

# Welcome student, WorkshopPLUS - Azure Arc

---

## Workshop Type

This workshop contains many labs that are not possible to fully complete during the assigned duration with your instructor. It is important to understand what your target is (i.e. which selection of labs you aim to complete within the assigned duration). The targeted lab selection depends on whether your workshop is a Closed or Open one.

A closed workshop usually means that all attendees are from the same organization and that a scoping discussion has been carried out in advance to decide which labs will be focussed on during the workshop. In contrast, an open workshop means that the attendees are from different organizations with no scoping discussion in advance of the workshop delivery.

**Please select the option that applies to you. If you are not sure please ask your instructor: is this an open workshop? [openwps](#)**

\*\*For Open Workshops\*\* The recommended set of labs to attempt during an open workshop are listed below (The first two labs must be carried out before attempting any other labs).

- Lab01: Lab environment deployment - **must be carried out**
- Lab02: Onboarding Windows and Linux Servers to Azure Arc -**must be carried out**
- Lab03: Securing Azure Arc-enabled servers with Microsoft Defender for Cloud
- Lab04: Governance across Azure Arc-enabled servers using Azure Policy and Azure Machine Configuration
- Lab05: Monitor your Azure Arc-enabled servers using Azure Monitor, Change Tracking and Inventory
- Lab07: Keep your Azure Arc-enabled servers patched using Azure Update Manager
- Lab08: Enrol your Windows Server 2012/R2 machines for Extended Security Updates with Azure Arc

We understand that some of the attendees will be experienced in Azure technologies and with the tools used in this workshop. In that case, these users might be able to finish the recommended labs and still have time to attempt the other labs if they wish to do so. Please note that your instructor might prioritize helping attendees who are attempting the recommended labs so please be patient when asking for help. You can also attempt the labs after the end of the workshop within the time allowed for your environment (consult your instructor if you are not sure).

**\*\*For Closed Workshops\*\*** A scoping activity should have been carried out by your instructor with people in your organization to understand your focus areas. This activity should have resulted in an agenda (a minimum set of labs) that you are expected to execute within the workshop. If you do not know this agenda already then consult your instructor. Please follow the suggested labs in your customized agenda first. If you have time after completing those labs, then you can move on to other labs that are of interest to you. Please note that your instructor might prioritize helping attendees who are attempting the labs in the customized agenda, so please be patient when asking for help. You can also attempt the labs after the end of the workshop within the time allowed for your environment (consult your instructor if you are not sure).

## Target Audience

This lab guidance is Level 300 primarily intended for IT professionals, system administrators, and cloud architects seeking to modernize their infrastructure and adopt or optimize their hybrid cloud strategy with Azure Arc. Through those labs, you'll:

- Establish basic level of proficiency in Azure Arc Technologies
- Gain hands-on experience in Azure Arc technology
- Get knowledge on applying Azure native services to Arc-enabled assets with:
  - Security and Governance
  - Management
  - Monitoring and Automation.

## Foreword

If you have any questions or the need for more clarity on what is happening during the lab, please don't hesitate to talk to the trainer.

Good luck!

# Lab Manual

---

## Table of Contents

The following modules are covered in this course. Select the appropriate module.

[LAB01: Lab environment deployment](#)

[LAB02: Onboarding Windows and Linux Servers to Azure Arc](#)

[LAB03: Securing Azure Arc-enabled servers with Microsoft Defender for Cloud](#)

[LAB04: Governance across Azure Arc-enabled servers using Azure Policy and Azure Machine Configuration](#)

[LAB05: Monitor your Azure Arc-enabled servers using Azure Monitor, Change Tracking and Inventory](#)

[LAB06: Gain security insights from your Arc-enabled servers using Microsoft Sentinel](#)

[LAB07: Keep your Azure Arc-enabled servers patched using Azure Update Manager](#)

[LAB08: Enroll your Windows Server 2012/ R2 machines for Extended Security Updates with Azure Arc](#)

[LAB09: This Lab is currently void](#)

[LAB10: Query and inventory your Azure Arc-enabled servers using Azure Resource Graph](#)

[LAB11: Additional automation capabilities for your Azure Arc-enabled servers](#)

[LAB12: Connect a SQL Server to Azure Arc](#)

[LAB13: Connect SQL Servers to Azure Arc using offline MSI installer](#)

[LAB14: Get insights on your Arc-enabled SQL Servers and Databases using the Azure Resource](#)

[LAB15: Enable and run SQL Server best practices assessment](#)

[LAB16: Protect your Arc-enabled SQL Server with Microsoft Defender for Cloud](#)

[LAB17: Select the optimal Azure SQL target using Migration Assessment](#)

# LAB01: Lab environment deployment

---

## Student Lab Manual

### Table of Contents

Exercise 1: Get familiar with your workshop environment

**Task 1 - View your workshop credentials and log into the workshop machine**

Exercise 2 - Lab pre-requisites

**Task 1 - Prepare the local development environment for lab deployment and login to Azure**

**Task 2 - Enable the Defender for Servers plan**

Exercise 3 - ArcBox deployment

**Task 1 - Deploy ArcBox using the Azure Portal**

**Task 2 - Connecting to the ArcBox Client virtual machine**

**Task 3 - Post-deployment automation**

# Exercise 1: Get familiar with your workshop environment

---

## **Objective**

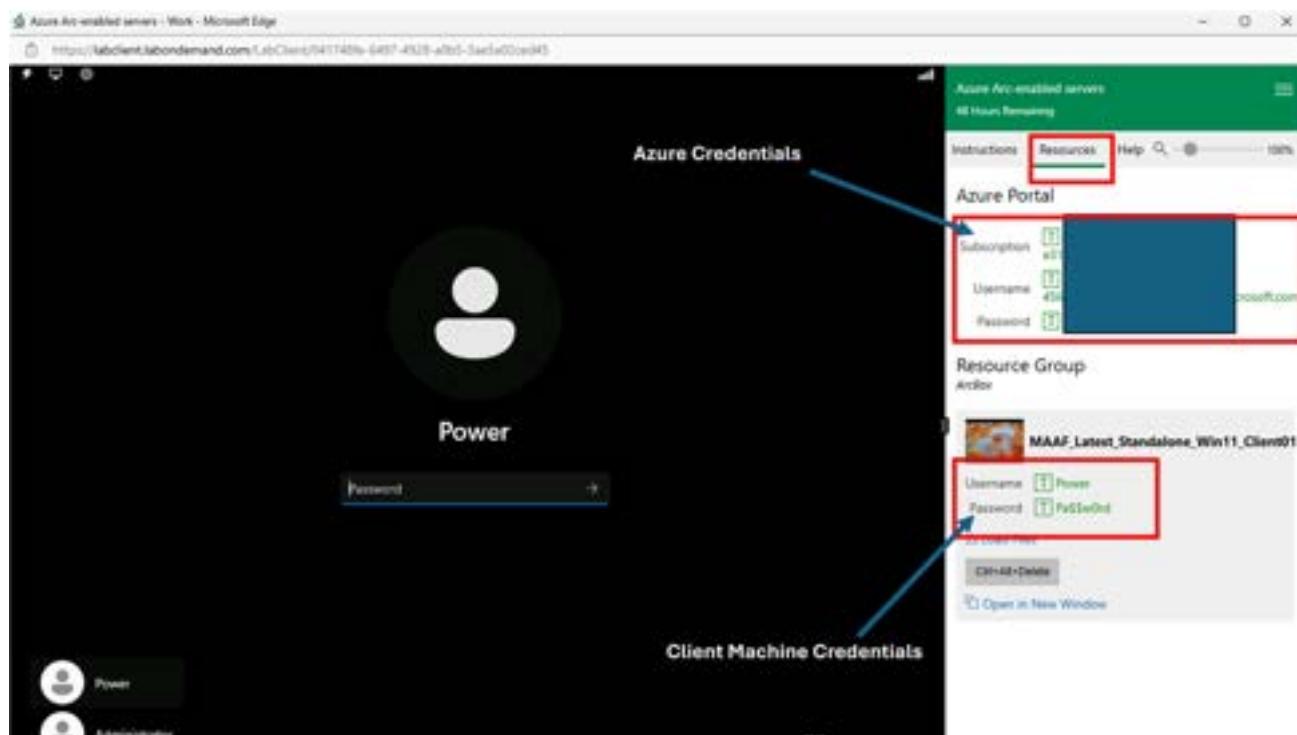
This lab will guide you through the necessary steps to set up your Azure environment.

## **Estimated Time to Complete This Lab**

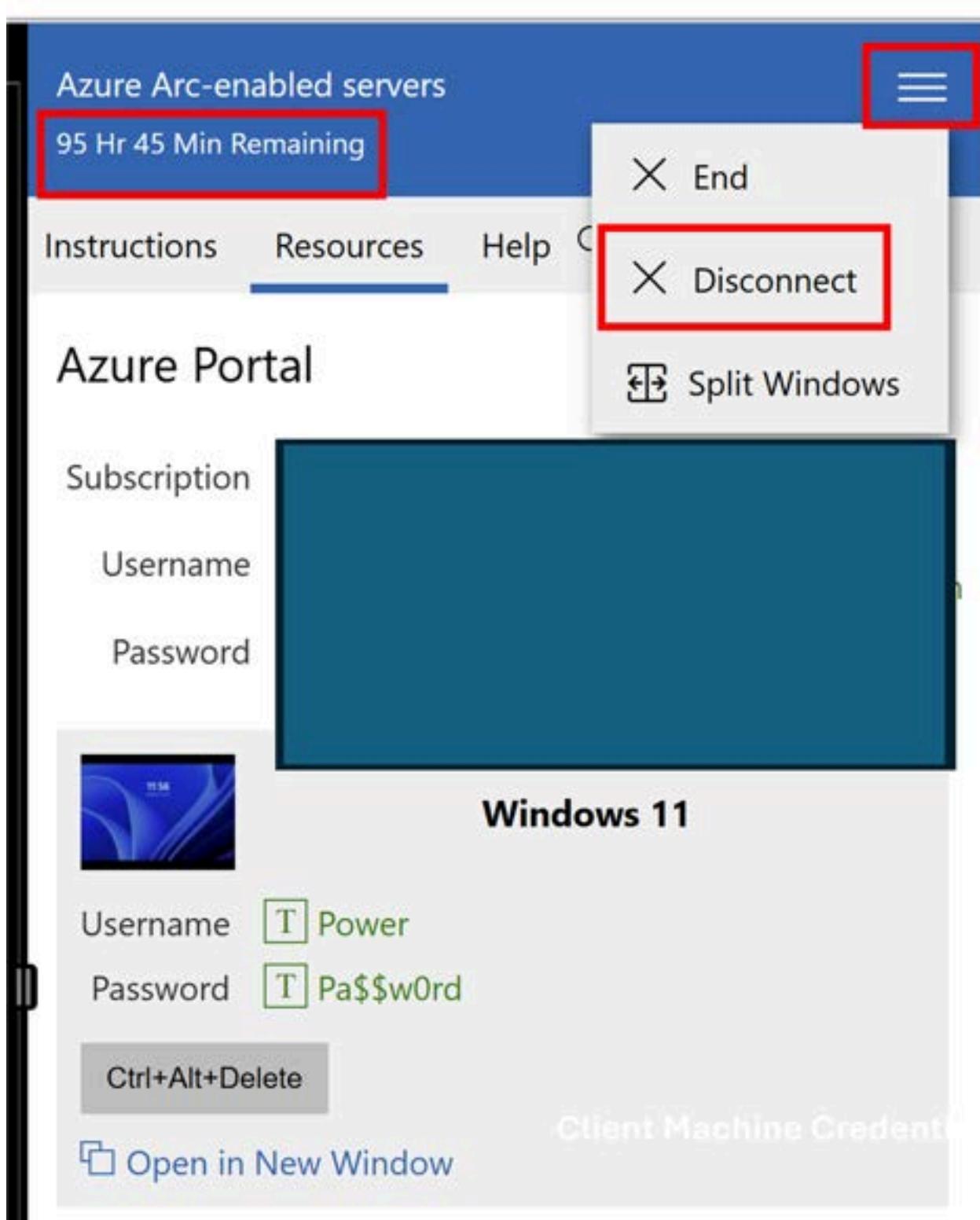
15 minutes

## Task 1: View your workshop credentials and log into the workshop machine

This lab is based on a Windows Client machine provisioned for you in the learning platform. At the top of this Instructions window, there is a menu bar with three items: **Instructions**, **Resources** and **Help** as well as a Zoom function. On the *Resources* tab you should see both the local lab machine credentials and also the Azure credentials.



- Do not use the **END** option as it will destroy your Azure resources and end your lab. Use the **Disconnect** option when you want to take a break from the lab. Your lab timer shows how long you have left before your lab is terminated.



- Notice that on this tab, and throughout the instructions for this lab, you will find **squares with a capital T inside the square. This option can be used to have the lab type text for you.** If your cursor is in the password box of the login screen, and if you click on the square box with the T in it, the lab will type the password for you. This typing can be used throughout the lab and the text will appear wherever your cursor is located. **However, please note that this might not work for**

**copying into Azure CloudShell and you will need to use Copy and Paste with the mouse right-click.**

Now log into the client machine and start with the first task of this lab. Have fun!

## Exercise 2 - Lab pre-requisites

---

### **Objective**

This exercise will walk you through preparing your local development environment to deploy the lab environment using the ArcBox sandbox.

### **Estimated Time to Complete This Lab**

15 minutes

### **Explanation**

ArcBox is a solution that deploys a complete sandbox environment with Windows and Linux machines simulating an on-premises environment. One of the Windows machines will be running a SQL Server. You will Arc-enable those machines and explore the different capabilities provided through Azure Arc. You will deploy ArcBox using the Azure Portal.

## Task 1: Prepare the local development environment for lab deployment and log into Azure

---

- Important:** Make sure that you carry out the steps in the Windows machine provided by the lab environment and not your local PC.
- 1. Make sure that you have the x64 version of Azure CLI version 2.66.0 or above. Start PowerShell as administrator and run the following command:

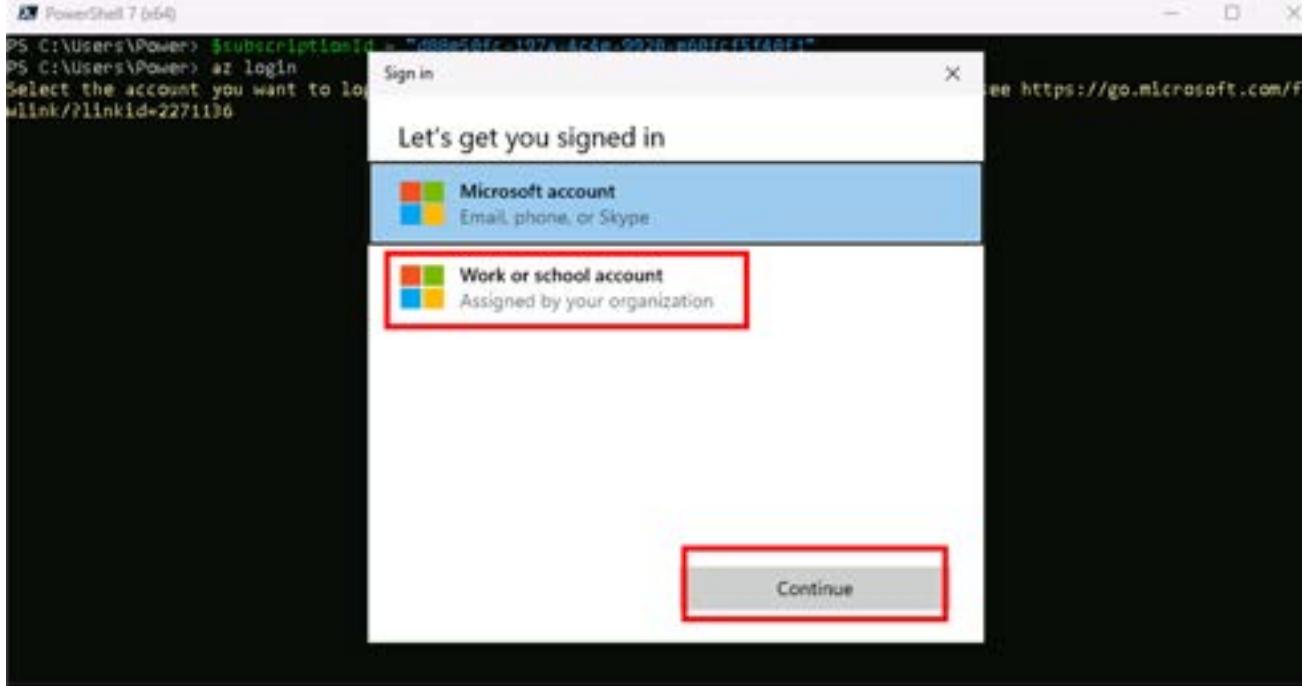
```
shell
▶ az --version
```

The output should confirm that you have the Azure CLI installed. If not then you can install it using the following command.

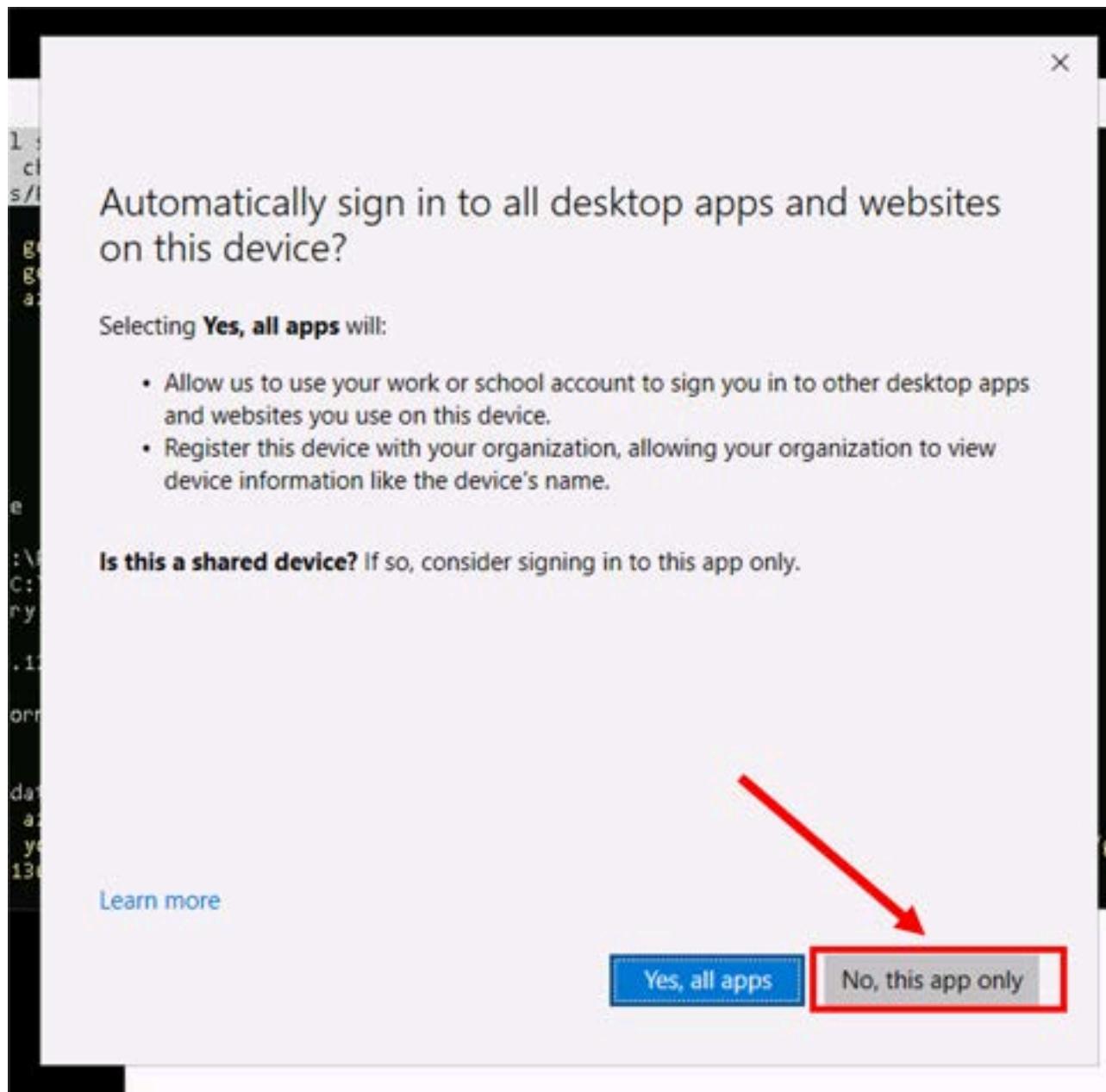
```
PowerShell
▶ $ProgressPreference = 'SilentlyContinue'; Invoke-WebRequest -Uri https://aka.ms/
```

- 2. Login to AZ CLI using the `az login` command. If you are prompted to choose an account type then select *Work or school account*.

```
shell
▶ az login
```



- You can use Notepad or Visual Studio Code for the rest of the commands to be able to edit the needed parameters in an easier way than the PowerShell console**
  
- 3. If you are prompted to *Automatically sign in to all desktop apps and websites on this device* select ***No, this app only***



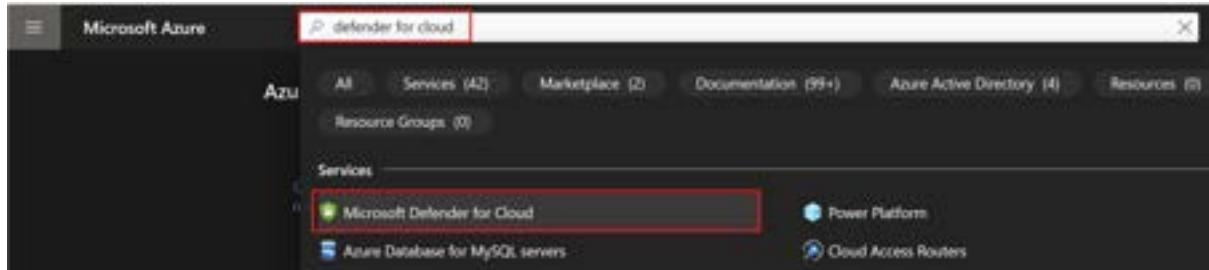
**Task 1 has been completed**

## Task 2: Enable Defender for Servers on your subscription

- 1. Open the EDGE browser and navigate to the Azure portal then log into Azure with lab provided credentials from the **Resources** tab

shell  
▶ <https://portal.azure.com>

- 2. From the Azure home page, search for defender and select Microsoft Defender for Cloud.



- 3. If you already have Defender plans setup at your subscription level, you may find that Defender is already turned on for your Arc-enabled servers. However, if Defender is not enabled, select *Environment settings* from the Management section on the left blade.

A screenshot of the Microsoft Defender for Cloud | Environment settings blade. The left sidebar shows 'Management' expanded, with 'Environment settings' selected (marked with a red circle labeled '1'). Other options in the sidebar include 'General', 'Cloud Security', 'Security solutions', and 'Workflow automation'. The main area displays a table of environment settings. The table has columns for 'Name', 'Total resources', 'Connectivity status', and 'Defender coverage'. The table shows several entries under the 'Azure' category, including 'Tenant Root Group', 'LOG', 'SSG Shared Development', 'SSG CSS - Dev', 'Lab Profiles', and 'Lab Profile 175106' (marked with a red circle labeled '2'). The 'Lab Profile 175106' row is highlighted with a red box.

- 4. Expand the Tenant Root Group, and then select **your subscription**.
- 5. Enable the plan for servers, you can select either *Plan 1* or *Plan 2* for this exercise

The screenshot shows the Microsoft Defender for Cloud Settings | Defender plans page. It includes sections for Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP). Under CSPM, there are two plans: 'Foundational CSPM' (Free) and 'Defender CSPM'. Under CWP, there is one plan: 'Plan 1 (3U/Server/Month)' (Change plan). The 'Monitoring coverage' section for Plan 1 has three settings: 'Vulnerability assessment for machines' (ON), 'Endpoint protection' (ON), and 'Agentless Scanning for machines' (OFF).

- 6. Click on the settings option in the *Monitoring coverage* and set the following capabilities as indicated:
- Vulnerability assessment for machines - **ON**.
  - Endpoint protection - **ON**.
  - Agentless Scanning for machines - **OFF**.

The screenshot shows the Microsoft Defender for Cloud Settings & monitoring page. It lists several components and their configurations:

- Log Analytics agent: 'Agent is in deployment path' (Learn more)
- Vulnerability assessment for machines: 'Manually manage Microsoft Defender vulnerability' (ON)
- Guest Configuration agent (optional): 'Deploy the agent to Azure virtual machines, hybrid-machines connected to Azure Arc, directly have this agent included in your Azure Container Instances, Learn more about the Guest Configuration agent, or Learn more about Container Configuration'
- Endpoint protection: 'Automatically manage Microsoft Defender for Endpoint'
- Agentless scanning for machines: 'Automatically manage Microsoft Defender for Cloud'
- File integrity Monitoring: 'Automatically manage File integrity monitoring (FIM), also known as change monitoring, monitors operating system files, Windows registry, application software, Linux system files, and more, for changes that might indicate an attack.'

Each configuration has a 'Status' indicator at the end of the row.

- 7. Click *Continue* then Click *Save*.

Home | Microsoft Defender for Cloud | Management settings

## Settings | Defender plans

Management

Search  Save View Settings & monitoring

Settings

- Defender plans
- Email notifications
- Workflow automation
- Continuous export

Policy settings

- Security policy
- Governance rule

**Cloud Security Posture Management (CSPM)**

Microsoft Defender CSPM provides advanced security posture management including agentless vulnerability scanning, data breach security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing existing only for servers, Database, and Storage resources at \$1/Month/resource.

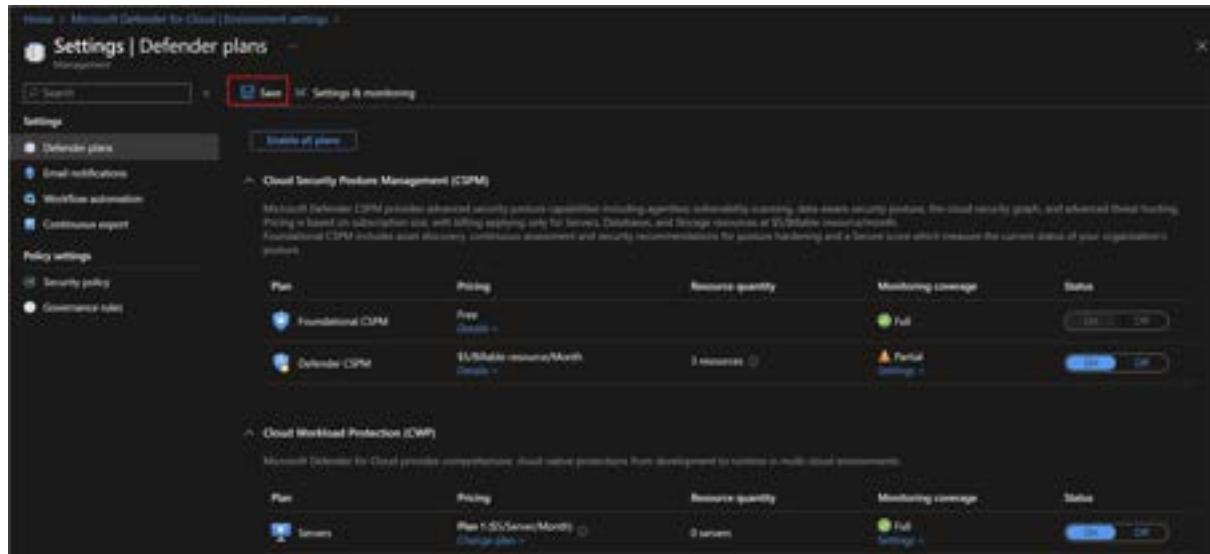
Foundational CSPM includes asset discovery, continuous assessment, and security recommendations for posture hardening and a Service Score which measures the current status of your organization's posture.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free <a href="#">Details</a>	3 resources	<span style="color: green;">Full</span>	<a href="#">Edit</a> <a href="#">Delete</a>
Defender CSPM	\$1/Month/resource/Month <a href="#">Change plan</a>	0 resources	<span style="color: orange;">Partial</span> <a href="#">Settings</a>	<a href="#">Edit</a> <a href="#">Delete</a>

**Cloud Workload Protection (CWP)**

Microsoft Defender for Cloud provides comprehensive cloud native protection from development to runtime in multi-cloud environments.

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Servers	\$1/Servers/Month <a href="#">Change plan</a>	0 servers	<span style="color: green;">Full</span> <a href="#">Settings</a>	<a href="#">Edit</a> <a href="#">Delete</a>



**Task 2 has been completed**

# Exercise 3 - ArcBox deployment

---

## **Objective**

In this exercise you will deploy the lab using the ArcBox solution which will deploy all the needed Azure resources to your subscription to be able to execute all the upcoming exercises.

## **Estimated Time to Complete This Lab**

45 minutes

## **Explanation**

ArcBox is a solution that deploys a complete sandbox environment with Windows and Linux machines simulating an on-premises environment. One of the Windows machines will be running a SQL Server. You will Arc-enable those machines and explore the different capabilities provided through Azure Arc. You will deploy ArcBox using the Azure Portal.

## Task 1: Deploy ArcBox using the Azure Portal

- 1. The specific setup of ArcBox used in this workshop can be deployed in any region that supports the Azure virtual machine SKU required (Standard\_E8s\_v5, v4 or v3). Occasionally, there might be restrictions on specific subscriptions that can prevent the deployment of a specific SKU even if it is available in a region. To check if there are any restrictions on your subscription you can run the following PowerShell command in **Azure Cloud Shell**. You can change the list of locations in the script if necessary by adding or removing regions. But **do not change the list of VM Skus**. If you prefer to run the command from the lab machine then make sure you login in PowerShell first using `Connect-AzAccount` command.

```
PowerShell
▶ $locations = "uksouth", "northeurope", "eastus", "eastus2", "centralus"
#Do not change the VMSKUs below
$VmSkus = "Standard_E8s_v5", "Standard_E8s_v4", "Standard_E8s_v3"
$locations | ForEach-Object -ThrottleLimit 10 -Parallel {
    Get-AzComputeResourceSku -Location $_ | Where-Object {$_[']. ResourceType -eq "
    }
```

The output will show if there are restrictions in any of the listed regions or in specific zones in the region (for a multi-zone region). Choose a region and VM Sku combination that has no restrictions to deploy the lab VM. For example, in the following diagram we can see that *uksouth* is a very good candidate to deploy the lab. On the other hand *centralus* is not because of the full restrictions. The *northeurope* region has restrictions only in zone 3 so it should allow you to deploy.

ResourceType	Name	Location	Zone	RestrictionInfo
VirtualMachines	Standard_E8s_v3	uksouth	{2, 1, 3}	
VirtualMachines	Standard_E8s_v4	uksouth	{2, 1, 3}	
VirtualMachines	Standard_E8s_v3	uksouth	{2, 1, 3}	
VirtualMachines	Standard_E8s_v7	centralus	{2, 1, 3}	type: Location, locations: centralus, type: Zone, locations: centralus, zones: 1, 2, 3)
VirtualMachines	Standard_E8s_v4	centralus	{2, 1, 3}	type: Location, locations: centralus, type: Zone, locations: centralus, zones: 1, 2, 3)
VirtualMachines	Standard_E8s_v5	centralus	{2, 1, 3}	type: Location, locations: centralus, type: Zone, locations: centralus, zones: 1, 2, 3)
VirtualMachines	Standard_E8s_v3	eastus2	{2, 1, 3}	type: Zone, locations: eastus2, zones: 1
VirtualMachines	Standard_E8s_v4	eastus2	{2, 1, 3}	type: Zone, locations: eastus2, zones: 1
VirtualMachines	Standard_E8s_v5	eastus2	{2, 1, 3}	type: Zone, locations: eastus2, zones: 1
VirtualMachines	Standard_E8s_v7	eastus	{1, 3, 2}	type: Location, locations: eastus, type: Zone, locations: eastus, zones: 1, 2, 3)
VirtualMachines	Standard_E8s_v4	eastus	{1, 2, 3}	type: Location, locations: eastus, type: Zone, locations: eastus, zones: 1, 2, 3)
VirtualMachines	Standard_E8s_v5	eastus	{1, 2, 3}	type: Location, locations: eastus, type: Zone, locations: eastus, zones: 1, 2, 3)
VirtualMachines	Standard_E8s_v3	northeurope	{1, 3, 2}	type: Zone, locations: northeurope, zones: 3
VirtualMachines	Standard_E8s_v4	northeurope	{2, 1, 3}	type: Zone, locations: northeurope, zones: 3
VirtualMachines	Standard_E8s_v5	northeurope	{2, 1, 3}	type: Zone, locations: northeurope, zones: 3

- Make sure that you have selected a region with no restrictions on the required virtual machine sku (as explained above). Failure to do so might cause your deployment to fail. You will need to enter the name of the selected region and VM SKU in the deployment template in the next step.**

- 2. Open the Microsoft Edge browser and paste the following URL.

 <https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FAzur>

- 3. Enter values for the the template parameters then click *Review + create*.



**The only acceptable resource group name is *ArcBox*. If you choose any other name then your deployment will fail.**

- Make sure to note the Windows admin username and password as you will use them in later exercises. In order to avoid using a username and password combination that does not meet the complexity requirements which would lead to the failure of the deployment, we recommend using the username **arcdemo** and the password **Arcboxlabs@12345**.
- Review the [complexity requirements](#) for the Windows virtual machine's password

# Custom deployment

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →



Customized template

6 resources

Edit template

Edit parameters

Visualize

## Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription • ⓘ

Resource group • ⓘ

ArcBox

Create new

## Instance details

Region • ⓘ

Check Restrictions before selecting region

Spn Tenant Id ⓘ

[tenant().tenantid]

Client Vm Sku • ⓘ

Check Restrictions before selecting SKU

Windows Admin Username • ⓘ

Windows Admin Password • ⓘ

Log Analytics Workspace Name • ⓘ

Github Account ⓘ

Azure

Github Branch ⓘ

main

Rdp Port ⓘ

3389

Ssh Port ⓘ

22

Email Address • ⓘ

Location

[resourceGroup().location]

Previous

Next

Review + create

The screenshot shows the Azure portal's deployment overview page for a template named "Microsoft.Template-20210416134842". The status is "Deployment is in progress". Deployment details include a start time of 4/16/2021, 14:45 PM, and a correlation ID of 29d135b-f1d9-432c-a625-7ef8f58e034a. The deployment is for a Microsoft Azure Internal Consumption Resource group. A "Deployment details" section is expanded, showing a table with columns: Resource, Type, Status, and Operation details. The table has one row labeled "No results.". On the right side, there are promotional banners for Security Center, Microsoft tutorials, and Azure experts.

The screenshot shows the Azure portal's deployment overview page for the same template. The status is now "Your deployment is complete". Deployment details show a start time of 4/16/2021, 14:45 PM, and a correlation ID of 29d135b-f1d9-432c-a625-7ef8f58e034a. The deployment is for the "Artiles" resource group. A "Next steps" button is visible at the bottom. The right side features the same promotional banners as the previous screenshot.

- The deployment takes around 20 minutes to complete.
- If you see any failure in the deployment, please check that you have selected a region with no restrictions on the virtual machine sku and consult your workshop instructor. In some cases a transient issue might cause a deployment error. The best action in these cases is to redeploy the template. **Make sure that you delete the whole resource group (not only the resources inside it) and once the deletion is completed you can redeploy the template.**

### Task 1 has been completed

## Task 2: Connecting to the ArcBox Client virtual machine

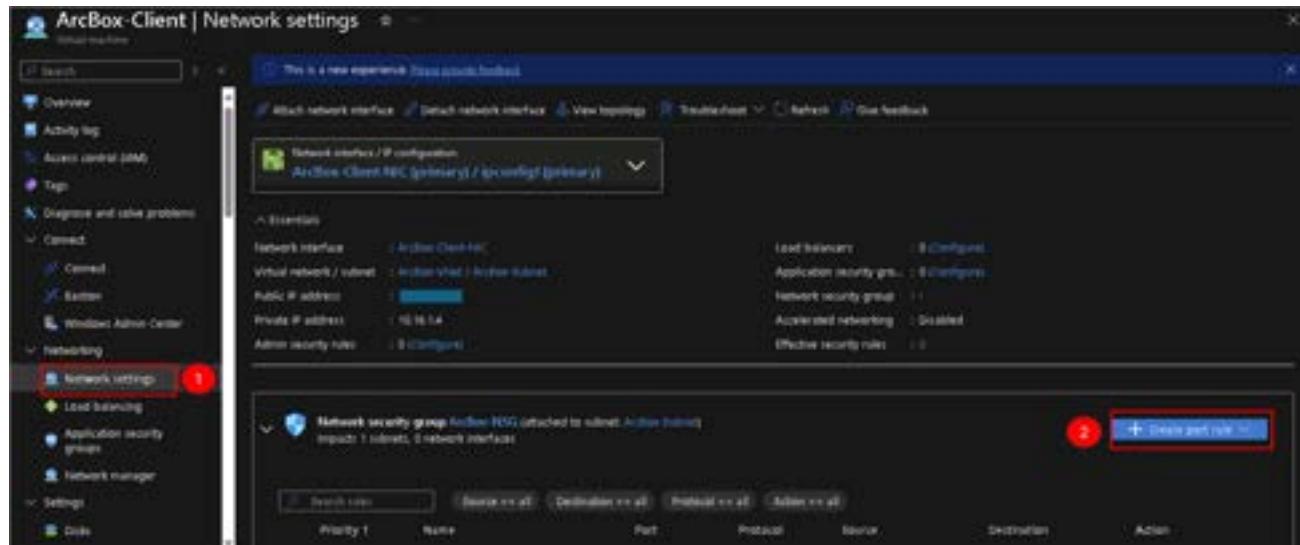
Various options are available to connect to *ArcBox-Client* VM on Azure. However, for this lab you will use the direct RDP method - available after configuring access to port 3389 on the *ArcBox-NSG* Network Security Group.

- Once you have logged on to the *ArcBox-Client* VM you might see some Powershell scripts in the process of being executed. DO NOT close any windows or stop any scripts. The set-up automation will close the completed windows automatically

### Connecting directly with RDP

By design, ArcBox does not open port 3389 on the network security group. Therefore, you must create an NSG rule to allow inbound 3389.

- 1. Open the *Network settings* for the *ArcBox-Client* machine in the Azure portal and click *Create port rule* to add a new inbound rule.



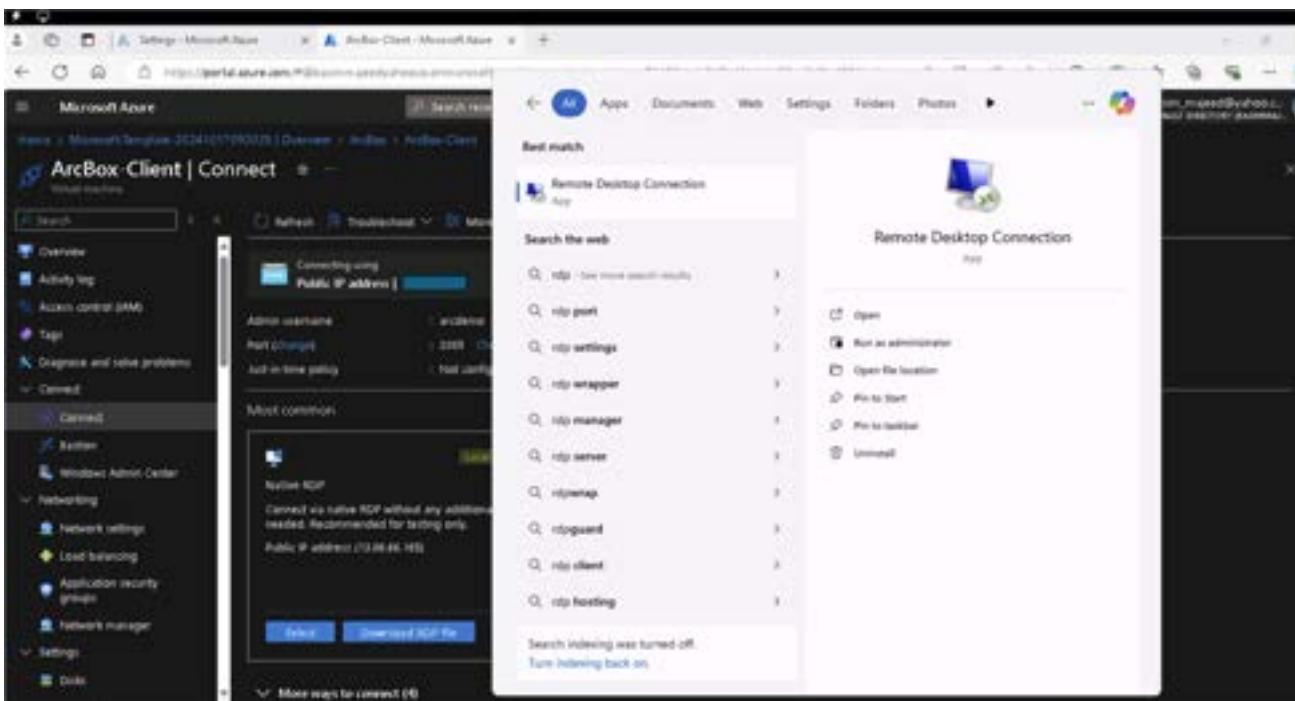
This screenshot shows the 'Network settings' page for an ArcBox-Client machine. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Connect, Connect, Windows Admin Center, Networking, Network settings, Load balancing, Application security group, Network manager, Settings, and Disk. The 'Network settings' item is selected. The main pane displays network details: Virtual network / subnet (ArcBox-Client / ArcBox-Subnet), Public IP address (10.16.14), Private IP address (10.16.14), and Admin security rules (0 Configured). It also shows Application security group (ArcBox-RSG) attached to subnet, Network security group (ArcBox-RSG), Accelerated networking (Disabled), and Effective security rules (0). Below this, a 'Network security group ArcBox-RSG (attached to subnet: ArcBox-Subnet)' section is shown, with a 'Create port rule' button and a 'Inbound port rule' link highlighted with a red box. A table lists inbound port rules:

Priority	Name	Port	Protocol	Source	Destination	Action
40000	AllowRDP	Any	Any	10.16.14/32	10.16.14/32	Allow
40001	AllowHyperVManagement	Any	Any	10.16.14/32	Any	Allow
40002	DenyAll	Any	Any	Any	Any	Deny

2. Specify the IP address that you will be connecting from (or use *My IP address*) and select RDP as the service. If you need to retrieve your public IP address (not required if you use the *My IP address* setting) then you can do so by accessing <https://icanhazip.com> or <https://whatsmyip.com>.

This screenshot shows the 'Network settings' page for an ArcBox-Client machine, similar to the previous one but with a different configuration. The 'Source IP' dropdown is set to 'My IP address'. The 'Service' dropdown is set to 'RDP'. The 'Protocol' dropdown has 'Any' selected. The 'Add' button is highlighted with a red box. Other settings like 'Source IP address and CIDR range', 'Source port range', 'Destination port range', and 'Protocol' (TCP, UDP, User-defined) are visible.

3. Now you can run the Remote Desktop Connection App and connect to the *ArcBox-Client* machine using the user name and password that you have set on the deployment template.

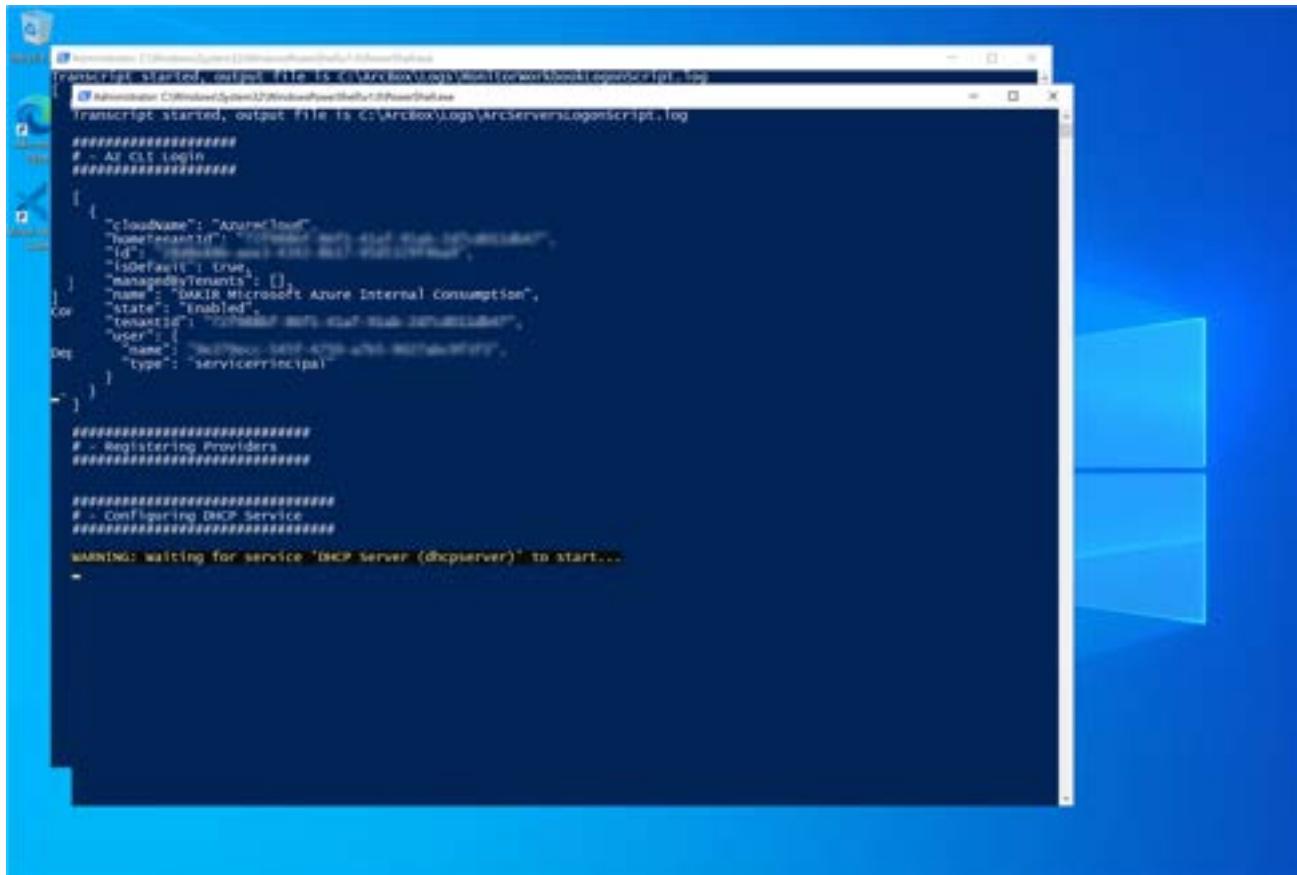


**Task 2 has been completed**

## Task 3: Post-deployment automation

---

- 1. Once you log into the *ArcBox-Client* VM, multiple automated scripts might be open and running. These scripts usually take 10-20 minutes to finish (**Do not close any windows and do not stop any running scripts!**), and once completed, the script windows will close automatically. At this point, the deployment is complete.



```
Administrator: C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
Transcript started, output file is C:\Arcbox\Logs\Arcservers\logonscript.log
Administrator: C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe
Transcript started, output file is C:\Arcbox\Logs\Arcservers\logonscript.log

# ~ AD CS Login
#####
# ~ Tenant
{
    "id": "00000000-0000-0000-0000-000000000000",
    "name": "AzureCloud",
    "tenantId": "72f988bf-6c4e-4673-8ff0-0ad83dd02d7e",
    "state": "Enabled"
}
# ~ User
{
    "id": "00000000-0000-0000-0000-000000000001",
    "name": "MKIB Microsoft Azure Internal Consumption",
    "state": "Enabled"
}
# ~ ServicePrincipal
{
    "id": "00000000-0000-0000-0000-000000000002",
    "name": "MKIB Microsoft Azure Internal Consumption",
    "type": "serviceprincipal"
}

#####
# ~ Registering Providers
#####

#####
# ~ Configuring DHCP Service
#####

WARNING: Waiting for service 'DHCP server (dhcpserver)' to start...
```

- 2. Deployment is complete when you see the following screen background! Let's begin exploring the features of Azure Arc-enabled servers with the other labs in this workshop.



**Task 3 has been completed**

**Congratulations, you have completed all tasks in this lab**

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB02: Onboarding Windows and Linux Servers to Azure Arc

---

## Student Lab Manual

### Table of Contents

Exercise 1 - Examine the existing Arc-connected machines

**Task 1 - Use the Azure portal to examine your Arc-enabled machines inventory**

**Task 2 - Examine the virtual machines that you will Arc-enable**

Exercise 2 - Onboard a Windows and a Linux machine to Azure Arc

**Task 1 - Generate a script to automate the download and installation of the Azure Arc connected machine agent for a Windows machine, and connect the machine to Azure Arc**

**Task 2 - Connect a Linux machine to Azure Arc using the direct internet access (without a proxy)**

**Task 3 - Connect a Linux machine to Azure Arc using a proxy and Arc Gateway**

# Exercise 1 - Examine the existing Arc-connected machines

---

## **Objective**

The deployment process that you have walked through in Lab01 should have set up a number of VMs running on Hyper-V in the ArcBox-Client machine. Two of these machines have been connected to Azure Arc for you by the set script. In this exercise you will verify that these two machines are indeed Arc-enabled and you will identify the other machines that you will Arc-enable.

## **Estimated Time to Complete This Lab**

10 minutes

## **Explanation**

The Arc-connected machines can be viewed on the Azure portal.

## Task 1: Use the Azure portal to examine your Arc-enabled machines inventory

- 1. Enter "Machines - Azure Arc" in the top search bar in the Azure portal and select it from the displayed services.

The screenshot shows the Microsoft Azure portal's search interface. The search bar at the top contains the text "Machines - Azure Arc" with a red circle containing the number 1 above it. Below the search bar, a list of services is displayed. The "Machines - Azure Arc" service is highlighted with a red box and the number 2 above it. Other visible services include "Virtual machines", "Azure Active Directory", "Azure Cosmos DB", "Virtual machine - Azure Arc (preview)", and several Azure Database and SQL-related services. The portal has a dark theme with light-colored text and icons.

- 2. You should see the machines that are connected to Arc already: *Arcbox-Ubuntu-01* and *ArcBox-Win2K25*.

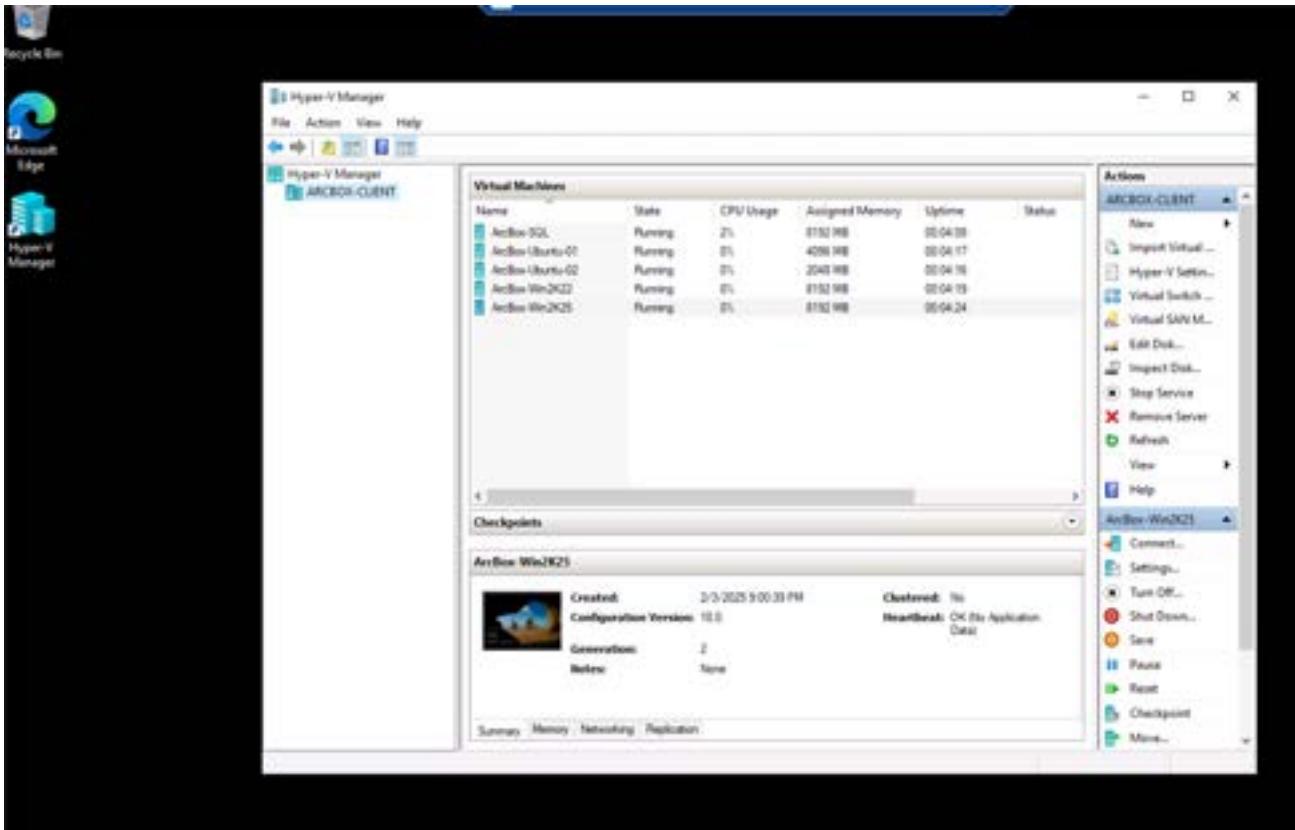
The screenshot shows the "Azure Arc | Machines" blade in the Azure portal. On the left, there is a navigation menu with sections like "Overview", "All Azure Arc resources", "Azure Arc resources", "Host environments", "Data services", and "SQL Server instances". The "Azure Arc resources" section is expanded, and the "Machines" item under it is highlighted with a red box. On the right, a table displays two records. The columns are "Name", "Kind", "Arc agent status", "Resource group", "Subscription", "Operating system", "Defender endpoint", and "Monitoring system". The two entries are:

Name	Kind	Arc agent status	Resource group	Subscription	Operating system	Defender endpoint	Monitoring system
Arcbox-Ubuntu-01	Ubuntu	Connected	devTestRG	Azure Dev Test Lab	Ubuntu 22.04.4 LTS	Enabled	Enabled
ArcBox-Win2K25	Windows	Connected	arcboxrg	Azure Dev Test Lab	Windows Server 2019	Enabled	Enabled

**Task 1 has been completed**

## Task 2: Examine the virtual machines that you will Arc-enable

- 1. You want to connect 2 more machines running as VMs in the ArcBox-Client. You can see these (ArcBox-Win2K22 and ArcBox-Ubuntu-02) by running the Hyper-V Manager in the ArcBox-Client (after you have connected to it with RDP as explained earlier in Lab01).



**Task 2 has been completed**

# Exercise 2 - Onboard a Windows and a Linux machine to Azure Arc

---

## Objective

In this exercise you will onboard the Windows machine ArcBox-Win2K22 and the Linux machine ArcBox-Ubuntu-02 to Azure Arc using the Service Principal onboarding method.

## Estimated Time to Complete This Lab

60 minutes

## Explanation

Connecting machines in your hybrid environment directly with Azure can be accomplished using different methods, depending on your requirements and the tools you prefer to use. One method to connect the machines to Azure Arc is to use a Microsoft Entra ID service principal. This service principal is a special limited management identity that has only the minimum permission necessary to connect machines to Azure. This method is safer than using a higher privileged account like a Subscription Contributor and follows access control security best practices. The service principal is used only during onboarding; it is not used for any other purpose.

The Azure Connected Machine agent for Linux and Windows communicates outbound securely to Azure Arc over TCP port 443. By default, the agent uses the default route to the internet to reach Azure services. You can optionally configure the agent to use a proxy server if your network requires it. There are a number of URLs that must be available in order to install and use the Connected Machine agent and onboard the machine to Azure Arc. The proxy must be configured to allow all these URLs including ones containing wildcards. However, the number of URLs can be consolidated using the Azure Arc Gateway service which reduces the number of URLs to a small set of endpoints that need to be allowed by the proxy.

In Task 1 of this exercise you will learn how to onboard a Windows machine to Azure Arc using direct internet access (without a proxy).

You will then learn how to onboard a Linux machine to Azure Arc using either the direct internet access (without a proxy) in task 2 or using a proxy together with the Azure Arc Gateway in task 3.

- For onboarding the Linux machine to Azure Arc, it is important to follow either Task 2 or Task 3.**

## Documentation

[Azure Connected Machine agent deployment options.](#)

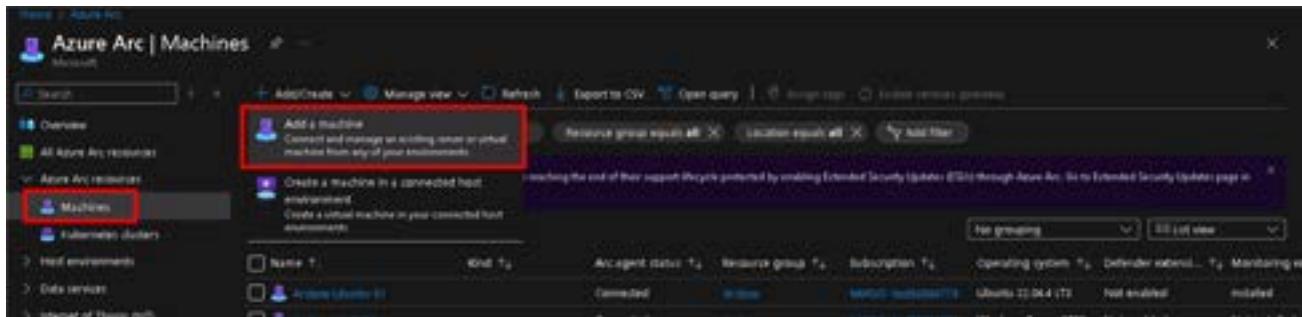
[Connect hybrid machines to Azure at scale.](#)

[Connected Machine agent network requirements](#)

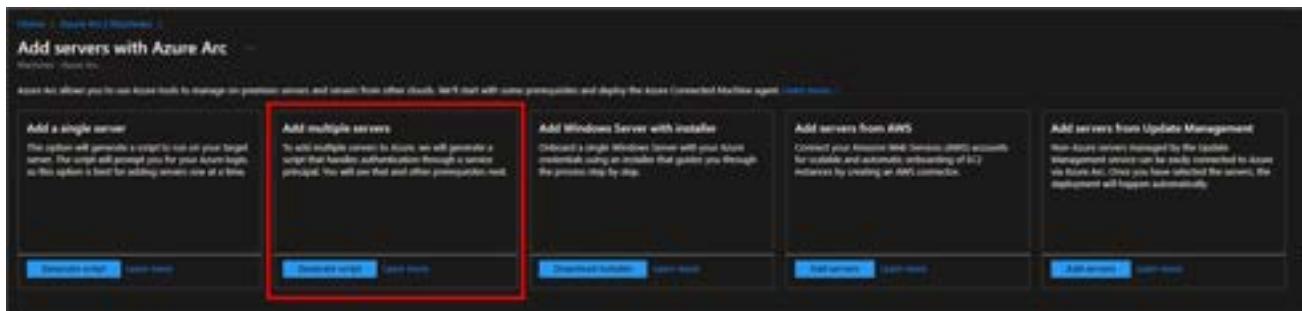
[Simplify network configuration requirements with Azure Arc gateway](#)

# Task 1: Generate a script to automate the download and installation of the Azure Arc connected machine agent for a Windows machine, and to connect the machine to Azure Arc

- 1. From the Azure portal go to the "Machines - Azure Arc" page and select "Add/Create" at the upper left, then select "Add a machine".



- 2. In the next screen, go to "Add multiple servers" and click on "Generate script".



- 3. Fill in the Resource Group, Region, Operating System (Windows), keep Connectivity as "Public endpoint". Keep the *Connect SQL Server* option ticked. In the Authentication section click on the "Create new" link under the "Service Principal" dropdown and then enter a name (ex:ArcOnboarding) and choose "Azure Connected Machine Onboarding" as the role and click "Create".

The screenshot shows two adjacent Azure portal pages. On the left, the 'Add multiple servers with Azure Arc' page has several fields highlighted with red boxes: 'Resource group' (containing 'ArcOnboarding'), 'Region' (containing 'US West'), 'Operating system' (containing 'Windows'), and 'Connect via RDP' (with the dropdown open). A red arrow points from the 'Resource group' field on the left to the 'Resource group' field on the right. On the right, the 'New Azure Arc service principal' page also has several fields highlighted with red boxes: 'Name' (containing 'ArcOnboarding'), 'Region' (containing 'US West'), 'Subscription' (containing 'Visual Studio Enterprise Subscription'), 'Resource group' (containing 'ArcOnboarding'), 'Client secret' (with the dropdown open), and 'Role assignment' (containing 'Azure Connected Server Onboarding').

4. Click on "Download and close" to save your new service principal ID and secret as a text file (you will use this in a future step).

The screenshot shows a modal dialog box titled 'Download service principal ID and secret'. It contains a warning message: 'You will not be able to retrieve the client secret again after you leave this page.' Below the message, it states: 'The client secret for this service principal will expire on 2024-10-30T16:24:13.925Z. You can generate a new secret for this service principal when it expires.' At the bottom is a large blue button labeled 'Download and close'. A red box highlights the entire dialog area.

5. Select your newly created "ArcOnboarding" service principal from the dropdown menu.

## Authentication

You can automate the onboarding of multiple servers with minimal permissions using a service principal instead of enabling a single server interactively. The built-in "Azure Connected Machine Onboarding" role allows the service principal to onboard servers to Azure Arc. Only those service principals with the "Azure Connected Machine Onboarding" role assigned to the resource group you selected will appear in the drop down below. You will need to generate a secret for the service principal and include it in the onboarding script before you can use it. [Learn more](#)

Service principal

ArcOnboarding

Create new

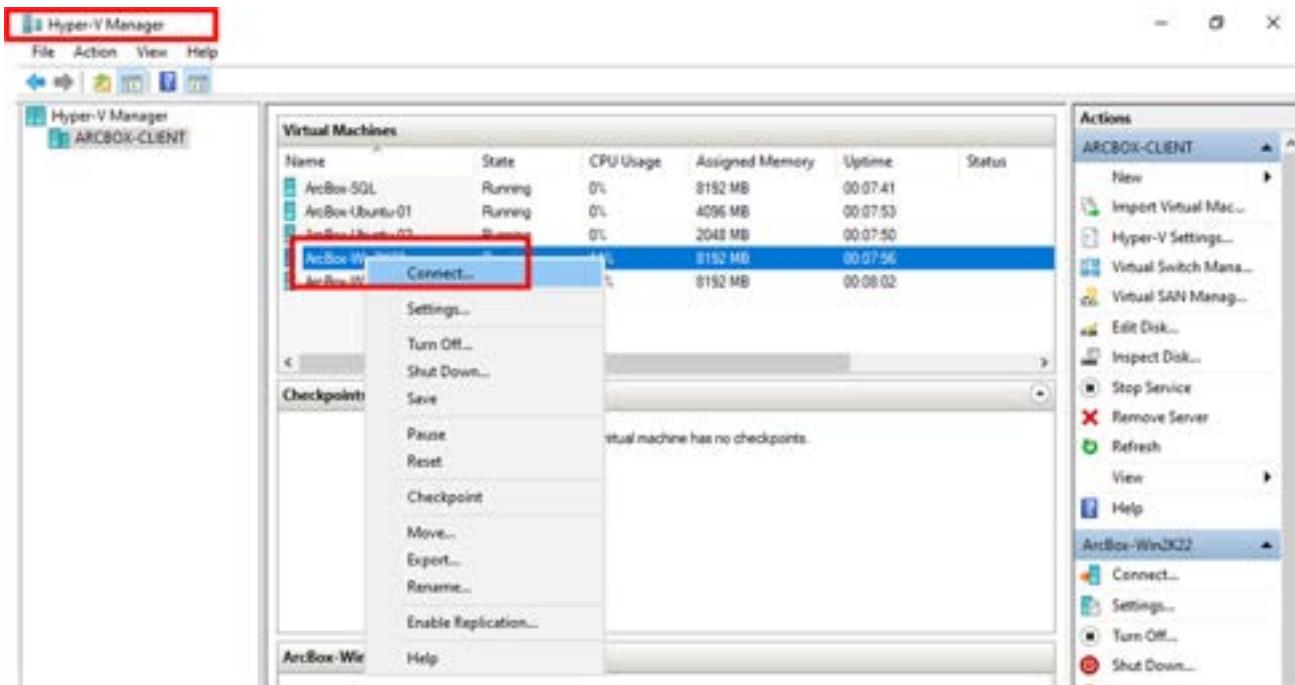
- 6. Then click on "Download and run script" and scroll down till you see the "Download" button, and next to it click on the icon that looks like two pieces of paper stacked on each other to copy your onboarding script.

```
1 $global:scriptPath = $myInvocation.MyCommand.Definition
2
3 function Restart-AsAdmin {
4     $pushCommand = "powershell"
5     if ($PSVersionTable.PSVersion.Major -ge 6) {
6         $pushCommand = "pwsh"
7     }
8
9     try {
10        Write-Host "This script requires administrator permissions to install the Azure Connected Machine
11        Agent. Attempting to restart script with elevated permissions..."
12        $arguments = "-NoExit -Command ""$($scriptPath)"""
13        Start-Process $pushCommand -Verb RunAs -ArgumentList $arguments
14        exit 0
15    } catch {
16        throw "Failed to elevate permissions. Please run this script as Administrator."
17    }
18
19    try {
20        if (-not ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)) {
21            if ([System.Environment]::UserInteractive) {
22                Restart-AsAdmin
23            } else {
24                throw "This script requires administrator permissions to install the Azure Connected Machine
25                Agent. Please run this script as Administrator."
26            }
27        }
28    }
29
30    # Add the service principal application ID and secret here
```

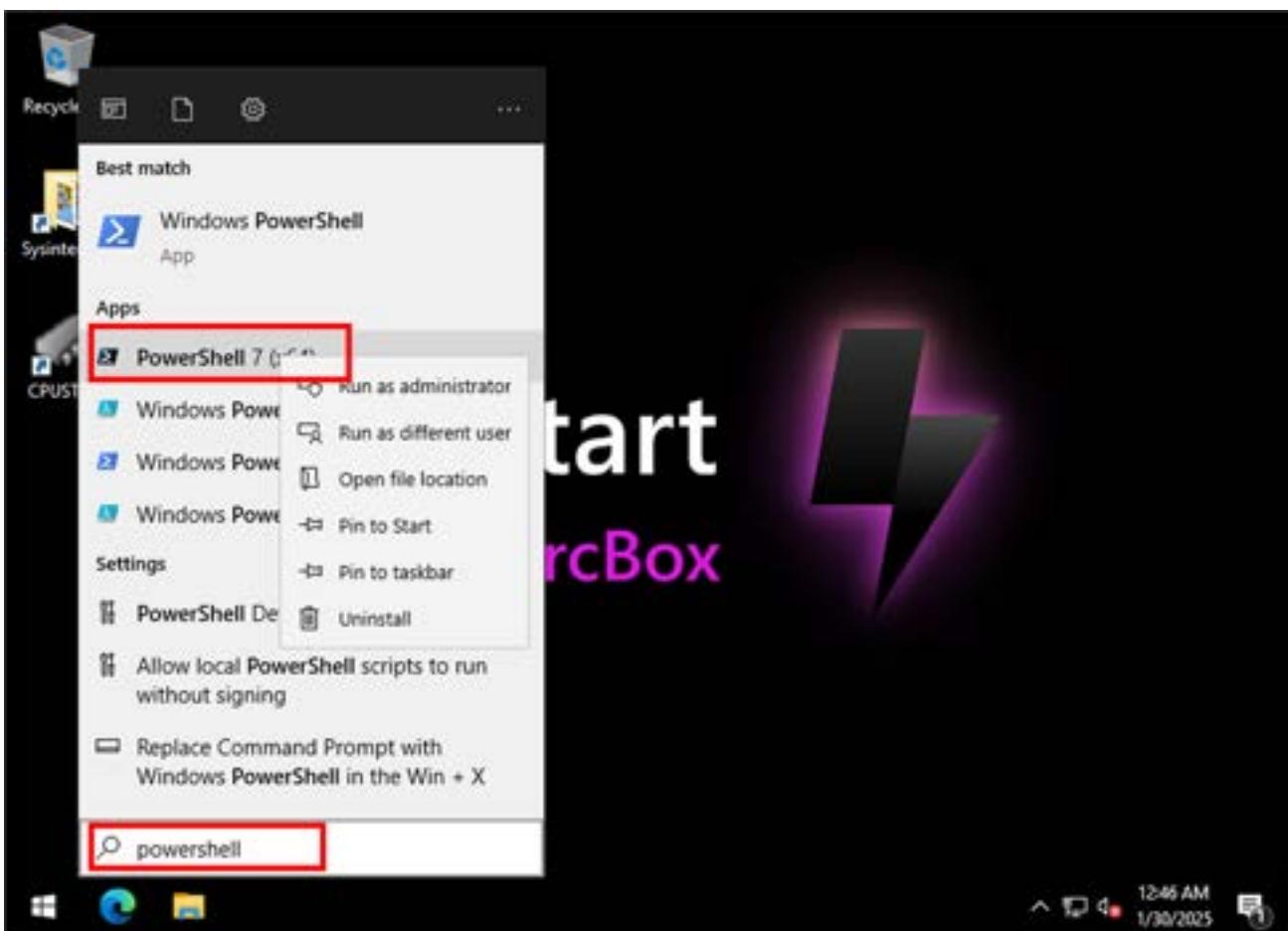
Download



- 7. Go to the ArcBox-Client machine via RDP and from Hyper-V manager right-click on the *ArcBox-Win2K22* VM and click "Connect" (Administrator default password is JS123!!). Next you will need to open an editor (Visual Studio Code or Notepad for example) and paste the content of the onboarding script.



