

😊 Sending Custom Logs

The end goal is to have a robust system in place that automatically collects and uploads Nginx log data from your VM to Azure Log Analytics, where you can monitor, analyze, and gain insights from the logs in a centralized location. This setup helps in proactive monitoring, troubleshooting, and ensuring the health and performance of your applications running on the VM.

1. In this lab, we are going to send our custom logs to the Log Analytics workspace.
2. For that, we are going to create a VM based on the Ubuntu server. Once the VM is deployed then we need to install Nginx on that server.

Project details

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

Subscription *	<input type="text" value="Azure Pass - Sponsorship"/>
Resource group *	<input type="text" value="demo-resource-group"/> Create new

Instance details

Virtual machine name *	<input type="text" value="linuxVM"/> ✓
Region *	<input type="text" value="(Europe) North Europe"/>
Availability options	<input type="text" value="No infrastructure redundancy required"/>
Security type	<input type="text" value="Trusted launch virtual machines"/> Configure security features
Image *	<input type="text" value="Ubuntu Server 22.04 LTS - x64 Gen2"/> See all images Configure VM generation
VM architecture	<input type="radio"/> Arm64 <input checked="" type="radio"/> x64

Size * ⓘ

Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (₹3,996.17/month)
 ▼

[See all sizes](#)

Enable Hibernation ⓘ

i Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. [Learn more ↗](#)

Administrator account

Authentication type ⓘ

SSH public key
 Password

Username * ⓘ

Password *

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

None
 Allow selected ports

Select inbound ports *

HTTP (80), SSH (22)
 ▼

3. Once your VM is deployed login to your VM using the Putty tool. Now you just need to run two commands. The first command is to update your VM and the second is for installing Nginx.

sudo apt-get update
sudo apt-get install nginx

```
linuxuser@linuxVM: ~
login as: linuxuser
linuxuser@40.113.93.121's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-1021-azure x86_64)

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

System information as of Wed May 29 09:16:12 UTC 2024

System load: 0.37          Processes:           122
Usage of /:   5.1% of 28.89GB  Users logged in:     0
Memory usage: 8%            IPv4 address for eth0: 10.0.0.6
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

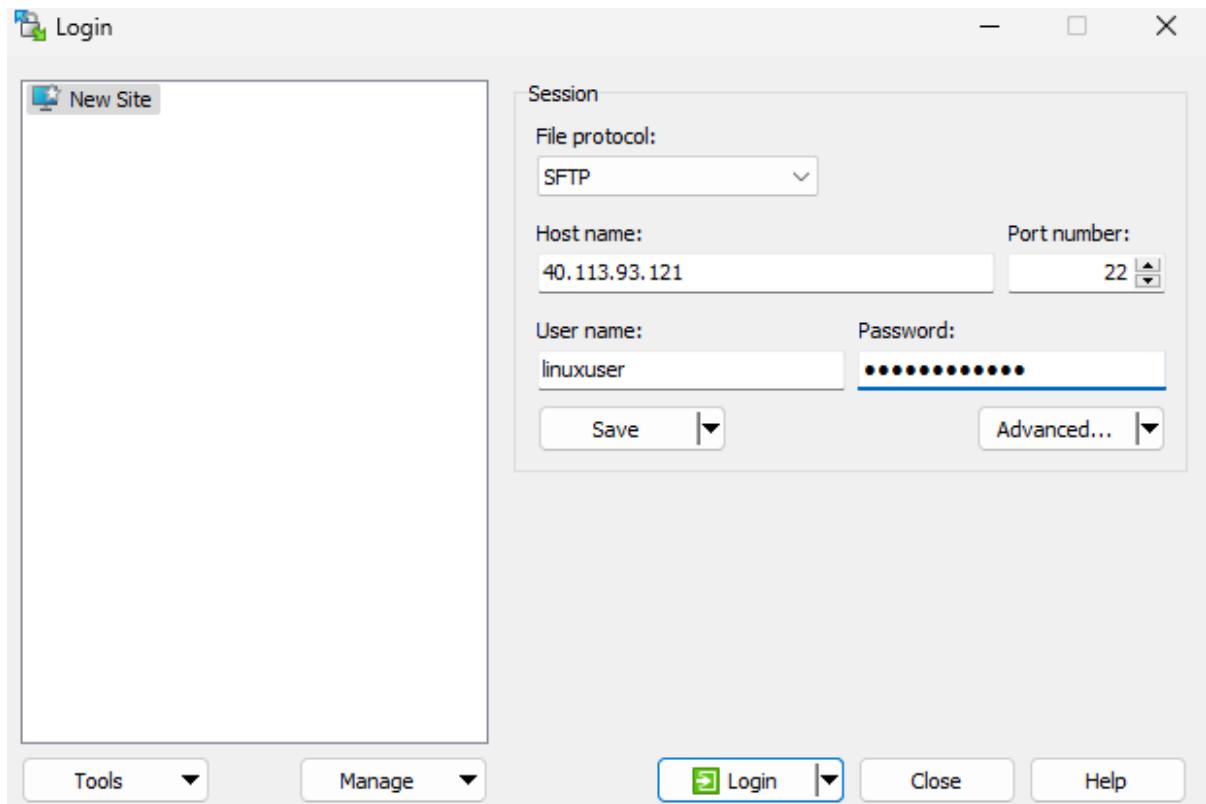
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

linuxuser@linuxVM:~$
```

