

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*.

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.

Name	Definition location	Policy type	Type	Definition type	Category
(ArcBox) Enable ChangeTracking and Inventory for Arc-enabled machines		Custom	Initiative	Change	
(ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines		Custom	Initiative	Monitor	
(ArcBox) Deploy Azure Monitor on Arc-enabled Linux machines		Custom	Initiative	Monitor	

3. [] Click "Assign Initiative".

The screenshot shows the 'Policy | Definitions' blade in the Azure portal. A policy named '(ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines' is selected. The 'Assign initiative' button is highlighted with a red box. Other buttons visible include 'Edit definition', 'Duplicate definition', and 'Delete initiative'. Below the buttons, there's a section titled 'Essentials' with details like Name, Description, Category, Version, Definition location, Definition ID, and Type. A table below lists three assignments with columns for Reference ID, Type, Evaluation type, and Default effect.

Reference ID	Type	Evaluation type	Default effect
6283192709368463229	Builtin	Automated	DeployIfNotExists
13316713835543462585	Builtin	Automated	DeployIfNotExists
15726849859455834337	Builtin	Automated	DeployIfNotExists

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

The screenshot shows the 'Assign initiative' blade. On the left, there are tabs for Basics, Advanced, Parameters, Remediation, Non-compliance messages, and Review + create. Under Basics, there's a 'Scope' section with a 'Learn more about setting the scope' link and a dropdown menu. On the right, a modal window titled 'Scope' is open, showing a 'Subscription' dropdown (labeled 2) set to a specific subscription, and a 'Resource Group' dropdown (labeled 3) set to 'ArcBox'. At the bottom of the blade, there are buttons for 'Review + create', 'Cancel', 'Previous', 'Next', 'Select' (labeled 4), and 'Clear All Selections'.

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

The screenshot shows the Azure portal interface for managing policy definitions. The top navigation bar includes 'Home', 'Policy | Definitions', and the specific definition name '(ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines'. The main content area is titled '(ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines' and has a sub-section 'Assign initiative'. Below this, there are tabs for 'Basics', 'Advanced', 'Parameters' (which is currently selected), 'Remediation', 'Non-compliance messages', and 'Review + create'. A search bar at the top allows filtering by parameter name. The 'Data Collection Rule Resource Id or Data Collection Endpoint Resource Id' field is a large input box with a placeholder 'Data Collection Rule Resource Id or Data Collection Endpoint Resource Id *'. At the bottom of the page are buttons for 'Review + create', 'Cancel', 'Previous', and 'Next'.

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.

The screenshot shows the Microsoft Azure portal homepage for a resource named 'ArcBox-Win2K19'. The top navigation bar includes 'Home', 'ArcBox-Win2K19', and a search bar containing 'data collection rules'. Below the search bar are buttons for 'All', 'Services (49)', 'Documentation (99+)', 'Resources (0)', 'Resource Groups (0)', and 'Marketplace (0)'. The main content area is titled 'Services' and lists several items: 'Data collection rules' (which is highlighted with a red box), 'Data Catalog', 'SQL databases', 'Connections', 'Azure Database for MySQL servers', 'Data Connectors', 'Data collection endpoints', 'Data factories', 'Documentation', 'Best practices for data collection rule creation and management i...', 'Add or delete tables and columns in Azure Monitor Logs - Azure ...', 'Structure of a data collection rule in Azure Monitor (preview) - Az...', 'Tools for migrating to Azure Monitor Agent from legacy agents - ...', 'Logs Ingestion API in Azure Monitor - Azure Monitor', 'Azure Monitor service limits - Azure Monitor', 'Tutorial - Editing Data Collection Rules - Azure Monitor', 'Sample data collection rule - custom logs - Azure Monitor', 'Continue searching in Azure Active Directory', and 'Give feedback'. On the left side, there is a sidebar with sections for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problem', 'Settings', 'Connect', 'Windows Admin Center (preview)', 'Security', 'Extensions', 'Properties', 'Locks', 'Operations', and 'Policies'. The 'Data collection rules' item in the 'Services' list is specifically highlighted with a red box.

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.

Name	Subscription	Resource group	Location	Data sources	Destinations
arcbox-ama-ct-dcr	Management	arcbox	East US	VM Insights, Performance Counters	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

No grouping List view

< Previous Page 1 of 1 Next > Give feedback

Home > Data collection rules > arcbox-ama-vmi-perfAndda-dcr

Search Delete Feedback CLI / PS

Overview Essentials

Resource group (move) : arcbox Data Sources : 2
Status : Provisioned Connected resources : 0
Location : East US Platform Type : All
Subscription (move) : Management
Subscription ID : Tags (edit) : Project : jumpstart_arcbox

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 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

Search Delete Feedback CLI API Versions

Resource ID /subscription /resourceGroups/arcbox/providers/Microsoft.Insights... 2022-06-01

Overview Essentials

Resource group (move) : arcbox
Status : Provisioned
Location : East US
Subscription (move) : Management
Subscription ID : e3b447fc
Tags (edit) : Project

Resource JSON

```

1  {
2      "properties": {
3          "description": "Data collection rule for VM Insights.",
4          "immutableId": "dcr-9ad99c061f2f4fb0bfe2328cbd60a371",
5          "dataSources": {
6              "performanceCounters": [
7                  {
8                      "streams": [
9                          "Microsoft-InsightsMetrics"
10                     ],
11                     "samplingFrequencyInSeconds": 60,
12                     "counterSpecifiers": [
13                         "\\\VmInsights\\DetailedMetrics"
14                     ],
15                     "name": "VMInsightsPerfCounters"
16                 }
17             ],
18             "extensions": [
19                 {
20                     "streams": [
21                         "Microsoft-ServiceMap"
22                     ],
23                     "extensionName": "DependencyAgent",
24                     "extensionSettings": {}
25                 }
26             ]
27         }
28     }
29 }
```

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

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

Assign initiative

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 * ⓘ

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.