- 8. Fill in the Service Principal Id, if it is not already populated, and the secret from the text file that was downloaded above into the script where you see "ENTER SECRET HERE". Start Powershell 7 and paste the script (after you have added the secret). This will execute the script.



```
Administrator: PowerShell 7(x64)
$gBody | ConvertTo-Json) | Out-Null;
>> Write-Host -ForegroundColor Red $_.Exception;
>> }
VERBOSE: Installing Azure Connected Machine Agent
VERBOSE: PowerShell version: 7.4.6
VERBOSE: Total Physical Memory: 8192 MB
VERBOSE: .NET Framework version: 4.8.4161
VERBOSE: Checking if this is an Azure virtual machine
VERBOSE: Error The request was canceled due to the configured HttpClient.Timeout of 1 seconds elapsing. checking if we are in Azure
VERBOSE: Downloading agent package from https://gbl.his.arc.azure.com/azcmagent/latest/AzureConnectedMachineAgent.msi to C:\Users\ADMINI~1\AppData\Local\Temp\2\AzureConnectedMachineAgent.msi
VERBOSE: Installing agent package
Installation of azcmagent completed successfully
INFO   Connecting machine to Azure... This might take a few minutes.
INFO   Testing connectivity to endpoints that are needed to connect to Azure... This might take a few minutes.
  28% [==>]
  30% [==>]
INFO   Creating resource i
e Resource ID=/subscriptions/
+ HybridCompute/machines/ArcBox_Win2K22
  60% [=====>]
  88% [=====>]
100% [=====>]
INFO   Connected machine to Azure
```

- 9. On successful completion a message is displayed to confirm the machine is connected to Azure Arc. We can also verify that our Windows machines are all now connected in the Azure portal (Machines - Azure Arc).

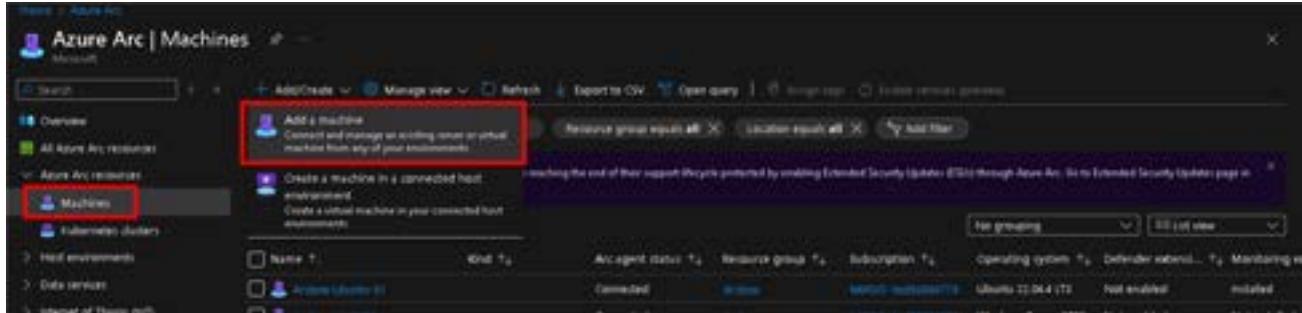
The screenshot shows the 'Azure Arc | Machines' blade in the Azure portal. A red box highlights the title bar. The left sidebar shows 'All Azure Arc resources' and 'Azure Arc resources' expanded, with 'Machines' selected. A red box highlights the 'Machines' section. The main area displays three machines: 'ArcBox\_Win2K22' (Windows Server 2022 Datacenter), 'ArcBox\_Win2K22' (Windows Server 2022 Datacenter), and 'ArcBox\_Win2K22' (Windows Server 2022 Datacenter). All three machines are listed as 'Connected' under the 'Arc agent status' column.

- 10. **Optional:** If you intend to attempt the Arc-enabled SQL server labs within this workshop, then you might want to run the same script inside the *ArcBox-SQL* VM to onboard this server ready for the coming labs, provided that you had selected the SQL onboarding option ticked when you created the script in the portal.

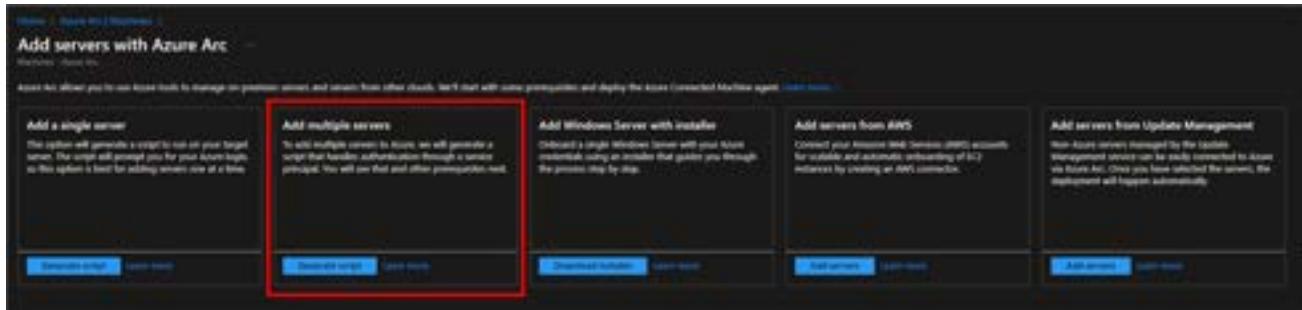
## Task 1 has been completed

## Task 2: Connect a Linux machine to Azure Arc using the direct internet access (without a proxy)

- 1. From the Azure portal go to the "Machines - Azure Arc" page and select "Add/Create" at the upper left, then select "Add a machine".



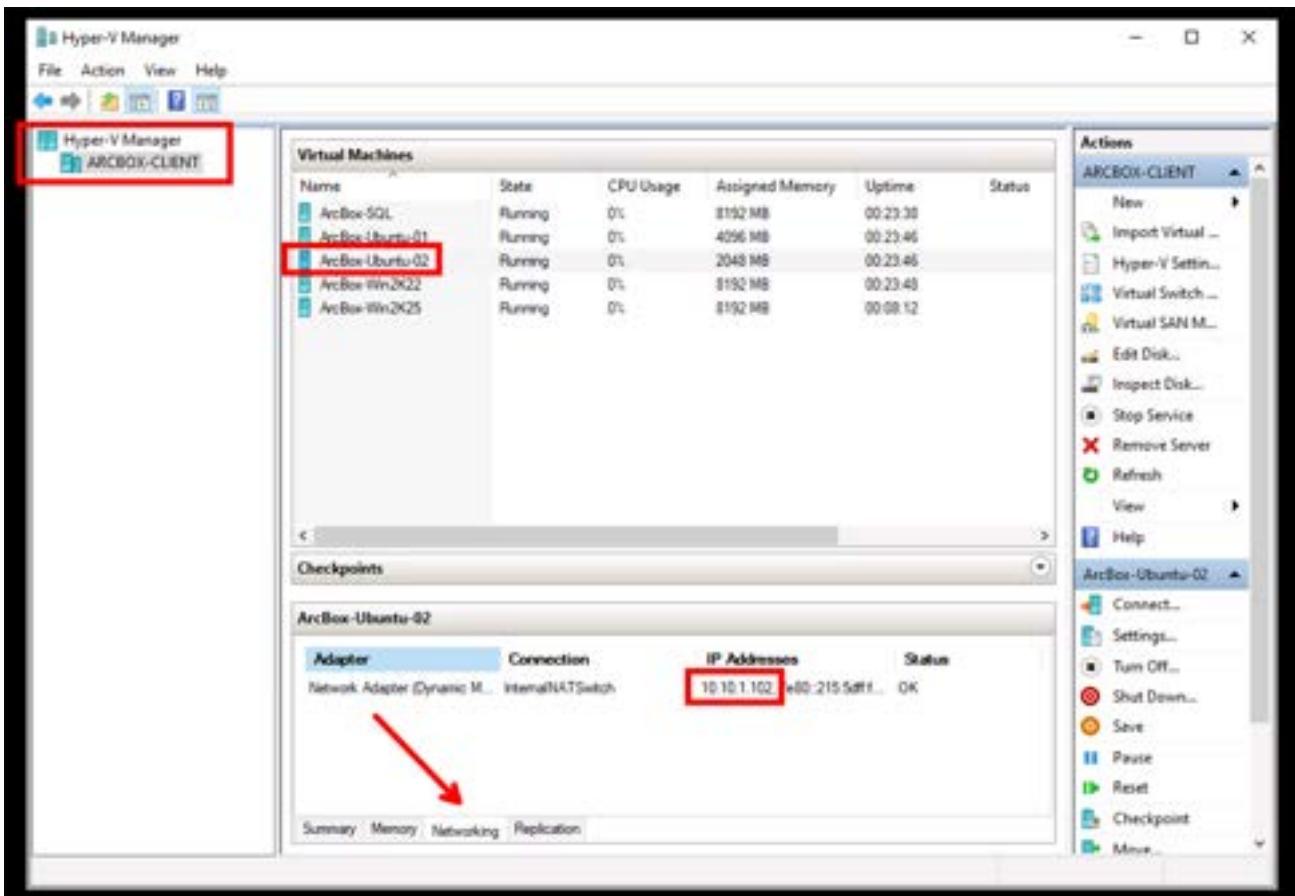
- 2. In the next screen, go to "Add multiple servers" and click on "Generate script".



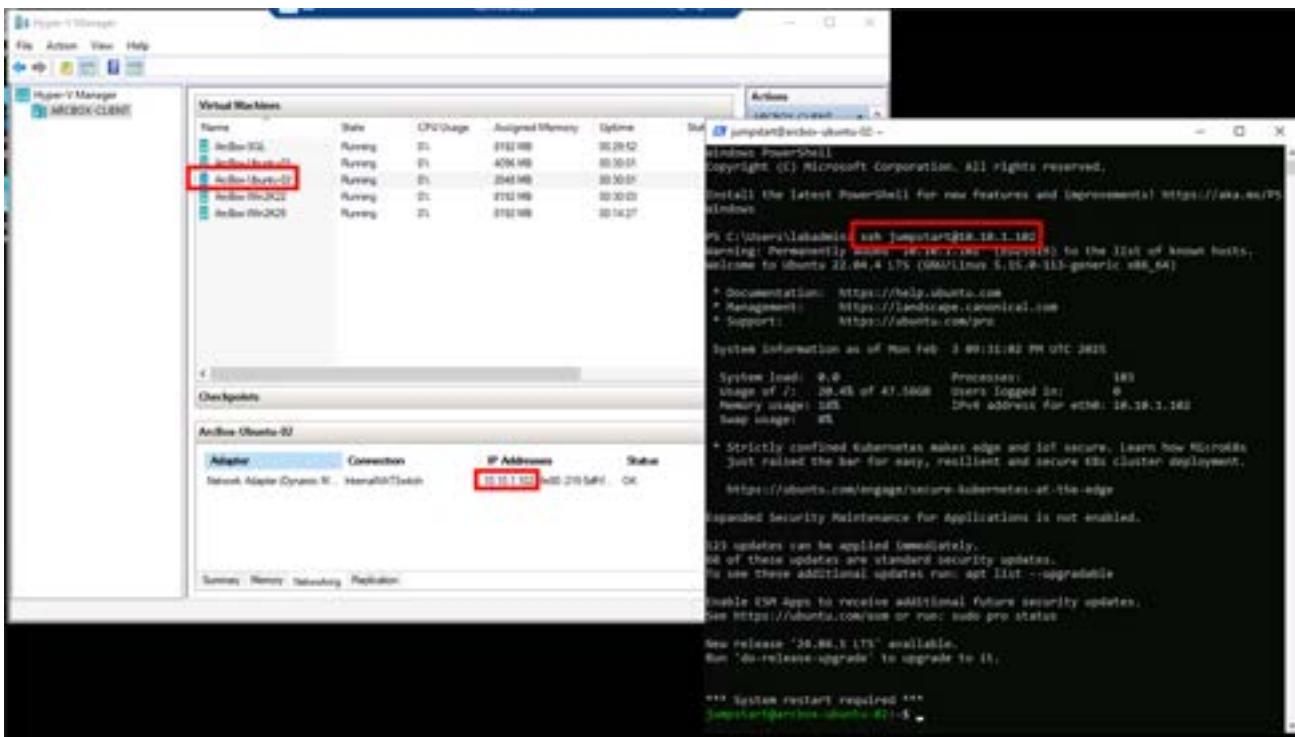
- 3. Fill in the required details but this time choose Linux for the Operating System box and choose the service principal in the "Authentication" dropdown that you created in the previous exercise. Then download the script to your local machine (or you can copy the content into the clipboard).
- 4. Make sure that the Service Principal Id is filled in, then add the client secret to the script using your editor. Also add the following 3 lines to the script **just below the last export statement** (to allow onboarding of Azure linux machines):

```
shell
▶ sudo ufw --force enable
  sudo ufw deny out from any to 169.254.169.254
  sudo ufw default allow incoming
```

- 5. Connect the ArcBox-Client machine, and from the "Networking" tab on Hyper-v Manager find the IP address of the Linux machine.



- 6. SSH into the ArcBox-Ubuntu-02 machine using "PowerShell". If you are prompted for a password then use JS123!!:



PowerShell

```
▶ ssh jumpstart@<Enter IP Address of the Linux machine>
```

- 7. Create an empty onboarding script file using the nano editor, and paste the script content from your local machine. Once you are in the editor, navigate using the arrow keys and not the mouse.

```
shell
```

```
▶ nano onboardingscript.sh
```

- 8. Save the file (Ctrl-O then Enter) and exit (Ctrl-X). Now you can run the script:

```
shell
```

```
▶ sudo bash ./onboardingscript.sh
```

- 9. Wait for the script to finish successfully. A message should confirm that the machine is now Arc-connected. You can also verify that our Linux machine is connected in the Azure portal (Machines - Azure Arc).



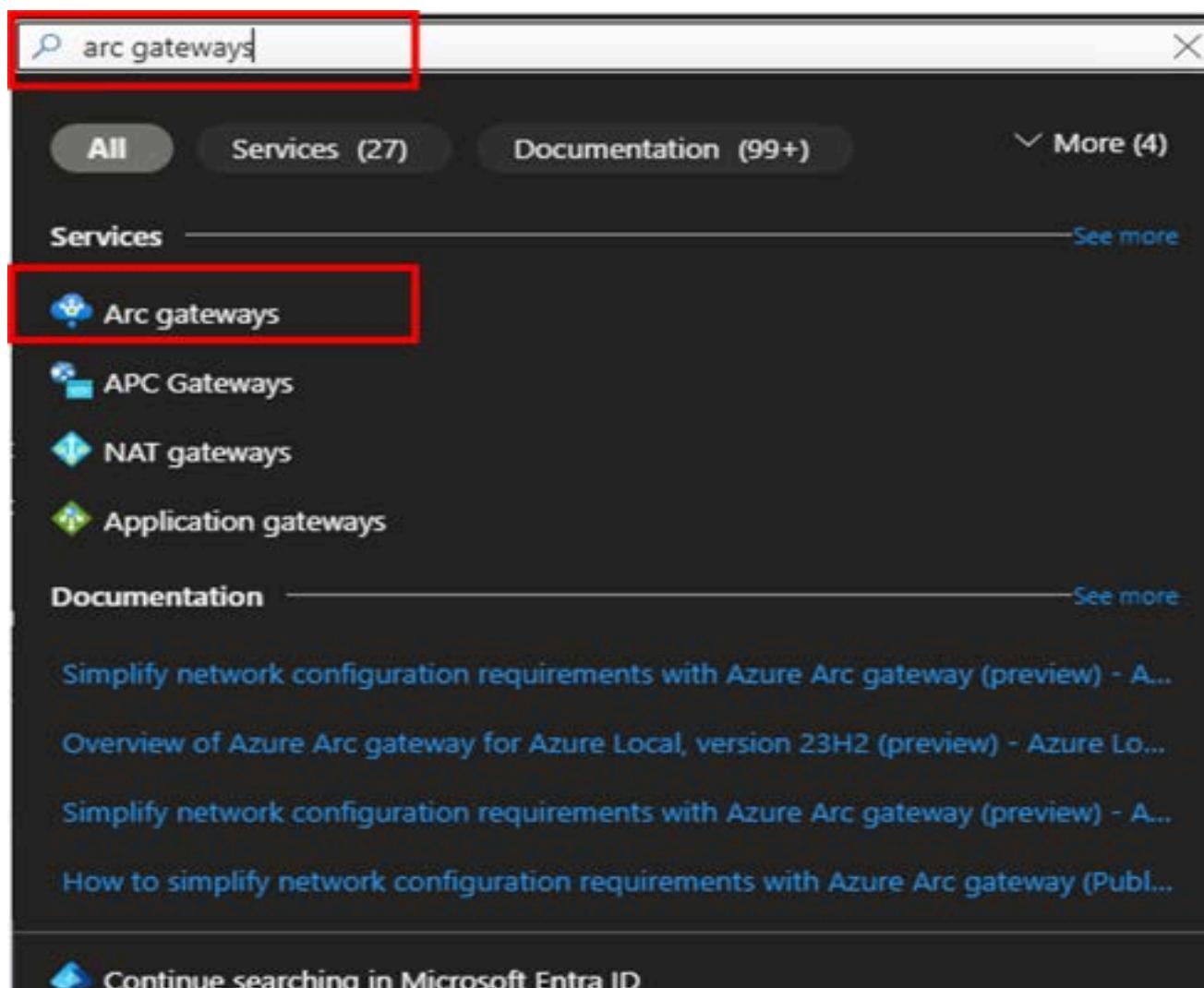
```
60% [=====→      ]
80% [=====→      ]
100% [=====]
INFO Connected machine to Azure
```

**Task 2 has been completed**

## Task 3: Connect a linux machine to Azure Arc using a proxy and Arc Gateway

- On the Ubuntu02 machine, run the following command - sudo apt purge azcmagent
- Delete Ubuntu02 machine from the Azure Arc - Machines by navigating to Azure Arc | Machines/arcbox-ubuntu-02, and select the delete option.

1. From the Azure portal search for *Arc gateways* and select from the search results, then click on the *Create* button.



- 2. Fill in the details of the resource group name, choose a name for your Arc Gateway and choose the region of your lab resources. Then move to the *Review + create* tab and create the gateway.

## Create an Arc gateway resource

Basics Tags Review + create

For customers who use enterprise firewalls or proxies to manage outbound traffic, the Arc gateway enables you to onboard infrastructure to Azure via Arc with only 7 endpoints required.

### Resource details

Select a name, location, subscription, and resource group for your Arc gateway resource. Your Arc gateway resource does not need to be in the same subscription, resource group, or location as the Arc-enabled resources that will be associated with the Arc gateway resource.

Subscription \* ⓘ

Resource group \* ⓘ  Select existing item...  
Create new

Name \*

Location \*  (Europe) UK South

- 3. The deployment will take few minutes and when it is done choose Go to resource.

### gatewaytest1.ArcGateway.1739390188385 | Overview

Deployment

Search  Delete Cancel Redeploy Download Refresh

Overview Deployment name : gatewaytest1.ArcGateway.1739390188385  
Inputs Subscription :   
Outputs Resource group : ArcBox

Deployment details  
Next steps

Go to resource

- 4. Find the Gateway URL and make a note of it to be used later.

Resource ID : /subscriptions/  
Gateway URL : 87c.gw.arcazure.com

- 5. From the *ArcBox-Client* machine open *Hyper-V Manager*, click the *ArcBox-Client* server, click the *ArcBox-Proxy* under Virtual Machines. From the *Networking* tab find the IPv4 address of the proxy. Make a note of this IP address.

Hyper-V Manager

File Action View Help

Hyper-V Manager ARCBOX-CLIENT

**Virtual Machines**

Name	State	CPU Usage	Assigned Memory
ArcBox-Proxy	Running	0%	2048 MB
ArcBox-SUL	Running	0%	8192 MB
ArcBox-Ubuntu-01	Running	0%	4096 MB
ArcBox-Ubuntu-02	Running	0%	2048 MB
ArcBox-Ubuntu-03	Paused	0%	2048 MB

**Checkpoints**

The selected virtual machine has no checkpoints.

**ArcBox-Proxy**

Adapter	Connection	IP Addresses
Network Adapter (Dynamic)	InternalNATSwitch	10.10.1.102, fe80::21

Summary Memory Networking Replication

**Actions**

ARCBOX-CLIENT

- New
- Import Virtual Machine...
- Hyper-V Settings...
- Virtual Switch...
- Virtual SAN...
- Edit Disk...
- Inspect Disk...
- Stop Service
- Remove Server
- Refresh
- View
- Help

ArcBox-Proxy

- Connect...
- Settings...
- Turn Off...
- Shut Down...
- Save
- Pause
- Reset

- 6. From the *ArcBox-Client* machine use Powershell 7 to ssh into the proxy server *ArcBox-Proxy* using the IP address you found in the previous steps.

PowerShell

▶ `ssh jumpstart@<Enter IP Address of the proxy machine>`

- 7. Once you have logged into the proxy machine edit the *whitelist.txt* file which contains the list of links allowed by the proxy. These should be similar to the links stated in [Arc Gateway documentation](#). If any of the links is missing then add it to the whitelist. Once you are in the editor, navigate using the arrow keys and not the mouse. Make sure that you fill in the Arc gateway URL that you have from the earlier steps, and also the region of your deployment.

PowerShell

▶ `sudo nano /etc/squid/whitelist.txt`

```
jumpstart@proxy: ~
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Thu Feb 13 07:03:29 PM UTC 2025

System load: 0.02          Processes:           101
Usage of /: 20.0% of 47.56GB  Users logged in:      0
Memory usage: 12%          IPv4 address for eth0: 10.10.1.104
Swap usage:  0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

58 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Feb 13 19:00:41 2025 from 10.10.1.1
jumpstart@proxy:~$ sudo nano /etc/squid/whitelist.txt
```

```
jumpstart@proxy: ~
GNU nano 6.2                               /etc/squid/whitelist.txt *
<*INSERT Arc Gateway URL here>
management.azure.com
login.microsoftonline.com
gbl.his.arc.azure.com
<INSERT your region here>.his.arc.azure.com
packages.microsoft.com
download.microsoft.com
```

- 8. Save the file (Ctrl-O then Enter) and exit (Ctrl-X).

- 9. In order for the new whitelist to be active, restart the Squid proxy service.

PowerShell

▶ `sudo systemctl restart squid`

- 10. **Optional:** If you want to have a look at how the Squid proxy server configuration uses the whitelist then open the file `/etc/squid/squid.conf` and examine the settings, including the port used 3128 which is the default Squid proxy port.
- 11. From the *ArcBox-Client* machine open *Hype-V Manager*, click the *ArcBox-Client* server, click the *ArcBox-Ubuntu-02* under Virtual Machines. From the *Networking* tab find the IPV4 address of the machine. Make a note of this IP address. Then ssh into it from Powershell 7.

PowerShell

▶ `ssh jumpstart@<Enter IP Address of the ArcBox-Ubuntu-02 machine>`

- 12. Configure the proxy settings on the ArcBox-Ubuntu-02 machine.

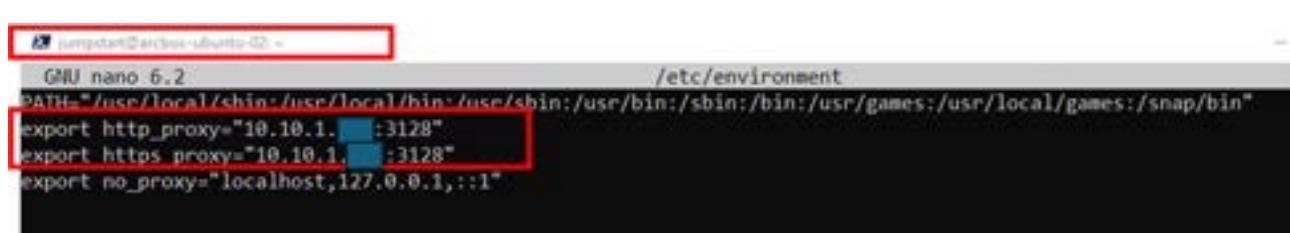
PowerShell

▶ `sudo nano /etc/environment`

- 13. Add the following 3 lines to the file making sure that you use the IP address of the **proxy server!** After you have done, Save the file (Ctrl-O then Enter) and exit (Ctrl-X).

PowerShell

▶ `export http_proxy="<proxy IP Address>:3128"`  
`export https_proxy="<proxy IP Address>:3128"`  
`export no_proxy="localhost,127.0.0.1,::1"`

- 
- 14. Type *EXIT* then re-login again to the *ArcBox-Ubuntu-02* for the changes to take effect.

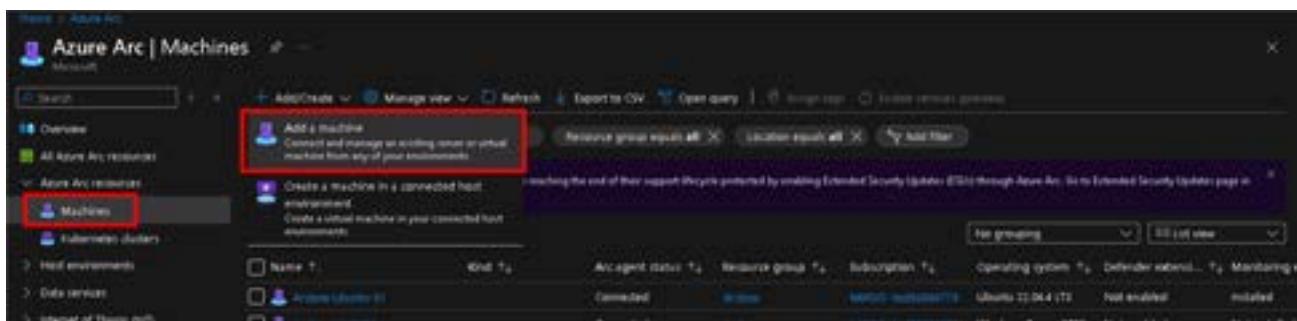
PowerShell

▶ `ssh jumpstart@<Enter IP Address of the ArcBox-Ubuntu-02 machine>`

- 15. Optional: Test that your proxy is blocking internet access

```
jumpstart@arcbox-ubuntu-02:~  
jumpstart@arcbox-ubuntu-02:~$ curl -I http://bing.com  
HTTP/1.1 403 Forbidden  
Server: squid/5.9  
Mime-Version: 1.0  
Date: Thu, 13 Feb 2025 13:40:33 GMT  
Content-Type: text/html; charset=utf-8  
Content-Length: 3485  
X-Squid-Error: ERR_ACCESS_DENIED 0  
Vary: Accept-Language  
Content-Language: en  
X-Cache: MISS from proxy  
X-Cache-Lookup: NONE from proxy:3128  
Via: 1.1 proxy (squid/5.9)  
Connection: keep-alive  
  
jumpstart@arcbox-ubuntu-02:~$
```

- 16. From the Azure portal go to the "Machines - Azure Arc" page and select "Add/Create" at the upper left, then select "Add a machine".



- 17. In the next screen, go to "Add multiple servers" and click on "Generate script".

Add servers with Azure Arc

Add a single server  
This option will generate a script to run on your target server. The script will connect you to your Azure Log Analytics workspace and install the Azure Connected Machine agent. [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 use that and other prerequisites, and... [Learn more](#)

Add Windows Server with install  
Download a single Windows Server with your license included, using an installer that guides you through the process step by step. [Download Windows Server](#) [Learn more](#)

Add servers from AWS  
Connect your Amazon Web Services (AWS) accounts for reliable and automatic rehosting of EC2 instances by creating an AWS connector. [Get started](#) [Learn more](#)

Add servers from Update Management  
Non-Azure servers managed by the Update Management connector can be integrated to Azure via Azure Arc. Once you have registered the servers, the deployment will happen automatically. [Get started](#) [Learn more](#)

18. Fill in the required details and choose Linux for the Operating System box. Set the connectivity method to *Proxy server*. Enter the URL of the proxy server and name of the Arc gateway as shown in the screenshots but make sure that they match with your own settings (the IP address of the proxy server that you observed earlier). Also Choose the service principal in the "Authentication" dropdown that you created in the previous exercise.

## Add multiple servers with Azure Arc

Basics Tags Download and run script

Complete the fields below to connect servers on-premises and in other clouds to be managed and governed in Azure. [Learn more](#)

### Project details

Select the subscription and resource group where you want the server to be managed within Azure.

Subscription

Resource group

### Server details

Select details for the servers that you want to add. An agent package will be generated for the selected server type.

Region

Operating system

### SQL Server

Connect SQL Server

Automatically connect any SQL Server instances to Azure Arc. [Learn more](#)

**Connectivity method**

Choose how the connected machine agent running in the server should connect to the Internet. This setting only applies to the Arc agent. Proxy settings for extensions are configured separately.

Connectivity method \*

Public endpoint

Proxy server

Private endpoint

The Arc gateway (preview) reduces the number of URLs that you must allow in your proxy servers to use Arc. To use the Arc gateway (preview) feature, a gateway resource is required. [Learn more](#)

Proxy server URL \*

Gateway resource

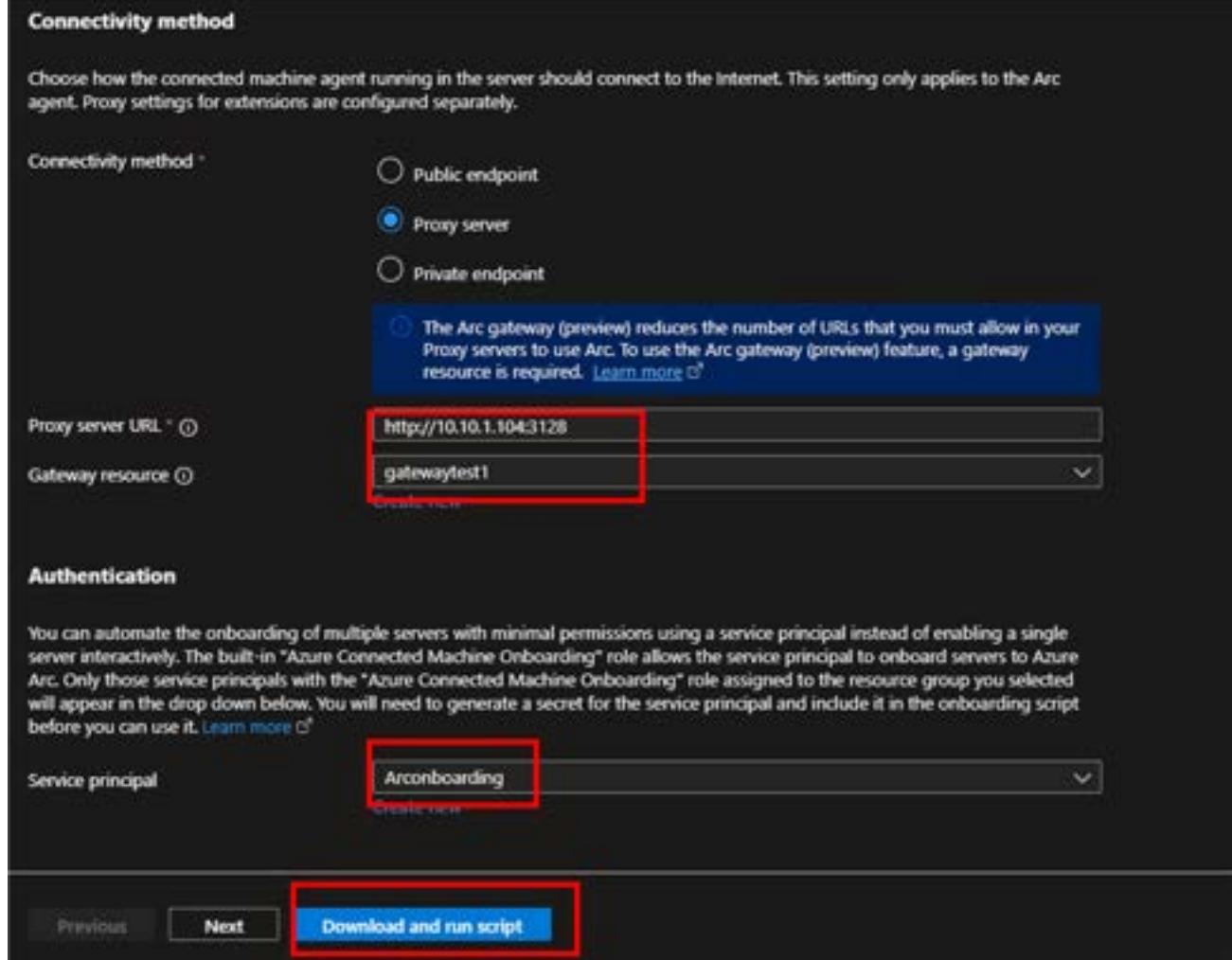
**Authentication**

You can automate the onboarding of multiple servers with minimal permissions using a service principal instead of enabling a single server interactively. The built-in "Azure Connected Machine Onboarding" role allows the service principal to onboard servers to Azure Arc. Only those service principals with the "Azure Connected Machine Onboarding" role assigned to the resource group you selected will appear in the drop down below. You will need to generate a secret for the service principal and include it in the onboarding script before you can use it. [Learn more](#)

Service principal

[Create new](#)

[Previous](#) [Next](#) **Download and run script**



- 19. On the *Download and run script* tab notice the reminder to ensure that the required endpoints are not blocked by the proxy server. These were the links that you added to the proxy whitelist earlier. Choose the *Basic script* option.

## 1. Ensure the network connectivity requirements are met

If outbound connectivity is restricted by your proxy server, make sure the URLs listed below are not blocked.

URL	Description
87cgw.arc.azure.com	Your Arc gateway URL
management.azure.com	Azure Resource Manager Endpoint, required for ARM control channel
login.microsoftonline.com	Microsoft Entra ID's endpoint, for acquiring identity access tokens
gblhis.arc.azure.com	The cloud service endpoint for communicating with Arc Agents
<region>.his.arc.azure.com	The cloud service endpoint for communicating with Arc Agents
packages.microsoft.com	Required to acquire Linux based Arc agent payload, only needed to connect Linux servers to Arc
download.microsoft.com	Used to download the Windows installation package

Before you run the script, make sure your server meets the following requirements.

- HTTPS access to Azure services  
All servers require access to port 443 and a set of outbound URLs for the Azure Arc agents to properly function.
- Local administrator permission

## 2. Select deployment method

Deployment method

Basic script

20. Copy the script or download it. You should see that your proxy IP address has been configured in the script.

```

20: output=$(wget https://gbl.his.arc.azure.com/azcmagent-linux -e use_proxy=yes -e https_proxy="http://10.10.1.104:3128" -O "$LINUX_INSTALL_SCRIPT" 2>&1);
21: if [ $? != 0 ]; then wget -qO- -e use_proxy=yes -e https_proxy="http://10.10.1.104:3128" --method=PUT
--body-data="{"subscriptionId": "$subscriptionId", "resourceGroup": "$resourceGroup",
"tenantId": "$tenantId", "location": "$location", "correlationId": "$correlationId",
"authType": "$authType", "operation": "onboarding", "messageType": "DownloadScriptFailed",
"message": "$output"}" "https://gbl.his.arc.azure.com/log" > /dev/null || true; fi;
echo "$output";
23:
24: # Install the hybrid agent
25: bash "$LINUX_INSTALL_SCRIPT" --proxy "http://10.10.1.104:3128";
26:
27: # Run connect command
28: sudo azcmagent connect --service-principal-id "$ServicePrincipalId" --service-principal-secret
"$ServicePrincipalClientSecret" --resource-group "$ResourceGroup" --tenant-id "$tenantId" --location
"$location" --subscription-id "$subscriptionId" --cloud "$cloud" --gateway-id "$gatewayId" --tags
'ArcSQLServerExtensionDeployment=Disabled' --correlation-id "$correlationId";
29:

```

[Download](#)



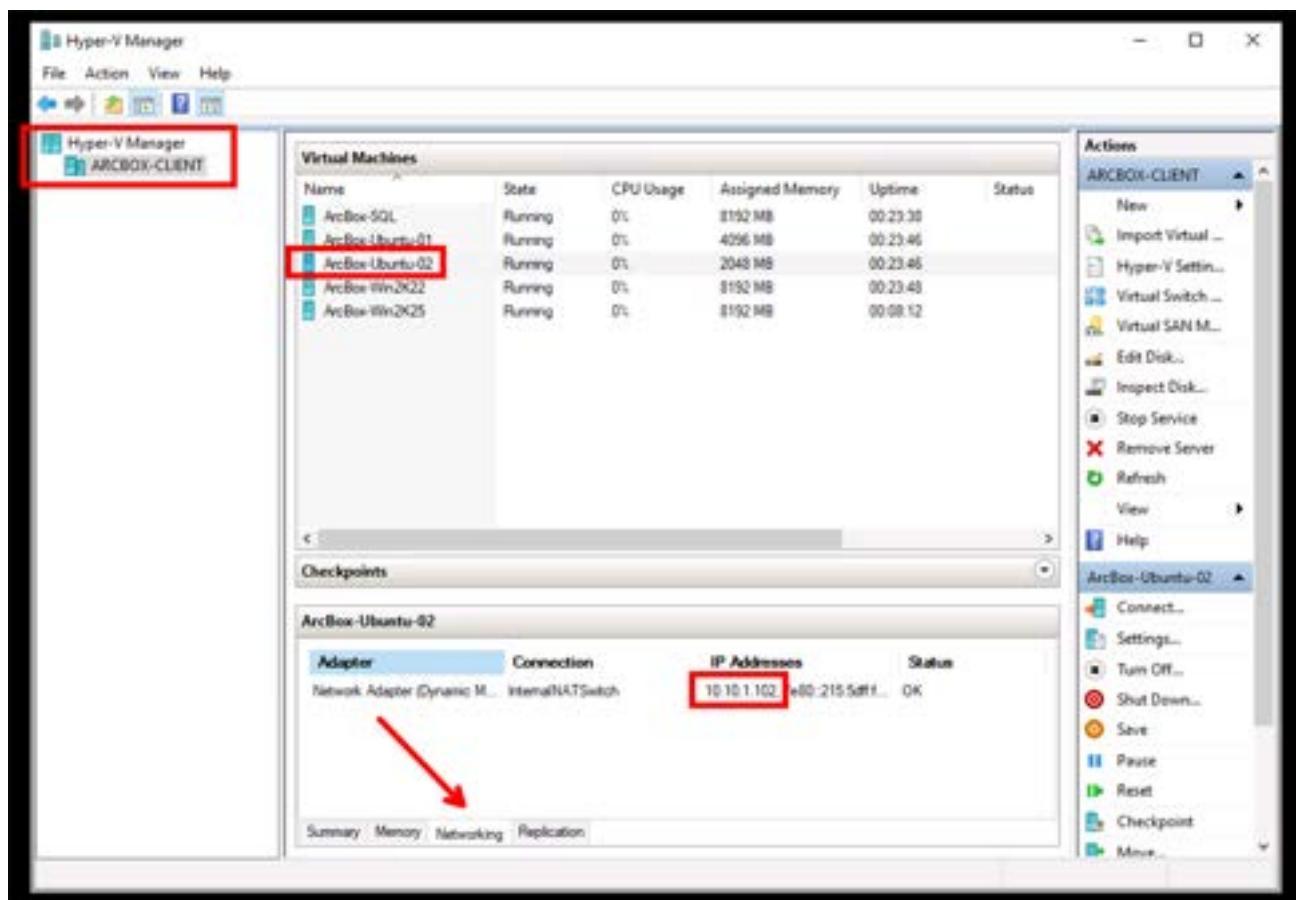
21. In your local editor, paste the script and make sure that the Service Principal Id and the client secret are filled in. Also add the following 3 lines to the script **just below the last export**

**statement** (to allow onboarding of Azure linux machines):

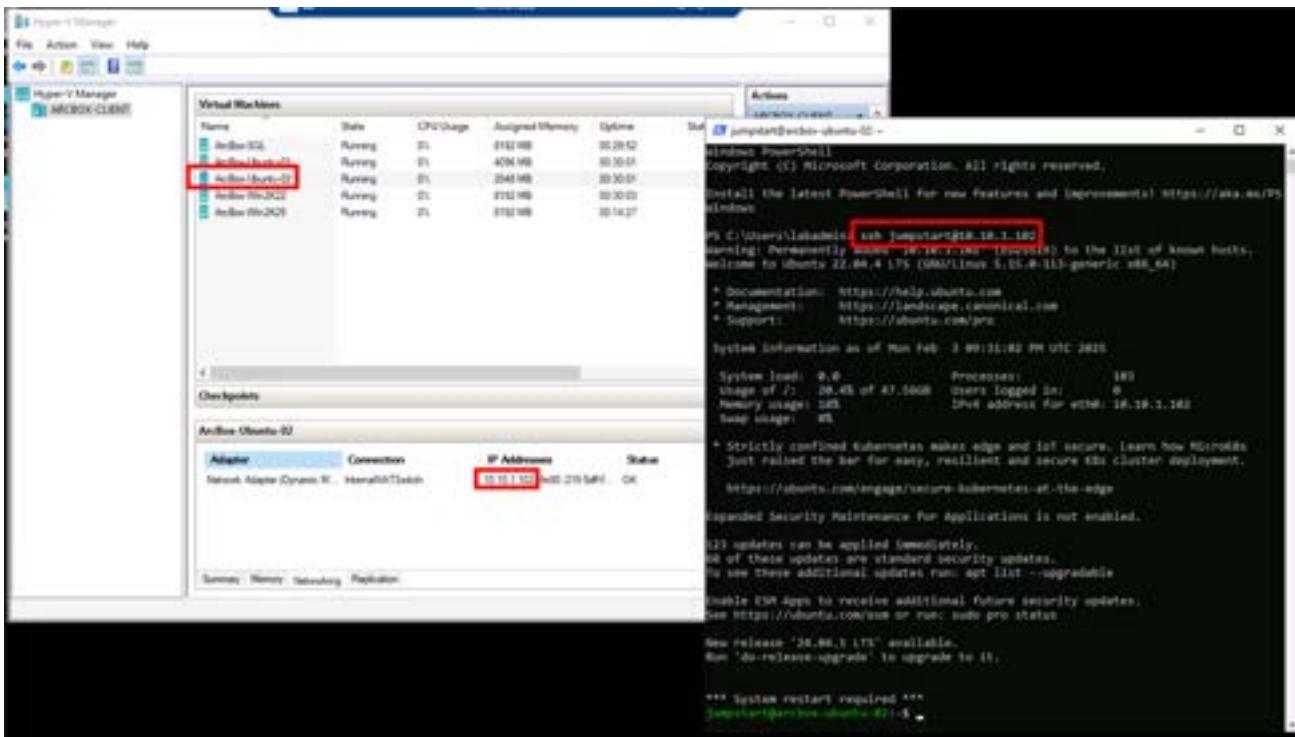
```
shell
```

```
▶ sudo ufw --force enable  
sudo ufw deny out from any to 169.254.169.254  
sudo ufw default allow incoming
```

- 22. Connect the ArcBox-Client machine. If you are still connected to the *ArcBox-Ubuntu-02* machine with ssh session then ignore the following 2 steps.
- 23. From the "Networking" tab on Hyper-v Manager find the IP address of the Linux machine *ArcBox-Ubuntu-02*.



- 24. SSH into the *ArcBox-Ubuntu-02* machine using "PowerShell". If you are prompted for a password then use *JS123!!*:



### PowerShell

▶ ssh jumpstart@<Enter IP Address of the Linux machine>

- 25. Create an empty onboarding script file using the nano editor, and paste (Right-click) the script content from your local machine. Once you are in the editor, navigate using the arrow keys and not the mouse.

### shell

▶ nano onboardingscript.sh

- 26. Save the file (Ctrl-O then Enter) and exit (Ctrl-X). Now you can run the script:

### shell

▶ sudo bash ./onboardingscript.sh

- 27. Wait for the script to finish successfully. A message should confirm that the machine is now Arc-connected. You can also verify that our Linux machine is connected in the Azure portal (Machines - Azure Arc).



- 28. You can confirm that the ArcBox-Ubuntu-02 is associated with your Arc gateway by navigating to the Azure portal page of the Arc gateway and examining the *Associated resources*.

The screenshot shows the Azure portal interface. On the left, there's a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, Associated resources (which is highlighted with a red box), Settings, Automation, and Help. The main content area has a search bar at the top. Below it, a table displays one record. The columns are: Name (checkbox), Kind, Connection status, Resource group, and Subscription. The single row shows 'ardexidentity' under 'Name', 'Connected' under 'Connection status', and a blue bar under 'Subscription'. A red box highlights the 'ardexidentity' name.

Name	Kind	Connection status	Resource group	Subscription
<input type="checkbox"/> ardexidentity		Connected		

**Task 2 has been completed**

**Congratulations, you have completed all tasks in this lab**

---

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB03: Securing Azure Arc-enabled servers with Microsoft Defender for Cloud

---

## Student Lab Manual

### Table of Contents

Exercise 1 - Detect threats on your servers using alerts

**Task 1 - Simulate malicious activities**

Exercise 2 - Enable vulnerability assessment

**Task 1 - Configure vulnerability assessment on your machines**

# Exercise 1 - Detect threats on your servers using alerts

---

## **Objective**

This exercise will walk you through simulating malicious activity on your machines and examine how Defender for Servers can alert you on those threats.

## **Estimated Time to Complete This Lab**

45 minutes

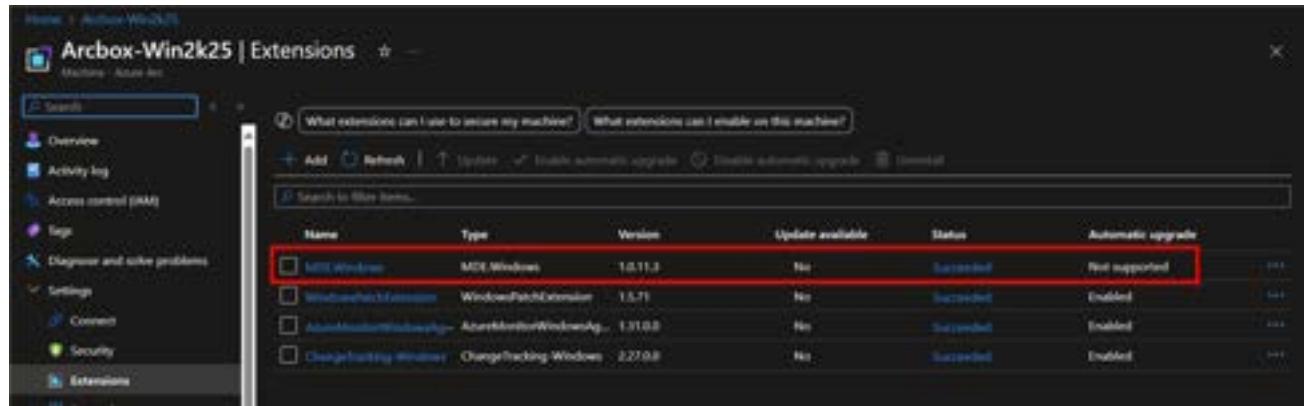
## **Explanation**

In this exercise, you will learn how to leverage Defender for Servers to detect threats and malicious activities.

## Task 1: Simulate malicious activities

- 1. To simulate a malicious activity on the *ArcBox-Win2K25* servers, rdp into the *ArcBox-Client* VM.

□ **Before simulating the alert, make sure that the 'MDE.Windows' is installed on the Arc-enabled server.** You can do this by checking the Extensions installed on the Arc enabled server *ArcBox-Win2k25* from the Azure portal.



- If the 'MDE.Windows' extension is missing then either the *Microsoft Defender for Cloud* configuration has not been set correctly as explained in Lab01 **OR** the configuration of the *Microsoft Defender for Cloud* has not taken effect yet. Go back to Lab01 and check that you have set the Defender for Cloud correctly in the step *Enable the Defender for Servers plan* and have saved the configuration.

- **2. If the 'MDE.Windows' extension is missing and not in the process of being created as seen in the Azure Portal** then you can manually install it on the *ArcBox-Win2k25* by running the following Powershell script either in the *ArcBox-Client* machine or in Powershell from the Azure Portal cloud shell, **making sure that the Resource Group name is correct**. Otherwise if the extension is installed then move to the next step.

- If you decide to run the manual installation of the *MDE.Windows* extension from the *ArcBox-Client* machine, then you will need to login from PowerShell using the *Connect-AzAccount* command and choosing the *Work or School* option. Additionally you will need to run the command *Install-Module Az.ConnectedMachine -Force* before continuing.

### PowerShell

```
▶ $vm = Get-AzConnectedMachine -ResourceGroupName "<Insert Resource Group Name>" -  
$mdePackage = Invoke-AzRestMethod -Uri https://management.azure.com/subscription  
  
$protectedSetting = @{  
    "defenderForEndpointOnboardingScript" = ($mdePackage.content | ConvertFrom-J  
    }  
}
```

```

$Setting = @{
    "azureResourceId" = $vm.Id
    "vNextEnabled" = $true
}
New-AzConnectedMachineExtension -Name 'MDE.Windows' -ExtensionType 'MDE.Windows'

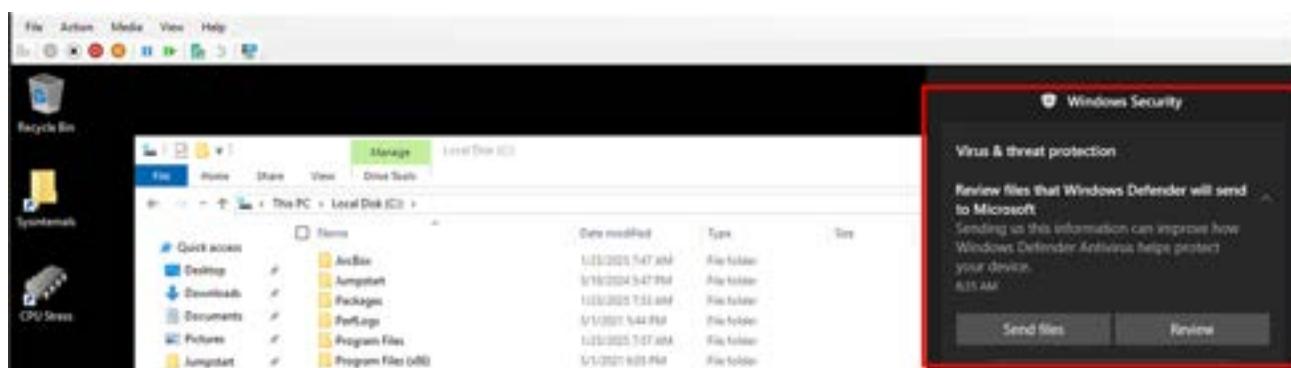
```

- 3. Wait for the installation of the MDE.Windows extension to be successful, then on the *ArcBox-Client* VM, go to Hyper-V manager and logon to the *ArcBox-Win2k25* VM using *JS123!!* as the Administrator password. Create an empty text file in the C: drive. Use the browser to open this [site](#) and find the malware test string. Copy the test string to the empty text file you created and save it as test.txt on the C: drive.



- 4. The local Anti-Malware software should detect this simulated threat on the *ArcBox-Win2k25* VM. Navigate to the Security tab of the *ArcBox-Win2k25* Arc-enabled server in the portal

**It might take up to 20 minutes or more for the alert to show up in the portal, you can move to the next exercise or lab and come back later to see the results if you prefer. This way, you can make better use of your time in this workshop.**



The screenshot shows the Microsoft Defender for Cloud portal interface. On the left, there's a navigation sidebar with various sections like Overview, Activity log, Access control (PAA), Tags, Diagnose and solve problems, Settings, Firewall, and Security (which is highlighted with a red box). The main content area has a header "Microsoft Defender for Cloud - Portal". Below the header, there are two cards: "For enhanced security visibility, update your cloud resources to Cloud Defender for Cloud" and "Use Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more". A "Recommendations" section follows, showing 3 items, 1 of which is selected. The selected recommendation is about Windows servers being configured in non-secure communication protocols. The "Security incidents and alerts" section is also highlighted with a red box, showing 2 open alerts, 2 active alerts, 0 in-progress alerts, and 1 affected resource. One alert listed is "TLS/SSL/TLS validation was prevented" from Microsoft.

5. You can also see the alerts from the *Defender for Cloud* portal, in the *Security alerts* pane. **If you don't see the alerts, make sure to select the Information severity in the filters..**

This screenshot shows the Microsoft Defender for Cloud portal's Security alerts page. The left sidebar includes General, Recommendations, Attack path analysis, Security alerts (which is selected and highlighted with a red box), Inventory, Cloud Security Engine, Workbooks, Community, Diagnose and solve problems, Cloud Security, and DevOps security (previewed). The main pane displays security statistics: 2 Open alerts, 2 Active alerts, 0 In progress alerts, and 1 Affected resource. A search bar and a filter for "Open alerts by severity" are present. A modal window titled "Severity" is open, showing a dropdown menu with "Information" selected. Other options in the dropdown are "Select all", "High", "Medium", "Low", and "Information".

This screenshot shows the Microsoft Defender for Cloud portal's Security alerts page with a different filter applied. The left sidebar and overall layout are similar to the previous screenshot. The "Severity" filter dropdown is open, showing "Information" selected. Other options are "Select all", "High", "Medium", "Low", and "Information". The main pane shows the same security statistics: 1 Open alerts, 1 Active alerts, 0 In progress alerts, and 1 Affected resource. The alert listed is "TLS/SSL/TLS validation was prevented" from Microsoft.

**Task 1 has been completed**

## Exercise 2 - Configure vulnerability assessment on your machines

---

### **Objective**

This exercise will walk you through enabling a vulnerability assessment solution on your machines.

### **Estimated Time to Complete This Lab**

20 minutes

### **Explanation**

In this exercise, you will learn how to configure a vulnerability assessment on your machines and view detected vulnerabilities.

## Task 1: Configure vulnerability assessment on your machines

---

- 1. After about 20-30 minutes from setting up Defender plans for servers (done in Lab01), you should start seeing recommendations for the Arc-enabled machines in the "Security" blade.
- 2. You should find the recommendation *Machines should have vulnerability findings resolved* if the vulnerability assessment has been enabled automatically on the subscription. Click on the recommendation.

The screenshot shows the Microsoft Defender for Cloud interface for an Arcbox-Win2k25 machine. The left sidebar lists various monitoring and configuration options. The main area displays a summary of findings: 5 recommendations and 1 security alert. A specific recommendation is highlighted with a red border: "Machine should have vulnerability findings resolved". Below this, there's a section for "Security incidents and alerts" with one entry: "Machine should have vulnerability findings resolved". The interface includes a legend for severity levels: High (red), Medium (blue), Low (green), and Info (yellow).

Machines should have vulnerability findings resolved

Severity: Low Findings interval: 12 Hours Tactics and techniques: Initial Access +5

Description: Identifying vulnerability findings on virtual machines is a recommended step in maintaining a secure environment. These findings, identified by vulnerability assessment solutions, highlight potential weaknesses that could be exploited by malicious actors. If these vulnerabilities are not addressed, they could lead to unauthorized access, data breaches, or even system failure. Therefore, it is important to resolve these findings promptly to ensure the security and integrity of the virtual machines.

Related recommendations (0)

Recommendation: Machines should have a vulnerability assessment solution Dependency type: Prerequisite Affected resources: 0 of 0

Remediation steps:

Security checks:

Findings: Disabled findings

ID	Security check	Category	Severity
CVE-2020-0001	Update Microsoft PowerShell	Update	High
CVE-2020-0002	Update Microsoft Windows Server 2019	Update	High
CVE-2020-0003	Update Microsoft Edge Chromium 80	Update	High
CVE-2020-0004	Update Microsoft Java Framework	Update	High

Showing 1 - 4 of 4 results.

Total actions: Trigger high-sev | Escalate | Assign review |

This means that Vulnerability Assessment is working on the server and you can end this lab at this point.

3. If you do not see this recommendation, click on the *Machines should have a vulnerability assessment solution*

Archiebox-Win2k25 | Security

Recommendations: 1 | Security alerts: 0 | Machine health: 0

Machine should have a vulnerability assessment solution

Description: Archiebox-Win2k25 needs your attention! Microsoft indicates for "Low" threat level. Fix it now!

Fix

Details for this recommendation: Archiebox-Win2k25 needs your attention! Microsoft indicates for "Low" threat level. Fix it now!

Recommendations: 1 | Security alerts: 0 | Machine health: 0

Machine should have a vulnerability assessment solution

Description: Archiebox-Win2k25 needs your attention! Microsoft indicates for "Low" threat level. Fix it now!

Fix

Details for this recommendation: Archiebox-Win2k25 needs your attention! Microsoft indicates for "Low" threat level. Fix it now!

Security incidents and alerts:

Details for this recommendation: Archiebox-Win2k25 needs your attention! Microsoft indicates for "Low" threat level. Fix it now!

Fix

4. Click on the "Machines should have a vulnerability assessment solution" recommendation and click "Fix"

Home > Azure Arc Machines > Arborbox-Win2025 | Security

## Machines should have a vulnerability assessment solution

● Change ● View policy definition ● Open query

Announcement in the Microsoft Defender for Cloud blog, and as part of our ongoing efforts to enhance the vulnerability management experience the "Bring Your Own License" (BYOL) feature in Microsoft Defender for Cloud is being deprecated. Reminder: Effective February 3, 2023, BYOL is no longer available for new machines and subscriptions. This serves as a reminder that new deployments must utilize alternative vulnerability management solutions.

Effective May 1, 2023, BYOL will be fully deprecated.

We recommend transitioning to the Microsoft Vulnerability Assessment solution or leveraging SSM resources to integrate external sources.

Severity: Medium Address interval: 24 Hours

● Description: Defender for Cloud regularly checks your connected machines to ensure they're running vulnerability assessment tools. Use this recommendation to deploy a vulnerability assessment solution.

● Related recommendations (1): Recommendation T<sub>1</sub> Dependency type: T<sub>2</sub> Affected resources: T<sub>3</sub>  
Machines should have vulnerability scanning enabled Deployed 20 of 25

● Remediation steps:

Fix now Trigger log scan Create alert Assign owner



Microsoft Azure Search resources, services, and docs (G+J) Copilot

Home > Azure Arc Machines > Arborbox-Win2025 | Security > Machines should have a vulnerability assessment solution >

## Machines should have a vulnerability assessment solution

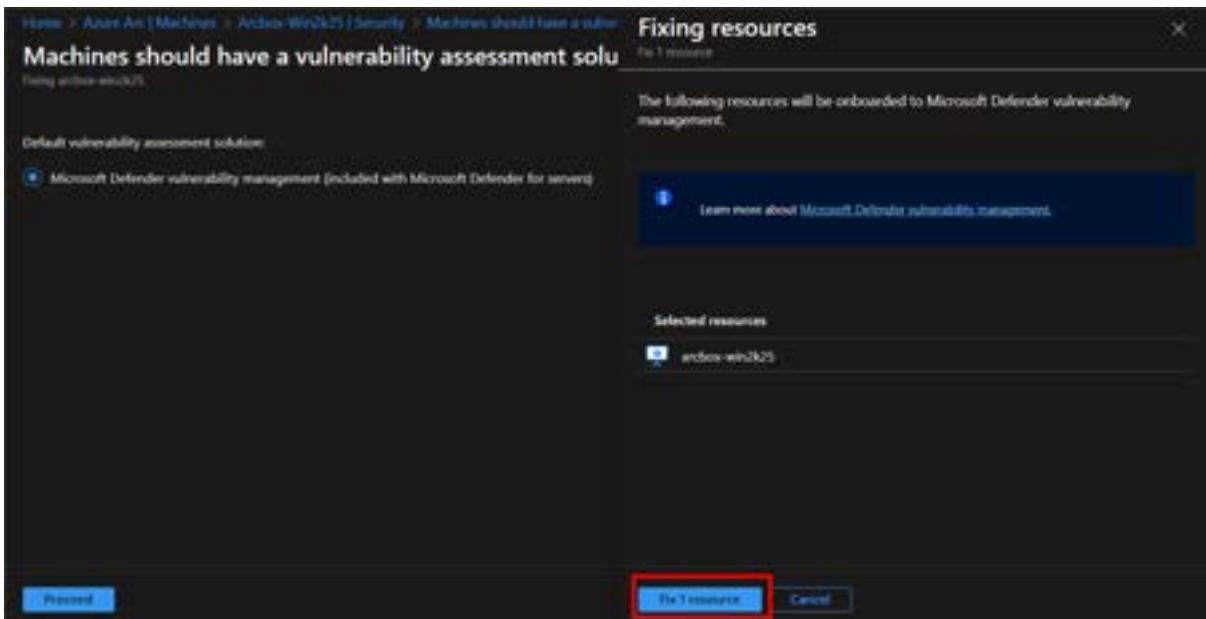
Fixing arborbox-win2025

Default vulnerability assessment solution:

Microsoft Defender vulnerability management (included with Microsoft Defender for servers)

Proceed





The screenshot shows the Microsoft Defender portal interface. At the top, it displays the navigation path: Home > Azure Arc | Machines > Andbox-Win2k25 | Security > Machines should have a vulnerability assessment solution. Below this, a sub-header reads 'Machines should have a vulnerability assessment solution'. A note below the header states 'Fixing andbox-win2k25.' Under the sub-header, there are three buttons: 'Exempt', 'View policy definition', and 'Open query'. A warning message is displayed: 'As highlighted in the Microsoft Defender for Cloud blog, and as part of our ongoing efforts to enhance the vulnerability management experience, the "Bring Your Own License" (BYOL) license in Microsoft Defender for Cloud is being deprecated. Recommended: Effective January 1, 2023, BYOL is no longer available for new machines and subscriptions. This serves as a reminder that new deployments must utilize Microsoft's vulnerability management solutions.' Below this, the policy details are shown: Severity is 'Medium', Freshness interval is '24 Hours'. The 'Description' section notes that Defender for Cloud regularly checks connected machines to ensure they're running vulnerability assessment tools. The 'Related recommendations' section lists 'Machines should have vulnerability findings' (1 recommendation, 1 affected resource). The 'Remediation steps' section is collapsed. At the bottom, there are buttons for 'Fix', 'Trigger logon user', 'Assign', and 'Assign owner'. On the right side, a 'Notifications' pane is open, showing a success message: 'Remediation successful: Successfully remediated the issue for the selected resources. Note: It can take several minutes after remediation completes to see the resources in the Healthy resources tab.' The timestamp 'a few seconds ago' is visible next to the message.

**Task 1 has been completed**

**Congratulations, you have completed all tasks in this lab**

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB04: Governance across Azure Arc-enabled servers using Azure Policy and Azure Machine Configuration

---

## Student Lab Manual

### Table of Contents

**Exercise 1** - Enforce governance across your Azure Arc-enabled servers using Azure Policy

[\*\*Task 1: Assign a built-in Azure Policy to the Arc resource group\*\*](#)

[\*\*Task 2: Examine the policy compliance\*\*](#)

[\*\*Task 3: Using the Guest Assignments views directly\*\*](#)

**Exercise 2** - Configure your Azure Arc-enabled servers using Azure Machine Configuration

[\*\*Task 1: Create Machine Configuration - custom configurations for Windows\*\*](#)

# **Exercise 1 - Enforce governance across your Azure Arc-enabled servers using Azure Policy**

---

## **Objective**

In this module you will use Azure Policy to Audit Arc-enabled Linux servers that have a certain application installed.

## **Estimated Time to Complete This Lab**

30 minutes

## **Explanation**

In this exercise, you will learn how to use Azure Policy to audit Arc-enabled Linux machines that have a specific application installed.

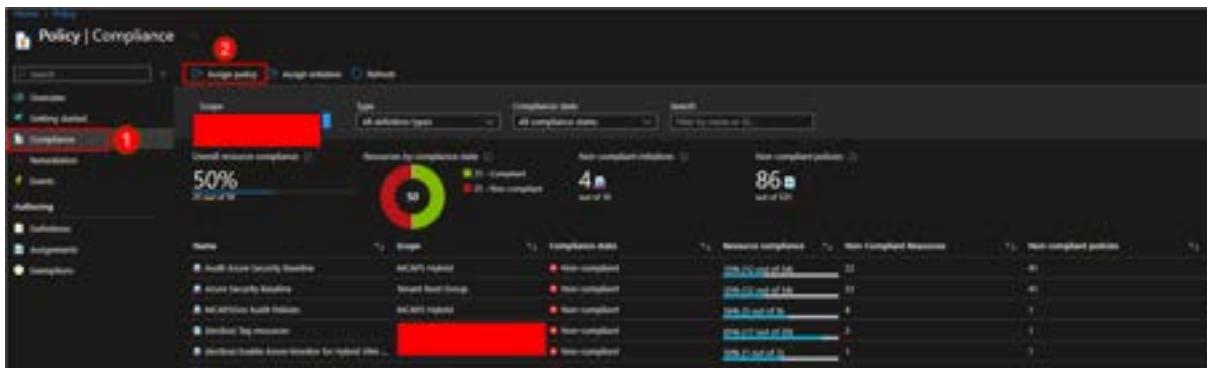
## Task 1: Assign a built-in Azure Policy to the Arc resource group

Azure policy can be assigned at Management Group, Subscription or Resource Group scope.

