Project Title: *Secure Remote Access Setup and Configuration for Virtual Machines

Duration: 3 weeks

Objective:

The objective of this project is to enable you to understand, configure, and secure remote access to virtual machines (VMs) running Linux operating systems. This group will be responsible for setting up a VM, ensuring it is securely accessible from a physical computer, and documenting the process and security measures.

Project Tasks:

Group A: Linux VM Configuration and Access

1. *Virtual Machine Setup:*
   - Create a Linux-based virtual machine using your Azure portal
   - Configure the network settings of the VM to ensure it is accessible from the network.

2. *User Account Management:*
   - Create user accounts on the Linux VM for each group member.
   - Assign appropriate permissions and configure sudo privileges as necessary.

3. *Enable Secure Shell (SSH):*
   - Ensure SSH is installed and running on the Linux VM.
   - Configure the firewall to allow SSH connections (default port TCP/22).

4. *Generate and Deploy SSH Keys:*
   - Generate SSH key pairs for each group member.
   - Deploy the public keys to the ~/.ssh/authorized_keys file on the Linux VM.

5. *Secure the Connection:*

   - Set up a Virtual Private Network (VPN) or Network Security Group (NSG) to restrict access to the VM to specific IP addresses.

   - Implement SSH key-based authentication and disable password-based logins for SSH.

   - Document the steps taken to secure the VM and the SSH connection.

6. *Test Remote Access:*

   - Each group member should test remote access to the Linux VM using SSH.

   - Troubleshoot and resolve any connection issues.

7. *Monitoring and Logging:*

   - Enable and configure logging on the Linux VM to track remote access attempts (syslog or other logging service).

   - Monitor the logs for any unauthorized access attempts and document the findings.

8. *Documentation:*

   - Prepare a comprehensive report detailing the setup, security measures, and testing process.

   - Include screenshots and command outputs where applicable.

Deliverables:

1. *Group Report:*

   - Each person in this group should submit a detailed report of their work, including the following:

     - VM setup process.

     - User account creation and management.

     - Security measures implemented.

     - Remote access testing procedures and results.

     - Monitoring and logging configuration.

     - Any issues encountered and how they were resolved.

2. *Presentation:*

- This group should prepare a presentation summarizing their findings and demonstrating how they configured and secured the VM.

- The presentation should include a live demo or video showing the remote access process.

3. *Peer Review:*

- You are to peer-review each other's work, providing feedback on the setup, security measures, and documentation.

Project Title: *Secure Remote Access Setup and Configuration for Virtual Machines

Duration: 3 weeks

Objective:

The objective of this project is to enable you to understand, configure, and secure remote access to virtual machines (VMs) running Linux operating systems. This group will be responsible for setting up a VM, ensuring it is securely accessible from a physical computer, and documenting the process and security measures.

Project Tasks:

Group A: Linux VM Configuration and Access

1. *Virtual Machine Setup:*

- Create a Linux-based virtual machine using your Azure portal

- Configure the network settings of the VM to ensure it is accessible from the network.

Solution

Step 1: Sign in to Azure Portal

1. Go to the Azure portal and sign in with your Azure account.

Step 2: Create a Virtual Machine

1. In the Azure portal, search for **Virtual machines** in the search bar and select it.
2. Click on **Create** and then **Azure virtual machine**.

Step 3: Configure Basic Settings

1. **Subscription**: Select your subscription.
2. **Resource group**: Create a new resource group or select an existing one.
3. **Virtual machine name**: Enter a name for your VM.
4. **Region**: Choose the region where you want to deploy the VM.
5. **Image**: Select the Linux distribution you prefer (e.g., Ubuntu Server 22.04 LTS).
6. **Size**: Choose the size of the VM based on your requirements.
7. **Authentication type**: Select Password.
8. **Username**: Enter a username.
9. **Password:** Enter a password

Step 4: Configure Disk

1. **VM disk encryption:** Check the box for Encryption at the host. However, my subscription do not support it.
2. OS disk size: select the disk size for the VM.
3. OS disk type: Select the type of disk for the VM depending on your workload. SSD preferably.
4. Delete with VM: check the box if you want it to be deleted with VM.
5. Key management: select the key management of your choice.

