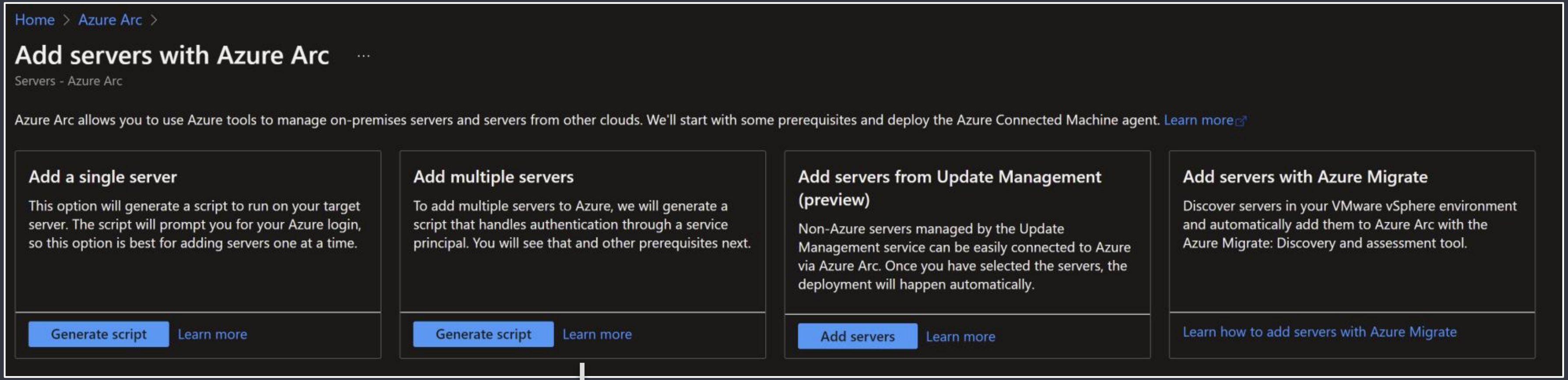
RBAC Role assignment

Service Principal

* *Microsoft.HybridCompute, Microsoft.GuestConfiguration*

Onboarding

Options for **onboarding**



Home > Azure Arc >

Add servers with Azure Arc ...

Servers - Azure Arc

Azure Arc allows you to use Azure tools to manage on-premises servers and servers from other clouds. We'll start with some prerequisites and deploy the Azure Connected Machine agent. Learn more

Add a single server

This option will generate a script to run on your target server. The script will prompt you for your Azure login, so this option is best for adding servers one at a time.

Generate script | Learn more

Add multiple servers

To add multiple servers to Azure, we will generate a script that handles authentication through a service principal. You will see that and other prerequisites next.

Generate script | Learn more

Add servers from Update Management (preview)

Non-Azure servers managed by the Update Management service can be easily connected to Azure via Azure Arc. Once you have selected the servers, the deployment will happen automatically.

Add servers | Learn more

Add servers with Azure Migrate

Discover servers in your VMware vSphere environment and automatically add them to Azure Arc with the Azure Migrate: Discovery and assessment tool.

Learn how to add servers with Azure Migrate

VMware vSphere with PowerCLI

Extend existing infra provisioning tooling
(e.g., Terraform)