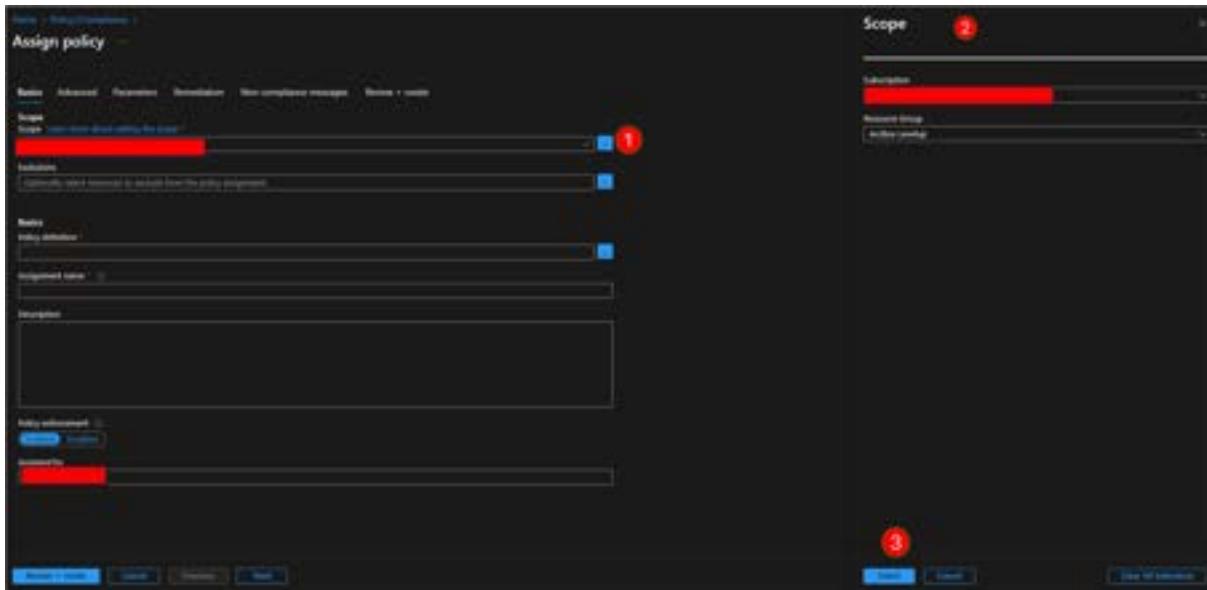
- In this scenario we will use the Resource Group scope.
- We will show two ways to accomplish this first task. **First we will use the Azure portal** (but if you prefer to use Powershell then skip to that section at the end of this first task)

1. In the Azure Portal search for the "Policy" resource and navigate to it.

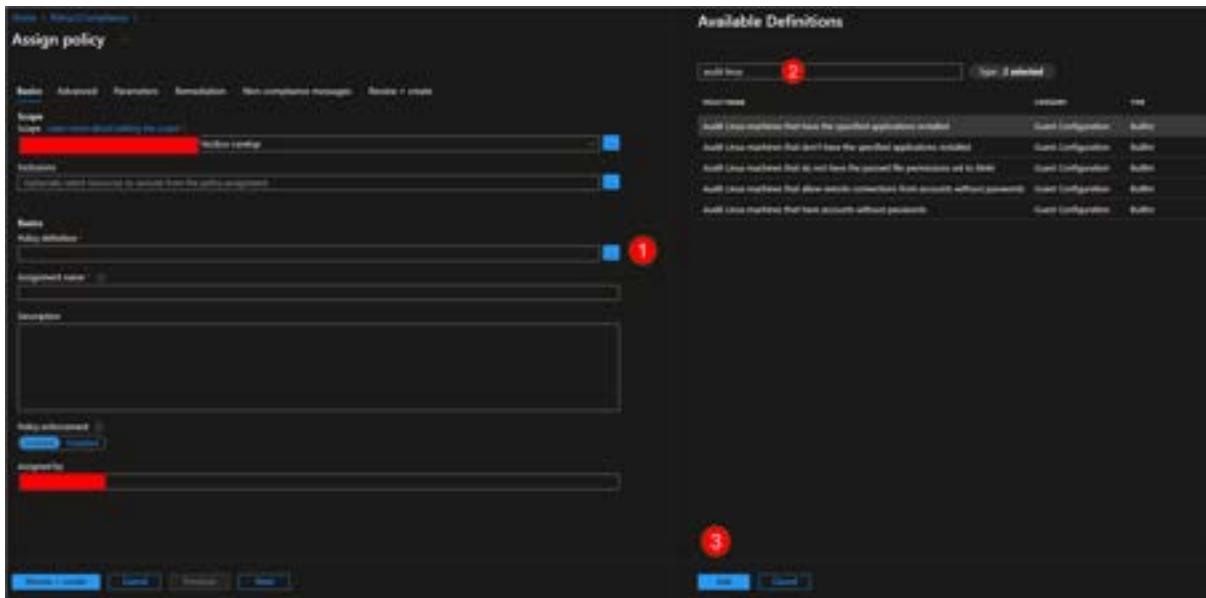
2. Click on "Compliance" in the left menu then click "**Assign policy**".



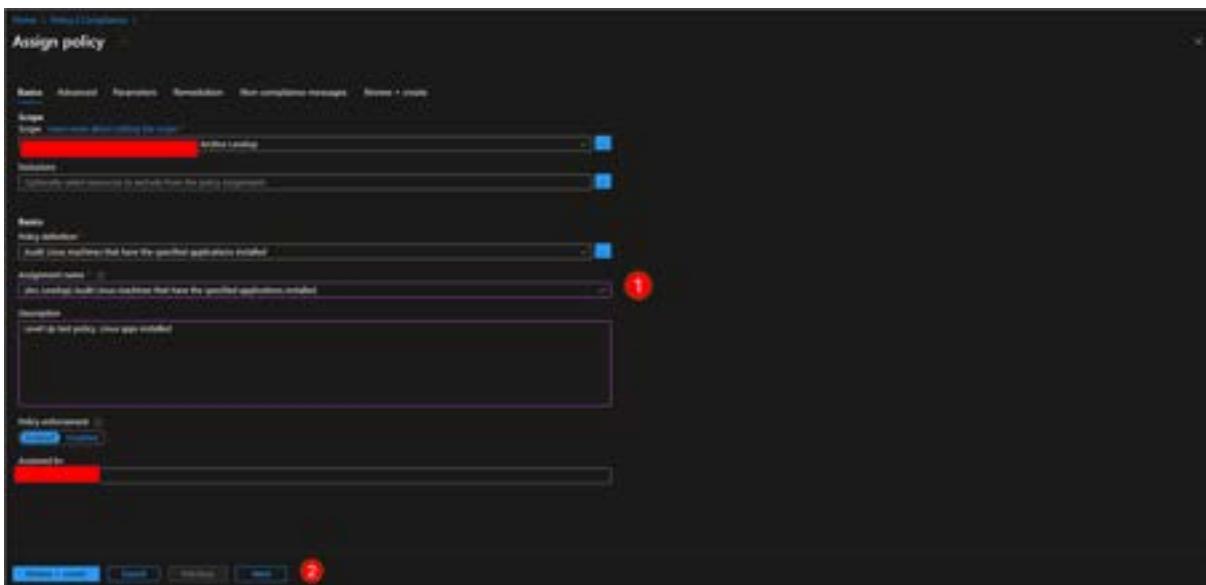
3. Set the scope of the policy assignment to the Subscription and the Resource Group as shown below:



4. Click on the ellipsis next to "Policy definition". This opens the "Available Definitions" panel, where you can start searching for "**Audit Linux machines that have the specified applications installed**" policy which belongs to the "Guest Configuration" category. Select this policy as shown below:



5. Modify the "Assignment name" so that it would be easy to identify our policy in the compliance list later as shown below, then click "Next" twice to reach the "Parameters" tab.



6. On the "Parameters" Screen, set the "**Include Arc connected servers**" to "**true**" and then set the name/s of the application/s you want to audit the Linux servers for. If you have more than one application then include them in a semicolon separated list enclosed in single quotes e.g. 'App1; App2; App3'.

## Assign policy

Basics

**Parameters**

Remediation

Non-compliance messages

Review + create



Search by parameter name



Only show parameters that need input or review

Include Arc connected servers \* ⓘ

true

Application names \* ⓘ

nano

7. Move to the "Non-compliance message" tab to add a message of your choice.

## Assign policy

Basics

Parameters

Remediation

**Non-compliance messages**

Review + create

Non-compliance messages help users understand why a resource is not compliant with the policy. The message will be displayed when a resource is denied and in the evaluation details of any non-compliant resource.

Non-compliance message

Application should not be installed

8. Next move to the "Review + create" tab and click "**Create**" to assign the policy.

- If you want to use **Powershell as an alternative method** to assign the policy, then the following procedure accomplishes the same as the portal method explained above.

- Run the following powershell commands making sure you use the correct resource group name

PowerShell

```
> '{
    "IncludeArcMachines":{
```

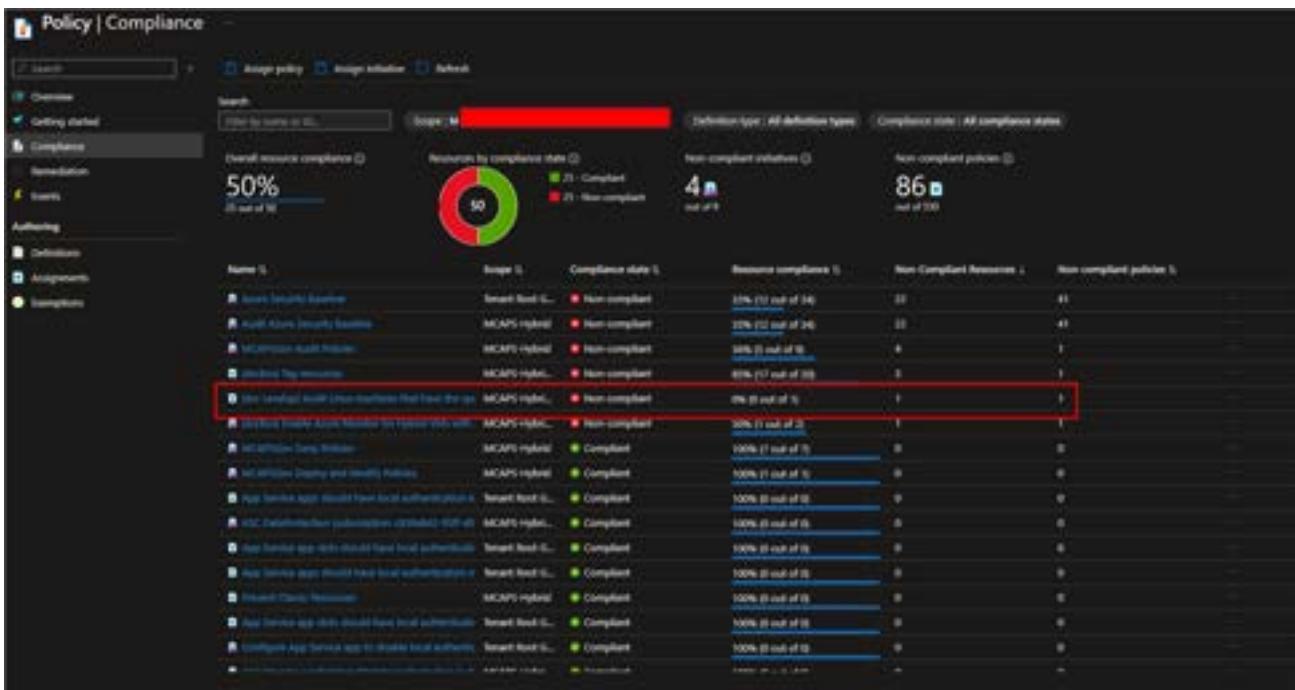
```
        "value":"true"
    },
    "ApplicationName": {
        "value":"nano"
    }
}' > .\params.json
$ResourceGroup = Get-AzResourceGroup -Name 'ArcBox'
$Policy = Get-AzPolicyDefinition -BuiltIn | Where-Object {$_.DisplayName -eq 'Audit Linux machines with nano in'}
New-AzPolicyAssignment -Name '(Arc Workshop) Audit Linux machines with nano in'
```

**Task 1 has been completed**

Click **Next** for the next task or [go back to the main table of content](#)

## Task 2: Examine the policy compliance

- The creation of the assignment and for it to take effect and get evaluated might take some time. You can keep refreshing the "Compliance" list until you can see an indication that there is at least one resource which is non-compliant with the policy we created (this depends on how many Arc-connected Linux servers with the specified applications we have).
- If this does not happen in a reasonable time then you can go to [task 3](#) where there is another view that might faster to show the compliance indication\*\*.
- We can also attempt to use PowerShell force a policy scan (see note at end of this task) which **might** improve the speed to populate the compliance dashboard.



- 1. Click on the policy from the name column and this will take you to a more detailed view of the specific policy compliance as shown below. You can then click on "Details" which will open another panel on the right hand side.
- If the "**Details**" link is not ready yet then you will need to wait for it, or try [task 3](#) for another way of looking at the compliance of specific servers, which might be faster to populate.

The screenshot shows the Azure Policy Compliance blade. At the top, it displays 'Overall resource compliance' at 0% and 'Resource by compliance state' with a red circle containing the number 1. Below this, there's a table titled 'Resource Compliance - Items'. One row in the table is highlighted with a red box and a red circle containing the number 1. This row corresponds to a server named 'not\_installed\_application\_linux' which is marked as 'Non-compliant'. To the right of the table, there's a detailed view of the 'Reason for non-compliance' section, which includes a red box and a red circle containing the number 2. It states: 'Reason for non-compliance: No agent extension exists for the chosen resource in the policy definition.' and 'Last evaluated resource level of 11'.

- 2. Click on the link below "Last evaluated resource ...". This will open the "Guest Assignment" screen showing exactly why that specific server is not compliant with the policy.

The screenshot shows the 'Guest Assignment' blade for the server 'not\_installed\_application\_linux'. The top navigation bar shows the full path: 'ArcBox-Ubuntu-01 / not\_installed\_application\_linux / Guest Assignment'. The main area displays the server details: 'Name: not\_installed\_application\_linux', 'Compliance status: Non-compliant', and 'Reason: The package 'rsync' is expected to run the modified rsync command on the local system'. A red box highlights the 'Reason' section, and a red circle containing the number 1 points to the 'Guest Assignment' link in the top right corner of the blade.

- The steps above helps you identify non-compliant resources and then you can act on resolving the non-compliance reasons.

- (Optional): As mentioned at the beginning of this task, **to force a policy scan** we can use the [Start-AzPolicyComplianceScan](#) PowerShell command.

For example the following PowerShell commands will focus the scan on our resource group, run the scan as a job and wait for it to complete in the background. Make sure you use the correct resource group name:

#### PowerShell

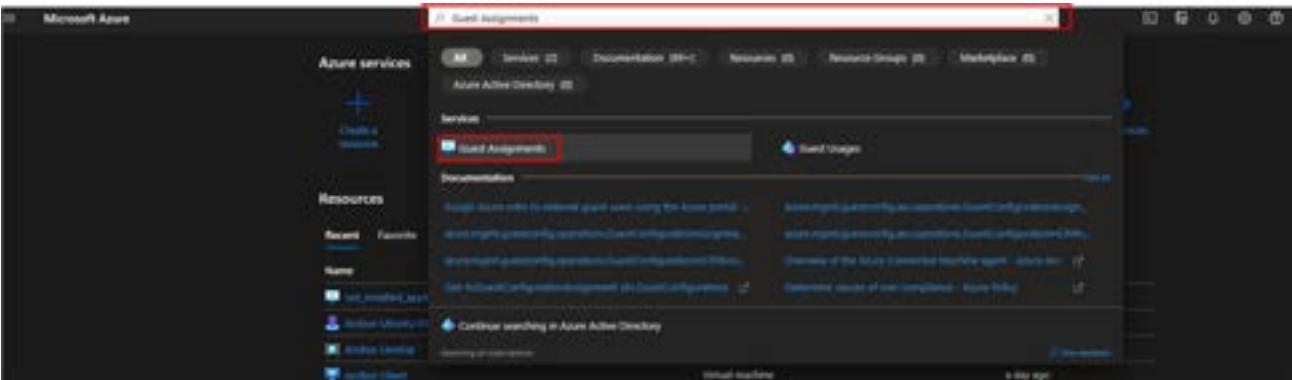
```
► $job = Start-AzPolicyComplianceScan -ResourceGroupName "ArcBox" -AsJob  
$job | Wait-Job
```

### Task 2 has been completed

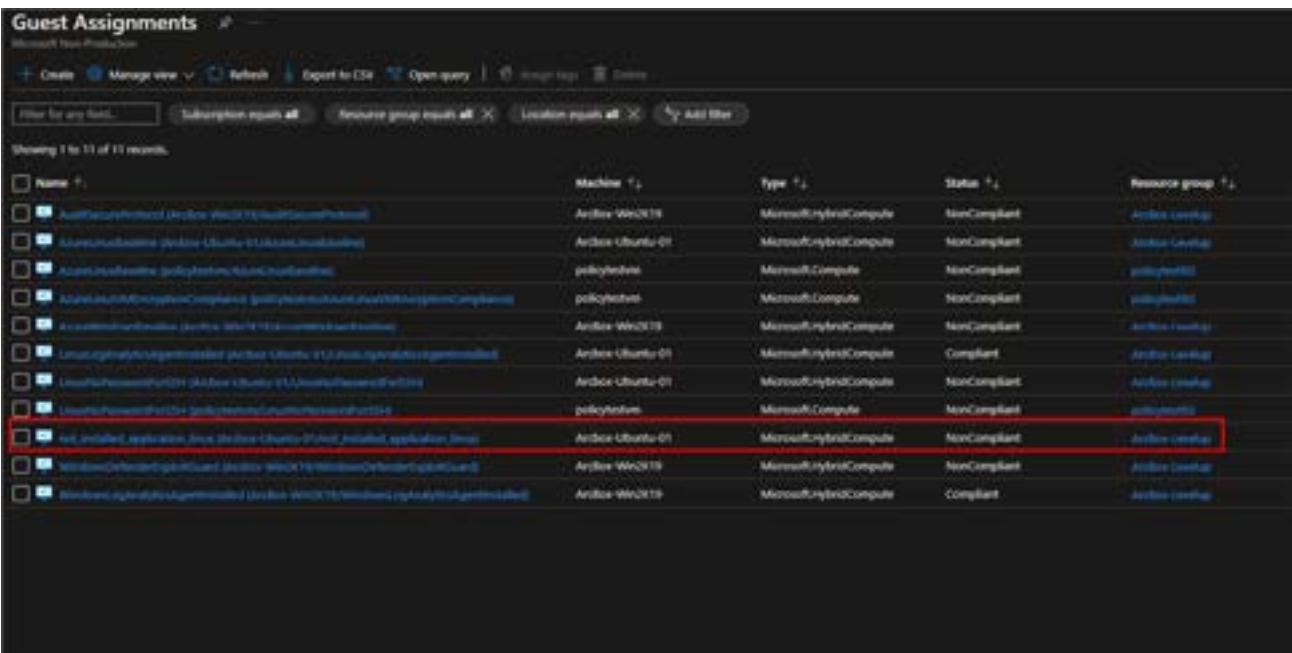
Click **Next** for the next task or [Go back to the main table of content](#)

## Task 3: Using the Guest Assignments views directly

- As mentioned in [task 2](#), the policy compliance dashboard can sometimes take a long time before it is updated with the accurate compliance details.
- 1. We can use a direct route to view the "**Guest Assignments**" for each resource by searching for "Guest Assignments" from the Azure portal and selecting it.



- 2. You can now look at the compliance of the individual resources and identify the ones that are affected by our policy assignment.



Name	Machine	Type	Status	Resource group
Autodesk.com VM (Ubuntu 20.04 LTS)	Autodesk-Win2019	MicrosoftHybridCompute	NonCompliant	Autodesk-London
Autodesk.com VM (Ubuntu 20.04 LTS) - Compliant	Autodesk-Ubuntu-01	MicrosoftHybridCompute	NonCompliant	Autodesk-London
Autodesk.com VM (Ubuntu 20.04 LTS) - NonCompliant	policy-ubuntu	MicrosoftCompute	NonCompliant	policy-ubuntu
Autodesk.com VM (Ubuntu 20.04 LTS) - NonCompliant	policy-ubuntu	MicrosoftCompute	NonCompliant	policy-ubuntu
Autodesk.com VM (Ubuntu 20.04 LTS) - NonCompliant	Autodesk-Win2019	MicrosoftHybridCompute	NonCompliant	Autodesk-London
Autodesk.com VM (Ubuntu 20.04 LTS) - NonCompliant	Autodesk-Ubuntu-01	MicrosoftHybridCompute	Compliant	Autodesk-London
Autodesk.com VM (Ubuntu 20.04 LTS) - NonCompliant	Autodesk-Ubuntu-01	MicrosoftHybridCompute	NonCompliant	Autodesk-London
Autodesk.com VM (Ubuntu 20.04 LTS) - NonCompliant	policy-ubuntu	MicrosoftCompute	NonCompliant	policy-ubuntu
Autodesk.com VM (Ubuntu 20.04 LTS) - NonCompliant	Autodesk-Ubuntu-01	MicrosoftHybridCompute	NonCompliant	Autodesk-London

- 3. Click on the identified policy/resource combination and this will take you to the screen that we saw earlier at the end of [task 2](#), showing the details of the compliance/non-compliance.

**Task 3 has been completed**

Click **Next** for the next exercise or [Go back to the main table of content](#)

## **Exercise 2 - Configure your Azure Arc-enabled servers using Azure Machine Configuration**

---

### **Objective**

In this module, you will learn to create and assign a custom Machine Configuration to an Azure Arc-enabled Windows servers to create a local user and control installed roles and features.

### **Estimated Time to Complete This Lab**

30 minutes

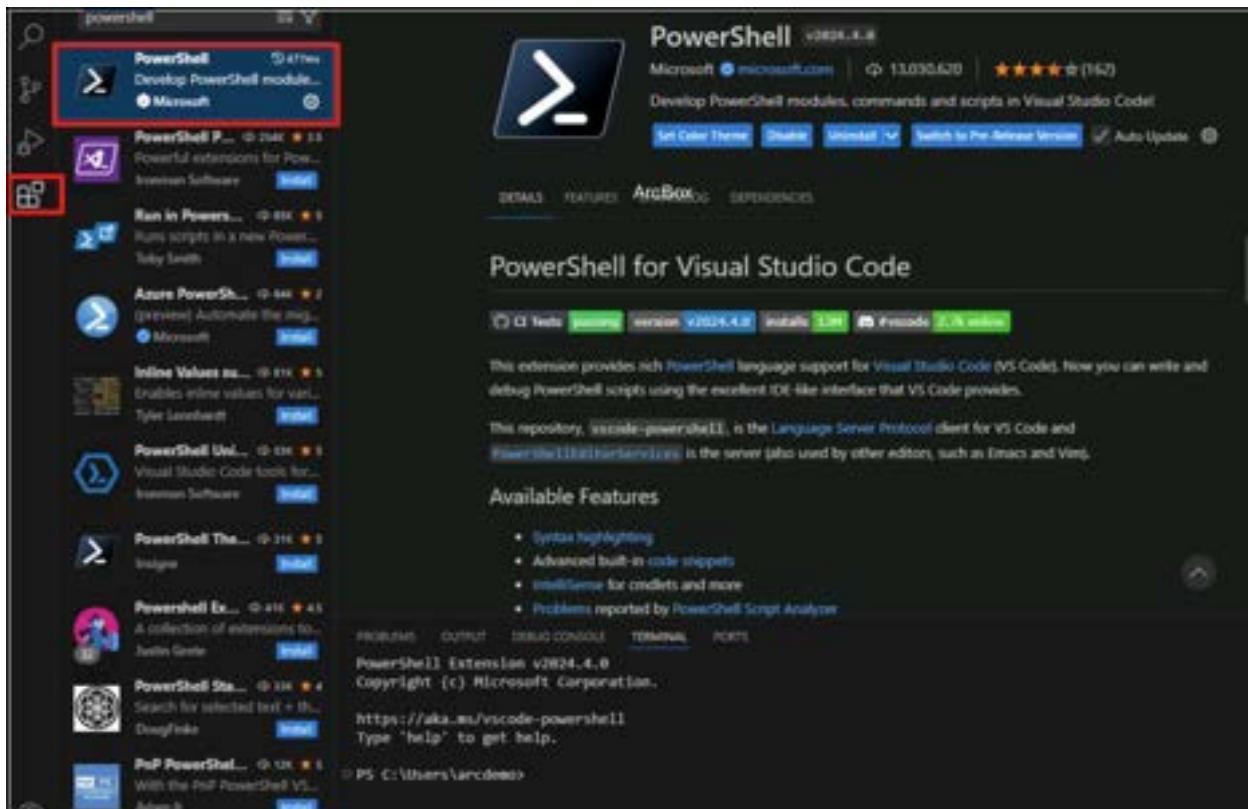
### **Explanation**

In this exercise, you will learn how to use Azure Machine Configuration to configure an Arc-enabled machine declaratively by creating a local user and installing a Windows Server role.

## Task 1: Create Machine Configuration - custom configurations for Windows

We will be using the **ArcBox Client** virtual machine for the configuration authoring.

1. RDP into the *ArcBox-Client* VM
2. Open **Visual Studio Code** from the desktop shortcut. Check if the Microsoft PowerShell Plugin is installed, if not then install it.



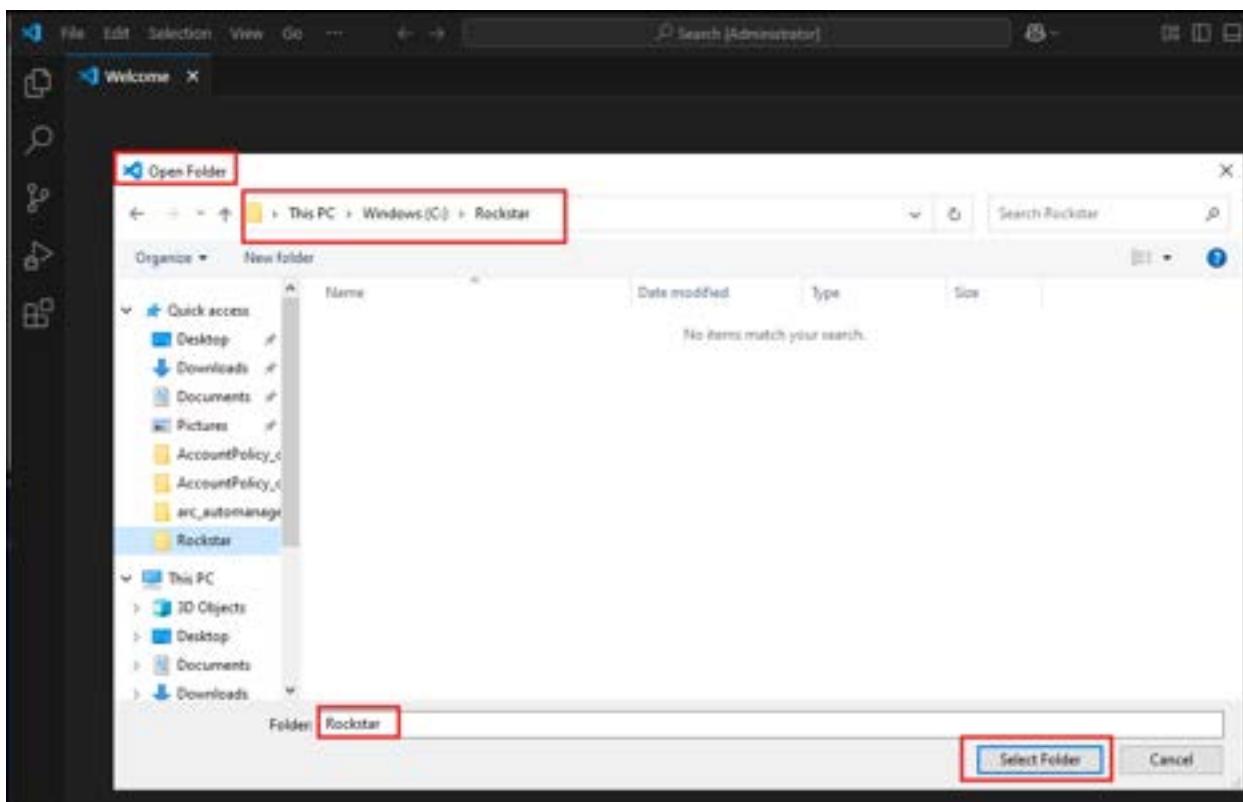
3. Copy Rockstar.zip from [https://github.com/microsoft/Azure\\_Arc\\_Workshop/raw/main/scripts/Rockstar.zip](https://github.com/microsoft/Azure_Arc_Workshop/raw/main/scripts/Rockstar.zip)
4. Unzip contents to C:\Rockstar\

## Custom configuration for Windows

A screenshot of Windows File Explorer. The address bar shows the path: This PC > Windows (C:) > Rockstar. The left sidebar lists 'Quick access', 'Desktop', 'Downloads', 'Documents', 'Pictures', and several folders named 'AccountPolicy\_c', 'arc\_automange', and 'Rockstar'. The main pane displays a table with the following data:

Name	Date modified	Type	Size
1. Azure Arc Policy Install Modules	5/7/2025 7:17 PM	PowerShell Source...	1 KB
2. Connect to Azure	5/7/2025 9:23 PM	PowerShell Source...	1 KB
3. Create Storage Account	5/7/2025 8:59 PM	PowerShell Source...	1 KB
4. Create Account Policies to MOF	5/7/2025 8:59 PM	PowerShell Source...	3 KB
5. Create a package	5/7/2025 8:59 PM	PowerShell Source...	1 KB
6. Test Package Policy Function	5/7/2025 8:59 PM	PowerShell Source...	1 KB
7. Up Load Package to Storage Account	5/7/2025 9:23 PM	PowerShell Source...	2 KB
8. Create an Azure Policy definition	5/7/2025 8:59 PM	PowerShell Source...	1 KB
9. Create Az Policy Definition in Azure Po...	5/7/2025 9:23 PM	PowerShell Source...	1 KB

5. In Visual Studio go to **File, Open Folder** and select **Rockstar**.



6. Start with code snippet **1** and run each in order until you finish with **9**.

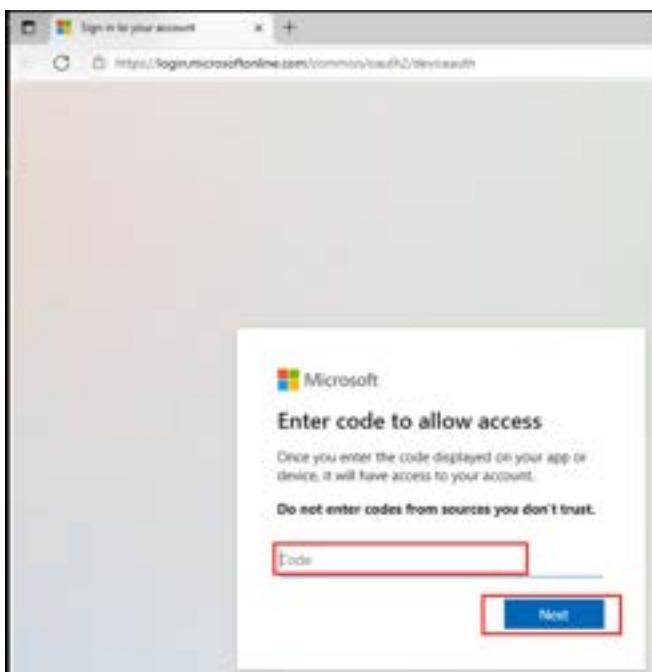
The screenshot shows a Windows desktop environment with VSCode open. The terminal tab is active, displaying a series of PowerShell command snippets. The code snippets are numbered 1 through 9 and correspond to the steps listed below. The terminal window has a dark theme and shows the IP address 40.69.169.96 at the top right.

```
> 1. Azure Arc Policy Install Modules.ps1 > 2. Connect to Azure.ps1 > 3. Create Sto...
> 1. Azure Arc Policy Install Modules.ps1
1: # Install Guest Configuration module and if not already present
2: Install-Module -Name GuestConfiguration -scope AllUsers
3: Install-Module -Name Az -scope AllUsers
4: Install-Module -Name PSDscResources -scope AllUsers
5: Install-Module -Name SecurityPolicyDsc -scope AllUsers
6: Install-Module -Name AuditPolicyDsc -scope AllUsers
```

[!knowledge] To run each additional code snippet you paste in VSCode, highlight the code you need to run and press **F8**.

[!knowledge] You can also run the rest of the code snippets in PowerShell directly without using VScode if you prefer.

7. The code snippet **1** is to install the required PowerShell modules.
8. The code snippet **2** is to **Connect using your own account**. You will need to sign in using the web browser. i.e To sign in, use a web browser to open the page <https://microsoft.com/devicelogin> and enter the code sample **dfkjdkfh** to authenticate
9. Connect to the Browser on **Arcbox-Client**. Enter Code and Click **Next**.



Note output:

# Account	SubscriptionName TenantId	Environment
# philbr@azures.microsoft.com	Sub1 885e7c88-b5df-4b07-89c7-029asfd2e40b AzureCloud	

10. Code snippet **3** creates the **Storage Account**

StorageAccountName	ResourceGroupName	PrimaryLocation	SKUName	Kind	AccessTier	CreationTime	ProvisioningState	EnableHttpsTrafficOnly	LastError
storageaccountstar	Arctics	centralus	Standard_LRS	StorageV2	Hot	5/13/2025 5:00:52 PM	Succeeded	True	

11. Code snippet **4** creates the **MOF File**. This will check for compliance and do the remediation.

# Output	# Directory: C:\Rockstar\AccountPolicy_config		
#Mode	LastWriteTime	Length	Name
#---	5/7/2025 7:39: PM	3567	localhost.mof

12. Code snippet **5** creates a package zip file to be uploaded to the storage account.

## Output	## Name	Path
## ----	## ----	## ----
## AccountPolicy_config	C:\Rockstar\AccountPolicy_config.zip	

13. Code snippet **6** tests package zip file against the local machine.

path\LocalProperties\1\0	AccountPolicy_config	complianceStatus
		False
		5/13/2025 7:39:57 PM
		AZUREAD-RIM-40FB-99A4-BD5E53B90405
		Compliance
		(@{complianceStatus=False; properties-> reason=System.Object[]; @({copyCompliance=True; properties-> reason=System.Object[]; @({complianceStatus=False; properties-> reason=System.Object[]}); @({copyCompliance=True; properties-> reason=System.Object[]})})-)
		5/13/2025 7:39:48 PM

14. Code snippet **7** Creates the AzStorageContainer, set the con and uploads the zip file.

# Output	# Name	blobType	Length	contentType	LastModified	accessTier_SnapshotTime	blobType	lastModified	blobType
# AccountPolicy_config.L_8K8zLk	836279	application/octet-stream	2025-05-07 18:58:32Z	None					

15. Code snippet **8** Creates an Azure Policy definition.

Name	Path	PolicyId
AccountPolicy_config	C:\Rockstar\AccountPolicy_config\policies\AccountPolicy_config_DeployIfNotExists.json	F4d3ef-78ba-4f30-8150-a91f81210005

16. Code snippet **9** Creates Az Policy Definition in Azure Policy.

## Assign Azure Policy

1. On the Arcbox-Client go to <https://portal.azure.com> go to **Policy**. Under **Authoring and Definitions**. Search (ArcBox).

Name	Latest version (ver.)	Definition location	Policy ID	Definition type	Category
(ArcBox) Account Login Policy Settings	1.0.0	Self	00000000-0000-0000-0000-000000000000	ChangeCheck/AllowDeny	Guest Configuration
(ArcBox) Change tracking and inventory for Arc-enabled machines	1.0.0	Self	00000000-0000-0000-0000-000000000000	Monitoring	
(ArcBox) Delete account from all connected Windows machines	1.0.0	Self	00000000-0000-0000-0000-000000000000	Monitoring	
(ArcBox) Delete account from all connected Linux machines	1.0.0	Self	00000000-0000-0000-0000-000000000000	Monitoring	
(ArcBox) Guest configuration settings	1.0.0	Self	00000000-0000-0000-0000-000000000000	Policy	Guest Configuration

2. Click on **(ArcBox) Account Login Policy Settings**.

Assignment	Description	Category	Definition
Guest Configuration	(ArcBox) Account Login Policy Settings	Guest Configuration	(ArcBox) Account Login Policy Settings

3. Click on **Assign Policy**.

Assignment	Description	Category	Definition
Guest Configuration	(ArcBox) Account Login Policy Settings	Guest Configuration	(ArcBox) Account Login Policy Settings

4. Click on the **ellipsis** to assign the **Resource Group**.

Home > Policy | Definitions > (ArcBox) Account Login Policy Settings >

### Assign policy

Basics Parameters Remediation Non-compliance messages Review + create

**Scope**

Scope \* Sub1

Learn more about setting the scope [\[?\]](#)

**Exclusions**

Optionally select resources to exclude from the policy assignment.

**Resource selectors (Expand)**

Using Resource selectors, you can further refine this assignment's applicability by targeting specific subsets of resources. Expand to learn more.

**Basics**

Policy definition \* (ArcBox) Account Login Policy Settings

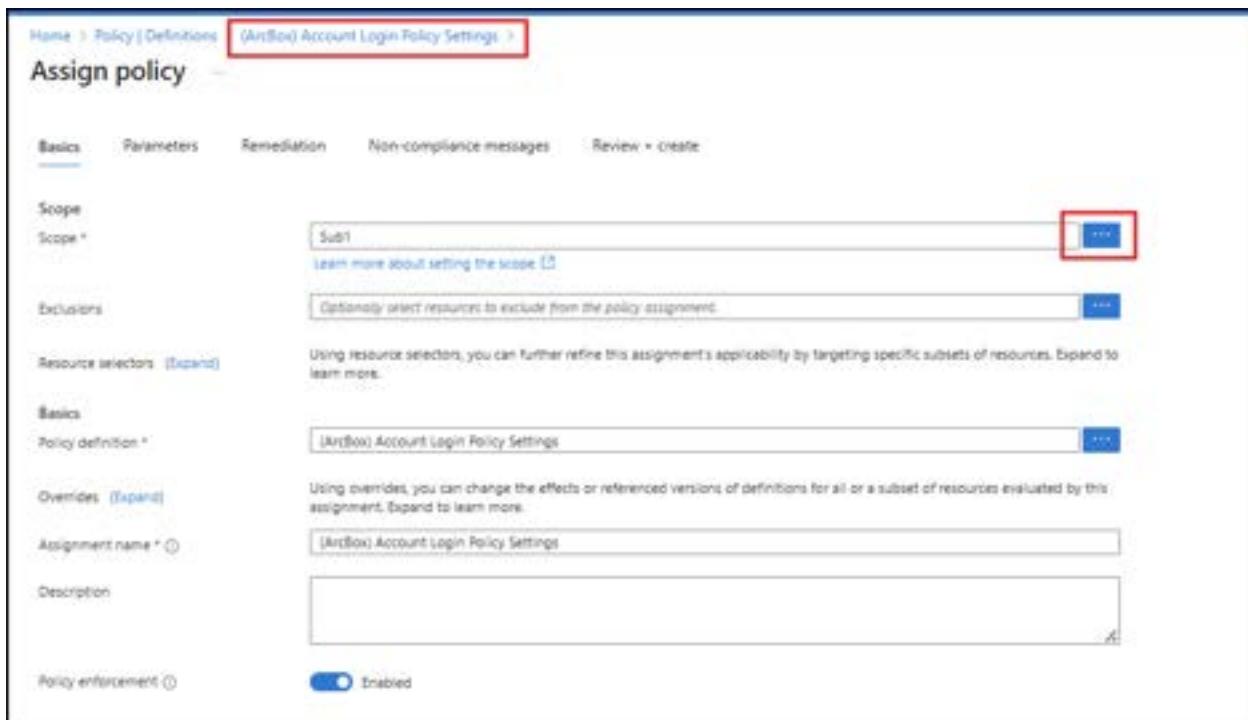
Overrides (Expand)

Using overrides, you can change the effects or referenced versions of definitions for all or a subset of resources evaluated by this assignment. Expand to learn more.

Assignment name \* (ArcBox) Account Login Policy Settings

Description

Policy enforcement  Enabled



5. Select the **Resource Group Arcbox**. Do not forget to click on **Select** on the bottom of the windows

### Scope

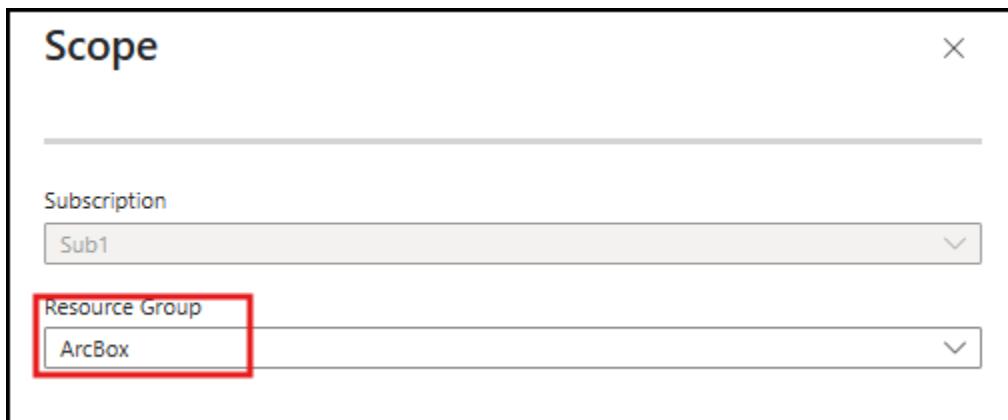
X

Subscription

Sub1

Resource Group

ArcBox



6. Select **Parameters**

Basics **Parameters** Remediation Non-compliance messages Review + create

Scope

Scope \* Sub1/ArcBox

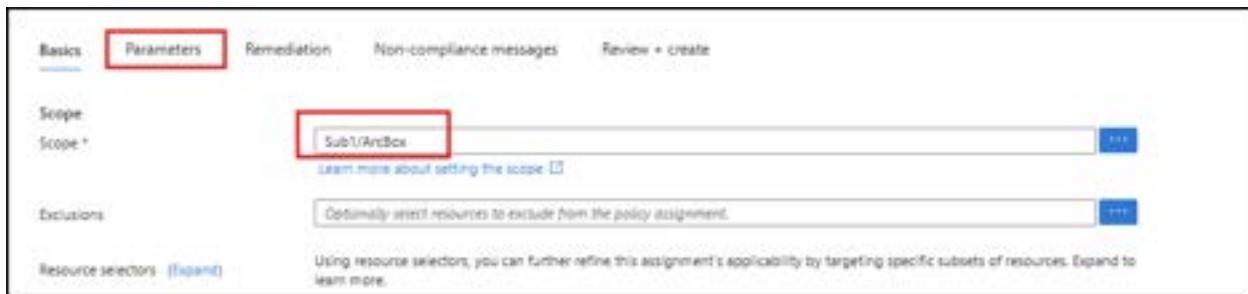
Learn more about setting the scope [\[?\]](#)

Exclusions

Optionally select resources to exclude from the policy assignment.

Resource selectors (Expand)

Using Resource selectors, you can further refine this assignment's applicability by targeting specific subsets of resources. Expand to learn more.



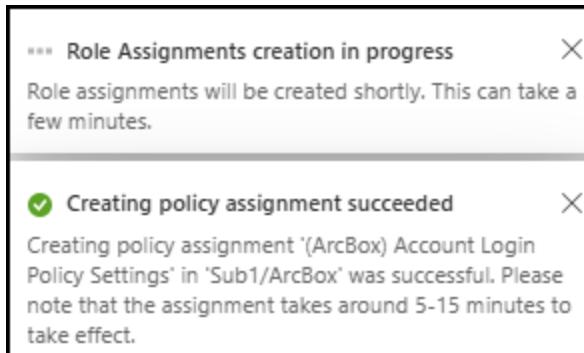
7. Make sure **Include Arc connected machines** is set to **true**.

The screenshot shows the 'Assign policy' interface. At the top, there are tabs for 'Basics', 'Parameters' (which is selected and underlined), 'Remediation', 'Non-compliance messages', and 'Review + create'. Below the tabs is a search bar labeled 'Search by parameter name' and a checkbox for 'Only show parameters that need input or review'. Under the 'Parameters' tab, there is a list of parameters. One parameter, 'Include Arc connected machines', is highlighted with a red box and has a value of 'true' in a dropdown menu. The 'Review + create' button at the bottom right of the tab area is also highlighted with a red box.

8. Click on **Review and Create**.

The screenshot shows the 'Review + create' page for the policy assignment. The 'Review + create' button is highlighted with a red box. The page is divided into several sections: 'Basics' (Scope: Sub1/ArcBox, Exclusions: none, Policy definition: (ArcBox) Account Login Policy Settings, Assignment name: (ArcBox) Account Login Policy Settings, Description: none, Policy enforcement: Default, Assigned by: Phil Bracher); 'Advanced' (Resource selectors: No selectors associated with this assignment, Overrides: No overrides associated with this assignment); 'Parameters' (Include Arc connected machines: true); 'Remediation' (Create a Managed Identity: Yes, Type of Managed Identity: System assigned managed identity, System assigned identity location: centralus, Create a remediation task: No); and 'Non-compliance messages' (Non-compliance messages: No non-compliance messages associated with this assignment).

9. Click on **Create** on the Bottom of the window. The **Policy is Assigned**.



## Check Azure Policy

1. To check policy compliance, in the Azure Portal, navigate to **Policy -> Compliance**
2. Set the scope to the resource group your instance of ArcBox is deployed to.



3. Filter for *(Arcbox)*



**[!alert] It may take 30 minutes or more for the policy remediation to be completed. You can move to the next exercise or lab and come back later to see the results if you prefer. This way, you can make better use of your time in this workshop.**

4. To get a Machine Configuration status for a specific machine, navigate to **Machines – Azure Arc** in the Azure Portal.
5. Click on ArcBox-Win2K25 -> **Machine Configuration**.

- If the status for *ArcBox-Win2K25/AccountPolicy\_Config..* is **not Compliant** or **Pending**, wait a few more minutes and click *Refresh*

Configuration Name	Version	Status	Rule	Type	Source
AccountPolicy_config	1.0	Non-compliant	10% (0 out of 9)	Audit	Azure Policy
AuthDecayProtection	1.1	Non-compliant	20% (0 out of 10)	Audit	Manual assignment
AccountMinimumLength	1.1	Non-compliant	30% (0 out of 34)	Audit	Manual assignment
MinPasswordStrength	1.1	Non-compliant	30% (0 out of 1)	Audit	Manual assignment

6. Click on *ArcBox-Win2K25/AccountPolicy\_Config..* to get a per-resource view of the compliance state in the assigned configuration

Name	Compliance state	Reason
(AccountPolicy)max_password_history	Non-compliant	Property 'minPasswordHistory' is Required: 34   Actual: 0. Property 'Name' is Required: 1   Actual: 0.
(AccountPolicy)max_Password_Len	Compliant	Actual: 10
(AccountPolicy)min_Password_Length	Non-compliant	Property 'minPasswordLength' is Required: 10   Actual: 0. Property 'Name' is Required: 1   Actual: 0.
(AccountPolicy)password_must_meet_complexity_requirements	Compliant	Actual: 10
(AccountPolicy)password_cooling_AgeBeforeExpiration	Compliant	Actual: 10
(AccountPolicy)account_lockout_threshold	Compliant	Actual: 10
(AccountPolicy)reset_Account_Coolout_Counter_Step	Non-compliant	Property 'Name' is Required: 1   Actual: 0. Property 'ResetAccount_Coolout_Counter_Step' is Required: 10   Actual: 0.
(AccountPolicy)reset_Account_Coolout	Non-compliant	Property 'Name' is Required: 1   Actual: 0. Property 'ResetAccount_Coolout' is Required: 1   Actual: 0.

## Remediate The Azure Policy

- To Remediate the Policy for a specific machine, navigate to **Policy** in the Azure Portal. Select **Remediation**. Filter for **(Arcbox)**. Select **(ArcBox) Account Login Policy Settings**.

Home > Policy

Policy | Remediation

Search: Arcbox

Overview Getting started Compliance Remediation Events Authoring Definitions Assignments Exemptions

Policy Definition 1: (Untitled) Account login Policy Settings

Assignment 1: K (Arcbox) Account login Policy Settings

Resources to Remediate 1: 4

Scope 1: Sub/Arcbox

2. Select Resources to Remediate and choose **Arcbox-win2k25**. Then Click on **Remediate**

New remediation task

Issue: Sub/Arcbox

Remediation Option

Select location(s) for this remediation to take place

All selected

Select specific resources to remediate

Remediation settings

Failure Threshold (percentage): 100

Select up to 100 non-compliant resources from the list below to remediate

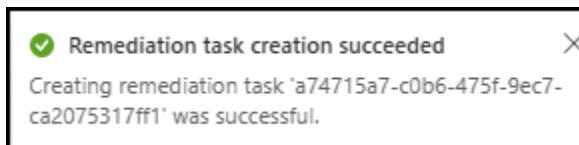
Search Location: All selected

Maximum of 100 non-compliant resources can be shown for this policy in the specified issue. Use the filters to narrow down your search.

Name (1)	Resource type (1)	Location
<input checked="" type="checkbox"/> arcbox-win2k25	Microsoft.HybridCompute/Machines	Central US
<input type="checkbox"/> arcbox-win2k21	Microsoft.HybridCompute/Machines	Central US
<input type="checkbox"/> arcbox-k8s	Microsoft.HybridCompute/Machines	Central US
<input type="checkbox"/> arcbox-client	Microsoft.Compute/VirtualMachines	Central US

Selected 1 associated resource(s) for remediation task creation

Remediate Cancel



The screenshot shows the Azure portal's Remediation tasks interface. At the top, there are buttons for Refresh, Issues (0), Policies to remediate (selected), and Remediation tasks (highlighted with a red box). A note below states: "Remediation task could not be shown if no corresponding assignment is defined. During remediation task creation, if a policyDefinitionId parameter is specified, its value should be the same as it is specified in the policy definition." Below this is a search bar labeled "Filter by name or ID:" and a "Remediation State - All selected" dropdown. The main table has columns: Start Time, Remediation State, Policy Definition, Scope, Locations, Remediated Resources, and Last Updated. One task is listed: "2023-05-16T01:47:45Z Run 10P" (In Progress) for "(Arch) Account Length Policy Settings".

[!knowledge]The **Azure PowerShell modules** are used for:

- Publishing the package to Azure storage
- Creating a policy definition
- Publishing the policy
- Connecting to the Azure Arc-enabled servers

[!knowledge]The **GuestConfiguration module** automates the process of creating custom content including:

- Creating a machine configuration content artifact (.zip)
- Validating the package meets requirements
- Installing the machine configuration agent locally for testing
- Validating the package can be used to audit settings in a machine
- Validating the package can be used to configure settings in a machine

[!knowledge] Version 3 of **Desired State Configuration module** is removing the dependency on MOF.

Initially, there is only support for DSC Resources written as PowerShell classes.

Due to using MOF-based DSC resources for the Windows demo-configuration, we are using version 2.0.5.

# LAB05: Monitor your Azure Arc-enabled servers using Azure Monitor, Change Tracking and Inventory

---

In this lab, you will learn how to deploy the Azure Monitor agent to your Arc-enabled Windows and Linux machines, how to deploy the dependency agent to your Arc-enabled Windows machines, how to enable the *VM Insights* solution to start monitoring your machines using Azure Monitor, how to run queries on the Log analytics workspace and how to configure alerts. In addition, you will learn how to use the Change Tracking and Inventory features to track changes in your machine.

## Student Lab Manual

### Table of Contents

Exercise 1 - Deploy Azure Monitor Agent (AMA) to your Arc-enabled machine using Azure Policy and define the Data Collection Rules

[\*\*Task 1 - Deploy the Azure Monitor Agent\*\*](#)

[\*\*Task 2 - Configure data collection for logs and metrics\*\*](#)

[\*\*Task 3 - View alerts and visualizations\*\*](#)

Exercise 2 - Monitor changes to your Azure Arc-enabled servers using Change Tracking and Inventory

[\*\*Task 1 - Prerequisites\*\*](#)

[\*\*Task 2 - Enable Change Tracking and Inventory\*\*](#)

[\*\*Task 3 - Track changes in Windows services\*\*](#)

[\*\*Task 4 - Track file changes\*\*](#)

[\*\*Task 5 - Query in Log Analytics\*\*](#)

# Exercise 1: Deploy Azure Monitor Agent (AMA) to your Arc-enabled machine using Azure Policy and define the Data Collection Rules

---

## **Objective**

Use Azure Policy to enforce the installation of the Azure Monitor Agent (AMA) to your Arc-enabled machine.

## **Estimated Time to Complete This Lab**

45 minutes

## **Explanation**

Azure Policy lets you set and enforce requirements for all new resources you create and resources you modify. VM insights policy initiatives, which are predefined sets of policies created for VM insights, install the agents required for VM insights and enable monitoring on all new virtual machines in your Azure environment.

# Task 1: Deploy the Azure Monitor Agent

- 1. In the Azure portal, search for *Policy*.

The screenshot shows the Microsoft Azure portal search results for the term "policy". The search bar at the top contains "policy". Below the search bar, the main navigation bar includes "Azure", "Services (8)", "Marketplace (23)", "Documentation (29+)", "Azure Active Directory (4)", and "Resources (8)". The "Services" section is expanded, showing "Policy" highlighted with a red box. Other items in this section include "Firewall Policies", "DNS Security Policies", and "Service endpoint policies". The "Marketplace" section lists several services like "Web Application Firewall (WAF)", "Azure Policy Manager By FS", and "Dark Cloud On-Demand". The "Documentation" section provides links to "Using Azure Policy to secure your Azure Kubernetes Service (AKS) cluster" and "Create and evaluate service endpoint policies - Azure portal". The bottom of the screen shows the URL "https://portal.azure.com/" and the user "admin@MglnvMCAP2...".

- 2. Click on "Definitions" and search for the *(ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines* policy. This is a predefined *Initiative* containing a group of policies to deploy the Azure Monitor Agent.

The screenshot shows the "Policy | Definitions" blade in the Azure portal. The left sidebar has sections for Overview, Getting started, Compliance, Remediation, Events, Authoring, Definitions (selected), Assignments, and Exemptions. The main area has a search bar with "(ArcBox)" and a "Search" button. It also includes filters for Scope: Management, Definition type: All definition types, Policy type: All policy types, and Category: All categories. The results table lists three items:

Name	Definition location	Policy ID	Type	Definition type	Category
Microsoft.Policy.ChangeTracking and Inventory for Arc-enabled machines	Management	1	Custom	Initiative	Change
Microsoft.Deploy.Azure Monitor on Arc-enabled Windows machines	Management	2	Custom	Initiative	Monitor
Microsoft.Deploy.Azure Monitor on Arc-enabled Linux machines	Management	3	Custom	Initiative	Monitor

- 3. Click "Assign Initiative".

(ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines

Initiative [ArcBox]

Assign initiative  Edit definition  Duplicate definition  Delete initiative

Essentials

Name: (ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines  
Description: This policy deploys Azure Monitor agents on Windows Arc connected machines.  
Category: Monitoring  
Version: 1.0.0

Definition location: Management  
Definition ID: /subscriptions/0e364470-0561-4f02-9fba-2a549c9a0000/providers/Microsoft.Authorization/policyDefinitions/0e364470-0561-4f02-9fba-2a549c9a0000  
Type: Custom

Policy (1) Groups (0) Parameters (0) JSON Assignments (0)

Filter by reference ID, policy name or ID Type: All selected Evaluation type: All selected

Policy (1)

- Configure Dependency agent on Arc-enabled Windows servers
- Configure Windows Machines to be associated with a Data Collection Rule or a Data Collection Blueprint
- Configure Windows Arc-enabled machines to host Azure Monitor Agent

Reference ID (1)	Type (1)	Evaluation type (1)	Default effect (1)
62819170936446329	Built-in	Automated	DeployIfCompliant
1331671383554040298	Built-in	Automated	DeployIfCompliant
1512684905941040337	Built-in	Automated	DeployIfCompliant

4. Select the right scope (management group, subscription and resource group) for the resource group where you deployed ArcBox.

Scope

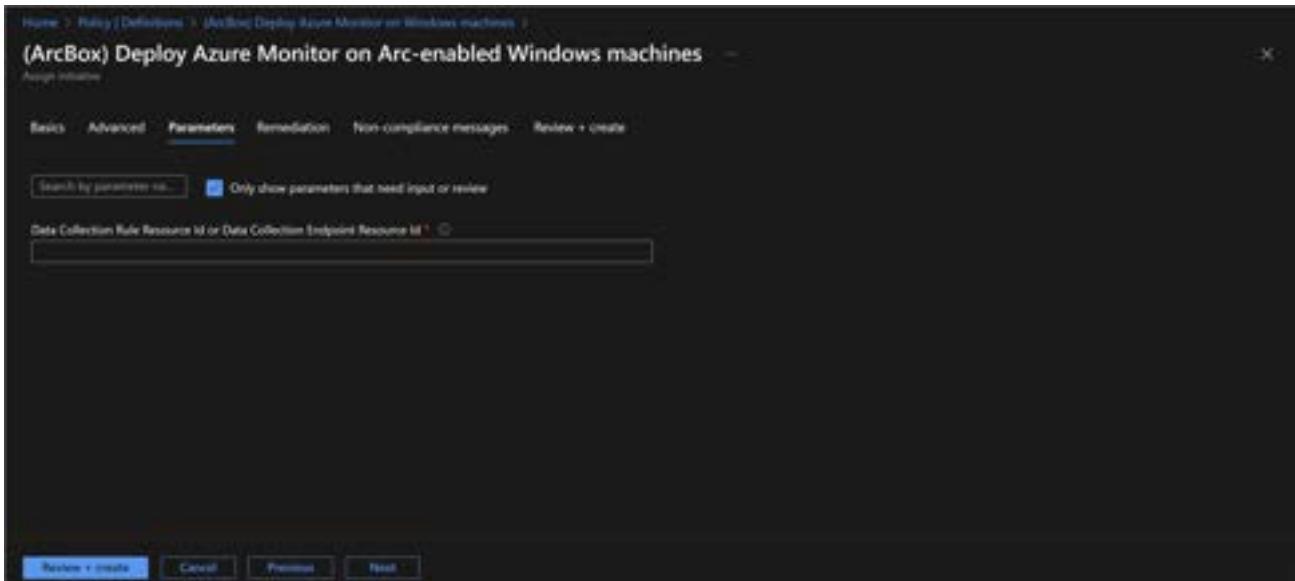
Subscription: Management ?

Resource Group: arcbox ?

4

Select Cancel Clear All Selections

5. After validating the scope, navigate to the parameters tab.



- 6. To get the "Data Collection Rule" resource Id, run the following command in PowerShell (making sure you enter the correct name of the resource group), copy the result into the field then click *create*.

**PowerShell**

- ▶ 

```
az resource show --name "arcbox-ama-vmi-perfAndda-dcr" `  
    --resource-group "<resource group name>" `  
    --resource-type Microsoft.Insights/dataCollectionRules `  
    --query id `  
    --output tsv
```

**i** Optionally you can also find the "Data Collection Rule" resource Id from the Azure portal. Search for the *arcbox-ama-vmi-perfAndda-dcr* data collection rule.

Microsoft Azure

Home > ArcBox-Win2K19

ArcBox-Win2  
Machine: Azure VM

All Services (49) Documentation (39+) Resources (0) Resource Groups (0) Marketplace (0)

Azure Active Directory (0)

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Connect

Windows Admin Center (preview)

Security

Extensions

Properties

Locks

Operations

Policies

data collection rules

Services

Data collection rules

SQL databases

Azure Database for MySQL servers

Data collection endpoints

Data Catalog

Connections

Data Connections

Data factories

Documentation

Best practices for data collection rule creation and management ...

Structure of a data collection rule in Azure Monitor (preview) - Azure Monitor

Logs ingestion API in Azure Monitor - Azure Monitor

Tutorial - Editing Data Collection Rules - Azure Monitor

Add or delete tables and columns in Azure Monitor Logs - Azure Monitor

Tools for migrating to Azure Monitor Agent from legacy agents - Azure Monitor

Azure Monitor service limits - Azure Monitor

Sample data collection rule - custom logs - Azure Monitor

Continue searching in Azure Active Directory

Search for all subscriptions, change

Give feedback

Home > Data collection rules

Create Manage view Refresh Export to CSV Open query Analytics Delete

Filter for any field Subscription equals all Resource group equals all Location equals all Add filter

No grouping Edit list view

Showing 1 to 3 of 3 records.

Name	Subscription	Resource group	Location	Data sources	Destinations
arcbox-win2k19	Management	arcbox	East US	VM Insights, Performance Counters	Azure Monitor Logs
arcbox-vm-logs-01	Management	arcbox	East US	VM Insights, Performance Counters	Azure Monitor Logs
MSVSD DefaultWorkspace-05a407a5b01-05e-	Management	DefaultResourceGroup-1-	East US	VM Insights, Performance Counters	Azure Monitor Logs

1 Previous Page 1 of 1 Next 1 Give feedback

Home > Data collection rules

### arcbox-ama-vmi-perfAndda-dcr

Data collection rule

Search  Delete Feedback CLI / PS

Overview Activity log Access control (IAM) Tags

Settings Locks Configuration Data sources Resources Automation Tasks (previewed) Export template Help New Support Request

Resource group (Input): arcbox  
Status: Provisioned Location: East US Subscription (Input): Microsoft  
Subscription ID: e194479 Tag ID: Project: arcmonitor\_azurebox

Essentials Data Sources: 12 Connected resources: 6 Platform Type: All

JSON View

Collect, Scope and Route your Resource Monitoring Data

Azure Monitor Data Collection Rules allow you to select what monitoring data you want to collect from which Resources and where you want that data to go. Learn more

Resources Data sources

Select which resources to collect data from for monitoring Define what data you want to collect and where you want that data to go.

Home > Data collection rules

### arcbox-ama-vmi-perfAndda-dcr

Data collection rule

Search  Delete Feedback CLI

Overview Activity log Access control (IAM) Tags

Settings Locks Configuration Data sources Resources Automation Tasks (previewed) Export template Help New Support Request

Resource ID: /subscriptions/e194479/resourceGroups/arcbox/providers/Microsoft.Insights/

API Version: 2022-06-01

Resource JSON

```
arcbox-ama-vmi-perfAndda-dcr
{
  "id": "/subscriptions/e194479/resourceGroups/arcbox/providers/Microsoft.Insights/",
  "name": "arcbox-ama-vmi-perfAndda-dcr",
  "type": "Microsoft.Insights/dataCollectionRules",
  "location": "East US",
  "tags": {},
  "properties": {
    "description": "Data collection rule for VM Insights",
    "isEnabled": "true",
    "metrics": [
      {
        "counter": "VMInsightsLatencyMetricPerSecond"
      }
    ],
    "metricsAggregation": {
      "frequency": "60",
      "timeWindow": "PT1H"
    },
    "metricsSampling": {
      "count": 1
    },
    "metricsTimeWindow": "PT1H"
  },
  "resources": [
    {
      "id": "/subscriptions/e194479/resourceGroups/arcbox/providers/Microsoft.Compute/virtualMachines/arcbox-01"
    }
  ],
  "datasources": [
    {
      "id": "/subscriptions/e194479/resourceGroups/arcbox/providers/Microsoft.DependencyAgent/agents/arcbox-01"
    }
  ],
  "performanceCounters": [
    {
      "id": "/subscriptions/e194479/resourceGroups/arcbox/providers/Microsoft.DependencyAgent/agents/arcbox-01/metrics/DependencyAgentLog"
    }
  ]
}
```

Home > Policy | Definitions > (ArcBox) Deploy Azure Monitor on Windows machines

(ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines

Assign instance

Basics Advanced Parameters Remediation Non-compliance messages Review + create

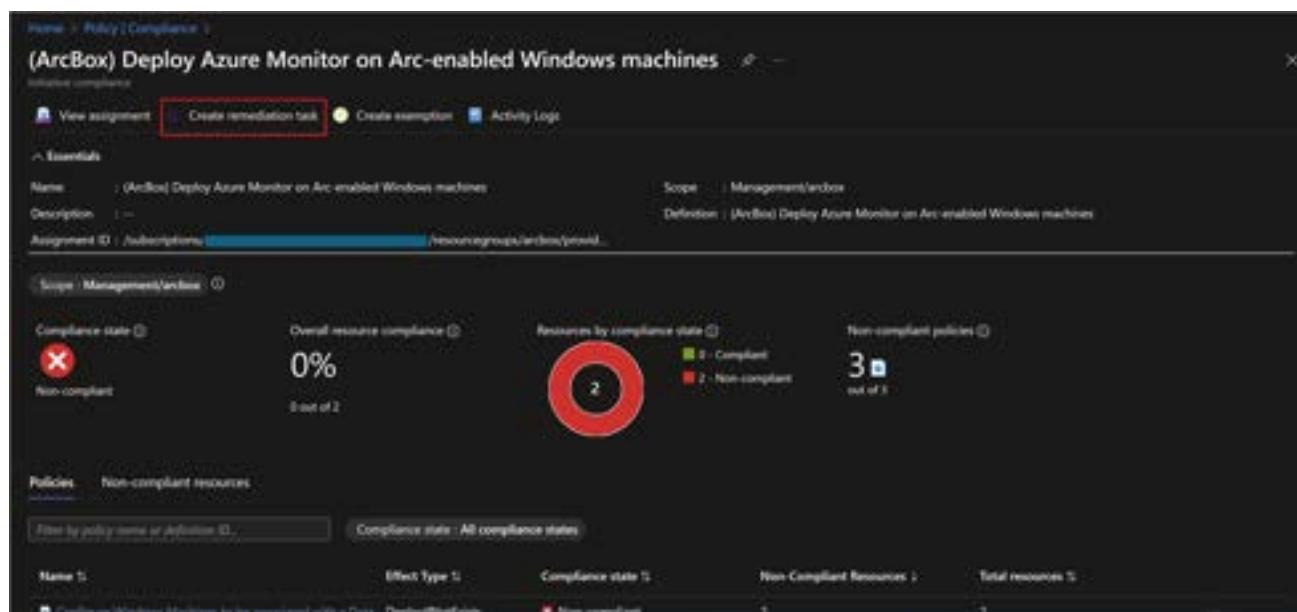
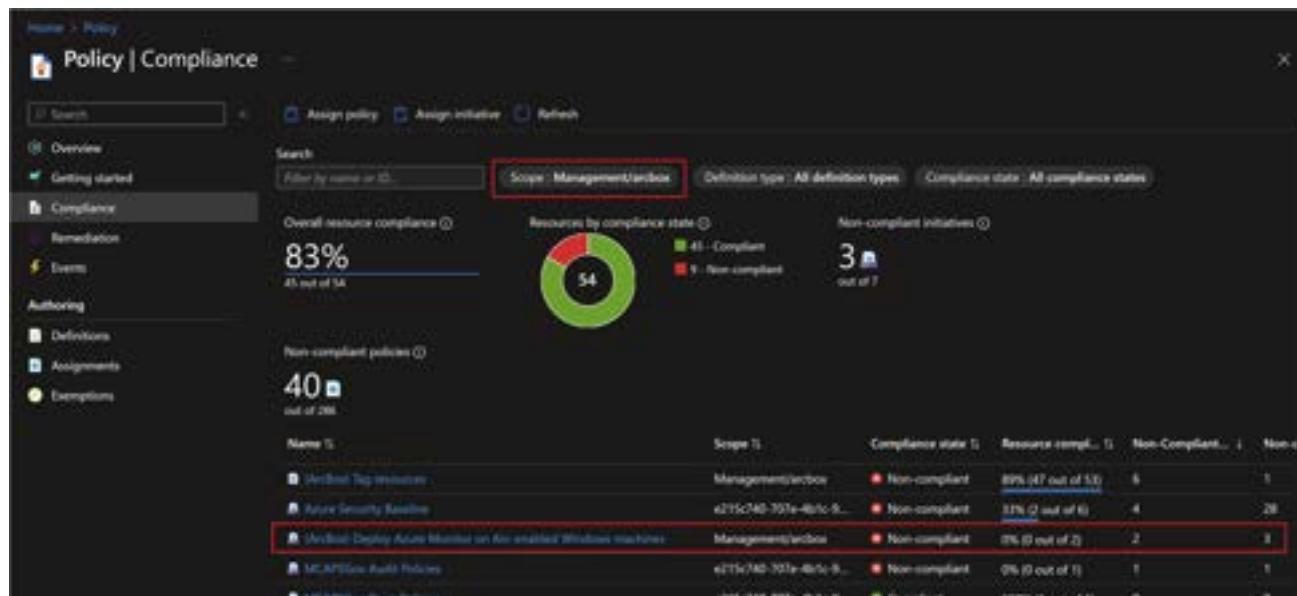
Search by parameter name...  Only show parameters that need input or review

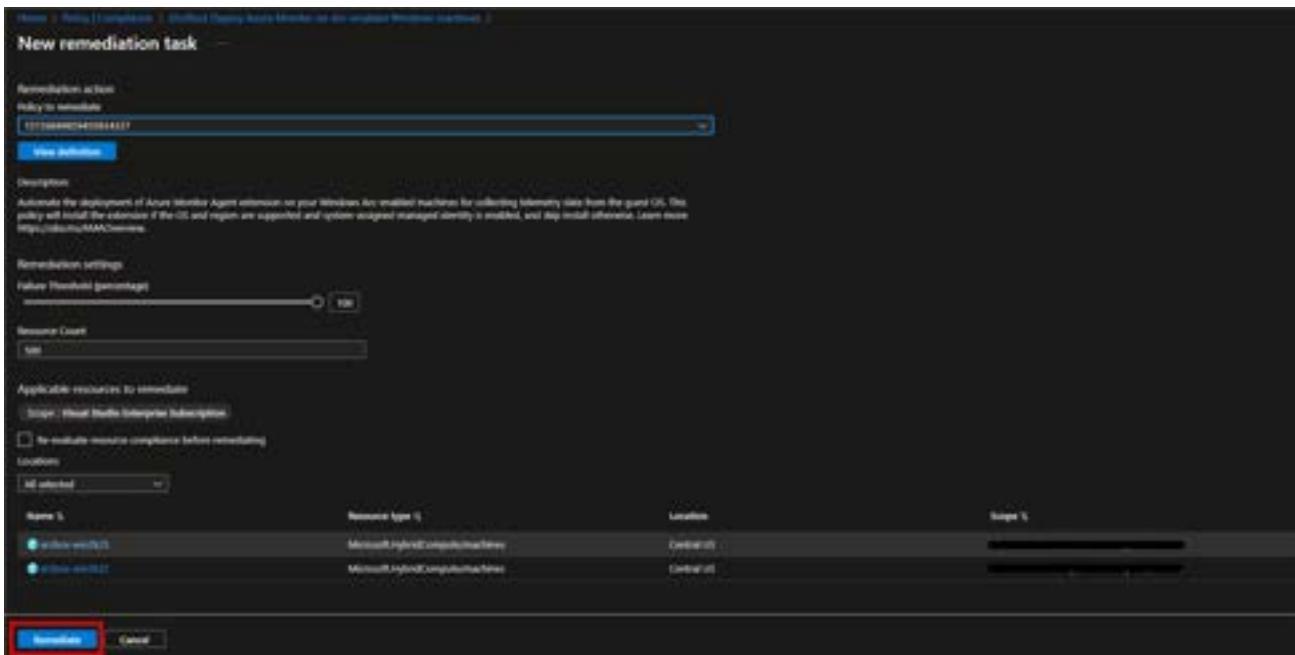
Data Collection Rule Resource Id or Data Collection Endpoint Resource Id:  /subscriptions/e194479/resourceGroups/arcbox/providers/Microsoft.Insights/

Review + create Cancel Previous Next

**NOTE:The policy will take 5-15 minutes to assess the current resources.**

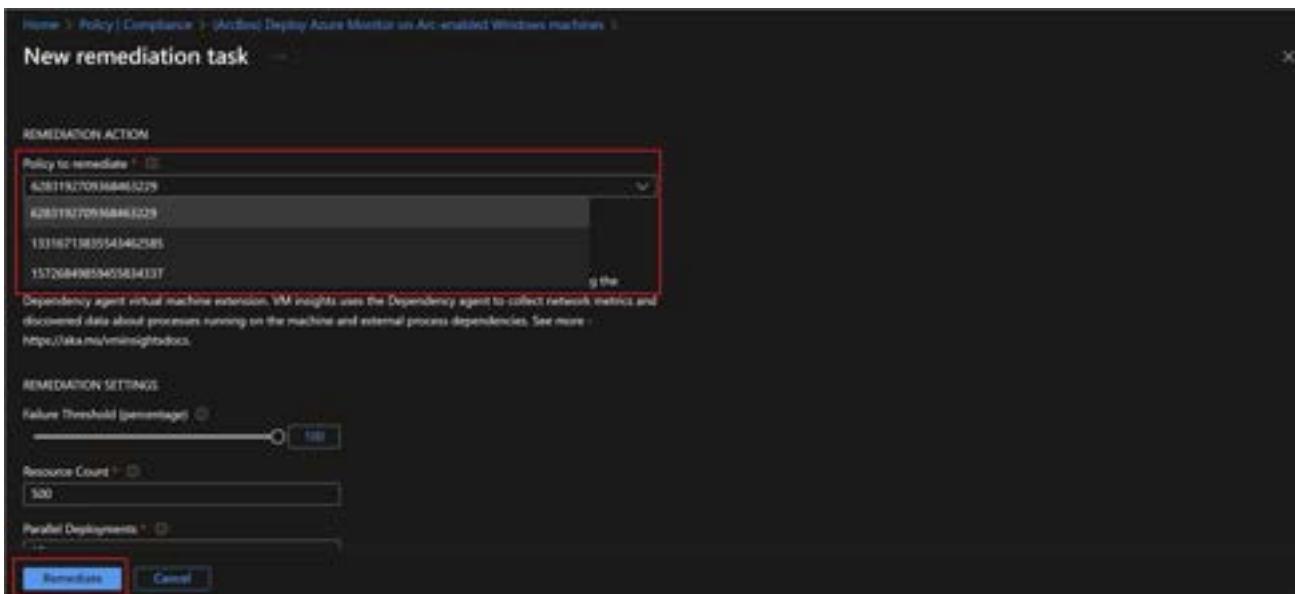
- 8. After the policy has reported compliance, create a remediation task to remediate existing machines.





