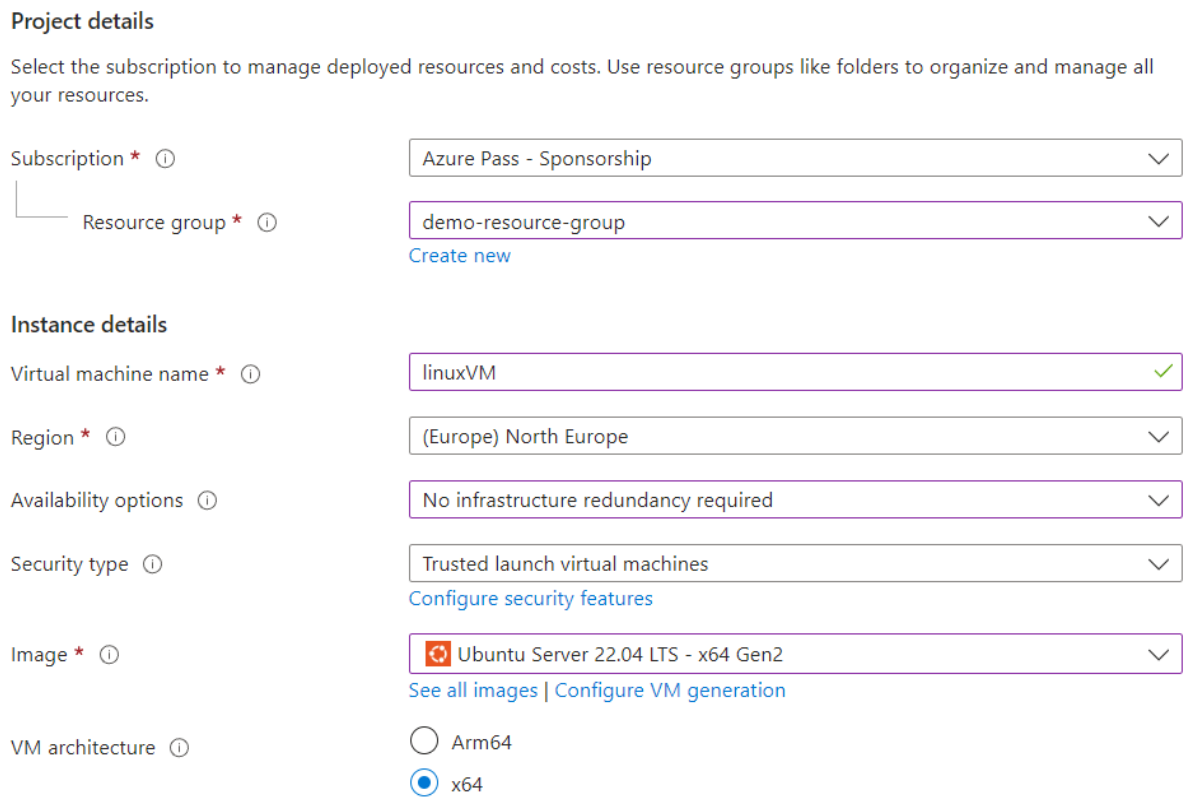
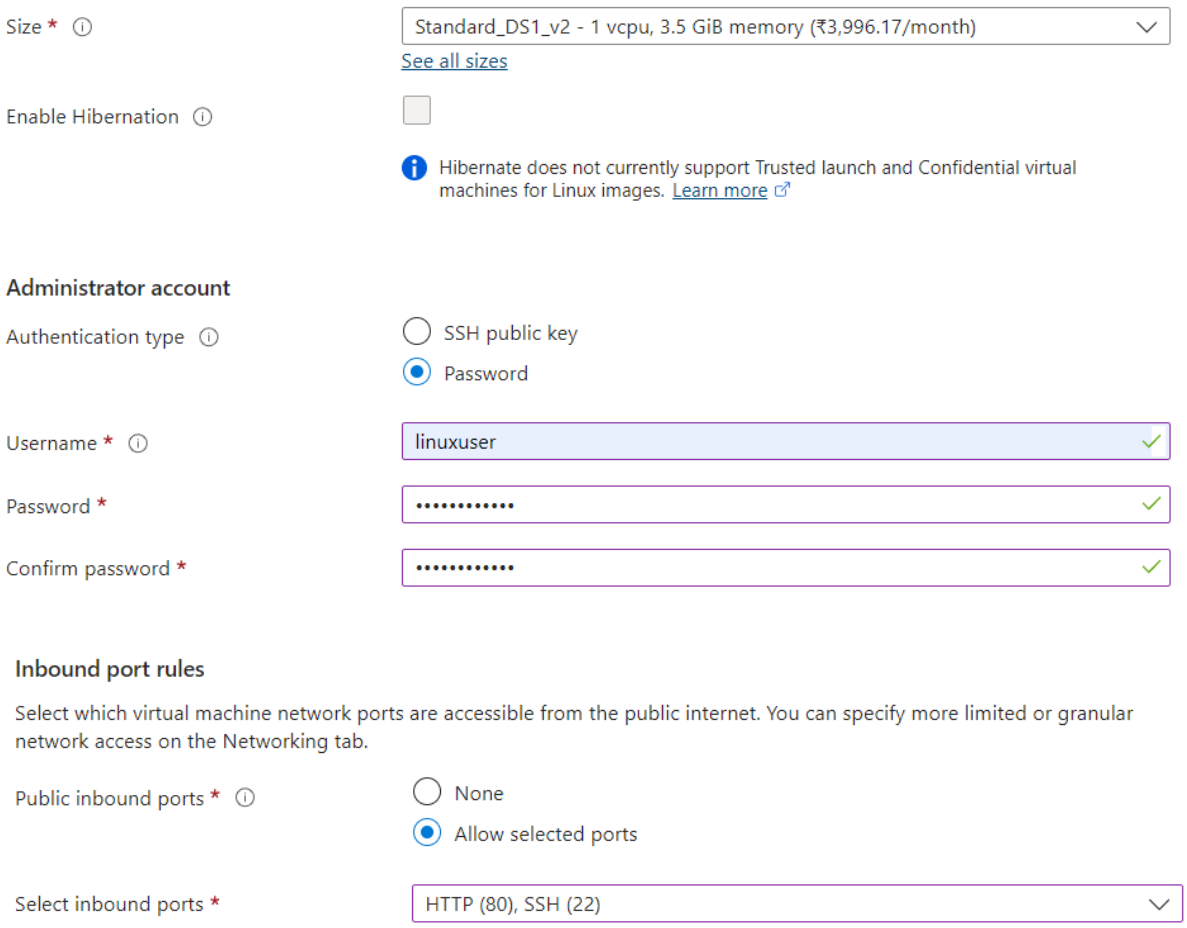
😊 Sending Custom Logs