Step 5: Configure Networking

1. **Virtual network**: Create a new virtual network or select an existing one.
2. **Subnet**: Create a new subnet or select an existing one.
3. **Public IP**: Ensure a public IP address is assigned to the VM.
4. **NIC network security group**: Select **Basic** and allow SSH (22) and HTTP (80) inbound ports.

Step 5: Review and Create

1. Click on **Review + create**.

2. Review all the settings and click on **Create**.

Step 6: Connect to Your VM

1. Once the VM is created, go to the **Virtual machines** section and select your VM.
2. Copy the public IP address of your VM.
3. Use an SSH client to connect to your VM:
4. ssh username@your_vm_public_ip

Configuration Parameter

Basics Configuration

Subscription: Azure subscription 1

Resource group: project_group_a

Virtual machine name: Project

Region: West US 2

Availability options: No infrastructure redundancy required

Zone options: Self-selected zone

Security type: Trusted launch virtual machines

Enable secure boot: Yes

Enable vTPM: Yes

Integrity monitoring: No

Image: Ubuntu Server 24.04 LTS - Gen2

VM architecture: x64

Size: Standard B1s (1 vcpu, 1 GiB memory)

Enable Hibernation: No

Authentication type: Password

Username: group_a@52.143.68.146

pass : group_a12345

Public inbound ports: SSH, RDP

Azure Spot: No

Disks Configuration

OS disk size: Image default

OS disk type: Premium SSD LRS

Use managed disks: Yes

Delete OS disk with VM: Enabled

Ephemeral OS disk: No

Networking Configuration

Virtual network: (new) Project-vnet

Subnet: (new) default (10.0.0.0/24)

Public IP: (new) Project-ip

Accelerated networking: Off

Place this virtual machine behind an existing load balancing solution? No

Delete public IP and NIC when VM is deleted: Disabled

Management

Microsoft Defender for Cloud: Basic (free)

System assigned managed identity: Off

Login with Microsoft Entra ID: Off

Auto-shutdown: Off

Backup: Disabled

Enable hotpatch: Off

Patch orchestration options: Image Default

Monitoring Configuration

Alerts: Off

Boot diagnostics: On

Enable OS guest diagnostics: Off

Enable application health monitoring: Off

Advanced

Extensions: None

VM applications: None

Cloud init: No

User data: No

Disk controller type: SCSI

Proximity placement group: None

Capacity reservation group: None

2. *User Account Management:*

- Create user accounts on the Linux VM for each group member.

- Assign appropriate permissions and configure sudo privileges as necessary.

Solution

Here's a step-by-step guide to help you set up user accounts for each group member:

Step 1: Connect to Your Linux VM

First, you need to connect to your Linux VM using password. You can do this from your local machine's terminal or using Azure Cloud Shell.

```
PS C:\Users\USER> ssh Group_a@20.7.71.254
Group_a@20.7.71.254's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1014-azure x86_64)

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

 System information as of Sun Sep 29 20:02:08 UTC 2024

  System load:  0.0               Processes:             110
  Usage of /:   6.7% of 28.02GB   Users logged in:       0
  Memory usage: 40%               IPv4 address for eth0: 10.0.0.4
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

14 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

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

Step 2: Create Folder and sub folder for User Accounts

Make folder called temitope and a subfolder called .ssh

#.ssh subfolder is where the authorised keys for ssh is stored

sudo mkdir -p /home/temitope/.ssh

Step3: Create an empty file called authorized_keys in sub folder for User Accounts

create an empty file called authorized_key where the ssh key will be stored

sudo touch /home/temitope/.ssh/authorized_keys

Step4: Create an administrator User Accounts

Create an administrator user account

sudo useradd -d /home/temitope temitope

Step 5: Set Password for the New User

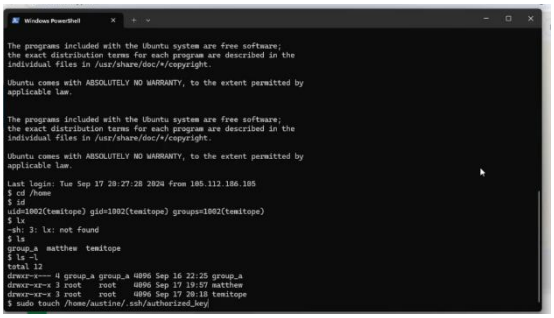
#set the user password

Command: sudo passwd temitope

Step 7: Grant the user a Sudo privileged as an administrator

#Add all user in group A to sudo group

Command: sudo usermod -aG sudo temitope

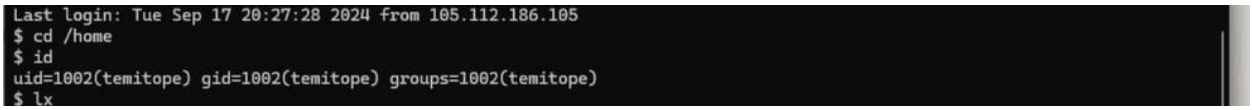


To Verify User Belongs to Sudo Group

Command: groups temitope or sudo cat /etc/group

To know the group User Belongs to

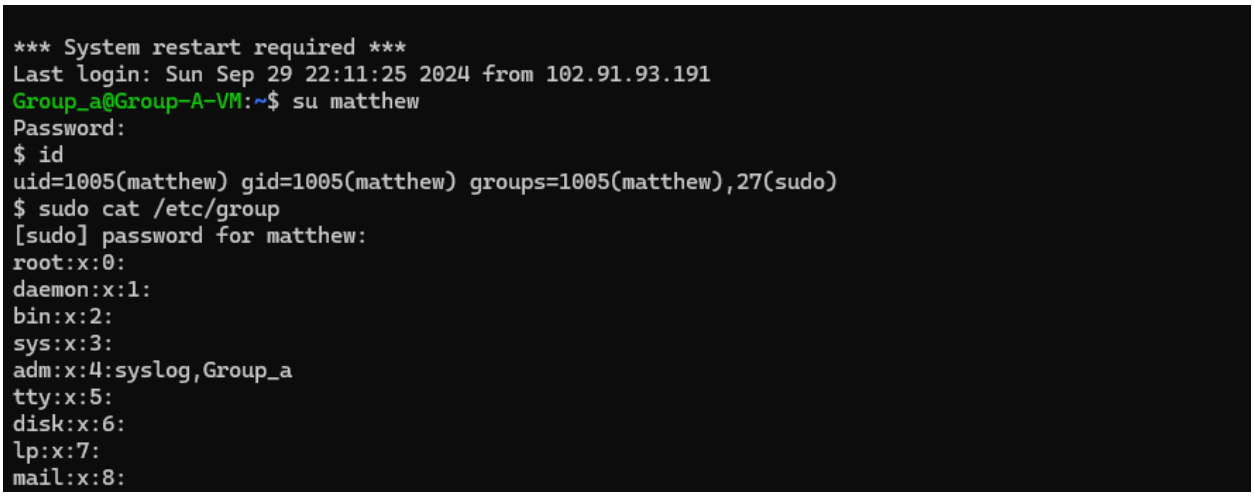
Command: Id



Step 8

Switch to your user account.

Command: su temitope (it prompts you to put in your password)