Home > Policy

Policy | Compliance

Assign policy Assign initiative Refresh

Overview Getting started Compliance Remediation Events

Authoring Definitions Assignments Exemptions

Overall resource compliance 83% 45 out of 54

Resources by compliance state ⓘ 45 - Compliant 9 - Non-compliant 54

Non-compliant initiatives ⓘ 3 out of 7

Non-compliant policies ⓘ 40 out of 286

Name ↑	Scope ↑	Compliance state ↑	Resource compl... ↑	Non-Compliant... ↓	Non-c...
(ArcBox) Tag resources	e215c740-707e-4b1c-9...	✗ Non-compliant	89% (47 out of 53)	6	1
Azure Security Baseline	e215c740-707e-4b1c-9...	✗ Non-compliant	33% (2 out of 6)	4	28
(ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines	e215c740-707e-4b1c-9...	✗ Non-compliant	0% (0 out of 2)	2	3
MCAPSGov Audit Policies	e215c740-707e-4b1c-9...	✗ Non-compliant	0% (0 out of 1)	1	1
MCAPSGov Deny Policies	e215c740-707e-4b1c-9...	✓ Compliant	100% (1 out of 1)	0	0

Home > Policy | Compliance >

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

Initiative compliance

[View assignment](#) [Create remediation task](#) [Create exemption](#) [Activity Logs](#)

[Essentials](#)

Name : (ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines
Description : --
Assignment ID : /subscriptions/.../resourcegroups/arcbox/providers...

Scope : Management/arcbox

Compliance state : Non-compliant (Red)
Overall resource compliance : 0% (0 out of 2)
Resources by compliance state : 0 - Compliant (Green), 2 - Non-compliant (Red)
Non-compliant policies : 3 out of 3

[Policies](#) [Non-compliant resources](#)

Filter by policy name or definition ID... Compliance state : All compliance states

Name ↓	Effect Type ↓	Compliance state ↓	Non-Compliant Resources ↓	Total resources ↓
Configure Windows Machines to be associated with a Data DeploymentEviction	DeployIfNotEvict	Non-compliant	2	2

Home > Policy | Compliance > (ArcBox) Deploy Azure Monitor on Arc-enabled Windows machines > New remediation task ...

Remediation action

Policy to remediate : 15726849859455834337

[View definition](#)

Description:

Automate the deployment of Azure Monitor Agent extension on your Windows Arc-enabled machines for collecting telemetry data from the guest OS. This policy will install the extension if the OS and region are supported and system-assigned managed identity is enabled, and skip install otherwise. Learn more: <https://aka.ms/AMAOversight>.

Remediation settings

Failure Threshold (percentage) : 100

Resource Count : 500

Applicable resources to remediate

Scope : Visual Studio Enterprise Subscription

Re-evaluate resource compliance before remediating

Locations

All selected

Name ↓	Resource type ↓	Location	Scope ↓
arcbox-win2k25	Microsoft.HybridCompute/machines	Central US	██████████
arcbox-win2k22	Microsoft.HybridCompute/machines	Central US	██████████

[Remediate](#) [Cancel](#)

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.

REMEDIATION ACTION

Policy to remediate *

- 6283192709368463229
- 6283192709368463229
- 13316713835543462585
- 15726849859455834337

Dependency agent virtual machine extension. VM insights uses the Dependency agent to collect network metrics and discovered data about processes running on the machine and external process dependencies. See more - <https://aka.ms/vminsightsdocs>.

REMEDIATION SETTINGS

Failure Threshold (percentage) 100

Resource Count * 500

Parallel Deployments * 1

Remediate Cancel

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.

Home > Policy

Policy | Remediation

Scope

Policies to remediate Remediation tasks

Remediation task would not be shown if its corresponding assignment is deleted. During remediation task creation, if a policyDefinitionReferenceId parameter is specified, its value should be the same as it is specified in the initiative definition.

Start Time	Remediation State	Policy Definition	Scope	Locations
9/6/2023, 1:57 PM	✓ Complete	Configure Windows Arc-enabled machines to run Azure Monitor Agent	All	All
9/6/2023, 1:57 PM	✓ Complete	Configure Windows Machines to be associated with a Data Collection Rule or a Data... Configure Dependency agent on Azure Arc enabled Windows servers	All	All
9/6/2023, 1:54 PM	✓ Complete	Configure Dependency agent on Azure Arc enabled Windows servers	All	All

Home > Arcbox-Win2k25

Arcbox-Win2k25 | Extensions

Machine - Azure Arc

Name	Type	Version	Update available	Status	Automatic upgrade
AzureMonitorWindowsAgent	AzureMonitorWindowsAgent	1.31.0.0	No	Succeeded	Enabled
DependencyAgentWindows	DependencyAgentWindows	9.10.18.4770	No	Succeeded	Enabled
MDE.Windows	MDE.Windows	1.0.11.3	No	Succeeded	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 these two machines to see the data collected by VM insights.