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.



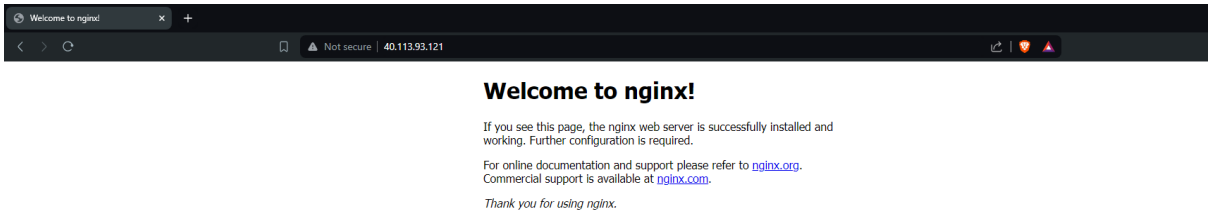


3. Once your VM is deployed login to your VM using the Putty tool. Now you just need to run two commands. The first command is to update your VM and the second is for installing Nginx.

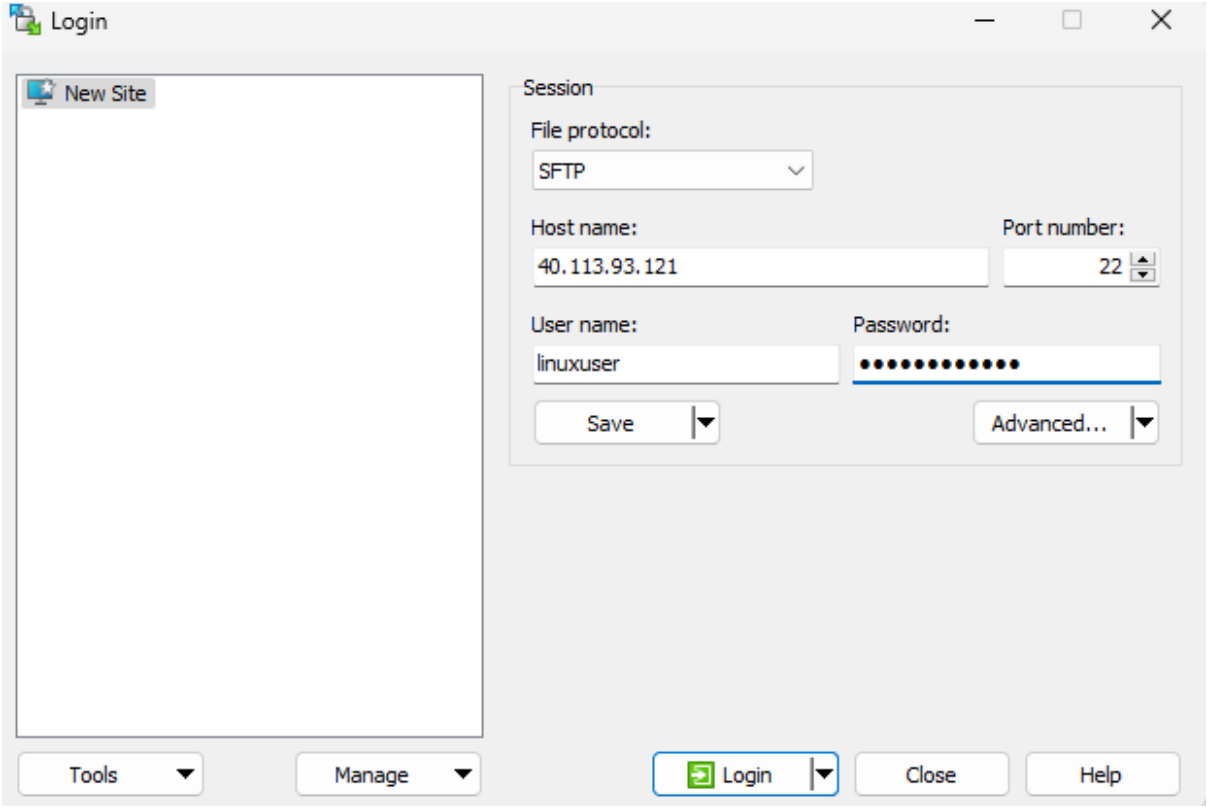
   sudo apt-get update
   sudo apt-get install nginx

```
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:~$
```

