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

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

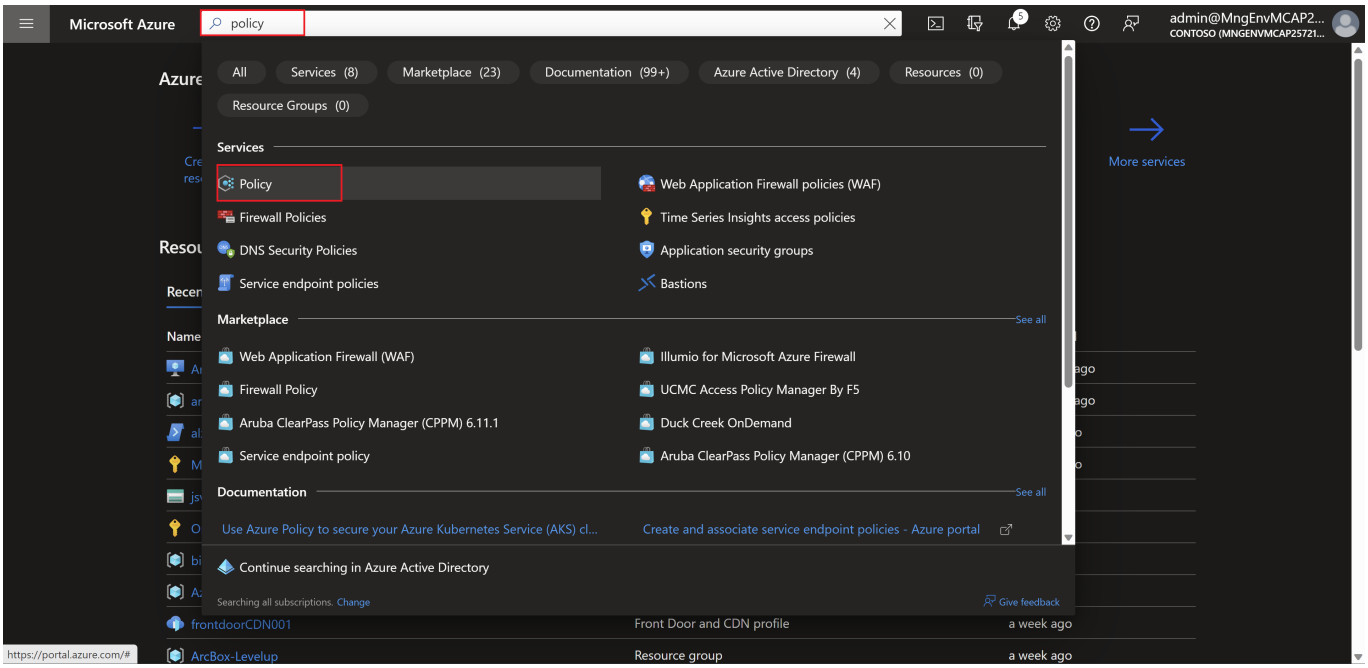
Explanation

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.

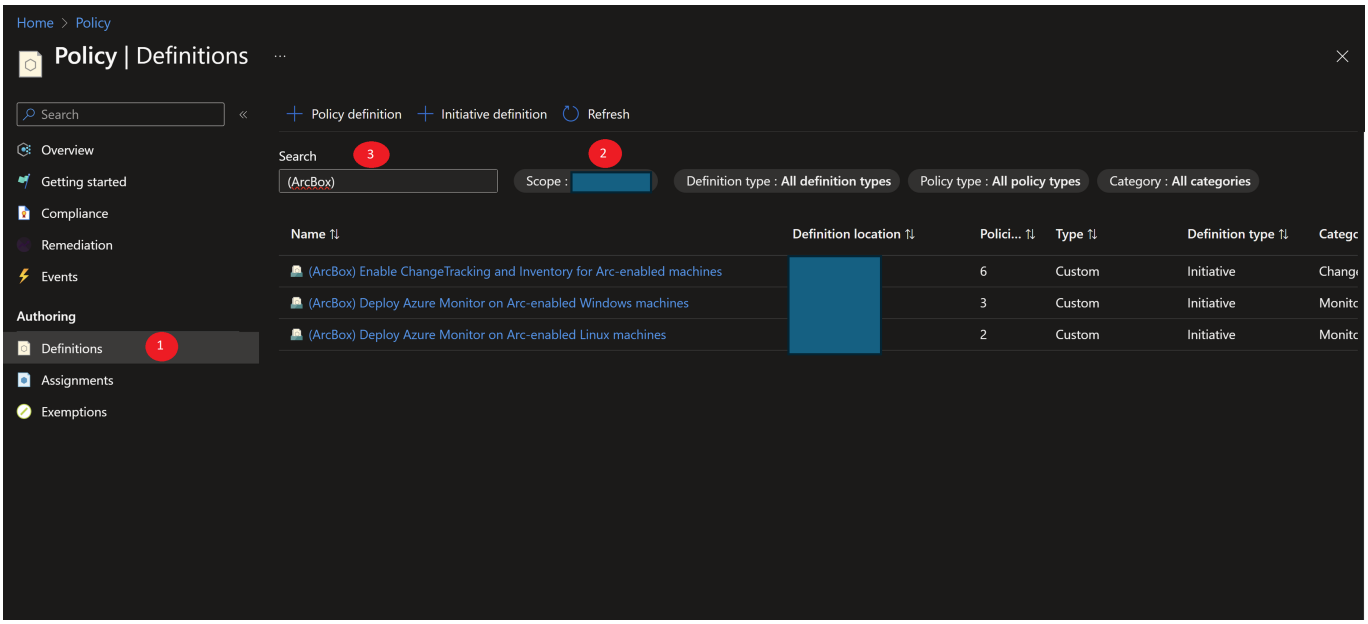
===

Task 1: Deploy the Azure Monitor Agent

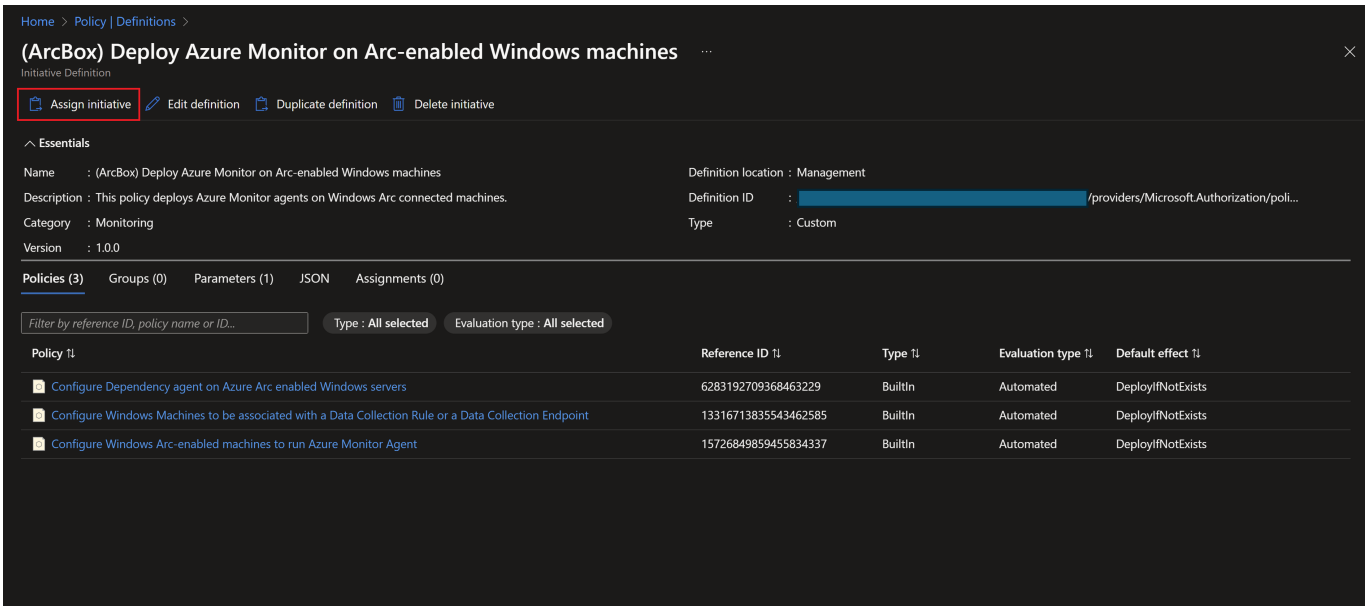
1. [] In the Azure portal, search for *Policy*.



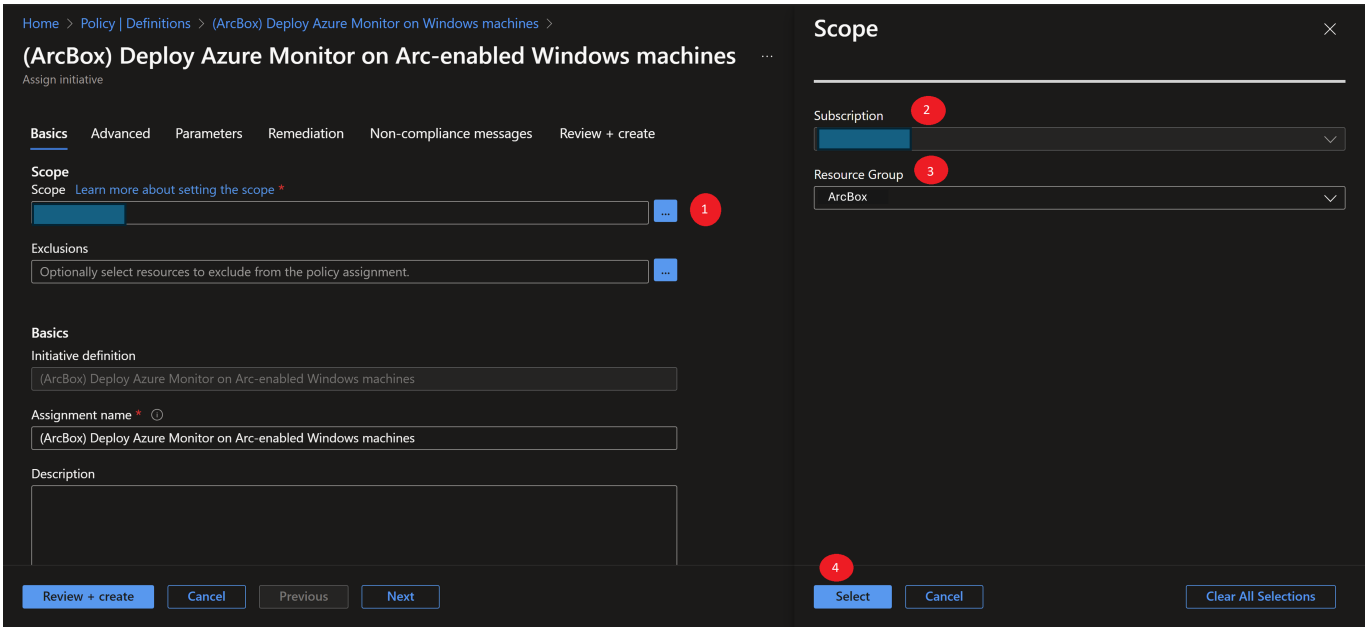
2. [] Click on "Definitions" and search for the *(ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines* policy. This is a predefined *Initiative* containing a group of policies to deploy the Azure Monitor Agent.



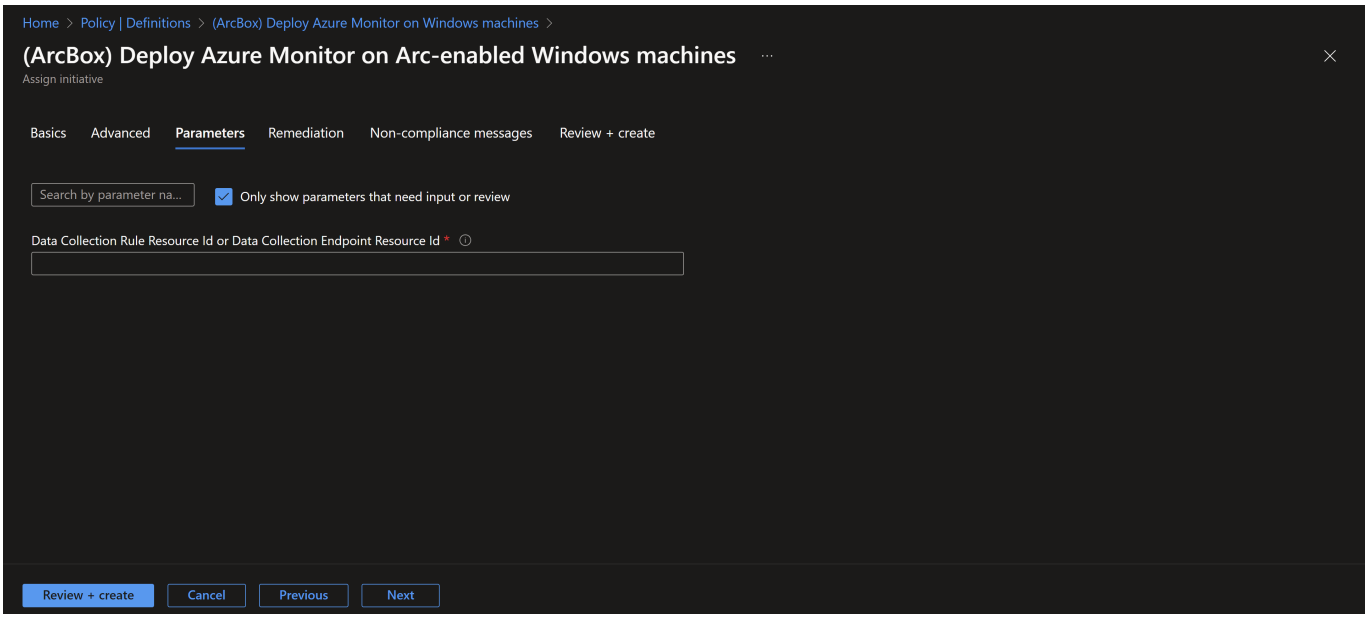
3. [] Click "Assign Initiative".



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



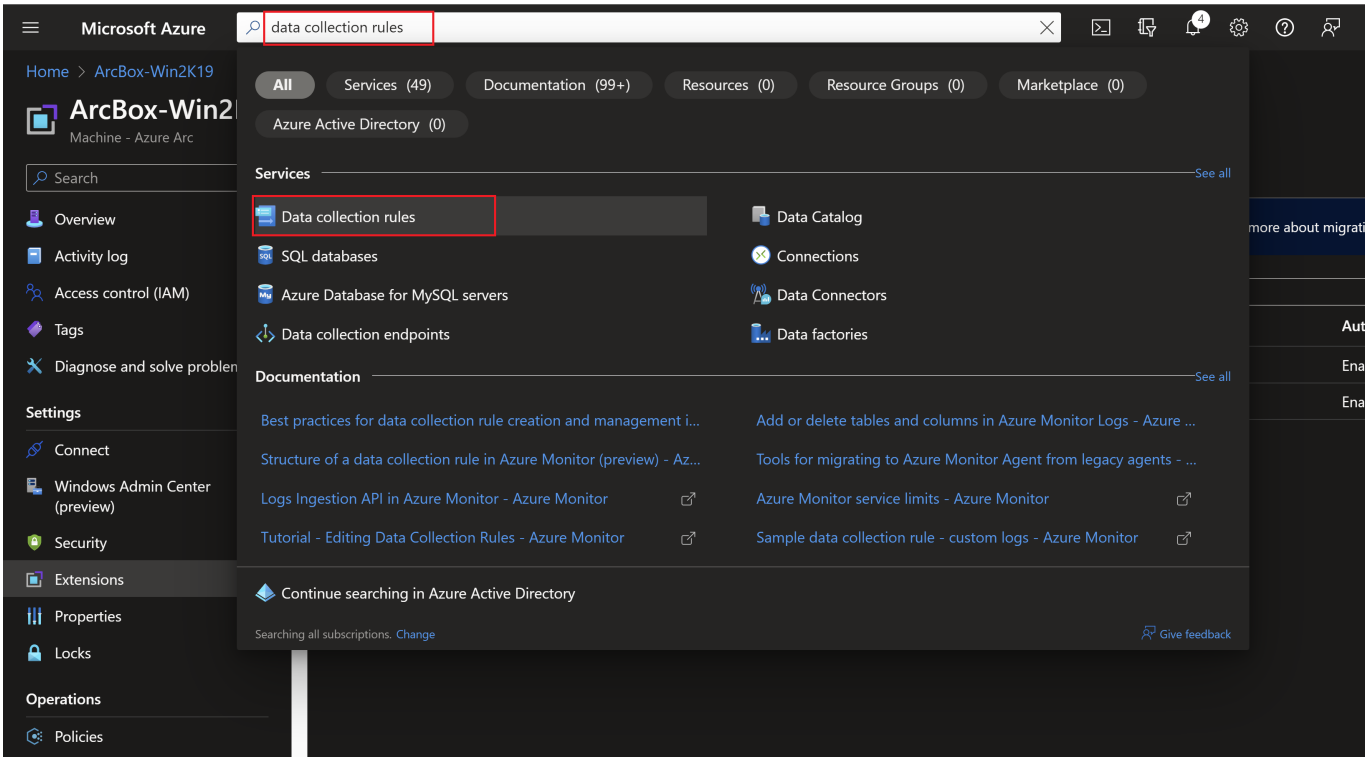
5. [] After validating the scope, navigate to the parameters tab.