Arcbox-Win2k25 | Insights

Get started **Performance** Map

Logical Disk Performance

DISK	CURRENT SIZE (GB)	CURRENT USED (%)	P95 IOPS READ	P95 IOPS WRITE	P95 IOPS TOTAL	P95 MB/s READ	P95 MB/s WRITE	P95 MB/s TOTAL
No Data								

CPU Utilization % **1m granularity**

Available Memory **1m granularity**

Arcbox-Ubuntu-01 | Insights

Get started **Performance** Map

Logical Disk Performance

DISK	CURRENT SIZE (GB)	CURRENT USED (%)	P95 IOPS READ	P95 IOPS WRITE	P95 IOPS TOTAL	P95 MB/s READ	P95 MB/s WRITE	P95 MB/s TOTAL
/	47.56	26%	0	12.37	12.37	0	0.05	0.05
/boot	0.95	33%	0	0	0	0	0	0
/boot/efi	0.5		0	0	0	0	0	0
/snap/core18/2667	0.05	100%	0	0	0	0	0	0
/snap/core18/2785	0.05	100%	0	0	0	0	0	0
/snap/core20/1778	0.06	100%	0	0	0	0	0	0
/snap/core20/1950	0.06	100%	0	0	0	0	0	0
/snap/lxd/22753	0.07	100%	0	0	0	0	0	0
/snap/lxd/24061	0.09	100%	0	0	0	0	0	0

Task 1 has been completed

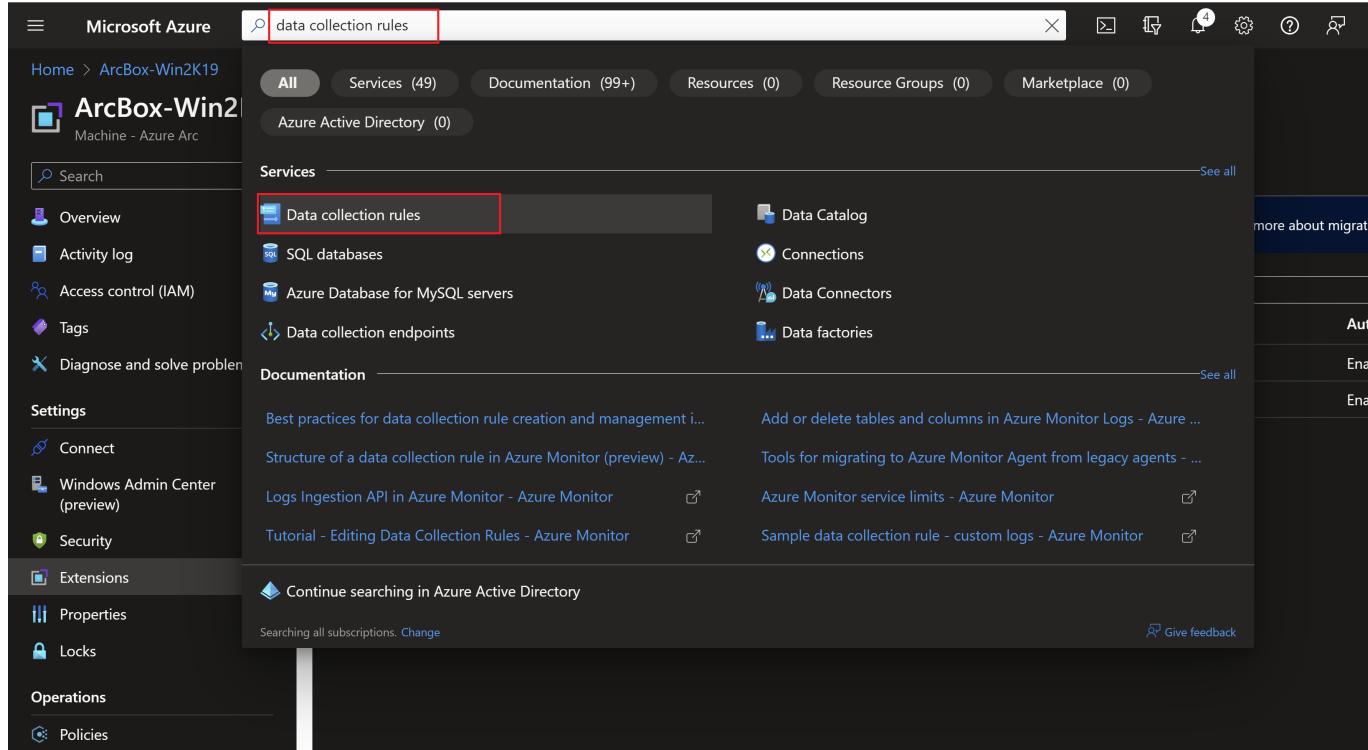
Click **Next** for the next task or [Go back to the main table of content](#)