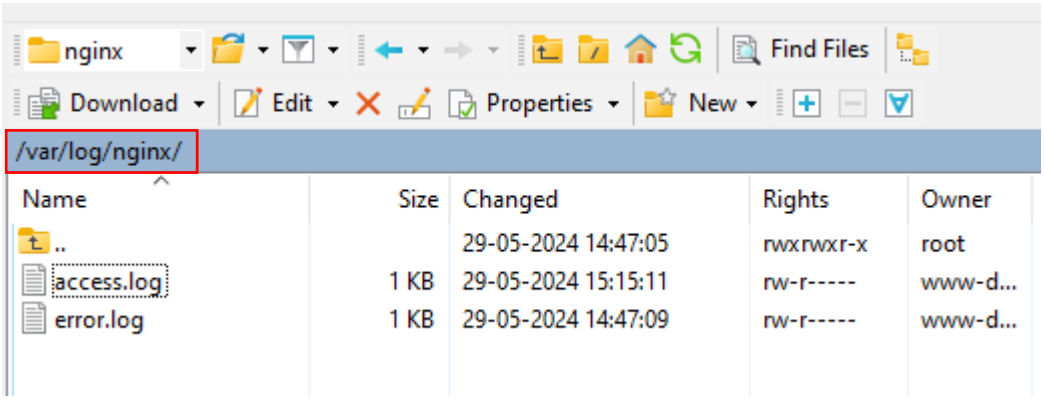
4. Once nginx is installed then verify it by pasting the public IP address of your VM in a new tab. Below you can see that nginx is running as expected.



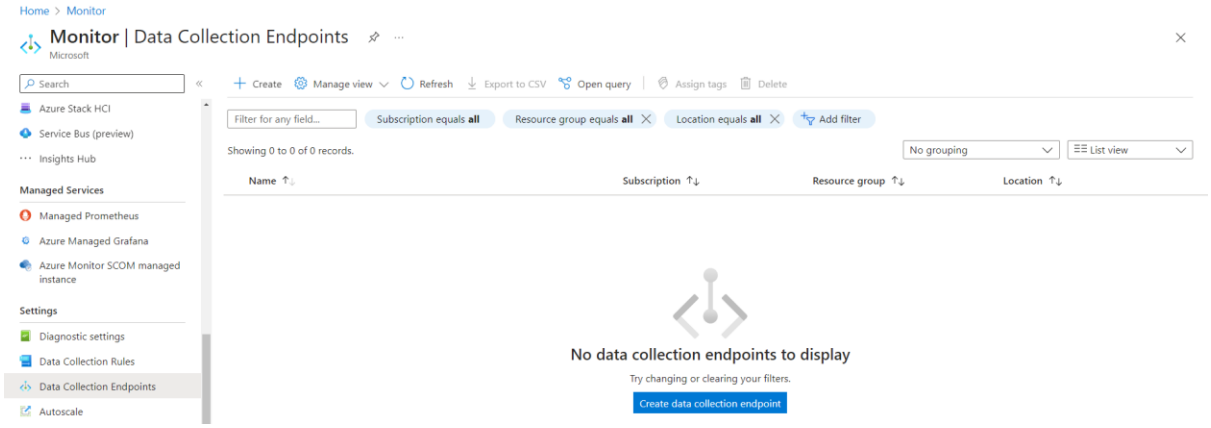
5. Nginx generates its own logs which get saved in our VM server and we are going to download those logs onto our laptop with the help of the Win SCP tool.
6. Now open the Win SCP tool on your laptop and paste the Public IP address of the VM then give the username and password of your VM then click on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



