



NIC Cloud
Connect

Oslo Spektrum
November 7 - 9

■ Viktor Hedberg



■ Mikael Nystrom

TRUESEC

■ @headburgh



■ @mikael_nystrom

■ MVP



■ MVP

■ 11+ Years



■ More years than Viktor been alive

■ Yes, and a lot...



■ Likes Steak, also tanks.

Azure Arc – Next Gen Server Management

- Azure Arc Agent
- Azure Arc Bridge

The Azure Arc Agent

- Control Plane in Azure
- Uses Extensions
- Licensing is mostly free



The Azure Arc Bridge

- Bridge between Azure and You
- VMware, Hyper-V, Azure Stack
- Uses a Kubernetes cluster
- Licensing is free



The Azure Arc Agent

- Windows Server 2008R2, 2012R2, 2016, 2019, 2022
- Windows 10/11
- Always outbound 443
- Inbound Port Control for listening services

```
Administrator: Windows PowerShell
PS C:\Windows\system32> azcmagent check
INFO Local machine time is: 2023-05-02 22:52:09.5457224 +0200 CEST m=+0.223412101
INFO HIS time is: 230502205209
INFO Difference in time between HIS clock and local clock: 0.009095 minute
ENDPOINT
https://agentserviceapi.guestconfiguration.azure.com |REACHABLE |PRIVATE |TLS |PROXY
https://gbl.his.arc.azure.com |true |false |TLS 1.2 |not used
https://login.microsoftonline.com |true |false |TLS 1.3 |not used
https://login.windows.net |true |false |TLS 1.2 |not used
https://management.azure.com |true |false |TLS 1.2 |not used
https://pas.windows.net |true |false |TLS 1.2 |not used
https://westeurope-gas.guestconfiguration.azure.com |true |false |TLS 1.2 |not used
https://weu.his.arc.azure.com |true |false |TLS 1.2 |not used
PS C:\Windows\system32>
```

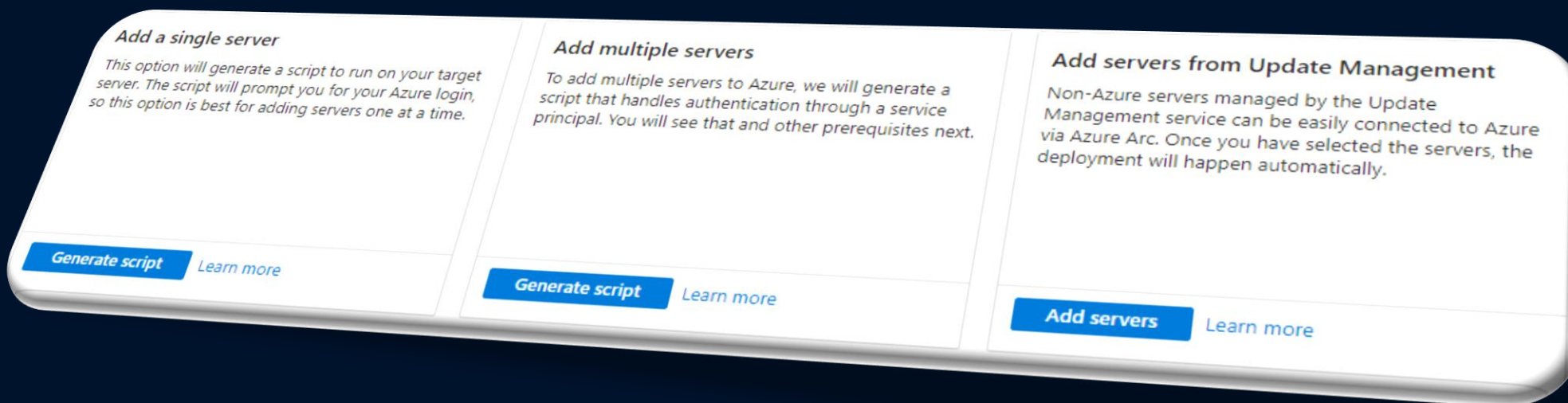
Demo

- Azure Arc Agent



Let's deploy it

- Single Computer = PowerShell script with credentials
- Multiple computer = PowerShell script with Service Principal
- Automation Update Agent...