====

Task 2: Configure data collection for logs and metrics

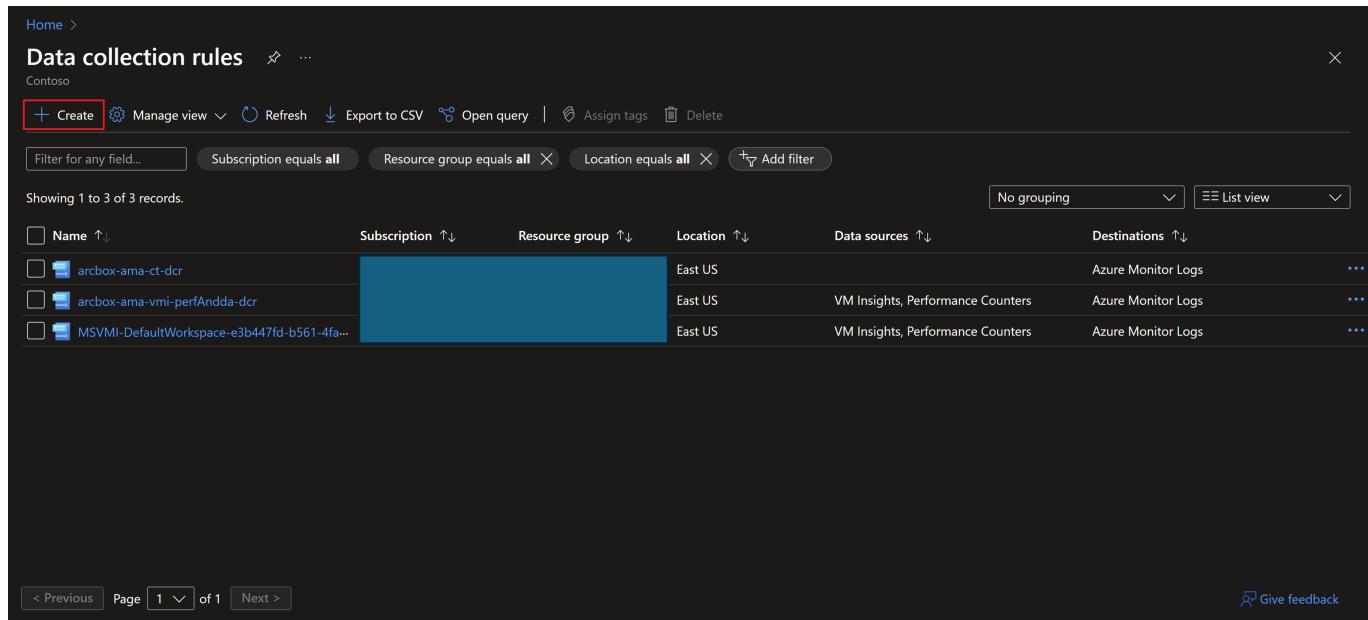
As part of the ArcBox automation, some alerts and workbooks have been created to demonstrate the different monitoring operations you can perform after onboarding the Arc-enabled machines. You will now configure some data collection rules to start sending the needed metrics and logs to the Log Analytics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

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



The screenshot shows the Microsoft Azure portal interface. The search bar at the top contains the text "data collection rules". Below the search bar, the "Services" section is expanded, showing various Azure services. The "Data collection rules" item is highlighted with a red box. Other visible items include Data Catalog, SQL databases, Azure Database for MySQL servers, Data collection endpoints, Data Connectors, Data factories, and several documentation links. The left sidebar shows navigation categories like Home, Services, Documentation, Resources, Resource Groups, Marketplace, and more.

2. [] Create a new data collection rule.



The screenshot shows the "Data collection rules" list page. The "Create" button is highlighted with a red box. The page displays three data collection rules:

Name	Subscription	Resource group	Location	Data sources	Destinations
arcbox-ama-ct-dcr	Contoso		East US		Azure Monitor Logs
arcbox-ama-vmi-perfAdda-dcr	Contoso		East US	VM Insights, Performance Counters	Azure Monitor Logs
MSVMI-DefaultWorkspace-e3b447fd-b561-4fa...	Contoso		East US	VM Insights, Performance Counters	Azure Monitor Logs

Pagination controls at the bottom indicate "Page 1 of 1". A "Give feedback" link is located in the bottom right corner.

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

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 * ✓

Subscription * ▾

Resource Group * ▾

Create new

Region * ▾

Platform Type * Windows Linux All

Data Collection Endpoint ▾

[Review + create](#) [< Previous](#) [Next : Resources >](#)

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

Home > Data collection rules >

Create Data Collection Rule

Data collection rule management

Basics **Resources** Collect and deliver Tags Review + create

To create a Collection Rule that collects platform metrics, click here. 1

Pick a set of resources to collect data from. The Azure Monitor Agent will be automatically installed on virtual machines, scale sets, and Arc-enabled servers. For AKS clusters for Windows 10 and 11 devices, [download the client installer](#) and follow the [guidance](#).

+ Add resources + Create endpoint

Enable Data Collection Endpoints

Only resources in the same region can be assigned to the same endpoint. [Learn more](#) 2

Name	Type	Location
No resources found.		

Select a scope

Browse Recent

Subscription ▾ Resource group ▾ Resource types All resource types ▾ Locations All locations ▾

Search to filter items...