**NOTE: When creating the remediation task, make sure to select the same region where you deployed ArcBox**

- 9. Create one remediation task per policy definition in the initiative.



- 10. After all remediation tasks have completed. You should see the Azure Monitor agent extension and the dependency agent extension deployed to the Arc-enabled machines.

The screenshot shows the 'Policy | Remediation' blade in the Azure portal. The left sidebar includes 'Overview', 'Getting started', 'Compliance', 'Remediation' (selected), 'Events', 'Authoring', 'Definitions', 'Assignments', and 'Templates'. The main area has tabs for 'Scope' (set to 'Management/Windows'), 'Policies to remediate' (set to 'Remediation tasks'), and 'Remediation tasks'. A note states: 'Remediation task would not be shown if its corresponding assignment is deleted. During remediation task creation, if a policyDefinitionReference parameter is specified, its value should be the same as it is specified in the initiative definition.' Below this, a search bar shows 'windows' and a dropdown for 'Remediation State' set to 'All'. A table lists three remediation tasks:

Start Time	Remediation State	Policy Definition	Scope	Locations
5/6/2023, 1:57 PM	Complete	Configure Windows Arc-enabled machines to run Azure Monitor Agent	Management/Windows	All
5/6/2023, 1:57 PM	Complete	Configure Windows Machines to be associated with a Data Collection Rule or a Data Collector	Management/Windows	All
5/6/2023, 1:54 PM	Complete	Configure Dependency agent on Azure Arc enabled Windows servers	Management/Windows	All

The screenshot shows the 'Arcbox-Win2k25 | Extensions' blade. The left sidebar includes 'Overview', 'Activity log', 'Access control (preview)', 'Logs', 'Diagnostic and error problems', 'Settings' (selected), 'Compute', 'Security', 'Insights' (selected), 'Properties', and 'Logs'. The main area shows a table of installed extensions:

Name	Type	Version	Update available	Status	Automatic update
Azure Monitor Agent	Administrative extension	1.21.00	No	Downloaded	Enabled
Dependency Agent	Dependency agent extension	0.0.164479	No	Downloaded	Enabled
NET Health	Machine Configuration extension	1.0.14	No	Downloaded	Not supported

- 11. Repeat the same steps in *Task 2* to assign the Linux policy for data collection (*ArcBox*) *Deploy Azure Monitor on Arc-enabled Linux machines*.
- 12. After configuring the agents and VM insights using Azure Policy, it will take 10-25 minutes for the insights data to start showing up. **However, for the purposes of this workshop, the agent was pre-installed on the ArcBox-Win2k25 and Arcbox-Ubuntu-01 Arc-enabled machines so that you can see the expected results without having to wait until the remediation tasks have completed.** Head over to the these two machines to see the data collected by VM insights.

The screenshot shows the 'Arcbox-Win2k25 | Insights' blade. The left sidebar includes 'Overview', 'Activity log', 'Access control (preview)', 'Logs', 'Diagnostic and error problems', 'Settings' (selected), 'Compute', 'Security', 'Insights' (selected), 'Properties', and 'Logs'. The main area shows a 'Performance' chart with a time range from 'Last 1 hour' to 'Last 1 day'. It displays 'Logical Disk Performance' and two charts: 'CPU Utilization % by priority' and 'Available Memory % by priority'. The 'CPU Utilization % by priority' chart shows utilization levels for Low, Medium, and High priorities. The 'Available Memory % by priority' chart shows memory availability for the same priorities.

The screenshot shows the Azure Arcbox-Ubuntu-01 Insights interface. The left sidebar has a red box around the 'Properties' section. The top navigation bar has a red box around the 'Performance' tab, which is currently selected. Below the navigation bar is a search bar and several monitoring-related buttons: Resource Group Monitoring, Azure Monitor, Refresh, Monitoring configuration, and Provide Feedback. The main content area displays a table titled 'Logical Disk Performance' for the time range 'Last hour as of 6 Sep 15:41'. The table has columns for Disk, Current Avg. IOPS, Current Avg. (%) IOPS, PPH Avg. Read, PPH Avg. Write, PPH Avg. Total, PPH Max. Read, PPH Max. Write, and PPH Max. Total. The data shows various disk paths like /, /boot, /root, /swapfile, /snapcore16/16f, /snapcore16/16g, /snapcore16/17h, /snapcore20/10o, /snapcore22/11s, and /tmpfs/100n, all with very low activity levels.

Disk	Current Avg. IOPS	Current Avg. (%) IOPS	PPH Avg. Read	PPH Avg. Write	PPH Avg. Total	PPH Max. Read	PPH Max. Write	PPH Max. Total
/	47.56	2%	0	12.37	13.37	0	0.01	0.01
/boot	0.00	0%	0	0	0	0	0	0
/root	0.1	0%	0	0	0	0	0	0
/swapfile	0.05	100%	0	0	0	0	0	0
/snapcore16/16f	0.05	100%	0	0	0	0	0	0
/snapcore16/16g	0.05	100%	0	0	0	0	0	0
/snapcore16/17h	0.06	100%	0	0	0	0	0	0
/snapcore20/10o	0.06	100%	0	0	0	0	0	0
/snapcore22/11s	0.07	100%	0	0	0	0	0	0
/tmpfs/100n	0.09	100%	0	0	0	0	0	0

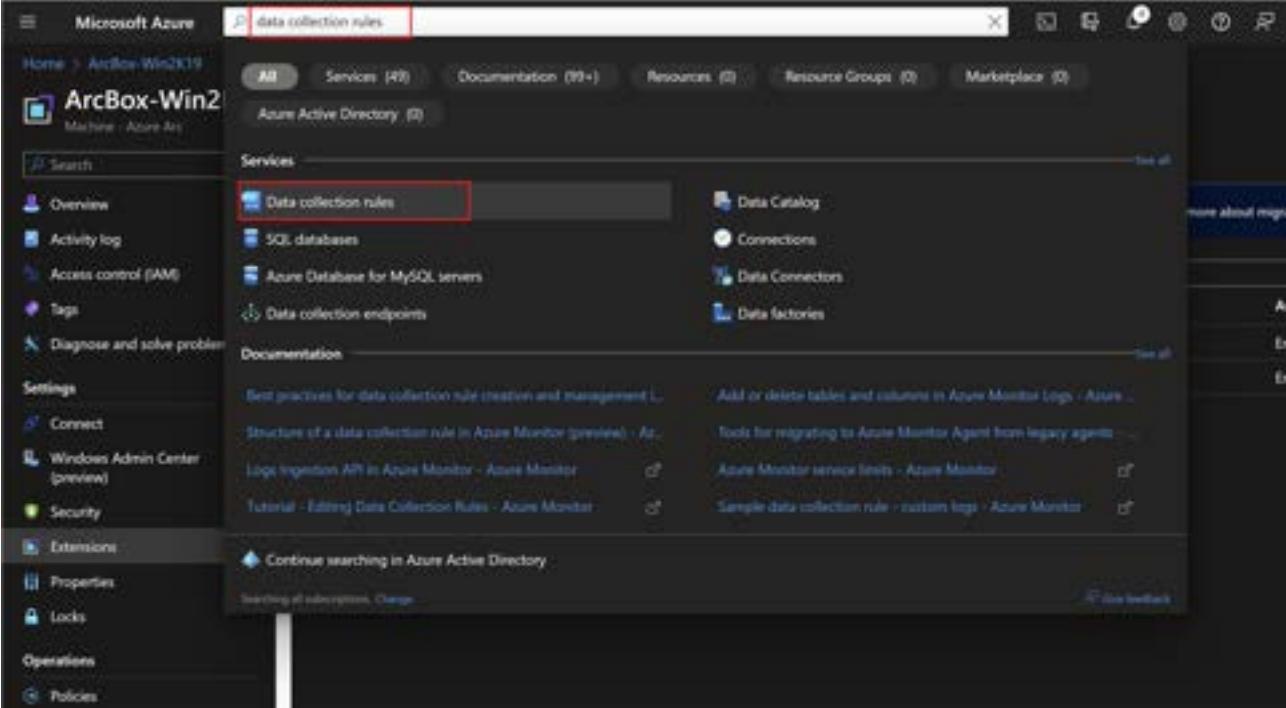
**Task 1 has been completed**

Click **Next** for the next task or [Go back to the main table of content](#)

## Task 2: Configure data collection for logs and metrics

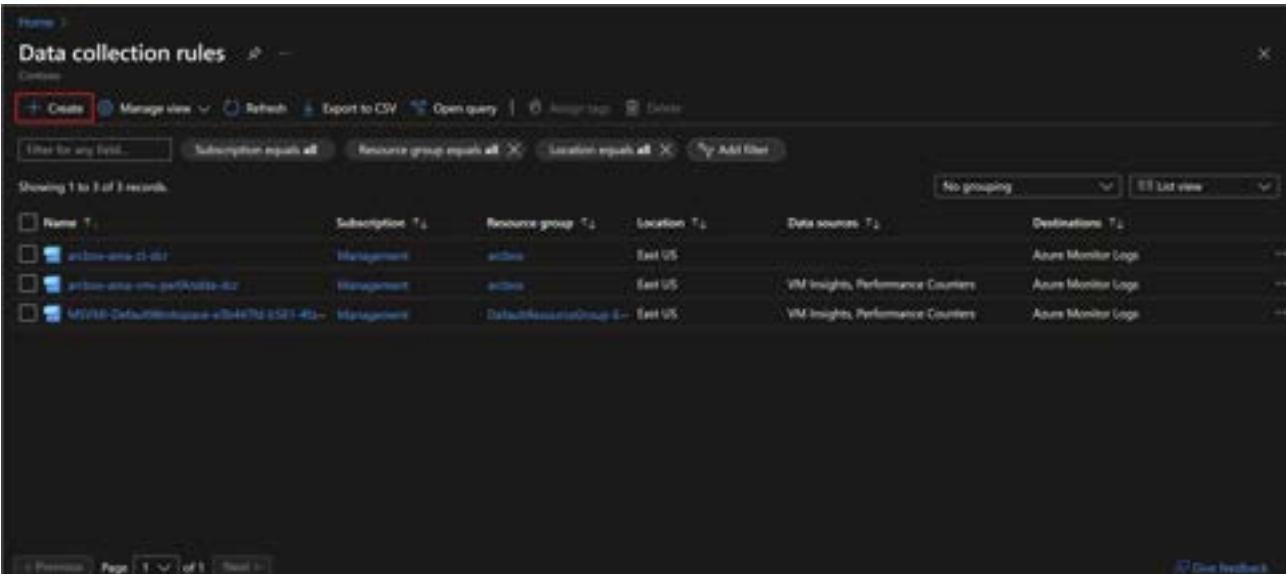
As part of the ArcBox automation, some alerts and workbooks have been created to demonstrate the different monitoring operations you can perform after onboarding the Arc-enabled machines. You will now configure some data collection rules to start sending the needed metrics and logs to the Log Analytics workspace.

- 1. In the Azure portal, search for *Data Collection rules*.



The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar with the text "data collection rules". Below the search bar, the main navigation bar includes "All", "Services (49)", "Documentation (99+)", "Resources (0)", "Resource Groups (0)", and "Marketplace (0)". On the left, there is a sidebar with sections for "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Settings", "Connect", "Windows Admin Center (preview)", "Security", "Extensions", "Properties", "Locks", "Operations", and "Policies". The "Services" section is expanded, showing "Data collection rules" (which is highlighted with a red box), "SQL databases", "Azure Database for MySQL servers", "Data collection endpoints", "Data Catalog", "Connections", "Data Connectors", and "Data factories". Below the services, there is a "Documentation" section with several links related to data collection rules and Azure Monitor.

- 2. Create a new data collection rule.

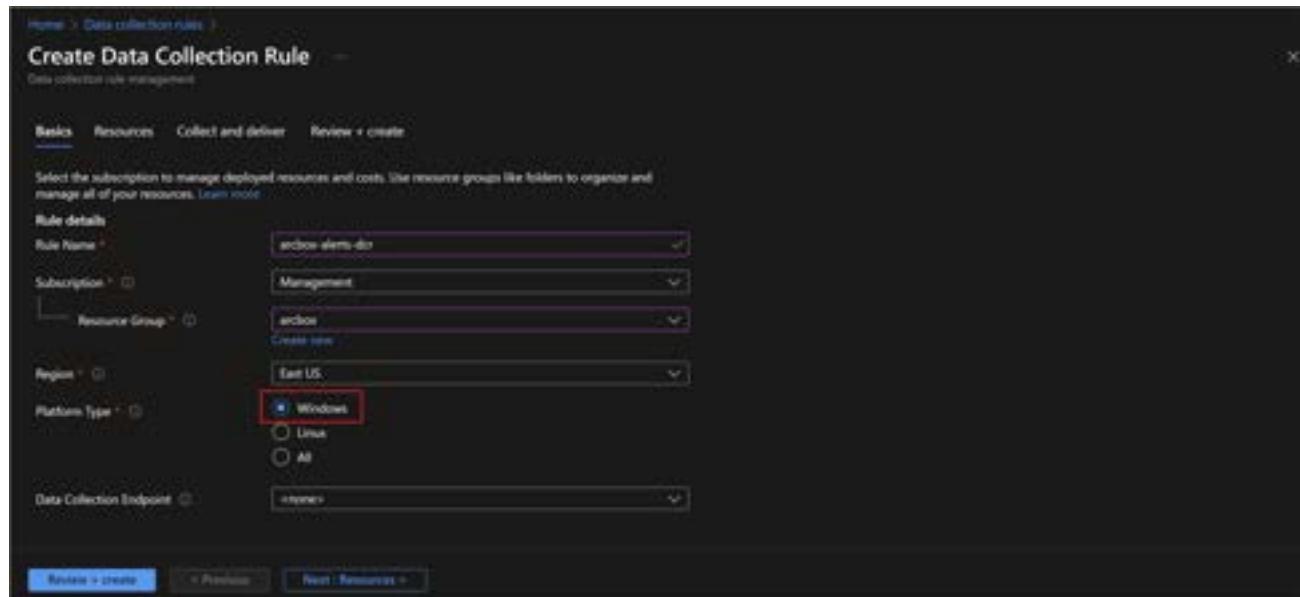


The screenshot shows the "Data collection rules" blade in the Azure portal. At the top, there is a header with "Data collection rules" and a "Create" button (which is highlighted with a red box). Below the header, there are filter options: "Subscription equals all", "Resource group equals all", "Location equals all", and "By Add Rule". There are also grouping and view options: "No grouping" and "List view". The main table displays four data collection rules:

Name	Subscription	Resource group	Location	Data sources	Destinations
arcbox-win2-001	Management	active	East US	VM Insights, Performance Counters	Azure Monitor Logs
arcbox-ana-win-performance-002	Management	active	East US	VM Insights, Performance Counters	Azure Monitor Logs
MSVMA-DefaultResourceGroup-e5b44f7d-05d1-402c	Management	DefaultResourceGroup-5	East US	VM Insights, Performance Counters	Azure Monitor Logs

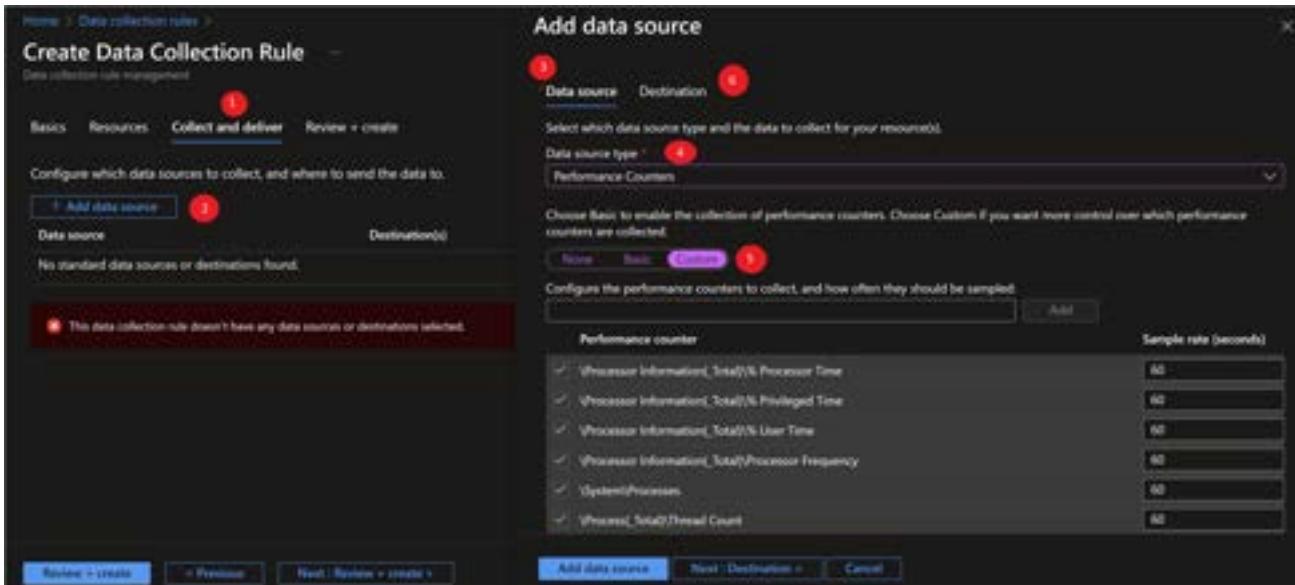
At the bottom, there are navigation buttons for "Previous", "Page 1 of 1", "Next", and a "Give feedback" link.

3. Provide a name and select the same resource group where ArcBox is deployed. Make sure to select Windows as the operating system.

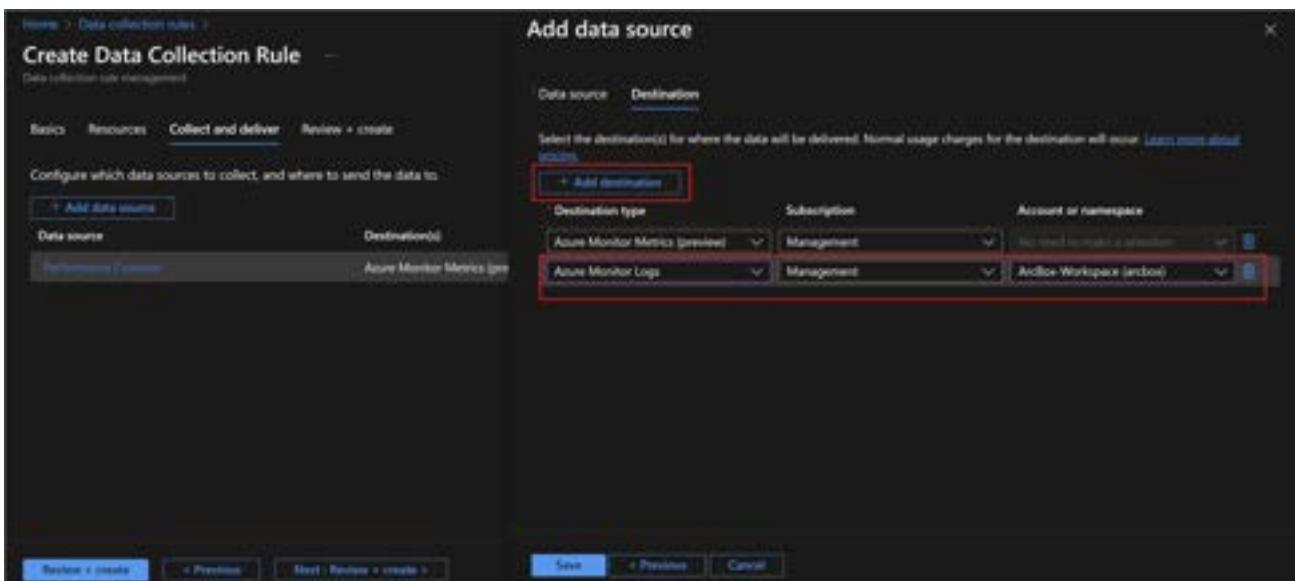


4. In the "Resources" tab, select the right resource group and the Arc-enabled servers onboarded.

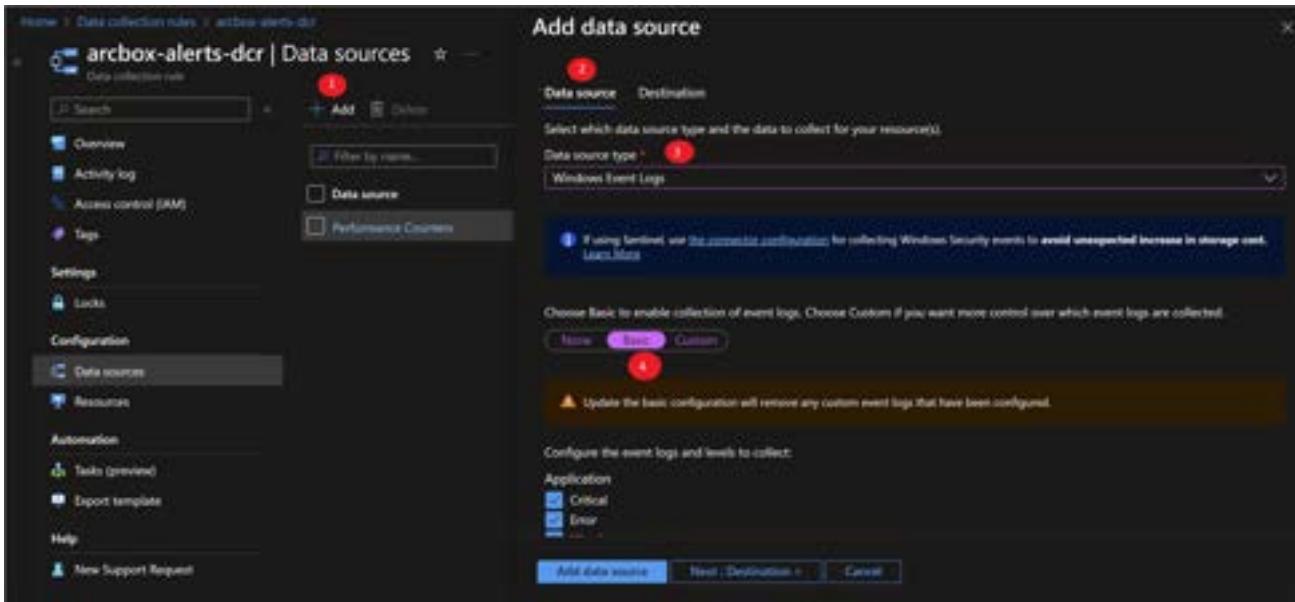
5. Add a new "Performance Counters" data source, and make sure to select all the custom counters.



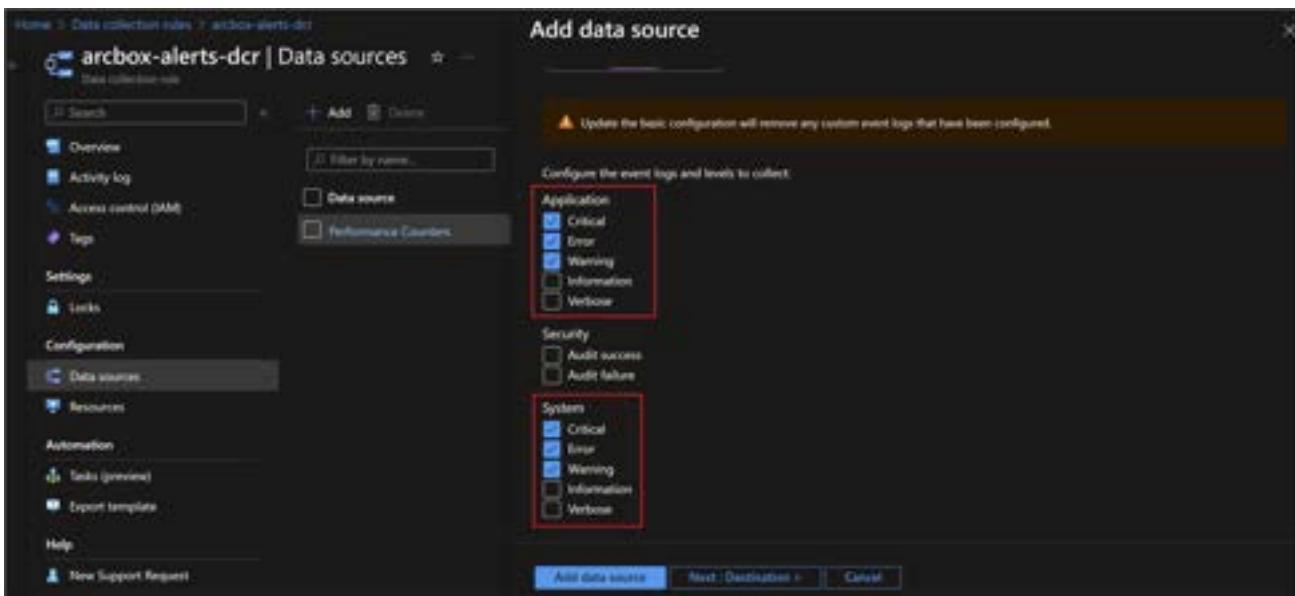
6. Add a new "Azure Monitor Logs" destination and select the log analytics workspace deployed in the ArcBox resource group and save.



7. Add a new "Windows Event logs" data source.



- 8. - Select *Critical*, *Error* and *Warning* events in the Application and System logs and add the data source.



- 9. Save and create the data collection rule.  
□ 10. Repeat the previous steps to create another Linux data collection rule.

Home > Data collection rules > Create Data Collection Rule

**Create Data Collection Rule**

Basics Resources Collect and deliver Review + create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources. Learn more.

**Rule details**

Role Name: archive-alerts-linux-dcr

Subscription: Management

Resource Group: archive

Region: East US

Platform Type: Linux

Data Collection Endpoint: archive

**Review + create** **Next: Resources**

Home > Data collection rules > Create Data Collection Rule

**Select a scope**

Basics Resources Collect and deliver Review + create

Pick a set of machines to collect data from. The Azure Monitor Agent will be installed on these machines. For Windows 10 and 11 devices, download the client installer and follow the guide.

This will also enable System Assigned Managed Identity on these machines. In addition to:

- + Add resources
- + Create endpoint

Enable Data Collection Endpoints:

Only virtual machines in the same region can be assigned to the same endpoint.

Name	Type
No resources found.	

**Subscription:** All subscriptions **Resource group:** archive **Resource types:** All resource types **Locations:** All locations

Scope:

- Management
- archive
- Archive Ubuntu-01

Resource type: Subscription Location: Machine: Archive Arc. East US

**Review + create** **Previous** **Next: Collect and deliver** **Apply** **Cancel** **Clear all selections**

Home > Data collection rules > Create Data Collection Rule

**Add data source**

Basics Resources Collect and deliver Review + create

Configure which data sources to collect, and where to send the data to.

+ Add data source

Data source	Destinations
Filebeat Configuration	Azure Monitor Metrics (pre)

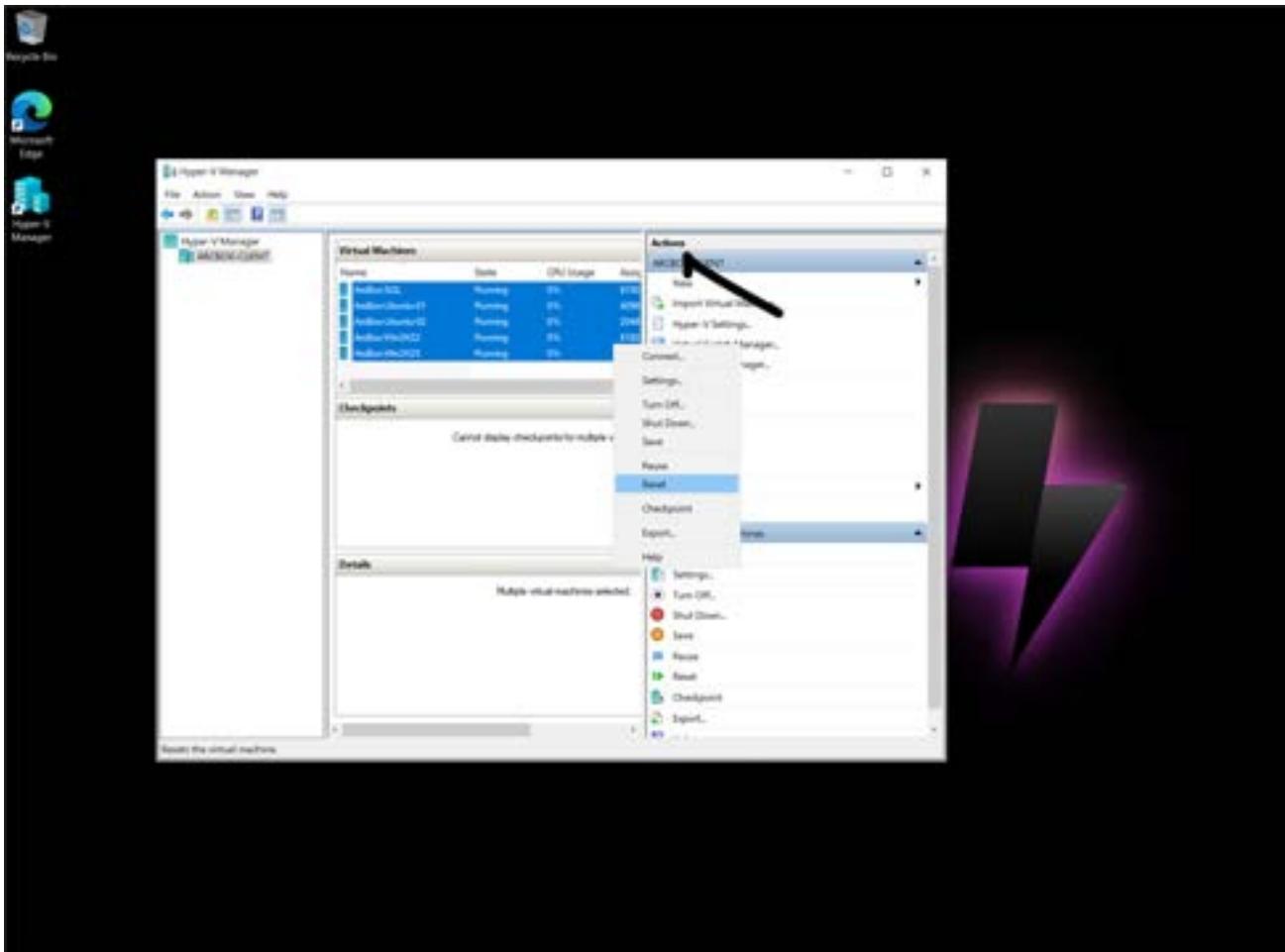
Data source: Destination: Select which data source type and the data to collect for your resources.

Data source type: Linux Syslog

Facility	Minimum log level
LOG_AUTH	LOG_DEBUG
LOG_AUTHPRIV	LOG_DEBUG
LOG_CRON	LOG_DEBUG
LOG_DAEMON	LOG_DEBUG
LOG_MARK	LOG_DEBUG
LOG_KERN	LOG_DEBUG
LOG_LOCAL0	LOG_DEBUG
LOG_LOCAL1	LOG_DEBUG
LOG_LOCAL2	LOG_DEBUG
LOG_LOCAL3	LOG_DEBUG

**Review + create** **Previous** **Next: Review + create** **Add data source** **Next: Destination** **Cancel**

11. After waiting for 5-10 minutes for the data collection rule to start collecting data, restart the servers in the Hyper-V manager on the *ArcBox-Client* VM to trigger some new events.



**Task 2 has been completed**

Click **Next** for the next task or [Go back to the main table of content](#)

## Task 3: View alerts and visualizations

**NOTE: It might take some time for all visualizations to load properly**

- 1. In Azure Monitor, click on *Alerts*. and select *Alert rules*

The screenshot shows the Azure Monitor Alerts interface. On the left, there's a navigation sidebar with options like Overview, Activity log, Metrics, Logs, Change Analysis, Service health, Workbooks, and Insights. The 'Alerts' option is selected, indicated by a red circle with a '1'. The main area displays alert statistics: Total alerts (0), Critical (0), Error (0), Warning (0), Informational (0), and Verbose (0). Below these stats are filters for Subscription, Time range, Alert condition, Severity, and User response. A large central area features a large exclamation mark icon.

- 2. Explore the alert rules created for you.

The screenshot shows the 'Processor Time Percent' alert rule details. On the left, a sidebar lists various metrics under 'Name: T2' (e.g., Heartbeat Metric, LogicalDisk Avg. Disk sec per Read, LogicalDisk Avg. Disk sec per Write, LogicalDisk Current Queue Length, LogicalDisk Free Space Percent, LogicalDisk Idle Time Percent, Memory Available Mbytes, Memory Committed Bytes In Use Percent, Memory Pages per Sec, Processor Time Percent, Unhandled System Shutdowns). The main panel shows the alert configuration: Scope (Resource: azuresqlworkspace, Hierarchy: Management > [alert]), Conditions (Average % Processor Time: 2, Estimated monthly cost: \$0.20), and Actions (Email to: [redacted]).

- 3. Go back to Azure Monitor and click on *Workbooks*. There are three workbooks deployed for you.

The screenshot shows the Azure Monitor Workbooks Gallery. The left sidebar has a red box around the 'Workbooks' item under 'Monitor'. The main area has a red box around the 'Recently modified workbooks' section, which contains three items: 'Azure Monitor Alerts', 'OS Performance and Capa...', and 'Windows Event Logs'. There are also sections for 'Getting started with workbooks', 'Virtual Machines', and 'Containers'.

The screenshot shows the Azure Monitor interface with the title "Monitor | Workbooks | OS Performance and Capacity". The left sidebar is titled "Workbooks" and lists various monitoring categories. The main area displays two charts and a summary table.

**Available Memory - Top 10 Computers**

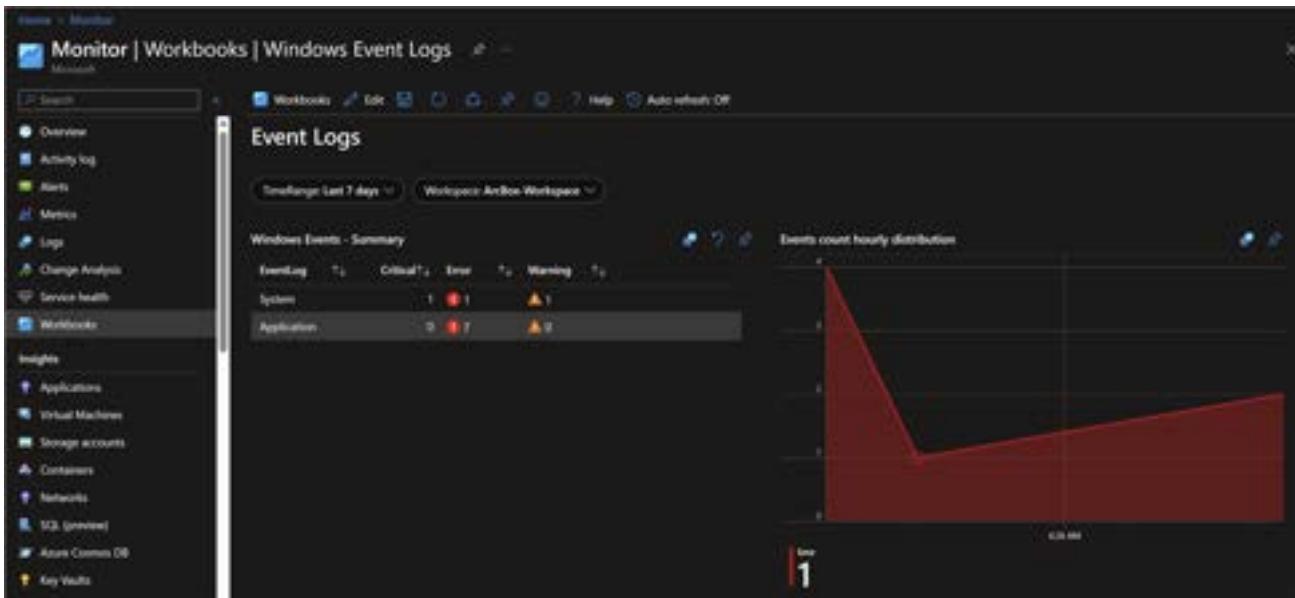
This chart shows available memory over time for the top 10 computers. The Y-axis ranges from 0 to 1000 GB. The data series shows a significant dip around June 2023, followed by a gradual recovery. A summary metric at the bottom indicates "903 ms".

**Download (Warning=10, Critical=10) - All Computers**

This chart shows download activity for all computers. The Y-axis ranges from 0 to 1000 MB/s. The data series shows a sharp drop in late June 2023, followed by a recovery. A summary metric at the bottom indicates "10.47 MB/s".

**Summary Metrics**

Metric	Value
Average CPU Usage	10.47 MB/s
Average RAM Usage	903 ms



**Task 3 has been completed**

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Exercise 2: Monitor changes to your Azure Arc-enabled servers using Change Tracking and Inventory

---

### **Objective**

Tracks changes in Your Azure Arc-enabled machines to help you pinpoint operational and environmental issues.

### **Estimated Time to Complete This Lab**

30 minutes

### **Explanation**

Change Tracking and Inventory is a built-in Azure service, provided by Azure Automation. The new version uses the Azure Monitor Agent AMA as opposed to the Log Analytics Agent. You will be using the new version in this exercise.

## Task 1: Prerequisites

---

The following are required for this task:

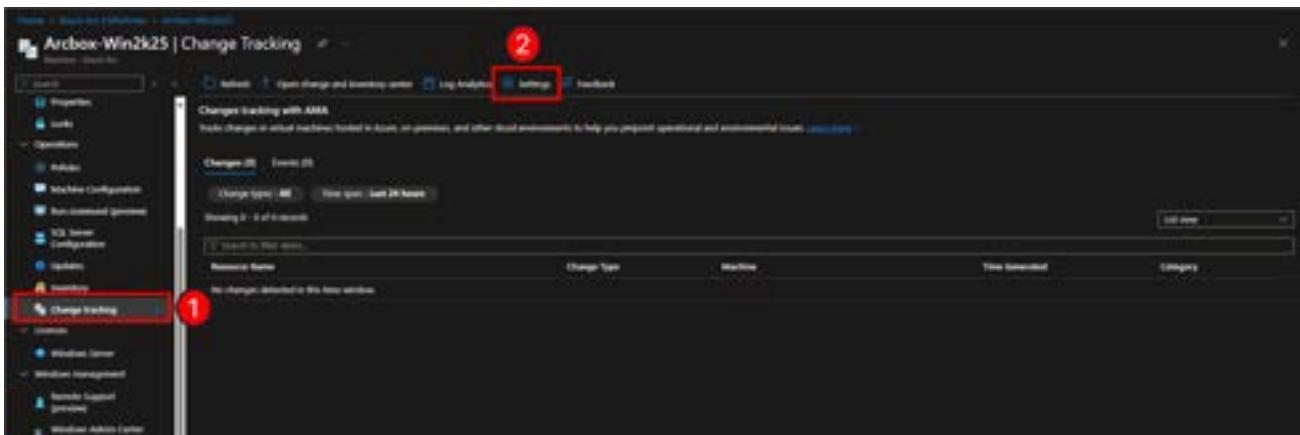
- 1. Ensure that the servers are already on-boarded to Azure Arc.
- 2. Ensure that the Azure Monitor agent (AMA) is already deployed on every Arc-enabled server (This was done in Exercise 1 of this lab).
- 3. Note the Current Limitations as listed in <https://learn.microsoft.com/azure/automation/change-tracking/overview-monitoring-agent?tabs=win-az-vm#current-limitations>.

**Task 1 has been completed**

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Task 2: Enable Change Tracking and Inventory

- 1. To enable these features you would need to set up a Data Collection Rule that would collect the right events and data for Change Tracking and Inventory and create an Azure policy to onboard your Arc-enabled machines to Change Tracking. **For the purposes of this workshop** - these tasks have all been done for you, so you do not need to do them manually. Follow the link [here](#) to learn how to do these yourself in future.
- 2. Verify that Change Tracking and Inventory is now enabled on the *ArcBox-Win2K25* Arc enabled server in the Azure Portal.



**Task 2 has been completed**

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Task 3: Track changes in Windows services

- ☐ 1. From the "Change tracking" settings select "Windows Services" and change the "Collection Frequency" to 10 minutes.

The screenshot shows the 'Data Collection Rule Configuration' page for a machine named 'ArcBox-Win2k25'. The top navigation bar includes 'Home', 'Azure Arc | Machines', 'ArcBox-Win2k25 | Change Tracking', and 'Change Tracking'. Below the navigation is a toolbar with 'Add', 'Delete', 'Refresh', 'Documentation', and 'Feedback' buttons. A red circle labeled '1' highlights the 'Windows Services' tab, which is currently selected. Another red circle labeled '2' highlights the 'Collection Frequency' dropdown menu, which is set to '10 min'.

- ☐ 2. Go to the ArcBox-Client machine via RDP and from Hyper-V manager right-click on *ArcBox-Win2K25* VM then click "Connect" (Administrator default password is JS123!!). Try stopping the "Print Spooler" and the "Windows Update" services using an Administrator PowerShell session (or from the Services desktop application).

```
PowerShell
▶ Stop-Service spooler
Stop-Service wuauserv
```

- ☐ 3. The service changes will eventually show up in the "Change tracking" page for the Arc-enabled machine. (By default Windows services status are updated every 30 minutes but you changed that to 10 minutes earlier to speed up the result for this task).

☐ **It may take 30 minutes or more for the changes to show up in the portal, you can move to the next task/exercise or lab and come back later to see the results if you prefer. This way, you can make better use of your time in this workshop.**

The screenshot shows the Azure portal interface for a virtual machine named 'Arbox-Win2k25'. The left sidebar has a red box around the 'Change tracking' item under the 'Monitoring' section, with a red circle labeled '1' on it. The main content area has three numbered callouts: '2' points to a service named 'spooler' in a list of recent changes; '3' points to a table titled 'Windows Update' showing a single row where 'Service' is 'spooler' and 'Value after' is 'Running'.

4. You can restart the stopped services on the server if you wish and change tracking will show the outcome in the portal after some time.

PowerShell

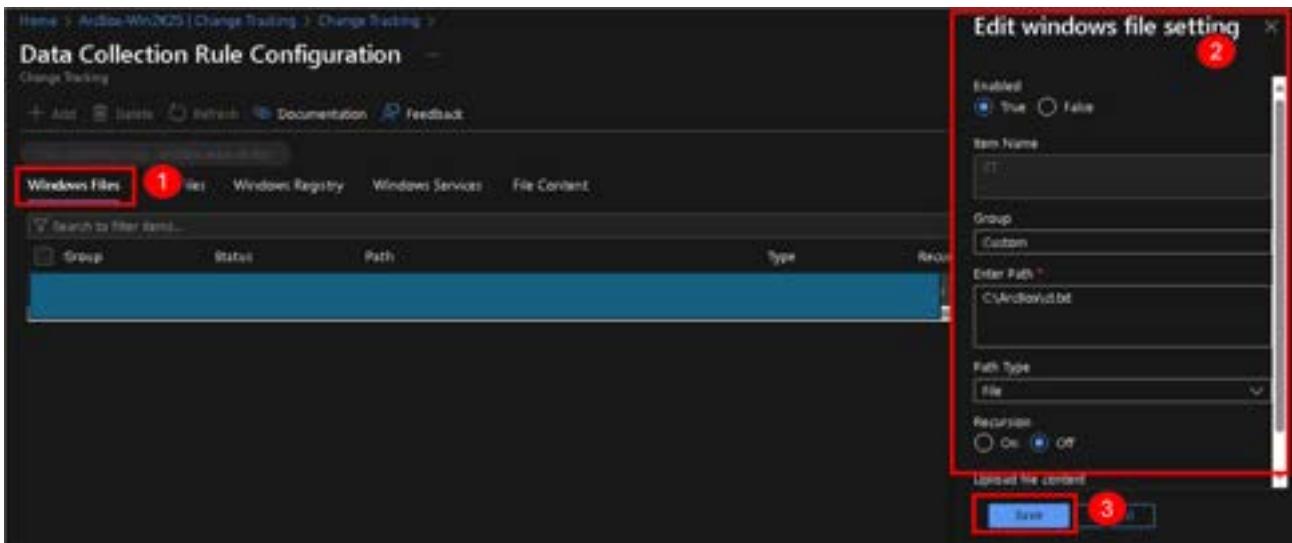
▶ Start-Service spooler  
Start-Service wuauserv

### Task 3 has been completed

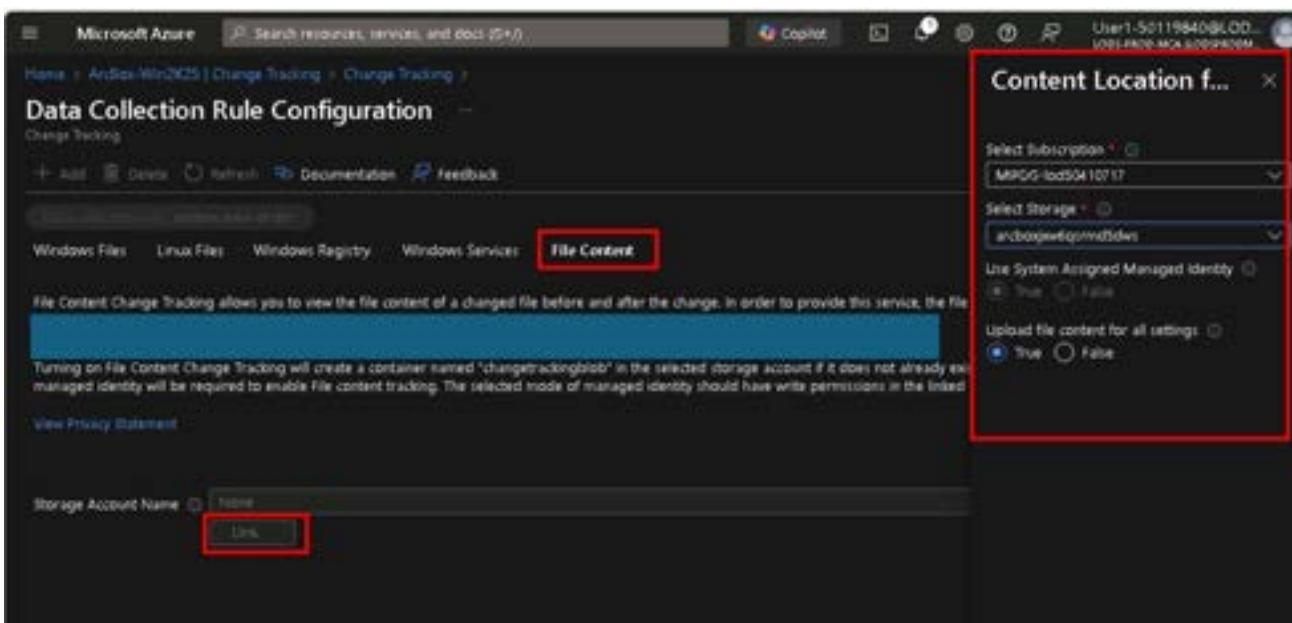
Click **Next** for the next exercise or [Go back to the main table of content](#)

## Task 4: Track file changes

- 1. Navigate to ArcBox-Win2K25 Arc-enabled Windows machines on the Azure Portal and select "Change tracking" then select "Settings" then select "Windows Files". You should see the "Add windows file setting" screen on the right hand side. Configure these settings to track the changes to the file "C:\ArcBox\ct.txt" and to upload the file content to storage.



- 2. Set the file location where changed files will be uploaded. You should have a storage account deployed in the resource group of this lab. Click the *Link* button and set the parameters.



- 3. Navigate to the storage account. Click on "Containers" and you should see a container created automatically for you by Azure Change Tracking.

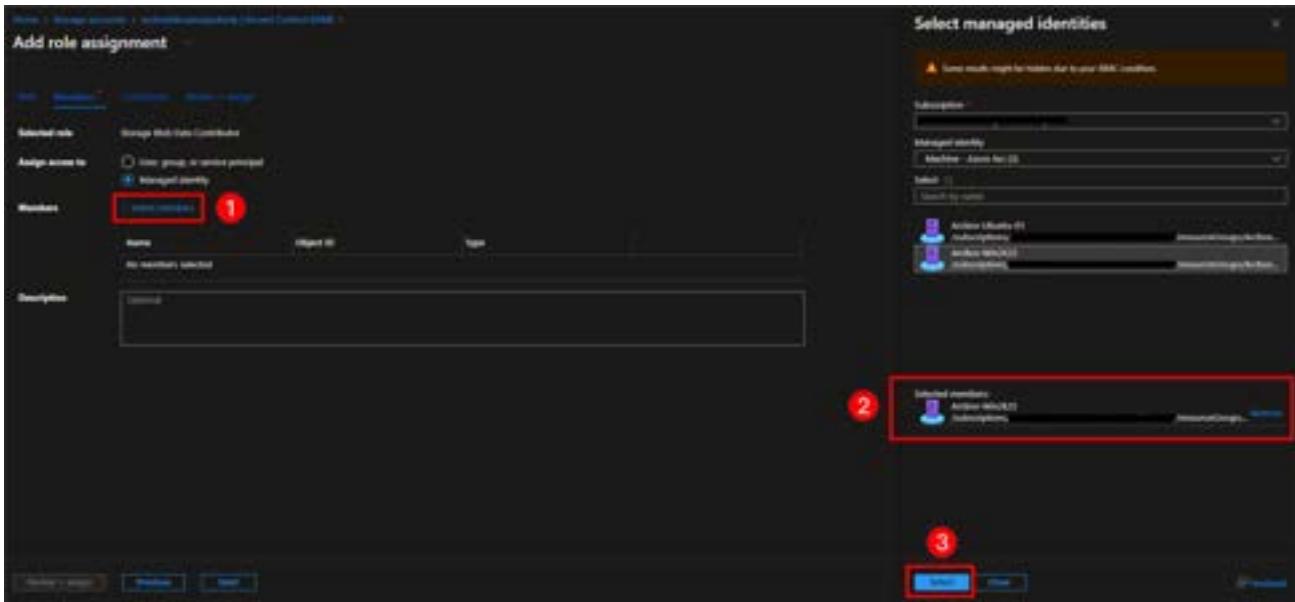
The screenshot shows the Azure Storage Accounts blade. In the top navigation bar, the 'Containers' link is highlighted with a red box. Below the navigation bar, there is a search bar and a 'Select container' dropdown. On the left, a sidebar lists various storage-related services like Activity Log, Logs, Diagnostic and log problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Health, Partner solutions, and Data storage. Under Data storage, the 'Containers' link is also highlighted with a red box. The main area displays a list of containers with columns for Name, Last modified, Assignment access level, and Used state. One container, 'changetrackingblob', is highlighted with a red box.

- 4. Click on the "changetrackingblob" container, and in the next page select "Access Control (IAM)", then on "Add role assignment".

The screenshot shows the 'Access Control (IAM)' blade for the 'changetrackingblob' container. The top navigation bar has a 'Containers' link. Below it, there are tabs for Overview, Diagnostic and solve problems, Access Control (IAM) (which is highlighted with a red box and has a red circle labeled '1'), Role assignments, Roles, Deny assignments, and Classic administration. The main content area has sections for 'My access', 'Check access', 'Grant access to this resource' (with a red box and red circle labeled '2' on the 'Add role assignment' button), 'View access to this resource', and 'View deny assignments'.

- 5. Select the Storage Blob Data Contributor role then assign the role to the Windows Arc enabled machines managed identity.

The screenshot shows the 'Add role assignment' blade. It has a 'Role definition type' dropdown set to 'Privilaged administrator roles'. Below it is a search bar and a 'Select role' dropdown. The main area lists roles with columns for Name, Description, Type, Category, and Details. One role, 'Storage Blob Data Contributor', is highlighted with a red box and has a red circle labeled '1' on its name.



- 6. Modify the C:\ArcBox\ct.txt file on the Arc-enabled machine.

**NOTE: To modify the file, open Notepad as Administrator, select File>Open, and then browse to C:\ArcBox\ct.txt**

- 7. Add a line like this from an administrative notepad and save the file.

```
shell
▶ Change 1
```

- 8. Eventually, the file changes will show up in the change tracking page of the machine (it might take some time to show so move on to other tasks and come back to check later). The file changed content will also be uploaded to the "changetrackingblob" storage container.

**□ It may take some for the changes to show up in the portal, you can move to the next task/exercise or lab and come back later to see the results if you prefer. This way, you can make better use of your time in this workshop.**

The screenshot shows the Azure Storage Explorer interface. At the top, the breadcrumb navigation bar reads "Home > Storage accounts > arctoys6comsites | Containers >". Below this, the container name "changetrackingblob" is displayed with a blue square icon and the word "Container". The main area is titled "Overview" and includes sections for "Diagnose and solve problems", "Access Control (IAM)", and "Settings". On the right, there are buttons for "Upload", "Change access level", "Refresh", "Delete", "Change tier", and "Acquire lease". The "Authentication method" is listed as "Access key (Switch to Microsoft Entra user account)" and the "Location" is "changetrackingblob / Arctoys-Win2K25". A search bar at the top right says "Search blobs by prefix (case-insensitive)" and has a "Show deleted blobs" toggle switch. Below the search bar is a "Add filter" button. The main content area displays a table with columns: Name, Modified, Access tier, Archive status, and Blob type. One row is visible, showing a file named "2025-04-10 16:17:23-ct.txt" with a modified date of "4/10/2025, 7:19:19 A..." and an access tier of "Hot (Inferred)".

**Task 4 has been completed**

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Task 5: Query in Log Analytics

---

- 1. On the Change tracking page from your Arc-enabled machine, select *Log Analytics*.
- 2. In the Logs search, look for content changes to the *ct.txt* file by entering and running the following query. The result should show information about the changes.

```
shell
▶ ConfigurationChange | where FieldsChanged contains "FileContentChecksum" and File
SystemPath == "C:\ArcBox\ct.txt"
▶ Run
Time range: Last 24 hours Show: 1000 results
KQL mode
1 ConfigurationChange | where FieldsChanged contains "FileContentChecksum" and FileSystemPath == "C:\ArcBox\ct.txt"
Results Chart
TimeGenerated(UTC) Computer ConfigChangeType ChangeCategory SourceComputerId Name FileSystemPath Size
2023-04-10T16:21:16.000Z ArcBox-Win2025 File Modified 00-0000-0000-0000-000000000000 ct.txt C:\ArcBox\ct.txt 64
```

- 4. (Optional) In Log Analytics, alerts are always created based on log analytics query result. If you want to be alerted when someone changes a file on any one of your server, then you can configure an alert by referring to this [tutorial](#).

**Task 5 has been completed**

---

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB06: Gain security insights from your Arc-enabled servers using Microsoft Sentinel

---

Student Lab Manual

Table of Contents

Exercise 1 - Configure data collection on Sentinel

**Task 1 - Configure data collection on Sentinel**

Exercise 2 - Simulating and viewing security events

**Task 1 - Simulating-and viewing security events**

# Exercise 1 - Configure data collection on Sentinel

---

## **Objective**

This exercise will walk you through how to enable data collection on Sentinel for Windows security events.

## **Estimated Time to Complete This Lab**

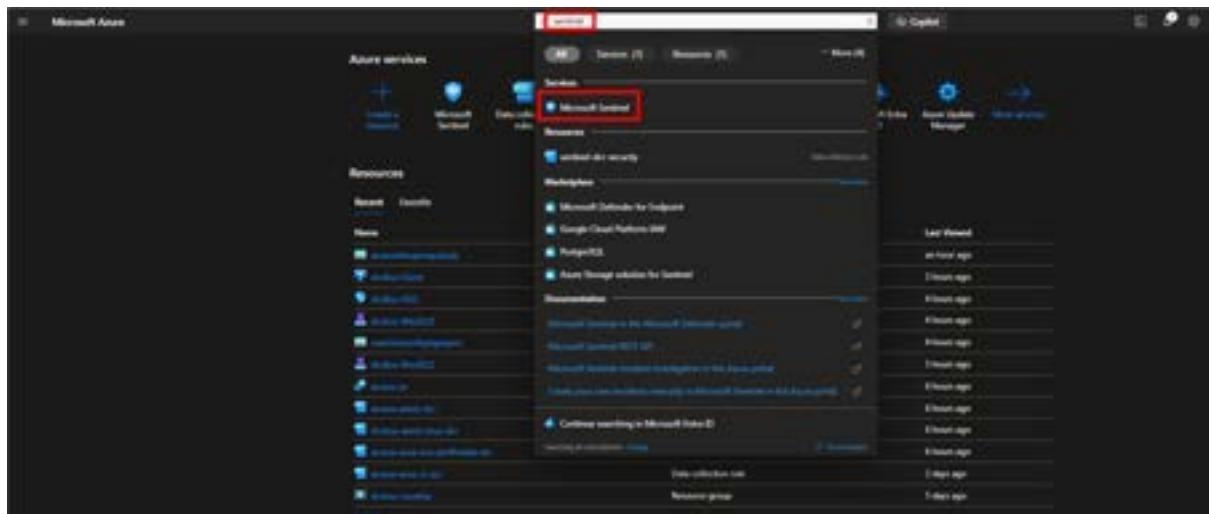
20 minutes

## **Explanation**

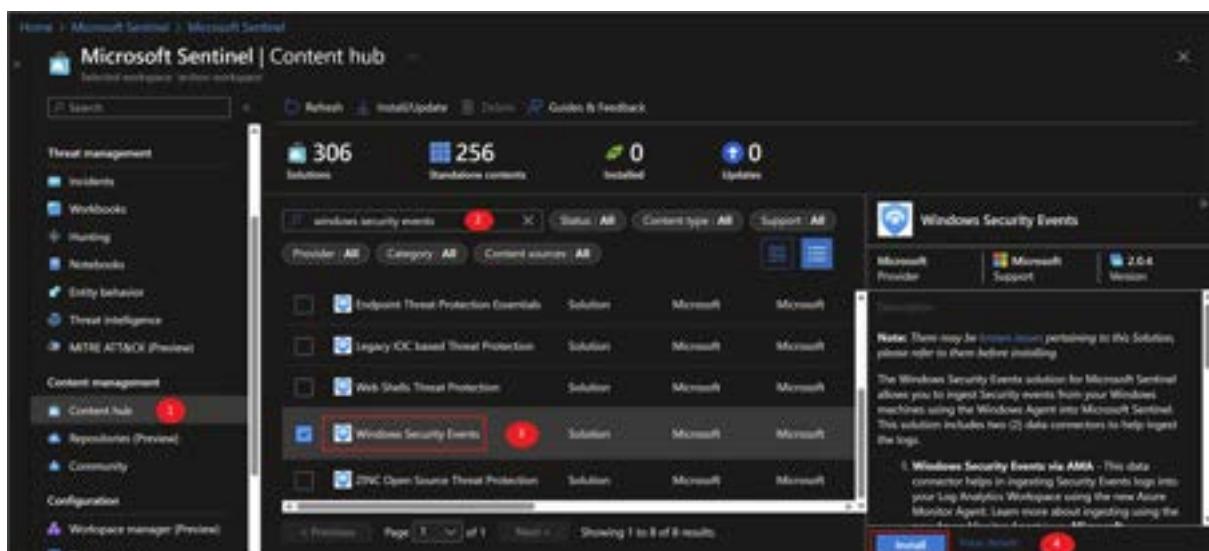
In this exercise, you will learn how to enable data collection on Sentinel for Windows security events, simulate failed logins and visualize them in Sentinel.

## Task 1: Configure data collection on Sentinel

- 1. In the Azure Portal, search for *Sentinel*



- 2. Click on "Content Hub" and search for "Windows Security Events" and install it.



- 3. After installation, click on "Manage" to configure the collector.

The screenshot shows the Microsoft Sentinel Content hub interface. On the left, there's a sidebar with navigation links like Notebooks, Entity behavior, Threat intelligence, METRATTACK (Preview), Content management (Content hubs, Repositories (Preview), Community), Configuration (Workspace manager (Preview), Data connectors, Analytics, Watchlist, Automation, Settings), and Help (Search, Refresh, Install system, Status, Update, Guides & Feedback). The main area has a search bar and filters for Provider (All), Category (All), and Content source (All). It displays a list of solutions, with 'Windows Security Events' highlighted. The right side shows a detailed view of the 'Windows Security Events' solution, including its provider (Microsoft), support (Microsoft), version (2.0.4), and a note about installing it. A red box highlights the 'Manage' button at the bottom.

- 4. Select the data connector and make sure you've selected the *Windows Security Events via AMA* and click "open connector page".

The screenshot shows the 'Windows Security Events' connector page. It features a summary bar with 67 installed content items and 22 configuration needed. The main content area lists 'Windows Security Events' and 'Windows Security Events via AMA'. The 'Windows Security Events via AMA' item is highlighted with a red box. The right panel shows a log viewer for the 'Windows Security Events via AMA' connector, with a red box highlighting the 'Open connector page' button at the bottom.

- 5. Create a new data collection rule.

The screenshot shows the Microsoft Sentinel interface for managing Windows Security Events via Azure Monitor Agents (AMA). On the left, there's a sidebar with a 'Windows Security Events via AMA' section. It includes a 'Description' block, a 'Last data received' section, and a 'Related content' area showing 6 Workbooks, 1 Query, and 20 Analytics rules templates. On the right, the main pane has a 'Instructions' section with a note about collecting data from non-Azure VMs. Below it is a 'Configuration' section with a 'Create data collection rule' button, which is highlighted with a red box.

6. Provide a name for the data collection rule and select the same resource group where you've deployed this level-up lab.

This screenshot shows the 'Create Data Collection Rule' dialog box. It has tabs for 'Basic', 'Resources', 'Collect', and 'Review + Create'. The 'Basic' tab is selected. It includes fields for 'Rule Name' (set to 'sentinel-aci-security'), 'Subscription' (set to 'Online'), and 'Resource Group' (set to 'ardex'). The 'Subscription' and 'Resource Group' dropdowns are highlighted with a red box.

7. Select one or multiple Windows Arc-enabled machines.

[Home](#) > Microsoft Sentinel | Content Hub > Windows Security Events via AMA

## Windows Security Events via AMA

Windows Security Events via AMA

Disconnected Status Microsoft Provider 3 Minutes Last Log Received

Description You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received 2/19/2025, 2:29:47 PM

Content source Version Windows Security Events 1.00

Author Microsoft Supported by Microsoft Corporation

Related content 0 Workbooks 1 Queries 20 Analytics rules: Tempa

Data received Go to log analysis

< Previous Next Collect >

**Create Data Collection Rule**

This will also enable System Assigned Managed identity on these machines, in addition to existing User Assigned identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned Identity for all other applications. [Learn more](#)

Subscriptions Resource Groups Resource Types Locations

Selected All Selected All Selected All Selected All

Search to filter items... Show Selected

Scope	Resource Type	Location
<input type="checkbox"/> Visual Studio Enterprise Subscription		
<input type="checkbox"/> Arbor		
<input checked="" type="checkbox"/> Arbor-Win2022	microsoft.hybrid/compute/machines	Central US
<input checked="" type="checkbox"/> Arbor-Win2025	microsoft.hybrid/compute/machines	Central US

- 8. Select the "Common" event type and create the data collection rule.

[Home](#) > Microsoft Sentinel | Content Hub > Windows Security Events via AMA

## Windows Security Events via AMA

Windows Security Events via AMA

Not connected Status Microsoft Provider Last Log Received

Description You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities.

Last data received

Related content 6 Workbooks 111 Queries 20 Analytics rules: Tempa

Data received Go to log analysis

**Create Data Collection Rule**

Basics Resources Collect Review + Create

Select which events to ingest:

All Security Events  Common  Minimal  Custom

Workspaces

To collect data

Configuration

Enable data collection Security Events

Rule name No data collection

< Previous Next / Review + Create >

The screenshot shows the Microsoft Sentinel interface for managing Windows Security Events via Application Management Agent (AMA). The left pane displays a summary of the connection status, showing 'Not connected' with a 'Microsoft Provider' and 'Last Log Received' field. It also includes a 'Description' section detailing the purpose of collecting security events from Windows machines, and a 'Related content' section with links to Workbooks, Queries, and Analytics rules templates. The right pane is titled 'Instructions' and contains two sections: 'Workspace data sources read and write permissions' (with a green checkmark) and 'To collect data from non-Azure VMs, they must have Azure Arc installed and enabled' (with a blue info icon). Below these is the 'Configuration' section, which includes an 'Enable data collection rule' link and a table for defining data collection rules. One rule is listed: 'Security Events logs are collected only from Windows agents'. The table columns are 'Rule name', 'Created by', and 'Event filter type'. A red box highlights the 'Security Events logs are collected only from Windows agents' row.