```
Group_a@Group-A-VM:~$ sudo cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,Group_a
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:Group_a
floppy:x:25:
tape:x:26:
sudo:x:27:Group_a,Austin,Damife,tosin,temitope,fola,matthew,frank
audio:x:29:
dip:x:30:Group_a
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:999:
systemd-network:x:998:
crontab:x:997:
systemd-timesync:x:996:
input:x:995:
sgx:x:994:
```

Step 9: Change Ownership for Directory

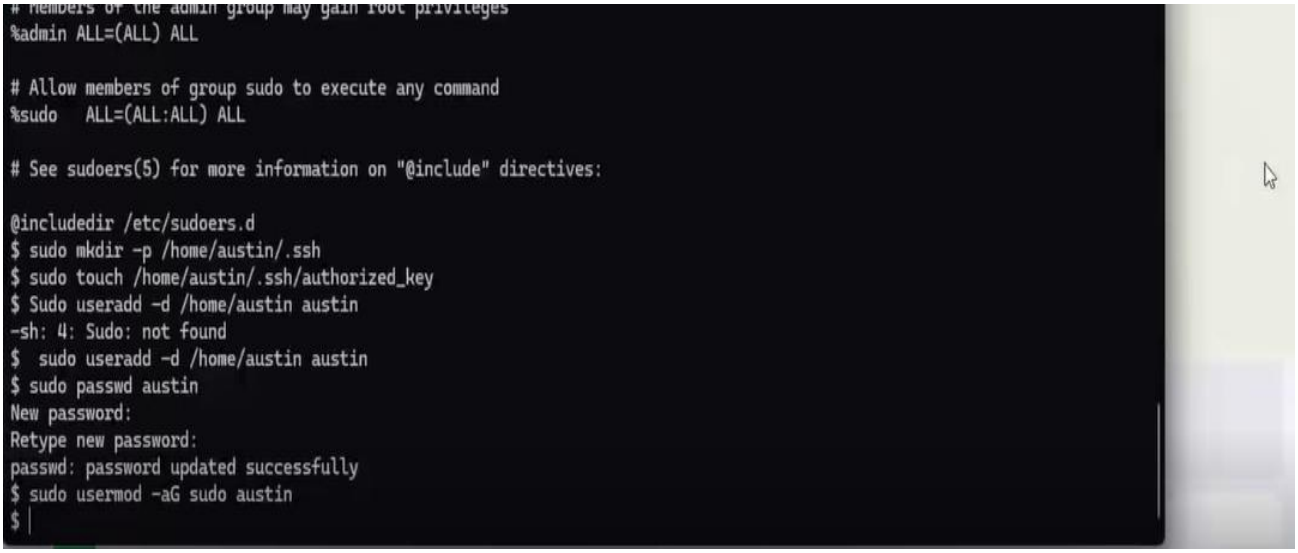
To assign ownership or changing ownership for the directory for each user

Command: sudo chown -R austin:austin /home/austin

Step 10: Grant user Permission require for directory and file

Command: sudo chmod 700 /home/austin/.ssh

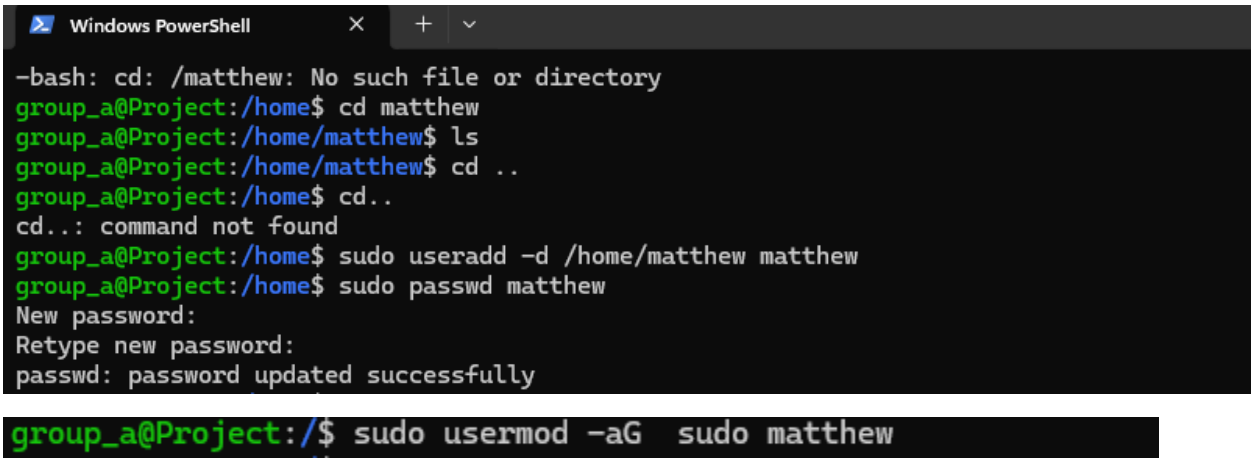
Command: sudo chmod 644 /home/austin/.ssh/authorized_keys



Step 11: Verify User Creation

You can verify that the user has been created and check their details using the id command:

id new_username