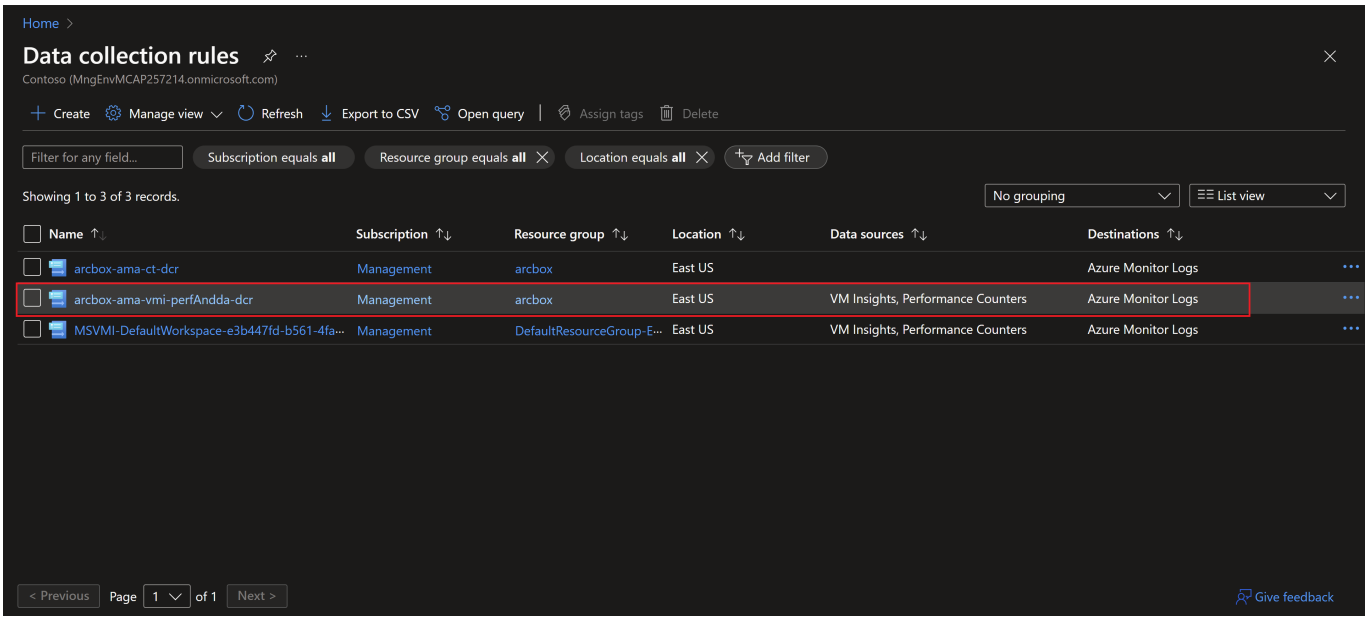


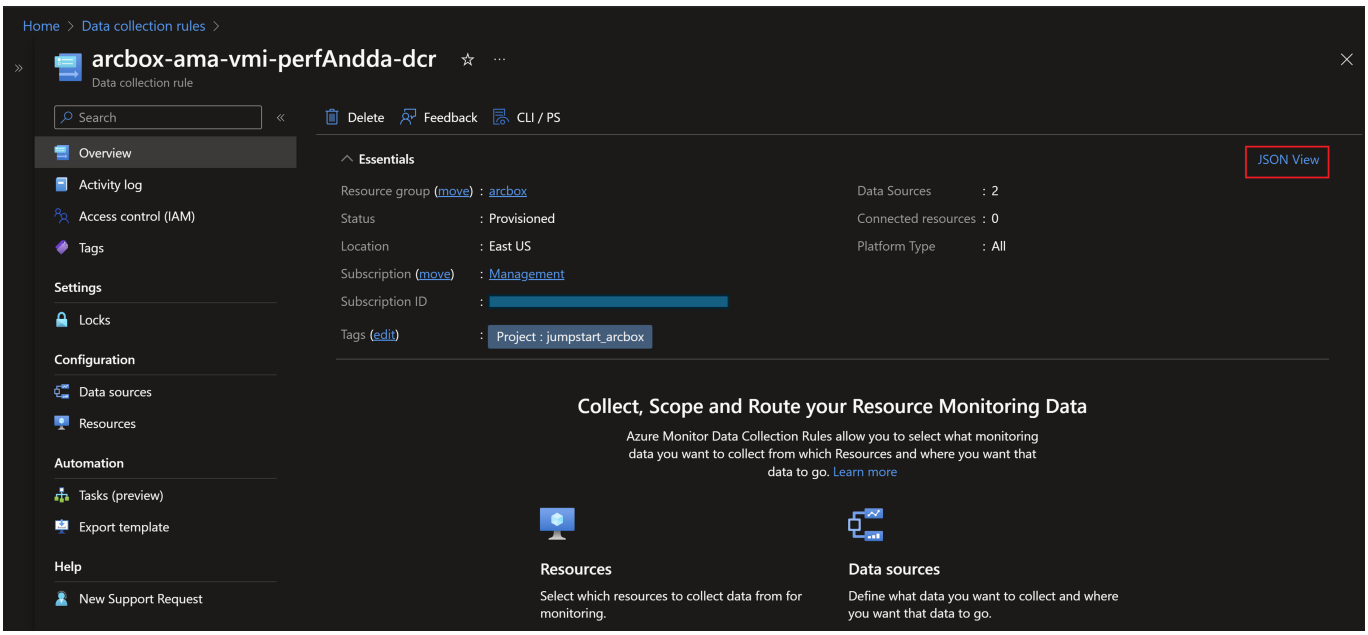
6. [] To get the "Data Collection Rule" resource Id, run the following command in PowerShell (making sure you enter the correct name of the resource group), copy the result into the field then click *create*.

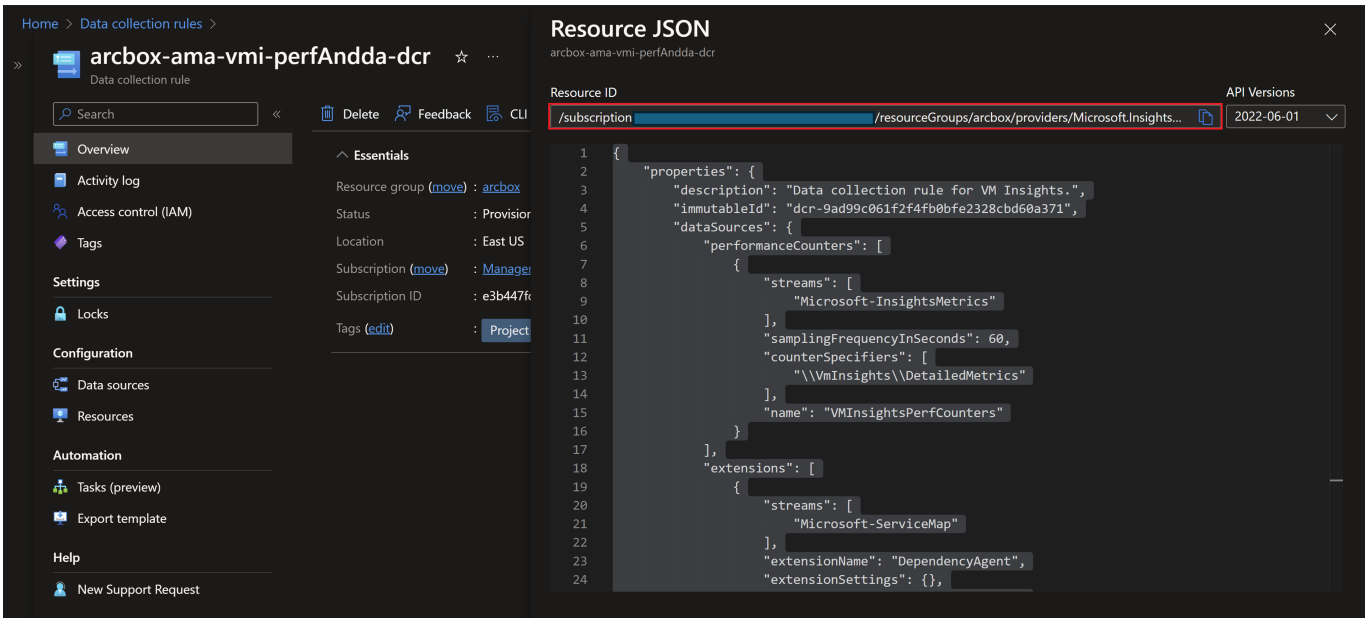
```
az resource show --name "arcbox-ama-vmi-perfAndda-dcr" `
                 --resource-group "<resource group name>" `
                 --resource-type Microsoft.Insights/dataCollectionRules `
                 --query id `
                 --output tsv
```

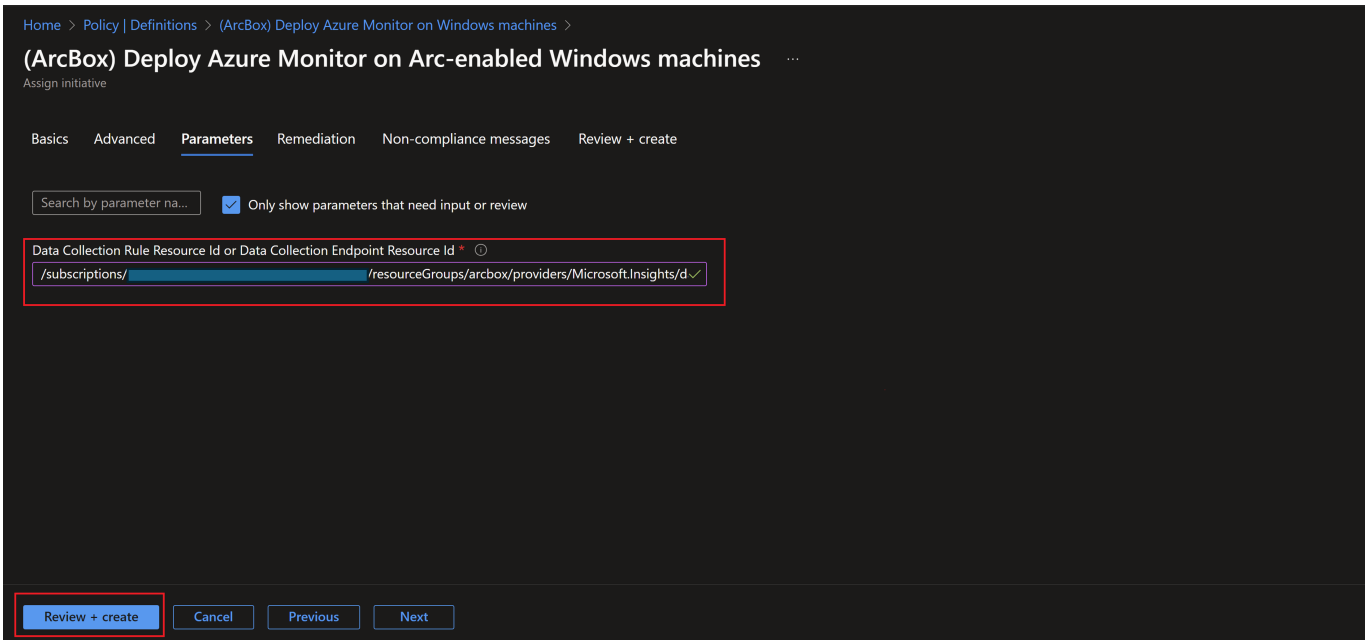
> [!Note] Optionally you can also find the "Data Collection Rule" resource Id from the Azure portal. Search for the *arcbox-ama-vmi-perfAndda-dcr* data collection rule.




Home
Data collection rules
Contoso (MngEnvMCAP257214.onmicrosoft.com)
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Delete
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
Showing 1 to 3 of 3 records.
No grouping
List view
Name
Subscription
Resource group
Location
Data sources
Destinations
arcbox-ama-ct-dcr
Management
arcbox
East US
Azure Monitor Logs
arcbox-ama-vmi-perfAndda-dcr
Management
arcbox
East US
VM Insights, Performance Counters
Azure Monitor Logs
MSVMI-DefaultWorkspace-e3b447fd-b561-4fa...
Management
DefaultResourceGroup-E...
East US
VM Insights, Performance Counters
Azure Monitor Logs
< Previous
Page 1 of 1
Next >
Give feedback

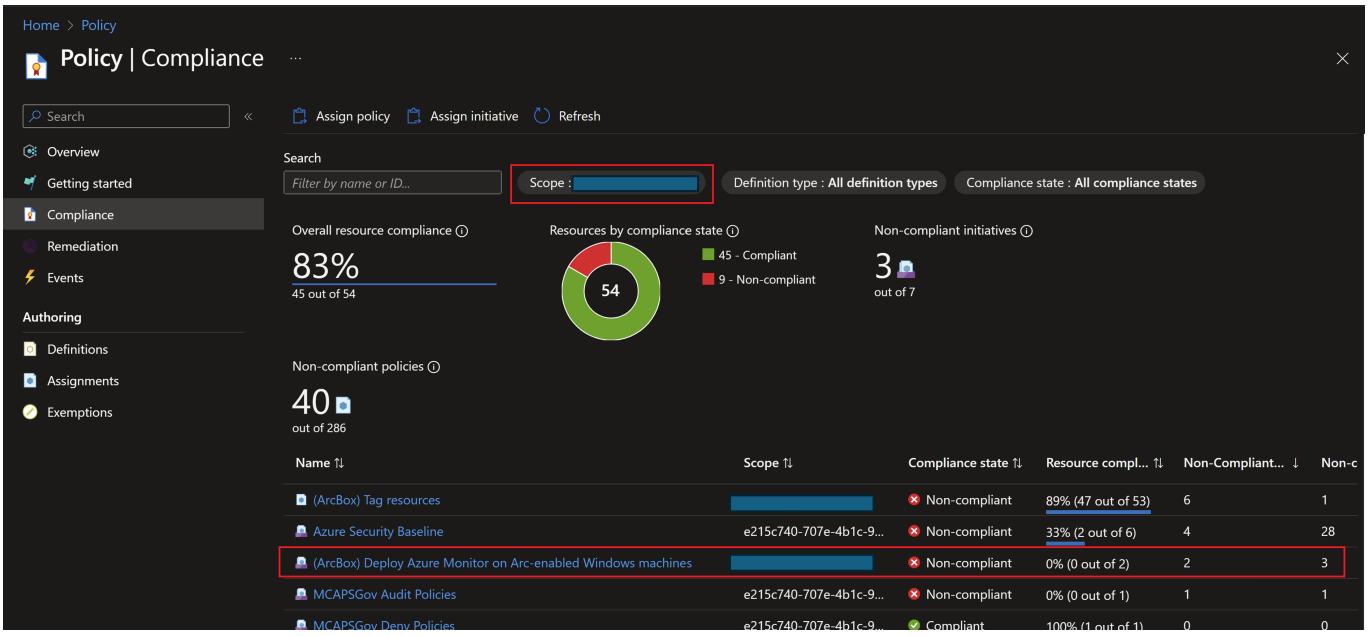

Home > Data collection rules
arcbox-ama-vmi-perfAndda-dcr
Data collection rule
Search
Delete
Feedback
CLI / PS
Overview
Activity log
Access control (IAM)
Tags
Settings
Locks
Configuration
Data sources
Resources
Automation
Tasks (preview)
Export template
Help
New Support Request
Essentials
JSON View
Resource group (move) : arcbox
Status : Provisioned
Location : East US
Subscription (move) : Management
Subscription ID :
Tags (edit) : Project : jumpstart_arcbox
Data Sources : 2
Connected resources : 0
Platform Type : All
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
Select which resources to collect data from for monitoring.
Data sources
Define what data you want to collect and where you want that data to go.