**Task 1 has been completed**

# Exercise 2 - Simulating and viewing security events

---

## **Objective**

This exercise will walk you through how to view Windows security events in Sentinel.

## **Estimated Time to Complete This Lab**

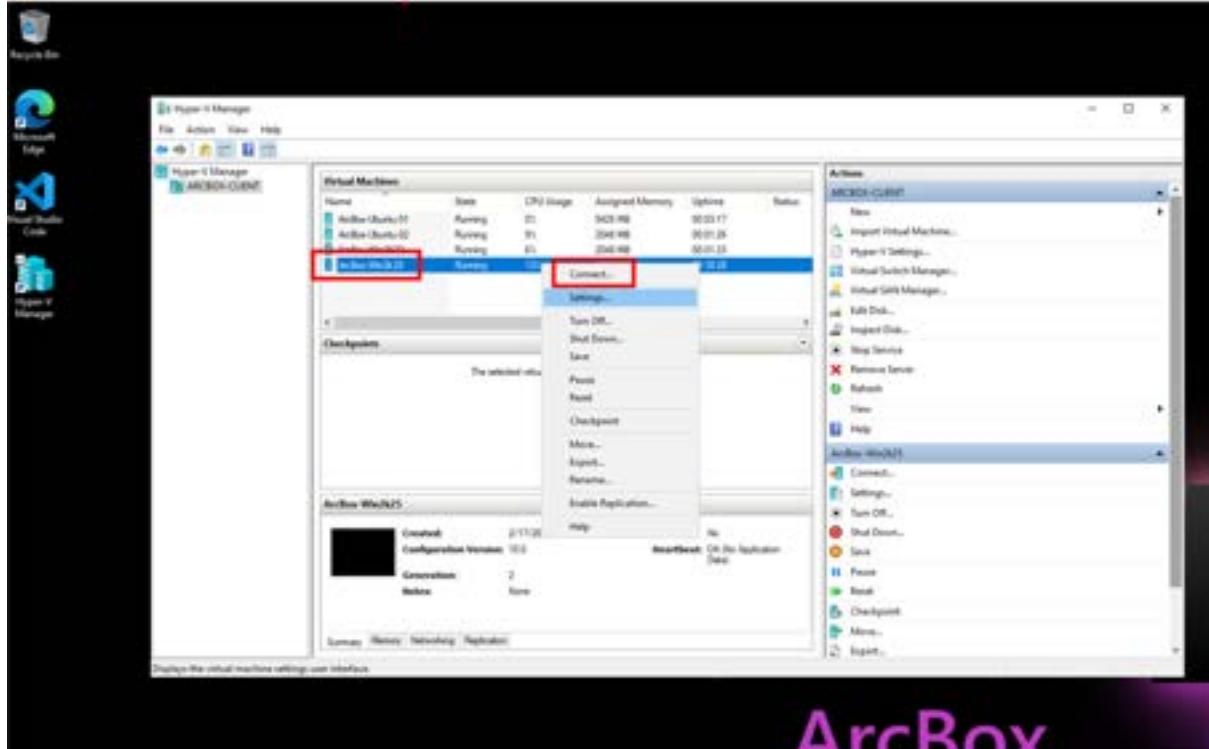
20 minutes

## **Explanation**

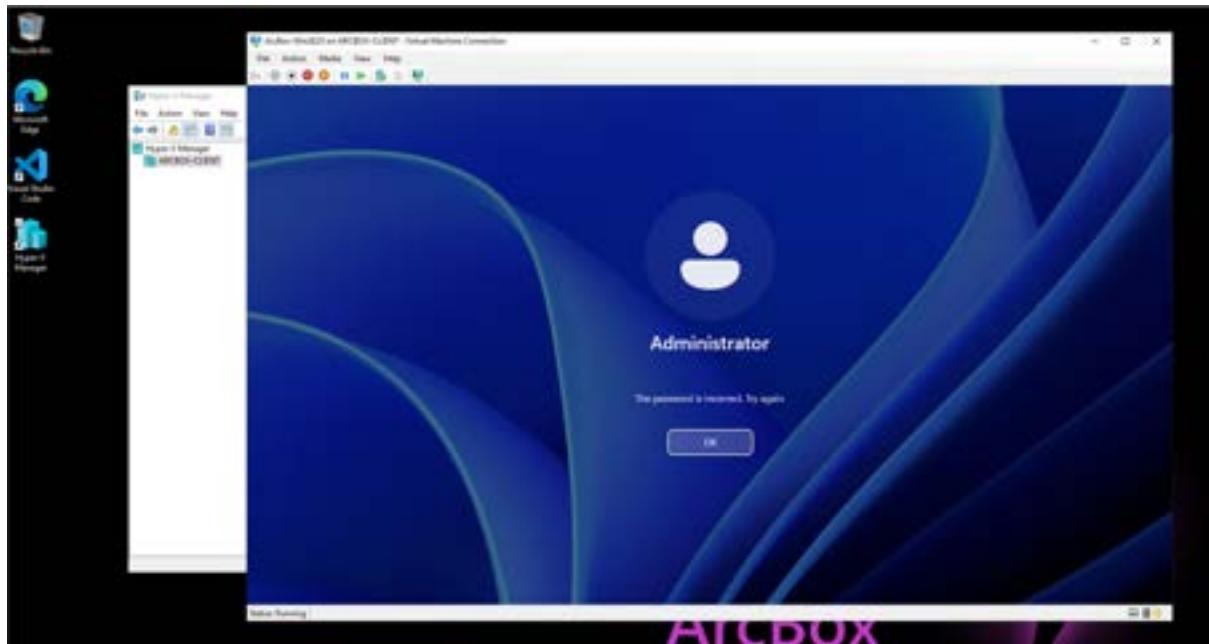
In this exercise, you will learn how to leverage Sentinel to view failed logins using Windows security events data collection.

## Task 1: Simulating-and viewing security events

- 1. After configuring Sentinel, now we need to simulate some failed login attempts on one or more Windows Arc-enabled machines.
- 2. Connect to *ArcBox-Client* VM, and open the *Hyper-v manager*.
- 3. Right-click one of the Windows machines and connect to it.



- 4. Simulate some failed login attempts by trying to login multiple times using an incorrect password.



- 5. After waiting for about 10-15 minutes for data to start getting ingested into the log analytics workspace, navigate to "Workbooks" and select the "Identity & Access" workbook.

The screenshot shows the Microsoft Sentinel Workbooks page. On the left, there's a navigation sidebar with various options like Overview, Logs, Metrics, Search, and Workbooks (which has a red notification badge). The main area displays a list of workbooks: 'Event Analytics' (Content source: Event Analytics), 'Identity & Access' (Content source: Connected Rule), and 'Connected Rule' (Content source: Connected Rule). A red circle highlights the 'Identity & Access' icon. To the right, there's a detailed view of the 'Identity & Access' template, including its description, required data types (Logs, Connected Rule), content source (Windows Security Events), author (Microsoft), and supported by (Microsoft Cloud). A red circle also highlights the 'Identity & Access' section in this detailed view.

- 6. Once data is being ingested, you will start seeing the failed login attempts in the workbook.

User activities						Machine activities					
Name	Type	Ti	Activity Count	Ti	Count	Name	Type	Ti	Activity Count	Ti	Count
✓ 1aef0-9a0e-40f0-aed6-1234567890ab	Computer	2				✓ 1aef0-9a0e-40f0-aed6-1234567890ab	Computer	2			
✓ 411a0a-8900-4700-9100-1234567890ab	Computer	4				✓ 411a0a-8900-4700-9100-1234567890ab	Computer	4			
✓ 411a0a-8900-4700-9100-1234567890ab	Computer	4				✓ 411a0a-8900-4700-9100-1234567890ab	Computer	4			
✓ administrator	Computer	2				✓ administrator	Computer	2			
✗ 4001 - An account failed to log on	Activity	4				✗ 4001 - An account failed to log on	Activity	4			
✓ 2001	Computer	4				✓ 2001	Computer	4			
✓ 2001	Computer	4				✓ 2001	Computer	4			
✓ 2001	Computer	4				✓ 2001	Computer	4			

## **Task 1 has been completed**



**Congratulations, you have completed all tasks in this lab**

Click **Next** for the next lab or [\*\*Go back to the main table of content\*\*](#)

# LAB07: Keep your Azure Arc-enabled servers patched using Azure Update Manager

---

## Student Lab Manual

### Table of Contents

Exercise 1 - Enable Azure update manager for the Arc-enabled servers.

**[Task 1 - Use the Azure portal and search for Azure Update manager](#)**

Exercise 2 - Apply machine updates for the Arc-enabled servers using Azure update manager

**[Task 1 - Create a maintenance configuration from Azure update manager](#)**

**[Task 2 - Apply one-time updates from Azure update manager](#)**

Exercise 3 - Monitor Azure update manager using the update reports.

**[Task 1 - Deploy the Azure update manager Overview workbook](#)**

## Lab overview

---

Azure Update Manager is the service that unifies all VMs running in Azure together with Azure Arc, putting all update tasks in 1 common area for all supported Linux and Windows versions.

In this Lab, you will setup Azure update manager and learn how to enable it to efficiently manage all updates for your machines, regardless of where they are. You will also see some of the default reports using workbooks to monitor your Azure update manager environment.

## Exercise 1 - Enable Azure update manager for the Arc-enabled servers.

---

### **Objective**

In this exercise, the goal is to see all the Arc-enabled servers in the Azure update manager portal and to be able to create an automatic recurring task to refresh the status of your machines.

### **Estimated Time to complete this lab**

20 minutes

## Task 1: Use the Azure portal and search for Azure Update manager

- 1. Find the Azure Update Manager in the Azure portal then click on "Machines" in the left blade to view all your Azure machines.

**Note that all Azure VMs and Arc Server VMs are already visible in this Azure Update Manager service. In addition, the required extensions are installed on the ArcBox-Win2k25 and Arcbox-Ubuntu-01 Arc-enabled machines so that you can perform the tasks in this lab faster should you want to do that. As such these two machines might already show that they require some updates before carrying out the assessment in the following steps.**

The screenshot shows the Azure Update Manager interface under the 'Machines' section. On the left, there's a navigation menu with 'Machines' highlighted. The main area displays summary statistics: Total machines (4), No updates data (1), No pending updates (0), Pending updates (3), and Pending reboot (0). Below this, a table lists four machines: Arcbox-Ubuntu-01, Arcbox-Win2k25, Arcbox-Win2k25, and Arcbox-Win2k25. All four machines are marked as having pending updates. The rows for Arcbox-Ubuntu-01 and the last two Arcbox-Win2k25 entries are highlighted with red boxes.

Name	Update status	ESU Status	Operating system	Resource type
Arcbox-Ubuntu-01	3 pending updates	N/A	Linux	Arc-enabled server
Arcbox-Win2k25	4 pending updates	N/A	Windows	Arc-enabled server
Arcbox-Win2k25	4 pending updates	N/A	Windows	Arc-enabled server

- 2. Select the Arc-enabled machines and click on the refresh button to refresh the current status of the selected VMs.

The screenshot shows the Azure Update Manager interface. At the top, there's a search bar, a 'Refresh' button (highlighted with a red box), and several navigation links like 'Check for updates', 'One-time update', 'Schedule updates', 'Settings', 'Maintenance configurations', 'Open query', and 'Export'. Below this is a filter section with dropdowns for 'Subscription', 'Resource group', 'Resource type', 'Workload', and 'Location'. The main area displays summary statistics: 'Total machines: 5', 'No updated data: 2', 'No pending updates: 0', 'Pending updates: 3', 'Pending reboot: 0', and 'Unsupported: 0'. Below these stats is a table titled 'Showing 5 of 5 records' with columns: 'Name', 'Update status', 'EMI Status', 'Operating system', 'Resource type', 'Patch orchestration', and 'Periodic assessment'. The table lists five VMs: 'ArcVM-Win01', 'ArcVM-Win02', 'ArcVM-Linux01', 'ArcVM-Win03', and 'ArcVM-Win04'. The first two VMs have 'Pending updates' status, while the others have 'No updated data'. The 'Periodic assessment' column for the first two VMs is set to 'No', indicating they are not yet assessed.

3. **Optional** - you can enable automatic recurring task for at scale refresh once every 24 hours.

select the Arc-enabled servers, click on settings then choose update settings, and set the periodic assessment drop down to enable.

Note that the rest of the VMs will automatically be enabled.

This screenshot shows the 'Change update settings' dialog for a selected subset of machines. The dialog title is 'Change update settings' and it says 'Select the update settings that you want to change for the machines. The selected update settings will be applied to all applicable selected machines.' There is a note about patch orchestration being applicable only to Arc-enabled servers. The dialog lists two groups of machines: 'Windows (2)' and 'Linux (2)'. Each group has a table with columns: 'Machine Name', 'Resource type', 'Periodic assessment', 'Impact', and 'Patch orchestration'. In the 'Impact' column, the dropdown menu is set to 'Select and apply to all' for both groups. The 'Patch orchestration' dropdown also has 'Select and apply to all' selected. At the bottom, there are 'Save' and 'Cancel' buttons.

**Task 1 has been completed**

## Exercise 2 - Apply machine updates for the Arc-enabled servers using Azure update manager

---

### **Objective**

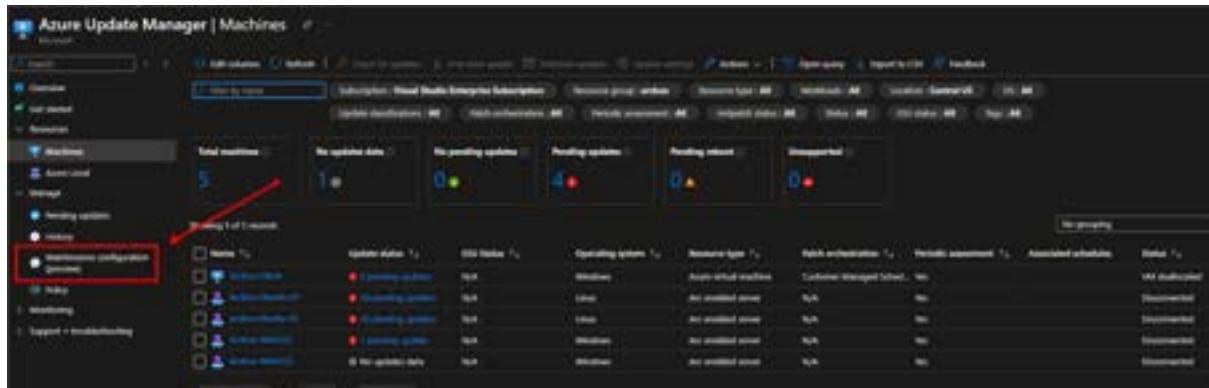
In this exercise, the goal is to apply machine updates for your Azure VMs including Azure Arc-enabled VMs using maintenance configuration and one time updates.

### **Estimated Time to complete this lab**

30 minutes

## Task 1: Create a maintenance configuration from Azure update manager.

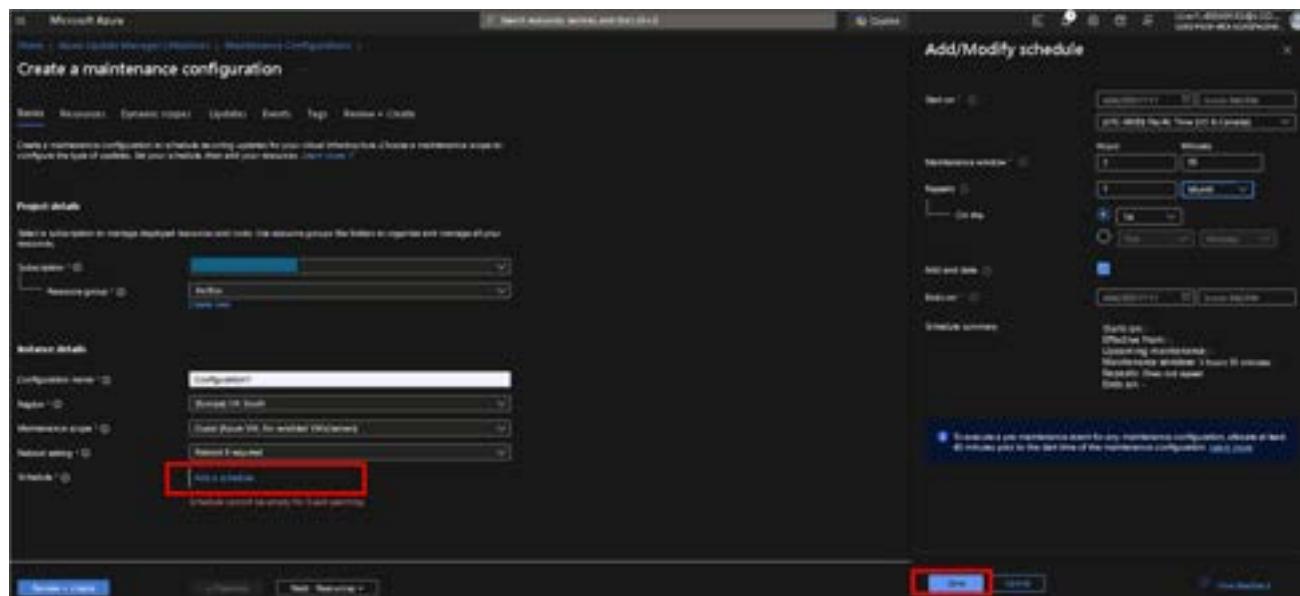
- 1. Click on *Maintenance configuration* under the "Manage" blade on the left as shown below, then select *Create maintenance configuration*.



The screenshot shows the Azure Update Manager interface. On the left, there's a navigation menu with 'Manage' selected. Under 'Manage', 'Maintenance' is highlighted. A red box surrounds the 'Maintenance configuration' link. To its right, there are sections for 'Total machines' (5), 'My update status' (1), 'My pending updates' (0), 'Pending updates' (4), 'Pending restart' (0), and 'Disconnected' (0). Below these are detailed tables for each category. The 'Pending updates' table includes columns for 'Update status', 'Disk Health', 'Operating system', 'Resource type', 'Patch recommendation', 'Health assessment', 'Associated schedule', and 'Status'.

- 2. Fill out the basics tab as shown below, make sure you choose a region based on your location. Leave the rest as default.

Note For countries in Asia and Europe, it is a good idea to use second Tuesday + 1 day to coincide with Patch Tuesday. Do not use "Second Wednesday of the month".



The screenshot shows the 'Create a maintenance configuration' blade. The 'Basics' tab is active. In the 'Maintenance details' section, there's a dropdown for 'Configuration' set to 'Configuration1' and a dropdown for 'Region' set to 'East US'. Under 'Maintenance scope', 'Resource group' is set to 'Arc-Enabled-Machines'. The 'Exclude' dropdown is set to 'None'. A red box highlights the 'Add to schedule' button. To the right, a modal titled 'Add/Modify schedule' shows a weekly recurrence with 'Start on' set to '2023-05-16' and 'End on' set to '2023-05-17'. The 'Schedule summary' shows 'Starts on: 2023-05-16, Effective from: 2023-05-16, Duration: 2 hours 30 minutes'. At the bottom, there are 'Save & Next Step' and 'Cancel' buttons.

- 3. **Optional** click on dynamic scopes > click on the subscriptions where your Arc-enabled machines are > click on "filter by" option and choose how machines are added to this maintenance configuration (by OS, location, resource group)

In this guide, we filtered by the OS type as shown below.

The screenshot shows the 'Edit dynamic scope' page in the Azure portal. At the top, there's a header with 'Home > Azure Security Center > Machine Learning > Machine Learning > Configuration > Dynamic scope'. Below the header, there's a section titled 'Define a dynamic scope' with a note about defining machines to be evaluated at run time. There are dropdowns for 'Subscription' (set to 'All resources') and 'Filter by' (set to '2 Resource types, 0 tags'). A table titled 'Preview of machines based on status' lists 5 machines: 'Windows Dev1' (Windows, virtual machine, Customer Managed Schedule, VM running, Connected), 'Windows Dev2' (Linux, Server - Azure Dev, Server - Azure Dev, Connected), 'Windows Dev3' (Linux, Server - Azure Dev, Server - Azure Dev, Connected), 'Windows Dev4' (Windows, Server - Azure Dev, Server - Azure Dev, Connected), and 'Windows Dev5' (Windows, Server - Azure Dev, Server - Azure Dev, Connected). At the bottom, there are 'Next' and 'Cancel' buttons, with 'Next' highlighted with a red box.

**Note:** If you want to enable dynamic scopes, you will need to enable the "Dynamic Scoping" preview feature in the subscription.

The screenshot shows the 'Preview features' page in the Azure portal. On the left, there's a sidebar with 'Subscriptions' (selected), 'My role >> All', 'Subscription: Alloted (1 of 1)', and 'Subscription name: Tg\_MQD9Hd99947'. The main area is titled 'Exploring pre-release features with Preview Features'. It shows a list of preview features: 'Dynamic' (selected and highlighted with a red box), 'Display Name', 'State', 'Provider', and 'Release Date'. The 'Dynamic' row shows 'Not Registered', 'Microsoft Maintenance', 'Tue Mar 14 2023', and 'Documentation'. There are tabs for 'Security' and 'Preview features'.

- 4. Click on the *Resources* tab to choose machines specifically instead of dynamically.

## Create a maintenance configuration

Basics Resources Dynamic scopes Updates Events Tags Review + Create

Assign resources to this maintenance configuration now, or assign them after the maintenance configuration deploys. You're limited to five resource assignments now, but you can add as many as you like after deployment.

**+ Add resources** — Remove resources

Name	Type	Resource group	Location	Subscription

Select resources

Select resources to assign to this maintenance configuration. Previously assigned resources will be shown below. [Learn more](#)

Filter by name

Subscription: **All** Resource group: **All** Location: **All** Resource type: **All**

Auto-select resources won't available soon to support your maintenance window. [Learn more](#)

Name	Type	Resource group	Location	Description	Operating system	Patch prioritization options
- Selected (0)						
- Available (0)						
<input type="checkbox"/> <b>Windows Client</b>	Virtual machine	Windows	Central	Windows	Windows	Customer Managed Schedule
<input checked="" type="checkbox"/> <b>Windows Server 2017</b>	Virtual machine	Windows	Central	Windows	Windows	Customer Managed Schedule
<input checked="" type="checkbox"/> <b>Windows Server 2016</b>	Virtual machine	Windows	Central	Windows	Windows	Customer Managed Schedule
<input checked="" type="checkbox"/> <b>Windows Server 2019</b>	Virtual machine	Windows	Central	Windows	Windows	Customer Managed Schedule
<input checked="" type="checkbox"/> <b>Windows Server 2022</b>	Virtual machine	Windows	Central	Windows	Windows	Customer Managed Schedule
- Unassigned resources (0)						

- 5. Click on the updates tab to choose what type of updates will be installed by this config as shown below.

Microsoft Azure

Create a maintenance configuration

Updates

+ Include update classification

Included classifications

Operating system Classification included

Windows Critical updates, Security updates

Linux Security and critical updates

Included KB ID packages

Operating system KB ID packages included

Windows All KB IDs included

Include update classification

Select the appropriate classifications below for your resource. Selected classifications will be installed. [Learn more](#)

Select all

Security and critical updates

Other updates

Select all

Critical updates

Security updates

Update rollups

Feature pack

Service pack

Definition updates

Patch

Add Cancel

Review + Create

Next: Events >

Include update classification

Task 1 has been completed

## Task 2: Apply one-time updates from Azure update manager.

Instead of using maintenance configs with specific recurring cycles, you can also setup one-time updates (immediately!). Start by forcing an immediate refresh.

- 1. Select your Arc-enabled machines, select "Check for updates" from the top menu

The screenshot shows the 'Azure Update Manager | Machines' interface. On the left, there's a sidebar with 'Overview', 'Get started', 'Resources' (which is selected and highlighted in red), 'Manage', 'History', 'Policy', 'Monitoring', and 'Support + troubleshooting'. The main area has a heading 'Check for updates' with a note: 'Initiate assessment immediately on the selected 2 Windows servers and 2 Linux machines by clicking Check for updates. Note that during this period any other update related operations will not be allowed for these machines.' Below this are summary boxes for 'Total machines' (5), 'No updates data' (2), 'No pending updates' (0), 'Pending updates' (3), 'Pending reboot' (0), and 'Unsupported' (0). A table lists 5 machines: 'Arcbox-Ubuntu-01' (Windows, pending update), 'arcbox-ubuntu-02' (Linux, no update data), 'ArcBox-Win2K22' (Windows, no update data), 'Arcbox-Win2k25' (Windows, pending update), and 'Arcbox-Win2k26' (Windows, pending update). The 'Check for updates' button at the top is also highlighted in red.

- 2. Wait for the assessment to finish then select from the top as shown below.

The screenshot shows the 'Notifications' page. At the top, there are icons for search, notifications (highlighted in red), settings, help, and user profile. Below is a heading 'Notifications' with a close button. It includes links for 'More events in the activity log' and 'Dismiss all'. A message box is displayed, containing a green checkmark icon, the text 'Assessment successful', and the message 'Assessment successfully completed for 4 machine(s). Succeeded for : Arcbox-Ubuntu-01, arcbox-ubuntu-02, ArcBox-Win2K22, Arcbox-Win2k25'. This message box is also highlighted with a red border. At the bottom right of the message box is the text 'a few seconds ago'.

The screenshot shows the Azure Update Manager interface. On the left, there's a navigation menu with options like Overview, Get started, Resources, Machines, Azure Stack HCI, Manage, History, Help, Monitoring, and Support + troubleshooting. Under the Machines section, there are several cards: Total machines (5), No updates found (0), No pending updates (0), Pending updates (5), Pending reboot (0), and Unsupported (0). Below these cards is a table titled 'Showing 1 of 5 results' with columns: Name, Update status, ISO Status, Operating system, Resource type, Patch orchestration, and Periodic assessment. The table lists five machines: 'Azure-Ubuntu-01' (Pending update, N/A, Linux, Arc-enabled server, Auto, N/A), 'Azure-Ubuntu-02' (All pending updates, N/A, Linux, Arc-enabled server, Auto, N/A), 'Azure-Ubuntu-03' (All pending updates, N/A, Linux, Arc-enabled server, Auto, N/A), 'Azure-Win2022' (Pending update, N/A, Windows, Arc-enabled server, Auto, N/A), and 'Azure-Win2025' (Pending update, N/A, Windows, Arc-enabled server, Auto, N/A). At the top right, there are buttons for One-time update, Schedule update, Settings, Maintenance configurations, Open query, Export to CSV, and Help. A red box highlights the 'One-time update' button.

3. Confirm your machines selection from the machines tab.

The screenshot shows the 'Install one-time updates' page. At the top, there are tabs for Machines (selected), Updates, Properties, and Review + install. Below the tabs, it says 'Select resources/machines to install updates. Updates to be installed can be selected in the next step. The updates available below are as per the last assessment performed on respective machines. To get information on the latest available updates, we recommend you perform a fresh assessment before installing updates.' There are 'Add machine' and 'Remove machine' buttons. The main area shows a table with columns: Machine Name, Update status, Operating system, and Resource type. Four machines are listed: 'Azure-Ubuntu-01' (40 pending updates, Linux, Arc-enabled server), 'Azure-Ubuntu-02' (80 pending updates, Linux, Arc-enabled server), 'Azure-Win2022' (4 pending updates, Windows, Arc-enabled server), and 'Azure-Win2025' (4 pending updates, Windows, Arc-enabled server). All machines have checkboxes checked.

4. Click on the updates tab and select updates of your choice to apply to your machines.

The screenshot shows the 'Install one-time updates' page with the 'Updates' tab selected. It includes filters for 'Select by update classification', 'Include by H1 Coverage', 'Exclude by H1 Coverage', and 'Include by maximum patch publish date'. Below these are sections for 'Operating system' (Windows and Linux) and 'Selected classification' (All classifications). The 'Preview of selected updates to install' section shows a list of updates: 'Windows Feature Updates - UpdateDefinition' (Classification: Classification, Published: 10/11/2023, 10:00:00 AM), 'Security Intelligence Update for Win... - Definition' (Classification: Classification, Published: 10/11/2023, 10:00:00 AM), 'PowerShell v7.4.14440.0 - Update' (Classification: Classification, Published: 10/11/2023, 10:00:00 AM), and 'Windows 11 Cumulative Update for Win... - Security' (Classification: Classification, Published: 10/11/2023, 10:00:00 AM). At the bottom, there are 'Previous' and 'Next' buttons, and a note: '110 updates selected across 4 machines'.

5. Click on the properties tab and select "reboot if required" and "60 minutes" for the Maintenance window.

Home > Azure Update Manager | Machines

## Install one-time updates

Azure Update Manager

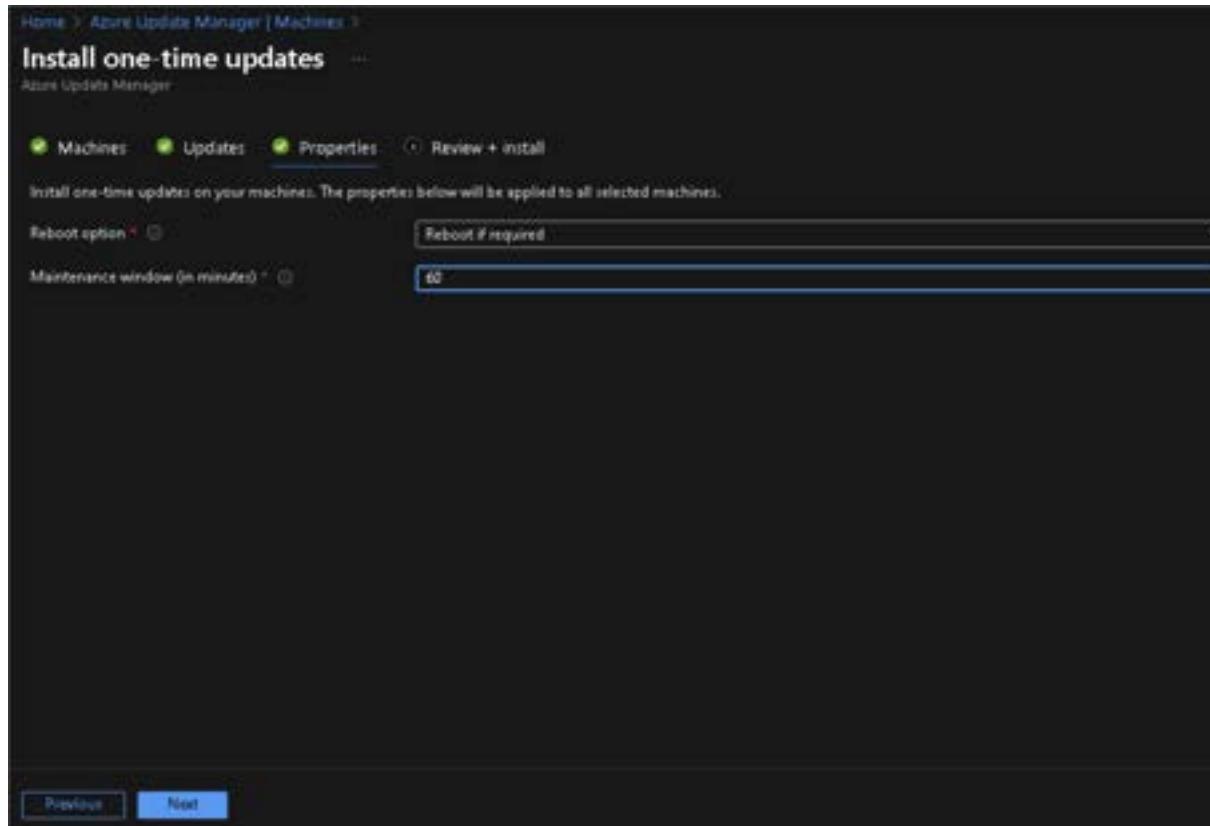
Machines Updates Properties Review + install

Install one-time updates on your machines. The properties below will be applied to all selected machines.

Reboot option: Reboot if required

Maintenance window (in minutes): 60

Previous Next



- 6. Wait for a few hours and a few reboots - this can take repeated forcing for machines that have not been updated for a long time.

### Task 2 has been completed

## Exercise 3 - Monitor Azure update manager using the update reports.

---

### **Objective**

In this exercise, the goal is to view different reports in Azure update manager that relate to your Azure Arc-enabled servers and how to navigate through them.

### **Estimated Time to complete this lab**

20 minutes

## Task 1: Deploy the Azure update manager Overview workbook.

Under the Monitoring part of the Update Manager, there is a default workbook, which is an overview of the Azure Update Manager. There are a few views in there that show the total number of machines connected, history of runs, and the status.

- 1. In Azure Update Manager, click on *Reports* under Monitoring. Select *Overview*.

The screenshot shows the 'Azure Update Manager | Reports | Gallery' interface. On the left, a navigation menu includes 'Overview', 'Get started', 'Resources' (with 'Machines' and 'Azure Local' sub-options), 'Manage' (with 'Pending updates', 'History', 'Maintenance configuration (preview)', 'Policy', and 'Monitoring' sub-options), 'Reports' (selected and highlighted in grey), 'New alert rule (Preview)', and 'Support + troubleshooting'. The main area displays 'Workbooks', 'Public Templates', and 'My Templates'. Under 'Quick start', there are two cards: 'Empty' (a completely empty workbook) and 'Dashboard (Preview)' (an empty dashboard preview). Below these are sections for 'Recently modified workbooks (0)' (No items found) and 'Azure Update Manager (2)'. The second item in this list, 'Update Compliance Report', is highlighted with a red box and has a red arrow pointing to it from the right side of the image. The card for 'Update Compliance Report' includes the text 'Overview' and 'Insights about machine configurations'.

- 2. Select the subscription that has your Azure Arc-enabled servers.

Note that there are a number of views in there that show the total number of machines connected, history of runs, and the status.

- 3. Expand the "Machines overall status & configurations" view of currently connected machines, split by Azure and Azure Arc VMs, and Windows and Linux numbers. Notice the View of manual vs periodic assessments and manual vs automatically updated

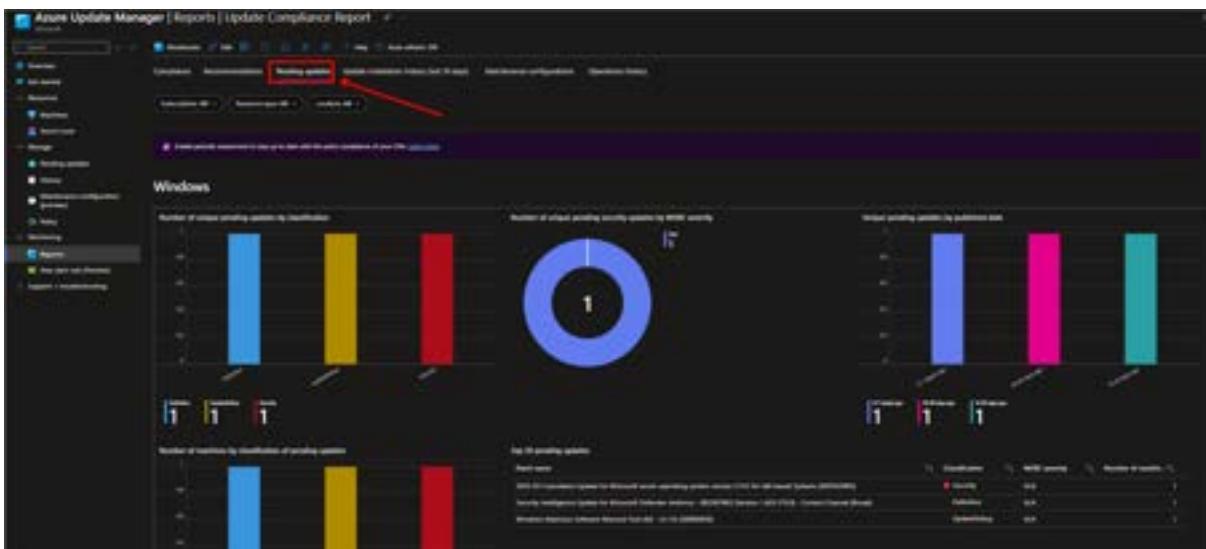
The screenshot shows the 'Azure Update Manager | Reports | Update Compliance Report' page. The left sidebar is identical to the one in the previous screenshot. The main content area features a header with tabs: 'Compliance' (selected and highlighted in blue), 'Recommendations', 'Pending updates', 'Update installation history (last 30 days)', 'Maintenance configurations', and 'Operations history'. Below this is a section titled 'Machines distribution by OS and Resource type'. This section contains a table with the following data:

Total	Azure virtual machines - Windows	Azure virtual machines - Linux	Arc-enabled servers - Windows	Arc-enabled servers - Linux
15	11	10	12	12

A red box highlights the entire 'Machines distribution by OS and Resource type' section, and a red arrow points to it from the right side of the image.



4. Expand the "Updates Data Overview" view and look at the updates by classification



Please expand the rest of the views "Schedules/maintenance configurations" and "History of installation runs" to visualize the updates running in Azure Update manager.

**Task 1 has been completed**

**Congratulations, you have completed all tasks in this lab**

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB08: Enroll your Windows Server 2012/ R2 machines for Extended Security Updates with Azure Arc

---

Student Lab Manual

Table of Contents

**Exercise 1** - Enable Extended Security Updates (ESU) license

[\*\*Task 1: Create a ESU license\*\*](#)

[\*\*Task 2: Link ESU license to Arc-enabled servers\*\*](#)

# Exercise 1 - Enable Extended Security Updates (ESU) license

---

## Objective

In this module, you will learn how to enable Extended Security Updates (ESU) for Azure Arc-enabled Windows Server 2012 R2 through the Azure portal.

## Estimated Time to Complete This Lab

30 minutes

## Explanation

Once Windows Server 2012 and 2012 R2 are registered as Azure Arc-enabled servers, you can enroll them for ESU via the Azure portal, connect through Azure Arc, and you'll be billed monthly via your Azure subscription.

## Documentation

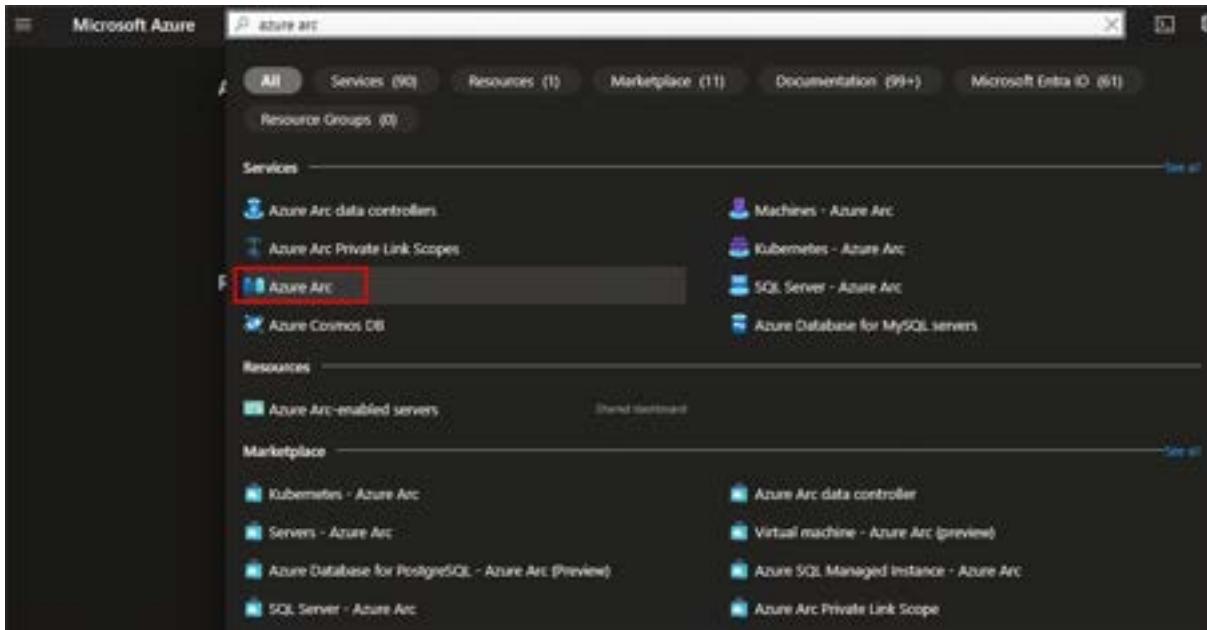
[Deliver Extended Security Updates for Windows Server 2012](#)

[License provisioning guidelines for Extended Security Updates for Windows Server 2012](#)

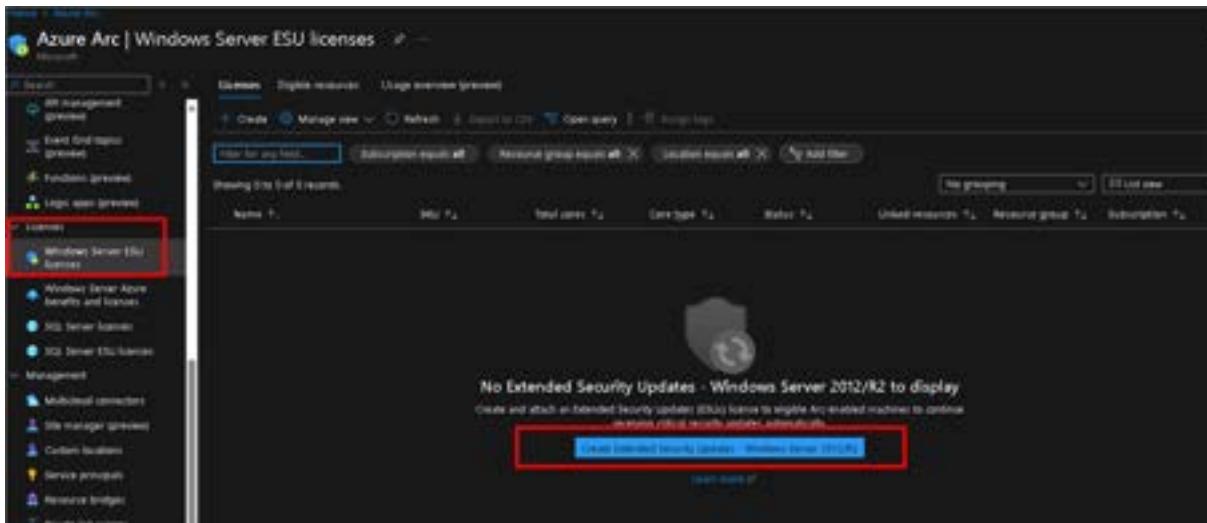
- ▶ >[!knowledge] To continue receiving security updates after extended support has

## Task 1: Create a ESU license

- 1. Navigate to the Azure Arc page



- 2. Select *Windows Server ESU licenses* in the left pane. Then click on *Create Extended Security Updates - Windows Server 2012/R2*



- 3. Provision Windows Server 2012 and 2012 R2 Extended Security Update licenses from Azure Arc.  
  
**□ Make sure to select "Activate later" for the license settings to avoid getting billed on the Azure Subscription**

## Create an Extended Security Updates license

X

### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription (1)

Resource group (1)
 ArcBox-LevelUp
[Create new](#)

### Instance details

License name \*
 ArcBox-ESU

Activate license

 [Activate now](#)

Start the billing cycle today. This license can be used to enable ESUs on eligible resources immediately.

 [Activate later](#)

ESUs and billing won't start until the license is activated.

Region (1)
 (US) East US

### License details

Provide the core type and pack amount needed for this ESU license. The minimum number of cores is 16 for physical and 8 for virtual core license. Once activated, the monthly cost will be calculated and billed to your Azure subscription. You can edit the number of cores later. [Learn more](#)

SKU (1)
 Windows Server 2012 or 2012 R2 Standard Edition
Core type (1)
 Virtual cores

#### Core packs

#### Amount needed

16 cores

0

2 cores

4

Total cores

8

Estimated cost

(1) Your total cost will be dependent on your SKU and total number of cores. [Learn more](#) (1)

Ensure that your Windows Server licenses have Software Assurance, your Windows Server licenses are acquired as subscription licenses, or you are covering WS workloads running on Authorized Mobility Partners' servers under license included offerings. [Learn more](#)

[Give feedback](#)
[Create](#)[Cancel](#)

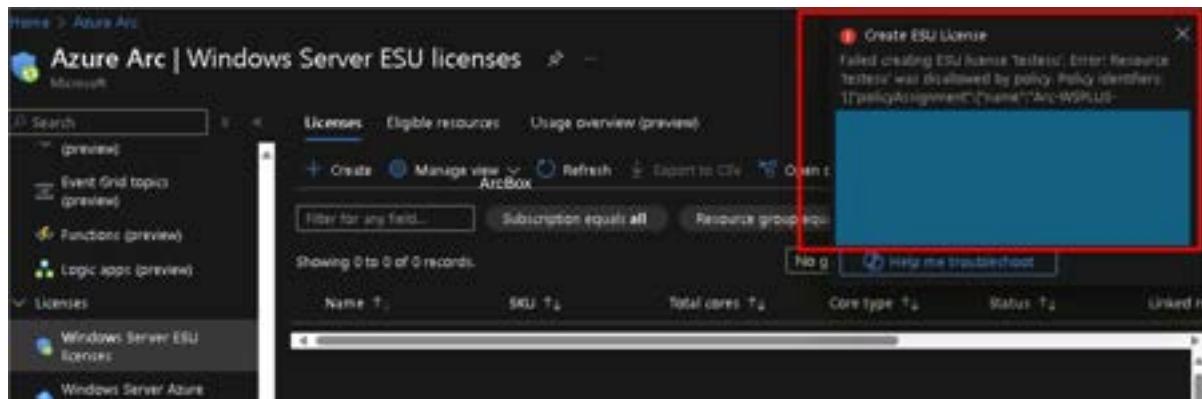
- When opting for ESU via Azure Arc for Windows Server, you have two licensing choices:

- vCore Licensing:** Pay based on the number of virtual cores (vCores) utilized by the operating system. This option uses the Standard edition rate. If you're operating multiple VMs, the cost will be calculated based on the total number of vCores across all VMs. **There is an 8-core minimum per VM for vCore licensing.**

**2. pCore Licensing:** Pay based on the number of physical cores (pCores) utilized by the host operating system. This option can use either edition. Note that with pCore licensing, up to 2 guest VMs running on a WS Standard host are covered (additional VMs require additional ESU licenses). With the WS Datacenter host, all VMs are covered without the need for additional licenses. **There is a 16-core minimum per server for pCore licensing.**

Please see [here](#) for details.

- 4. In this lab environment you will not be able to create an actual license due to the cost involved with back-billing. So when you attempt to create the license you should see the following message:



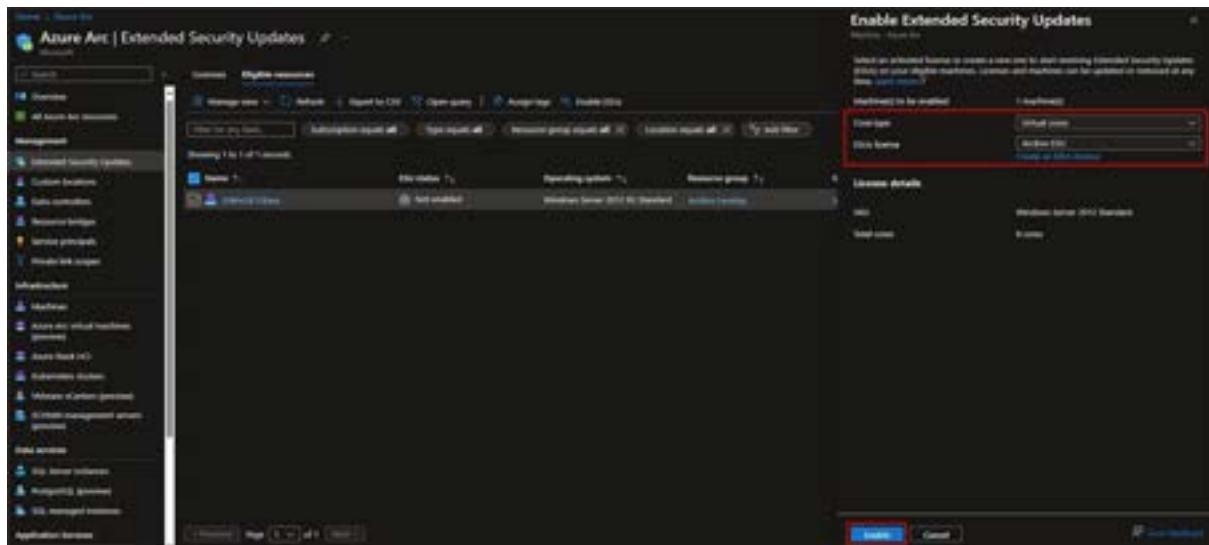
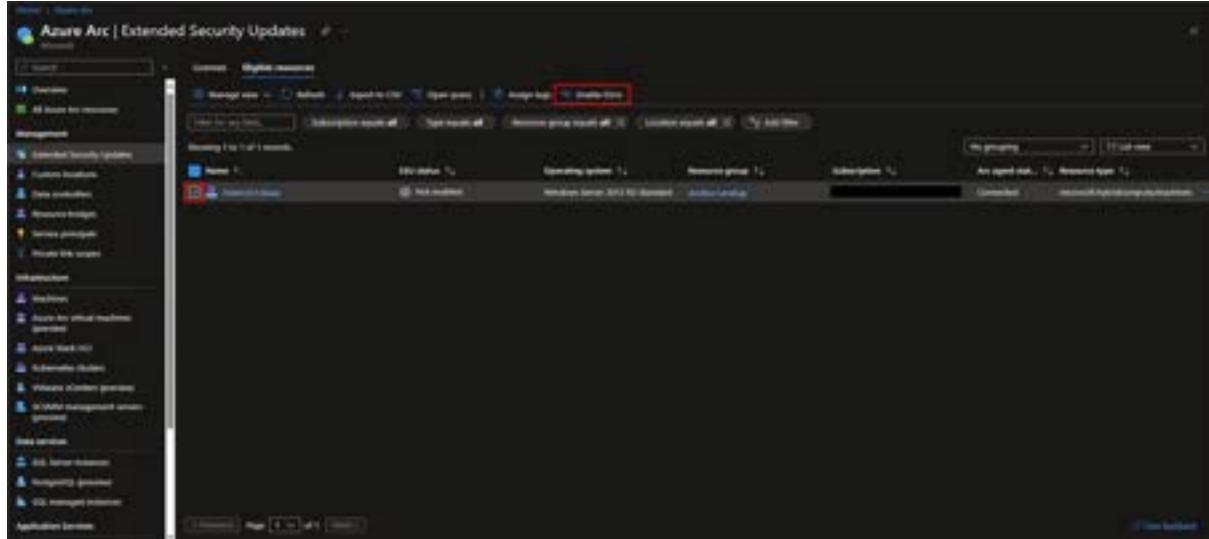
**Task 1 has been completed**

Click **Next** for the next task or [Go back to the main table of content](#)

## Task 2: Link ESU license to Arc-enabled servers

Since this lab environment does not allow the creation of an actual ESU license, you will not be able to link it to any Arc-enabled machine. So the guidance in this task is just informational and you will not have a Windows server 2012 machine provisioned within this lab.

1. Select one or more Arc-enabled servers to link to an Extended Security Update license.



2. The status of the selected machines changes to **Enabled**.

The screenshot shows the 'Azure Arc | Extended Security Updates' blade in the Azure portal. On the left, there's a navigation menu with sections like 'Databases', 'Managed', 'Extended Security Updates', 'Customer locations', 'File controllers', 'Resource bridges', 'Service principals', 'Private link scopes', 'Infrastructure', 'Machines', 'Mobile device enrollment providers', 'Azure Stack HCS', 'Automation clusters', 'Managed clusters (preview)', 'Network management (preview)', 'Data services', 'App Service instances', 'Analytics servers', and 'SQL Managed instances'. The 'Extended Security Updates' section is currently selected. In the main pane, there's a search bar at the top with filters for 'Subscription', 'Resource group', 'Operating system', 'Status', and 'Resource type'. Below the search bar, there's a table titled 'Showing 1 of 1 results' with one row. The row contains a checkbox labeled 'Select', a column for 'Name' (containing 'Windows Server 2012 R2 Standard'), a column for 'Status' (containing 'Activated' with a green checkmark), and columns for 'Operating system', 'Resource group', 'Subscription', 'Last updated', and 'Resource type'. At the bottom of the table, there are buttons for 'Import CSV', 'Open query', 'Edit', 'Delete', and 'Copy URL'.

- Once you've linked a server to an activated ESU license, the server is eligible to receive Windows Server 2012 and 2012 R2 ESUs.

### Task 2 has been completed

**Congratulations, you have completed all tasks in this lab**

---

Click **Next** for the next lab or [Go back to the main table of content](#)

## LAB09: Learn about Windows Admin Center single pane glass management

### Table of Contents

#### Exercise 1 - Manage your Arc-enabled Windows machines using the Windows Admin Center in Azure

##### [Task 1 - Pre-requisites](#)

##### [Task 2 - Deploy the Windows Admin Center VM extension](#)

##### [Task 3 - Connect and explore Windows Admin Center \(preview\)](#)

====

#### Exercise 1 - Manage your Arc-enabled Windows machines using the Windows Admin Center

In this exercise you will learn how to use the Windows Admin Center in the Azure portal to manage the Windows operating system of your Arc-enabled servers, known as hybrid machines. You can securely manage hybrid machines from anywhere without needing a VPN, public IP address, or other inbound connectivity to your machine.

#### Estimated Time to Complete This Lab

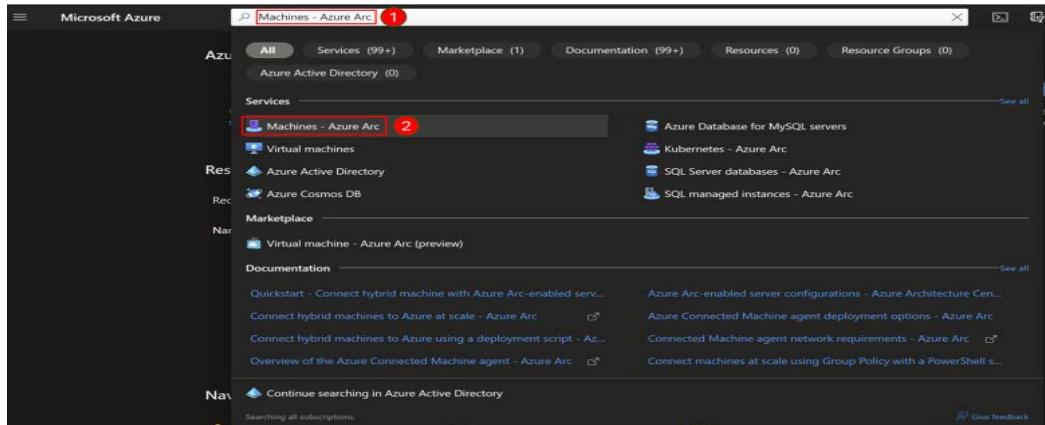
40 minutes

====

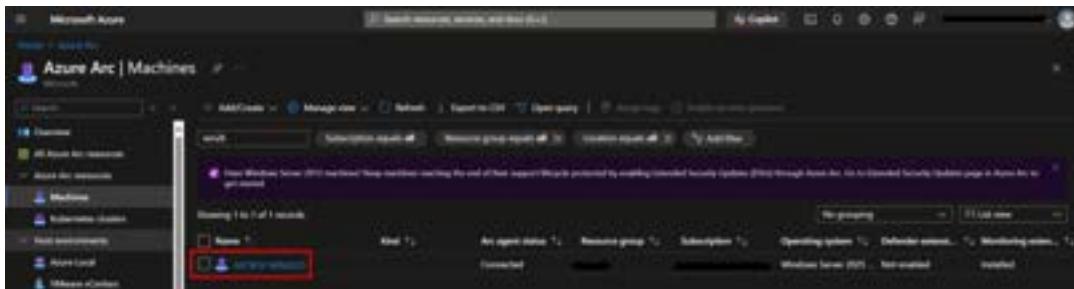
#### Task 1: Pre-requisites

##### Pre-requisite 1: Azure permissions

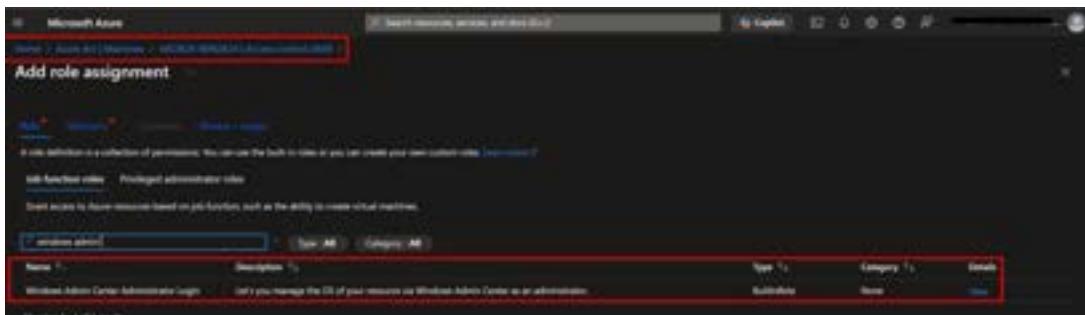
1. [] To install the Windows Admin Center extension for an Arc-enabled server resource, your account must be granted the Owner, Contributor, or Windows Admin Center Administrator Login role in Azure. **Check with your subscription administrator to verify that you have the required roles.**
2. [] Connecting to Windows Admin Center requires you to have Reader and Windows Admin Center Administrator Login permissions at the Arc-enabled server resource. The following steps helps you to set these up.
3. [] Enter "Machines - Azure Arc" in the top search bar in the Azure portal and select it from the displayed services.



4. [] Click on *ArcBox-Win2K25* Arc-enabled Windows server.



5. [] From the selected Windows machine click "Access control (IAM)" then add the role "Admin Center Administrator Login" to your access (use the lab user identity as in the *Resources* tab in the labs environment).



6. [] Follow similar steps to assign yourself Reader permissions at the Arc-enabled server resource.

#### Pre-requisite 2: Set Windows Server Licensing

1. [] To be able to install the Windows Admin Center extension for an Arc-enabled server resource, you must set the "Windows Server" licensing to either PAYGO (Pay as you go) or attest that you have SA (Software Assurance). In this case we will use the Software Assurance attestation.



[!Important] **Important note about Licensing:** The Azure Arc-enabled server must be officially licensed through a valid licensing channel. Unlicensed servers aren't eligible for benefits such as Windows Admin Center. [Refer to this document for further information](#)

### Task 1 has been completed

Click **Next** for the next task or [Go back to the main table of content](#)

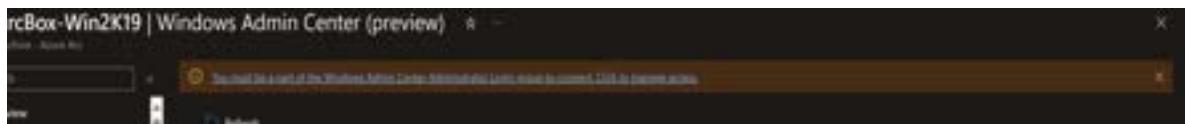
====

### Task 2: Deploy the Windows Admin Center VM extension

1. [] Open the Azure portal and navigate to the *ArcBox-Win2K25* machine.
2. [] Under the Settings group, select Windows Admin Center, then click "Set up".
3. [] Specify the port on which you wish to install Windows Admin Center, and then select Install.



4. [] If you get the following message after the installation is complete then you need to go back to the previous step and set up the permissions as explained in Pre-requisite.



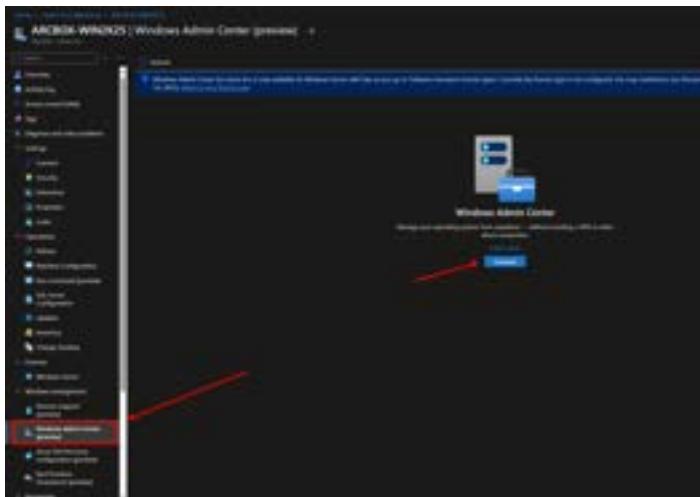
## Task 2 has been completed

Click **Next** for the next task or [Go back to the main table of content](#)

====

## Task 3: Connect and explore Windows Admin Center (preview)

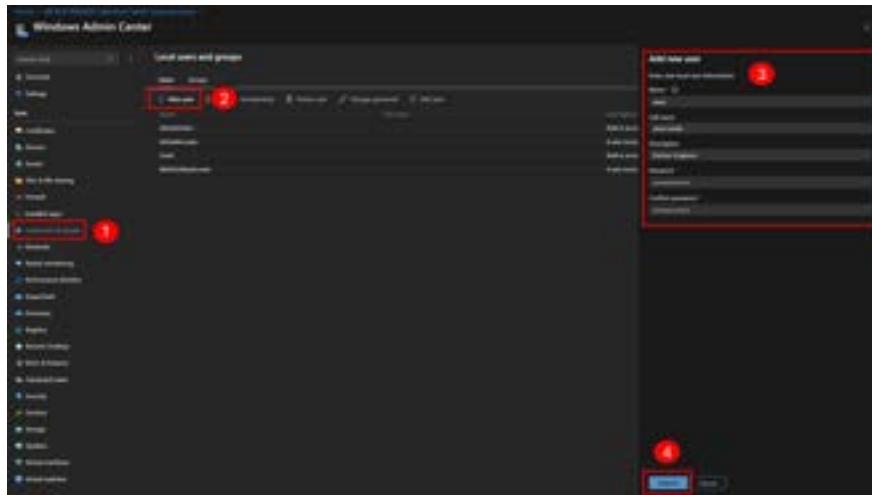
1. [] Once the installation is complete then you can connect to the Windows Admin Center.



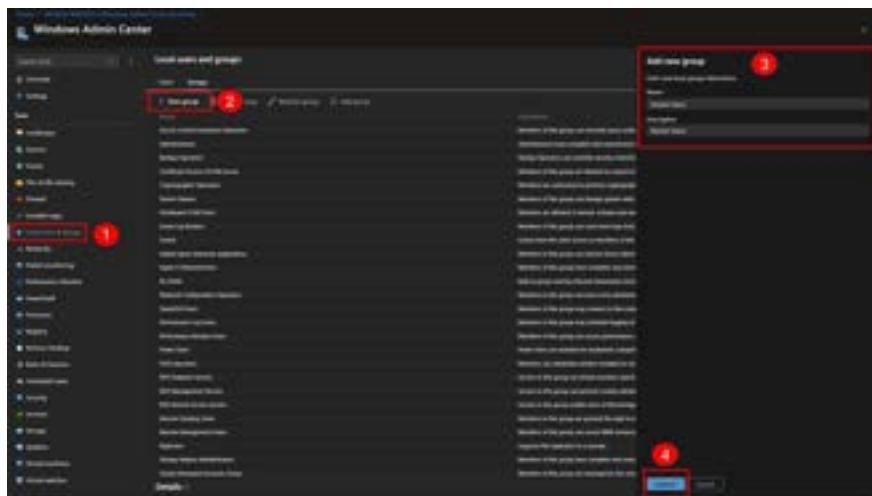
2. [] Start exploring the capabilities offered by the Windows Admin Center to manage your Arc-enabled Windows machine.



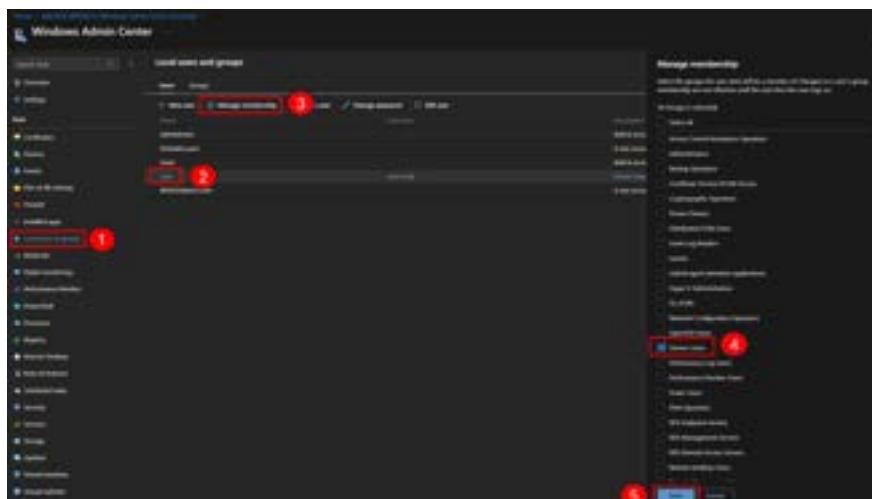
3. [] Let us use the Windows Admin Center to add a local user, a new group and assign the new user to the new group. From the left menu select "Local users & groups". Then from the "Users" tab click "New user". Enter the user details and click on "Submit". Verify that the user has been added.



4. [] Now select the "Groups" tab and click on "New Group". Enter the group details and click on "Submit". Verify that the group has been added.



5. [] Back to the "Users" tab, select the new user you have added, then click "Manage membership". Add the selected user to the new group and save.



**Task 3 has been completed**

**Congratulations, you have completed all tasks in this lab**

Click **Next** for the next lab or [\*\*Go back to the main table of content\*\*](#)

# LAB10: Query and inventory your Azure Arc-enabled servers using Azure Resource Graph

---

## Student Lab Manual

### Table of Contents

Exercise 1 - Use Resource Graph Queries in the Azure Portal and in Powershell to examine your Arc-enabled servers

**[Task 1 - Apply resource tags to Azure Arc-enabled servers](#)**

**[Task 2 - The Azure Resource Graph Explorer](#)**

**[Task 3 - Run a query to show all Azure Arc-enabled servers in your subscription](#)**

**[Task 4 - Query your server inventory using the available metadata](#)**

**[Task 5 - Use the resource tags in your Graph Query](#)**

**[Task 6 - List the extensions installed on the Azure Arc-enabled servers](#)**

**[Task 7 - Query other properties](#)**

# Exercise 1 - Use Resource Graph Queries in the Azure Portal and in Powershell to examine your Arc-enabled servers

---

## **Objective**

In this exercise, you will learn how to use the Azure Resource queries both in the Azure Graph Explorer and Powershell to demonstrate inventory management of your Azure Arc connected servers. Note that the results you get by running the graph queries in this module might be different from the sample screenshots as your environment might be different e.g. as a result of working with the other labs.