```
Last login: Tue Sep 17 19:55:45 2024 from 105.112.186.105
group_a@Project:~$ sudo usermod -aG  sudo temitope
group_a@Project:~$ cd /etc
group_a@Project:/etc$ cat config
cat: config: No such file or directory
group_a@Project:/etc$ ls
```

```
group_a@Project:/$ id
uid=1000(group_a) gid=1000(group_a) groups=1000(group_a),4(adm),24(cdrom),27(sudo),30(dip),105(lxd)
```

```
group_a@Project:/$ sudo cat /etc/group
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,group_a
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:group_a
floppy:x:25:
tape:x:26:
sudo:x:27:group_a,matthew,temitope
audio:x:29:
dip:x:30:group_a
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:
```

3. *Enable Secure Shell (SSH):*

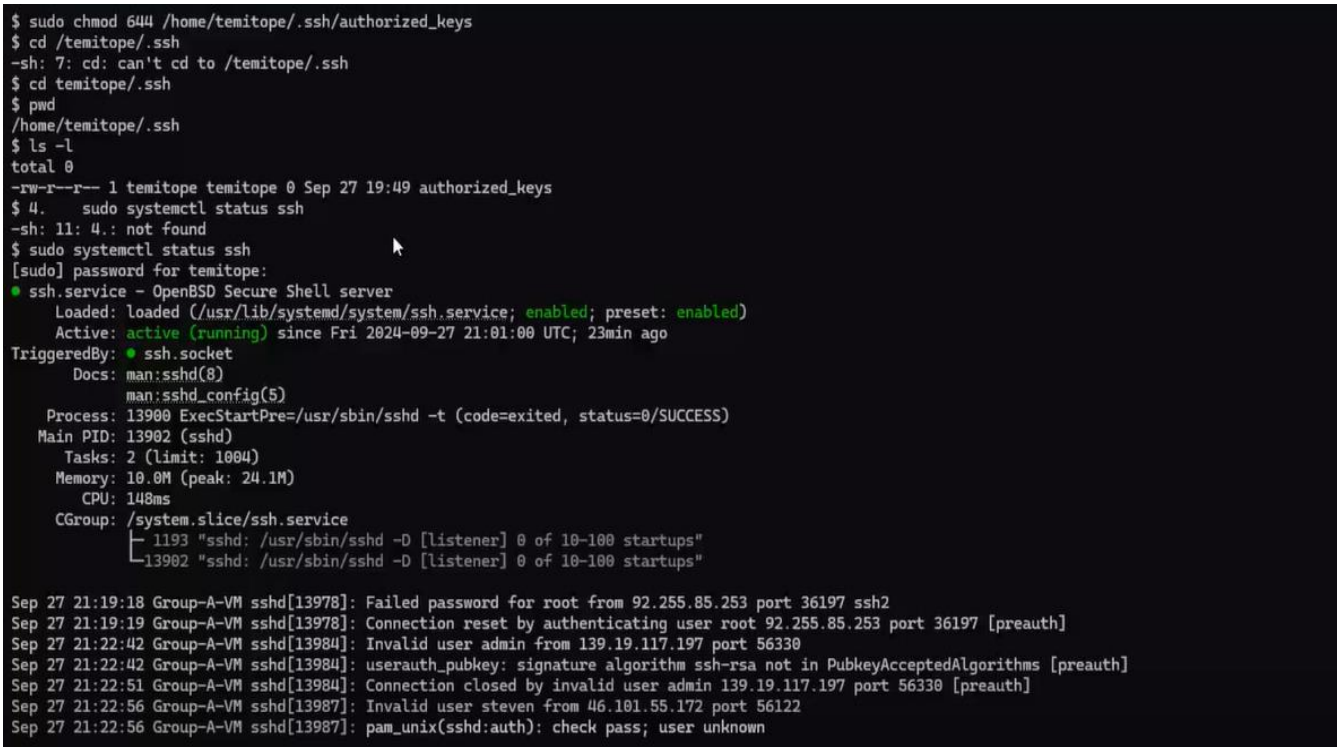
- Ensure SSH is installed and running on the Linux VM.

- Configure the firewall to allow SSH connections (default port TCP/22).

Solutiion

Step 1: Ensure SSH is Installed and Running