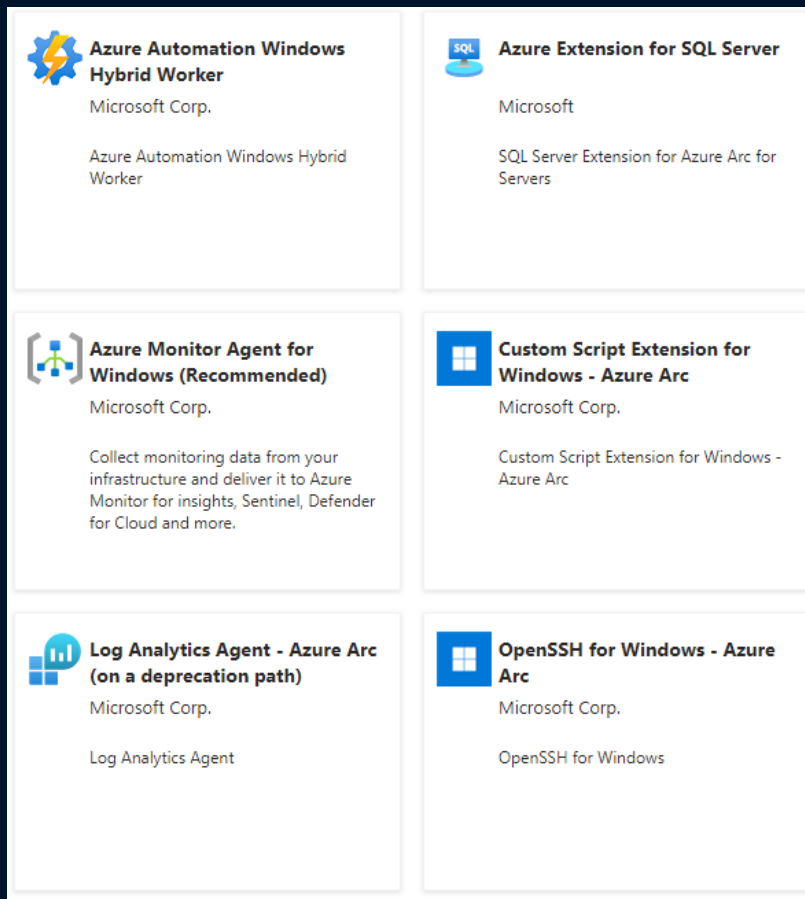
Demo

- Deploy agent



Extensions

- Hybrid Worker
- Azure Monitor
- Log Analytics
- SQL
- Script Extension
- OpenSSH
- Windows Admin Center
- Microsoft Defender for Endpoint
- Windows Patch Extension
- Windows OS Update Extension



Demo

- Extensions



Configuring stuff in Azure

- Log Analytics Workspace
- Azure Automation
- Data Collection Rule
- Defender for Cloud
- Automanage

