



# Connecting another VM to the Workspace

In this lab, we're expanding the coverage of our Log Analytics Workspace by connecting another Windows virtual machine (VM) to it. The end goal is to consolidate log and telemetry data from multiple VMs into a single repository for centralized monitoring, analysis, and troubleshooting. This enables us to gain comprehensive insights into the health, performance, and security of our Azure environment, facilitating effective management and optimization of resources.

1. First, go back to your VM, and from the left pane choose to go towards Extension and Application.
2. There are some extensions that get installed when you enable that feature of the data collection rule of sending data onto the Log Analytics workspace.

The screenshot shows the 'Extensions + applications' blade for a virtual machine named 'appvm'. The left sidebar has options like Disks, Extensions + applications (which is selected), Configuration, Advisor recommendations, Properties, and Locks. The main area shows a table with one item:

Name	Type	Version	Status	Automatic upgrade status
AzureMonitorWindowsAgent	Microsoft.Azure.Monitor...	1.1*	Provisioning succeeded	Disabled

3. Now we will create another Windows VM. Below you can see that we have two virtual machines.

The screenshot shows the 'Virtual machines' blade. The top navigation bar includes 'Create', 'Switch to classic', 'Reservations', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', 'Start', 'Restart', 'Stop', and more. The main table lists two virtual machines:

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size
appvm	Virtual machine	Azure Pass - Sponsors...	demo-resource-group	North Europe	Running	Windows	Standard_DS1_v2
newvm	Virtual machine	Azure Pass - Sponsors...	demo-resource-group	North Europe	Creating	Windows	Standard_DS1_v2

4. Once your machine is created then you need to go to the data collection rule which we created earlier.
5. For that go to all resources and check for it and open it.

The screenshot shows the 'Data collection rule' blade for a resource named 'windows-rule'. The top navigation bar includes 'Data collection rule', 'demo-resource-group', 'North Europe', and 'Azure Pass - Sponsorship'. The main table shows the rule configuration:

Source type	Source name	Subscription	Resource group	Location	Status
Log Analytics workspace	demo-log-workspace	Azure Pass - Sponsors...	demo-resource-group	North Europe	Active

6. In the data collection rule we created two data sources, and we want to connect them with our new VM.

**Data sources**

- Data source
- Performance Counters
- Windows Event Logs

Destination(s)
Azure Monitor Metrics (preview), Azure Monitor Logs
Azure Monitor Logs

7. For that go to resources and click on Add. Then choose your new VM and click on save.

**Resources**

**Add**

Name	Type	Location
appvm	Virtual machine	North Europe
newvm	Virtual machine	North Europe

**Browse**    Recent

Resource group	Resource types	Locations
All resource groups	All resource types	All locations

Scope                      Resource type              Location

<input type="checkbox"/> Azure Pass - Sponsorship	Subscription	-
<input type="checkbox"/> demo-resource-group	Resource group	-
<input type="checkbox"/> appvm	Virtual machine	North Europe
<input checked="" type="checkbox"/> newvm	Virtual machine	North Europe

8. And below you can see that we have our new VM in place and by that we have connected our new VM with the logs that we required.

9. Now we have this new VM as a resources for this data collection rule.

**Resources**

Name	Type	Location	Data collection endpoint	Resource group	Subscription
appvm	Virtual machine	North Europe	<a href="#">+ Create endpoint</a>	demo-resource-group	Azure Pass - Sponsorship
newvm	Virtual machine	North Europe	<a href="#">+ Create endpoint</a>	demo-resource-group	Azure Pass - Sponsorship

10. Now go to your new VM and from the left go to extension and applications. Here you will see that an extension is getting created but it is currently in transitioning state.

The screenshot shows the 'Extensions + applications' blade for a virtual machine named 'newvm'. The 'Extensions' tab is selected. A single extension, 'AzureMonitorWindows...', is listed. The blade includes a search bar, a settings sidebar with options like 'Disks', 'Configuration', and 'Advisor recommendations', and a status summary at the bottom.