Scope	Resource type	Location
<input type="checkbox"/> ArcBox	Subscription	-
<input type="checkbox"/> Arcbox-Win2k25	Resource group	-
<input checked="" type="checkbox"/> Arcbox-Win2k25	Machine - Azure Arc	Central US

3 4 5

[Review + create](#) [< Previous](#) [Next : Collect and deliver >](#) [Apply](#) [Cancel](#) [Clear all selections](#)

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

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 **2**

Data source Destination(s)

No standard data sources or destinations found.

This data collection rule doesn't have any data sources or destinations selected.

Add data source Next : Review + create < Previous Next : Destination > Cancel

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

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)

Add data source Next : Review + create < Previous Next : Destination > Save Cancel

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

The screenshot shows the Arcbox interface. On the left, the navigation menu includes Home, Data collection rules, arcbox-alerts-dcr (selected), Data sources (highlighted), Overview, Activity log, Access control (IAM), Tags, Settings, Locks, Configuration (highlighted), Data sources (selected), Resources, Automation, Tasks (preview), Export template, Help, and New Support Request. On the right, the 'Add data source' dialog is open, showing the 'Data source' tab selected. Step 1 points to the 'Add' button in the top-left corner of the main interface. Step 2 points to the 'Data source' tab in the dialog. Step 3 points to the 'Windows Event Logs' dropdown under 'Data source type'. Step 4 points to the 'Basic' configuration option.

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

The screenshot shows the Arcbox interface. The left sidebar is identical to the previous screenshot. The right side shows the 'Add data source' dialog. A red box highlights the 'Application' section where 'Critical', 'Error', and 'Warning' checkboxes are checked. Another red box highlights the 'System' section where 'Critical', 'Error', and 'Warning' checkboxes are also checked. The 'Information' and 'Verbose' checkboxes are unchecked in both sections.

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 *

Subscription *

Resource Group * [Create new](#)

Region *

Platform Type * [Windows](#) [All](#)

Data Collection Endpoint

[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 automatically installed. For Windows 10 and 11 devices, [download the client installer](#) and follow the [guidance](#).

This will also enable System Assigned Managed Identity on these machines, in addition to User Assigned Managed Identity.

+ Add resources + Create endpoint

Enable Data Collection Endpoints

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

Name	Type	Scope	Resource type	Location
No resources found.				
Arcbox-Ubuntu-01	Machine - Azure Arc	ArcBox	Subscription	-

[Review + create](#) [< Previous](#) [Next : Collect and deliver >](#) [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 (previews)

[Review + create](#) [< Previous](#) [Next : Review + create >](#)

Add data source

* Data source [Destination](#)

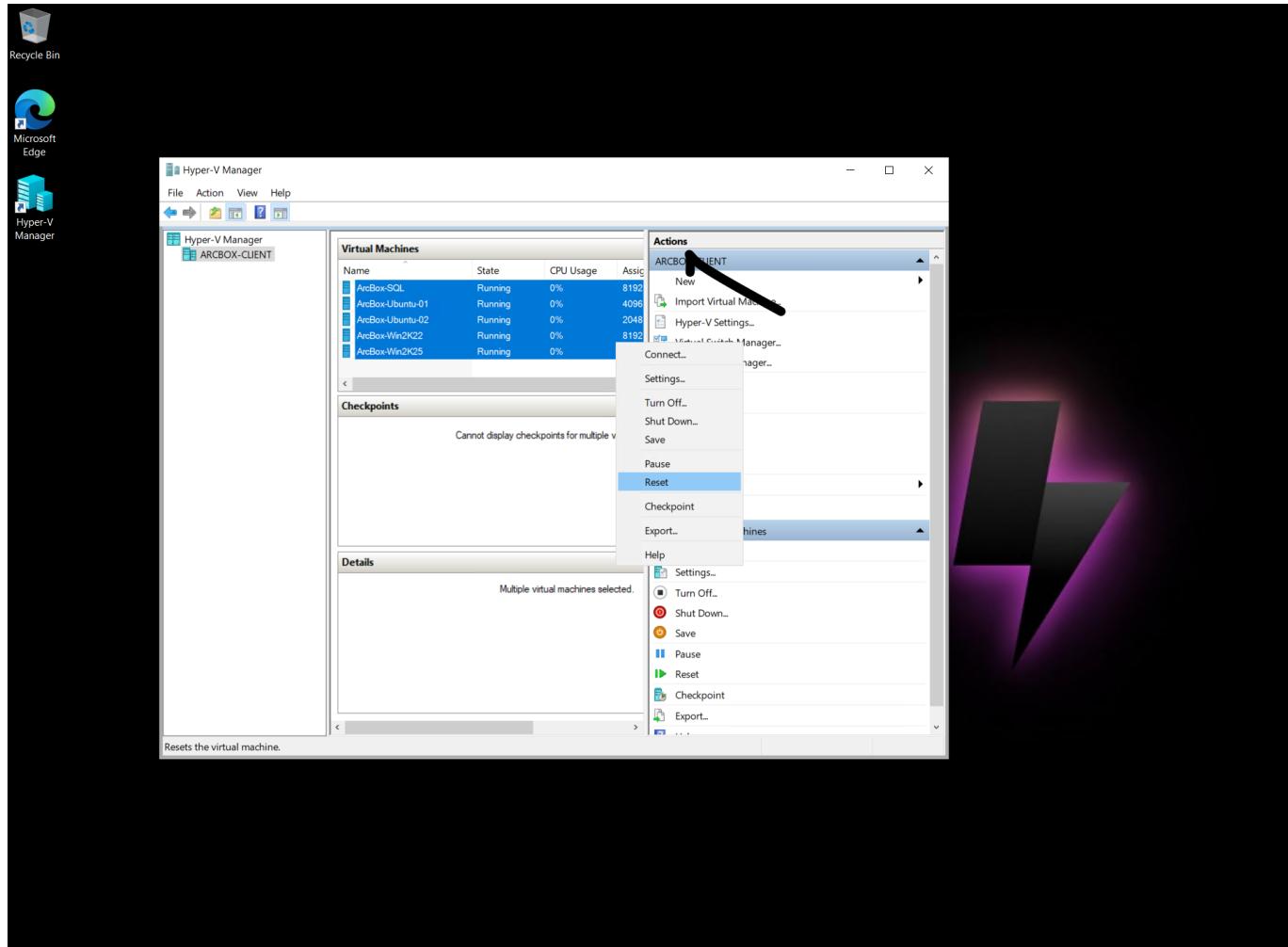
Select which data source type and the data to collect for your resource(s).