1. **Connect to your VM**:
2. ssh username@your_vm_public_ip
3. **Check if SSH is installed**:
4. sudo systemctl status ssh
5. Enter the Ctrl + C to go back to command prompt



If SSH is not installed, you can install it using:

sudo apt update

sudo apt install openssh-server

6. **Start and enable the SSH service**:
7. sudo systemctl start ssh
8. sudo systemctl enable ssh

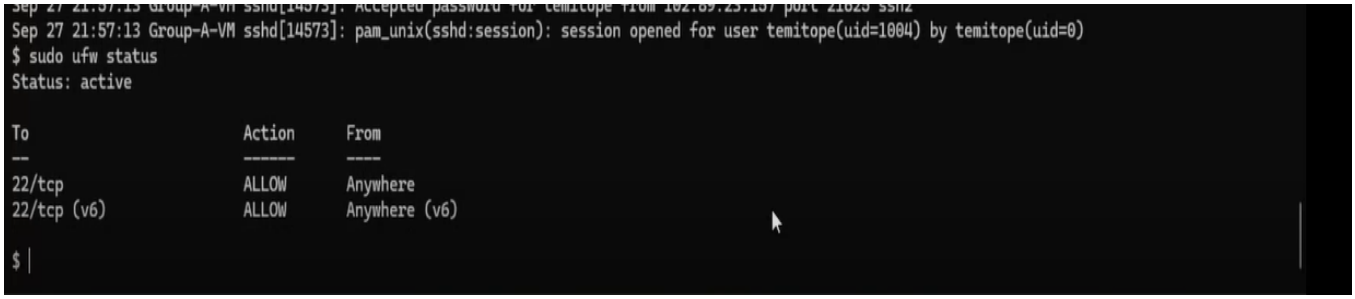
Step 2: Configure the Firewall to Allow SSH Connections

1. **Check the status of the firewall**:
2. sudo ufw status
3. **Allow SSH connections (default port TCP/22)**:
4. sudo ufw allow ssh

Alternatively, you can specify the port explicitly:

sudo ufw allow 22/tcp

5. **Enable the firewall**:
6. sudo ufw enable
7. **Verify the firewall rules**:
8. sudo ufw status



4. *Generate and Deploy SSH Keys:*

- Generate SSH key pairs for each group member.

- Deploy the public keys to the ~/.ssh/authorized_keys file on the Linux VM.