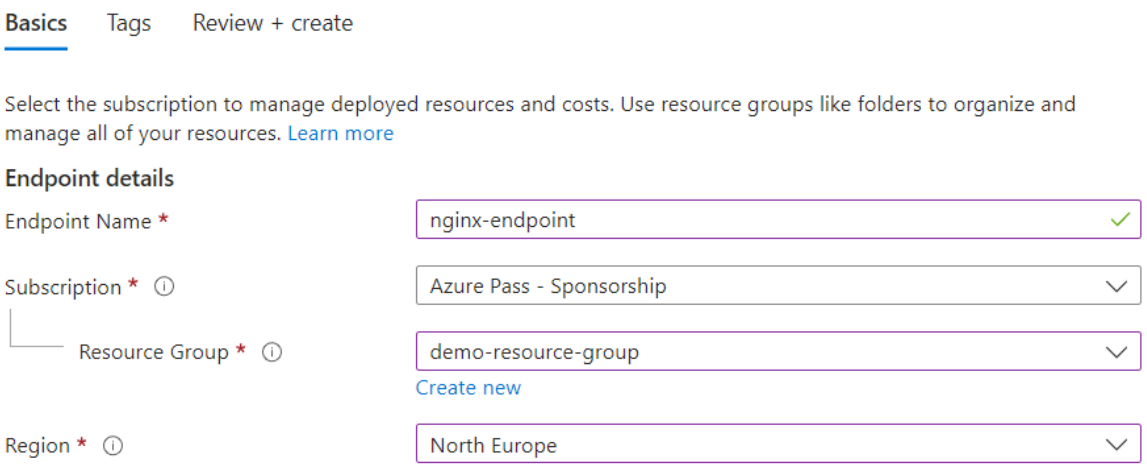
7. Now you need to go to this location in your VM then you will see the access.log file. You need to drag this file to the left side where you can see your laptop storage and paste it there.



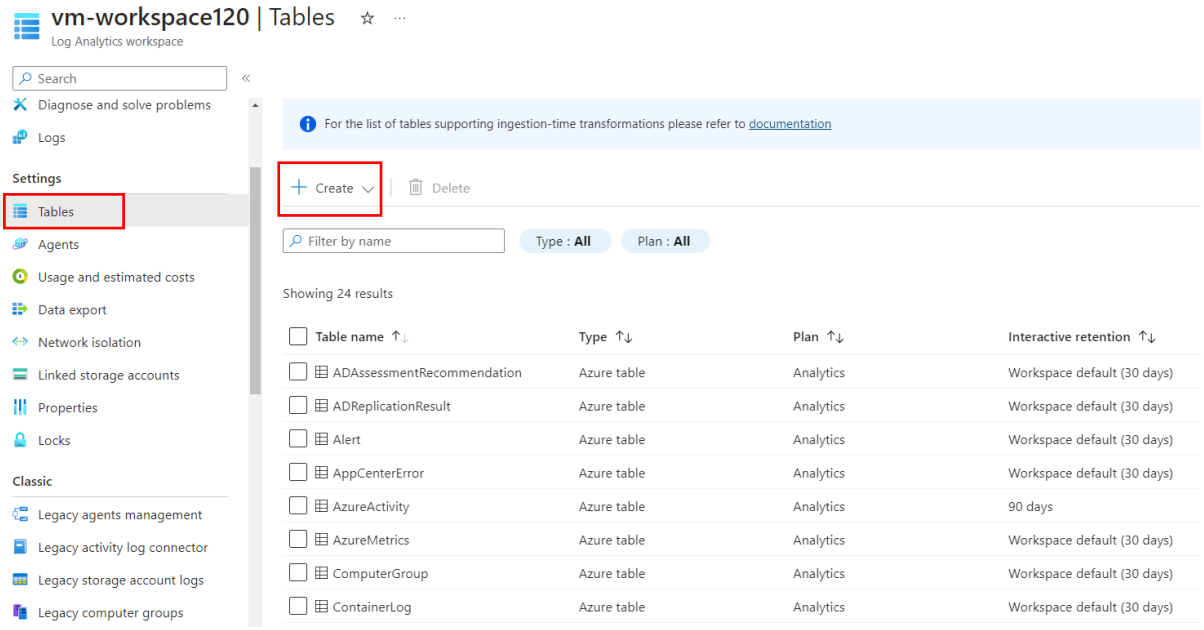
8. After that come to Azure portal and open Azure monitor then from the left pane go to data collection endpoints and create an endpoint.



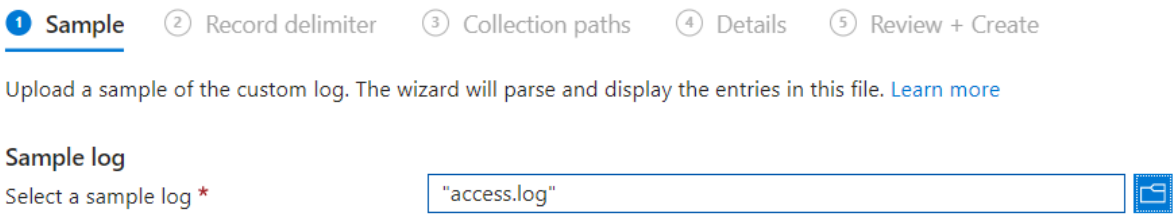
9. Now you just need to give it name and choose your resource group, then choose your region. Then go to review page and create your endpoint.