Data source type *

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*

The screenshot shows the Azure Monitor Alerts interface. On the left, there's a navigation sidebar with links like Overview, Activity log, Alerts (which has a red notification badge '1'), Metrics, Logs, Change Analysis, Service health, Workbooks, Insights (Applications, Virtual Machines, Storage accounts, Containers, Networks, SQL (preview)), and Help. The main area has a search bar, a 'View as timeline (preview)' button, and a 'Create' button. It displays a summary of alerts: Total alerts (0), Critical (0), Error (0), Warning (0), Informational (0), and Verbose (0). Below this is a table with columns: Name (sorted by name), Severity (sorted by severity), Affected resource (sorted by affected resource), Alert condition (sorted by alert condition), User response (sorted by user response), and Fire time (sorted by fire time). A large exclamation mark icon is centered at the bottom.

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

The screenshot shows the Alert rules page for the 'Processor Time Percent' metric. The left sidebar lists various alert rules: Heartbeat Missed, 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 (which is selected and shown in detail), and Unexpected System Shutdown. The main pane shows the details for the 'Processor Time Percent' rule, including its scope (Resource: ArcBox) and conditions (Time series monitored: Average.%Processor Tim... 2, Estimated monthly cost: \$0.20). The actions section shows one email action associated with the rule.

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

The screenshot shows the Workbooks | Gallery page. The left sidebar includes links for Overview, Activity log, Alerts, Metrics, Logs, Change Analysis, Service health, and Workbooks (which is selected and highlighted with a red box). Other links in the sidebar include Applications, Virtual Machines, Storage accounts, and Containers. The main area shows a 'Quick start' section with an 'Empty' workbook (a completely empty workbook). Below it is a 'Recently modified workbooks (3)' section, which contains three workbooks: 'Azure Monitor Alerts' (by arcbox - System Administrator), 'OS Performance and Capa...' (by arcbox - System Administrator), and 'Windows Event Logs' (by arcbox - System Administrator). These three workbooks are also highlighted with a red box. Other sections visible include 'Getting started with workbooks (2)', 'Documentation' (links to official Workbooks documentation), 'Resource Picker' (allows selection of resources to analyze), and 'Virtual Machines (4)'.

Monitor | Workbooks | Azure Monitor Alerts

Subscriptions: Sandbox-Subscription | Resource groups: All | Resource types: All | Resources: All | Time Range: Last 30 days | State: All

StartTime	Name	Severity	State	MonitorCondition	SignalType	TargetResource
2/12/2025, 11:35:21.714 AM	Sandbox-Subscription-HybridVMLowDataDiskSpaceAlert	Sev 2	New	⚠ Fired	Log	arcbox-ubuntu-01
2/12/2025, 11:35:21.600 AM	Sandbox-Subscription-HybridVMLowDataDiskSpaceAlert	Sev 2	New	⚠ Fired	Log	arcbox-ubuntu-01
2/12/2025, 11:35:21.493 AM	Sandbox-Subscription-HybridVMLowDataDiskSpaceAlert	Sev 2	New	⚠ Fired	Log	arcbox-ubuntu-01
2/12/2025, 11:35:21.386 AM	Sandbox-Subscription-HybridVMLowDataDiskSpaceAlert	Sev 2	New	⚠ Fired	Log	arcbox-ubuntu-01
2/12/2025, 11:35:21.275 AM	Sandbox-Subscription-HybridVMLowDataDiskSpaceAlert	Sev 2	New	⚠ Fired	Log	arcbox-ubuntu-01
2/12/2025, 11:35:21.140 AM	Sandbox-Subscription-HybridVMLowDataDiskSpaceAlert	Sev 2	New	⚠ Fired	Log	arcbox-ubuntu-01
2/12/2025, 11:35:21.024 AM	Sandbox-Subscription-HybridVMLowDataDiskSpaceAlert	Sev 2	New	⚠ Fired	Log	arcbox-ubuntu-01
2/12/2025, 11:35:20.878 AM	Sandbox-Subscription-HybridVMDisconnectedAlert	Sev 1	New	🟢 Resolved	Log	ArcBox-SQL
2/11/2025, 8:32:21.897 PM	Sandbox-Subscription-HybridVMDisconnectedAlert	Sev 1	New	🟢 Resolved	Log	ArcBox-Win2k25
2/11/2025, 8:32:21.828 PM	Sandbox-Subscription-HybridVMDisconnectedAlert	Sev 1	New	🟢 Resolved	Log	ArcBox-Win2k22
2/11/2025, 8:32:21.732 PM	Sandbox-Subscription-HybridVMDisconnectedAlert	Sev 1	New	🟢 Resolved	Log	ArcBox-Win2k22

