SCENARIO 1: Create Linux VM and Store Daily Logs

🔷 Objective:

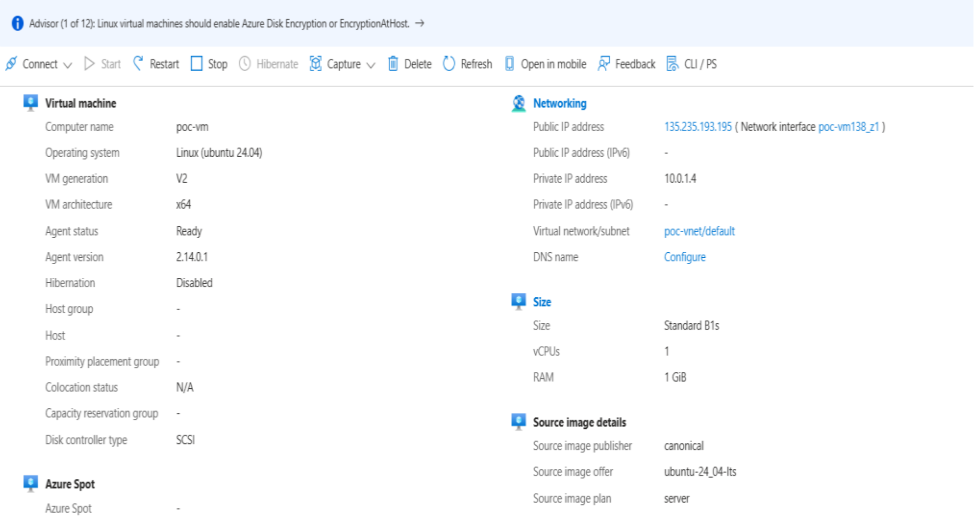
Log daily user activity and store it as a log file.

💡 Architecture:

User Activity → Linux VM → Cron Job → /var/logs/auth.log-<date>.log

🛠️ Implementation:

- Provision a **Linux VM : poc-vm** from Azure.



Advisor (1 of 12): Linux virtual machines should enable Azure Disk Encryption or EncryptionAtHost. →

Virtual machine

Computer name	poc-vm
Operating system	Linux (ubuntu 24.04)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.14.0.1
Hibernation	Disabled
Host group	-
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-
Disk controller type	SCSI

Azure Spot

Azure Spot	-

Networking

Public IP address	135.235.193.195 (Network interface poc-vm138_z1)
Public IP address (IPv6)	-
Private IP address	10.0.1.4
Private IP address (IPv6)	-
Virtual network/subnet	poc-vnet/default
DNS name	Configure

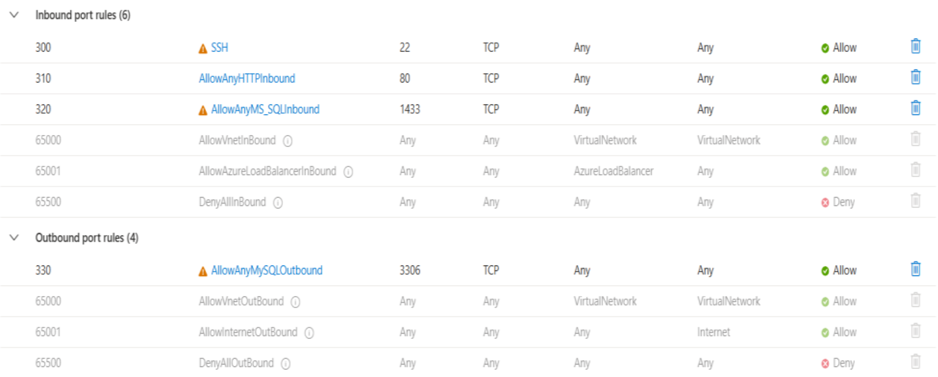
Size

Size	Standard B1s
vCPUs	1
RAM	1 GiB

Source image details

Source image publisher	canonical
Source image offer	ubuntu-24_04-lts
Source image plan	server