SCCM/MECM with PSH or Task Sequence

Windows Admin Center

AD Group Policy

Soon coming to the Portal

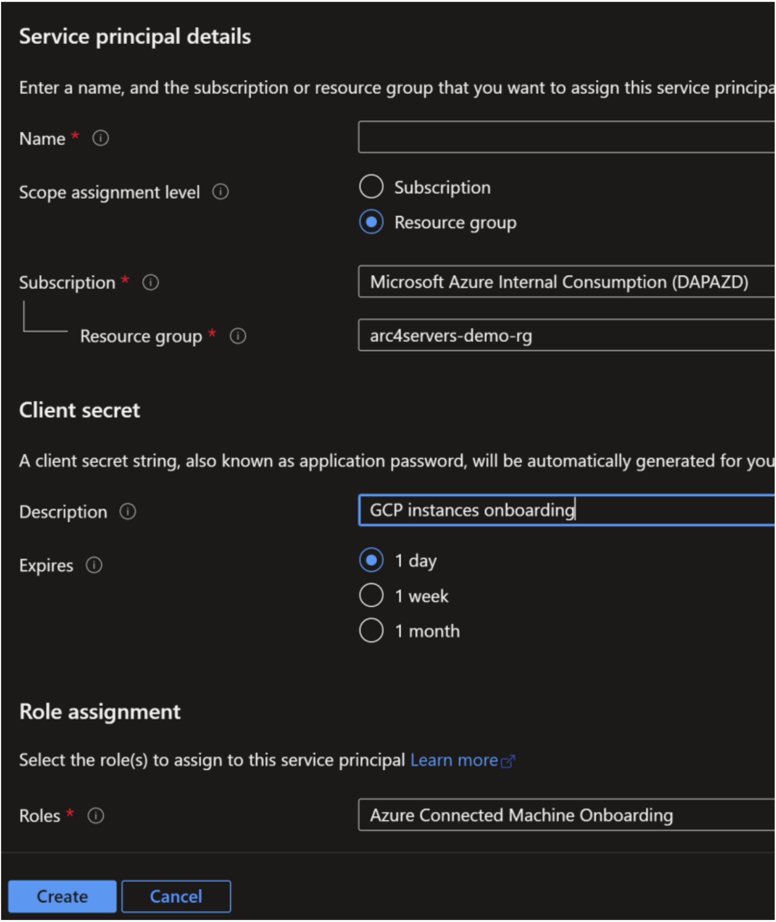
Ansible Playbook

Onboarding SPN **security** hardening

- Limit the scope (blast radius)
- Limit permissions (specific role)
- Limit the secret lifetime

  SPN credentials is used only once for onboarding, CMA uses Managed Identity and HIMDS

- Extra: Limit **source IPs** for onboarding
  - Conditional Access Policies for SPNs (Preview)
  - Allow onboarding from within 'Trusted locations'
  - Source: @SeifBassem, Blob post



Service principal details

Enter a name, and the subscription or resource group that you want to assign this service principa

Name * ⓘ

Scope assignment level ⓘ ○ Subscription ● Resource group

Subscription * ⓘ Microsoft Azure Internal Consumption (DAPAZD)

Resource group * ⓘ arc4servers-demo-rg

Client secret

A client secret string, also known as application password, will be automatically generated for you

Description ⓘ GCP instances onboarding

Expires ⓘ ● 1 day ○ 1 week ○ 1 month

Role assignment

Select the role(s) to assign to this service principal Learn more

Roles * ⓘ Azure Connected Machine Onboarding

Onboarding **tips & tricks**

- **Customize** resource name for Arc server (e.g., due to reserved resource name error)

  ```
  > azcmagent connect … --resource-name XYZ
  ```

- **Validate** network connectivity

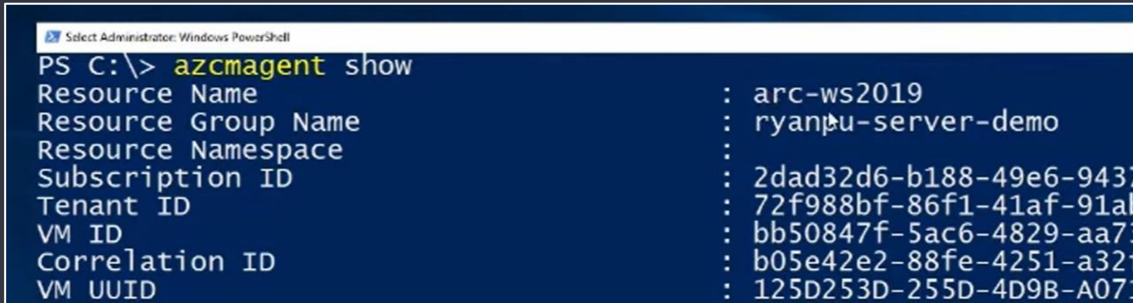
  ```
  > azcmagent check --location <regionName>
  ```