Monitor | Workbooks | OS Performance and Capacity

Available MBytes - Top 10 Computers

9:10 AM 9:20 AM 9:30 AM 9:40 AM 9:50 AM 10 AM 10:10 AM 10:20 AM 10:30 AM

arcbox-ubuntu-01 (Avg) 1903 MiB

Thresholds (Warning < 4 GB; Critical < 1 GB) - All Computers

Status	Computer	Average	Trend
🔴	arcbox-ubuntu-01	778.24 MiB	Upward

% Committed Bytes In Use - Top 10 Computers

Thresholds (Warning>60; Critical>90) - All Computers

Status	Computer	Average	Trend
⚠	ArcBox-Client	68.328%	Upward
🟢	Arcbox-Win2k25	48.47%	Upward
🟢	arcbox-ubuntu-01	38.734%	Upward

Monitor | Workbooks | Windows Event Logs

Event Logs

TimeRange: Last 7 days | Workspace: ArcBox-Workspace

Windows Events - Summary

EventLog	Critical	Error	Warning
System	1	1	1
Application	0	7	0

Events count hourly distribution

Error 1

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.

The screenshot shows the Azure Arc interface for the machine 'Arcbox-Win2k25'. In the left sidebar, under the 'Inventory' section, the 'Change tracking' link is highlighted with a red box and the number '1'. At the top right, there is a 'Settings' button, which is also highlighted with a red box and the number '2'. The main content area displays 'Changes tracking with AMA' and a table showing 'No changes detected in this time window'.

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.

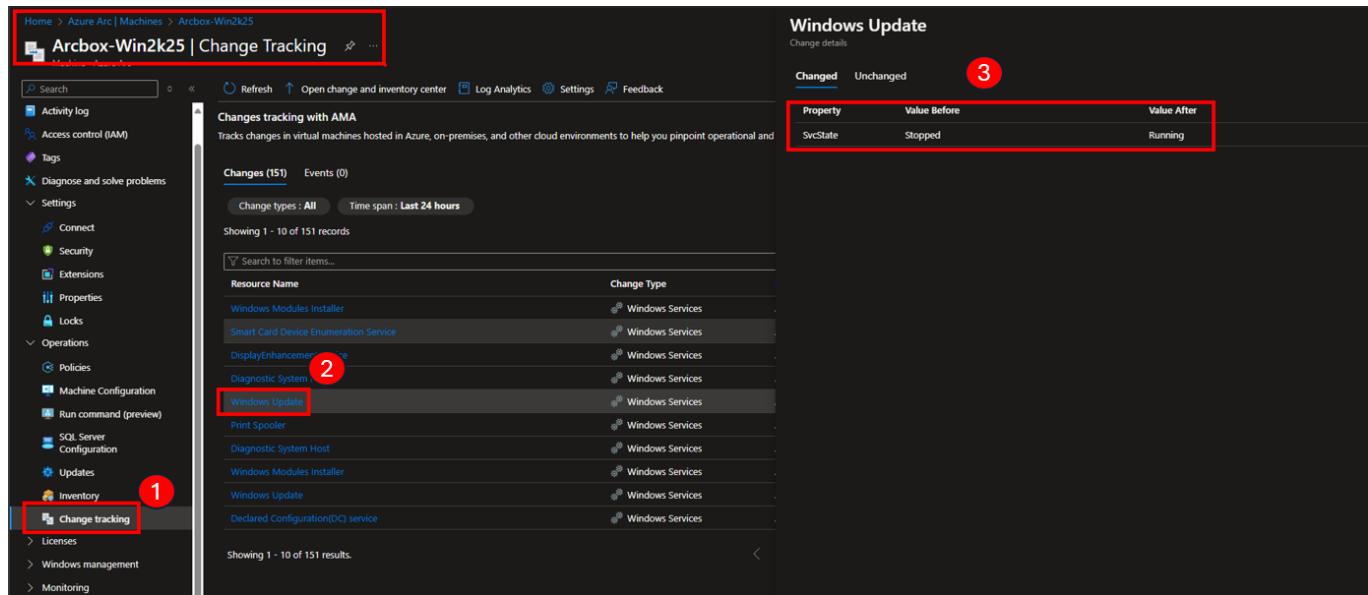
The screenshot shows the 'Data Collection Rule Configuration' page for a specific rule. The 'Windows Services' tab is selected and highlighted with a red box and the number '1'. Below it, a slider for 'Collection Frequency' is set to '10 min', which is also highlighted with a red box and the number '2'. The page also includes tabs for 'Windows Files', 'Linux Files', 'Windows Registry', and 'File Content'.

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.