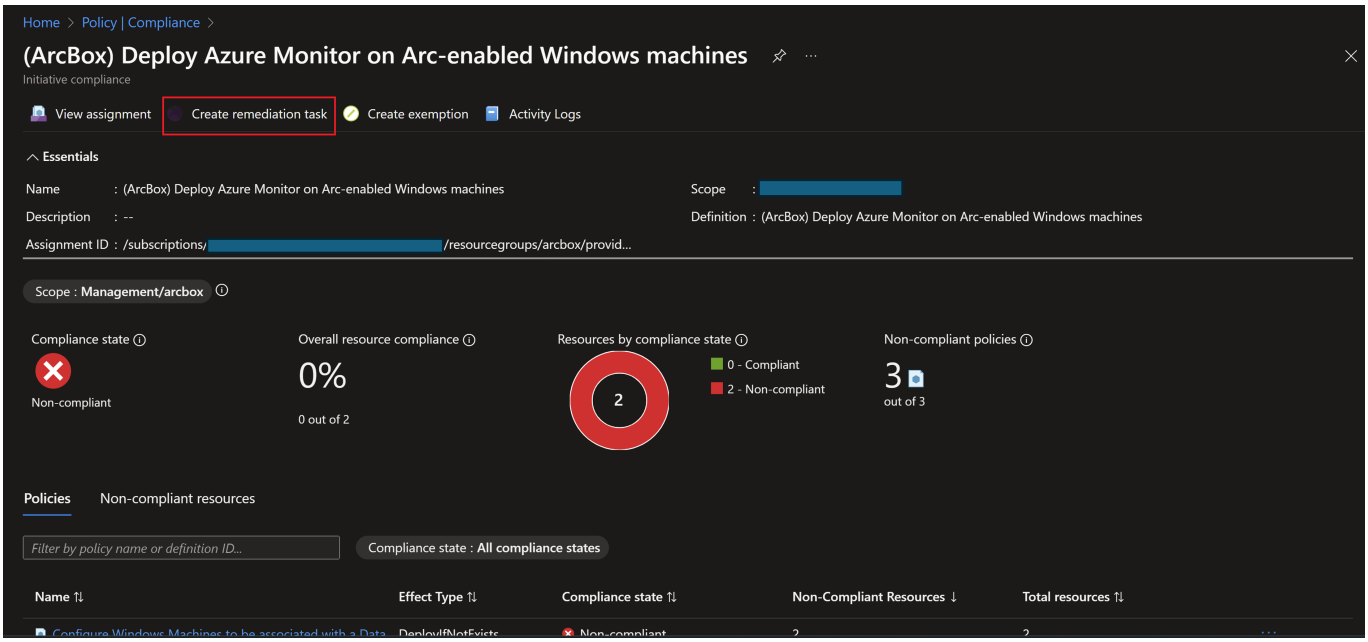

Home > Data collection rules
arcbox-ama-vmi-perfAndda-dcr
Data collection rule
Resource JSON
arcbox-ama-vmi-perfAndda-dcr
Resource ID
/subscription /resourceGroups/arcbox/providers/Microsoft.Insights...
API Versions
2022-06-01
{
"properties": {
"description": "Data collection rule for VM Insights.",
"immutableId": "dcr-9ad99c061f2f4fb0bfe2328cbd60a371",
"dataSources": {
"performanceCounters": [
{
"streams": [
"Microsoft-InsightsMetrics"
],
"samplingFrequencyInSeconds": 60,
"counterSpecifiers": [
"\\VmInsights\\DetailedMetrics"
],
"name": "VMInsightsPerfCounters"
}
],
"extensions": [
{
"streams": [
"Microsoft-ServiceMap"
],
"extensionName": "DependencyAgent",
"extensionSettings": {},

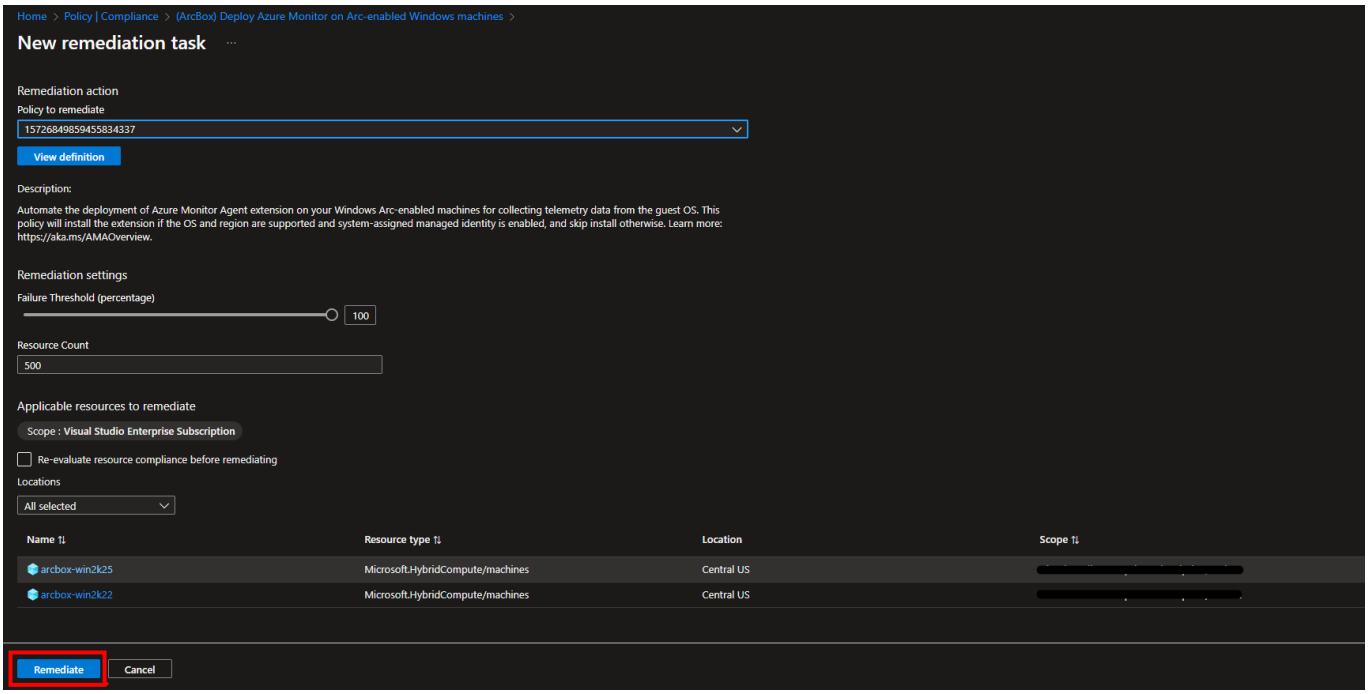


NOTE:The policy will take 5-15 minutes to assess the current resources.

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

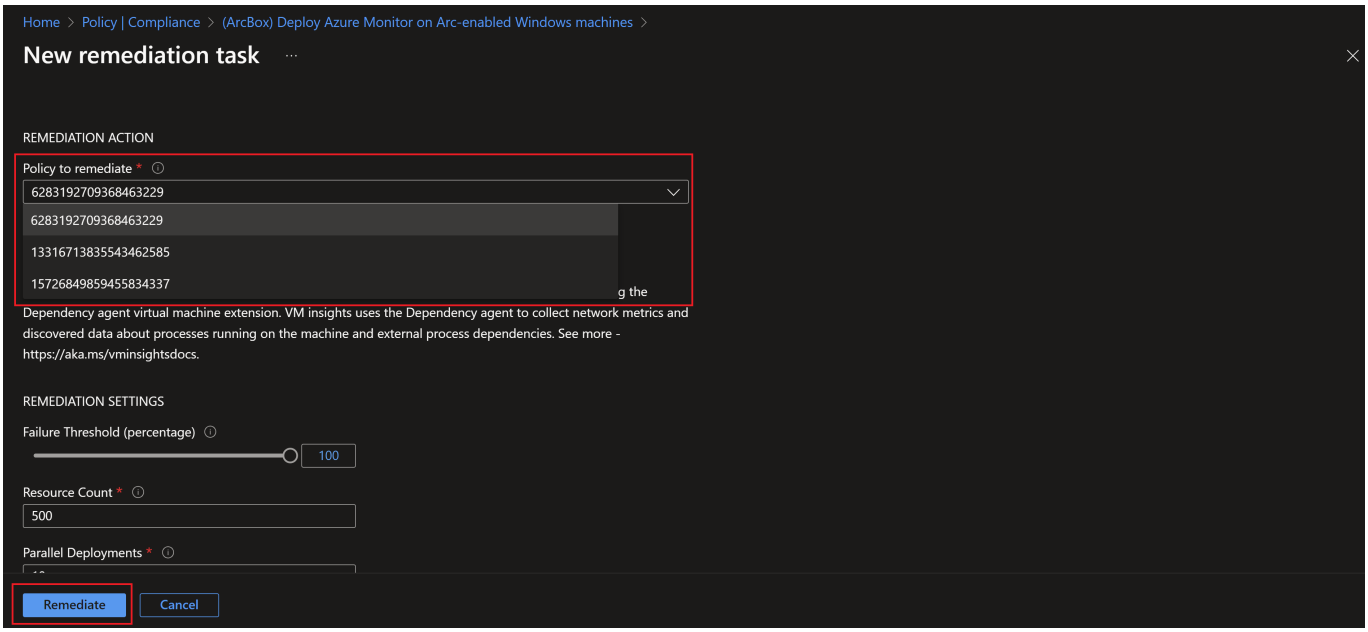




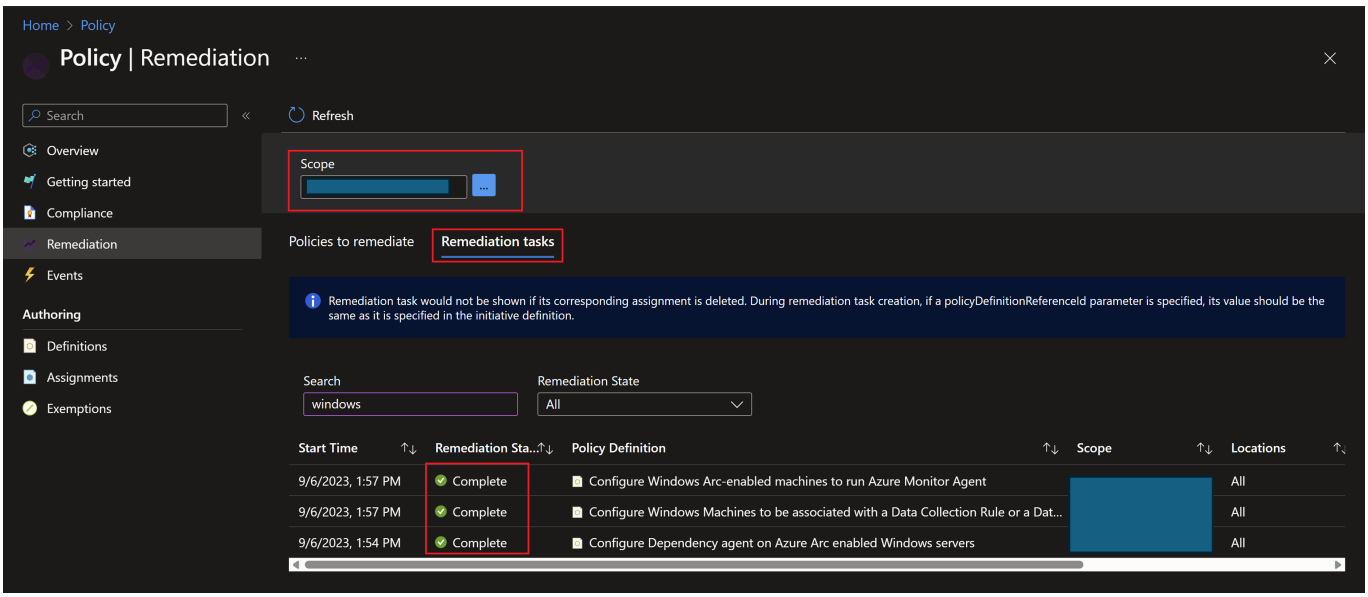


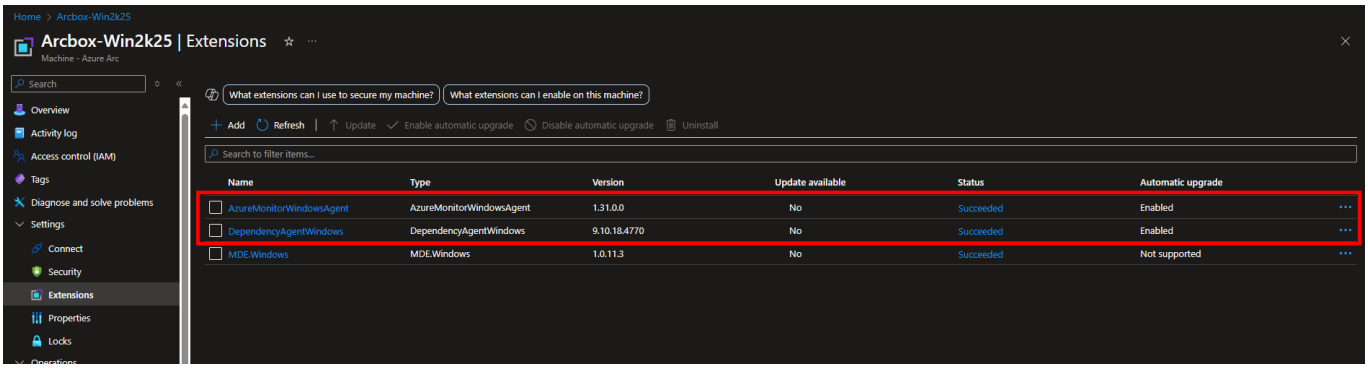
NOTE: When creating the remediation task, make sure to select the same region where you deployed ArcBox

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.

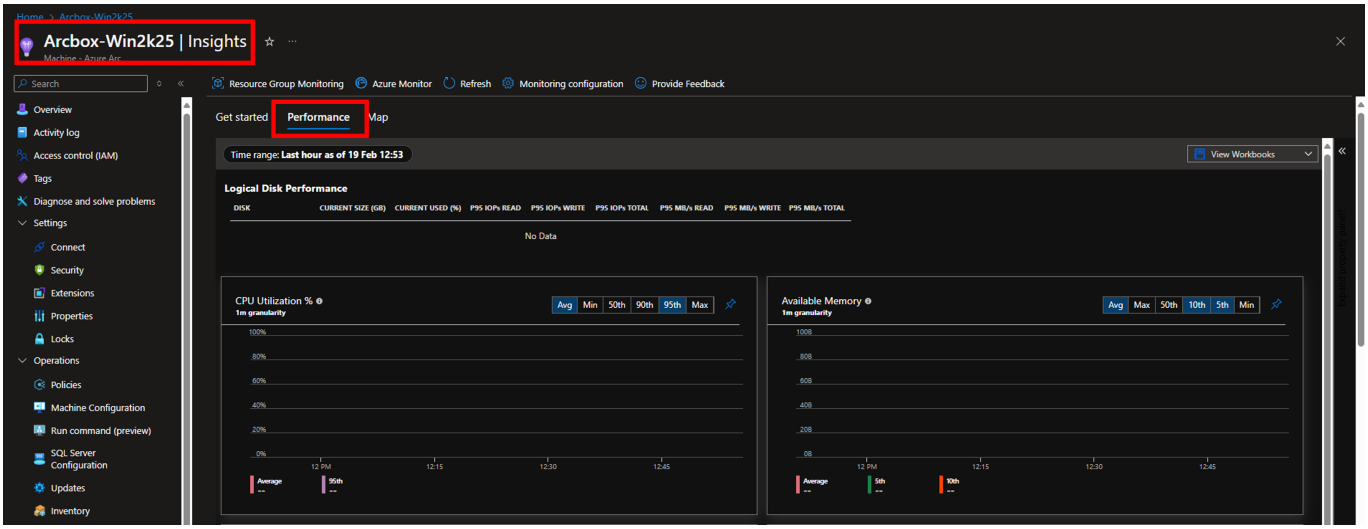


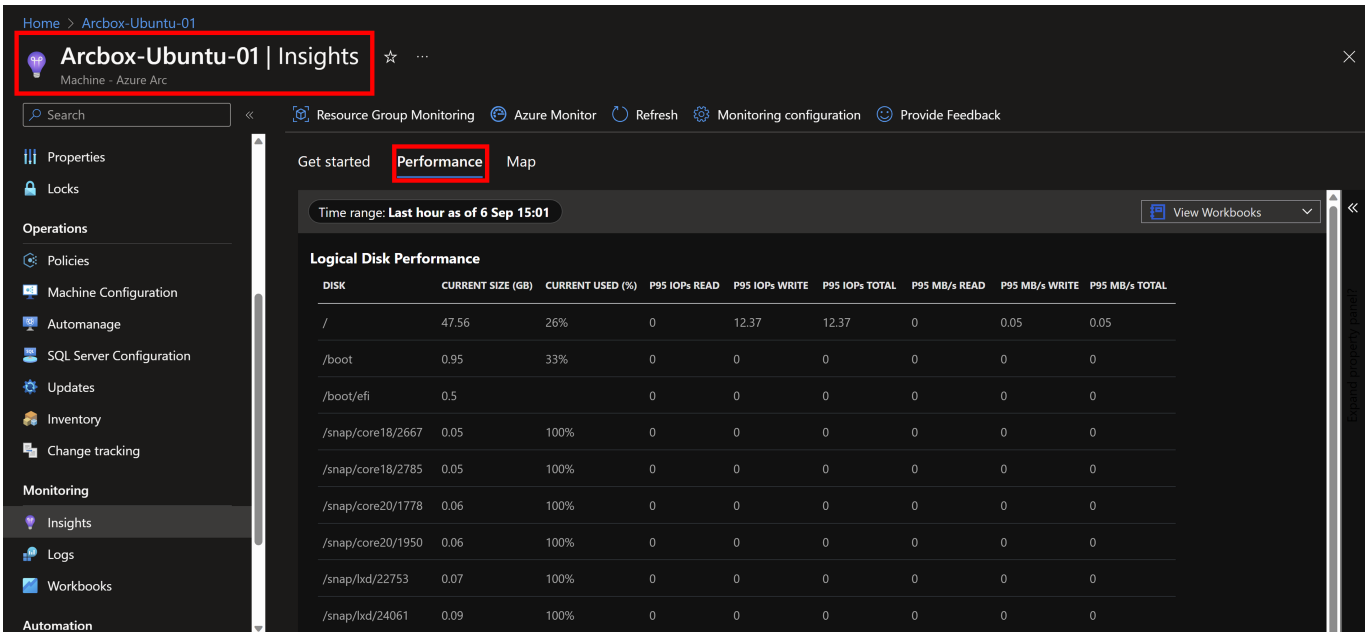


11. [] Repeat the same steps in *Task 2* to assign the Linux policy for data collection *(ArcBox) Deploy Azure Monitor on Arc-enabled Linux machines.*

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.