- **Regional** availability (e.g., Norway East is not available yet)

  https://azure.microsoft.com/en-us/global-infrastructure/services/?products=azure-arc&regions=all

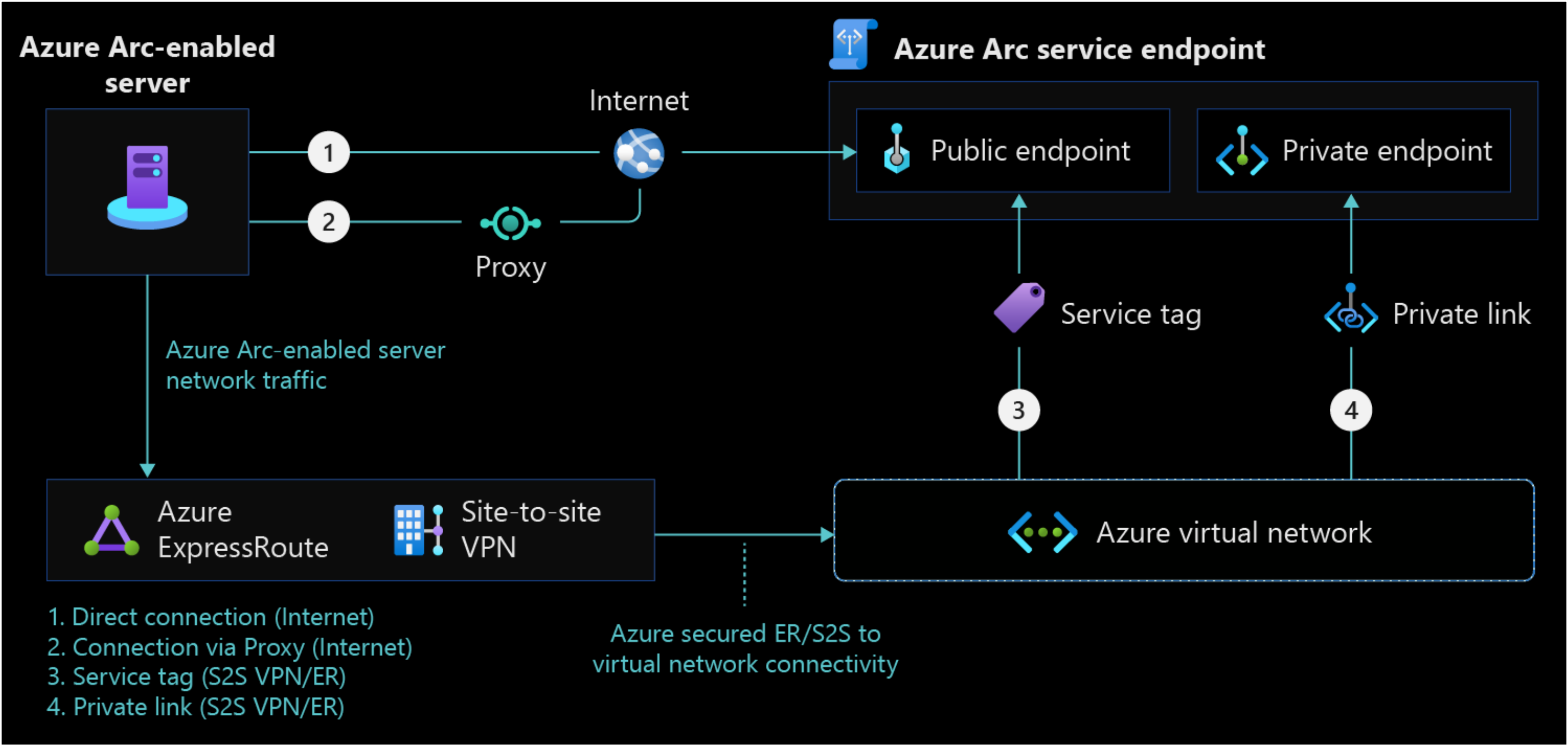
- **Check** agent status and other metadata

  ```
  > azcmagent show
  ```