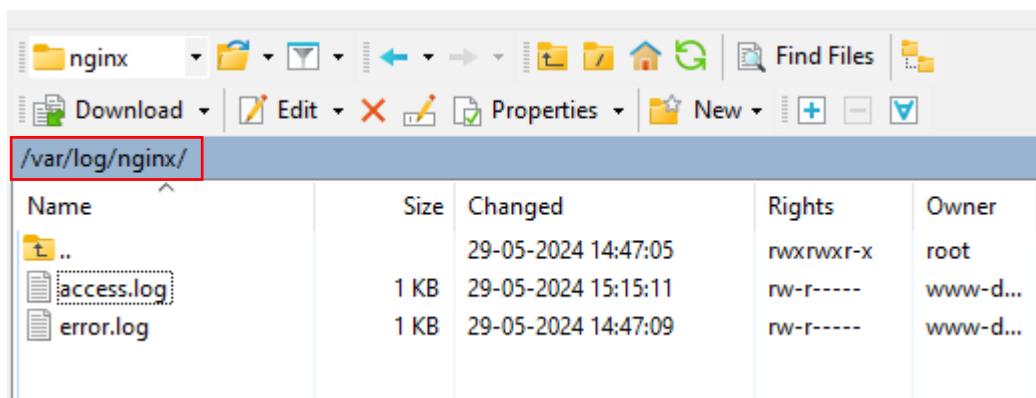
- Once nginx is installed then verify it by pasting the public IP address of your VM in a new tab. Below you can see that nginx is running as expected.



5. Nginx generates its own logs which get saved in our VM server and we are going to download those logs onto our laptop with the help of the Win SCP tool.
6. Now open the Win SCP tool on your laptop and paste the Public IP address of the VM then give the username and password of your VM then click on login.



7. Now you need to go to this location in your VM then you will see the access.log file. You need to drag this file to the left side where you can see your laptop storage and paste it there.



8. After that come to Azure portal and open Azure monitor then from the left pane go to data collection endpoints and create an endpoint.

The screenshot shows the Azure Monitor Data Collection Endpoints page. The left sidebar includes links for Home, Monitor, Azure Stack HCI, Service Bus (preview), Insights Hub, Managed Services (Prometheus, Azure Managed Grafana, SCOM managed instance), Settings (Diagnostic settings, Data Collection Rules, Data Collection Endpoints - highlighted in blue), and Autoscale. The main content area has a search bar and filter buttons for Subscription (all), Resource group (all), and Location (all). It displays a message: "Showing 0 to 0 of 0 records." Below this is a sorting section with columns for Name, Subscription, Resource group, and Location. A central message says "No data collection endpoints to display" with a "Create data collection endpoint" button.

9. Now you just need to give it name and choose your resource group, then choose your region. Then go to review page and create your endpoint.

[Basics](#) [Tags](#) [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](#)

Endpoint details

Endpoint Name *	<input type="text" value="nginx-endpoint"/>
Subscription *	<input type="text" value="Azure Pass - Sponsorship"/>
Resource Group *	<input type="text" value="demo-resource-group"/> Create new
Region *	<input type="text" value="North Europe"/>

10. After that you need to come to log analytics workspace. Then to tables and here you will see the inbuilt tables then click on create and choose **MMA based**.

11. First you need to choose your file which you downloaded from Win SCP.

12. Then you can see that it is understanding the logs.

13. Now in the collection paths you need to choose Linux as your path and in the path write the exact same path as shown below.



Define one or more paths on the agent where it can locate the custom log. [Learn more](#)

Collection paths

Type	Path	
Linux	/var/log/nginx/access.log	
Select type		

14. Then give it a name and just create it.



Add a name and description to the custom log.

This name will be used for the log type, and will always end with _CL to distinguish it as a custom log. [Learn more](#)

Details

Custom log name *	<input type="text" value="Access"/>
Description	<input type="text" value="Description"/>

15. Now the next step is to create the data collection rule in Azure Monitor. Below you can see that we already have two rules in place. Now click on create.

Name	Subscription	Resource group	Location	Data sources	Destinations	Kind
MSVMI-vm-insight...	Azure Pass - Sponsors...	demo-resource-group	North Europe	VM Insights, Performance Count...	Azure Monitor Logs	All
windows-rule	Azure Pass - Sponsors...	demo-resource-group	North Europe	Performance Counters, Window...	Azure Monitor Logs	Windows

16. This time give it name choose your resource group and the region. After that, the platform type is Linux and then choose your endpoint which we created earlier.