Solution

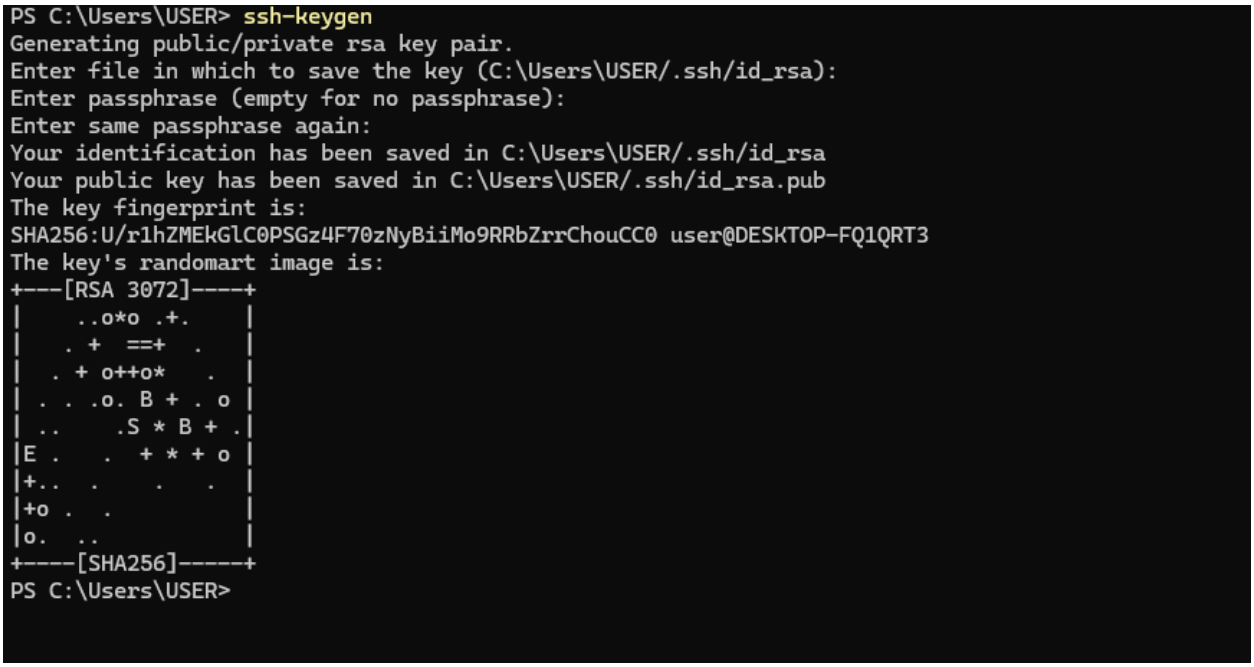
Here's how each group member generates SSH key pairs on your local machine and deploy the public keys to the ~/.ssh/authorized_keys file on the Linux VM:

Step 1: Generate SSH Key Pairs

Each group member needs to generate their own SSH key pair on their local machine. Here's how to do it:

1. **Open a terminal** on the local machine. e.g Powershell
2. **Generate the SSH key pair**:

   Command: ssh-keygen



3. **Follow the prompts** to save the key pair. By default, it will be saved in ~/.ssh/id_rsa and ~/.ssh/id_rsa.pub by press Enter key on the keyboard.

Step 2: Copy the Public Key to the VM

Each group member needs to copy their public key to their directory that is assigned to thmem ~/.ssh/authorized_keys file on the Linux VM. Here's how:

1. **Use the** scp(secure copy) **command** to copy the public key:
2. Scp C:\~/.ssh/id_rsa.pub username@ your_vm_Public IP address: home/your directory/.ssh/authorized_keys