Task 1 has been completed

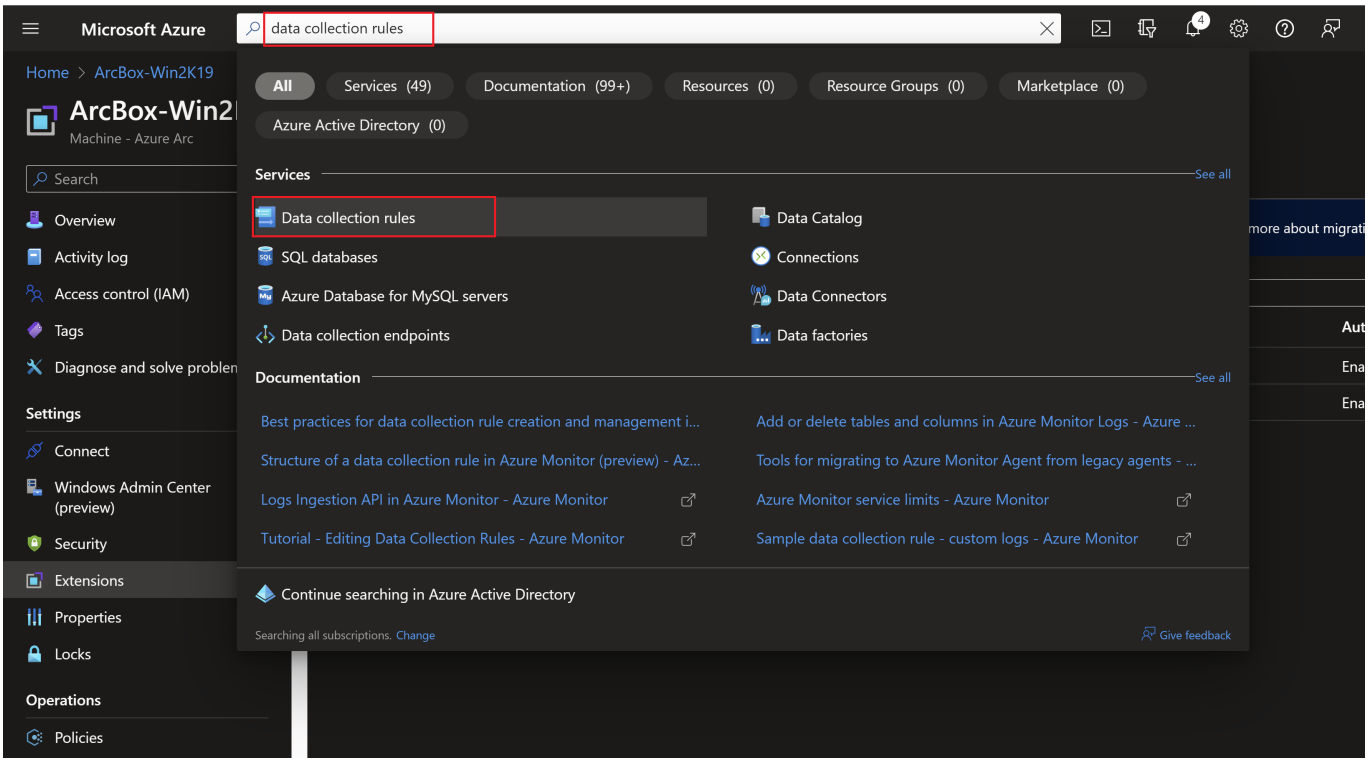
Click **Next** for the next task or **Go back to the main table of content**

===

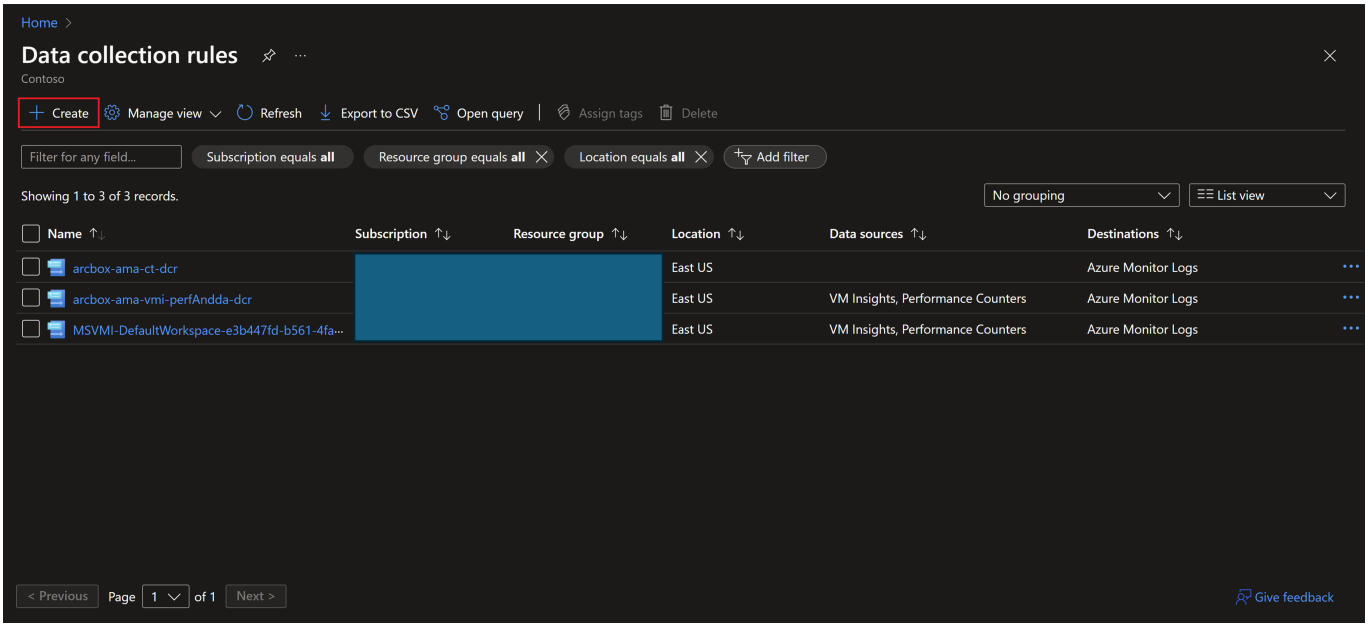
Task 2: Configure data collection for logs and metrics

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.

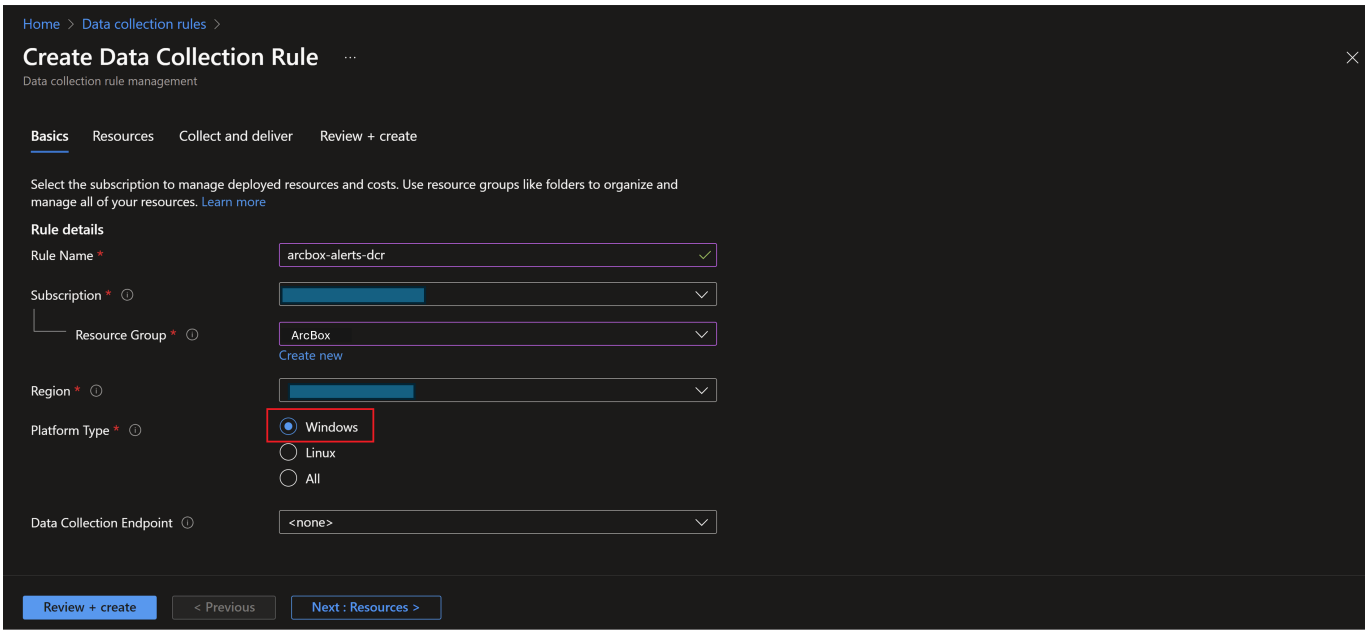
1. [] In the Azure portal, search for *Data Collection rules*.



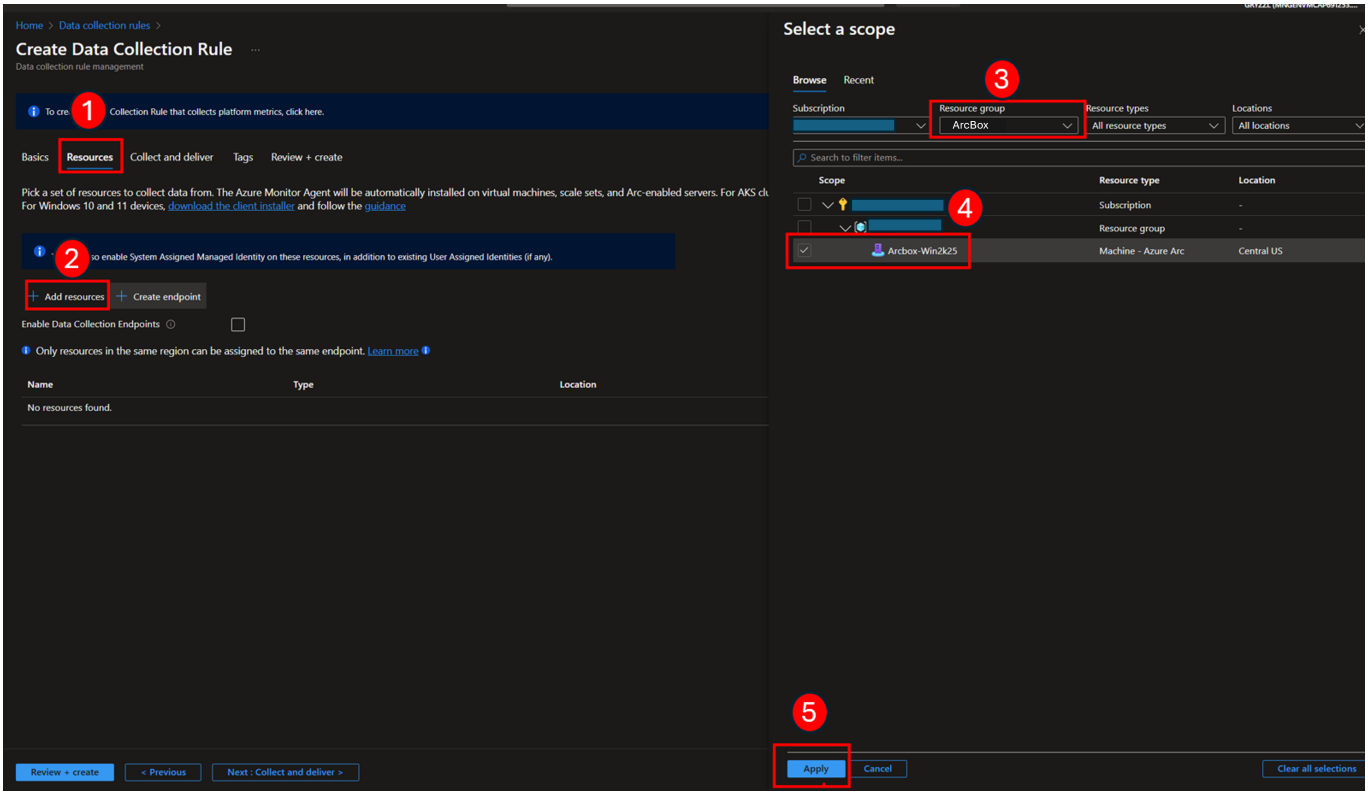
2. [] Create a new data collection rule.



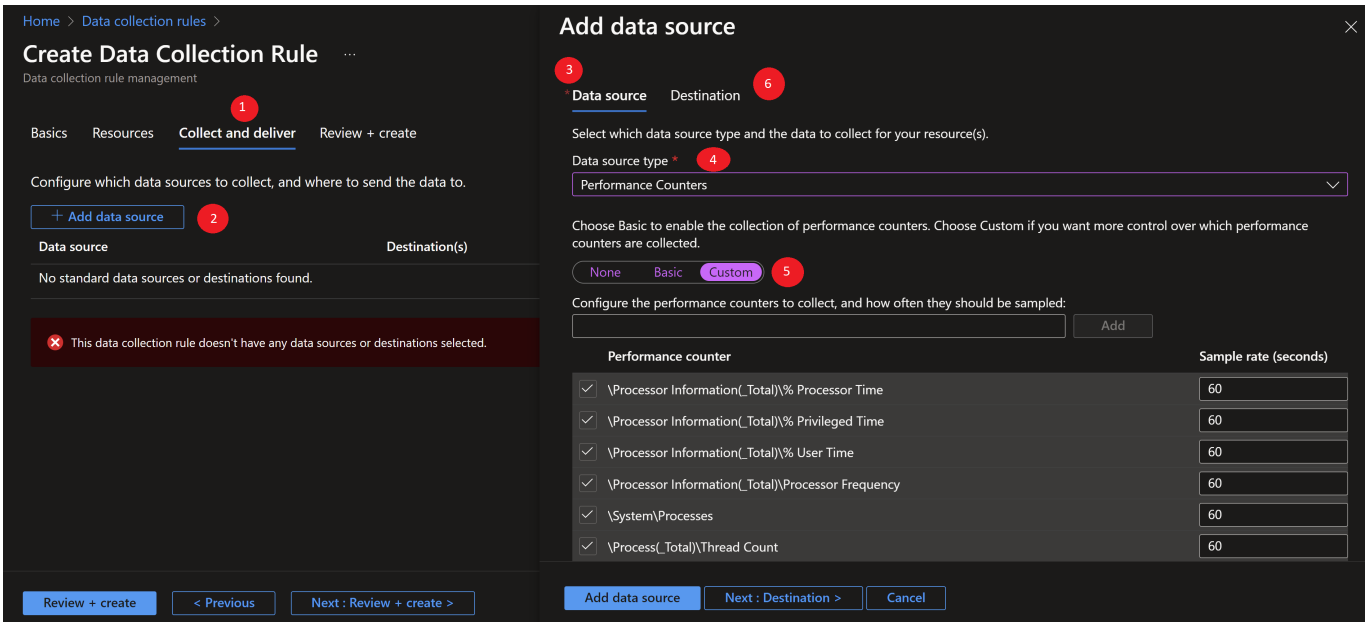
3. [] Provide a name and select the same resource group where ArcBox is deployed. Make sure to select Windows as the operating system.