## **Estimated Time to Complete This Lab**

30 minutes

## **Explanation**

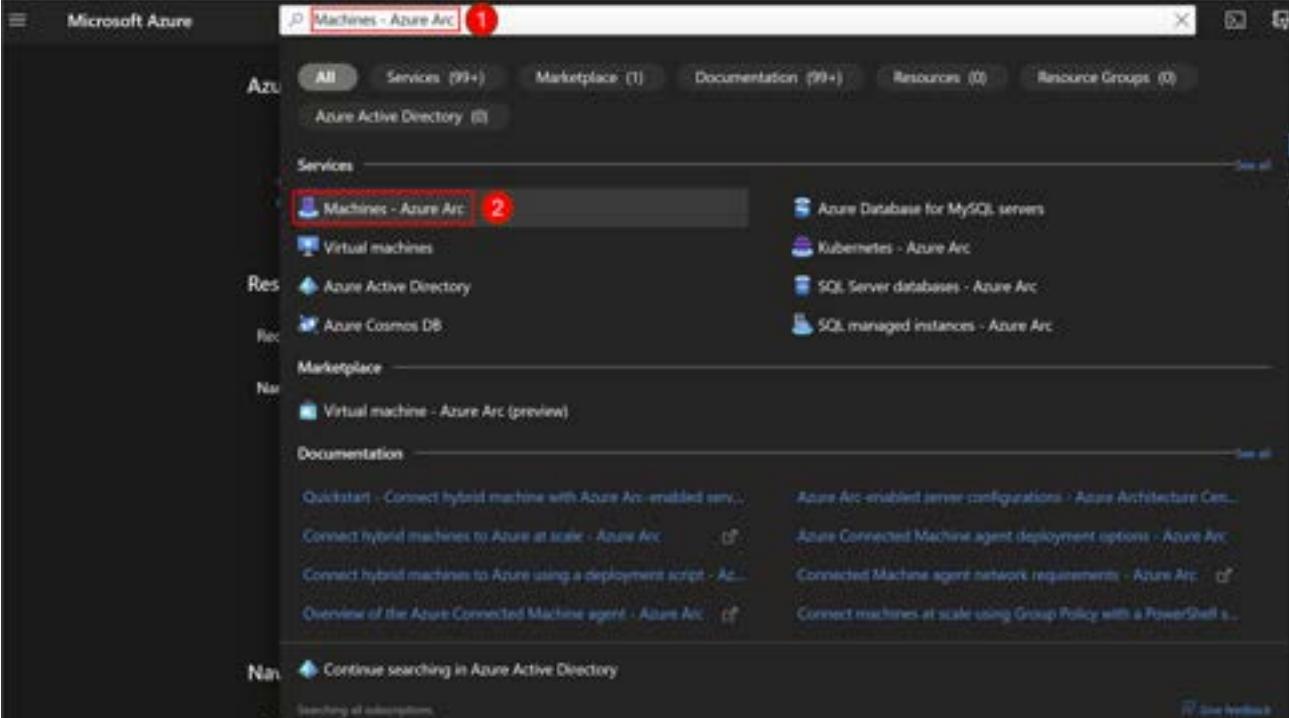
Azure Resource Graph is an extremely powerful extension to Azure Resource Management that provides efficient resource exploration at scale. It also provides the ability to do complex filtering and grouping. It can do this because it uses a subset of the Kusto Query Language (KQL).

There are a number of tables you can query in Azure Resource Graph. The most common table is the "resources" table. This is where all resources in your Azure subscriptions will live. With few exceptions everything in Azure is a resource. Queries can be run against the Azure Resource Graph API, with PowerShell, or in the Azure portal.

## Task 1: Apply resource tags to Azure Arc-enabled servers

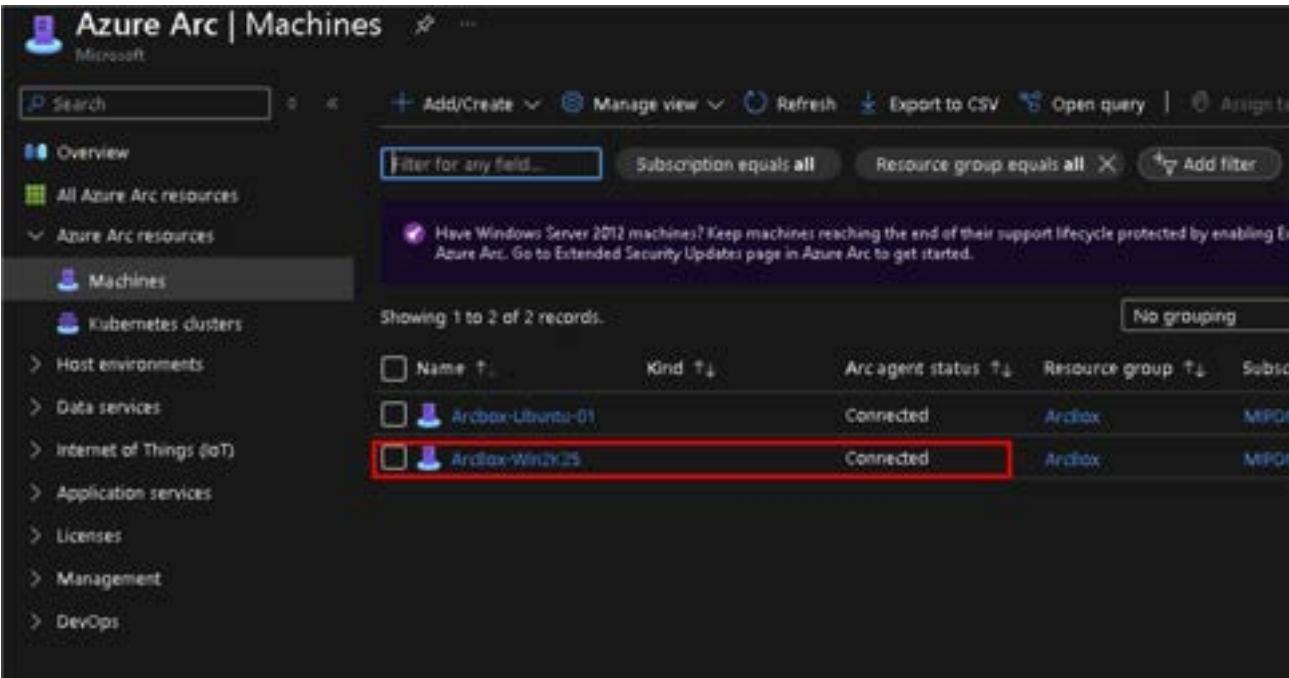
In this first step, you will assign Azure resource tags to some of your Azure Arc-enabled servers. This gives you the ability to easily organize and manage server inventory.

- 1. Enter "Machines - Azure Arc" in the top search bar in the Azure portal and select it from the displayed services.



The screenshot shows the Microsoft Azure portal's search interface. The search bar at the top contains the text "Machines - Azure Arc". A red circle with the number "1" is positioned above the search bar. Below the search bar, the "All" tab is selected. The search results list several services under the "Services" category, including "Machines - Azure Arc" (which is highlighted with a red circle containing "2"), "Virtual machines", "Azure Active Directory", "Azure Cosmos DB", and "Virtual machine - Azure Arc (preview)". To the right of these, there are additional service options: "Azure Database for MySQL servers", "Kubernetes - Azure Arc", "SQL Server databases - Azure Arc", and "SQL managed instances - Azure Arc". Below the service list, there are sections for "Documentation" and "Marketplace". At the bottom of the search results, there is a "Continue searching in Azure Active Directory" link and a "View feedback" button.

- 2. Click on any of your Azure Arc-enabled servers.



The screenshot shows the "Azure Arc | Machines" blade in the Azure portal. The left sidebar has a tree view with "Overview", "All Azure Arc resources", "Azure Arc resources" (expanded), "Machines" (selected and highlighted with a red box), "Kubernetes clusters", and several collapsed categories like "Host environments", "Data services", etc. The main area has a heading "Showing 1 to 2 of 2 records." and a table with two rows. The columns are "Name" (with a sorting arrow), "Kind" (with a sorting arrow), "Arc agent status" (with a sorting arrow), "Resource group" (with a sorting arrow), and "Subscription" (with a sorting arrow). The first row is for "Arcbox-Ubuntu-01" and the second row is for "Arcbox-Win2k25" (also highlighted with a red box). There are filter buttons at the top of the table: "Filter for any field...", "Subscription equals all", "Resource group equals all", and "Add filter". A note at the top right says: "Have Windows Server 2012 machines? Keep machines reaching the end of their support lifecycle protected by enabling Extended Security Updates. Go to Extended Security Updates page in Azure Arc to get started." A "No grouping" button is also visible at the top right of the table.

3. Click on "Tags". Add a new tag with Name="Scenario" and Value="azure\_arc\_servers\_inventory". Click Apply when ready.

The screenshot shows the 'Tags' blade for the machine 'ArcBox-Win2K25'. On the left, a sidebar lists various management options like Overview, Activity log, Access control (IAM), and Tags. The 'Tags' option is selected and highlighted with a red box. The main area displays a table of existing tags. A new tag is being added with the name 'Scenario' and the value 'azure\_arc\_servers\_inventory'. This row is also highlighted with a red box. At the bottom of the table, there is a button labeled 'Apply' which is also highlighted with a red box. To the right of the table, there is a note about activating Windows.

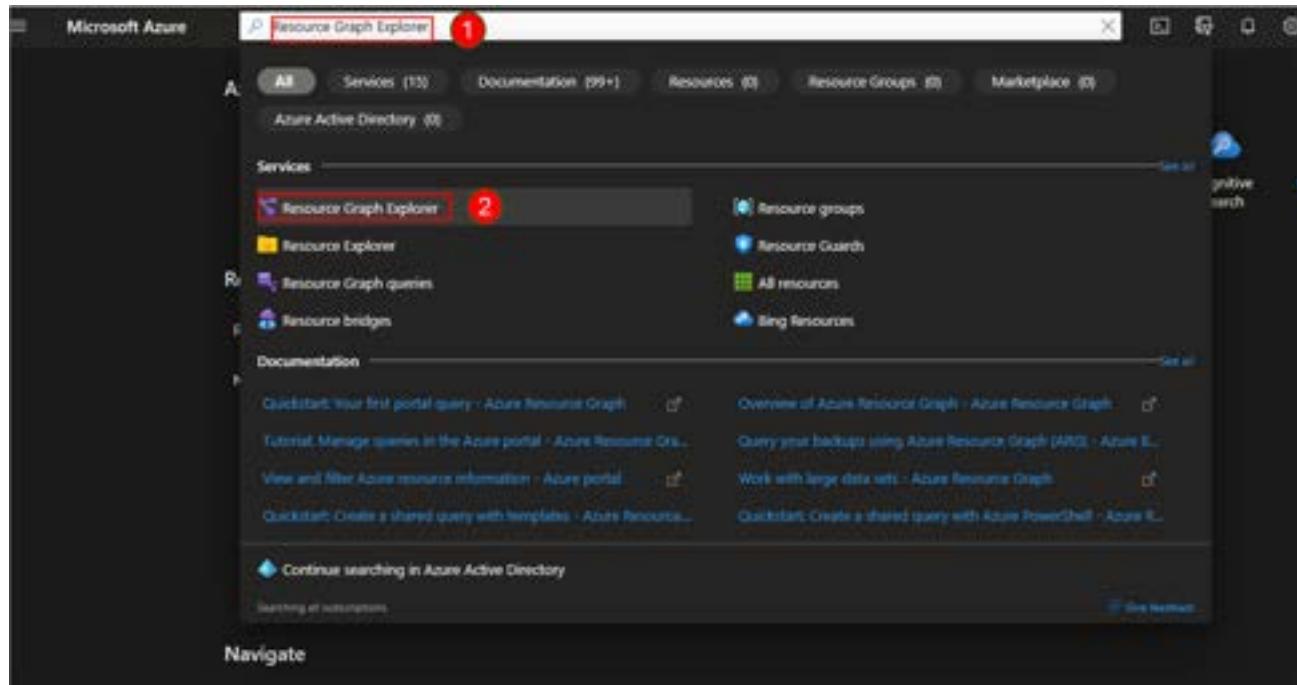
4. Repeat the same process in other Azure Arc-enabled servers if you wish. This new tag will be used later when working with Resource Graph Explorer queries.

### Task 1 has been completed

Click **Next** for the next task or [Go back to the main table of content](#)

## Task 2: The Azure Resource Graph Explorer

- 1. Now we will explore our hybrid server inventory using a number of Azure Graph Queries. Enter "Resource Graph Explorer" in the top search bar in the Azure portal and select it.



- 2. The scope of the Resource Graph Explorer can be set as seen below

The screenshot shows the Azure Resource Graph Explorer interface. At the top, there is a search bar with the text "Search resources, services, and docs (0+)" and a feedback button. Below the search bar is a toolbar with buttons for "New query", "Open a query", "Set authorization scope", and "Run query", along with save and cancel buttons. On the left, there is a sidebar titled "Scope" with a "Category" dropdown set to "Subscription". A red box highlights the "Subscription" dropdown and the "Subscription" item in the list. The main pane shows a "Query 1" card with a "Results" tab. At the bottom, there are three example queries: "Count Azure resources", "Count key vault resources", and "List resources sorted by name".

**Task 2 has been completed**

Click **Next** for the next task or [Go back to the main table of content](#)

## Task 3: Run a query to show all Azure Arc-enabled servers in your subscription

- 1. In the query window, enter and run the following query and examine the results which should show your Arc-enabled servers. Note the use of the KQL equals operator (= $\sim$ ) which is case insensitive [KQL =~ \(equals\) operator](#).

```
shell
```

```
▶ Resources  
| where type =~ 'Microsoft.HybridCompute/machines'
```

The screenshot shows the Azure Resource Graph Explorer interface. On the left, there's a sidebar with categories like General, AI + machine learning, Analytics, Compute, Containers, Database, DevOps, Hybrid + multicloud, Identity, Integration, Internet of Things, Management and governance, and Migration. The main area has tabs for 'Query', 'Results', 'Charts', and 'Messages'. The 'Query' tab contains the KQL query: 'Resources | where type =~ "Microsoft.HybridCompute/machines"'. The 'Results' tab displays a table with two rows of data. The columns are: Name, Type, tenantid, kind, location, resource group, subscription, managedby, and sku. The data is as follows:

Name	Type	tenantid	kind	location	resource group	subscription	managedby	sku
anotherUbuntu01	Machine - Azure Arc	42e01212-074e-44f6-8...	Linux	can-south	abcde	MYRG-testRG002	null	Standard
anotherWin01	Machine - Azure Arc	42e01212-074e-44f6-8...	Windows	can-south	abcde	MYRG-testRG002	null	Standard

- 2. Scroll to the right on the results pane and click "See Details" to see all the Azure Arc-enabled server metadata. Note for example the list of detected properties, we will be using these in the next task.
- 3. You can also run the same query using PowerShell (e.g. using Azure Cloud Shell) providing that you have added the required module "Az.ResourceGraph" as explained in [Run your first Resource Graph query using Azure PowerShell](#).

To install the PowerShell module, run the following command

```
powershell
```

```
▶ Install-Module -Name Az.ResourceGraph
```

Then run the query in PowerShell

```
powershell
```

```
▶ Search-AzGraph -Query "Resources | where type =~ 'Microsoft.HybridCompute/machi
```

**Task 3 has been completed**

Click **Next** for the next task or [Go back to the main table of content](#)

## Task 4: Query your server inventory using the available metadata

- 1. Use PowerShell and/or the Resource Graph Explorer to summarize the server count by "logical cores" which is one of the detected properties referred to in the previous task.

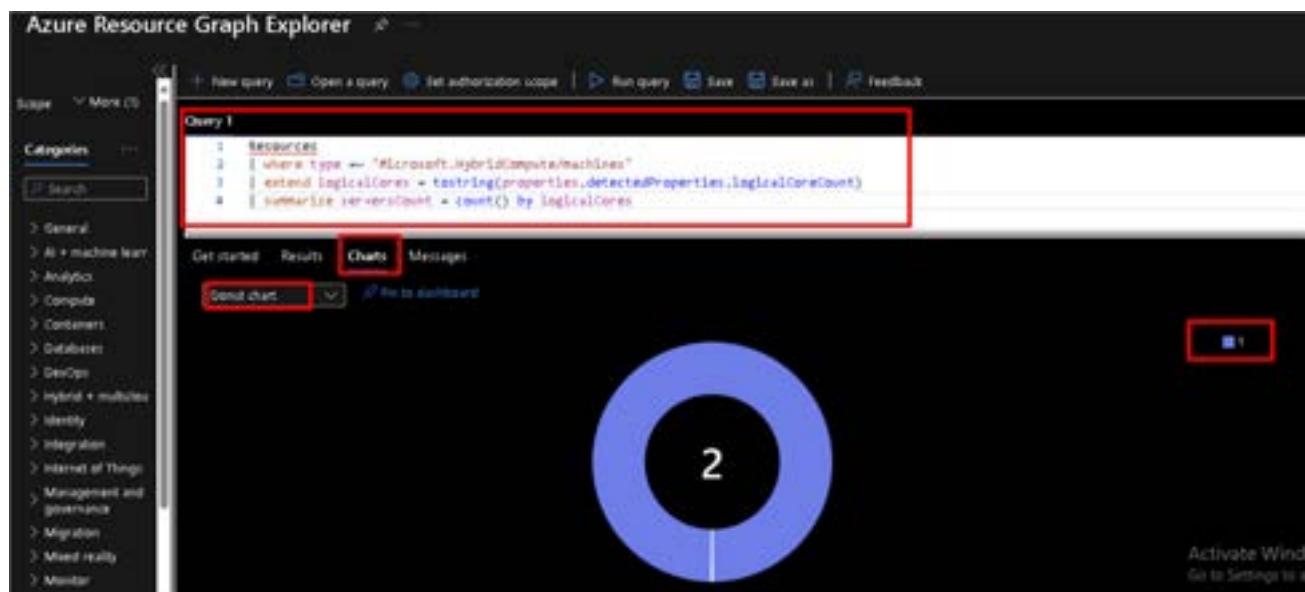
Using the Portal:

```
portal
▶ Resources
| where type =~ 'Microsoft.HybridCompute/machines'
| extend logicalCores = tostring(properties.detectedProperties.logicalCoreCount)
| summarize serversCount = count() by logicalCores
```

Using PowerShell:

```
powershell
▶ Search-AzGraph -Query "Resources
| where type =~ 'Microsoft.HybridCompute/machines'
| extend logicalCores = tostring(properties.detectedProperties.logicalCoreCount)
| summarize serversCount = count() by logicalCores"
```

- 2. The Graph Explorer allows you to get a graphical view of your results by selecting the "charts" option.



**Task 4 has been completed**

Click **Next** for the next task or [Go back to the main table of content](#)

## Task 5: Use the resource tags in your Graph Query

---

- 1. Let's now build a query that uses the tag we assigned earlier to some of our Azure Arc-enabled servers. Use the following query that includes a check for resources that have a value for the "Scenario" tag. Feel free to use the portal or PowerShell. Check that the results match the servers that you set tags for earlier.

Using the Portal:

```
portal
▶ Resources
| where type =~ 'Microsoft.HybridCompute/machines' and isnotempty(tags['Scenario']
| extend Scenario = tags['Scenario']
| project name, tags
```

Using PowerShell:

```
powershell
▶ Search-AzGraph -Query "Resources
| where type =~ 'Microsoft.HybridCompute/machines' and isnotempty(tags['Scenario']
| extend Scenario = tags['Scenario']
| project name, tags"
```

### Task 5 has been completed

Click **Next** for the next task or [Go back to the main table of content](#)

## Task 6: List the extensions installed on the Azure Arc-enabled servers

---

- 1. Run the following advanced query which allows you to see what extensions are installed on the Arc-enabled servers. Notice that running the query in PowerShell requires us to escape the \$ character as explained in [Escape Characters](#).

Using the Portal:

```
portal
▶ Resources
| where type == 'microsoft.hybridcompute/machines'
| project id, JoinID = toupper(id), ComputerName = tostring(properties.osProfile
| join kind=leftouter(
    Resources
        | where type == 'microsoft.hybridcompute/machines/extensions'
        | project MachineId = toupper(substring(id, 0, indexof(id, '/extensions'))),
) on $left.JoinID == $right.MachineId
| summarize Extensions = make_list(ExtensionName) by id, ComputerName, OSName
| order by tolower(OSName) desc
```

Using PowerShell:

```
powershell
▶ Search-AzGraph -Query "Resources
| where type == 'microsoft.hybridcompute/machines'
| project id, JoinID = toupper(id), ComputerName = tostring(properties.osProfile
| join kind=leftouter(
    Resources
        | where type == 'microsoft.hybridcompute/machines/extensions'
        | project MachineId = toupper(substring(id, 0, indexof(id, '/extensions'))),
) on `\$left.JoinID == `\$right.MachineId
| summarize Extensions = make_list(ExtensionName) by id, ComputerName, OSName
| order by tolower(OSName) desc"
```

- 2. If you have used the portal to run the query then you should see results similar to those shown in the screenshot below.

+ New query Open a query Set authentication scope Run query Save Save as Feedback

Query 1

```
1 resources
2 | where type == "microsoft.hybridcompute/machines"
3 | project id, displayName = toUpper(id), ComputerName = toString(properties.osProfile.computerName), OSName = toString(properties.osName)
4 | join $left=leftOuter(
5     resources
6     | where type == "microsoft.hybridcompute/machines/extensions"
7     | project machineId = toUpper(substring(id, 0, indexof(id, "/extensions"))), ExtensionName = name
8   ) on $left.machineId == right.machineId
9 | summarize Extensions = make_list(ExtensionName) by id, ComputerName, OSName
10 | order by displayName asc
```

Get started Results Charts Messages

Download formatted results as CSV [Print to dashboard](#)

Formatted results  On

Name	ComputerName	OSName	Extensions
Andes-Win2025	Andes-Win2025	Windows	[{"ChangeTracking": "Windows", "WindowsOsUpdateExtension": "AzureMonitor"}, {"ChangeTracking": "Linux", "AzureMonitorLogAgent": "LinuxOsUpdateExtensi..."}]
Andes-Ubuntu-01	andres-ubuntu-01	Linux	[{"ChangeTracking": "Linux", "AzureMonitorLogAgent": "LinuxOsUpdateExtensi..."}]

**Task 6 has been completed**

Click **Next** for the next task or [Go back to the main table of content](#)

## Task 7: Query other properties

- 1. Azure Arc provides additional properties on the Azure Arc-enabled server resource that we can query with Resource Graph Explorer. In the following example, we list some of these key properties, like the Azure Arc Agent version installed on your Azure Arc-enabled servers

Using the Portal

```
portal
▶ Resources
| where type =~ 'Microsoft.HybridCompute/machines'
| extend arcAgentVersion = tostring(properties.[agentVersion]), osName = tostring(properties.[osName])
| extend osVersion = tostring(properties.[osVersion]), osSku = tostring(properties.[osSku])
| extend lastStatusChange = tostring(properties.[lastStatusChange])
| project name, arcAgentVersion, osName, osVersion, osSku, lastStatusChange
```

Using PowerShell

```
powershell
▶ Search-AzGraph -Query "Resources
| where type =~ 'Microsoft.HybridCompute/machines'
| extend arcAgentVersion = tostring(properties.[agentVersion]), osName = tostring(properties.[osName])
| extend osVersion = tostring(properties.[osVersion]), osSku = tostring(properties.[osSku])
| extend lastStatusChange = tostring(properties.[lastStatusChange])
| project name, arcAgentVersion, osName, osVersion, osSku, lastStatusChange"
```

- 2. Running the query in the portal should result in something like the following

The screenshot shows the Azure Resource Graph Explorer interface. On the left, there's a sidebar with 'Categories' and 'Tags' sections. The main area has a 'Query' tab open with the following query text:

```
Resources
| where type =~ 'Microsoft.HybridCompute/machines'
| extend arcAgentVersion = tostring(properties.[agentVersion]), osName = tostring(properties.[osName])
| extend osVersion = tostring(properties.[osVersion]), osSku = tostring(properties.[osSku])
| extend lastStatusChange = tostring(properties.[lastStatusChange])
| project name, arcAgentVersion, osName, osVersion, osSku, lastStatusChange
```

Below the query, there are tabs for 'Get started', 'Results', 'Charts', and 'Messages'. The 'Results' tab is selected, showing a table with the following data:

name	arcAgentVersion	osName	osVersion	osSku	lastStatusChange
Archer-V01-0X29	1.49.02952.1090	windows	10.0.29100.2908	Windows Server 2022 Datacenter	2023-05-24T12:00:12.000Z
Archer-Ubuntu-01	1.49.02952.1092	linux	5.10.0-119-generic	Ubuntu 22.04.4 LTS	2023-05-24T19:03:23.474Z

A red box highlights the entire table. At the bottom right of the table, there's a 'Formatted results' toggle switch that is turned on.

**Task 7 has been completed**

**Congratulations, you have completed all tasks in this lab**

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB11: Additional automation capabilities for your Azure Arc-enabled servers

---

## Student Lab Manual

### Table of Contents

Exercise 1 - Run automation runbooks on your Azure Arc-enabled servers using Hybrid runbook workers

**[Task 1 - Create Automation account using the Azure Portal](#)**

**[Task 2 - Create Automation account using Powershell](#)**

**[Task 3 - Add Hybrid Runbook Workers using the Azure Portal](#)**

**[Task 4 - Add Hybrid Runbook Workers using Powershell](#)**

**[Task 5 - Create and start a runbook](#)**

Exercise 2 - Securely Connect to your Azure Arc-enabled servers using SSH access

**[Task 1 - Install prerequisites on client machine](#)**

**[Task 2 - Enable SSH service on Arc-enabled servers](#)**

**[Task 3 - Connect to Arc-enabled servers](#)**

**[Task 4 - Optional: Azure AD/Entra ID based SSH Login](#)**

Exercise 3 - Run PowerShell and Shell scripts on Azure Arc-enabled servers using the Run command

**[Task 1 - Check the pre-requisites](#)**

**[Task 2 - Use the Run command to execute a simple PowerShell script within an Arc-connected Windows machine](#)**

**[Task 3 - Use the Run command to execute a simple Shell command within an Arc-connected Linux machine](#)**

**[Task 4 - Direct the output of a Run command to Azure storage blob](#)**

## **Exercise 1 - Run automation runbooks on your Azure Arc-enabled servers using Hybrid runbook workers**

---

### **Objective**

Onboard Azure Arc-enabled servers as Hybrid runbook workers in Azure Automation.

### **Estimated Time to Complete This Lab**

20 minutes

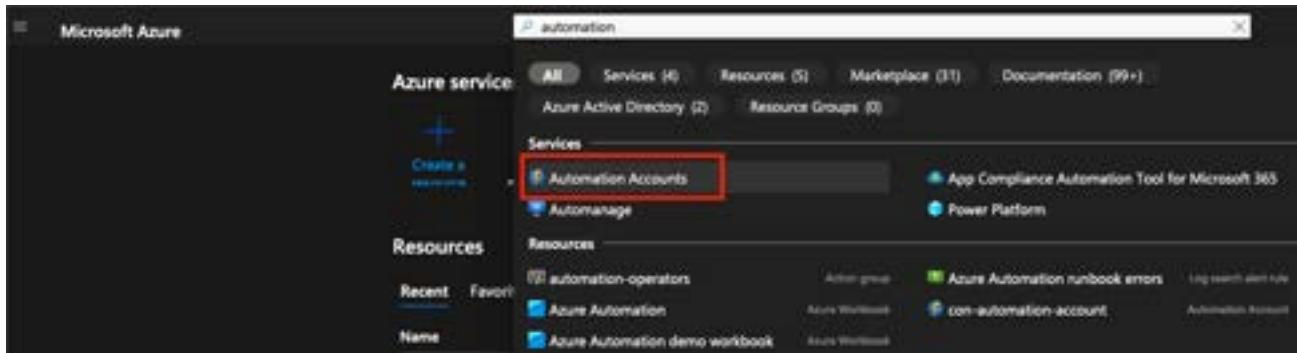
### **Explanation**

In this module we will onboard Azure Arc-enabled servers as Hybrid runbook workers in Azure Automation. We will then create and start runbooks on the hybrid runbook workers to see how this feature can be leveraged.

## Task 1: Create Automation account using the Azure Portal

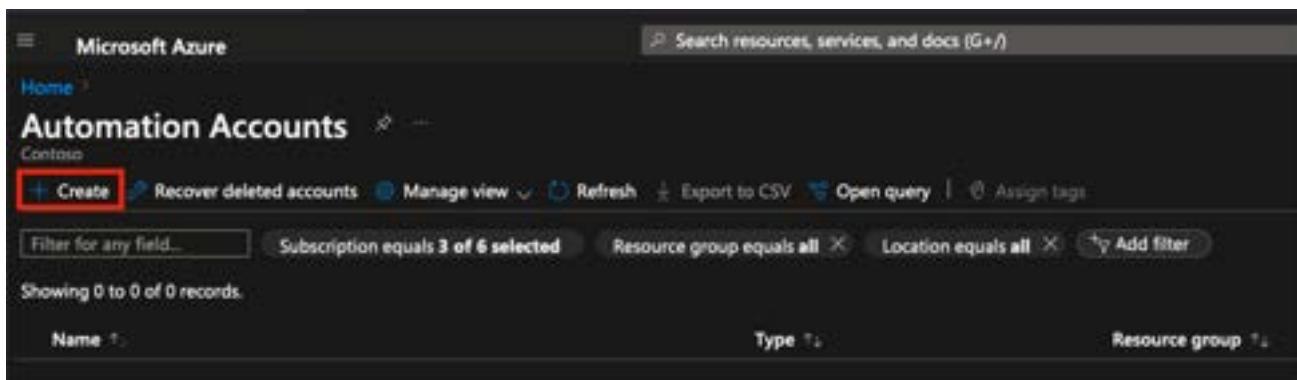
- You have two options to create an Automation account. You can either follow the steps in this task to use the Azure Portal, or if you prefer to use Powershell then jump to [Task 2](#) and continue from there.

- 1. In the Azure Portal, search for *automation* and navigate to *Automation accounts*



The screenshot shows the Microsoft Azure search interface. A search bar at the top contains the text "automation". Below the search bar, a navigation bar has tabs for "All", "Services (4)", "Resources (5)", "Marketplace (31)", and "Documentation (99+)". Under the "Services" tab, a list of services is shown, with "Automation Accounts" highlighted by a red box. Other listed services include "App Compliance Automation Tool for Microsoft 365" and "Power Platform". Below the service list, there are sections for "Recent" and "Favori" resources, and a "Name" filter dropdown.

- 2. Click on "Create"



The screenshot shows the "Automation Accounts" blade in the Azure portal. At the top, there's a header with "Home > Automation Accounts". Below the header, there's a toolbar with buttons for "Create", "Recover deleted accounts", "Manage view", "Refresh", "Export to CSV", "Open query", and "Assign tags". There are also filter options for "Subscription", "Resource group", and "Location". The main area displays a message "Showing 0 to 0 of 0 records." Below this, there are columns for "Name", "Type", and "Resource group".

- 3. Select the subscription and resource group where you have deployed ArcBox.
- 4. Enter *ArcBox-Automation* as the name for the Automation Account.
- 5. Select the same region as your ArcBox environment is deployed to.
- 6. Click Next

Microsoft Azure Search resources, services, and docs (G+/)

Home > Automation Accounts > Create an Automation Account

Basics Advanced Networking Tags Review + Create

Create an Automation Account to hold the Automation runbooks & configuration used for automating operations and management tasks around Azure and non-Azure resources. You could execute cloud jobs in a serverless environment or use hybrid jobs on your compute via Azure Virtual machines, Arc-enabled servers or Arc-enabled VMWare VM (preview). [Learn more](#)

Subscription: [dropdown] Resource group: \* [dropdown]  
Select a resource group [Create new](#)

Instance Details  
Automation account name:  Enter name  
Region: East US

7. Leave the default settings for *Managed Identities* in place and click Next

Microsoft Azure Search resources, services, and docs (G+/)

Home > Automation Accounts > Create an Automation Account

Basics Advanced Networking Tags Review + Create

Managed Identities

Use Managed Identities as the recommended method for authenticating with Azure resources from the runbooks. Managed identity would be more secure than Runas account since it doesn't require any credentials to be stored. [Learn more](#)

System assigned   
User assigned

8. Leave the default settings for *Connectivity configuration* in place and click Next

Microsoft Azure

Home > Automation Accounts >

## Create an Automation Account

Basics Advanced Networking **Networking** Tags Review + Create

### Network connectivity

You can connect to your automation account either through public IP addresses for public access or through a private endpoint for private access. [Learn more](#)

Connectivity configuration  Public access  Private access

**Tip:** When you select public access, traffic from all public networks can access this Automation account resource. Select private access if you want to restrict access to automation endpoints only from authorized virtual networks required for secure applications or environments.

- 9. Optionally, add any tags you may want to add to the resource. Click Next

Microsoft Azure

Home > Automation Accounts >

## Create an Automation Account

Basics Advanced Networking **Tags** Review + Create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

**Tip:** Note: Automation accounts are limited to 15 tags.

Name	:	Value
	:	

- 10. Click Create

Home &gt; Automation Accounts &gt;

## Create an Automation Account

Validation passed

Basics Advanced Networking Tags Review + Create

### Basics

Name	ArcBox-Automation
Subscription	Demo
Resource group	arcbox-demo-rg
Region	East US

### Advanced

System assigned identity	Yes
User assigned identity	None

### Networking

Network connectivity	Public access
----------------------	---------------

### Tags

(none)

Create

Previous

Next

**Task 1 has been completed**

Click **Next** for the next task or [go back to the main table of content](#)

## Task 2: Create Automation account using Powershell

---

This task is an alternative to, and only needed if you have not executed [task 1](#). You can jump straight to [task 3](#) if you have already provisioned an Automation account using the Azure portal.

- 1. From the *ArcBox-Client* machine start PowerShell 7.
- 2. Customize the parameter values in the following Powershell script to reflect your environment for the resource group name and location. Paste the code in the PowerShell window and press Enter.

```
powershell
▶ New-AzAutomationAccount -Location "<Your chosen Location>" -Name "ArcBox-A
```

The output should look similar to this:

```
New-AzAutomationAccount @AutomationAccountParams

SubscriptionId      : [REDACTED]
ResourceGroupName   : jan-arcbox-01-rg
AutomationAccountName : ArcBox-Automation
Location           : East US
State               : Ok
Plan                : Basic
CreationTime        : 9/6/2023 7:53:30 PM +00:00
LastModifiedTime    : 9/6/2023 7:53:30 PM +00:00
LastModifiedBy      :
Tags                : {[Project, jumpstart_arcbox]}
Identity            : Microsoft.Azure.Management.Automation.Models.Identity
Encryption          : Microsoft.Azure.Management.Automation.Models.EncryptionProperties
PublicNetworkAccess :
```

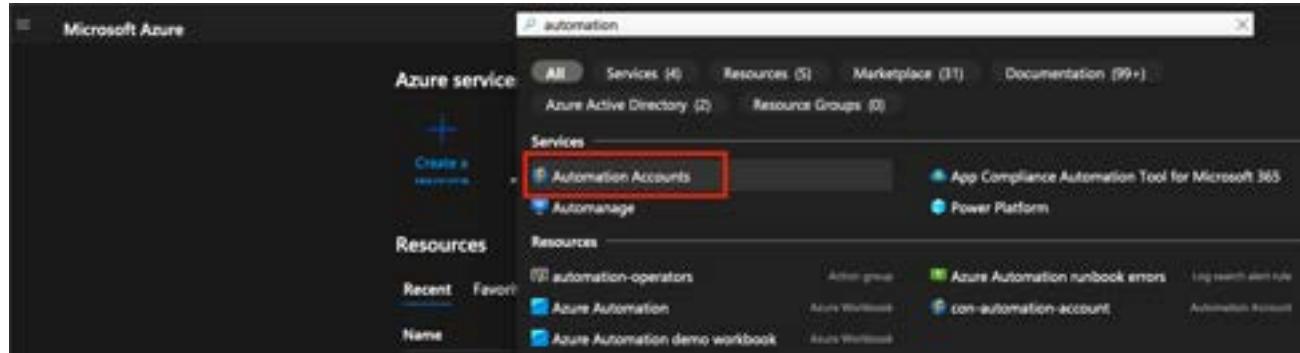
**Task 2 has been completed**

Click **Next** for the next task or [go back to the main table of content](#)

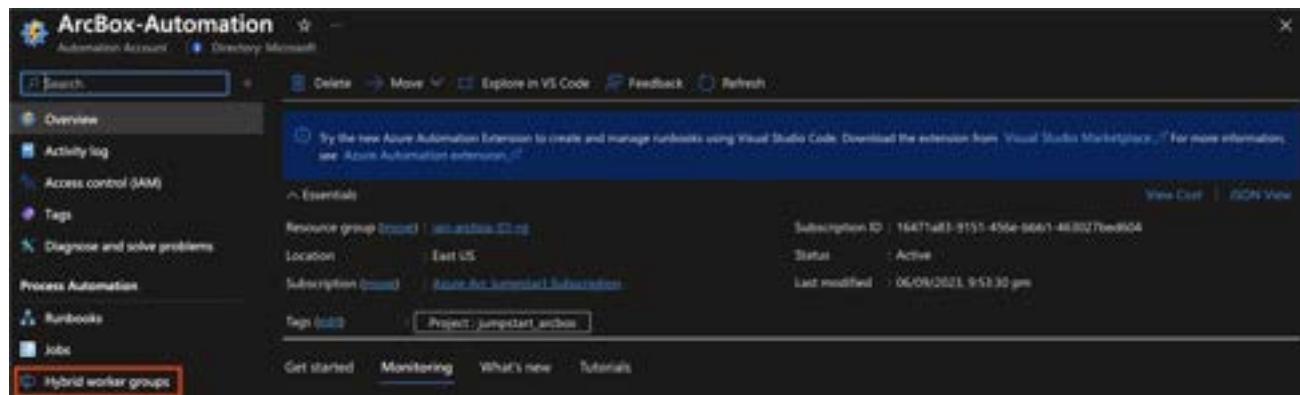
## Task 3 - Add Hybrid Runbook Workers using the Azure Portal

- You have two options to add hybrid runbook workers. You can either follow the steps in this task to use the Azure Portal, or if you prefer to use Powershell then jump to Task [task 4](#) and continue from there.

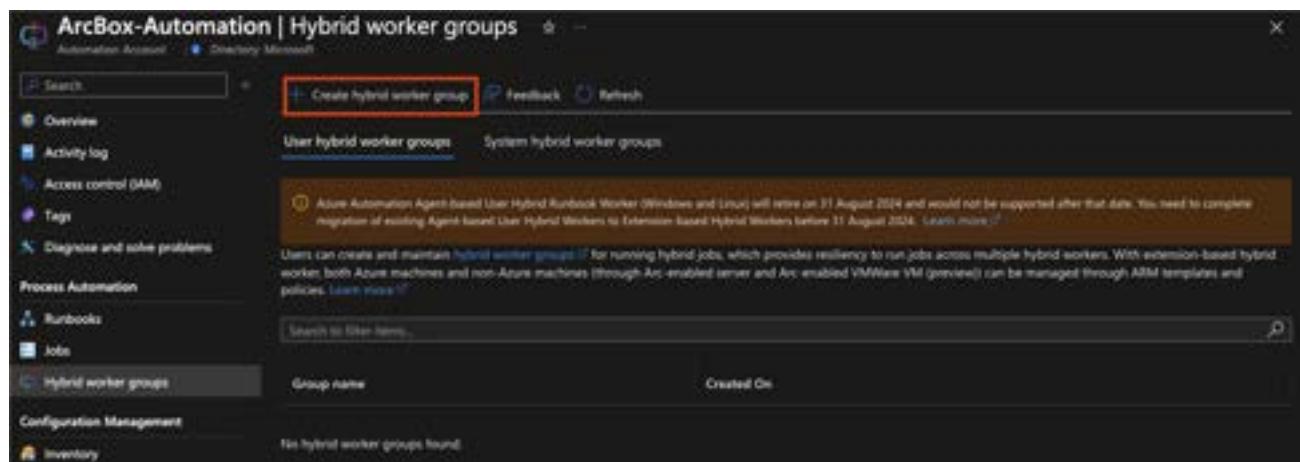
- 1. In the Azure Portal, search for *automation* and navigate to *Automation accounts*



- 2. Navigate to the ArcBox-Automation account you created previously
- 3. Select *Hybrid worker groups*:



- 4. Click *Create hybrid worker group*:



5. Type *windows-workers* as the name of the new Hybrid worker group, leave the default value for *Use Hybrid Worker Credentials* and click Next

The screenshot shows the 'Create Hybrid worker group' page in the Azure portal. The 'Basics' tab is selected. A red box highlights the 'Name' input field, which contains 'windows-workers'. Below it is a 'Use Hybrid Worker Credentials' section with 'Custom' and 'Default' options. The page also includes a brief description of hybrid workers and instructions to complete the Basics tab and then click 'Review + Create'.

6. Click *Add machines*:

The screenshot shows the 'Create Hybrid worker group' page with the 'Hybrid workers' tab selected. A red box highlights the '+ Add machines' button. Below it is a table header with columns: Machine Name, Subscription ID, Resource Group, Operating System, and Location. The table body shows a single row with 'No Machines Selected'.

7. Select *ArcBox-Win2K22* and click *Add*:

Add machines as hybrid worker

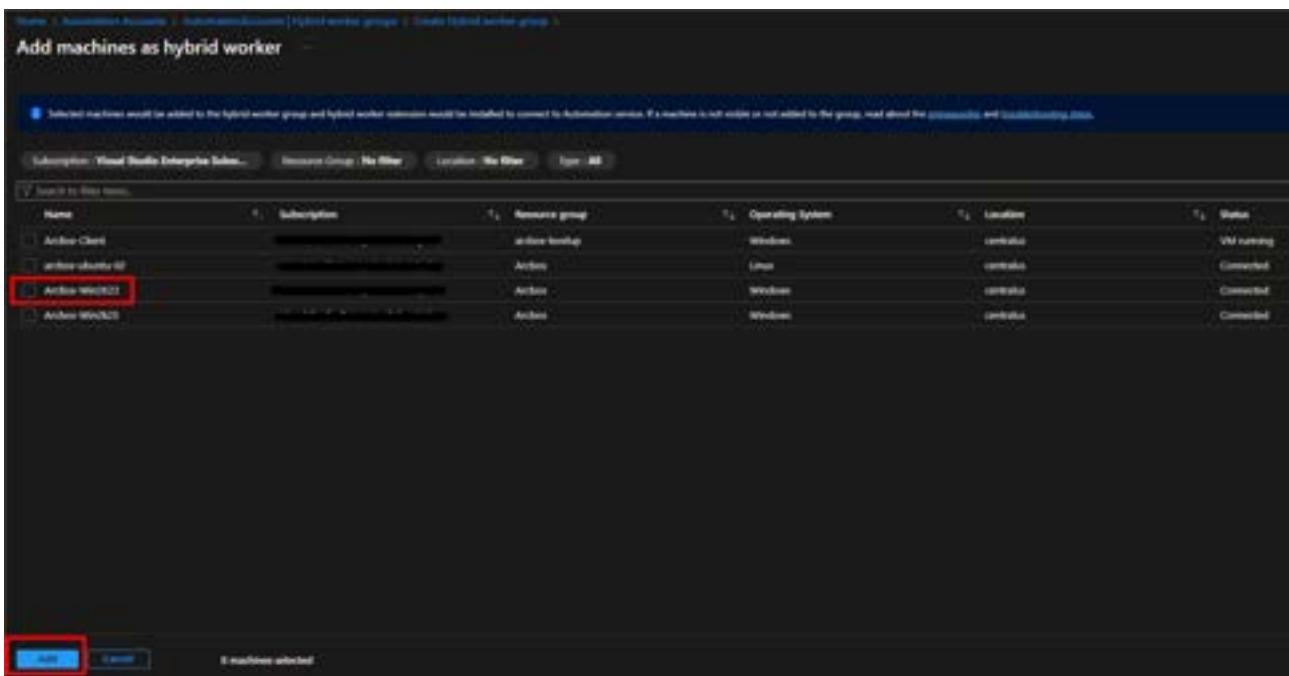
Selected machines would be added to the hybrid worker group and hybrid worker extension would be installed to connect to Automation service. If a machine is not visible or not added to the group, read about the [processes](#) and [troubleshooting steps](#).

Subscription: Visual Studio Enterprise Sub... Resource Group: No filter Location: No filter Export All

Search for more items.

Name	Subscription	Resource group	Operating System	Location	Status
ArcBox-Client	[REDACTED]	[REDACTED]	Windows	[REDACTED]	VM running
arcbox-ubuntu-01	[REDACTED]	[REDACTED]	Ubuntu	[REDACTED]	Connected
<b>ArcBox-WIN2022</b>	[REDACTED]	[REDACTED]	Windows	[REDACTED]	Connected
ArcBox-WIN2023	[REDACTED]	[REDACTED]	Windows	[REDACTED]	Connected

**Add machines** **Remove** 0 machines selected



- 8. Click *Review + Create*:

Create Hybrid worker group

Hybrid worker group

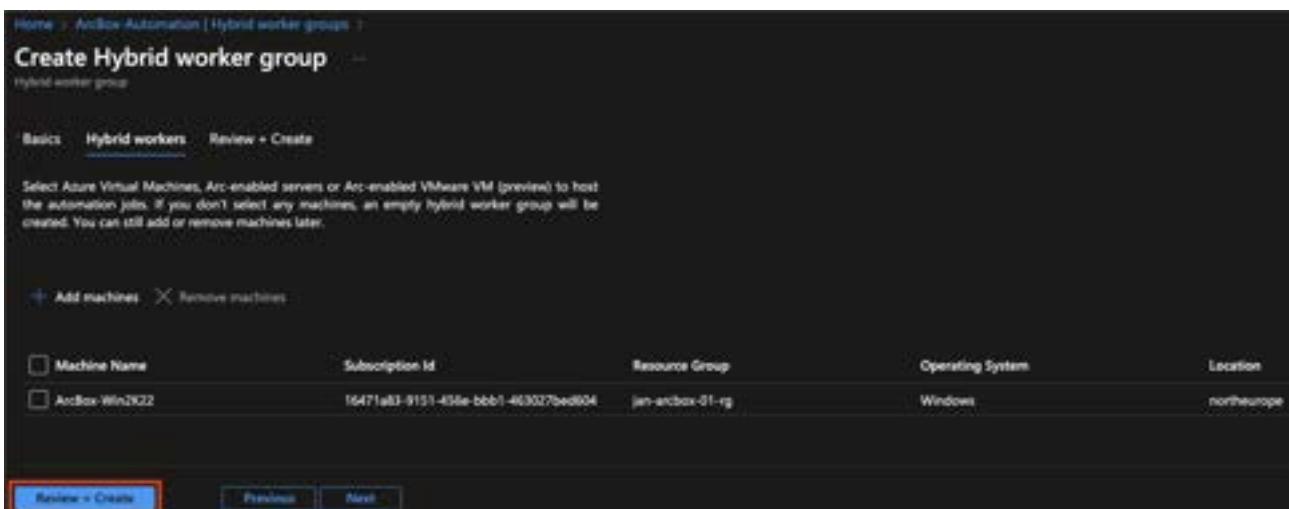
Basics Hybrid workers Review + Create

Select Azure Virtual Machines, Arc-enabled servers or Arc-enabled VMware VM (preview) to host the automation jobs. If you don't select any machines, an empty hybrid worker group will be created. You can still add or remove machines later.

+ Add machines X Remove machines

Machine Name	Subscription Id	Resource Group	Operating System	Location
ArcBox-WIN2022	16471a83-9151-456e-bbb1-463027bed004	[REDACTED]	Windows	northEurope

**Review + Create** Previous Next



- 9. Click *Create*:

Create Hybrid worker group

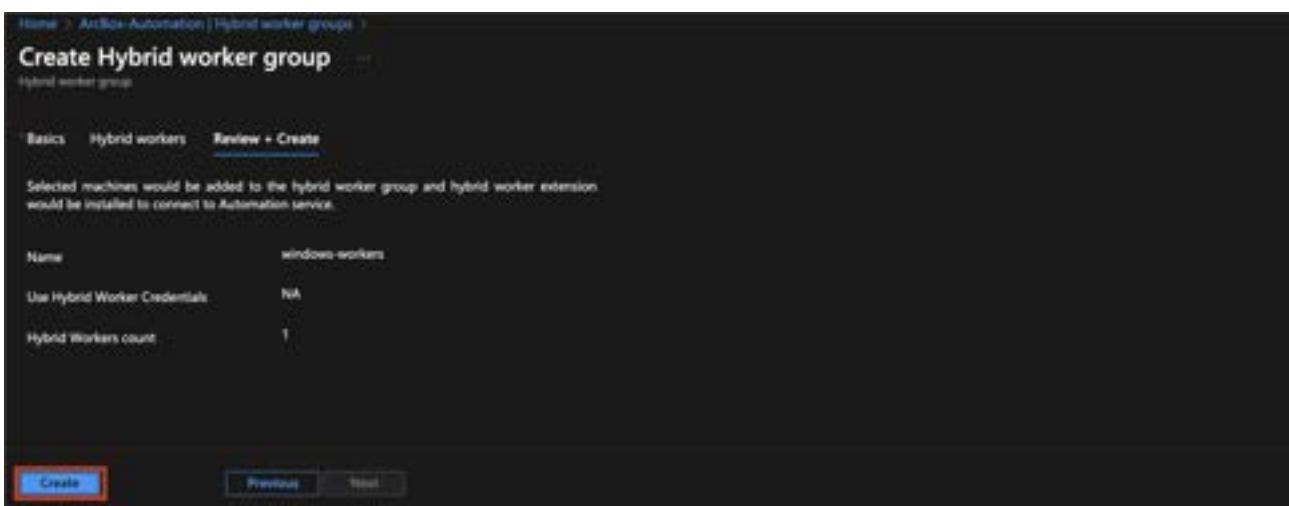
Hybrid worker group

Basics Hybrid workers Review + Create

Selected machines would be added to the hybrid worker group and hybrid worker extension would be installed to connect to Automation service.

Name	windows-workers
Use Hybrid Worker Credentials	NA
Hybrid Workers count	1

**Create** Previous Next



10. Wait for the following activities to be finished:

The screenshot shows the Azure Notifications center with the following activity logs:

- HybridWorkerExtension installation status**: Extension installation status for the machines which were successfully added as hybrid workers. Success: 1 Failure: 0. (a minute ago)
- HybridWorkerExtension installation succeeded**: Machine name: 'ArcBox-Win2K22'. (a minute ago)
- Hybrid worker addition status: 'windows-workers'**: Success: 1 Failure: 0. (3 minutes ago)
- Created hybrid worker group successfully**: Group name: 'windows-workers'. (3 minutes ago)

11. Repeat the above steps to create an additional Hybrid worker group called *linux-workers* where you select to onboard the machine *ArcBox-Ubuntu01* to the group.
12. After completing this task you should have the following Hybrid worker groups:

The screenshot shows the Azure ArcBox-Automation Hybrid worker groups page. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Process Automation, Runbooks, Jobs, and Hybrid worker groups (which is currently selected). The main content area has tabs for User hybrid worker groups and System hybrid worker groups, with the User tab selected. A warning message states: "Agent-based Hybrid Worker support will retire on 31 August 2024 and would no longer be supported after that date. You need to complete migration of existing Agent-based User Hybrid Workers to Extension-based Hybrid Workers before 31 August 2024. Learn more." Below this, it says: "Users can create and manage hybrid worker groups for running hybrid jobs, which provides redundancy to run jobs across multiple hybrid workers. With extension-based hybrid workers (both Azure machines and non-Azure machines) through ARM-enabled servers and ARM-enabled VMware VM (preview) can be managed through ARM templates and policies. Learn more." A search bar is at the top right. The main table lists one hybrid worker group:

Group Name	Created On
Windows-workers	06/06/2023, 10:29 pm

### Task 3 has been completed

Click **Next** for the next task or [go back to the main table of content](#)

## Task 4 - Add Hybrid Runbook Workers using Powershell

- This task is an alternative to [task 3](#), and only needed if you have not executed task 3. You can jump straight to [task 5](#) if you have already added the hybrid runbook workers from the Azure portal.

- 1. From the ArcBox-Client machine start PowerShell 7.
  - 2. Copy the following Powershell script into a text editor and customize the parameter values to reflect your environment for the resource group name if needed (**repeat for all occurrences!**). Paste the code in the Cloud Shell PowerShell window and press Enter.

```
powershell

# Retrieve service URL for Automation account (used when registering Arc-enabled
$AutomationAccount = Get-AzResource -ResourceGroupName "ArcBox" -Name "ArcBox-Au
$AutomationAccountInfo = Invoke-AzRestMethod -SubscriptionId $AutomationAccount.
$AutomationHybridServiceUrl = ($AutomationAccountInfo.Content | ConvertFrom-Json

# Create the Linux Hybrid Worker Group
New-AzAutomationHybridRunbookWorkerGroup -Name linux-workers -ResourceGroupName .

#Get the Arc-enabled Linux VM and add to the Hybrid Worker to the group
$ArcResource = Get-AzConnectedMachine -ResourceGroupName ArcBox -Name Arcbox-Ubu
New-AzAutomationHybridRunbookWorker -ResourceGroupName ArcBox -AutomationAccount
$ArcResource = Get-AzConnectedMachine -ResourceGroupName ArcBox -Name Arcbox-Ubu
$settings = @{
    "AutomationAccountURL" = $AutomationHybridServiceUrl
}
New-AzConnectedMachineExtension -ResourceGroupName $ArcResource.ResourceGroupNam

# Create the Windows Hybrid Worker Group
New-AzAutomationHybridRunbookWorkerGroup -Name windows-workers -ResourceGroupNam

#Get the Arc-enabled Windows VM and add to the Hybrid Worker to the group
$ArcResource = Get-AzConnectedMachine -ResourceGroupName ArcBox -Name ArcBox-Win
New-AzAutomationHybridRunbookWorker -ResourceGroupName ArcBox -AutomationAccount
$ArcResource = Get-AzConnectedMachine -ResourceGroupName ArcBox -Name Arcbox-Win
$settings = @{
    "AutomationAccountURL" = $AutomationHybridServiceUrl
}
New-AzConnectedMachineExtension -ResourceGroupName $ArcResource.ResourceGroupNam
```

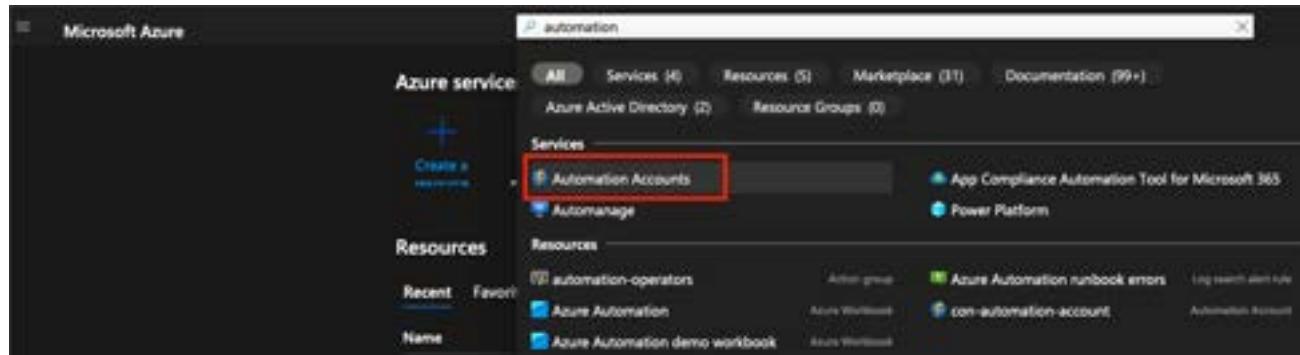
- 3. It will take few minutes to execute the script.

**Task 4 has been completed**

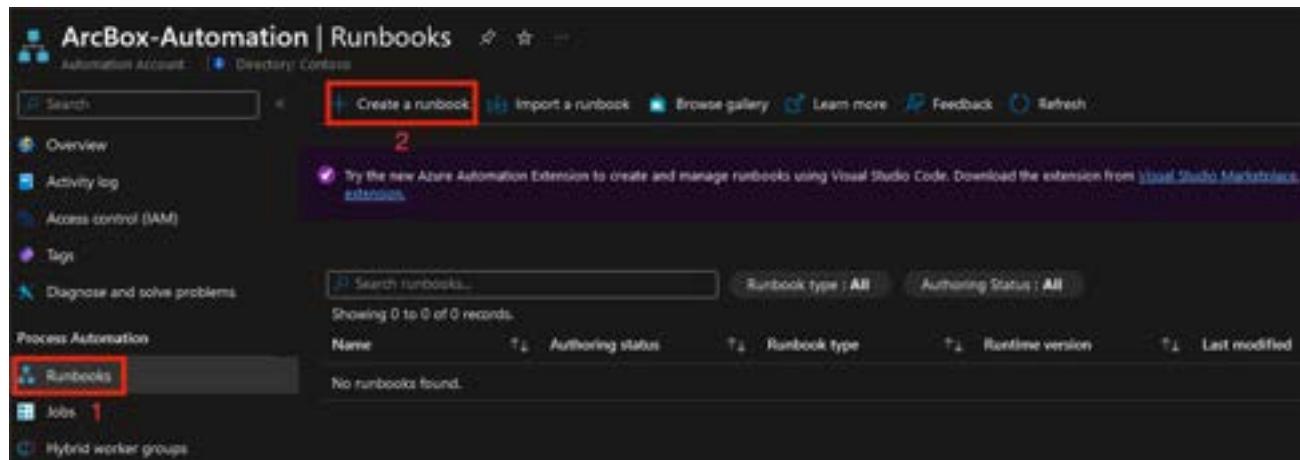
Click **Next** for the next task or [go back to the main table of content](#)

## Task 5 - Create and start a runbook

1. In the Azure Portal, search for *automation* and navigate to *Automation accounts*



2. Navigate to the *ArcBox-Automation* account you created previously. Select *Runbooks* and click *Create a runbook*



3. Enter the following values then click *Create*

- Name: Start-DiskClean
- Runbook type: PowerShell
- Runtime version: 7.2
- Description: Invoke disk cleanup

## Create a runbook

**Name\*** Start-DiskClean

**Runbook type\*** PowerShell

**Runtime version\*** 7.2 (preview)

**Description** Invoke disk cleanup

**Info:** During runbook execution, PowerShell modules targeting 7.2 runtime version will be used. Please make sure the required PowerShell modules are present in 7.2 runtime version.

**Create** **Cancel**

- 4. After provisioning, the runbook editor will open the newly created runbook:

Home > Automation Accounts > ArcBox-Automation | Runbooks > Start-DiskClean (ArcBox-Automation|Start-DiskClean)

### Edit PowerShell Runbook

Start-DiskClean

Save Publish Revert to published Test pane Edit in VS Code Feedback

CMDLETS RUNBOOKS ASSETS

- 5. Paste the following script into the editor pane then Save:

```
powershell
if ($IsWindows) {
    Write-Output 'Free disk space before cleanup action'
    Get-Volume -DriveLetter C | Out-String
    Write-Output "Windows Update component store cleanup"
    Dism.exe /online /Cleanup-Image /StartComponentCleanup /ResetBase
    $SystemTemp = "$env:SystemRoot\Temp"
    Write-Output "Empty the system temporary folder: $SystemTemp"
    Get-ChildItem -Path $SystemTemp -Recurse | Remove-Item -Force -Recurse
```

```

        Write-Output 'Free disk space after cleanup action'

        Get-Volume -DriveLetter C | Out-String

    } elseif ($IsLinux) {

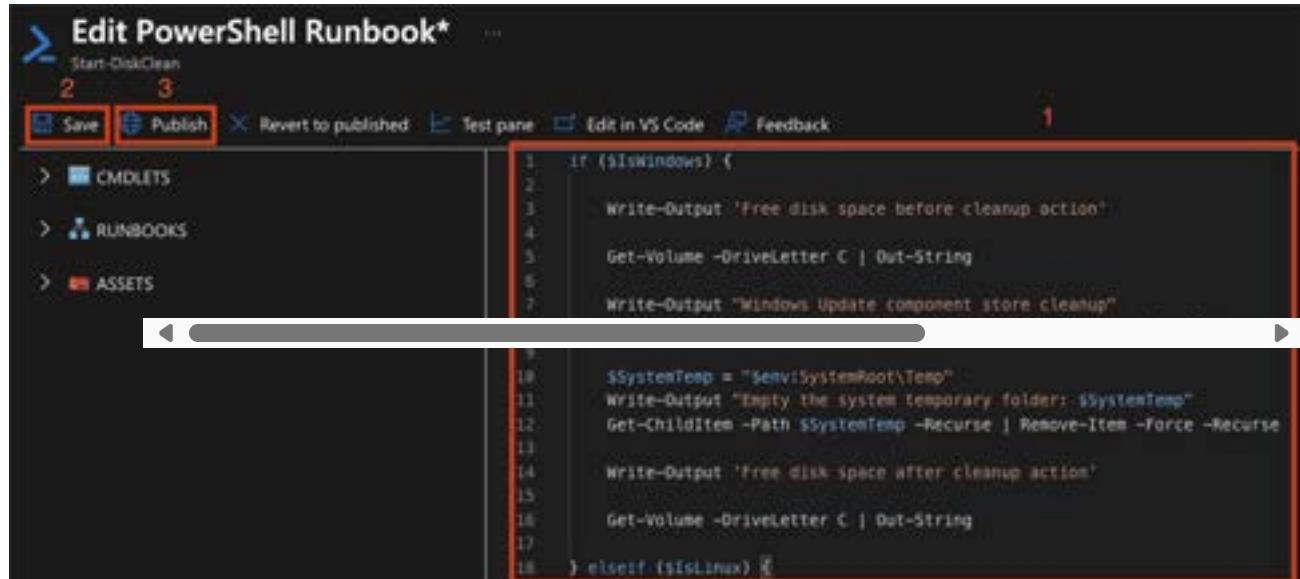
        Write-Output 'Free disk space before cleanup action'
        df -h -m
        # Specify the directory where your log files are located
        $logDir = '/var/log'
        # Define the number of days to retain log files
        $daysToKeep = 7
        # Get the current date
        $currentDate = Get-Date
        # Calculate the date threshold for log file deletion
        $thresholdDate = $currentDate.AddDays(-$daysToKeep)
        # List log files in the specified directory that are older than the threshold
        $filesToDelete = Get-ChildItem -Path $logDir -File | Where-Object { $_.LastWriteTime -lt $thresholdDate }

        # Delete the old log files
        foreach ($file in $filesToDelete) {
            Remove-Item -Path $file.FullName -Force
        }
        Write-Output 'Free disk space after cleanup action'
        df -h -m

    }
}

```

6. Click Publish

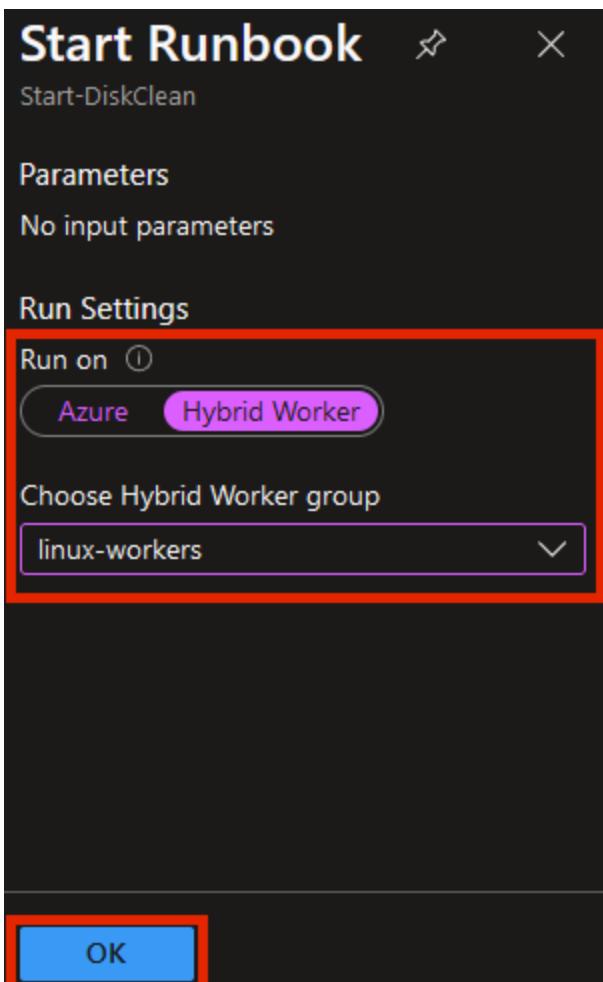


7. Click Start

**Note: You may need to click Refresh for the Start button to become active**

The screenshot shows the Azure ArcRunbook Editor interface. At the top, there's a navigation bar with 'Start-DiskClean (ArcBox-Automation/Start-DiskClean)' and various action buttons like 'Start', 'View', 'Edit', etc. Below the navigation is a sidebar with sections like 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Resources' (Jobs, Schedules, Webhooks), 'Runbook settings', 'Properties', and 'Description'. The main area is titled 'Essentials' and displays information such as 'Resource group: arcbox-automation', 'Account: ArcBox-Automation', 'Location: East US', 'Subscription: Test', 'Status: Published', 'Runbook type: PowerShell', 'Runtime version: 7.2 (preview)', and 'Last modified: 1/9/2023, 7:58 AM'. There are tabs for 'Job' and 'Power (Import/Update)'. Below this, there's a 'Recent Jobs' section with a single entry: 'Status: Created, Last updated: [redacted]'. On the far left, there's a vertical sidebar with 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Resources' (Jobs, Schedules, Webhooks), 'Runbook settings', 'Properties', and 'Description'.

- 8. Select *Hybrid Worker* and select *linux-workers* under *Choose Hybrid Worker group*. Click *OK*



- 9. Click on the *Output* tab and wait for the job to finish. You should notice that the amount of free space has increased after the cleanup action has completed.

Home > ArcBox-Automation | Runbooks > Start-DiskClean (ArcBox-Automation/Start-DiskClean) >

## Start-DiskClean 09/09/2023, 08:51

Job

► Resume  Stop || Suspend  Refresh

Essentials

ID : fa7388d2-652f-4d18-b7d1-8e6b7fecb215	Created : 09/09/2023, 08:51:33
Status : Completed	Last Update : 09/09/2023, 08:52:13
Ran on : linux-workers	Runbook : Start-DiskClean
Ran As : User	Source snapshot : <a href="#">View source snapshot</a>

Input Output Errors Warnings All Logs Exception

```
Free disk space before cleanup action
Filesystem      1M-blocks  Used Available Use% Mounted on
tmpfs          392       2       391  1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  48701 11559  34951 25% /
tmpfs          1956      1       1954  1% /dev/shm
tmpfs           5       0       5  0% /run/lock
/dev/ada2      974   253       654 28% /boot
/dev/sdal      511       7       505  2% /boot/efi
tmpfs          392       1       392  1% /run/user/1000

Free disk space after cleanup action
Filesystem      1M-blocks  Used Available Use% Mounted on
tmpfs          392       2       391  1% /run
/dev/mapper/ubuntu--vg-ubuntu--lv  48701 11555  34955 25% /
tmpfs          1956      1       1954  1% /dev/shm
tmpfs           5       0       5  0% /run/lock
/dev/ada2      974   253       654 28% /boot
/dev/sdal      511       7       505  2% /boot/efi
tmpfs          392       1       392  1% /run/user/1000
```

- The provided runbook is a starting point for cleaning a single directory. Additional logic and directories may be added as required for specific scenarios. For example, it is also possible to add logic to connect to other machines in order to perform cleanup actions on those.
- 10. Next, you will be running the same runbook on a Windows machine. Navigate back to the runbook overview page for *Start-DiskClean* and click *Start*.

Home > Automation Accounts > ArcBox-Automation | Runbooks > Start-DiskClean (ArcBox-Automation/Start-DiskClean)

Start  View  Edit  Link to schedule  Add webhook  Delete  Export  Feedback  Refresh

Overview

Resource group : <a href="#">arcbox-automation</a>	Subscription ID : 870d0cfd-402e-48de-1040e958363
Author : ArcBox-Automation	Status : Published
Location : East US	Runbook type : PowerShell
Subscription : <a href="#">Default</a>	Runtime version : 7.2 (preview)
	Last modified : 9/9/2023, 7:58 AM

Resources

- Jobs
- Schedules
- Webhooks

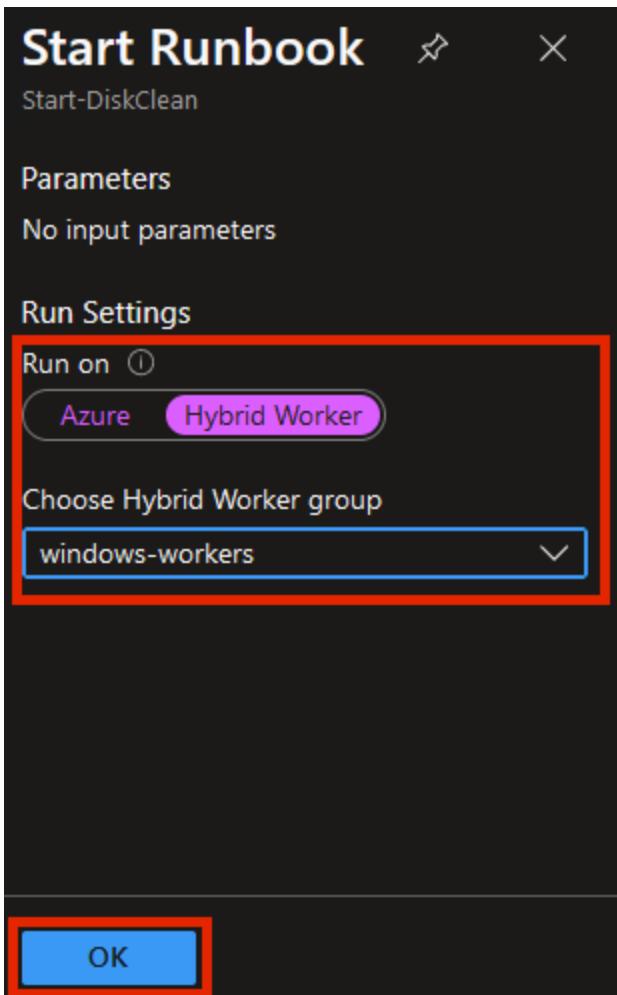
Runbook settings

- Properties
- Description

Recent Jobs

Status	Created	Last updated
No job found.		