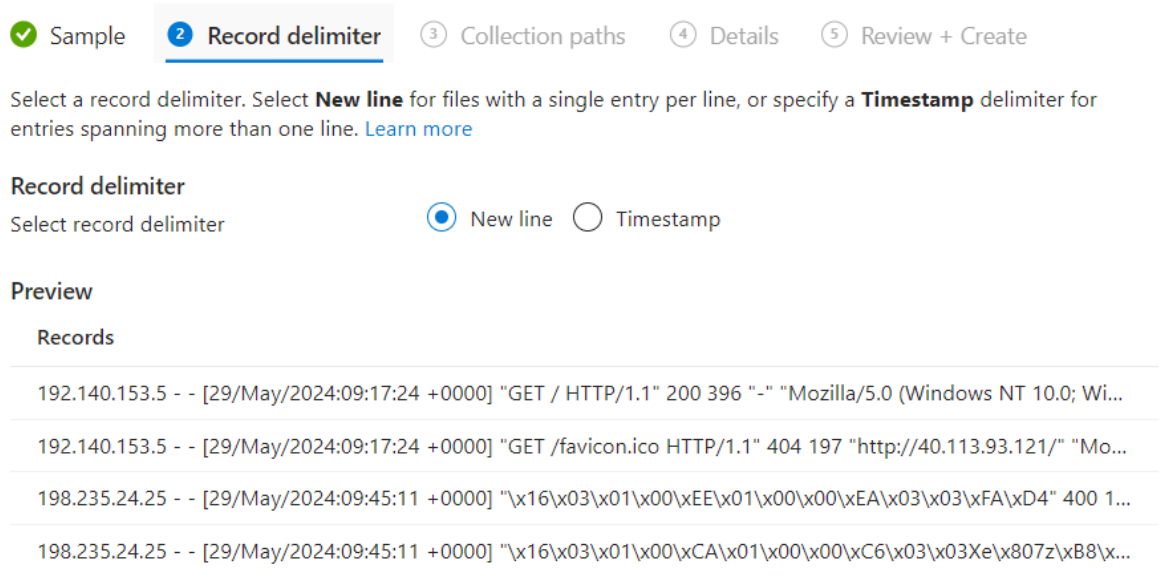
10. After that you need to come to log analytics workspace. Then to tables and here you will see the inbuilt tables then click on create and choose **MMA based**.



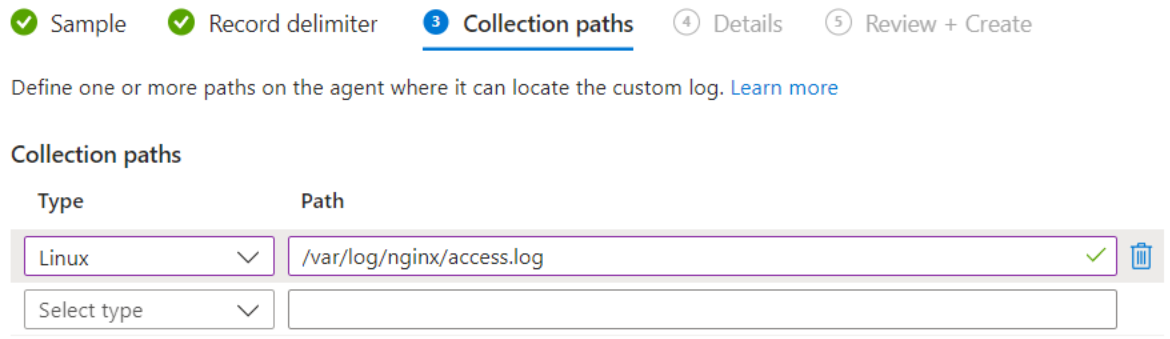
11. First you need to choose your file which you downloaded from Win SCP.



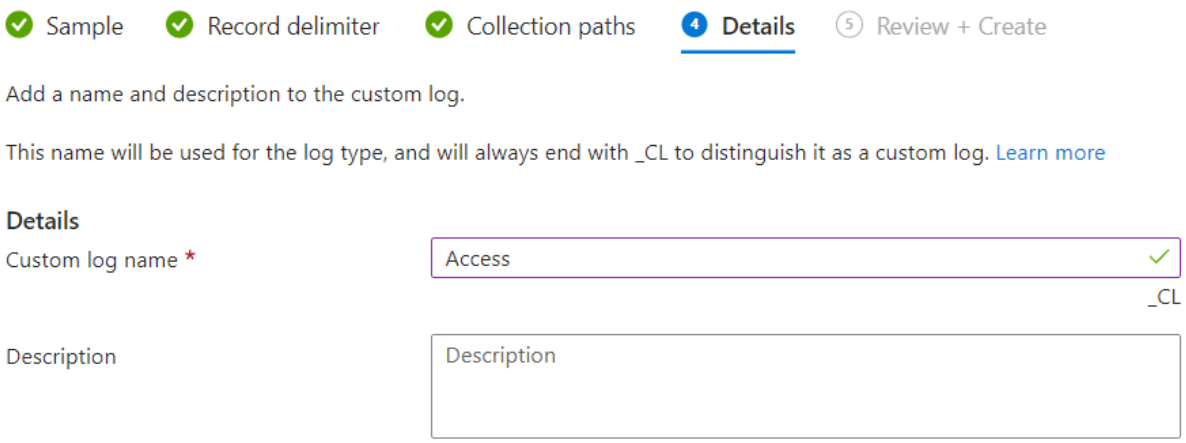
12. Then you can see that it is understanding the logs.