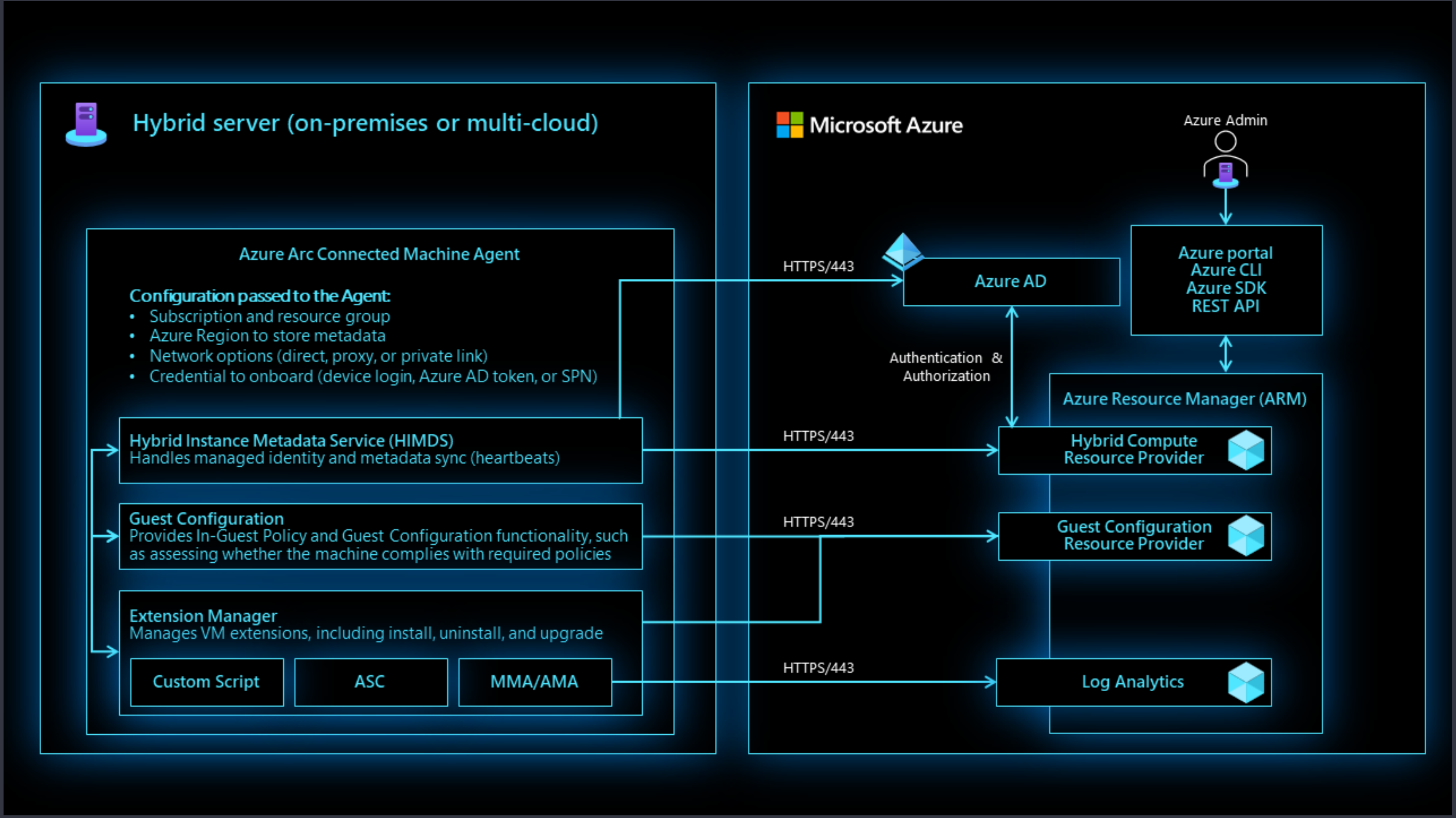
```
PS C:\> azcmagent show
Resource Name                                  : arc-ws2019
Resource Group Name                            : ryanpu-server-demo
Resource Namespace                             :
Subscription ID                                : 2dad32d6-b188-49e6-943
Tenant ID                                      : 72f988bf-86f1-41af-91a
VM ID                                          : bb50847f-5ac6-4829-aa7
Correlation ID                                 : b05e42e2-88fe-4251-a32
VM UUID                                        : 125D253D-255D-4D9B-A07
```