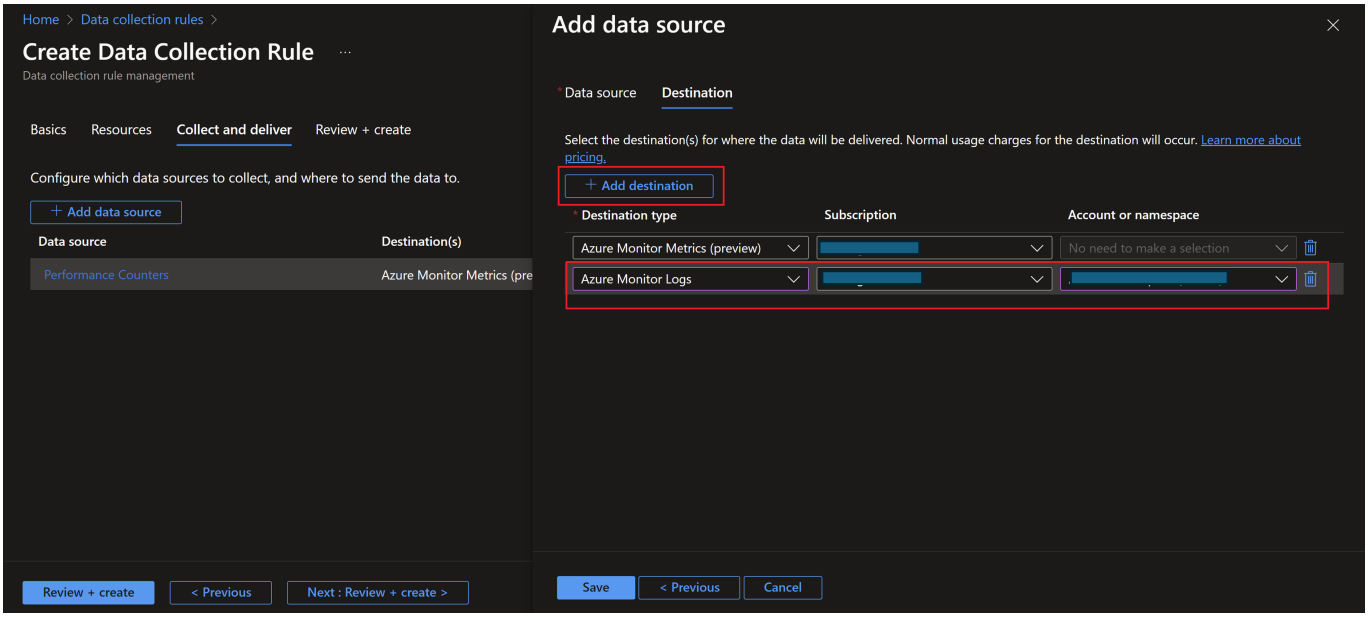
4. [] In the "Resources" tab, select the right resource group and the Arc-enabled servers onboarded.



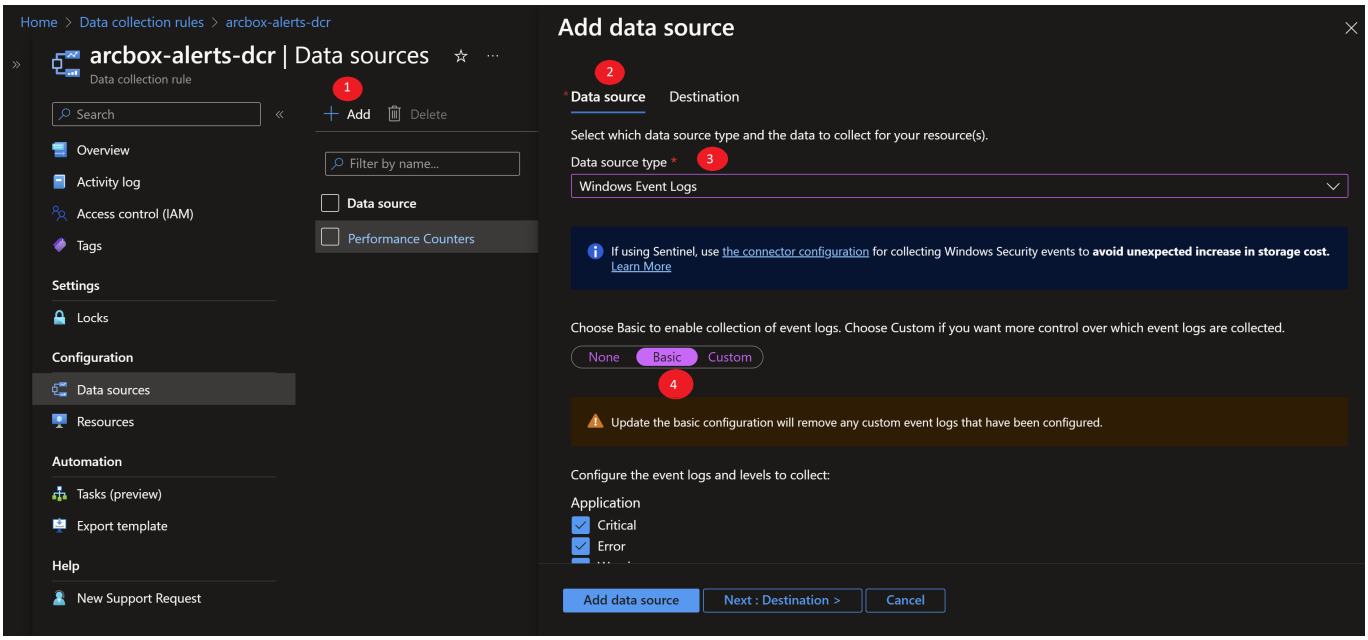
5. [] Add a new "Performance Counters" data source, and make sure to select all the custom counters.



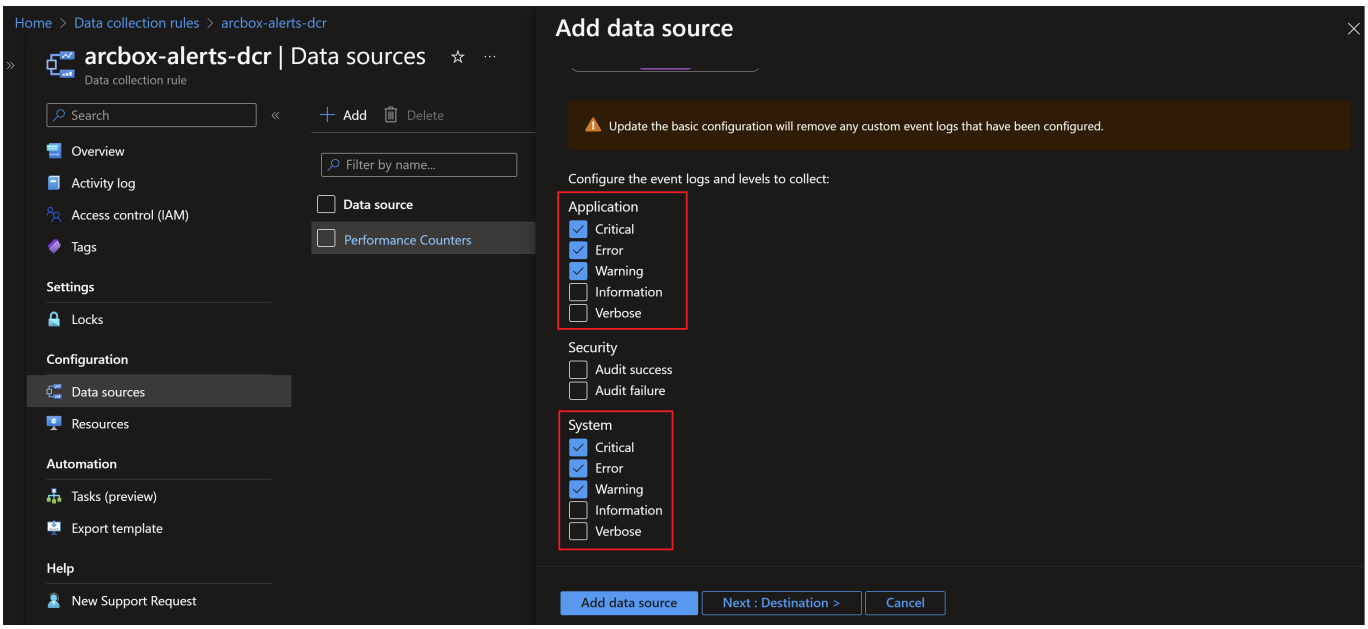
6. [] Add a new "Azure Monitor Logs" destination and select the log analytics workspace deployed in the ArcBox resource group and save.



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

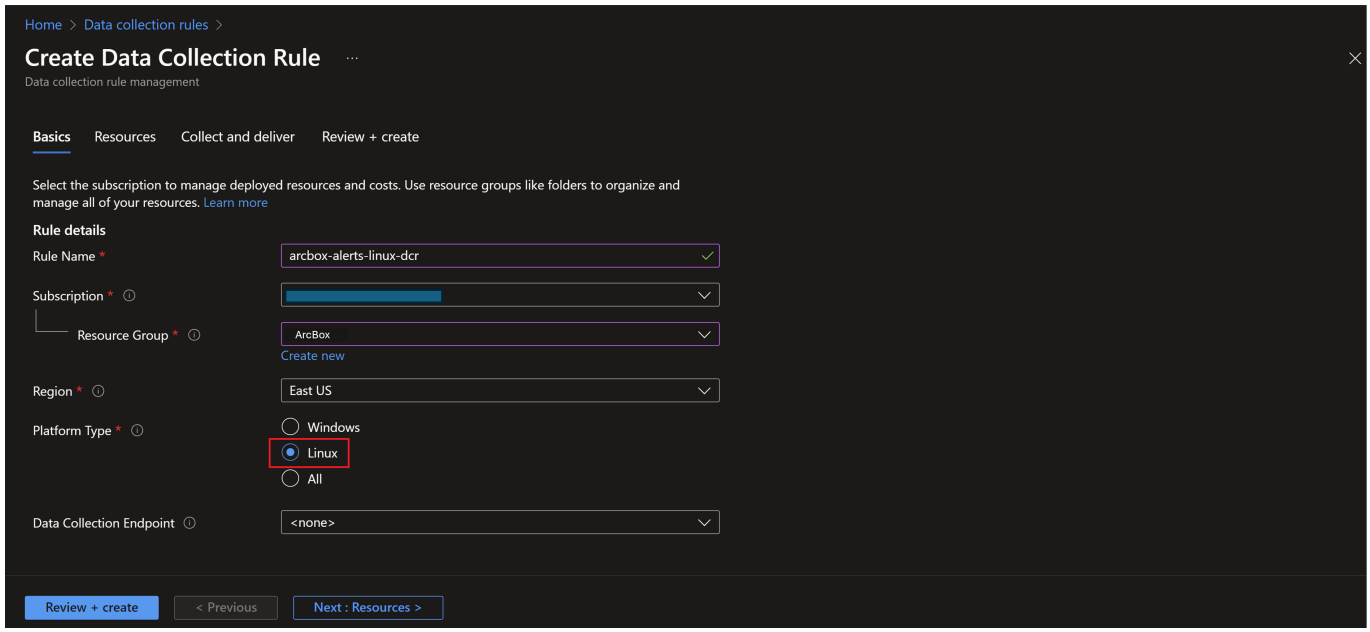


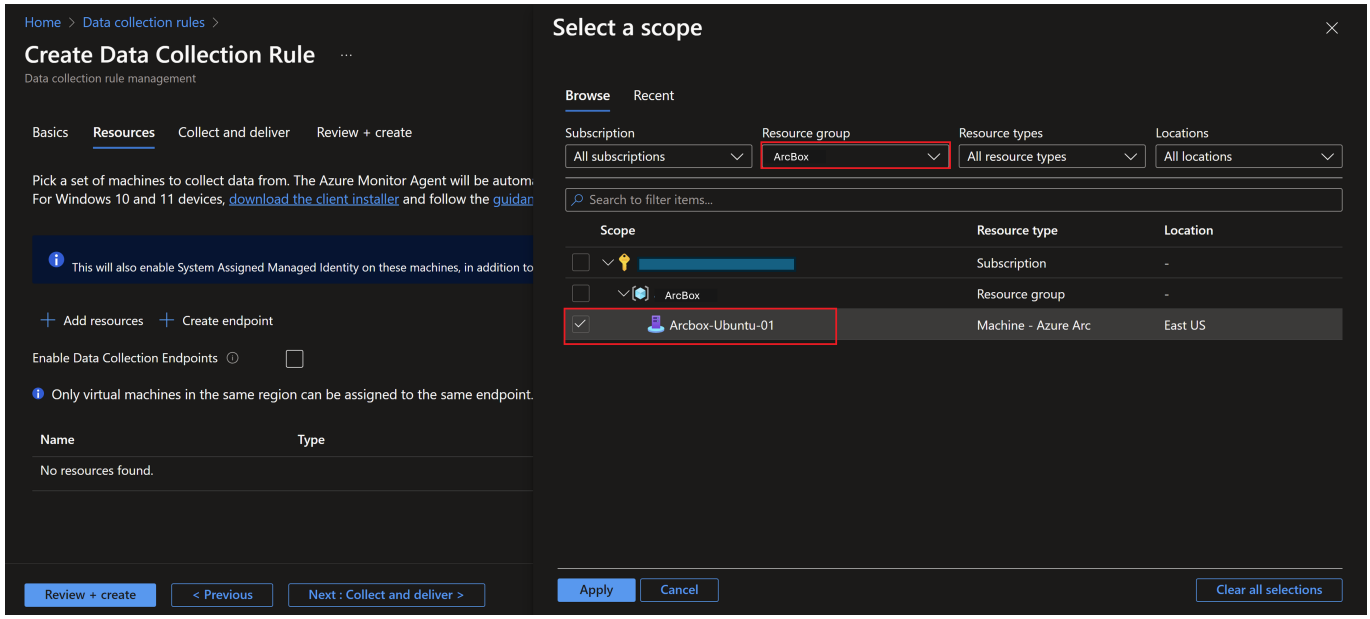
8. [] - Select *Critial*, *Error* and *Warning* events in the Application and System logs and add the data source.

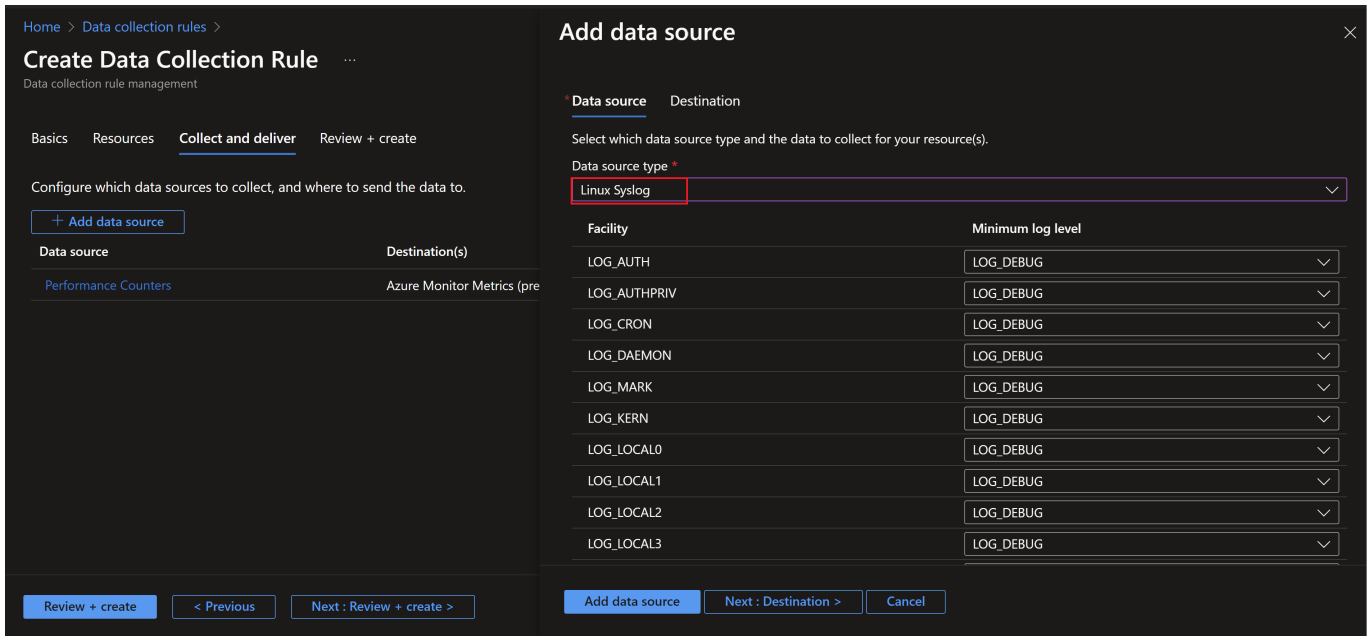


9. [] Save and create the data collection rule.