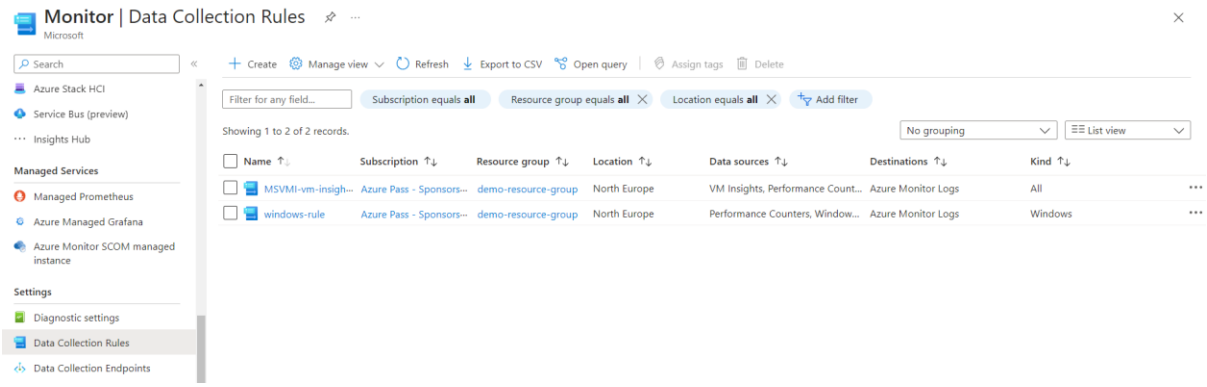
13. Now in the collection paths you need to choose Linux as your path and in the path write the exact same path as shown below.



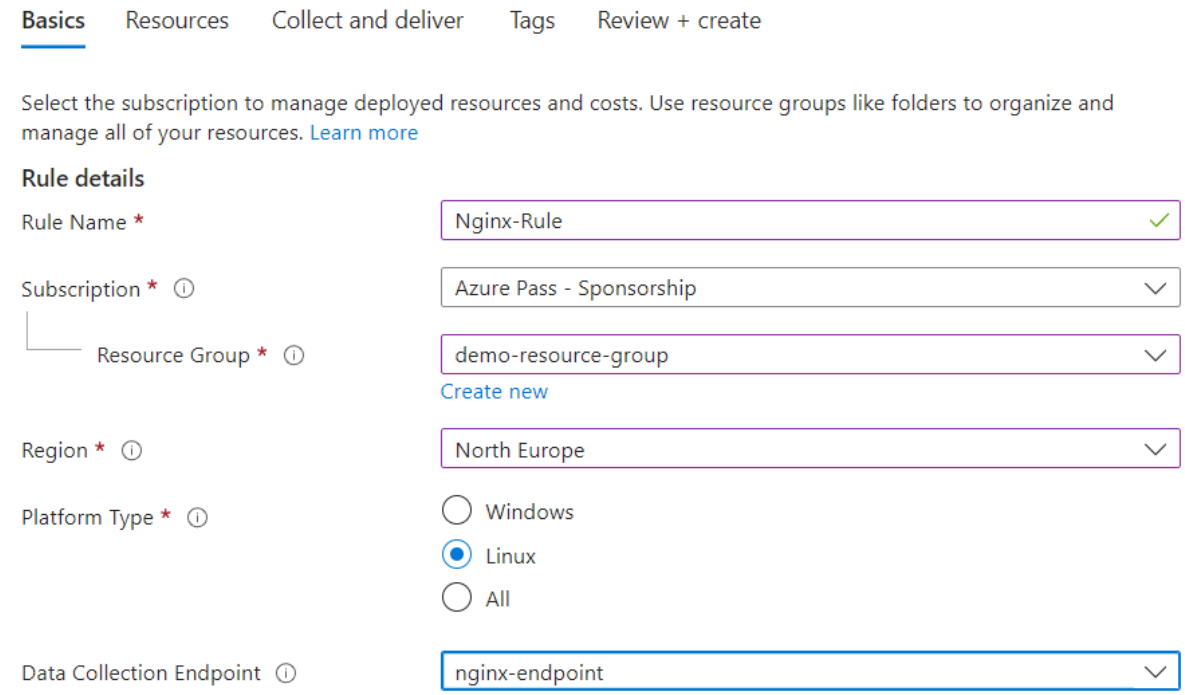
14. Then give it a name and just create it.