  - ### Allow Inbound and Outbound Rules for VM



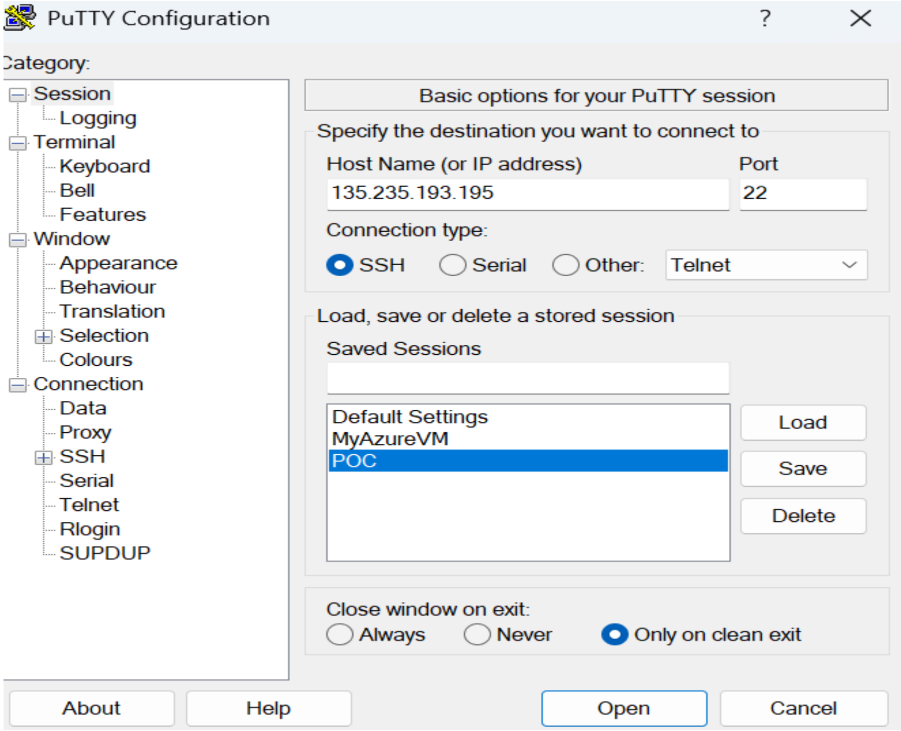
Inbound port rules (6)

300	⚠ SSH	22	TCP	Any	Any	✓ Allow
310	AllowAnyHTTPInbound	80	TCP	Any	Any	✓ Allow
320	⚠ AllowAnyMS_SQLInbound	1433	TCP	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Outbound port rules (4)

330	⚠ AllowAnyMySQLOutbound	3306	TCP	Any	Any	✓ Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

  - ### Access the VM using Putty

- 

  Specify the destination you want to connect to

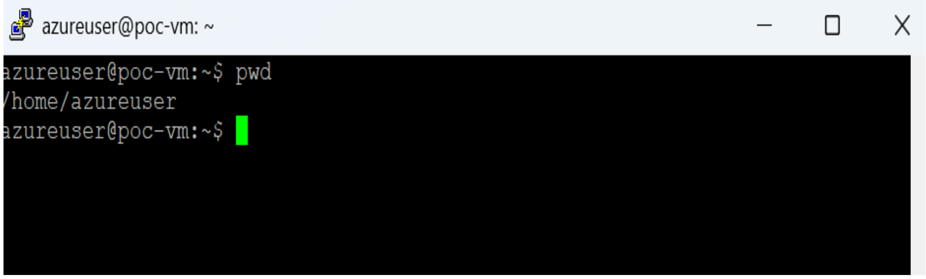
  Host Name (or IP address): 135.235.193.195

  Port: 22

  Connection type: ● SSH ○ Serial ○ Other: Telnet

  Saved Sessions: Default Settings, MyAzureVM, POC

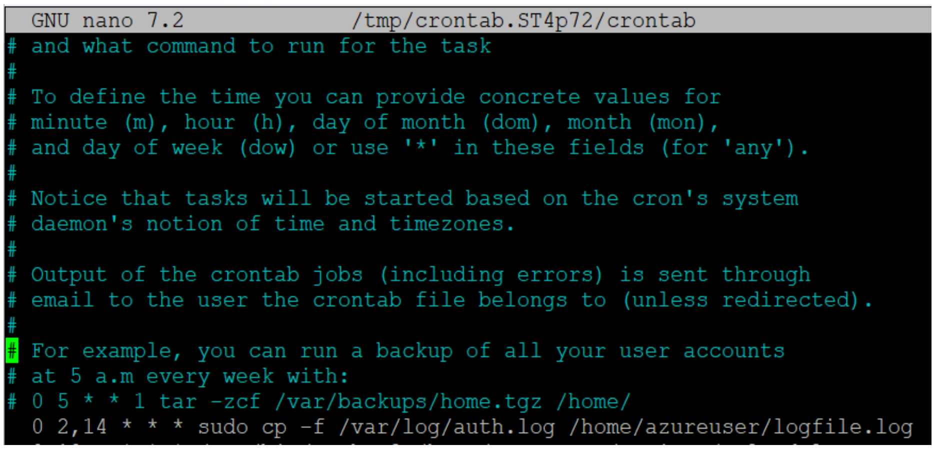
  Close window on exit: ○ Always ○ Never ● Only on clean exit

- 

  ```
  azureuser@poc-vm:~$ pwd
  /home/azureuser
  azureuser@poc-vm:~$
  ```

- **Use crontab to run it daily:**

# 0 2,14 * * * sudo cp -f /var/log/auth.log /home/azureuser/logfile.log (Executes twice in a day at 2 am and 2 pm)



```
  GNU nano 7.2               /tmp/crontab.ST4p72/crontab
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
  0 2,14 * * * sudo cp -f /var/log/auth.log /home/azureuser/logfile.log
```