Property	Value Before	Value After
SvcState	Stopped	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.

```
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.

Data Collection Rule Configuration

Change Tracking

+ Add Delete Refresh Documentation Feedback

Data collection rule : arcbox-ama-ct-dcr

Windows Files 1

Search to filter items...

Group	Status	Path	Type	Recursion

Item Name: CT
Group: Custom
Enter Path: C:\ArcBox\ct.txt
Path Type: File
Recursion: Off

Upload file content

Save 3

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.

Data Collection Rule Configuration

Change Tracking

+ Add Delete Refresh Documentation Feedback

Data collection rule : arcbox-ama-ct-dcr

File Content

File Content Change Tracking allows you to view the file content of a changed file before and after the change. In order to provide this service, the file

Turning on File Content Change Tracking will create a container named "changetrackingblob" in the selected storage account if it does not already exist. A managed identity will be required to enable File content tracking. The selected mode of managed identity should have write permissions in the linked storage account.

View Privacy Statement

Storage Account Name: None

Link

Content Location f...

Select Subscription: MIPDG-loc50410717

Select Storage: arcboxjxw6qsrm5dws

Use System Assigned Managed Identity: True

Upload file content for all settings: True

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

Storage accounts

Default Directory

+ Create Restore ...

Filter for any field...

Name: arcboxhkoqwcepudsdy machineconfigstgwjms

Overview Activity log Tags Diagnose and solve problems Access Control (IAM) Data migration Events Storage browser Storage Mover Partner solutions Data storage Containers

Search containers by prefix

Name	Last modified	Anonymous access level	Lease state
Slogs	10/15/2024, 4:45:21 AM	Private	Available
changetrackingblob	10/11/2024, 3:02:26 PM	Private	Available

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

Home > Storage accounts > arboxmoun6b25byamm | Containers > changetrackingblob

changetrackingblob | Access Control (IAM)

Container

Search | Add | Download role assignments | Edit columns | Refresh | Remove | Feedback

Overview

Diagnose and solve problems

Access Control (IAM) 1

My access
View my level of access to this resource.

Check access

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Settings

Shared access tokens

Access policy

Properties

Metadata

Grant access to this resource
Grant access to resources by assigning a role. [Learn more](#)

Add role assignment 2

View access to this resource
View the role assignments that grant access to this and other resources. [Learn more](#)

View

View deny assignments
View the role assignments that have been denied access to specific actions at this scope. [Learn more](#)

View

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

Home > Storage accounts > arboxmoun6b25byamm | Containers > changetrackingblob | Access Control (IAM) >

Add role assignment

Role **Members*** **Conditions (optional)** **Review + assign**

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Assignment type

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Name	Description	Type	Category	Details
Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to VMs; r...	BuiltinRole	Analytics	View
Managed Application Contributor Role	Allows for creating managed application resources.	BuiltinRole	Management + Governance	View
Monitoring Contributor	Can read all monitoring data and update monitoring settings.	BuiltinRole	Monitor	View
Resource Policy Contributor	Users with rights to create/modify resource policy, create support ticket and read resources/hierarchy.	BuiltinRole	Management + Governance	View
Storage Account Contributor	Lets you manage storage accounts, including accessing storage account keys which provide full access to storage account data.	BuiltinRole	Storage	View
Storage Blob Data Contributor 1	Allows for read, write and delete access to Azure Storage blob containers and data	BuiltinRole	Storage	View
Storage Blob Data Owner	Allows for full access to Azure Storage blob containers and data, including assigning POSIX access control.	BuiltinRole	Storage	View

Showing 1 - 7 of 7 results.

Home > Storage accounts > arboxhkoqwccepubsdy | Access Control (IAM) >

Add role assignment

Role **Members*** **Conditions** **Review + assign**

Selected role Storage Blob Data Contributor

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#) 1

Description Optional

Select managed identities

Some results might be hidden due to your ABAC condition.

Subscription:

Managed identity:

Select: Search by name

ArcBox-Ubuntu-01 /subscriptions/ /resourceGroups/Arcbox...

ArcBox-Win2k22 /subscriptions/ /resourceGroups/Arcbox...

Selected members: ArcBox-Win2k22 /subscriptions/ /resourceGroups... [Remove](#)

Select 2 3

Review + assign **Previous** **Next** **Feedback**

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.

The screenshot shows the Azure Storage Accounts blade. The breadcrumb path at the top is 'Home > Storage accounts > arcboxjxw6qsrm5dws | Containers > changetrackingblob'. The main area shows a table of blobs. One blob, '2025-04-10 16:17:23-ct.txt', is highlighted with a red box. The table columns are Name, Modified, Access tier, Archive status, and Blob. The blob details are: Name '2025-04-10 16:17:23-ct.txt', Modified '4/10/2025, 7:19:19 A...', Access tier 'Hot (Inferred)', Archive status 'Not yet archived', and Blob type 'Block blob'.

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"
```

The screenshot shows the Log Analytics interface with a query result. The query is:

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

The results table has the following data:

TimeGenerated [UTC]	Computer	ConfigChangeType	ChangeCategory	SourceComputerId	Name	FileSystemPath	Size
> 4/10/2025, 2:19:18.000 PM	ArcBox-Win2K25	Files	Modified	0000000-0000-0000-0000-000000000000	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](#)