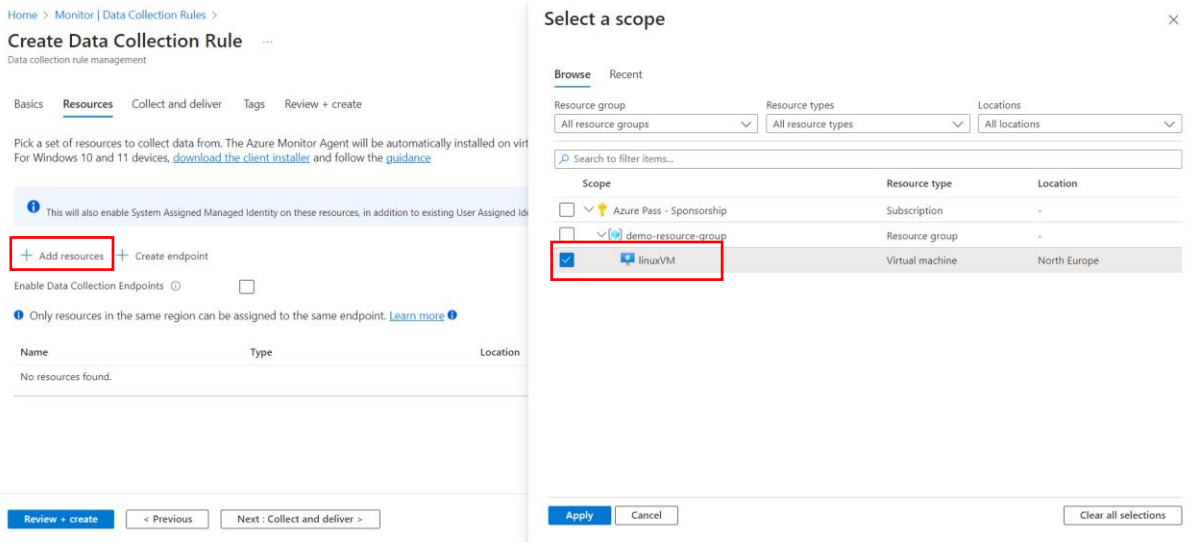
15. Now the next step is to create the data collection rule in Azure Monitor. Below you can see that we already have two rules in place. Now click on create.

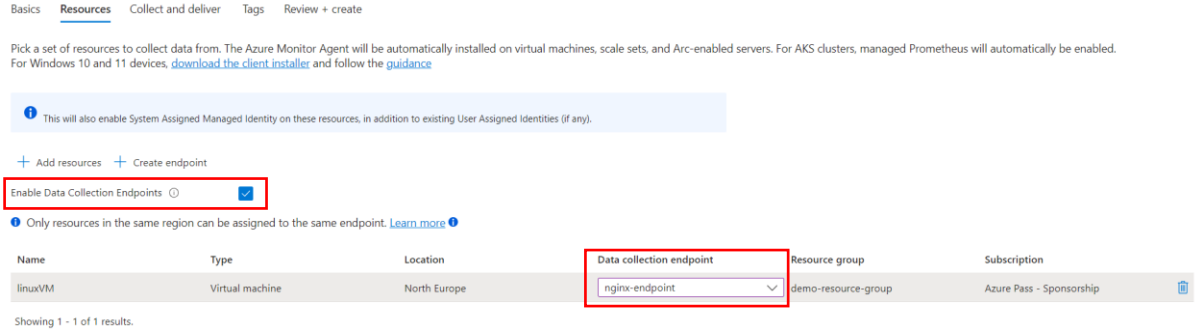


16. This time give it name choose your resource group and the region. After that, the platform type is Linux and then choose your endpoint which we created earlier.

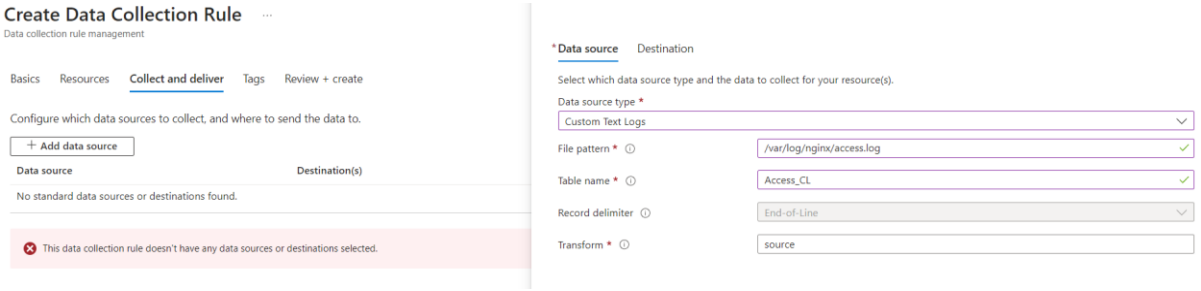


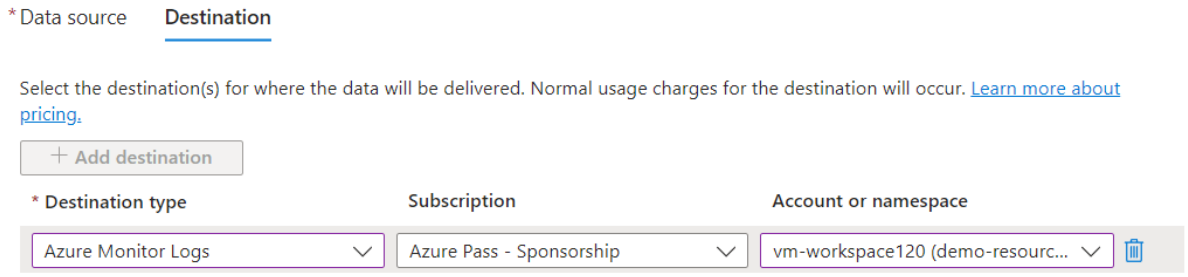
17. Then you need to click on add resources and choose your Linux VM. After that you need to enable the data collection endpoint, then choose your endpoint as shown below.