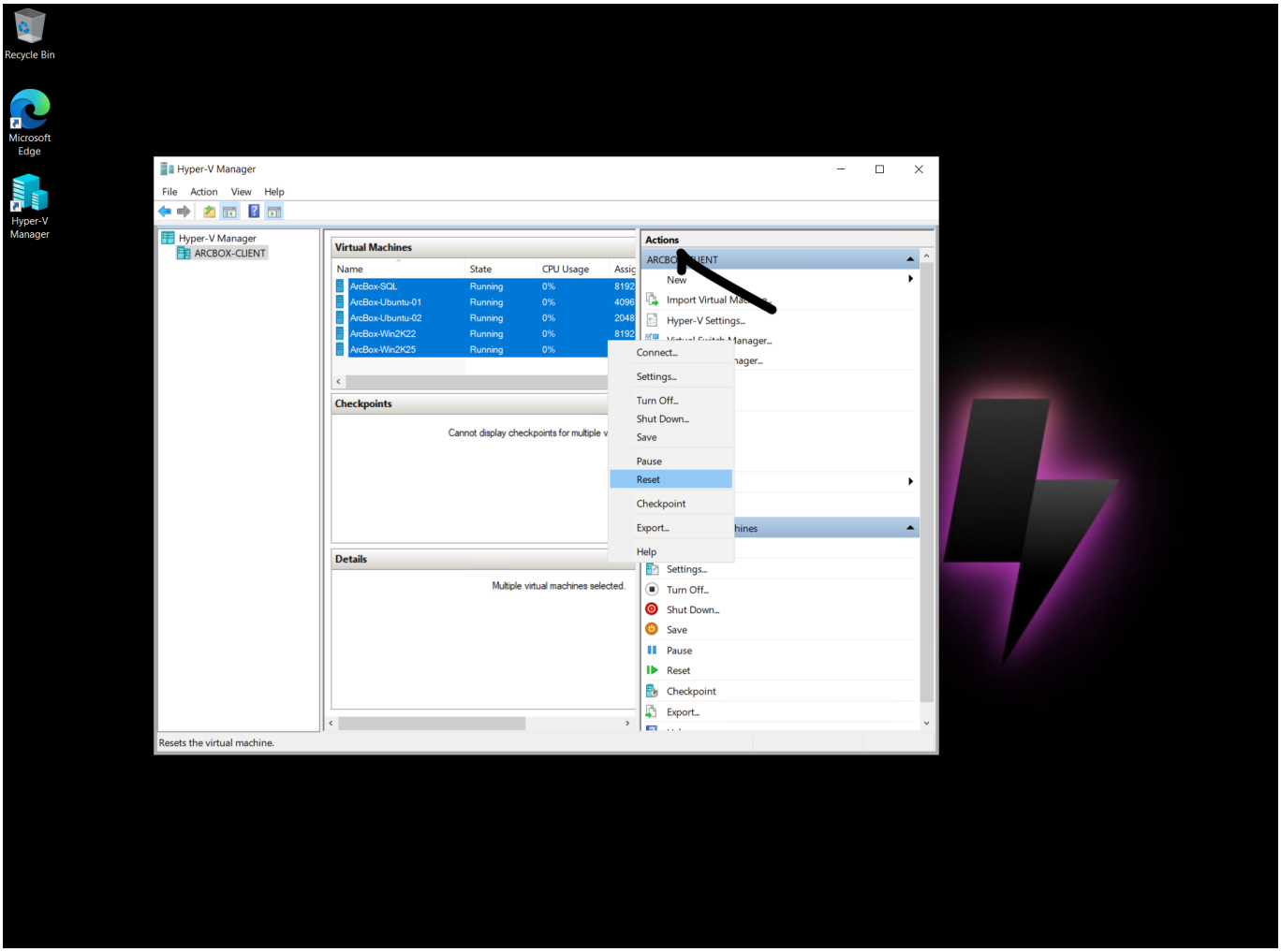
10. [] Repeat the previous steps to create another Linux data collection rule.


Home > Data collection rules >
Create Data Collection Rule
Data collection rule management
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
Rule Name * arcbox-alerts-linux-dcr
Subscription *
Resource Group * ArcBox
Create new
Region * East US
Platform Type * Windows Linux All
Data Collection Endpoint <none>
Review + create
< Previous
Next : Resources >


Home > Data collection rules >
Create Data Collection Rule
Data collection rule management
Basics Resources Collect and deliver Review + create
Pick a set of machines to collect data from. The Azure Monitor Agent will be autom
For Windows 10 and 11 devices, download the client installer and follow the guidar
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.
Review + create
< Previous
Next : Collect and deliver >
Select a scope
Browse Recent
Subscription Resource group Resource types Locations
All subscriptions ArcBox All resource types All locations
Search to filter items...
Scope Resource type Location
Subscription -
ArcBox Resource group -
Arcbox-Ubuntu-01 Machine - Azure Arc East US
Apply Cancel Clear all selections


Home > Data collection rules >
Create Data Collection Rule
Data collection rule management
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 Destination(s)
Performance Counters Azure Monitor Metrics (pre
Review + create
< Previous
Next : Review + create >
Add data source
Data source Destination
Select which data source type and the data to collect for your resource(s).
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
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

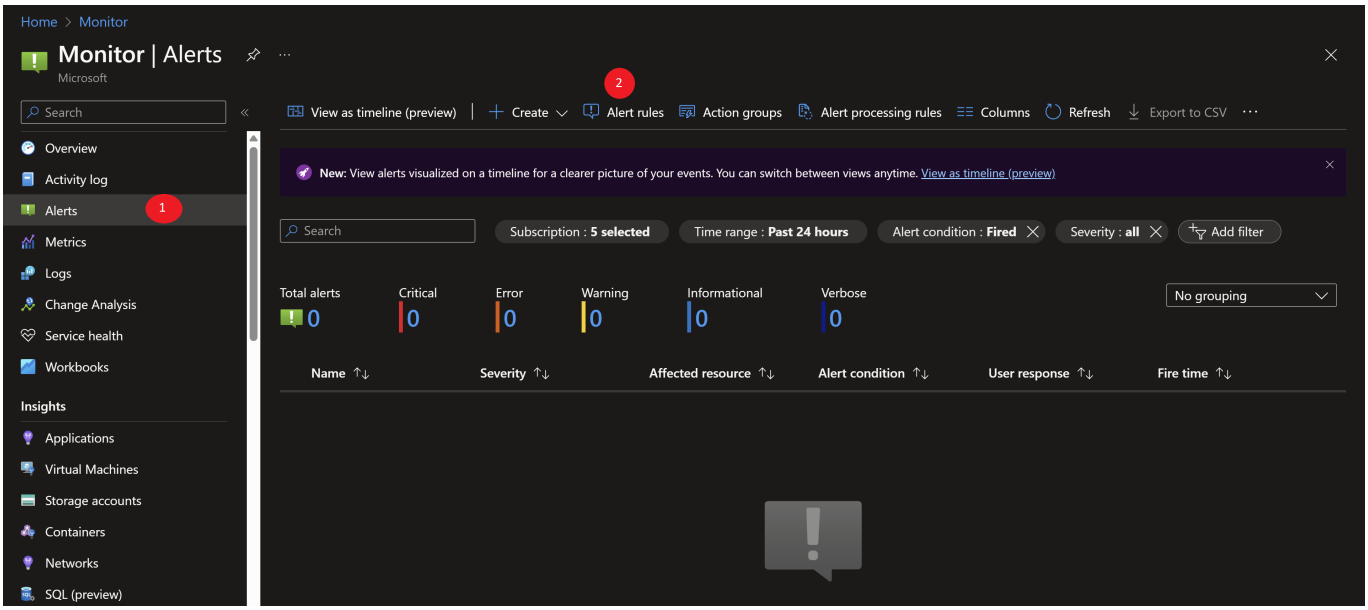
Click **Next** for the next task or **Go back to the main table of content**

===

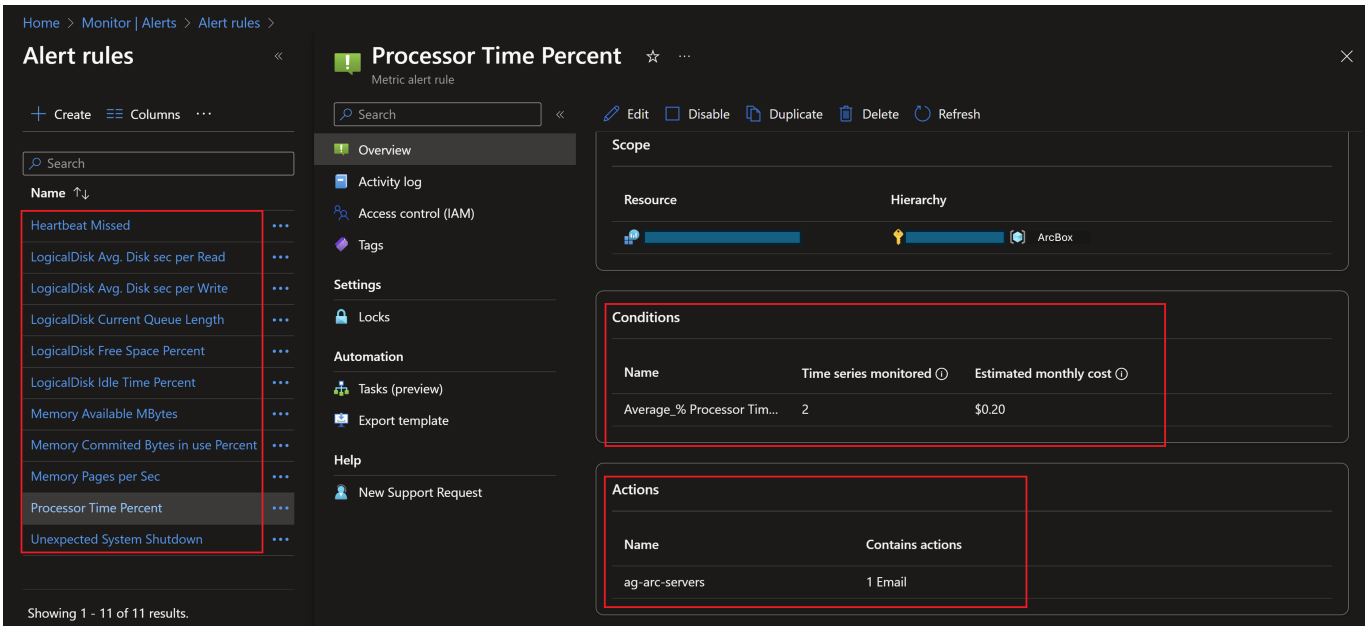
Task 3: View alerts and visualizations

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

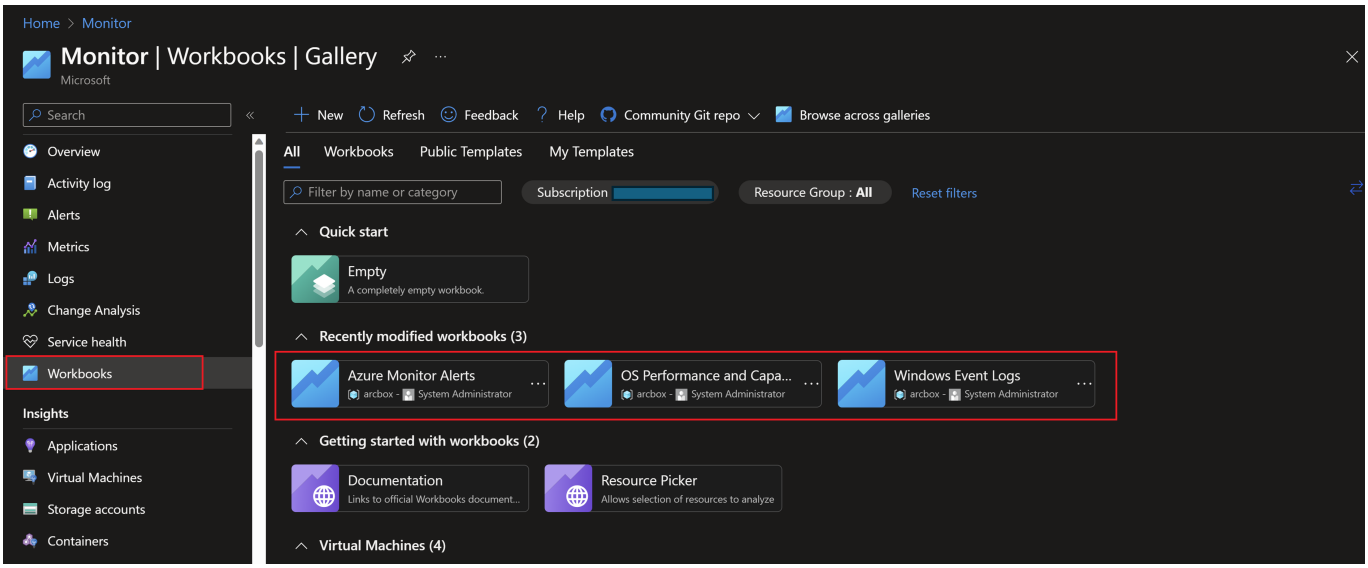
1. [] In Azure Monitor, click on *Alerts*. and select *Alert rules*

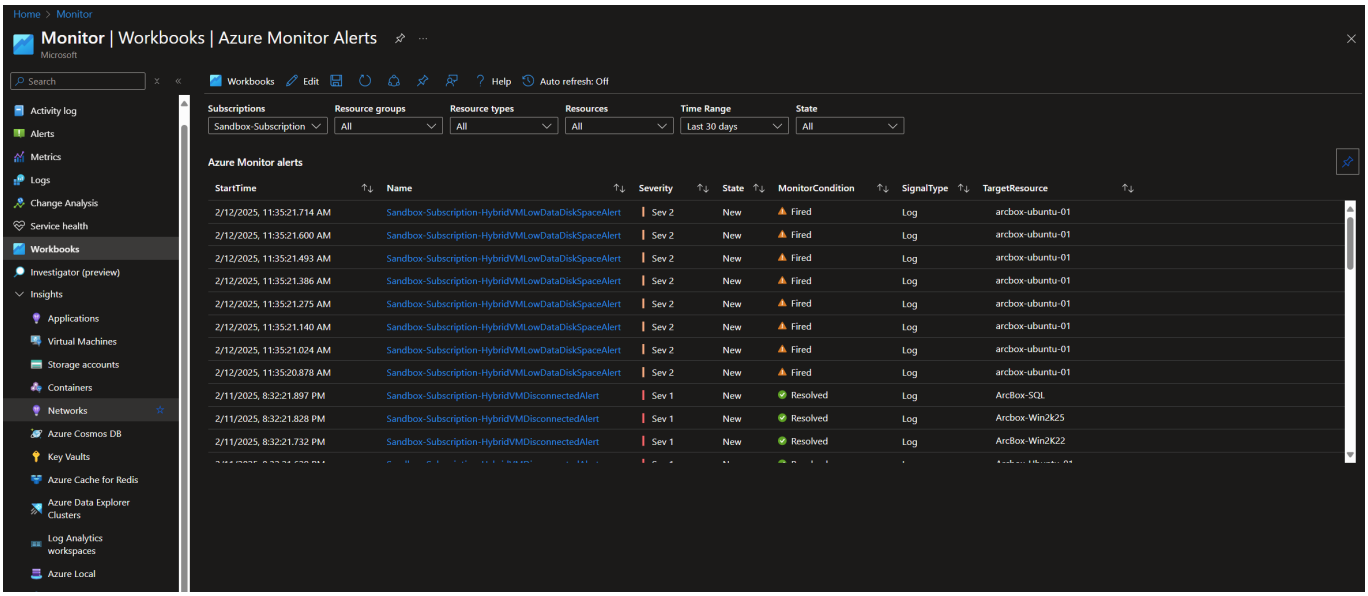


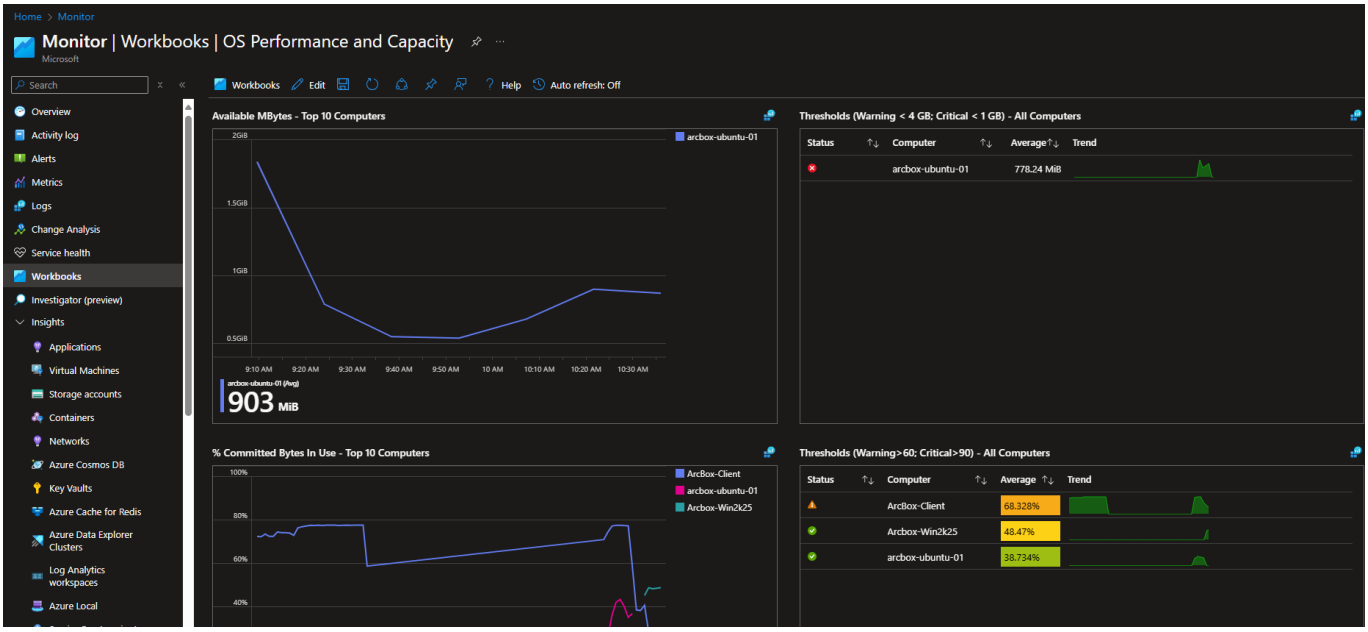
2. [] Explore the alert rules crated for you.