11. So, you have to wait for 10-15 minutes until your data gets to the logs in log analytics workspace.
12. Now after some time if you go to log analytics workspace and then to the logs here you will see the same logs.
13. But if you run them then you will notice that you have the logs for both app VM and new VM.

The screenshot shows the 'vm-workspace120' Log Analytics workspace. A query titled 'New Query 1' is running, showing results for the 'Event' table. The results table has columns: TimeGenerated [UTC], Source, EventLog, Computer, and EventLevel. The data shows multiple entries for 'Service Control Manager' events on both 'newvm' and 'appvm' computers, all with an event level of 4.

TimeGenerated [UTC]	Source	EventLog	Computer	EventLevel
> 5/11/2024, 3:57:40.159 PM	Service Control Manager	System	newvm	4
> 5/11/2024, 3:57:34.124 PM	Service Control Manager	System	newvm	4
> 5/11/2024, 3:57:30.109 PM	Service Control Manager	System	newvm	4
> 5/11/2024, 3:57:29.395 PM	Service Control Manager	System	newvm	4
> 5/11/2024, 3:57:27.730 PM	Service Control Manager	System	newvm	4
> 5/11/2024, 3:57:27.683 PM	Service Control Manager	System	newvm	4
> 5/11/2024, 3:45:03.916 PM	Service Control Manager	System	appvm	4
> 5/11/2024, 3:43:02.488 PM	Service Control Manager	System	appvm	4
> 5/11/2024, 3:38:04.794 PM	Service Control Manager	System	appvm	4
> 5/11/2024, 3:34:05.756 PM	Service Control Manager	System	appvm	4

14. Now check logs for the other tables too.

vm-workspace120 | Logs Log Analytics workspace

New Query 1\*

vm-workspace120 Select scope

Run Time range : Last 24 hours

Save Share New alert rule Export Pin to ...

Tables Queries Functions ...

1 Heartbeat

Results Chart

TimeGenerated [UTC]	SourceComputerId	ComputerIP	Computer	Category
5/11/2024, 4:00:51.849 PM	f1258c81-5b9a-43f7-af44-b37b...	52.164.226.120	newvm	Azure M
5/11/2024, 4:00:48.259 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure M
5/11/2024, 3:59:51.849 PM	f1258c81-5b9a-43f7-af44-b37b...	52.164.226.120	newvm	Azure M
5/11/2024, 3:59:48.241 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure M
5/11/2024, 3:58:51.842 PM	f1258c81-5b9a-43f7-af44-b37b...	52.164.226.120	newvm	Azure M
5/11/2024, 3:58:48.233 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure M
5/11/2024, 3:57:48.205 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure M
5/11/2024, 3:56:48.197 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure M
5/11/2024, 3:55:48.179 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure M
5/11/2024, 3:54:48.171 PM	c4f0e9e0-ada0-49a4-84c9-aa3...	40.69.34.28	appvm	Azure M

vm-workspace120 | Logs Log Analytics workspace

New Query 1\*

vm-workspace120 Select scope

Run Time range : Last 24 hours

Save Share New alert rule Export Pin to ...

Tables Queries Functions ...

1 Perf

Results Chart

TimeGenerated [UTC]	Computer	ObjectName	CounterName	InstanceName
5/11/2024, 4:00:48.639 PM	appvm	Network Interface	Bytes Sent/sec	Microso
5/11/2024, 4:00:48.639 PM	appvm	Network Interface	Bytes Received/sec	Microso
5/11/2024, 4:00:48.639 PM	appvm	Network Interface	Packets/sec	Microso
5/11/2024, 4:00:48.639 PM	appvm	Network Interface	Packets Outbound Errors	Microso
5/11/2024, 4:00:48.639 PM	appvm	Network Interface	Packets Received Errors	Microso
5/11/2024, 3:59:52.652 PM	newvm	LogicalDisk	Disk Transfers/sec	_Total
5/11/2024, 3:59:52.652 PM	newvm	Process	Thread Count	_Total
5/11/2024, 3:59:52.652 PM	newvm	LogicalDisk	Disk Reads/sec	_Total
5/11/2024, 3:59:52.652 PM	newvm	Processor Information	% Processor Time	_Total