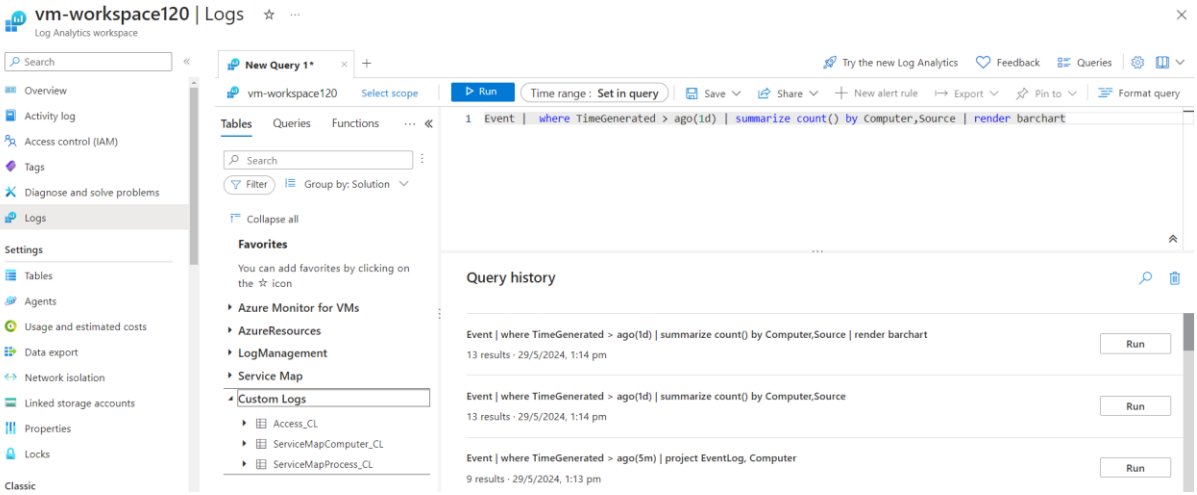


18. Then in collect and deliver, in the data source you need to give the file location and then the table name as shown below. Now go to the destination tab and choose your destination for your workspace.

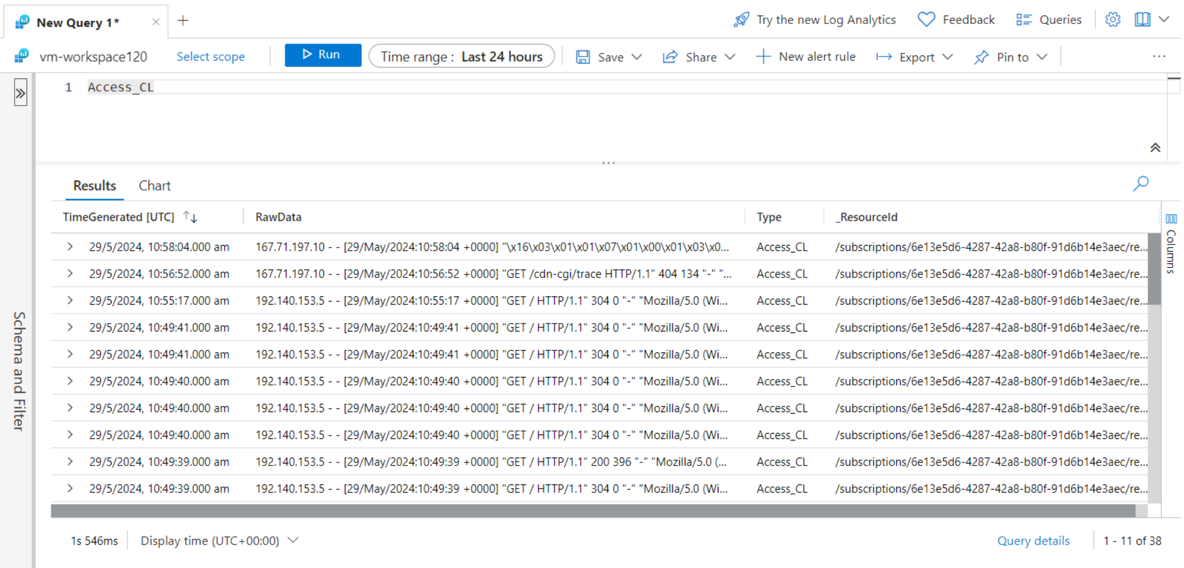




19. Then just go to the review page and create it. Now you have to wait for 20 minutes to have the data in place. Also, you can go and refresh the nginx page for some time.
20. After some time go to Log Analytics Workspace and go to Logs then expand tables for custom logs there you will see Access_CL.



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



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