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 *	<input type="text" value="Nginx-Rule"/> ✓
Subscription *	<input type="text" value="Azure Pass - Sponsorship"/>
Resource Group *	<input type="text" value="demo-resource-group"/> ✓ Create new
Region *	<input type="text" value="North Europe"/>
Platform Type *	<input type="radio"/> Windows <input checked="" type="radio"/> Linux <input type="radio"/> All
Data Collection Endpoint	<input type="text" value="nginx-endpoint"/>

17. Then you need to click on add resources and choose your Linux VM. After that you need to enable the data collection endpoint, then choose your endpoint as shown below.

Home > Monitor | Data Collection Rules >

Create Data Collection Rule ...

Data collection rule management

Basics Resources Collect and deliver Tags Review + create

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

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

+ Add resources + Create endpoint

Enable Data Collection Endpoints

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

Name	Type	Location
No resources found.		

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

Basics Resources Collect and deliver Tags Review + create

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, managed Prometheus will automatically be enabled. For Windows 10 and 11 devices, [download the client installer](#) and follow the [guidance](#)

This will also enable System Assigned Managed Identity on these resources, in addition to existing User Assigned Identities (if any).

+ Add resources + Create endpoint

Enable Data Collection Endpoints

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

Name	Type	Location	Data collection endpoint	Resource group	Subscription
linuxVM	Virtual machine	North Europe	nginx-endpoint	demo-resource-group	Azure Pass - Sponsorship

Showing 1 - 1 of 1 results.

18. Then in collect and deliver, in the data source you need to give the file location and then the table name as shown below. Now go to the destination tab and choose your destination for your workspace.

The screenshot shows the 'Create Data Collection Rule' page. The 'Data source' tab is selected, displaying configuration for 'Custom Text Logs'. The 'File pattern' is set to '/var/log/nginx/access.log', 'Table name' to 'Access_CL', 'Record delimiter' to 'End-of-Line', and 'Transform' to 'source'. The 'Destination' tab is also visible, showing 'Azure Monitor Logs' selected as the destination type, 'Subscription' as Azure Pass - Sponsorship, and 'Account or namespace' as vm-workspace120 (demo-resource...).

19. Then just go to the review page and create it. Now you have to wait for 20 minutes to have the data in place. Also, you can go and refresh the nginx page for some time.

20. After some time go to Log Analytics Workspace and go to Logs then expand tables for custom logs there you will see Access_CL.

The screenshot shows the 'vm-workspace120 | Logs' page in Log Analytics. The left sidebar includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', and 'Logs'. Under 'Logs', there are sections for 'Settings', 'Tables', 'Agents', 'Usage and estimated costs', 'Data export', 'Network isolation', 'Linked storage accounts', 'Properties', and 'Locks'. The main area shows a query editor with a single event being run. Below the editor is a 'Query history' pane containing three previous queries, each with a 'Run' button.

21. Then in the query write the table and click on Run and you will see the data accordingly.

New Query 1* + Try the new Log Analytics Feedback Queries ...

vm-workspace120 Select scope Run Time range: Last 24 hours Save Share New alert rule Export Pin to ...

1 Access_CL

Results Chart Columns

TimeGenerated [UTC] ↑	RawData	Type	_ResourceId
> 29/5/2024, 10:58:04.000 am	167.71.197.10 - - [29/May/2024:10:58:04 +0000] "\x16\x03\x01\x07\x01\x00\x01\x03\x00" "GET /cdn-cgi/trace HTTP/1.1" 404 134 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:56:52.000 am	167.71.197.10 - - [29/May/2024:10:56:52 +0000] "GET /cdn-cgi/trace HTTP/1.1" 404 134 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:55:17.000 am	192.140.153.5 - - [29/May/2024:10:55:17 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:49:41.000 am	192.140.153.5 - - [29/May/2024:10:49:41 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:49:41.000 am	192.140.153.5 - - [29/May/2024:10:49:41 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:49:41.000 am	192.140.153.5 - - [29/May/2024:10:49:41 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:49:40.000 am	192.140.153.5 - - [29/May/2024:10:49:40 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:49:40.000 am	192.140.153.5 - - [29/May/2024:10:49:40 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:49:40.000 am	192.140.153.5 - - [29/May/2024:10:49:40 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:49:39.000 am	192.140.153.5 - - [29/May/2024:10:49:39 +0000] "GET / HTTP/1.1" 200 396 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId
> 29/5/2024, 10:49:39.000 am	192.140.153.5 - - [29/May/2024:10:49:39 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.195 Safari/537.36" "-"	Access_CL	/subscriptions/6e13e5d6-4287-42a8-b80f-91d6b14e3aec/resourceGroups/rg-vm-workspace120/providers/microsoft.insights/components/Access_CL/_ResourceId

1s 546ms | Display time (UTC+00:00) | Query details | 1 - 11 of 38

22. Once you are done then just delete all of the resources that you have.