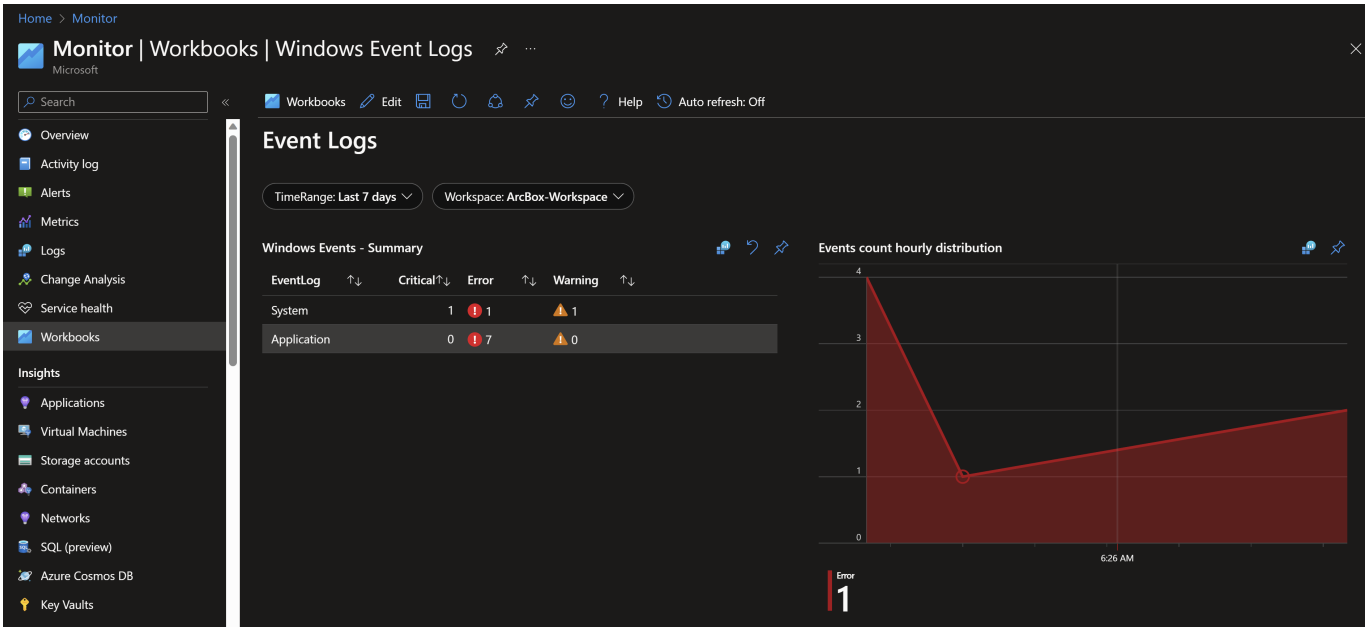


3. [] Go back to Azure Monitor and click on *Workbooks*. There are three workbooks deployed for you.









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

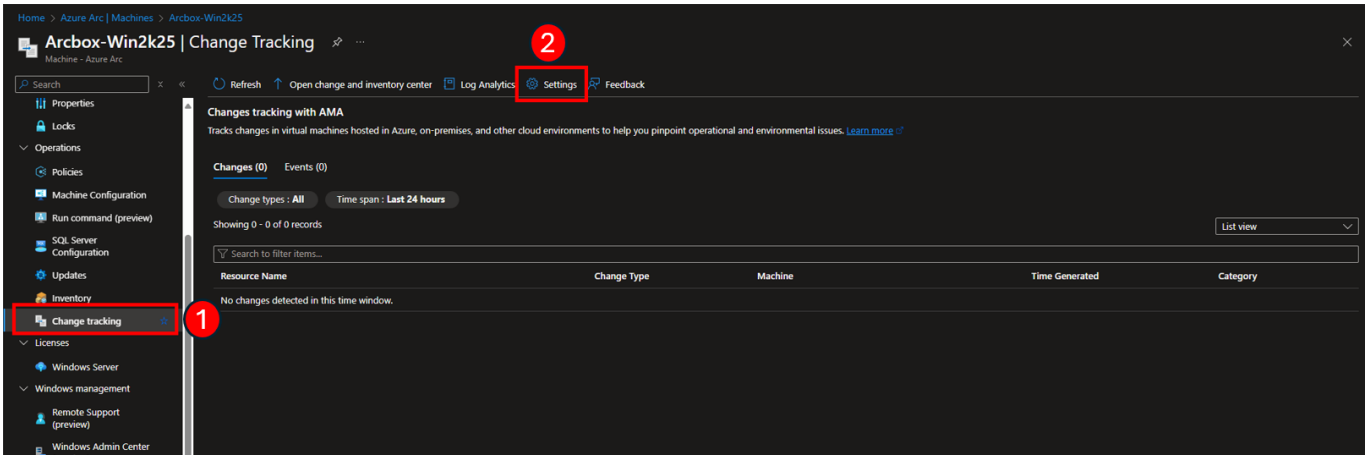
Click **Next** for the next exercise or **Go back to the main table of content**

===

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.



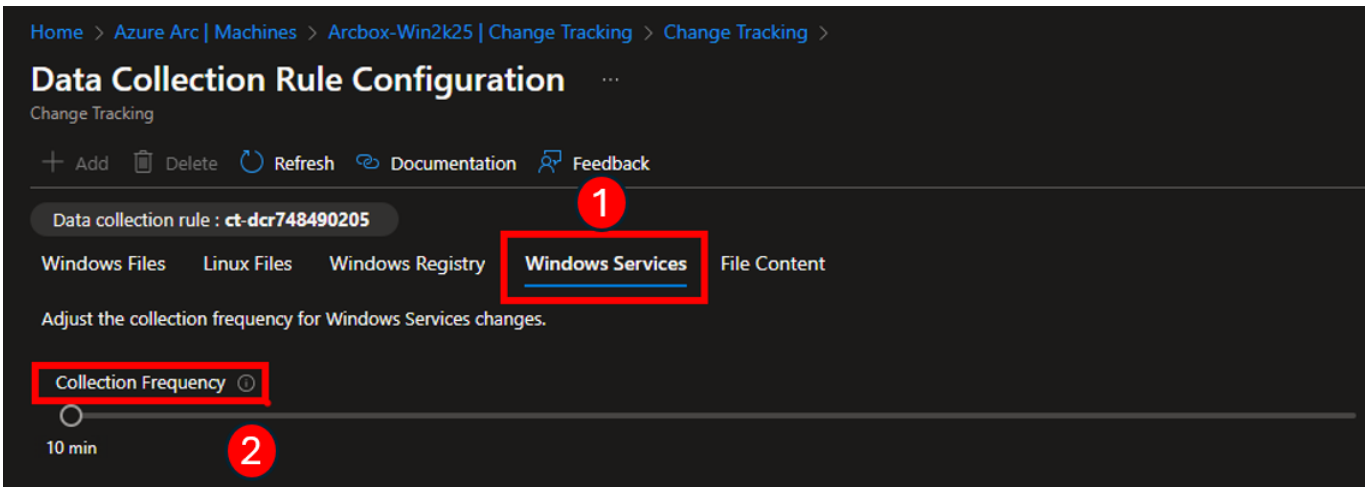
Task 2 has been completed

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.

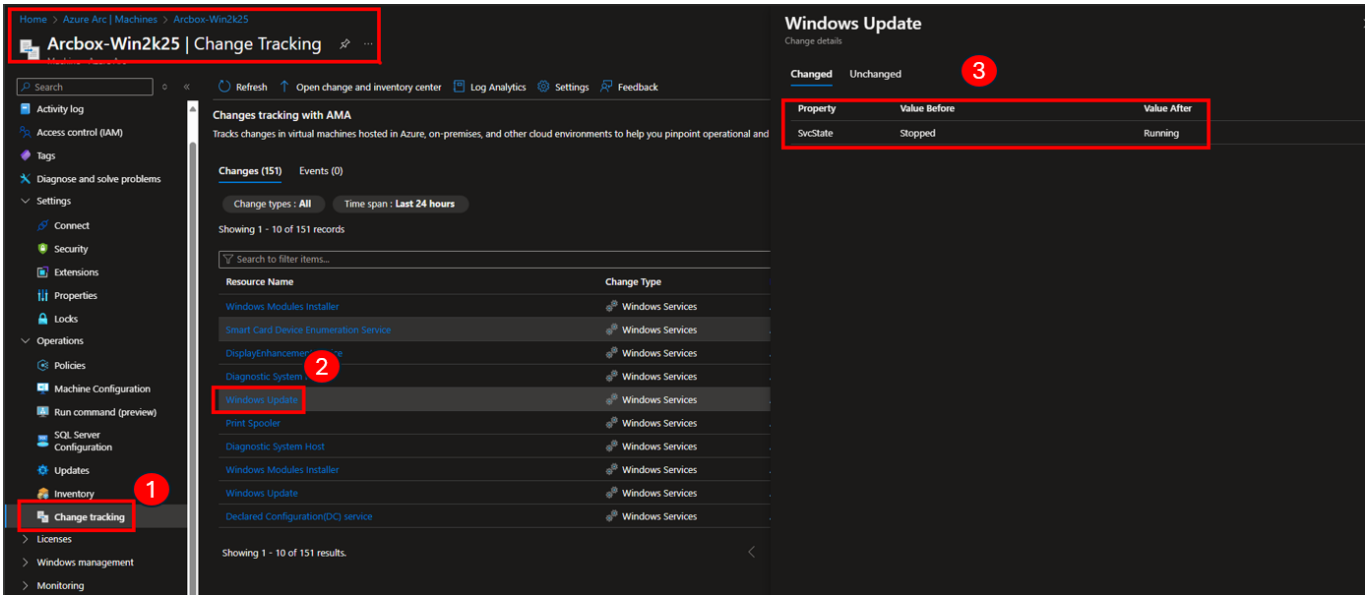


2. [] Go to the ArcBox-Client machine via RDP and from Hyper-V manager right-click on *ArcBox-Win2K25* VM then click "Connect" (Administrator default password is JS123!!). Try stopping the "Print Spooler" and the "Windows Update" services using an Administrator PowerShell session (or from the Services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

```
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).

> [!hint] **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**.



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.