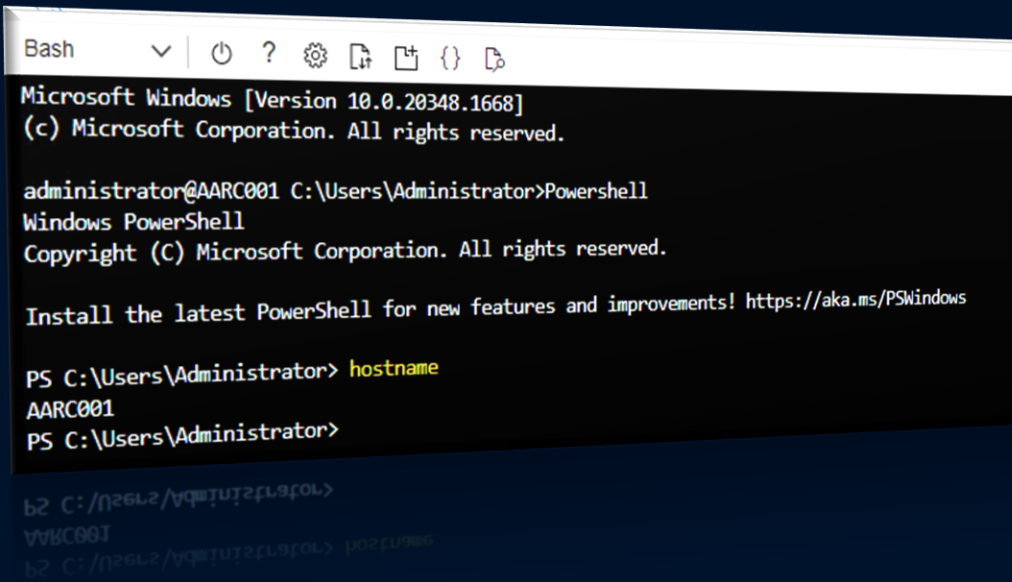
Demo

- Configuring stuff in Azure



Windows Admin Center and SSH

- Moving the control plane to Azure
- Access your servers without the need to be “on” the network, but secure

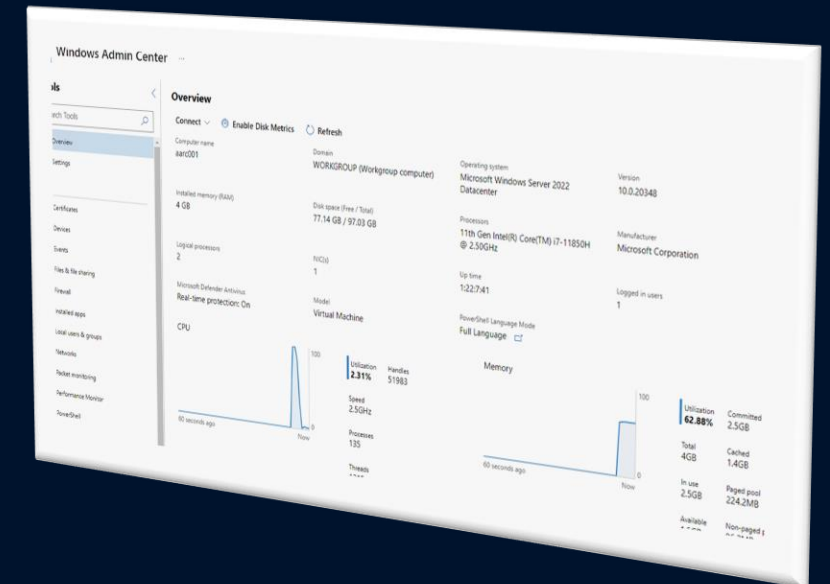
A terminal window titled 'Bash' with a dark background and white text. It shows the execution of 'PowerShell' and 'hostname' commands. The output of 'hostname' is 'AARC001'.

```
Bash
Microsoft Windows [Version 10.0.20348.1668]
(c) Microsoft Corporation. All rights reserved.

administrator@AARC001 C:\Users\Administrator>PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> hostname
AARC001
PS C:\Users\Administrator>
```