- 11. Select *Hybrid Worker* and select *windows-workers* under *Choose Hybrid Worker group*, then Click *OK*.



- 12. Click on the *Output* tab and wait for the job to finish.
- The cleanup action may run for a few minutes, so feel free to continue and revisit the job output later.
  - When completed, you should notice that the amount of free space has increased after the cleanup action has completed.

Start-DiskClean 11/09/2023, 22:44

Job

Resume Stop Suspend Refresh

Essentials

ID : 7d578905-66da-44ea-99cb-74fa7e3a8f38	Created : 11/09/2023, 22:44:53
Status : Completed	Last Update : 11/09/2023, 22:54:35
Ran on : windows-workers	Runbook : Start-DiskClean
Ran As : User	Source snapshot : <a href="#">View source snapshot</a>

Input Output Errors Warnings All Logs Exception

Free disk space before cleanup action

DriveLetter	FriendlyName	FileSystemType	DriveType	HealthStatus	OperationalStatus	SizeRemaining	Size
C		NTFS	Fixed	Healthy	OK	81.04 GB	99.37 GB

Windows Update component store cleanup

Deployment Image Servicing and Management tool  
Version: 10.0.20348.681

Image Version: 10.0.20348.1787

[===== 10.0% ]  
[===== 19.0% ]  
[===== 20.0% ]  
[===== 20.0% ]

Free disk space after cleanup action

DriveLetter	FriendlyName	FileSystemType	DriveType	HealthStatus	OperationalStatus	SizeRemaining	Size
C		NTFS	Fixed	Healthy	OK	82.42 GB	99.37 GB

**Task 5 has been completed**

---

Click **Next** for the next exercise or [Go back to the main table of content](#)

## **Exercise 2 - Securely Connect to your Azure Arc-enabled servers using SSH access**

---

### **Objective**

Enable SSH based connections to Arc-enabled servers without requiring a public IP address or additional open ports.

### **Estimated Time to Complete This Lab**

20 minutes

### **Explanation**

This feature enables SSH based connections to Arc-enabled servers without requiring a public IP address or additional open ports. In this exercise, you will learn how to enable and configure this functionality. At the end, you will interactively explore how to access to Arc-enabled Windows and Linux machines.

## Task 1: Install prerequisites on client machine

---

It is possible to leverage both Azure CLI and Azure PowerShell to connect to Arc-enabled servers. Choose the one to use based on your own preferences.

- 1. RDP into the *ArcBox-Client* VM.
- 2. Open PowerShell and install either the Azure CLI extension or the Azure PowerShell modules based on your preference of tooling.

### Azure CLI

► `shell az extension add --name ssh`

or

### Azure PowerShell

► `PowerShell Install-Module -Name Az.Ssh -Scope CurrentUser -Repository PSGallery`  
`Install-Module -Name Az.Ssh.ArcProxy -Scope CurrentUser -Repository PSGallery`

- We recommend that you install the tools on the ArcBox Client virtual machine, but you may also choose to use your local machine if you want to verify that the Arc-enabled servers is reachable from any internet-connected machine after performing the tasks in this module.

### Task 1 has been completed

Click **Next** for the next task or [go back to the main table of content](#)

## Task 2 - Enable SSH service on Arc-enabled servers

---

We will use two Arc-enabled servers running in ArcBox for this module:

- *ArcBox-Win2K22*
- *ArcBox-Ubuntu-01*

- 1. RDP into the *ArcBox-Client* VM
- 2. Open Hyper-V Manager
- 3. Right click *ArcBox-Win2K22* and select Connect twice
- 4. Login to the operating system using username Administrator and the password you used when deploying ArcBox, by default this is **JS123!!**
- 5. Open PowerShell and install OpenSSH for Windows by running the following:

PowerShell

```
# Install the OpenSSH Server
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

# Start the sshd service
Start-Service sshd

# Configure the service to start automatically
Set-Service -Name sshd -StartupType 'Automatic'

# Confirm the Windows Firewall is configured to allow SSH. The rule should
# if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction Silen
# Write-Output "Firewall Rule 'OpenSSH-Server-In-TCP' does not exist, creatin
# New-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -DisplayName "OpenSSH !
# } else {
#     Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been created and
# }
```

- 6. Close the connection to *ArcBox-Win2K22*
- 7. Right click *ArcBox-Ubuntu-01* in Hyper-V Manager and select Connect
- 8. Login to the operating system using username **jumpstart** and the password **JS123!!**
- 9. Run the command ➤ `systemctl status ssh` to verify that the SSH service is active and running
- 10. Close the connection to *ArcBox-Ubuntu-01*

**Task 2 has been completed**

Click **Next** for the next task or [go back to the main table of content](#)

## Task 3 - Connect to Arc-enabled servers

---

- 1. From the *ArcBox-Client* VM, open a PowerShell session and use the below commands to connect to **ArcBox-Ubuntu-01** using SSH:

### Azure CLI

```
▶ shell $serverName = "ArcBox-Ubuntu-01" $localUser = "jumpstart" $resourceGroup = "ArcBox" az ssh arc --resource-group $resourceGroup --name $serverName --local-user $localUser or
```

### Azure PowerShell

```
▶ PowerShell $serverName = "ArcBox-Ubuntu-01" $localUser = "jumpstart" $resourceGroup = "ArcBox" Enter-AzVM -ResourceGroupName $resourceGroup -Name $serverName -LocalUser $localUser
```

- 2. The first time you connect to an Arc-enabled server using SSH, you will see the following prompt:

Port 22 is not allowed for SSH connections in this resource. Would you like to update the current Service Configuration in the endpoint to allow connections to port 22? If you would like to update the Service Configuration to allow connections to a different port, please provide the -Port parameter or manually set up the Service Configuration. (y/n)

- 3. It is possible to pre-configure this setting on the Arc-enabled servers by following the steps in the section *Enable functionality on your Arc-enabled server* in the [documentation](#). However, for this exercise, type ▶ yes and press Enter to proceed.

```
PS C:\Users\arcdemo> az ssh arc --resource-group $Env:resourceGroup --name $serverName --local-user $localUser
The authenticity of host 'arcbox-ubuntu-01 (<no hostip for proxy command>)' can't be established.
ECDSA key fingerprint is SHA256:tmUJUPFFW9dsJgXPZ2K8manuo24aVLuhZ2GkHEmusuc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'arcbox-ubuntu-01' (ECDSA) to the list of known hosts.
arcdemo@arcbox-ubuntu-01's password: -
```

```
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-137-generic x86_64)
```

```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
```

```
System information as of Mon 23 Jan 2023 07:40:10 AM UTC
```

```
System load: 0.61          Processes: 143
Usage of /: 42.3% of 47.56GB  Users logged in: 0
Memory usage: 26%          IPv4 address for eth0: 10.10.1.104
Swap usage: 0%
```

```
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.
```

```
https://ubuntu.com/engage/secure-kubernetes-at-the-edge
```

```
15 updates can be applied immediately.
```

```
To see these additional updates run: apt list --upgradable
```

```
Last login: Fri Jan 20 21:06:23 2023 from 127.0.0.1
```

```
arcdemo@arcbox-ubuntu-01:~$ -
```

- 4. Following the previous method, connect to ArcBox-Win2K22 via SSH.

## Azure CLI

```
▶ shell $serverName = "ArcBox-Win2K22" $localUser = "Administrator" $resourceGroup = "ArcBox" az ssh arc --resource-group $resourceGroup --name $serverName --local-user $localUser
```

or

## Azure PowerShell

```
▶ PowerShell $serverName = "ArcBox-Win2K22" $localUser = "Administrator" $resourceGroup = "ArcBox" Enter-AzVM -ResourceGroupName $resourceGroup -Name $serverName -LocalUser $localUser
```

```
PS C:\Users\arcdemo> az ssh arc --resource-group $Env:resourceGroup --name $serverName --local-user $localUser
The authenticity of host 'arcbox-win2k22 (<no hostip for proxy command>)' can't be established.
ECDSA key fingerprint is SHA256:RCu06BLhtQ8lgr5OFXW6h2BXRT2xocNWB0ZEq2KBizU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'arcbox-win2k22' (ECDSA) to the list of known hosts.
Administrator@arcbox-win2k22's password: -
```

```
Microsoft Windows [Version 10.0.20348.1366]
(c) Microsoft Corporation. All rights reserved.
```

```
Administrator@ARCBOX-WIN2K22 C:\Users\Administrator>
```

- 5. In addition to SSH, you can also connect to the Azure Arc-enabled servers, Windows Server virtual machines using **Remote Desktop** tunneled via SSH.

## Azure CLI

```
``shell $serverName = "ArcBox-Win2K22" $localUser = "Administrator" $resourceGroup = "ArcBox" az ssh arc --resource-group $resourceGroup --name $serverName --local-user $localUser --rdp
```

```

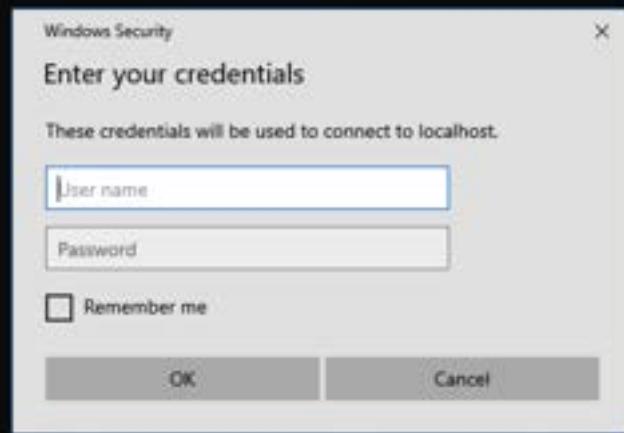
or

## Azure PowerShell

```
``PowerShell $serverName = "ArcBox-Win2K22" $localUser = "Administrator" $resourceGroup = "ArcBox" Enter-AzVM -ResourceGroupName $resourceGroup -Name $serverName -LocalUser $localUser -Rdp
```

```

```
PS C:\Users\arcdemo> az ssh arc --resource-group $env:resourceGroup --name $servername --local-user $localUser --rdp
RDP feature is in preview.
The authenticity of host 'arcbox-win2k22 (no hostip for proxy command)' can't be established.
ECDSA key fingerprint is SHA256:RCU06BLhtQ8lgr5QFXWh28XRT2xcNaB02Eq2K8IzU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Administrator@arcbox-win2k22's password:
Launching Remote Desktop Connection
To close this session, close the Remote Desktop Connection window.
```



**Task 3 has been completed**

Click **Next** for the next task or [go back to the main table of content](#)

## Task 4 - Optional: Azure Entra ID based SSH Login

---

- 1. The *Azure AD based SSH Login – Azure Arc VM extension* can be added from the extensions menu of the Arc server in the Azure portal. The Azure AD login extension can also be installed locally via a package manager via: ➤ `apt-get install aadsshlogin` or the following command:

shell

```
▶ $serverName = "ArcBox-Ubuntu-01"  
$resourceGroup = "ArcBox"  
az connectedmachine extension create --machine-name $serverName --resource
```

- 2. Configure role assignments for the Arc-enabled server *ArcBox-Ubuntu-01* using the Azure portal. Two Azure roles are used to authorize VM login:

- **Virtual Machine Administrator Login:** Users who have this role assigned can log in to an Azure virtual machine with administrator privileges.
- **Virtual Machine User Login:** Users who have this role assigned can log in to an Azure virtual machine with regular user privileges.

- 3. After assigning one of the two roles to your personal Azure Entra ID user account, run the following commands on the *ArcBox-Client* to connect to *ArcBox-Ubuntu-01* using SSH and Entra ID-based authentication (you can use either Azure CLI or PowerShell) :

### Azure CLI

```
▶ shell # Log out from the Service Principal context az logout # Log in using your  
personal account az login $serverName = "ArcBox-Ubuntu-01" $resourceGroup = "ArcBox"  
az ssh arc --resource-group $resourceGroup --name $serverName
```

### Azure PowerShell

```
```PowerShell # Log out from the Service Principal context Disconnect-AzAccount # Log in using your  
personal account Connect-AzAccount $serverName = "ArcBox-Ubuntu-01" $resourceGroup = "ArcBox"  
Enter-AzVM -ResourceGroupName $resourceGroup -Name $serverName
```

...

- 4. You should now be connected and authenticated using your Azure Entra ID account. Verify this by running:

shell

```
▶ whoami
```

- 5. Exit the ssh session by typing *exit*.

**Exercise 2 has been completed**

## **Exercise 3 - Run PowerShell and Shell scripts on Azure Arc-enabled servers using the Run command**

---

### **Objective**

Run PowerShell and Shell commands on Arc-enabled Windows and Linux servers.

### **Estimated Time to Complete This Lab**

30 minutes

### **Explanation**

The Run command feature uses the Connected Machine agent to remotely run PowerShell scripts within an Azure Arc-connected Windows machine and Shell scripts within an Azure Arc-connected Linux machine. This capability is useful in all scenarios where you want to run a script within an Arc-connected machine. It allows you to troubleshoot and remediate a machine that doesn't have the RDP or SSH port open because of improper network or administrative user configuration.

- Use PowerShell 7.0 on the ArcBox-Client to run the commands in the rest of this Exercise. Or alternatively you can use Azure Cloud Shell but you might need to deal with some Powershell module compatibility settings.**

## Task 1: Check the pre-requisites

---

- 1. Check the version of the Azure CLI extension "connectedmachine" on your client machine using the following command:

PowerShell

```
▶ az extension list --query "[?name=='connectedmachine'].version"
```

- 2. If the "connectedmachine" extension does not exist, or if the version of the Azure CLI extension is older than "1.0.0" then remove the old version (if it exists) and install the new one:

PowerShell

```
▶ #Remove the old version of the extension  
az extension remove --name connectedmachine
```

PowerShell

```
▶ #Install latest version of the extension  
az extension add --name connectedmachine --allow-preview True
```

- 3. Check if the installed version of module Az.ConnectedMachine is 1.0.0 or higher. Use the following PowerShell command to check the installed version:

PowerShell

```
▶ Get-Module -Name Az.ConnectedMachine
```

- 4. If you need to install the latest version then use the following PowerShell command:

PowerShell

```
▶ Install-Module -Name Az.ConnectedMachine -Force
```

### Task 1 has been completed

Click **Next** for the next task or [go back to the main table of content](#)

## Task 2: Use the Run command to execute a simple PowerShell script within an Arc-connected Windows machine

- 1. Run the following Azure CLI command after adding the appropriate resource group, name of the Arc-connected machine, a name identifying the command, and the location of your Arc-connected machine:

```
PowerShell
```

```
▶ az connectedmachine run-command create --resource-group <Resource Group Name>
```

For example:

```
PowerShell
```

```
▶ az connectedmachine run-command create --resource-group ArcBox --machine-na
```

- If you receive an error message about the command not being recognized or that a preview version is needed then go back to the **Check the pre-requisites** step and follow the instructions to first remove the *connectedmachine* extension, then to install the extension with **--allow-preview True** option.

After a couple of minutes the result is returned. If the execution is successful then you will see the following within the longer returned JSON string:

```
▶ PowerShell "executionState": "Succeeded", "exitCode": 0, "output": "Hello World",
```

- 2. You can also execute the script using a PowerShell command. Add the appropriate variable values to the following command then run it:

```
PowerShell
```

```
▶ New-AzConnectedMachineRunCommand -ResourceGroupName "<Resource Group Name>
```

The successful execution of the PowerShell command will show the following output:

```
InstanceViewExecutionMessage      : RunCommand script execution completed
InstanceViewState                  : Succeeded
InstanceViewExitCode               : 0
InstanceViewOutput                 : Hello World
```

**Task 2 has been completed**

Click **Next** for the next task or [go back to the main table of content](#)

## Task 3: Use the Run command to execute a simple Shell command within an Arc-connected Linux machine

---

- 1. Run the following Azure CLI command after adding the appropriate parameters:

PowerShell

```
▶ az connectedmachine run-command create --resource-group <Resource Group Name>
```



Or in PowerShell:

```
▶ PowerShell New-AzConnectedMachineRunCommand -ResourceGroupName "<Resource Group Name>" -Location "<Location>" -SourceScript "ifconfig" -RunCommandName "<Identifying Name of command>" -MachineName "<Machine Name>"
```

If the execution is successful then you should have an output that includes the result of the ifconfig command as a string. Notice that the line breaks are indicated by the "\n" string:

```
"output": "eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500\n      inet 10.10.1.102 netmask 255.255.255.0\n        broadcast 10.10.1.255\n          inet6 fe80::215:5dff:fe01:403 prefixlen 64 scopeid 0x20<link>\n            ether 00:15:5d:01:\n              04:03 txqueuelen 1000 (Ethernet)\n                RX packets 27507 bytes 26632258 (26.6 MB)\n                  RX errors 0 dropped 0 overruns 0 frame 0\n                TX packets 13246 bytes 4237820 (4.2 MB)\n                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0\n\nlo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536\n      inet 127.0.0.1 netmask 255.0.0.0\n        inet6 ::1\n          prefixlen 128 scopeid 0x10<host>\n            loop txqueuelen 1000 (Local Loopback)\n              RX packets 10160 bytes 1743552 (1.7 MB)\n                RX errors 0 dropped 0 overruns 0 frame 0\n              TX packets 10160 bytes 1743552 (1.7 MB)\n                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0\n",\n    \"startTime\": \"2024-03-26T13:06:44+00:00\"\n},
```

### Task 3 has been completed

Click **Next** for the next task or [go back to the main table of content](#)

## Task 4: Direct the output of a Run command to Azure storage blob

---

- 1. Create a storage account (if you do not have one) using the following command after filling in the required parameters:

PowerShell

```
▶ az storage account create --name <Storage account name> --resource-group <
```

- 2. Create a storage container to which you will direct the output of the run command:

PowerShell

```
▶ az storage container create --name <container name> --account-name <Storage
```

- 3. Create a blob SAS URI with the following permissions: Read, Write, Create, delete, and append. You will need an end date for the validity of the SAS token, for example one day from the current date. Also, to be able to use the SAS URI in our run command you will need to remove any double quotes from the beginning and the end of the generated URI.

PowerShell

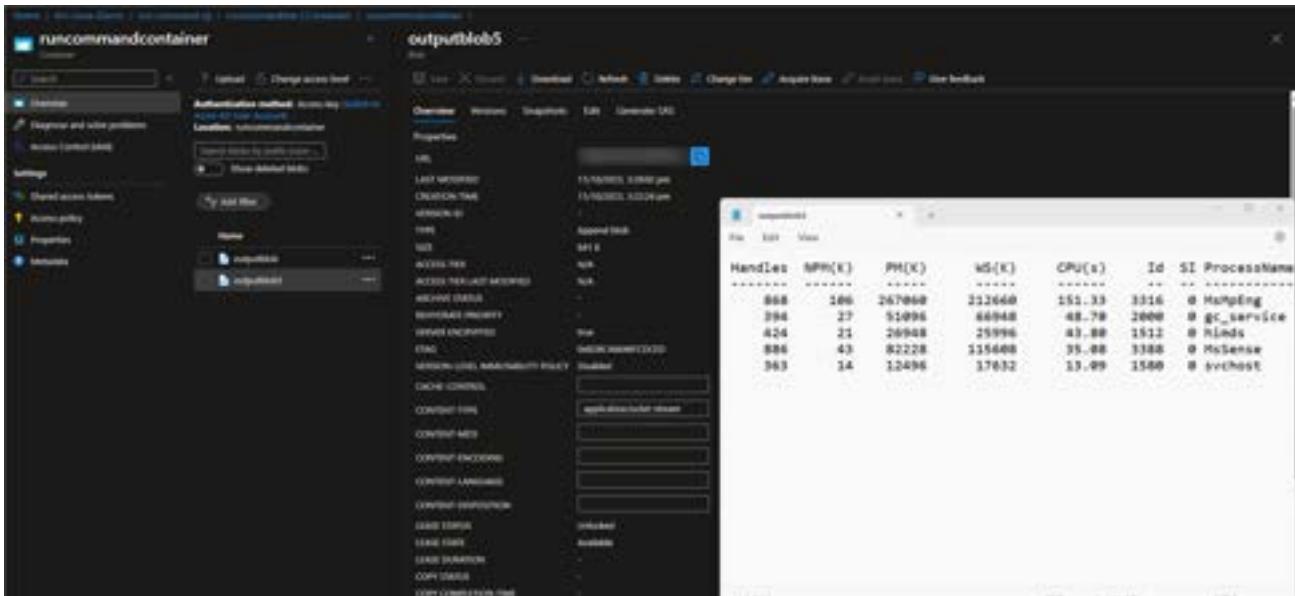
```
▶ $end=(Get-date).AddDays(1) | Get-Date -UFormat '+%Y-%m-%dT%H:%MZ'  
$sasuri = $(az storage blob generate-sas --account-name <storage account na
```

- 4. Execute the following run command which runs a PowerShell script within the Arc-enabled Windows machine. The run command directs the output to the append blob:

PowerShell

```
▶ az connectedmachine run-command create --resource-group "<Resource Group Name>"  
New-AzConnectedMachineRunCommand -ResourceGroupName "<Resource Group Name>"
```

- 5. Examine the storage container in the Azure portal or using the Azure storage explorer. Look for the output of the command in the blob specified by the SAS URI used in the run command. The output should be the top five processes for CPU usage in the machine.



**Task 4 has been completed**

**Exercise 2 has been completed**

---

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB12: Connect a SQL Server to Azure Arc

---

Azure Arc automatically installs the Azure extension for SQL Server when a server connected to Azure Arc has SQL Server installed. All the SQL Server instance resources are automatically created in Azure, providing a centralized management platform for all your SQL Server instances.

## Student Lab Manual

### Table of Contents

#### Exercise 1 - Pre-Requisites

##### **Task 1 - Review Pre-requisites**

#### Exercise 2 - Review Existing Arc Resources

##### **Task 1 - Use the Azure portal to examine you Arc-enabled machines inventory**

#### Exercise 3 - Add SQL Server to Azure Arc

##### **Task1 - Onboard a Windows Server to Azure Arc to automatically Arc-enable the SQL Server**

##### **Task2 - Verify that the SQL Server has been onboarded**

# Exercise 1 - Pre-Requisites

---

## **Objective**

Review the necessary pre-requisites to Arc-enable SQL Servers.

## **Estimated Time to Complete This Exercise**

10 minutes

## Task 1: Review Pre-requisites

---

Before you add an Azure Arc-enabled SQL Server you will need the following pre-requisites. **Note that in this lab environment these pre-requisites have already been provided and are listed here for information only.**

- 1. A virtual or physical machine running SQL Server: The machine hosting SQL Server must be connected to the internet directly or via a proxy server.
- 2. A user account with permissions: An account with local admin rights. [Learn more about the required Azure permissions](#).
- 3. PowerShell: Powershell must be installed on the computer executing the onboarding script. [Learn how to install Powershell](#)
- 4. Registered resource providers: The Microsoft.AzureArcData and Microsoft.HybridCompute resource providers must be registered. [Learn more about registering resource providers](#)

### Task 1 has been completed

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Exercise 2 - Review Existing Arc Resources

---

### **Objective**

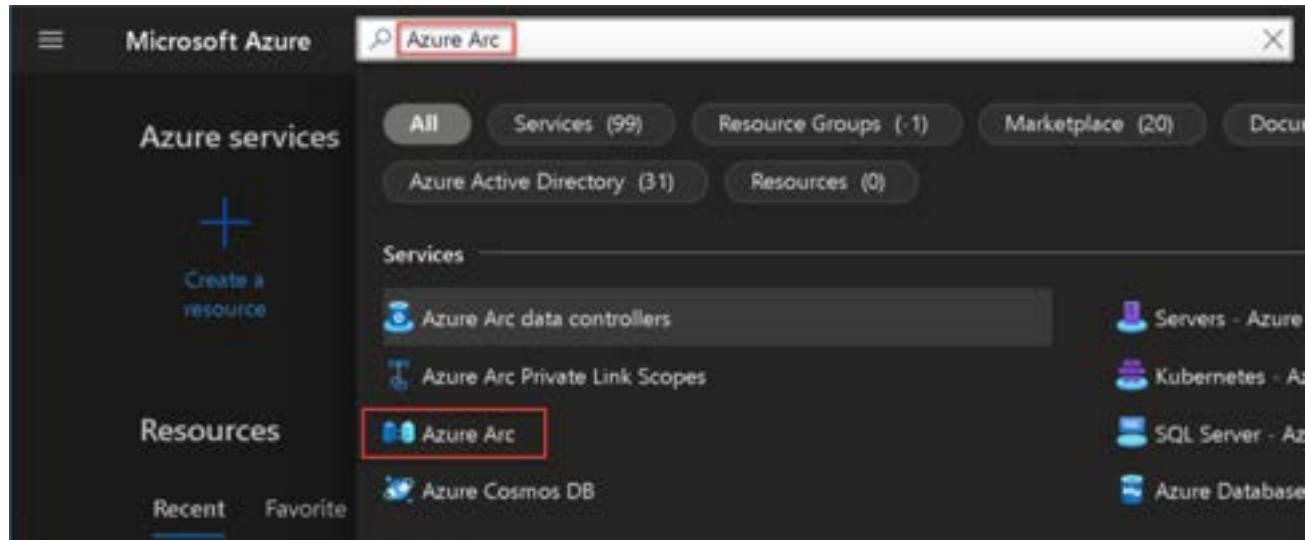
The deployment process that you have walked through in Lab01 should have set up a number of Server VMs running on Hyper-V in the ArcBox-Client machine. One of these Servers *ArcBox-SQL* has a SQL server deployed. In this exercise you will Arc-enable this SQL server.

### **Estimated Time to Complete This Exercise**

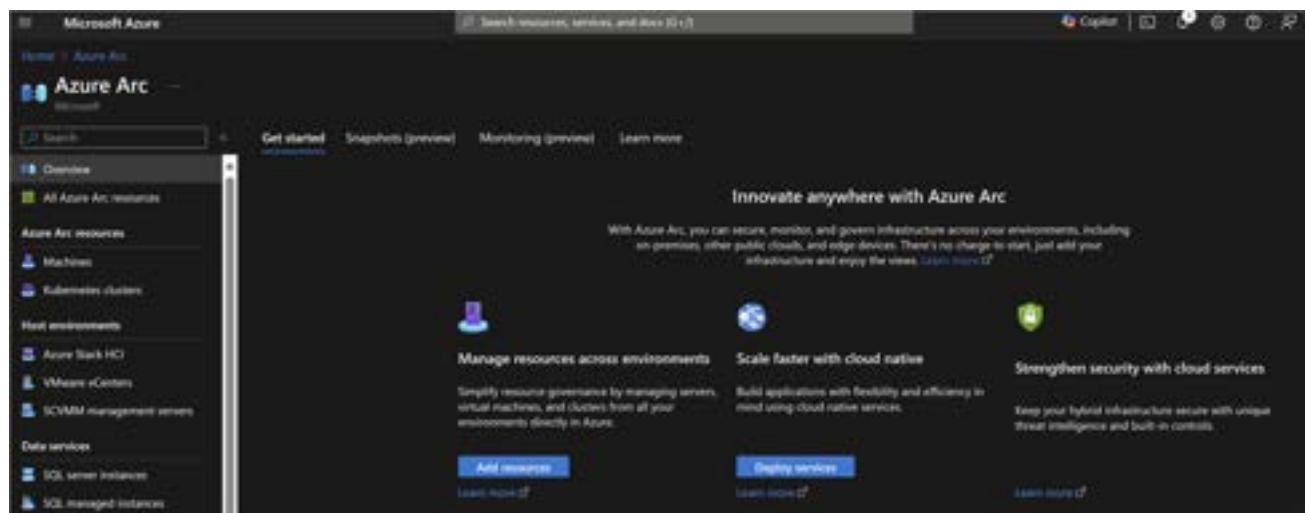
15 minutes

## Task 1: Use the Azure portal to examine your Arc-enabled machines inventory

- ☐ 1. In the Azure portal search for *Azure Arc* in the search bar



- ☐ 2. In the Azure Arc page you should see the *Overview* option



- ☐ 3. Click the *All Azure Arc Resources* option, and you should see the Arc-enabled Windows and Linux servers, but you notice that the *ArcBox-SQL* Windows machine is not Arc-enabled, neither is the SQL Server deployed on it

☐ Note that the Azure Arc resources showing in your portal might be different from the picture below but you should not see the *ArcBox-SQL* machine unless you have onboarded the the Windows server *ArcBox-SQL* optionally in Lab02.

☐ If during Lab02 of this workshop you have also onboarded the Windows server *ArcBox-SQL* then you will see two Arc-enabled resources one for the Windows server and one for the SQL server

hosted inside the Windows server. In the latter case you can jump to Exercise 3 - Task 2.

The screenshot shows the Azure Arc Machines blade. On the left, there's a navigation menu with 'Machines' highlighted. The main area displays three machine resources:

Name	State	Agent status
Azure VM	Connected	Connected
Windows Server 2019	Connected	Connected
Windows Server 2022	Connected	Connected

Below the table, there are columns for Resource group, Subscription, Reporting system, Underlying instance, Monitoring interval, and Update status. The 'Reporting system' column shows 'Metrics (CloudWatch Metrics)' for all three machines.

### Task 1 has been completed

Click **Next** for the next exercise or [Go back to the main table of content](#)

# Exercise 3 - Add SQL Server to Azure Arc

---

## **Objective**

In this exercise you will onboard a SQL Server to Azure Arc by first onboarding the Windows Server hosting the SQL Server. Once the Windows Server is Arc-enabled, it will automatically Arc-enable the SQL Server.

## **Estimated Time to Complete This Lab**

20 minutes

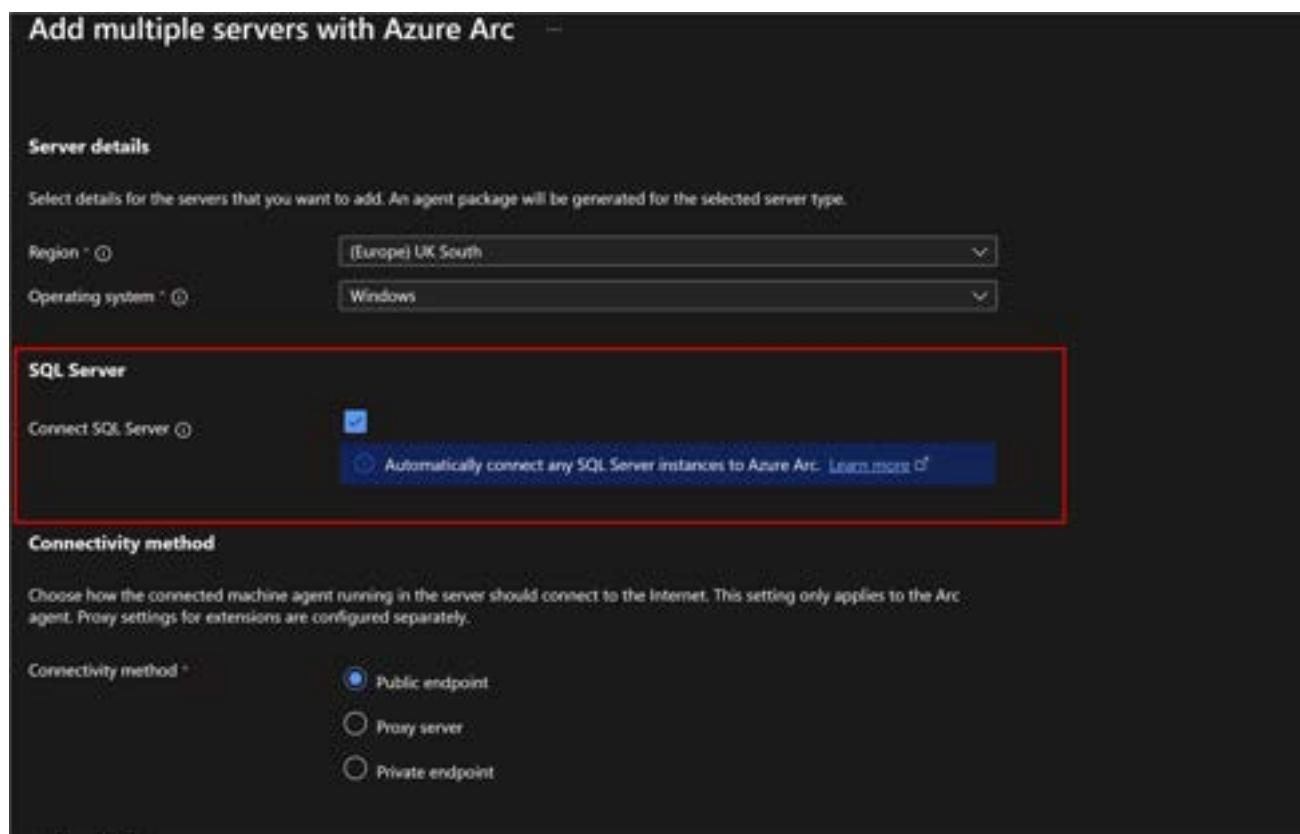
## **Explanation**

Connecting machines in your hybrid environment directly with Azure can be accomplished using different methods, depending on your requirements and the tools you prefer to use. In this instance you will use the same method of *Lab02* to onboard the Windows machine that hosts the SQL Server.

## Task 1: Onboard a Windows Server to Azure Arc to automatically Arc-enable the SQL Server

- 1. Refer to *Lab02 , Exercise 2* and follow the steps to onboard the nested *ArcBox-SQL* VM. However, this time make sure that you tick the *Connect SQL Server* option as shown below. This will automatically onboard the SQL Server to Arc in addition to the Windows server.

## Task 2: Verify that the SQL Server has been onboarded



- 1. After 5-10 minutes you should notice that the SQL Server *ArcBox-SQL* has also been onboarded. Confirm that the *ArcBox-SQL* VM has been onboarded by viewing all the Azure Arc resources as explained above in *Exercise 1* of this lab.

The screenshot shows the 'Azure Arc | All Azure Arc resources' blade. The left sidebar includes 'Overview', 'All Azure Arc resources' (which is selected), 'Management', 'Extended Security Updates', 'Custom locations', and 'Data controllers'. The main area displays a table of resources with columns for Name, Resource group, and Location. Three resources are listed: 'ARCBX-SQ' (Resource group: 'ArcBox', Location: 'East US'), 'ARCBX-SQ' (Resource group: 'ArcBox', Location: 'East US'), and 'ArcBox (nested)' (Resource group: 'ArcBox', Location: 'East US'). The first two rows are highlighted with a red box.

- **If after more than 10 minutes** you still do not see the SQL Server *ArcBox-SQL* in the portal, then go to the ***ArcBox-SQL Windows server*** from the Arc page on the Azure portal and check the installed extensions. If you do not see the *WindowsAgent.SqlServer* extension then install it manually by adding it from the portal. After the installation completes you should see the SQL server onboarded.

# LAB13: Connect SQL Servers to Azure Arc using offline MSI installer

---

- This lab shows an alternative method to that of the previous lab for onboarding SQL Servers. You can treat it as an optional lab if you want to move to other labs that explore the capabilities that Azure Arc facilitate for managing SQL Servers.**

In the previous Lab you looked at onboarding a SQL Server to Azure Arc automatically by onboarding the machine that hosts the SQL Server to Azure Arc. In this lab you will look at an alternative method of onboarding the SQL Server using an MSI installer. This method is useful when you want to onboard a number of SQL Servers at scale or if the automatic method of onboarding was not successful. The exercises will be carried out using one server only (due to resource limitations on the lab infrastructure) but the method is applicable to multiple server deployment. Also note that you will be starting from the point where the Windows Server VM itself is connected to Arc and you will only be onboarding the SQL Server that is running on the Windows VM.

The onboarding involves installing an extension on the Arc-enabled Windows machine, namely the *WindowsAgent.SqlServer* extension. This extension, once installed, will detect any running SQL Servers and onboard them automatically to Arc.

## Student Lab Manual

### Table of Contents

Exercise 1 - Disconnect the Arc-enabled SQL Server instances from Azure Arc using Azure portal

[\*\*Task 1 - Uninstall Azure extension for SQL Server\*\*](#)

[\*\*Task 2 - Remove the Arc-enabled SQL Server\*\*](#)

Exercise 2 - Install SQL Server extension using offline MSI installer and using PowerShell remote execution

[\*\*Task 1 - Connect A SQL Server to Arc using remote Powershell\*\*](#)

# Exercise 1 - Disconnect the Arc-enabled SQL Server instances from Azure Arc using Azure portal

---

## **Objective**

In this exercise you will disconnect the SQL Servers from Arc so that you can practice with other methods of onboarding them at scale. You will keep the Windows Server machine that has the SQL Server installed on it connected to Arc, and you will only remove the SQL Server Arc registration.

## **Estimated Time to Complete This Exercise**

15 minutes

## Task 1: Uninstall Azure extension for SQL Server

1. From the Azure portal go to *Azure Arc* page and select the *All Azure Arc Resources* option. Select the *ArcBox-SQL* machine hosting a SQL server

The screenshot shows the 'Azure Arc | All Azure Arc resources' page. On the left, there's a navigation sidebar with options like Overview, Management, Extended Security Updates, Custom locations, Data controllers, and Machine. The main area displays a table with three records. The first record, 'ArcBox-SQL', is selected and highlighted with a red box. The columns in the table are Name, Resource group, and Location.

Name	Resource group	Location
ARCBOX-SQL	Arctis	East US
ARCBOX-SQL	Arctis	East US
Arctis-Main-ET	Arctis	East US

2. On the Server page , under *Extensions* select the *WindowsAgent.SqlServer* extension and then click *Uninstall*. Confirm the request.

The screenshot shows the 'Machine - Azure Arc' page. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Connect, Windows Admin Center (preview), Security, Extensions (highlighted with a red box and labeled 1), Properties, Locks, Operations, Policies, Machine Configuration, Automigrate, SQL Server Configuration, and Helpdesk. The main area shows a list of extensions. The 'WindowsAgent.SqlServer' extension is selected and highlighted with a red box (labeled 2). The 'Uninstall' button is highlighted with a red box and labeled with a red number 3.

Name	Type	Version	Update available	Status
ChangeTracking Windows	ChangeTracking Windows	2.20.0.0	No	Succeeded
MDS Windows	MDS Windows	1.9.3	No	Succeeded
<b>WindowsAgent.SqlServer</b>	WindowsAgent.SqlServer	1.12504.99	No	Succeeded

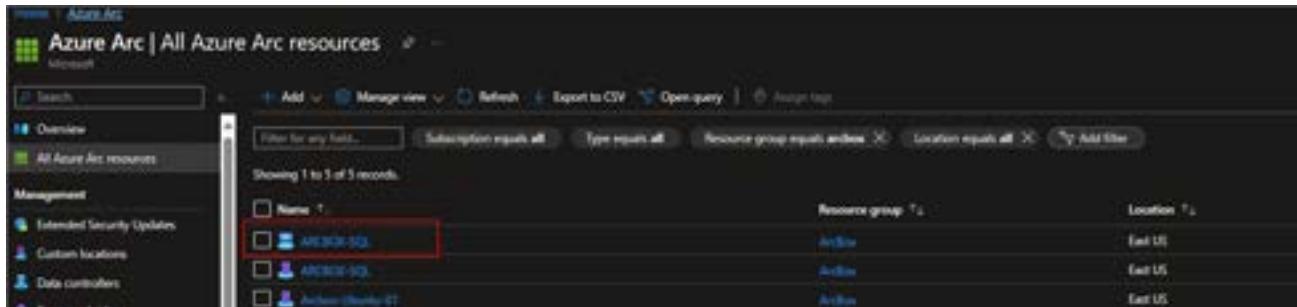
3. Wait for the Agent to be uninstalled and disappear from the list of extensions.

### Task 1 has been completed

Click **Next** for the next exercise or [Go back to the main table of content](#)

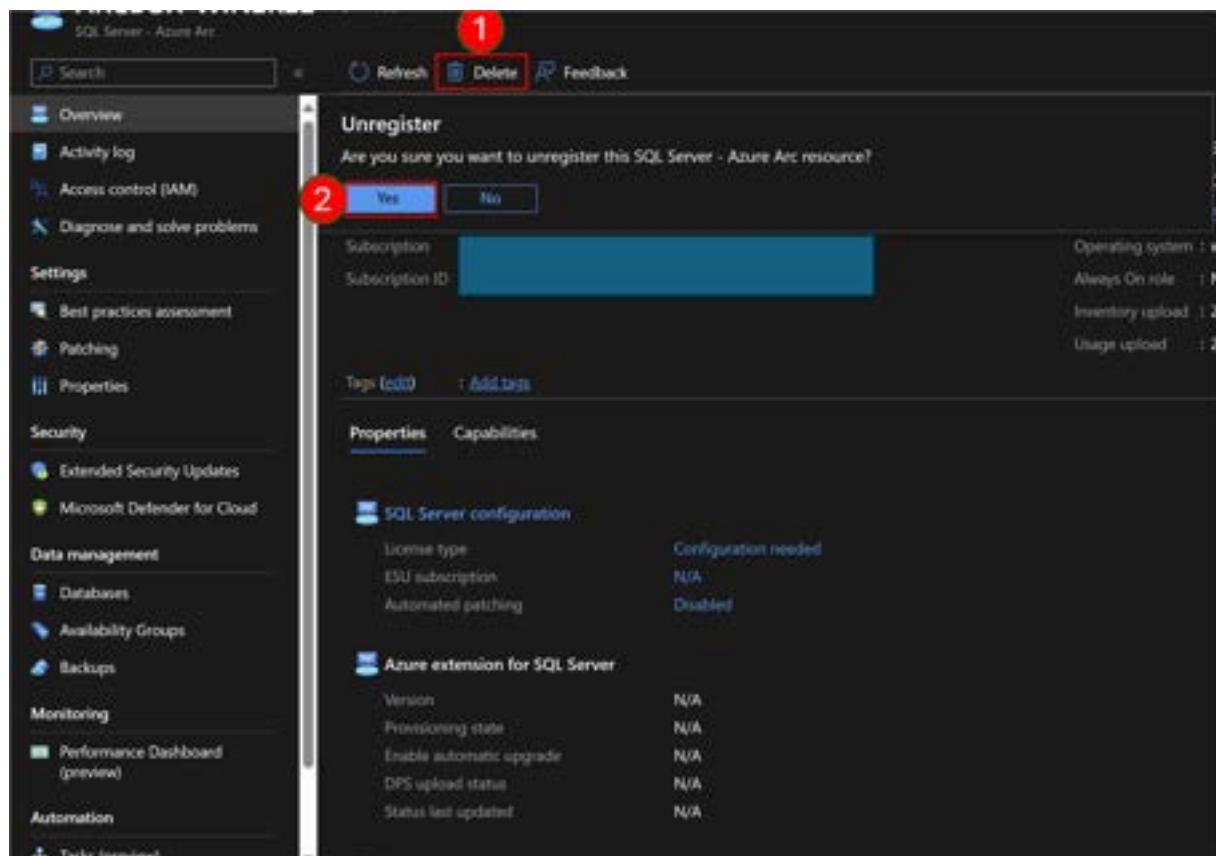
## Task 2: Remove the Arc-enabled SQL Server

1. From the Azure portal go to the *Azure Arc* page and select the *All Azure Arc Resources* option. Select the SQL Server *ArcBox-SQL*



The screenshot shows the Azure Arc - All Azure Arc resources page. The left sidebar has sections like Overview, Management, and Data controllers. The main area lists three resources: 'ArcBox-SQL' (selected), 'ArcBox-SQL', and 'ArcBox-SQL'. Each resource has columns for Name, Resource group, and Location.

2. Click on the Delete tab and Confirm that you want to unregister the resource when prompted



The screenshot shows the SQL Server - Azure Arc resource details page. The left sidebar includes sections like Overview, Activity log, and Properties. The main area shows resource details: Subscription ID, Tags, Properties, and Capabilities. A modal dialog titled 'Unregister' asks 'Are you sure you want to unregister this SQL Server - Azure Arc resource?'. The 'Yes' button is highlighted with a red circle.

**Task 2 has been completed**

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Exercise 2 - Install SQL Server extension using offline MSI installer and using PowerShell remote execution

---

### **Objective**

There are many ways to install SQL server extension depending on the your preference. In this module you will learn how to install SQL Server extension using offline MSI installer and using PowerShell remoting.

### **Estimated Time to Complete This Exercise**

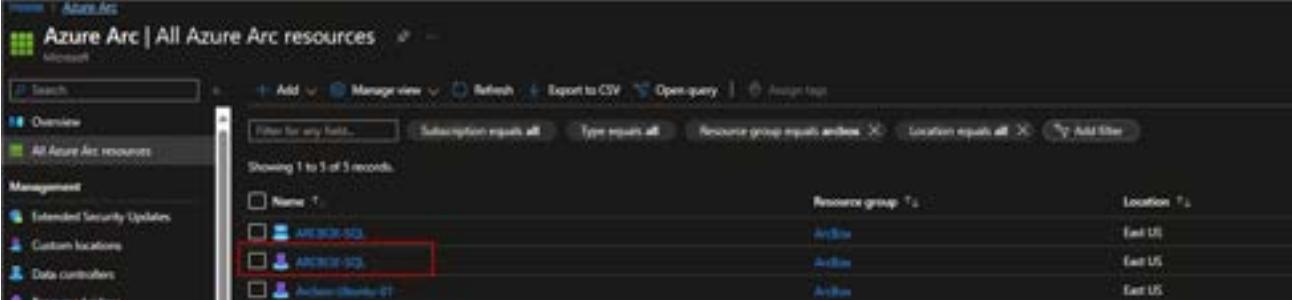
30 minutes

## Task 1: Connect A SQL Server to Arc using remote Powershell

- 1. Logon to ArcBox-Client VM, open Windows explorer and navigate to C:\ArcBox folder. Verify that the *InstallArcSQLExtensionAtScale.ps1* PowerShell script file exists.
- 2. Open *InstallArcSQLExtensionAtScale.ps1* in PowerShell ISE editor to review script. Note that the script attempts to download the .msi installer and then tries to run the installer on the list of servers (in this case only one server is specified, *ArcBox-SQL*). The action installs the *WindowsAgent.SqlServer* extension on the specified servers remotely.
- 3. Open PowerShell command line window and change directory to "C:\ArcBox" folder. Then run the following commands to install the SQL Server extension at scale , **after inserting the password JS123!! in the script.**

```
powershell  
▶ $secWindowsPassword = ConvertTo-SecureString "<Insert password before running>"  
  .\InstallArcSQLExtensionAtScale.ps1 -remoteWindowsAdminPassword $secWindowsPassw  
  
PS C:\ArcBox> .\InstallArcSQLExtensionAtScale.ps1 -remoteWindowsAdminPassword $secWindowsPassw  
Deploying ArcBox-Sql server to Azure Arc.  
Copying C:\ArcBox\AzureExtensions\InstallForSQLServer.msi on remote server.  
C:\ArcBox\AzureExtensions\InstallForSQLServer.msi file copied on remote server.  
Installing C:\ArcBox\AzureExtensions\InstallForSQLServer.msi file on remote server.  
Handles: 109 (K) 196 (X) 195 (K) CPU(s): 0 0.00 3828 0 released  
104 8 3848 1758 0.01 3828 0 released  
Installed C:\ArcBox\AzureExtensions\InstallForSQLServer.msi file on remote server.  
Installing Arc-enabled SQL Server extension on remote server.  
Authorisation successful.  
Uninstalling SQL Server from Azure Arc. It will take few minutes. Please see C:\Users\Administrator\Documents\AzureExtensionForSQLServerInstallation.log file for more information.  
Installing Azure Connected Machine Agent.  
Arc Server resource is already onboarded.  
Installing Azure Extension for SQL Server. This may take 5-6 minutes.
```

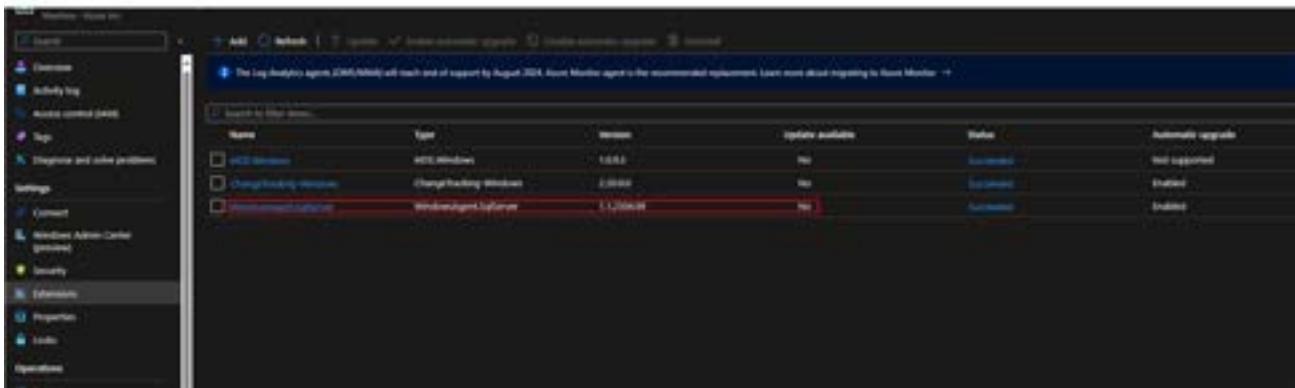
- 4. In case some of the servers are already onboarded to Arc, you might see a message indicating that the extension already exists. Otherwise the script will install the extension on the specified list of machines. Wait for the script execution to complete.
- 5. From the Azure portal go to *Azure Arc* page and select the *All Azure Arc Resources* option. Select the *ArcBox-SQL* machine hosting a SQL server.



The screenshot shows the Azure Arc | All Azure Arc resources page. The left sidebar has sections for Overview, All Azure Arc resources, Management, Extended Security Updates, Custom locations, Data controllers, and Premium support. The main area displays a table with three records:

Name	Resource group	TU	Location
ARCBX-SQ	ArcBox	T1	East US
ARCBX-SQ	ArcBox	T1	East US
ArcBox (Ubuntu 22)	ArcBox	T1	East US

- 6. On the Server page , under *Extensions* verify that the *WindowsAgent.SqlServer* extension has been re-installed.



- 7. From the Azure portal go to *Azure Arc* page and select the *All Azure Arc Resources* option. Verify that the *ArcBox-SQL* SQL Server is now Arc-enabled again.

Name	Resource group	Location
ArcBox-SQL	ArcBox	East US
ArcBox-SQ2	ArcBox	East US
ArcBox-SQ3	ArcBox	East US

**Task 1 has been completed**

---

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB14: Get insights on your Arc-enabled SQL Servers and Databases using the Azure Resource Graph

---

## Student Lab Manual

### Table of Contents

Exercise 1 - Collect insights on your SQL Server instances

**[Task 1 - Use the Azure Portal to examine your SQL servers and databases](#)**

**[Task 2 - Query SQL Servers and Databases using the Resource Graph Explorer](#)**

# Exercise 1 - Collect insights on your SQL Server instances

---

## **Objective**

In this exercise you will examine the Arc-enabled SQL Servers and the databases deployed on them.

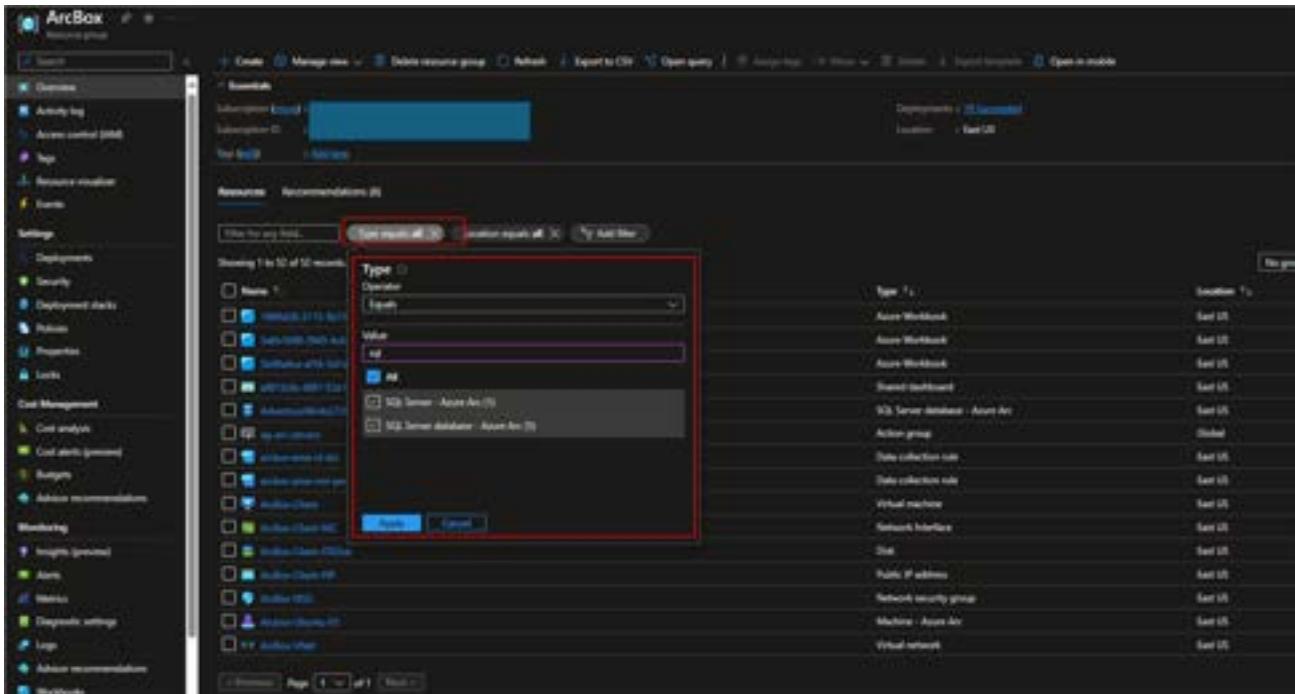
## **Estimated Time to Complete This Exercise**

30 minutes

## Task 1: Use the Azure Portal to examine your SQL servers and databases

---

- 1. From the Azure portal home page, look for Resource Groups and select the one where you have been using in this workshop. Review the of *SQL Server – Azure Arc* and *SQL Server database – Azure Arc* resources that have now been onboarded. To make it easier you can filter by type or order by Type



- 2. Your SQL Servers are displayed in the format *Server Instance* and your databases are in the format *Database (Server Instance/Database)* where *Instance* only applies for named instances

The screenshot shows the ArcBox Azure Resource Group interface. On the left, there's a navigation sidebar with categories like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings, Security, Deployment stacks, Policies, Properties, Locks, Cost Management, Budgets, Admin recommendations, Monitoring, Insights (preview), and Alerts. The main area has tabs for Overview, Activity log, and Resources. The Resources tab is active, displaying a list of resources. A search bar at the top of the list says "Type for any term" and "Type again 2 selected". A filter bar below it says "Showing 1 to 6 of 6 records" and "Show hidden types". The list itself has columns for Name, Type, and Location. One item is highlighted with a red box: "AdventureworksDW (ARCBOX SQL) [AdventureworksDW] [2019]" with Type "SQL Server database - Azure Arc" and Location "East US". Other items include "ARCBOX SQL" (Type "SQL Server - Azure Arc", Location "East US"), "master (ARCBOX SQL master)" (Type "SQL Server database - Azure Arc", Location "East US"), "model (ARCBOX SQL model)" (Type "SQL Server database - Azure Arc", Location "East US"), "msdb (ARCBOX SQL msdb)" (Type "SQL Server database - Azure Arc", Location "East US"), and "tempdb (ARCBOX SQL tempdb)" (Type "SQL Server database - Azure Arc", Location "East US").

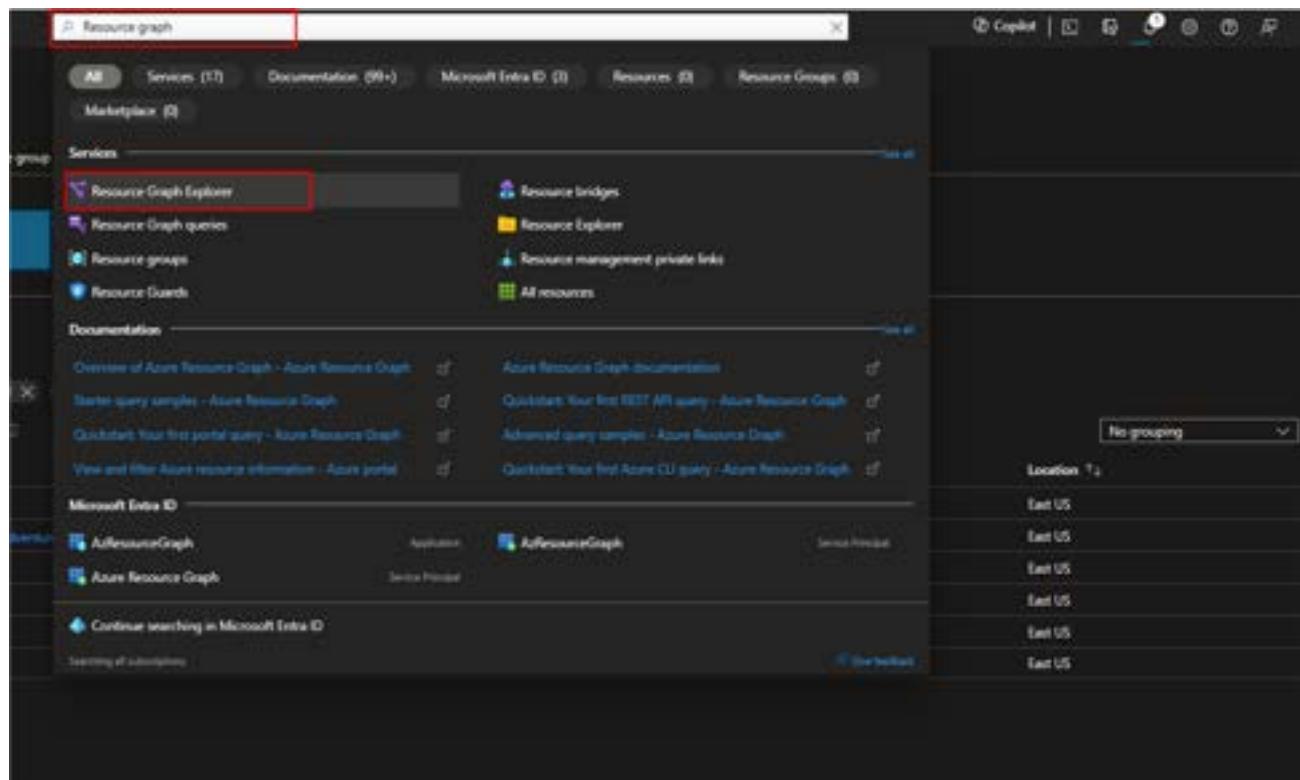
3. Click on any SQL server or database to examine further details and properties about them

### Task 1 has been completed

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Task 2: Query SQL Servers and Databases using the Resource Graph Explorer

- 1. From the Home page of the Azure portal, click on the search bar and type Resource graph and then select *Resource Graph Explorer*



- 2. Copy and paste the following into the Query window and then click *Run query*. It will list all of your Arc-Enabled SQL Servers by Resource group.