Network topology and connectivity CDR



1. Direct connection (Internet)
2. Connection via Proxy (Internet)
3. Service tag (S2S VPN/ER)
4. Private link (S2S VPN/ER)

Connected Machine Agent – how it works



Hybrid server (on-premises or multi-cloud)

Azure Arc Connected Machine Agent

Configuration passed to the Agent:

- Subscription and resource group
- Azure Region to store metadata
- Network options (direct, proxy, or private link)
- Credential to onboard (device login, Azure AD token, or SPN)

Hybrid Instance Metadata Service (HIMDS)
Handles managed identity and metadata sync (heartbeats)

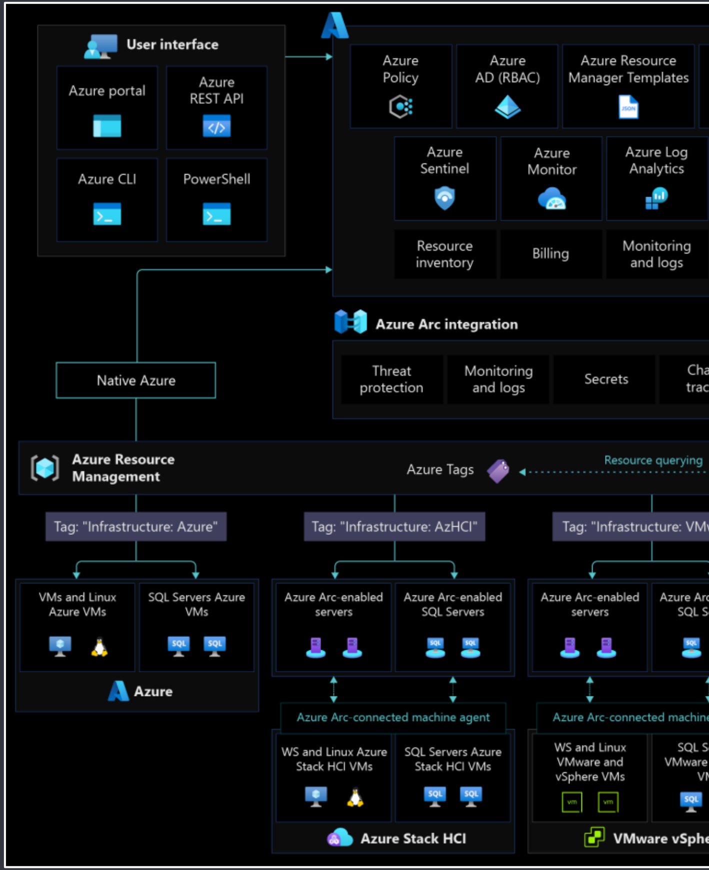
Guest Configuration
Provides In-Guest Policy and Guest Configuration functionality, such as assessing whether the machine complies with required policies

Extension Manager
Manages VM extensions, including install, uninstall, and upgrade

Govern and organize your (Arc) resources

Resource organization CDR

- Scaffold for management scopes (ALZ) with policy-driven governance
- Naming standards
    - No documented constraints
    - Unique server name per RG
    - Reserved names
- Tag definition and enforcement
    - Policy for appending mandatory tags
- Resource Manager limits
    - 5000 Arc-server instances per RG (no sub-level limit)
    - Same limit for extensions