```
Start-Service spooler
Start-Service wuauserv
```

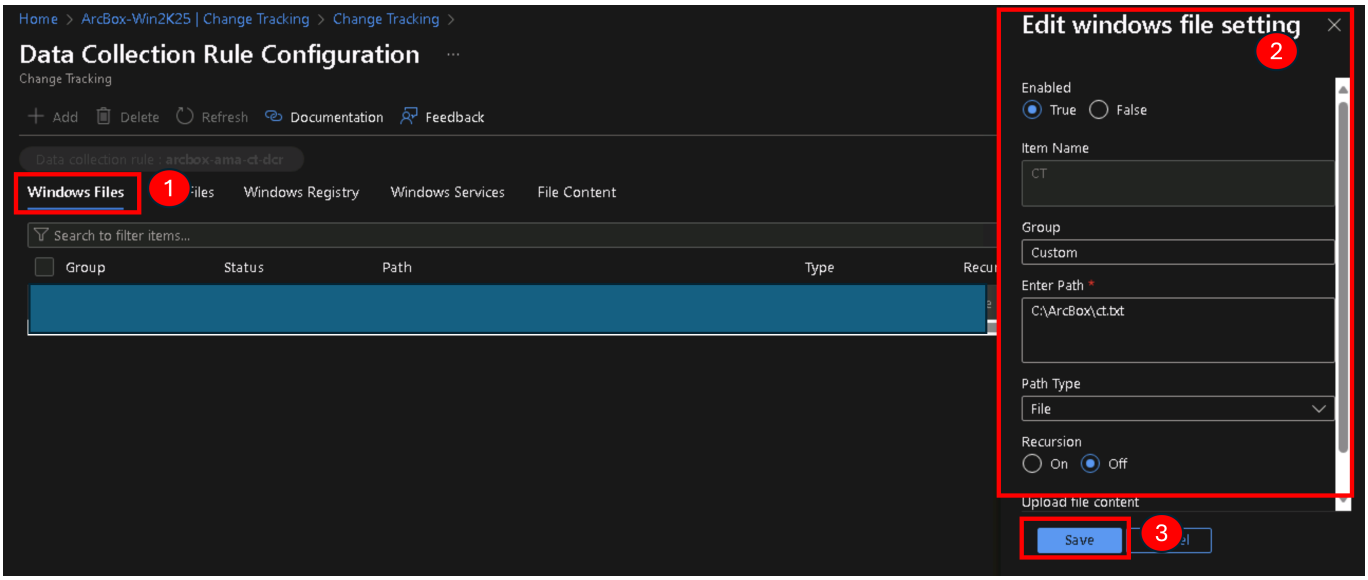
Task 3 has been completed

Click **Next** for the next exercise or **Go back to the main table of content**

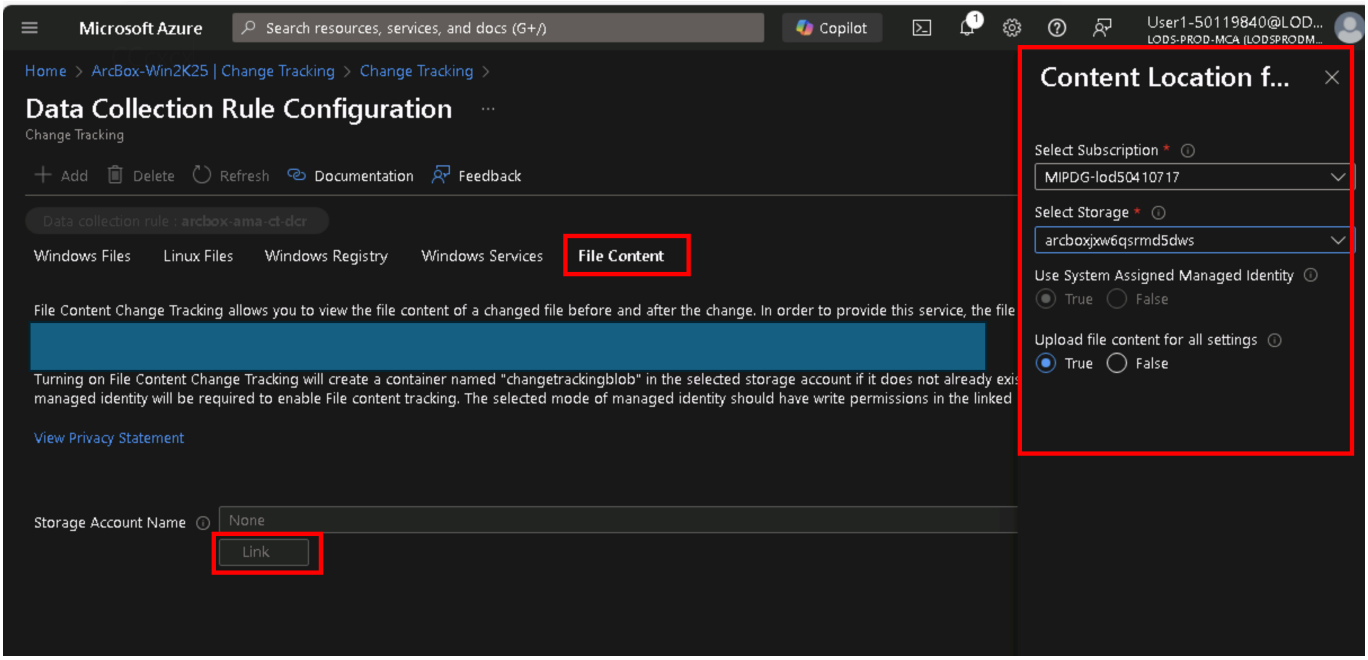
===

Task 4: Track file changes

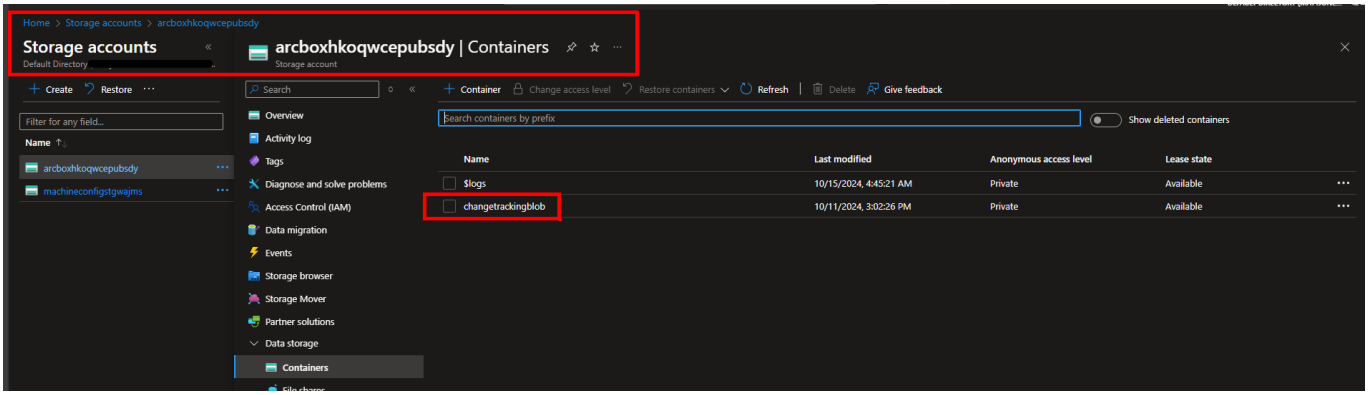
1. [] Navigate to *ArcBox-Win2K25* Arc-enabled Windows machines on the Azure Portal and select "Change tracking" then select "Settings" then select "Windows Files". You should see the "Add windows file setting" screen on the right hand side. Configure these settings to track the changes to the file "C:\ArcBox\ct.txt"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



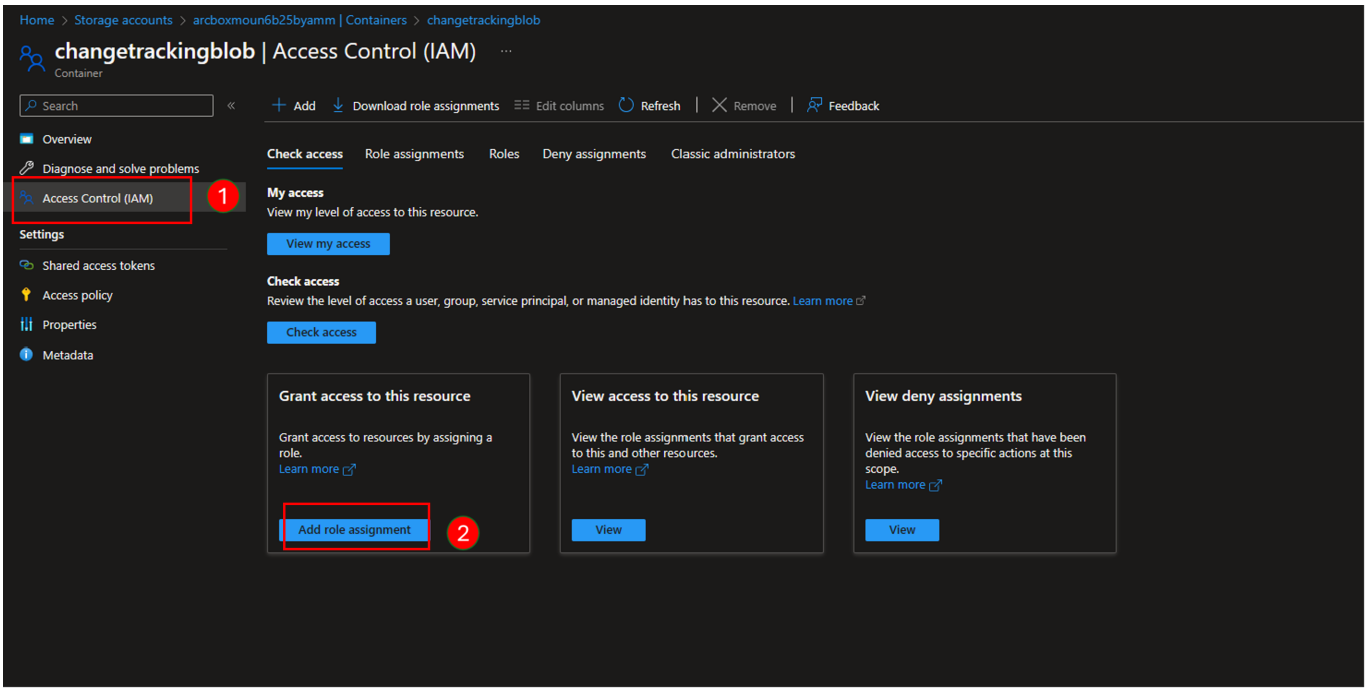
2. [] Set the file location where changed files will be uploaded. You should have a storage account deployed in the resource group of this lab. Click the *Link* button and set the parameters.



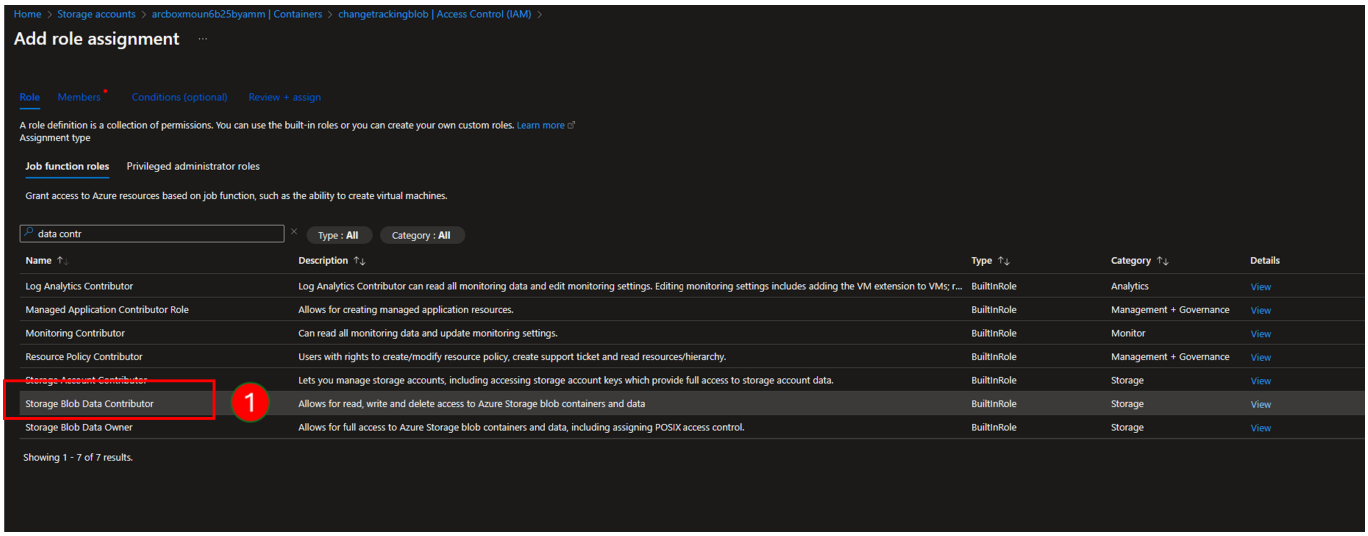
3. [] Navigate to the storage account. Click on "Containers" and you should see a container created automatically for you by Azure Change Tracking.

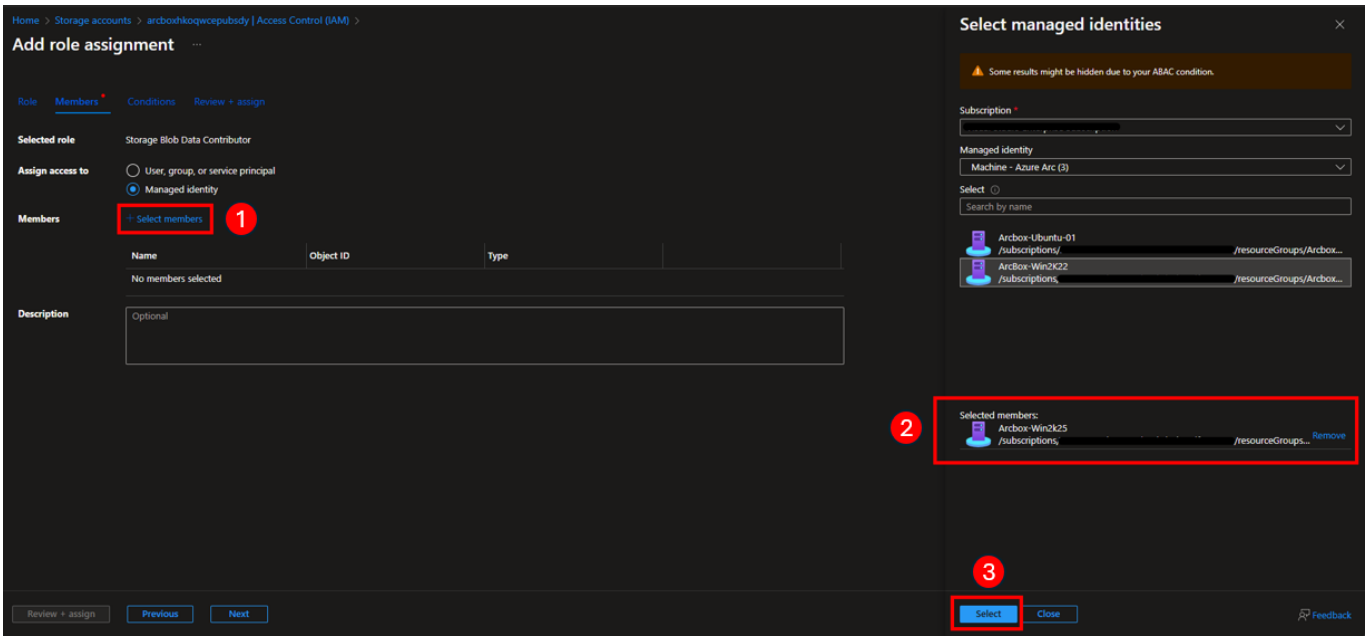


4. [] Click on the "changetrackingblob" container, and in the next page select "Access Control (IAM)", then on "Add role assignment".



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





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

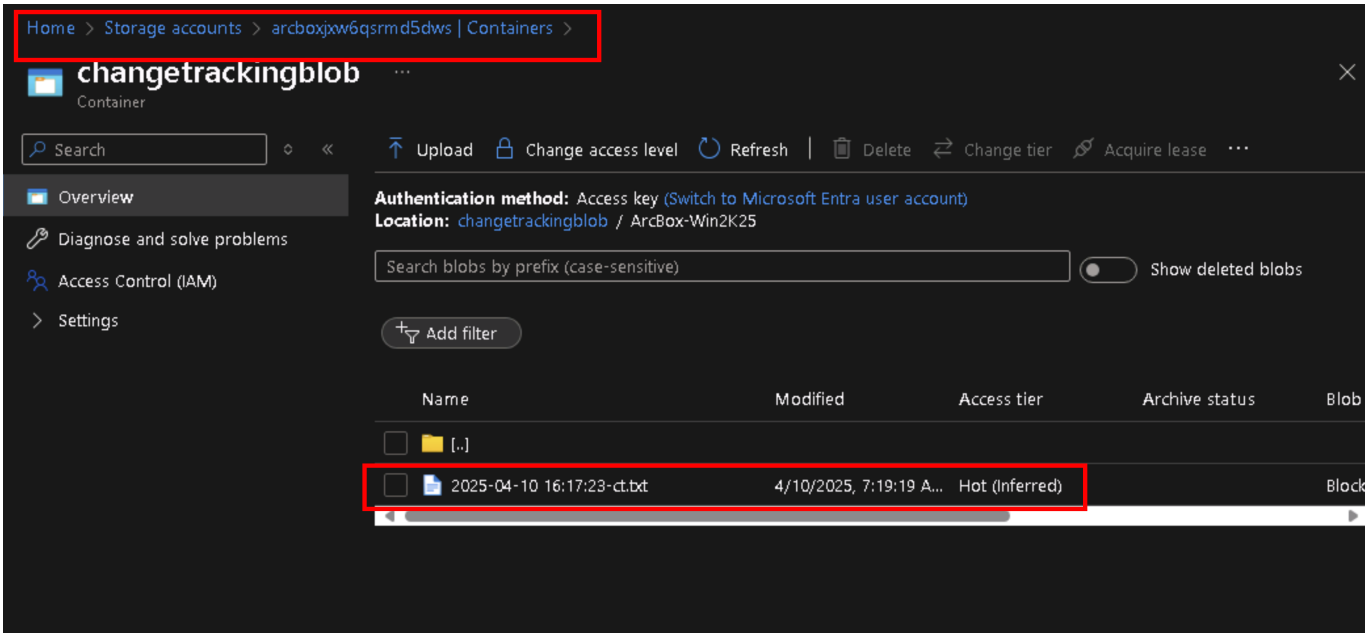
NOTE: To modify the file, open *Notepad* as Administrator, select File>Open, and then browse to C:\ArcBox\ct.txt

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

```
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.

> [!hint] **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**.



Task 4 has been completed

Click **Next** for the next exercise or **Go back to the main table of content**

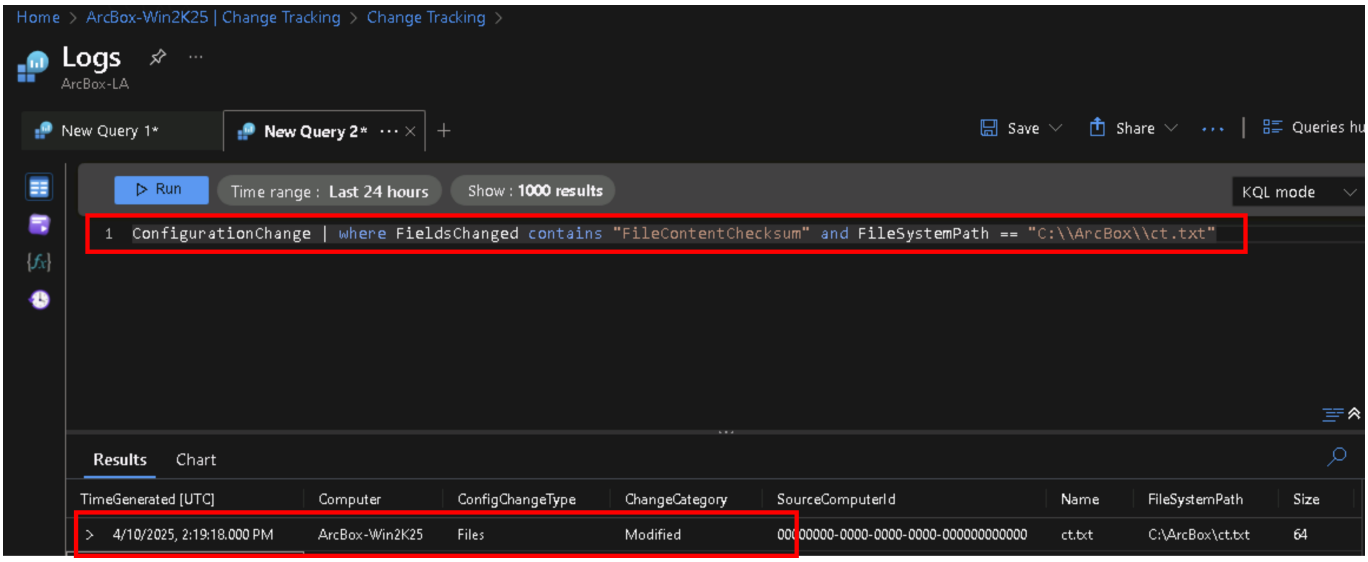
===

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.

```
ConfigurationChange | where FieldsChanged contains "FileContentChecksum" and
FileSystemPath == "C:\\ArcBox\\ct.txt"
```



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**