Demo

- WAC and SSH



The Azure Arc Bridge

```
Welcome to CBL-Mariner 2.0.20221026 (x86_64) - Kernel 5.15.70.1-1.cm2 (-)
e0752e801ba7809d45e0bfff098b579239fd9c3c2297e-control-plane-0 login: [ OK ] Started Kubernetes Kubelet Server.
[ OK ] Started Kubernetes systemd probe.
[ OK ] Stopping Kubernetes Kubelet Server...
[ OK ] Stopped Kubernetes Kubelet Server.
[ OK ] Started Kubernetes Kubelet Server.
[ OK ] Started Kubernetes Kubelet Server.
[ OK ] Started Kubernetes systemd probe.
ci-info: +-----+Authorized keys from /home/clouduser/.ssh/authorized_keys for user clouduser+-----+
+-----+
ci-info: +-----+
+-----+
ci-info: | Keytype |                               Fingerprint (sha256)                               | Options |
Comment |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
ci-info: | ssh-rsa | 69:51:bc:25:a5:7b:c2:72:1e:d5:ce:b4:a6:9c:17:37:7f:31:8a:70:e3:9b:03:59:92:70:c5:b7:05:c2:f4:8e | - |
- |
ci-info: | ssh-rsa | b1:21:7f:de:ca:b0:c2:31:ee:d4:8c:59:35:45:b4:3c:6d:da:38:d6:69:a9:5d:3f:a2:c2:01:3c:47:9c:5e:a5 | - |
- |
ci-info: +-----+
+-----+
e0752e801ba7809d45e0bfff098b579239fd9c3c2297e-control-plane-0 login: _
603256801P9380394260P1LP038P233S33193C3C55336-control-plane-0 login: _
```


The Azure Arc Bridge

CBL-Mariner Linux

This is the official CBL-Mariner Linux build system. You can use this repository to build a boot-able CBL-Mariner Linux image and use it as an AKS container host, where you can host your Kubernetes containers - Available in AKS (Azure Kubernetes Service).

CBL-Mariner Linux is a lightweight operating system, containing only the packages needed for a cloud environment. CBL-Mariner can be customized through custom packages and tools, to fit the requirements of your application. CBL-Mariner undergoes Azure validation tests, is compatible with Azure agents, and is built and tested by the Azure Edge & Platform to power various use cases, ranging from Azure services to powering IoT infrastructure. CBL-Mariner is the internally recommended Linux distribution for use with Microsoft cloud services and related products.



The Azure Arc Bridge

- The bridge between Azure and you
- Kubernetes services VM that runs in your environment
- Integrates with
 - VMware vSphere
 - System Center Virtual Machine Manager
 - Azure Stack HCI

Demo

- Deploying VMs



Deploying Azure Arc Bridge

- Script based deployment for SCVMM
 - Download and deploy a CBL mariner Image
 - Configure the VM
- It needs “Service Account”, this account will be the “user” that is used by Azure, make sure you have tried it!
- It needs 4 static IP addresses on the same subnet as the SCVMM server
- It requires to be HA, but it asks for it, but you can say no 😊
- It stores all configuration in the account you are using (temp folders)

Configuring Azure Arc Bridge

- Use RGs as a security boundary (just like folders)
- Publish Networks to RGs
- Publish Templates to RGs
- Publish Clouds to RGs
- Publish VMs to RGs
- Set permissions on RGs

Azure Arc Enabled Kubernetes Cluster User Role	List cluster user credentials action.	BuiltinRole
Azure Arc Kubernetes Admin	Lets you manage all resources under cluster/namespace, except update or delete resource quotas and namespaces.	BuiltinRole
Azure Arc Kubernetes Cluster Admin	Lets you manage all resources in the cluster.	BuiltinRole
Azure Arc Kubernetes Viewer	Lets you view all resources in cluster/namespace, except secrets.	BuiltinRole
Azure Arc Kubernetes Writer	Lets you update everything in cluster/namespace, except (cluster)roles and (cluster)role bindings.	BuiltinRole
Azure Arc ScVmm Administrator role	Arc ScVmm VM Administrator has permissions to perform all ScVmm actions.	BuiltinRole
Azure Arc ScVmm Private Cloud User	Azure Arc ScVmm Private Cloud User has permissions to use the ScVmm resources to deploy VMs.	BuiltinRole
Azure Arc ScVmm Private Clouds Onboarding	Azure Arc ScVmm Private Clouds Onboarding role has permissions to provision all the required resources for onboard and deboard vmm server instances to...	BuiltinRole
Azure Arc ScVmm VM Contributor	Arc ScVmm VM Contributor has permissions to perform all VM actions.	BuiltinRole
Azure Arc VMware Administrator role	Arc VMware VM Contributor has permissions to perform all connected VMwarevSphere actions.	BuiltinRole
Azure Arc VMware Private Cloud User	Azure Arc VMware Private Cloud User has permissions to use the VMware cloud resources to deploy VMs.	BuiltinRole
Azure Arc VMware Private Clouds Onboarding	Azure Arc VMware Private Clouds Onboarding role has permissions to provision all the required resources for onboard and deboard vCenter instances to Az...	BuiltinRole
Azure Arc VMware VM Contributor	Arc VMware VM Contributor has permissions to perform all VM actions.	BuiltinRole