```
shell
▶ Resources
| where type == "microsoft.azurearcdata/sqlserverinstances"
| project name, resourceGroup, properties
```

The screenshot shows the Azure Resource Graph Explorer interface. A red box labeled '1' highlights the query editor at the top, which contains the following JSON query:

```
Resources  
| where type == "Microsoft.Sql/servers/instances"  
| project name, resourceGroup, properties
```

A red box labeled '2' highlights the 'Run query' button in the top navigation bar.

A red box labeled '3' highlights the 'See details' link next to the provisioningState value in the results table.

Name	Resource Group	Properties
ARCBX-SQL	arcbox	{ "provisioningState": "Succeeded", "status": "Connected", "version": "SQL Server 2019", "licenseType": "Free", "collation": "SQL_Latin1_General_CI_AS", "azureDefenderStatusLastUpdated": null, "azureDefenderStatus": "Unknown", "containerResourceId": "/subscriptions/.../resourcegroups/Ar...", "tcpDynamicPorts": 55... }

3. Examine the information displayed by the *See details* link

The screenshot shows the 'Details' modal window for the ARCBX-SQL resource. It displays three fields: 'name' (ARCBOX-SQL), 'resourceGroup' (arcbox), and 'properties'. The 'properties' field is expanded to show a JSON object with various properties. A red box highlights the 'See details' link next to the 'provisioningState' value.

name	resourceGroup	properties
ARCBOX-SQL	arcbox	<pre>1 { 2   "provisioningState": "Succeeded", 3   "status": "Connected", 4   "version": "SQL Server 2019", 5   "licenseType": "Free", 6   "collation": "SQL_Latin1_General_CI_AS", 7   "azureDefenderStatusLastUpdated": null, 8   "azureDefenderStatus": "Unknown", 9   "containerResourceId": "/subscriptions/.../resourcegroups/Ar...", 10  "tcpDynamicPorts": 55...</pre>

4. Run the following query to return details about your databases. Examine the results from clicking the *See details* link for each database

```
shell
```

```
▶ Resources
| where type == "microsoft.azurearcdata/sqlserverinstances/databases"
| project id, name, resourceGroup, properties
```

ID	Name	Resource Group	Properties
subscriptions...AdventureworksLT	AdventureworksLT	AdventureworksLT	{processingState:"Succeeded", databaseCreate... See details
subscriptions...master	master	AdventureworksLT	{processingState:"Succeeded", databaseCreate... See details
subscriptions...model	model	AdventureworksLT	{processingState:"Succeeded", databaseCreate... See details
subscriptions...tempdb	tempdb	AdventureworksLT	{processingState:"Succeeded", databaseCreate... See details

5. Click on the See details links to provide a better view of the properties for each database in the result set
6. Run the following query to show the compatibility levels of the databases on all your Arc-enabled servers

```
shell
```

```
▶ resources
| where type == "microsoft.azurearcdata/sqlserverinstances"
| project InstanceId = id, InstanceName = name, Version = tostring(properties.ver...
| join kind = inner (
resources
| where type == "microsoft.azurearcdata/sqlserverinstances/databases"
| where name !in ("master", "model", "msdb", "tempdb")
| project InstanceId = substring(id, 0, indexof(id, "Databases", 0) - 1), DatabaseName = value, Compatibl...
) on InstanceId
| project InstanceName, DatabaseName, CompatibilityLevel = strcat(Version, " - L")
```

**Task 2 has been completed**

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB15: Enable and run SQL Server best practices assessment

---

Best practices assessment provides a mechanism to evaluate the configuration of your SQL Server. After you enable best practices assessment, an assessment scans your SQL Server instance and databases to provide recommendations for things like:

- SQL Server and database configurations
- Index management
- Deprecated features
- Enabled or missing trace flags
- Statistics
- & more

## Student Lab Manual

### Table of Contents

#### Exercise 1 - Carry out SQL Server Best Practices Assessment

##### **Task 1 - Prerequisites**

##### **Task 2 - Enable and run SQL Server best practices assessment**

#### Exercise 2 - View Assessment Results

##### **Task 1 - View and resolve assessment issues**

##### **Task 2 - Use Log Queries with Assessment results**

# Exercise 1 - Carry out SQL Server Best Practices Assessment

---

## **Objective**

In this exercise you will set up and execute SQL Server Best Practices Assessment for your Arc-enabled SQL Server.

## **Estimated Time to Complete This Exercise**

30 minutes

# Task 1: SQL Server Best Practice Assessment Prerequisites

- 1. Make Sure that your SQL Server instance is connected to Azure Arc. From Azure portal go the *Azure Arc* page and select *SQL Server instances*. You should see the *ArcBox-SQL* SQL server connected.

The screenshot shows the Azure Arc | SQL Server instances page. On the left, there's a navigation menu with sections like Service principals, Private link resources, Infrastructure (Machine, Azure Arc virtual machines (preview), Azure Stack HD, Kubernetes clusters, VMware vCenters, SCVMM management servers), Data services (SQL Server instances, PostgreSQL (preview), SQL managed instances), Application Services (API management (preview), App services (preview), Event Grid topics (preview)), and Monitoring (Metrics, Log Analytics). The 'SQL Server instances' section is selected. In the main pane, it says 'Showing 1 to 1 of 1 records.' and lists one item: 'Name: ArcBox-SQL' with 'Status: Connected'. A red box highlights the 'Connected' status.

- 2. Make sure that you have a Log Analytics workspace deployed in your resource group so that you can upload assessment results to it. The set-up scripts for this workshop should have set up one for you already in your lab resource group.

The screenshot shows the ArcBox Resource Group page. The left sidebar has sections like Overview, Activity log, Access control (IAM), Tags, Resource visualizer, Events, Settings (Deployments, Security, Deployment stacks, Policies, Properties, Locks), Cost Management (Cost analysis, Cost alerts (preview), Budgets, Advisor recommendations), and Monitoring (Insights (preview)). The 'Overview' tab is selected. In the main pane, it shows a table of resources under the 'Resources' tab. One row is highlighted with a red box: 'Name: ALWS01' (Type: Log Analytics workspace, Location: East US).

- 3. Make sure that you have the following roles enabled and active **on the Resource Group Level** : *Monitoring Contributor, Log Analytics Contributor and Azure Connected Machine Resource Administrator*. If these roles are not enabled then go to the \_Access Control (IAM) tab on the Resource Group page and enable them **making sure to set the Assignment Type to Active**.

Home > Resource groups > ArcBox

## assignments - ArcBox

ArcBox | Access control (IAM) Resource group

Search

Overview Activity log Access control (IAM) Tags Resource visualizer Events Settings Deployments Security Deployment stacks Policies Properties

Current role assignments Eligible assignments

Assignments for the selected user, group, service principal, or managed identity at this scope or inherited to this scope.

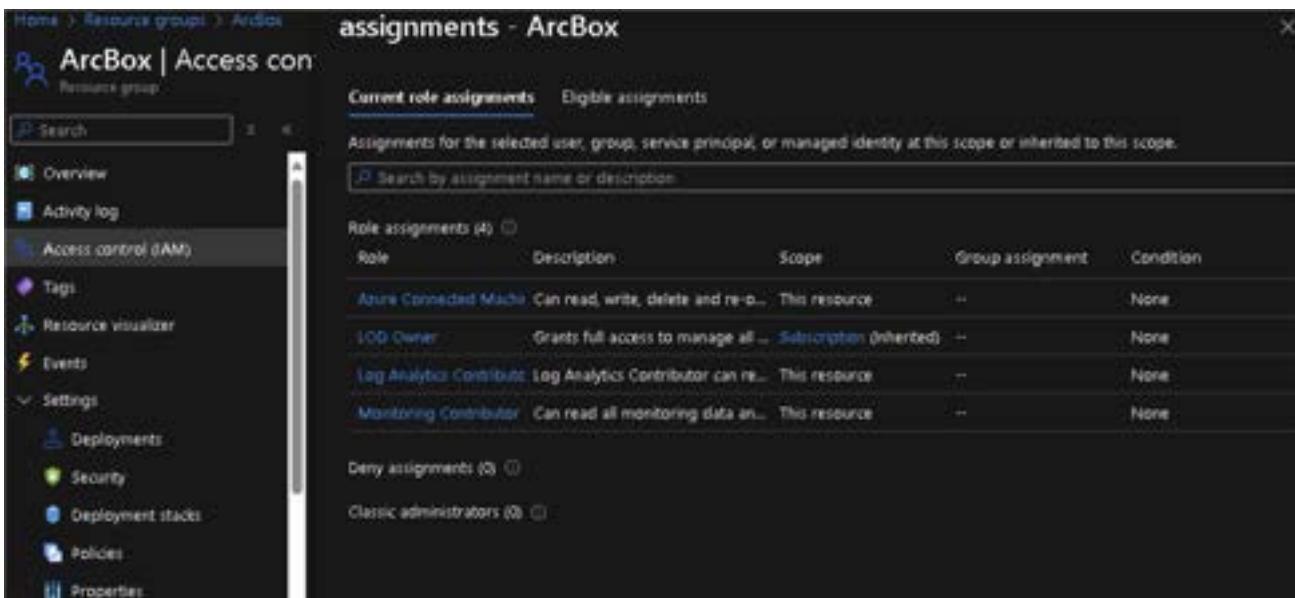
Search by assignment name or description

Role assignments (4)

Role	Description	Scope	Group assignment	Condition
Azure Connected Machine	Can read, write, delete and re-p... This resource	--		None
Log Owner	Grants full access to manage all ... Subscription (inherited)	--		None
Log Analytics Contributor	Log Analytics Contributor can re... This resource	--		None
Monitoring Contributor	Can read all monitoring data in... This resource	--		None

Deny assignments (0)

Classic administrators (0)



**Task 1 has been completed**

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Task 2: Enable and run SQL Server best practices assessment

---

- 1. Go to your Arc-enabled SQL Server resource and click on the *Best Practices Assessment* under the *Setting* menu. If you are asked for a license type then follow the portal instructions and assign a PAYG license.

The screenshot shows the Azure portal interface for an Arc-enabled SQL Server resource named 'ARCBOX-SQL'. The left sidebar lists various settings like Overview, Activity log, and Best practices assessment. The 'Best practices assessment' item is highlighted with a red box. The main content area displays the resource's properties, including its version (SQL Server 2019), edition (Developer), and computer name (ArcBoxSQL). It also shows patching details (License type: Pay-as-you-go, ESM subscription: N/A, Automated patching: Disabled) and Azure extension for SQL Server information (Version: 1.1.2512.104, Provisioning state: Succeeded, Status last updated: 05/12/2023, 23:59:26 GMT). At the bottom, it shows the status of the Azure Connected Machine agent (Agent status: Connected).

- 2. Select the log analytics workspace that you have in the same subscription as your Arc-enabled SQL Server resource and click on *Enable Assessment*.

The screenshot shows the Azure portal interface for the 'ARCBOX-SQL' resource group. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Diagnose and solve problems, Settings (with 'Best practices assessment' highlighted by a red box and circled with a red number 1), Patching, Properties, Security, Data management, Monitoring, and Automation. The main content area is titled 'Best practices assessment' and contains the following information:

- Assessment status:** Disabled (highlighted by a red box and circled with a red number 2).
- Log Analytics Workspace:** ARROWS (highlighted by a red box and circled with a red number 2).
- Assessment schedule frequency:** None (Enable assessment to schedule) (highlighted by a red box and circled with a red number 3).
- Assessment results:** The results of previous assessments.
- Start date:** No results.
- Status:**

- 3. Wait until Best Practice Assessment is enabled which might take few minutes. Once the deployment of the best practice assessment is completed you can either start the assessment manually or you can use the *Configuration* option to either schedule or disable the assessment. Examine the *Configuration* settings **but do not click Schedule assessment** as you will use the manual option in this lab. Close the *Configuration* settings.

This screenshot shows the same 'Best practices assessment' page after the configuration changes have been applied. A prominent blue progress bar at the top says 'Please wait while assessment settings are being activated'. The rest of the page remains largely the same, with the 'Assessment status' now showing 'Enabled' and the 'Schedule assessment' section showing the following configuration:

- Frequency:** Monthly (selected)
- Day of week:** Monday
- Recurrence:** Every 1 week(s)
- Assessment start (local machine time):** (dropdown menu)

A 'Schedule assessment' button is located at the bottom of this section.

- 4. Click *Run assessment* to manually start the assessment. You should see the progress indicator after a couple of minutes. Note that the assessment will take a bit of time to complete and you might need to refresh the page to see the results.

ARCBOX-SQL | Best practices assessment

SQL Server - Azure Arc

Run assessment Refresh Configuration Feedback

Overview

Activity log

Access control (IAM)

Diagnose and solve problems

Settings

Best practices assessment

Patching

Properties

Security

- Extended Security Updates
- Microsoft Defender for Cloud

Data management

- Databases
- Availability Groups
- Backups

Monitoring

- Performance Dashboard (preview)

Autoscale

Best practices assessment

The best practices assessment continuously scans all your SQL Server instances and databases on the host machine and evaluates the configurations for SQL Server best practices. Learn more

Assessment status: Enabled

Log Analytics workspace: None

Assessment schedule frequency: The assessment is scheduled weekly at 00:00 (local machine time), for every 1 week(s) on Sunday.

Assessment results

The results of previous assessments

Start date	Status
2023-12-09 08:00 AM UTC	Scheduled
2023-12-06 01:21 PM UTC	In Progress - running assessment

## Task 2 has been completed

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Exercise 2 - Work with Best Practices Assessment results

---

### **Estimated Time to Complete This Exercise**

45 minutes

## Task 1: View and resolve assessment issues

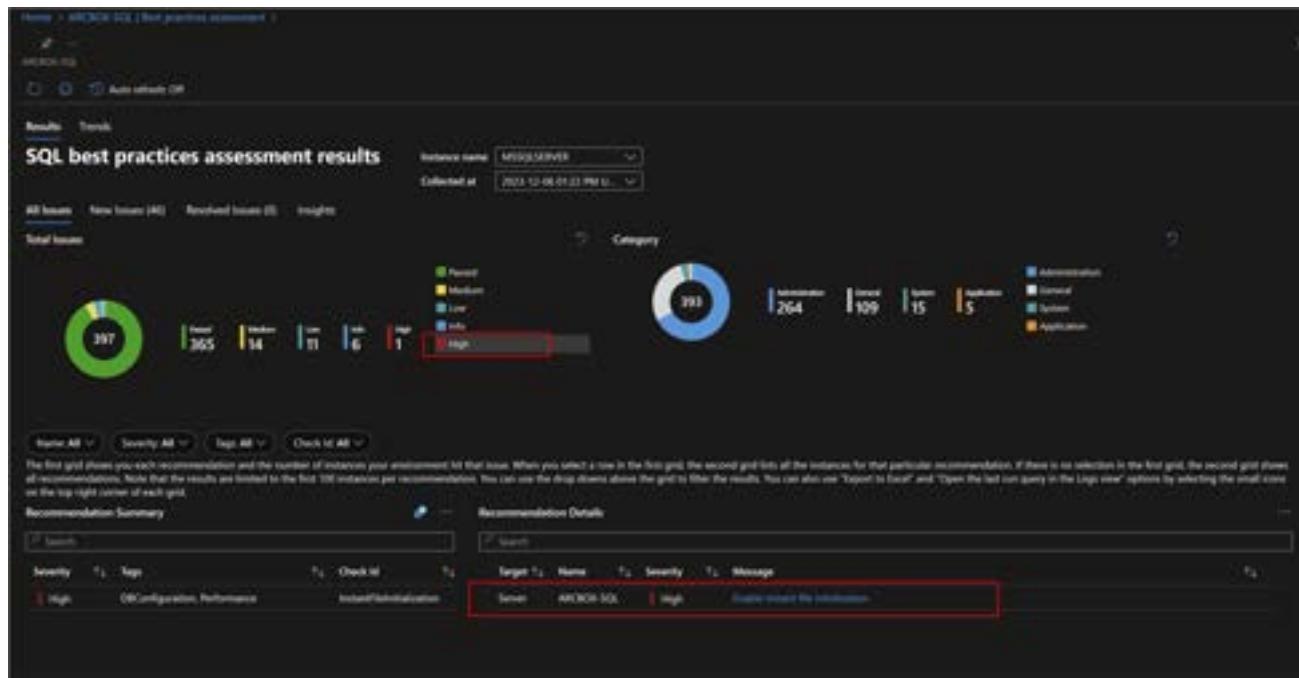
1. Once the assessment is completed, click on the assessment to move to the results screen.

The screenshot shows the 'Best practices assessment' page for the 'ARCBOX-SQL' resource. The left sidebar lists various settings like Overview, Activity log, Access control (IAM), Diagnosis and solve problems, and Best practices assessment (which is selected). The main area displays the 'Assessment status' as 'Completed'. It shows the start date as '2023-12-10 08:00 AM UTC' and the status as 'Completed'. A red box highlights the 'Completed' status.

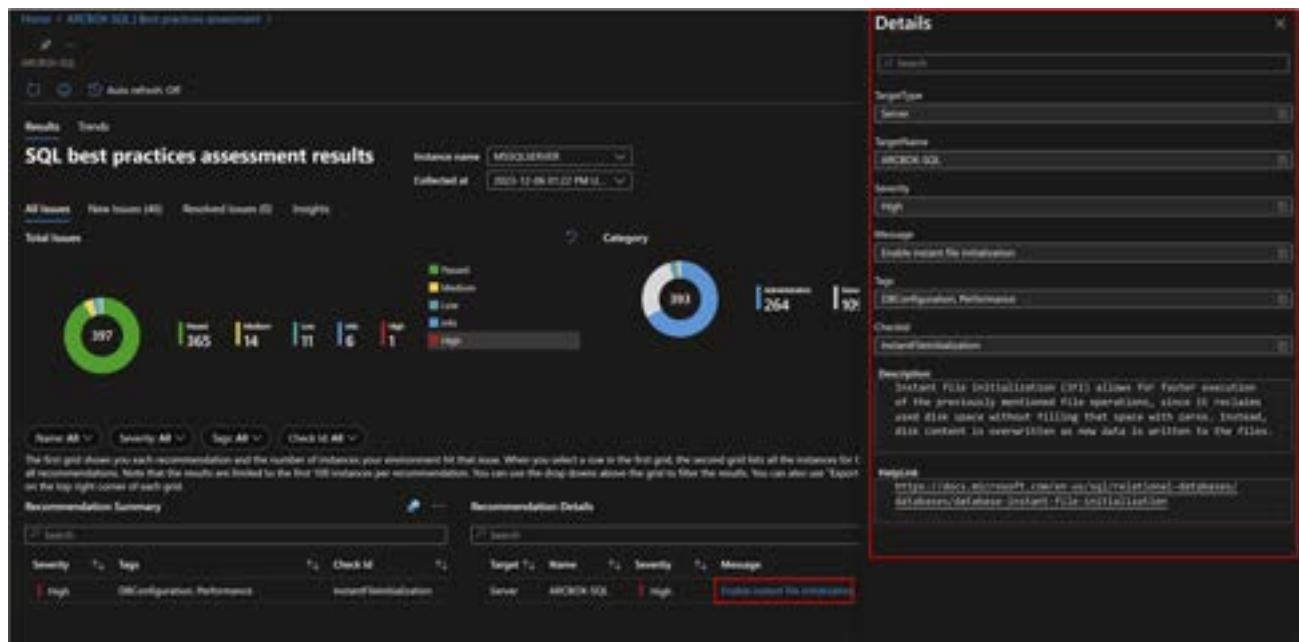
2. On the Results page, if there are several assessments that are completed, you can choose from *Collected at* dropdown menu. The Results page reports all the issues categorized based on their severity. The recommendations are organized into All, New and Resolved tabs. The tabs can be used to view all the recommendations from the currently selected run, the newer recommendations compared to the previous run, and the resolved recommendations from the previous runs respectively. The tabs help to keep track of the progress between the runs.

The screenshot shows the 'SQL best practices assessment results' page for the 'MSSQLSERVER' instance. The top section displays the instance name, collection time, and a summary of findings: 397 total issues (365 New, 34 Medium, 11 Low, 6 Info, 1 High). Below this is a 'Recommendation Summary' grid showing recommendations categorized by severity (High, Medium, Low, Info, High) and target (Server, Database). The 'High' category has one entry: 'Check ID: 200 Configuration, Performance' with 'Target T1: Server' and 'Message: Update recent file relocations'. The 'Medium' category has four entries: 'Index, Performance' (Target T1: Server, Message: Review SQL Server and index statistics and consider using 'Compute' columnstore index), 'I/O, Performance, Resource' (Target T1: Database, Message: Optimize page size for higher I/O), 'Index, Performance' (Target T1: Database, Message: Create 'clustered' or 'nonclustered' indexes on primary key or foreign key columns to increase), and 'Index fragmentation' (Target T1: Database, Message: Create 'clustered' or 'nonclustered' indexes on primary key or foreign key columns to increase).

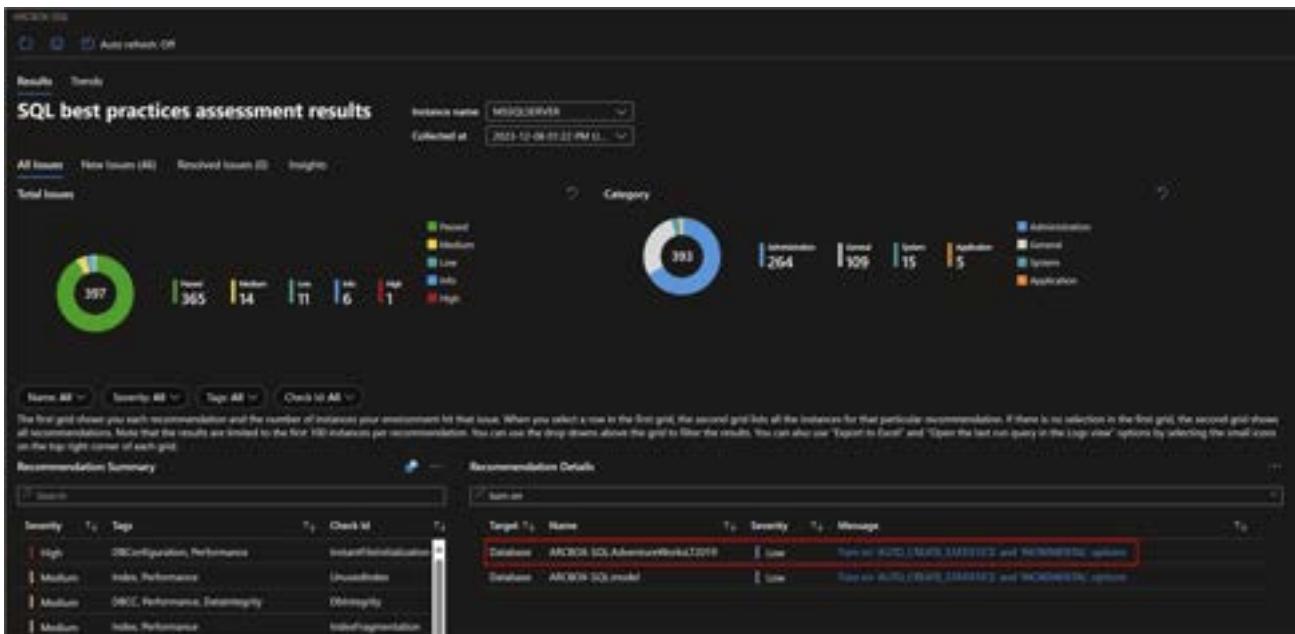
3. To filter the issues by high severity, click on "High" on the Total Issues chart. To clear the filter click on high once again. Filtering can be applied by categories as well.



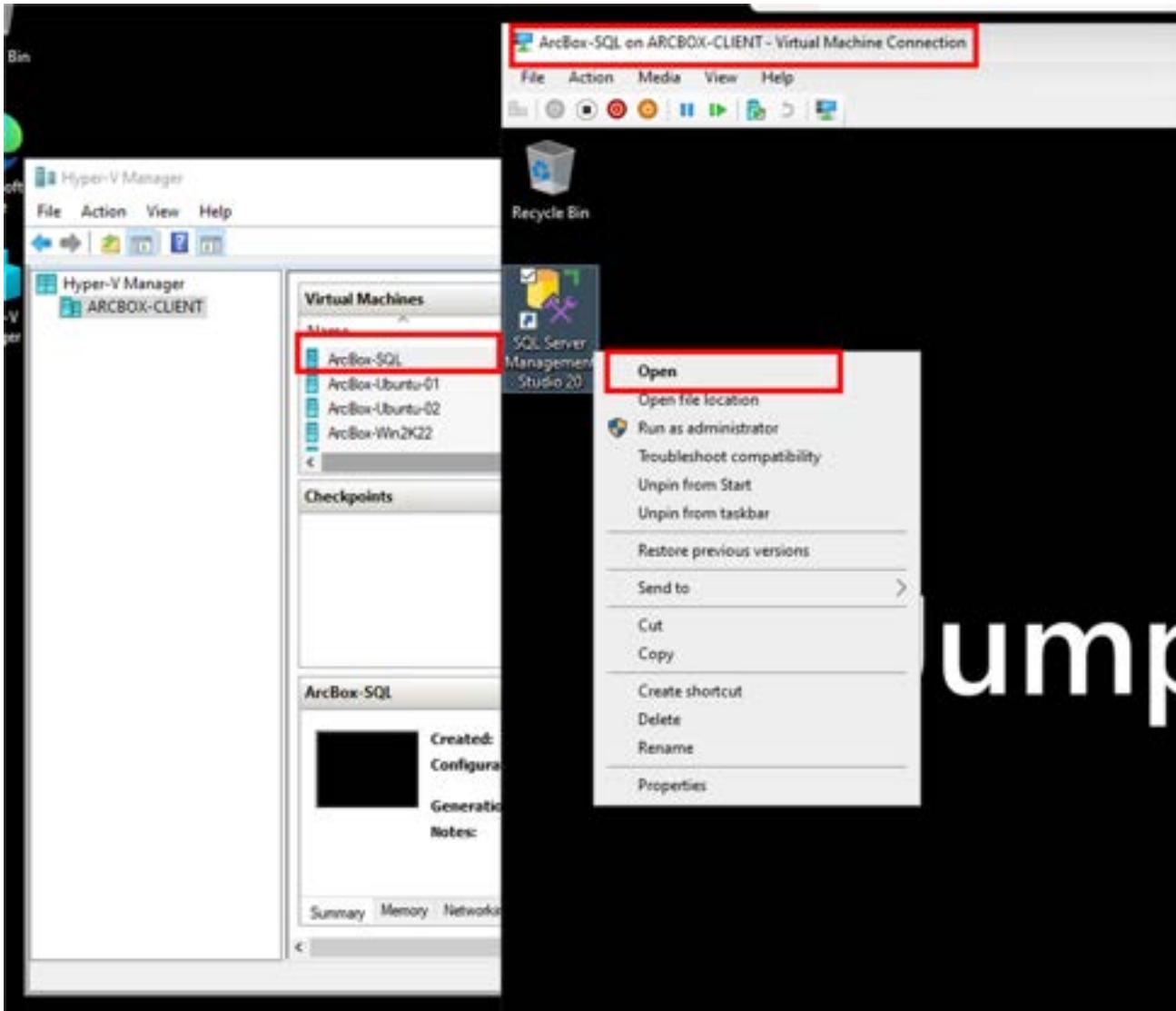
4. To view details for a recommendation, in the recommendation summary menu click on the high severity issue, then in the *Recommendation Details* table click on the message item.



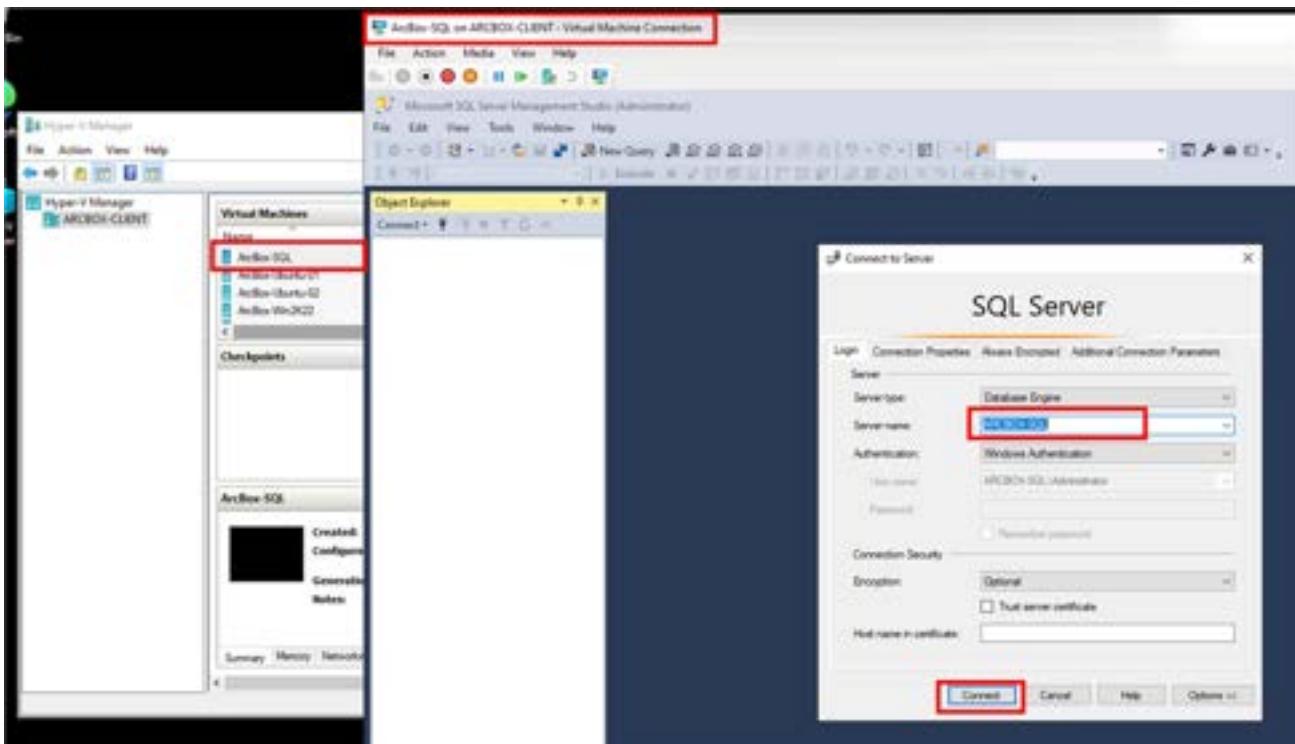
5. You are going to address a specific recommendation now. Remove any filters and scroll through the *Recommendation Details* table (or use the associated search field) to find the issue "Turn on 'Auto\_Create\_Statistics' and 'Incremental' options" for the AdventureWorks database.



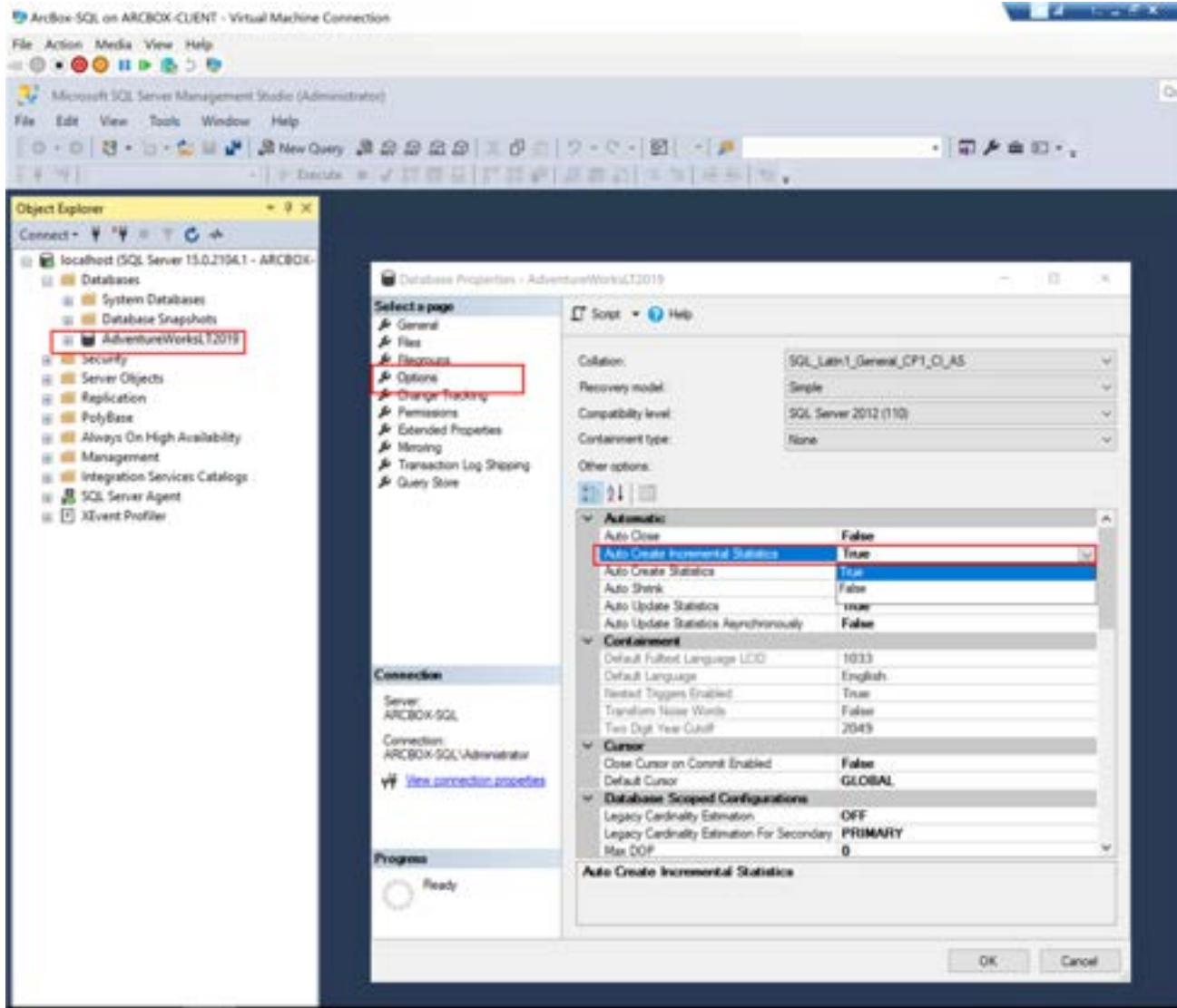
- 6. To Fix the issue "Turn on 'Auto\_Create\_Statistics' and 'Incremental' options", logon to the ArcBox-Client\_machine and connect to ArcBox-SQL from the Hyper-V console (password JS123!!). Start the *SQL Server Management Studio* application and connect to the SQL Server instance.



- 7. Connect to the SQL Server instance



- 8. Right-Click on the *AdventureWorksLT2019* database and select the *Properties* then *Options*. Find the *Auto Create Incremental Statistics* option and change it from False to True. Confirm your action by clicking *OK*.



- 9. Rerun assessment and check the resolved issues. (To re-run the assessment, go to the *Best practices assessment* page on the Arc-enabled SQL Server in the Azure portal as you did in the previous exercise). Once the new assessment is complete, go the *Resolved Issues* tab and check that your issues has been resolved.

Home - ARCON SQL | Best practices assessment |

ARCON SQL

Add refresh off

Results Trends

**SQL best practices assessment results**

Instance name: ARCON-SERVER  
Collected at: 2023-12-06 00:29 PM U...

All issues New issues (0) Resolved issues (3) Insights

3 Low 2 Medium 1 High

Search

Target	TargetName	T	Severity	T	Message	T	Tags	T	CheckID
Server	ARCON-SQL	1	Medium	Enable Optimized for Active and Standby servers on heavy OLTP Ad-Hoc workload to conserve memory. Performance, QueryOptimizer					PlanOptimizer
Server	ARCON-SQL	1	Low	Use robust practices for SQL Server version 16.0.2104 instead of found deprecated features. Syntax, Deprecated, Security, UpdateIssues, Performance					DegradedFeatures
Database	ARCON-SQLAdventureworksDW	1	Low	Turn on AUTO_CREATE_STATISTICS and AUTO_UPDATE_STATISTICS options.					AutoCreateStatistics

### Task 1 has been completed

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Task 2: Use Log Queries with Assessment results

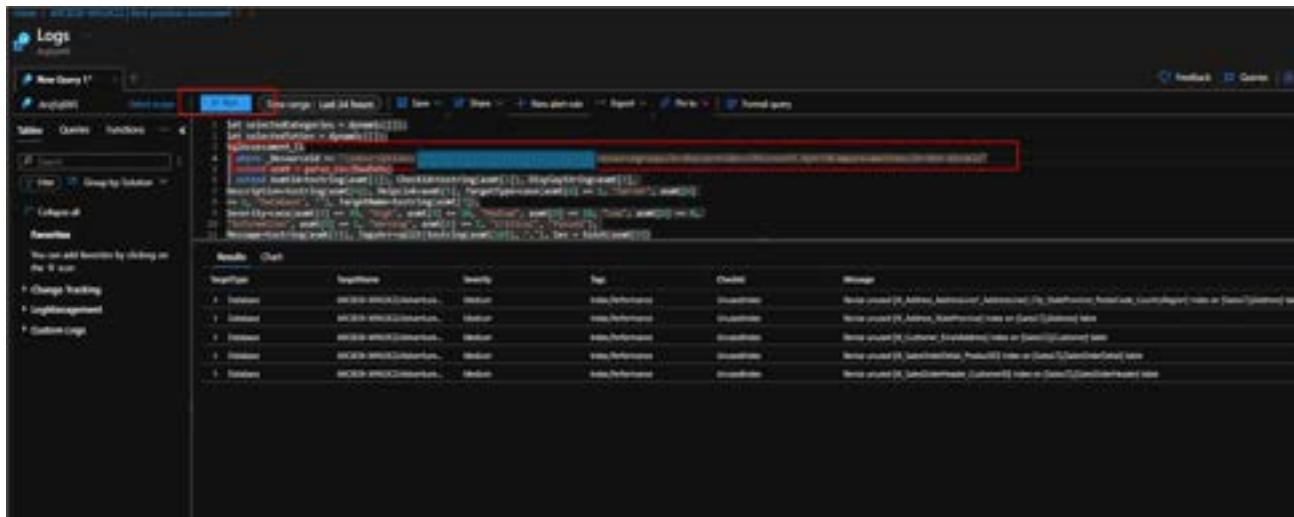
- 1. You can get more detailed insights using Log Analytics Queries. Click on *Query logs* on the top of the grid in assessment results, this will take you to query editor.

- 2. Click *Select scope* and then Select the specific "Log Analytics workspace" used for uploading assessment data from Arc-enabled SQL Server and click *Apply*.

- 3. Query the logs to gain more insights into your SQL Server environment. For example, you can use the following query to identify all unused indexes in a specific instance. Enter the Subscription Id

and Resource group name in the forth line of the query then paste the query into the Query pane and click the *Run* button. Then view the results of your query.

```
▶ shell
let selectedCategories = dynamic([]);
let selectedTotSev = dynamic([]);
SqlAssessment_CL
| where _ResourceId =~ "/subscriptions/XXXXXXXXXXXX/resourcegroups/XXXX/provider
| extend asmt = parse_csv(RawData)
| extend AsmtId=tostring(asmt[1]), CheckId=tostring(asmt[2]), DisplayString=asmt
Description=tostring(asmt[4]), HelpLink=asmt[5], TargetType=case(asmt[6] == 1, "
== 2, "Database", ""), TargetName=tostring(asmt[7]),
Severity=case(asmt[8] == 30, "High", asmt[8] == 20, "Medium", asmt[8] == 10, "Lo
"Information", asmt[8] == 1, "Warning", asmt[8] == 2, "Critical", "Passed"),
Message=tostring(asmt[9]), TagsArr=split(tostring(asmt[10]), ","), Sev = toint(a
| where CheckId == "UnusedIndex"
| project
TargetType,
TargetName,
Severity,
Tags=strcat_array(array_slice(TagsArr, 1, -1), ','),
CheckId,
Message
| distinct *
```



## **Task 2 has been completed**

Click **Next** for the next lab or [Go back to the main table of content](#)

# LAB16: Protect your Arc-enabled SQL Server with Microsoft Defender for Cloud

---

## Student Lab Manual

### Table of Contents

Exercise 1 - Enable Defender for Cloud for SQL Server on machines

**Task 1 - Enable Defender for Cloud to protect your Arc-enabled SQL servers at the subscription level**

**Task 2 - Enable Defender for Cloud to protect a specific Arc-enabled SQL server**

Exercise 2 - Generate Defender for Cloud Incidents and Alerts

**Task 1 - Simulate security incidents**

# Exercise 1 - Enable Defender for Cloud for SQL Server on machines

---

## **Objective**

In this exercise you will learn how to enable the Azure Defender for Cloud service to protect your Arc-enabled SQL server.

## **Estimated Time to Complete This Exercise**

30 minutes

## Task 1: Enable Defender for Cloud to protect your Arc-enabled SQL servers at the subscription level

- 1. In the Azure Portal search for *Microsoft Defender for Cloud* and select it from the search results

The screenshot shows the Azure Portal search results for the query "defender". The search bar at the top contains "defender". Below the search bar, there are several categories: "All", "Services (3)", "Resources (1)", "Marketplace (31)", "Documentation (99+)", and "Microsoft Entra ID (31)". The "Services" section is expanded, showing "Microsoft Defender EASM" and "Microsoft Defender for Cloud". "Microsoft Defender for Cloud" is highlighted with a red box. Other services listed include Microsoft Defender for IoT, Microsoft Defender for Endpoint, MDR for Microsoft 365 Defender, Microsoft Defender for SQL Server, Microsoft Sentinel and Microsoft 365 Defender SOC (MDR), Microsoft Defender for Endpoint Managed Services (MDR), Cyber Care - Managed Azure Defender, Microsoft Defender for Identity solution for Sentinel, and Microsoft Defender Threat Intelligence. The "Documentation" section lists various articles related to Microsoft Defender for Cloud, such as "Microsoft Defender for Resource Manager - the benefits and features", "Protect your servers with Defender for Servers - Microsoft Defender", "Microsoft Defender for Azure SQL - the benefits and features - Microsoft Defender", "Overview of the extensions that collect data from your workloads - Microsoft Defender", "Connect on-premises machines - Microsoft Defender for Cloud", "Understand just-in-time virtual machine access - Microsoft Defender", "Enable and configure Microsoft Defender for Storage (classic) - Microsoft Defender", and "Release notes - Microsoft Defender for Cloud". The "Microsoft Entra ID" section shows service principals for "DefenderWorkflow", "defendersql1", "defendersql2", and "DefenderForInt". At the bottom, there is a link to "Continue searching in Microsoft Entra ID" and a "Give feedback" button.

- 2. From the *Microsoft Defender for Cloud* page select *Environment settings* and under the hierarchy select your subscription

The screenshot shows the Microsoft Defender for Cloud Environment settings page. On the left, there's a navigation sidebar with sections like General, Cloud security, and Management. Under Management, 'Environment settings' is highlighted with a red box. The main area displays various metrics and a list of resources. At the top right, there are four cards: Governance rules, Data sensitivity, Direct onboarding, and Integrations. Below these are summary counts for Azure subscriptions (1), AWS accounts (0), GCP projects (0), GitHub connections (0), Azure DevOps connections (0), and GitLab connections (0). A search bar and filters for environments, standards, coverage, and connectivity status are present. The main list shows items like 'Name: T4' and 'Alerts' under 'Tenant Root Group (1 of 1 subscriptions)'. A specific row for 'MCAPS-Root (1 of 1 subscriptions)' has a red box around its monitoring coverage status.

- 3. On the subscription Defender plans settings set the *Status* to *On* if it is not set already. Then click on *Settings* under the *Monitoring coverage* column

The screenshot shows the 'Settings & monitoring' page. The left sidebar includes options like Defender plans, Security policies, Audit notifications, Monitor automation, and Extended log. Under 'Defender plans', there's a section for 'Cloud workload protection plan'. The main table lists various cloud services with their monitoring coverage status. One row for 'Sql' has a red box around its 'Monitoring coverage' status, which is currently set to 'Partial'. The 'Status' column for this row also has a red box around it, indicating it can be changed.

- 4. On the *Settings & monitoring* page set the *Status of the \_Azure Monitoring Agent for Sql server on machines* to *On*

The screenshot shows the 'Autoprov configuration' screen. It lists two components: 'Log Analytics agent' and 'Azure Monitoring Agent for SQL servers on machines'. Both components have checkboxes for 'Log Analytics workspace' and 'Azure Monitor workspace'. The 'Log Analytics workspace' checkboxes are highlighted with red boxes.

- 5. On the *Autoprov configuration* screen select the Log Analytics workspace, tick the option to *Register Azure SQL Server instances by enabling SQL IaaS extension automatic registration* then click *Apply*

The screenshot shows the 'Autoprov configuration' screen. In the 'Configure' section, there is a checkbox labeled 'Register Azure SQL Server instances by enabling SQL IaaS extension automatic registration'. This checkbox is highlighted with a red box.

- 6. Select *Continue* to save the settings

The screenshot shows the 'Autoprov configuration' screen. At the bottom right, there is a blue 'Continue' button which is highlighted with a red box.

7. Once you are back on the Defender plan settings page, click on *Select types* under the *Pricing* column

The screenshot shows the 'Settings | Defender plans' page in the Azure portal. The left sidebar has 'Defender plans' selected. The main area displays two sections: 'Cloud Workload Protection (CWP)' and 'Cloud Workload Protection (CWP) - preview'. Under 'Cloud Workload Protection (CWP)', there is a table with columns: Plan, Pricing, Resource quantity, Monitoring coverage, and Status. One row is highlighted with a red box around the 'Selected' checkbox in the 'Selected types' column for the 'Selected' plan.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Selected	Plan 2 (\$11/Server Month) Cloud Workload Protection	21 servers	Partial (Coverage)	<span>On</span>
App Service	\$10/Month/Unit Cloud Workload Protection	1 instances	Full	<span>On</span>
Database	\$200/1TB Transactions Cloud Workload Protection	Protected 1/TB databases	Full	<span>On</span>
Storage	\$10/1TB Month Cloud Workload Protection	1 storage accounts	Full	<span>On</span>
Container	\$200/1GB Month Cloud Workload Protection	1 container registries (10 containers used)	Partial (Coverage)	<span>On</span>
File storage (previewed)	\$10/1TB Month	1 file storage accounts	Full	<span>On</span>
Content Delivery (previewed)	\$1.25/Usage	1 content delivery endpoints	Full	<span>On</span>
Key Vault	\$200/1TB Transactions	1 key vaults	Full	<span>On</span>

8. Make sure that the *SQL servers on machines* option is set to *On*, then click *Continue*

## Resource types selection



Defender for cloud offers protection for a variety of database resource types, both SQL servers and managed cloud database services. [Learn more](#)



### Azure SQL Databases ⓘ

Pricing:

\$15/Server/Month

Resource quantity:

0 servers



### SQL servers on machines ⓘ

Pricing:

\$15/Server/Month - servers in Azure

\$0.015/Core/Hour - servers outside Azure

Resource quantity:

1 servers



### Open-source relational databases ⓘ

Pricing:

\$15/Server/Month

Resource quantity:

0 servers



### Azure Cosmos DB ⓘ

Pricing:

\$0.0012 per 100RU/s per hour

Resource quantity:

0 Azure Cosmos DB accounts



9. Save the Settings for Defender

The screenshot shows the 'Settings | Defender plans' page. On the left, there's a sidebar with options: 'Defender plans' (selected), 'Defender policies', 'Email notifications', 'Endpoint detection', and 'Compliance report'. The main area has tabs for 'Plans' (selected) and 'Settings & monitoring'. Below is a table with columns: Plan, Priority, Resource quantity, Monitoring coverage, and Status. There are two sections: 'Cloud Workload Protection (CWP)' and 'Cloud Workload Protection (CWP) - Advanced'. The CWP section contains 10 items, and the CWP - Advanced section contains 10 items. Each item row includes a 'Details' link.

Plan	Priority	Resource quantity	Monitoring coverage	Status
Plan 1 (Windows Server - Legacy plan)	High	25 servers	Partial (warning)	<input type="button" value="Edit"/>
Plan 2 (Windows Server - Legacy plan)	Medium	5 servers	Full	<input type="button" value="Edit"/>
Plan 3 (Windows Server - Legacy plan)	Medium	Protected 10 instances	Full	<input type="button" value="Edit"/>
Plan 4 (Windows Server - Legacy plan)	Medium	1 storage account	Full	<input type="button" value="Edit"/>
Plan 5 (Windows Server - Legacy plan)	Medium	1 instance registered 0 Azuremeter zones	Partial (warning)	<input type="button" value="Edit"/>
Plan 6 (Windows Server - Legacy plan)	Medium	1 Azuremeter zone	Full	<input type="button" value="Edit"/>
Plan 7 (Windows Server - Legacy plan)	Medium	1 instance registered	Full	<input type="button" value="Edit"/>
Plan 8 (Windows Server - Legacy plan)	Medium	1 key vault	Full	<input type="button" value="Edit"/>
Plan 9 (Windows Server - Legacy plan)	Medium	1 key vault	Full	<input type="button" value="Edit"/>
Plan 10 (Windows Server - Legacy plan)	Medium	1 resource manager	Full	<input type="button" value="Edit"/>

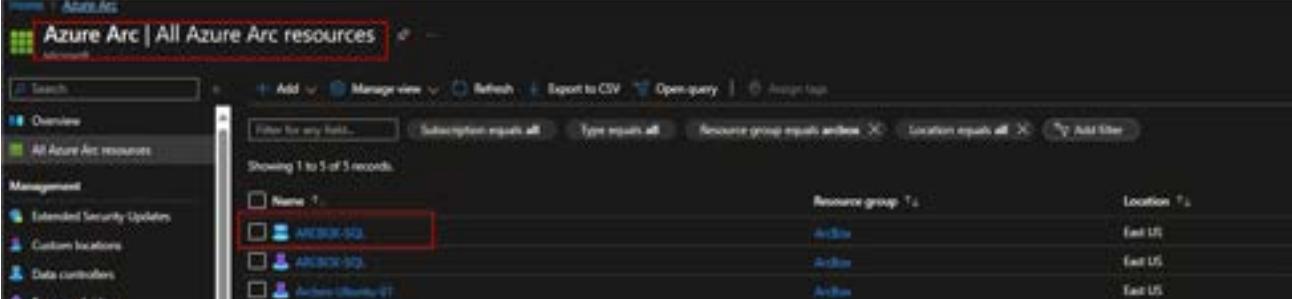
**Task 1 has been completed**

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Task 2: Enable Defender for Cloud to protect a specific Arc-enabled SQL server

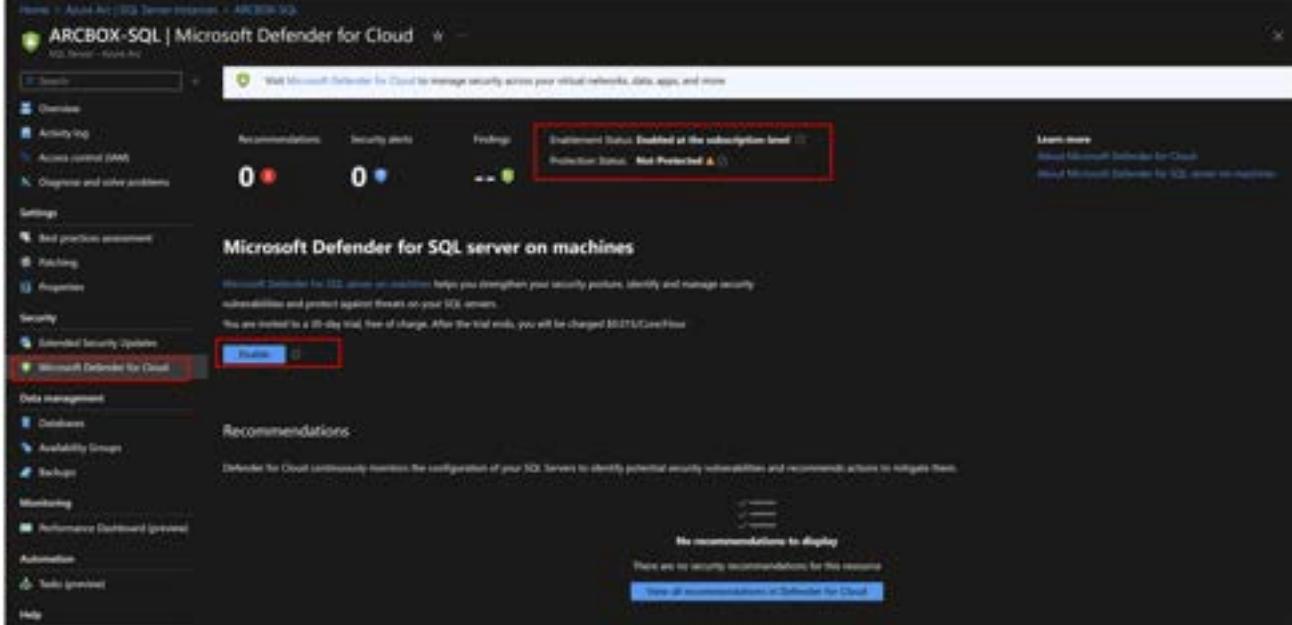
In the previous task you set up the Defender for Cloud to protect your SQL servers at the subscription level, by setting up a policy to ensure the required extensions are installed on all SQL servers. In this step you will look at enabling Defender for Cloud to protect a single SQL Server.

- 1. From the Azure portal go to *Azure Arc | All Azure Arc resources* page and select your SQL Server.



The screenshot shows the 'Azure Arc | All Azure Arc resources' page in the Azure portal. The left sidebar includes 'Management' sections for 'Extended Security Updates', 'Custom locations', 'Data controllers', and 'Resource controller'. The main area displays a table with four rows, each representing a server. The first row has a checkbox labeled 'Name: 1' and a small icon. The second row has a checkbox and a blue square icon containing 'ARCBOX-SQL'. The third and fourth rows have checkboxes and purple square icons. The columns are 'Resource group', 'Location', 'Status', and 'Last check'. The 'Location' column shows 'East US' for all three rows. The 'Status' column shows 'Active' for the first two and 'Standby' for the last two. The 'Last check' column shows '2023-07-10' for all three rows.

- 2. On the Server page select *Microsoft Defender for Cloud* and check if Defender is enabled. If it is not enabled then click the *Enable* button. Note that although you set up Defender to protect your SQL servers at the subscription level in the previous task, the effect of that policy setting might not have propagated yet to your specific SQL server



The screenshot shows the 'ARCBOX-SQL | Microsoft Defender for Cloud' page. The left sidebar lists 'Overview', 'Activity log', 'Access control (IAM)', 'Diagnose and solve problems', 'Settings' (with 'Extended Security Updates' and 'Microsoft Defender for Cloud' selected), 'Data management' (with 'Database', 'Availability Groups', and 'Backup' listed), 'Monitoring' (with 'Performance Dashboard (preview)'), 'Automation' (with 'Task preview'), and 'Help'. The main content area features a 'What is Microsoft Defender for Cloud?' banner. Below it, the 'Microsoft Defender for Cloud' section displays 'Recommendations' (0 red, 0 blue), 'Security alerts' (0 blue), and 'Findings' (0 green). A status bar indicates 'Enrollment status: Enabled at the subscription level' and 'Protection status: Not Protected'. A prominent 'Enable' button is highlighted with a red box. To the right, there's a 'Learn more' section with links to 'About Microsoft Defender for Cloud' and 'Microsoft Defender for SQL server on machines'. At the bottom, there's a 'Recommendations' section stating 'Defender for Cloud continuously monitors the configuration of your SQL servers to identify potential security vulnerabilities and recommends actions to mitigate them.' and a 'No recommendations to display' message.

- 3. Defender for Cloud is now enabled for your SQL server. There might be some delay in showing the *Protection Status* but you can continue with the rest of the lab

The screenshot shows the Microsoft Defender for Cloud dashboard for the resource group 'ARCBX-SQL'. The top navigation bar includes 'ARCBX-SQL | Microsoft Defender for Cloud' and 'Big Bang - Azure SQL'. Below the navigation is a search bar and a link to 'Get started with Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more...'. The main dashboard features a summary section with counts for 'Recommendations' (2 red), 'Security alerts' (0 blue), and 'Findings' (25 green). A prominent red box highlights the 'Subscription Status Enabled at the subscription level' message and the 'Protection Status Protected' status. On the left, a sidebar lists various service categories: Overview, Activity log, Access control (IAM), Diagnostic and audit policies, Settings (with 'Cloud platform assessment' checked), Monitoring, Properties, Security (with 'Advanced security updates' checked), Microsoft Defender for Cloud (which is selected and highlighted in red), Data management (with 'Databases', 'Availability Groups', and 'Backups'), Monitoring (with 'Performance Dashboard (preview)'), Automation (with 'Auto (preview)'), Help, and Support + Troubleshooting. The main content area displays 'Recommendations' (1 of 2 results) and 'Security Incidents and alerts' (0). The 'Recommendations' section includes a table with two rows: 'VM servers on machines should have vulnerability findings removed' (Severity: High, Type: Cloud) and 'Information in security configuration on your Windows machines should be remediated given by cloud configuration' (Severity: Low, Type: Cloud). The 'Security Incidents and alerts' section includes a link to 'View additional recommendations in Defender for Cloud'.

## Task 2 has been completed

Click **Next** for the next exercise or [Go back to the main table of content](#)

## Exercise 2 - Generate Defender for Cloud Incidents and Alerts

---

### **Objective**

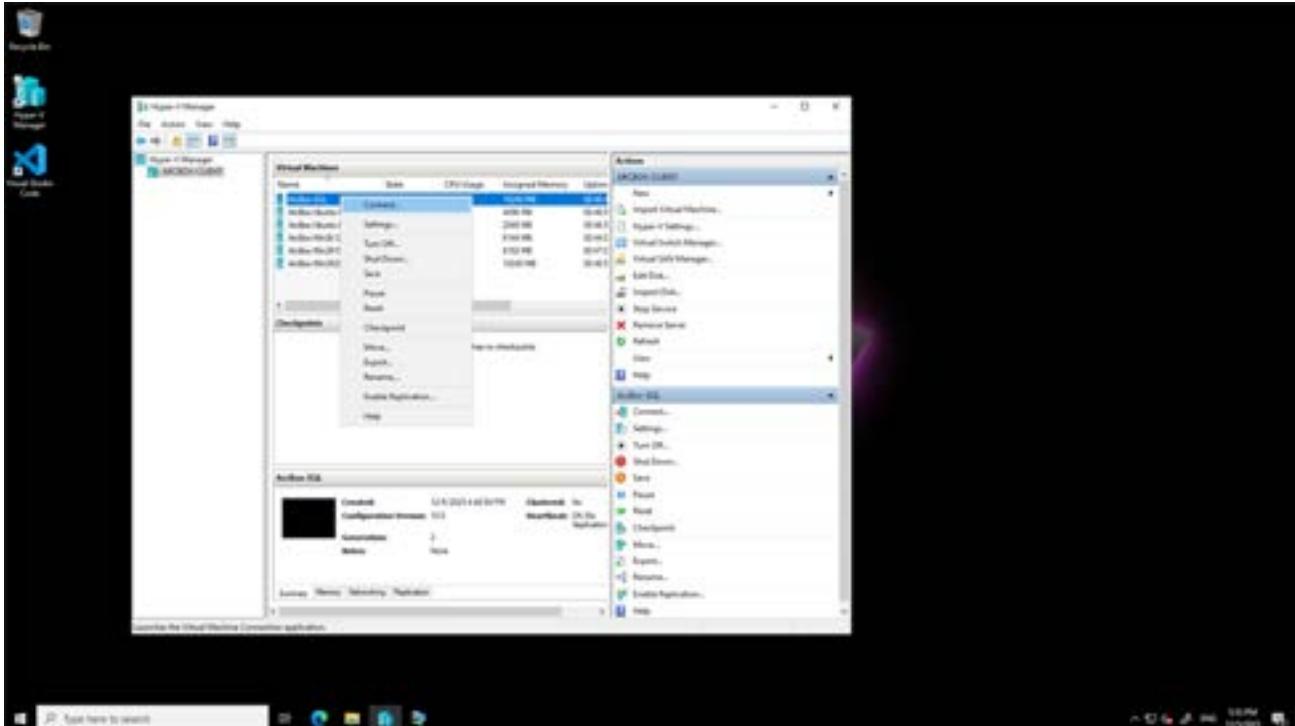
In this exercise you will simulated a number of security incidents on your Arc-enabled SQL server and examine the alerts generated by Defender for Cloud.

### **Estimated Time to Complete This Exercise**

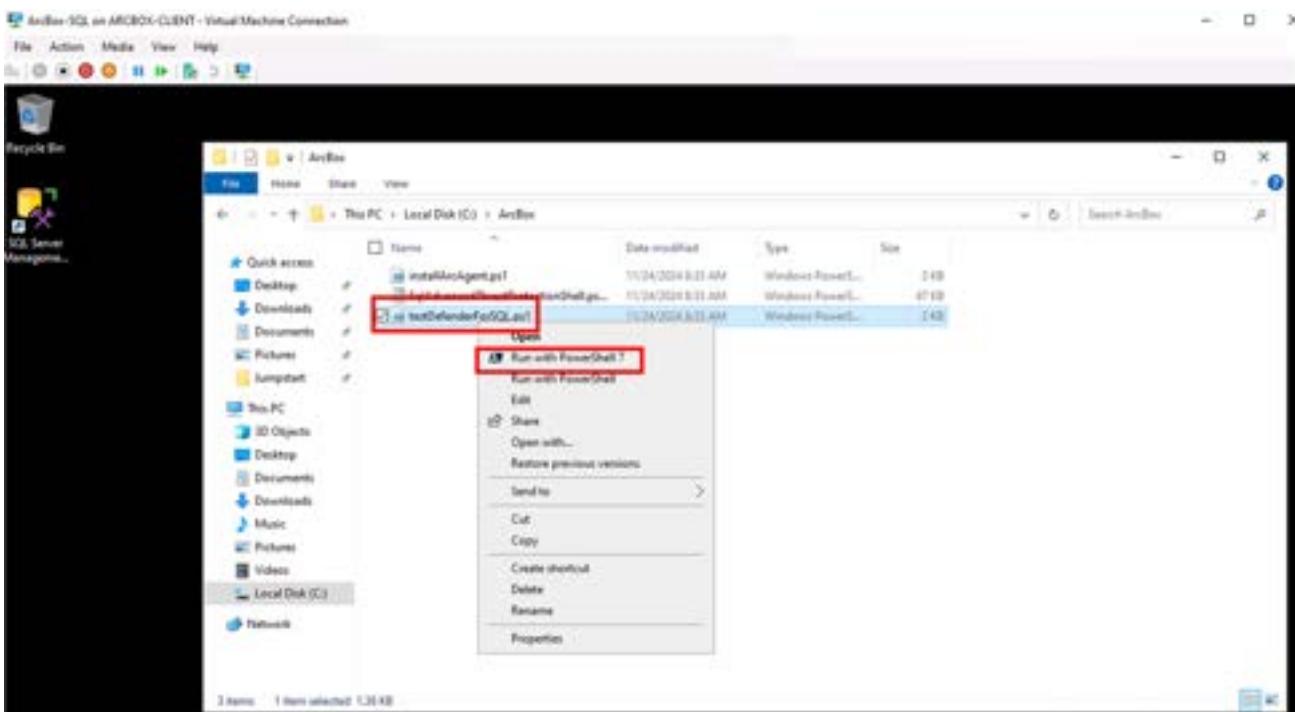
30 minutes

## Task 1: Simulate security incidents

- ☐ 1. Connect and login to the ArcBox-Client machine. Open Hyper-V Manager and connect to the ArcBox-SQL virtual machine (Administrator password JS123!!)



- ☐ 2. **On the nested ArcBox-SQL** Open the file explorer and navigate to the ArcBox folder on the C: drive. Right click on the testDefenderForSQL.ps1 file and run with PowerShell.



- 3. The script will simulate a number of threats on the Arc-enabled SQL server.

```
Executing Defender for SQL threat simulation script.
Current working directory: C:\ArcBox
[Info] For a list of available commands in the module run:
Get-Command -Module SqlAdvancedThreatProtectionShell

CommandType      Name          Version   Source
Function        Get-SqlManagementPackVersion       0.0       SqlAdvancedThreatProtectionShell
Function        Get-SqlAgentMonitoringAgentAndLogSpace    0.0       SqlAdvancedThreatProtectionShell
Function        Get-SqlMpServerInstancesVersions     0.0       SqlAdvancedThreatProtectionShell
Function        Set-SqlMpEventLogLevel           0.0       SqlAdvancedThreatProtectionShell
Function        Start-SqlMpStartTracing          0.0       SqlAdvancedThreatProtectionShell
Function        Stop-SqlMpStopTracing          0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpDatafiltration        0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpAgentStatus          0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpRateForce           0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpLogSection          0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpInstanceStatus       0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpLogSuspiciousApp      0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpPrincipalAnomaly      0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpShellExternalSourceAnomaly 0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpShellOffFusion        0.0       SqlAdvancedThreatProtectionShell

EXECUTING SQL INJECTION
OK | Successfully tested sql injection on ARCBX-SQL
```

```
Executing Defender for SQL threat simulation script.
Current working directory: C:\ArcBox
[Info] For a list of available commands in the module run:
Get-Command -Module SqlAdvancedThreatProtectionShell

CommandType      Name          Version   Source
Function        Get-SqlManagementPackVersion       0.0       SqlAdvancedThreatProtectionShell
Function        Get-SqlAgentMonitoringAgentAndLogSpace    0.0       SqlAdvancedThreatProtectionShell
Function        Get-SqlMpServerInstancesVersions     0.0       SqlAdvancedThreatProtectionShell
Function        Set-SqlMpEventLogLevel           0.0       SqlAdvancedThreatProtectionShell
Function        Start-SqlMpStartTracing          0.0       SqlAdvancedThreatProtectionShell
Function        Stop-SqlMpStopTracing          0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpDatafiltration        0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpAgentStatus          0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpRateForce           0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpLogSection          0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpInstanceStatus       0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpLogSuspiciousApp      0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpPrincipalAnomaly      0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpShellExternalSourceAnomaly 0.0       SqlAdvancedThreatProtectionShell
Function        Test-SqlMpShellOffFusion        0.0       SqlAdvancedThreatProtectionShell

EXECUTING SQL INJECTION
OK | Successfully tested sql injection on ARCBX-SQL
```

- 4. Go to your Arc SQL Server ArcBox-SQL and select *Microsoft Defender for Cloud*. You should see that some alerts have been generated

Azure Arc | All Azure Arc resources

Name	Resource group	Location
ARCTEST-SQL	Arctis	East US
ARCTEST-SQL	Arctis	East US
Arcus (Ubuntu 18)	Arctis	East US

Home > Azure Arc | All Azure Arc resources > ARCTEST-SQL

## ARCTEST-SQL | Microsoft Defender for Cloud

SQL Server - Azure Arc

Search

Visit Microsoft Defender for Cloud to manage security across yo

Overview

Activity log

Access control (IAM)

Diagnose and solve problems

Recommendations 5 !

Security alerts 3 !

Findings 25 !

Best practices assessment

Patching

Properties

Extended Security Updates

Microsoft Defender for Cloud

Recommendations

Defender for Cloud continuously monitors the configuration of your SQL

Description

SQL servers on machines should have vulnerability findings resolved

5. You can scroll down further to find your alerts

The screenshot shows the Microsoft Defender for Cloud interface. On the left, there's a navigation sidebar with options like 'Overview', 'Database', 'Activity log', 'Access control (IAM)', 'Diagnose and solve problems', 'Settings', 'Best practices assessment', 'Monitoring', 'Metrics', 'Logs', 'Metrics', 'Logs', 'Help', and 'Support + Troubleshooting'. The 'Microsoft Defender for Cloud' section is selected. The main area is titled 'Security incidents and alerts' and displays a table of alerts. The table has columns for 'Alert title', 'Type', 'Count', 'Last updated', 'Type', 'State', 'Last activity time', 'Type', 'Severity', and 'Last updated'. There are three rows: 1. 'Unknown password with referenced path has been injected by SQL Server - MySQL' (Type: Microsoft, State: Active, Severity: Medium). 2. 'Suspected brute-force attack attempt' (Type: Microsoft, State: Active, Severity: High). 3. 'Unknown SQL injection' (Type: Microsoft, State: Active, Severity: High). Below this is a section titled 'Vulnerability assessment findings' with a table showing findings for 'Security Check'. The table includes columns for 'ID', 'Type', 'Affected resource', 'Applies to', 'Type', 'Severity', and 'Last updated'. There are three findings: 1. 'Affected resource information in the database should match the respective database information in the master' (Type: Microsoft, Severity: High). 2. 'Latest updates should be installed' (Type: Microsoft, Severity: High). 3. 'Execute permissions to access the registry should be removed' (Type: Microsoft, Severity: High).

- 6. Click on the *Suspected brute-force attack attempt* and on the next screen click on one of the instances of *Suspected brute-force attack attempt* (if there is more than one). This will open a screen with the alert description

This screenshot shows a detailed view of a security alert. At the top, there's a header with 'Security alerts' and various filter and search options. The main area shows a list of alerts with columns for 'Start date', 'End date', 'Status', 'Severity', 'Affected resource', 'Resource Group', and 'Activity start time (UTC)'. One alert is highlighted with a red border: 'Suspected brute-force attack attempt' (Severity: High). To the right, a modal window provides more details about this specific alert. The modal has tabs for 'Alert description' and 'Affected resource'. The 'Alert description' tab contains text explaining what a brute-force attack is and how to investigate it. It also includes a 'View full details' button. The 'Affected resource' tab lists 'ARCBX-001 Admin Arc machine' and 'ARCBX-002 Admin Arc machine'.

- 7. Click *View full details* to see more information on the user, client ip address and cause

The screenshot shows a security alert titled "Suspected brute-force attack attempt". Key details include:

- Alert status:** High (Severity), Active.
- Time:** 10/12/23, 09:02 am.
- Compressed entry ID:** 00000000-0000-0000-0000-000000000000.
- Potential cause:** Brute-force attack penetration testing.
- Agent ID:** 11111111-1111-1111-1111-111111111111.
- Client IP address:** 172.16.1.1.
- Client principal name:** user1@.
- Client application:** SQL Server.
- Log Analytics workspace ID:** Log Analytics workspace ID.
- Sql server name:** ABCDB01-001.
- Sql instance name:** MIGRATION01.
- Comprehensibility:** HIGH (92%).

- 8. Click on *Take action* to get the option to review logs as well as information to help mitigate the attack and prevent future attacks. You can also trigger a response, suppress alerts or configure email notifications

The screenshot shows the same security alert with the "Take action" tab selected. The available actions are:

- Inspect resource context:** Starts with examining the resource logs around the time of the alert. Includes a "View logs" button.
- Mitigate the threat:** Includes:
  - Apply [apply these instructions](#) to block future attacks.
  - Customize blocking for [none](#) of the offending agent and broadening your firewall.
  - When possible, use [minimum authentication](#) and double TOTP, known authentication.
  - Use [existing principals](#) and avoid reusing them across multiple databases.
  - If applicable, disable default and well-known application/database accounts such as SA.
- Prevent future attacks:** Includes:
  - Run trap 1 active security recommendations on [COMPUTER-1044](#).
    - high: [SQL Server users should have vulnerability mitigation enabled](#)
    - high: [Windows users should be configured to receive system service notifications](#)
    - high: [Windows users should be configured to use secure communication protocols](#)
  - Adding security recommendations can prevent future attacks by inducing attack surface.
  - View 1 recommendation(s)
- Trigger automated response**
- Suppress marker alerts**
- Configure email notification settings**

- 9. Optionally repeat the alert investigation for the other alerts (e.g. *Potential SQL Injection* alert)

## Task 2 has been completed

Click **Next** for the next exercise or [Go back to the main table of content](#)



# LAB17: Select the optimal Azure SQL target using Migration Assessment

---

In this lab you will learn how to use the Arc-enabled SQL Server assessment for migration to Azure. This assessment plays a vital role in the success of your cloud migration and modernization journey.

The assessment aggregates all the configuration and performance data and tries to find the best match across various Azure SQL service tiers and configurations and picks a configuration that can match or exceed the SQL instance performance requirements, optimizing the cost.

## Student Lab Manual

### Table of Contents

Exercise 1 - Review and analyze the migration assessment results

**[Task 1 - Review the migration readiness to Azure SQL Managed Instance \(MI\) and SQL Server on Azure VM](#)**

**[Task 2 - Review the migration readiness to Azure SQL DB](#)**

# Exercise 1: Review and analyze the migration assessment results

---

## **Objective**

In this exercise you will review the readiness for target deployment types and the Azure SQL size recommendation. The assessment takes into consideration three migration targets; Azure SQL Managed Instances, SQL Server on Azure VM and Azure SQL database.

## **Estimated Time to Complete This Exercise**

30 minutes

## Task 1: Review the migration readiness to Azure SQL Managed Instance (MI) and SQL Server on Azure VM

- 1. From the Azure portal go to *Azure Arc | All Azure Arc resources* page and select your SQL Server.

The screenshot shows the 'Azure Arc | All Azure Arc resources' page in the Azure portal. It lists three resources under the 'All Azure Arc resources' section. The first two resources, both named 'ARCTIC-SQL', are highlighted with a red box. The third resource, 'ARCTIC-VMSQL', is also listed. The table includes columns for Name, Resource group, and Location.

Name	Resource group	Location
ARCTIC-SQL	Arctics	East US
ARCTIC-SQL	Arctics	East US
ARCTIC-VMSQL	Arctics	East US

- 2. From the SQL server resource page select *Assessments (preview)* under the *Migration* folder in the left pane. Review the *Readiness* status and the recommended configurations to host your Arc-enabled SQL Server on an Azure SQL MI or on Azure VM. The readiness is based on the performance evaluation for the Arc-enabled SQL Server instances.

The screenshot shows the 'SQL Server' resource page in the Azure portal. The left sidebar has a red circle around the 'Assessments (preview)' link under the 'Migration' section. The main area displays three migration scenarios: 'Azure SQL MI', 'SQL Server on Azure VM', and 'Azure SQL DB'. Each scenario has a 'Readiness' status (Ready) and a list of recommended configurations. A red box highlights the 'Azure SQL MI' scenario.

- 3. Review the following link to understand the [assessment confidence rating](#).

## Task 2: Review the migration readiness to Azure SQL DB

- 1. On the Assessment page, review the *Readiness* status and the recommended configurations to host specific databases from your Arc-enabled SQL Server to Azure SQL database. Click on the link showing the number of databases that can be migrated without issues.

The screenshot shows the Azure SQL Assessment preview interface. On the left, a navigation pane includes options like Databases, Activity Log, Audit, Diagnose and solve problems, and Performance. The 'Assessments' section is highlighted with a red box and a circled '1'. The main area displays 'SQL Server migration scenarios' for three targets:

- Azure SQL MI**: Status: Ready. Suggested Azure SQL configuration: General Purpose, Provisioned, 4 vCores, 32 GB Storage. Configuration: 4 vCore, 32 GB.
- SQL Server on Azure VM**: Status: Ready. Suggested Azure VM configuration: Standard\_D2v2, 4 vCores, 2 vCores, 2 Processor\\_v2\\_CPU. Configuration: 4 vCore, 32 GB.
- Azure SQL DB**: Status: Ready. Suggested Azure SQL configuration: General Purpose, 4 vCores, 2 vCores, 2 Processor\\_v2\\_CPU. Configuration: 4 vCore, 32 GB. A red box highlights the 'Suggested Azure SQL configuration' for this target.

Below the scenarios, there's a table for 'Compatibility required for migration':

Object	Version	Support end date	Database feature support status	Total DB size (MB)	Logical file size (MB)
AdventureworksLT2014	SQL Server 2016	2020-06-01	Unreleased	1040	1040

At the bottom, there's a 'Review compatibility changes' section with a progress bar from 0% to 100%.

2. Note the database name and recommended Azure SQL DB compute and storage.

The screenshot shows the 'User databases' table in the Azure SQL Assessment preview interface. It lists one database, 'AdventureworksLT2014', with the following details:

Database	Migration readiness	Rating criteria	Azure SQL configuration (Compute)	Azure SQL configuration (Storage)	DB size (MB)	CPUs	Total CPU	Throughput
AdventureworksLT2014	Ready	Performance-based	General Purpose, Provisioned, Gen1, 2 vCores	100 GB Storage	1040	4.16	4.16	0.05

3. Click the *Ready* link under *Migration readiness* to see migration detail such as issues and warnings.

### Exercise 1 has been completed

---

Click **Next** for the next lab or [Go back to the main table of content](#)