Inventory and tagging

- Extend the onboarding script with Cloud Provider’s metadata

Example code for getting Zone and Instance ID for a Windows VM on GCP:

```
# Get GCP VM Instance data
$GCPZone = Invoke-RestMethod -Headers @{'Metadata-Flavor' = 'Google'} -Uri
"http://metadata.google.internal/computeMetadata/v1/instance/zone"
$GCPInstanceId = Invoke-RestMethod -Headers @{'Metadata-Flavor' = 'Google'} -Uri
"http://metadata.google.internal/computeMetadata/v1/instance/id"

# Create Tags
$tags = "Datacenter=GCP,CountryOrRegion=Germany,GCPZone=$GCPZone,GCPInstanceId=$GCPInstanceId“

...

# Run connect command
& "$env:ProgramFiles\AzureConnectedMachineAgent\azcmagent.exe" connect --service-principal-id
$env:appId --service-principal-secret $env:password --resource-group $env:resourceGroup --tenant-id
$env:tenantId --location $env:location --subscription-id $env:subscriptionId --tags "$tags“
--correlation-id "d009f5dd-dba8-4ac7-bac9-b54ef3a6671a"
```

Source: @thomasmaurer, blog post

Monitor status and health

Extension-based Management

- **wrapper** for software installation & configuration / small apps providing post-deployment config and automation tasks
- **purpose:** enable services on Arc machines
- **auto-update** in Preview
- only one extension per extension type can be installed/enabled per VM/Arc server
- Check **requirements** for each service!

```
- MicrosoftMonitoringAgent
- DependencyAgentWindows
- CustomScriptExtension
- IaaSAntimalware
- WindowsAgent.AzureSecurityCenter
- KeyVaultForWindows
- WindowsAgent.SqlServer
- AzureMonitorWindowsAgent
- HybridWorkerForWindows
```

```
- OmsAgentForLinux
- DependencyAgentLinux
- CustomScript
- LinuxAgent.AzureSecurityCenter
- KeyVaultForLinux
- AzureMonitorLinuxAgent
- HybridWorkerForLinux
```

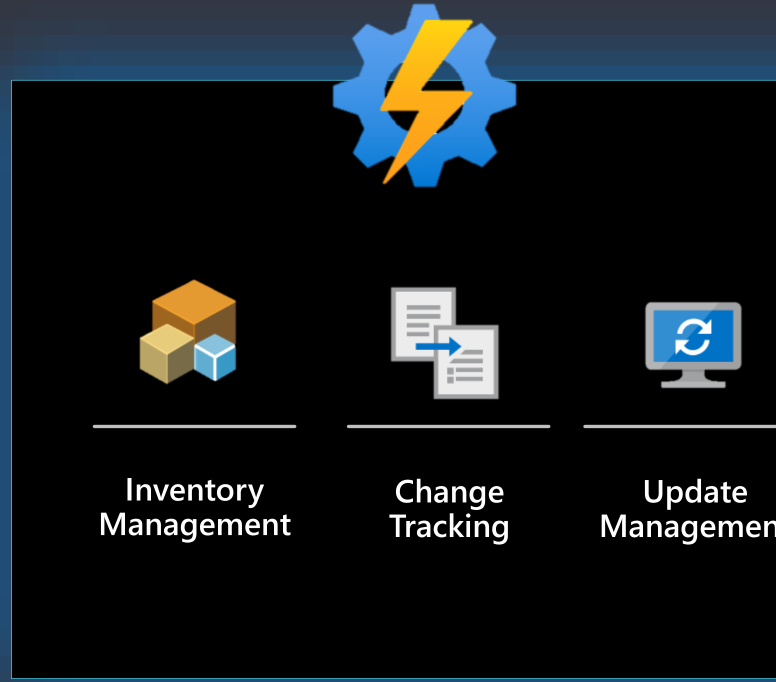
Monitoring agents

- MMA (Log Analytics, OMS) vs. AMA vs. Dependency Agent
  - MMA is used by Azure Monitor, Defender, Sentinel, Automation
- Which one to pick?
- Workspace: RBAC for log data
- Agent deployment “at scale”
- Workbooks and dashboards