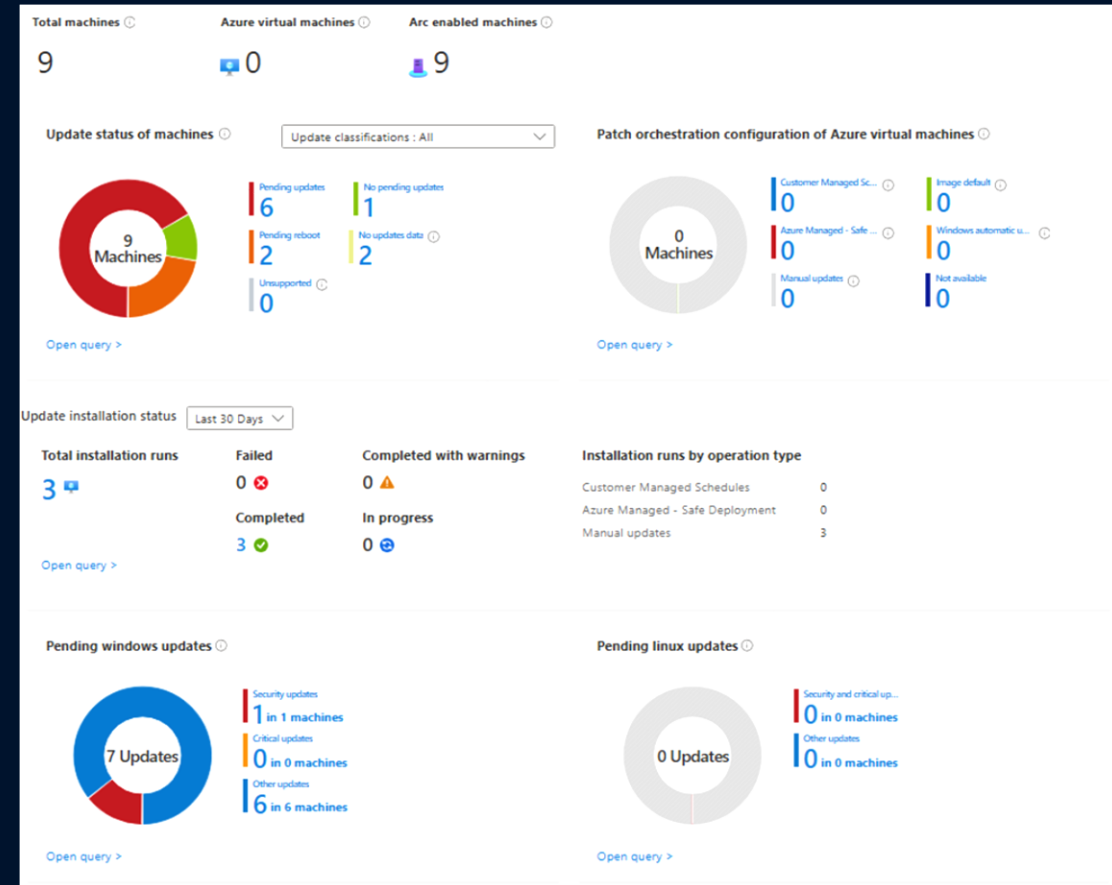
Demo

- Configuring Azure Arc Bridge



Azure Update Manager

- Finally! A server patching solution that works!



Demo

- Azure Update Manager



Thank you!