Configure and automate

Configure and Automate

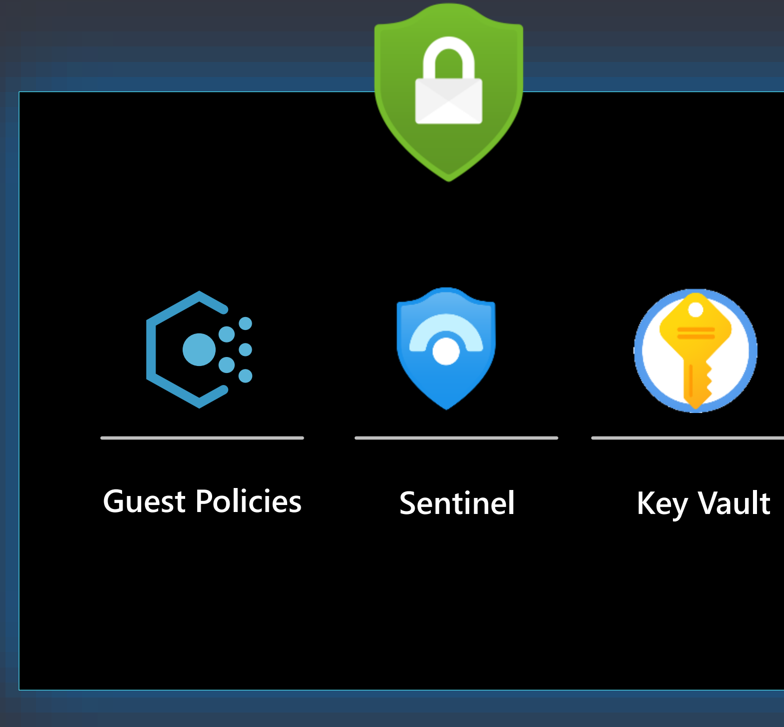
- Azure Automation services
    - Update Management
    - Change Tracking and Inventory
    - Hybrid Runbooks
    - (State Configuration)
- Custom script extension
- Azure Automanage
    - *Not all features are available for Connected Machines*



Protect and secure

Configure and Automate

- Managed Identity and HIMDS
  - *Secret auto-rotation*
- Microsoft Defender for Cloud
  - Advisor recommendations
- Azure Policy Guest configuration
  - Enforce security baseline for OS level
- Microsoft Sentinel
- Key Vault integration and cert management
- Azure Backup



Guest Policies

Sentinel

Key Vault

Offboarding

- Uninstall / disable all extensions first
- Deregister using azcmagent
- Uninstall CMA agent from the server
- Cleanup in Azure:
  - resource group
  - SPN and role assignments
- *Note: collected telemetry doesn't get deleted*

Azure Arc Jumpstart

For meeting Azure Arc customers and partners where they are, we created the Azure Arc Jumpstart project that introduce a ”supermarket” experience by being able to take “off the shelf” automated scenarios and implement it.

- Provide a “zero to hero” scenarios for multiple environments and deployment type using as much automation as possible.
- Ready to go technical demos
- Jumpstart ArcBox is a sandbox environment that allows users to explore all the major capabilities of Azure Arc in a click of a button.
- Jumpstart Lighting is a show where people come to share their Azure Arc/Jumpstart/Hybrid experience.

aka.ms/AzureArcJumpstart

Resources

- **Microsoft Learn** – Manage Hybrid Infrastructure with Azure Arc
  - https://docs.microsoft.com/en-us/learn/paths/manage-hybrid-infrastructure-with-azure-arc/
- Azure Arc Jumpstart **YouTube** channel
  - https://www.youtube.com/channel/UCoIJw-P_9Jp6Jo_0Ca9avcA
- Azure Arc Jumpstart **project site**
  - https://azurearcjumpstart.io/azure_arc_jumpstart/azure_arc_servers/
- **Microsoft Docs** – Azure Arc-enabled servers
  - https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview
- Cloud Adoption Framework – **Landing zone accelerator** for Azure Arc
  - https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/hybrid/enterprise-scale-landing-zone

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2022

nic X edition