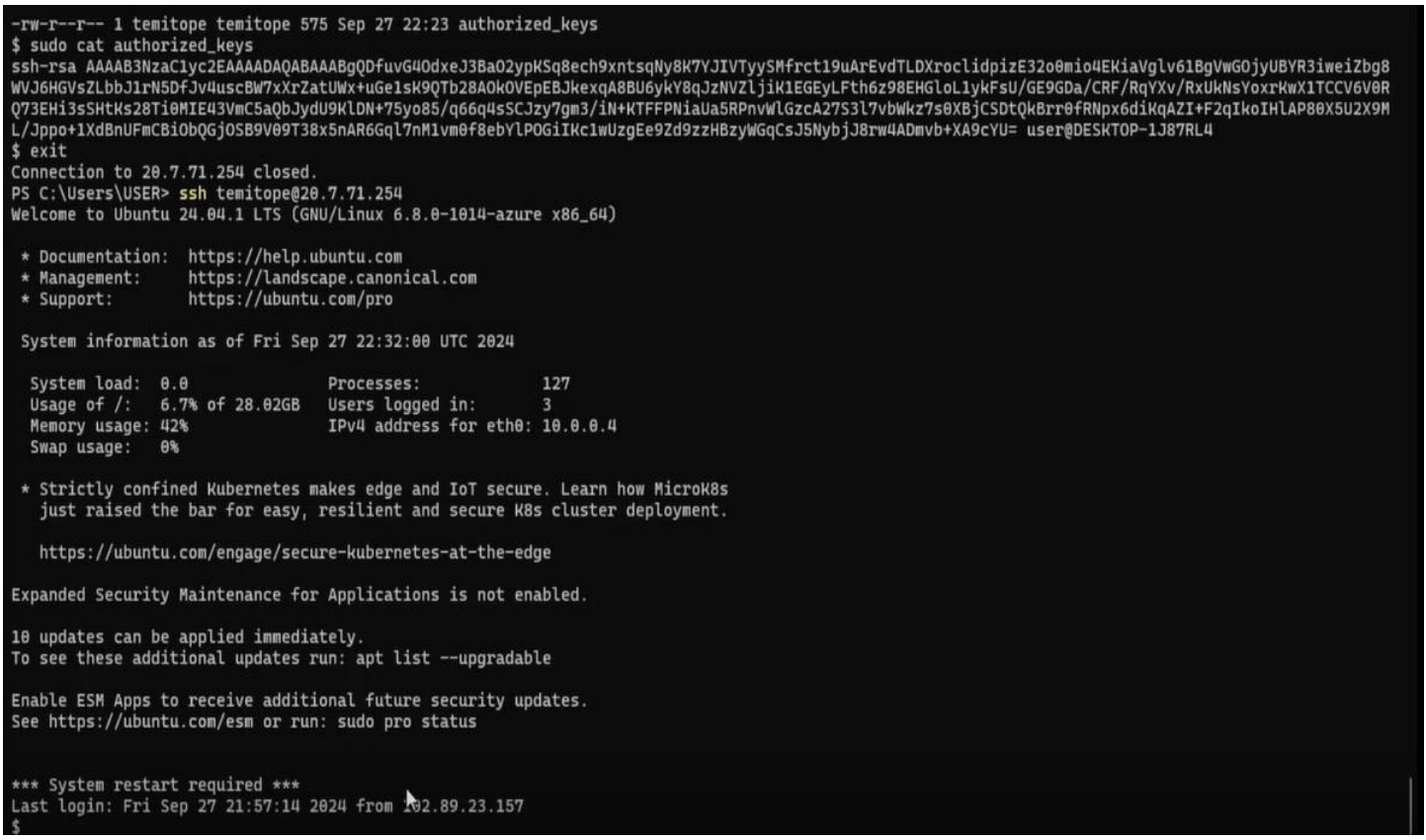
Example:

Command scp C:\Users\USER\.ssh\id_rsa.pub temitope@20.7.71.254:/home/temitope/.ssh/authorized_keys

Step 3: Verify the Setup

1. **Connect to the VM using SSH**:
2. ssh username@your_vm_public_ip

If the setup is correct, you should be able to log in without being prompted for a password



5. *Secure the Connection:*

- Set up a Virtual Private Network (VPN) or Network Security Group (NSG) to restrict access to the VM to specific IP addresses.

- Implement SSH key-based authentication and disable password-based logins for SSH.

- Document the steps taken to secure the VM and the SSH connection.

Solution

Let's go through the steps to set up a Network Security Group (NSG) to restrict access to your VM, implement SSH key-based authentication, disable password-based logins, and document the entire process.

Step 1: Set Up a Network Security Group (NSG)

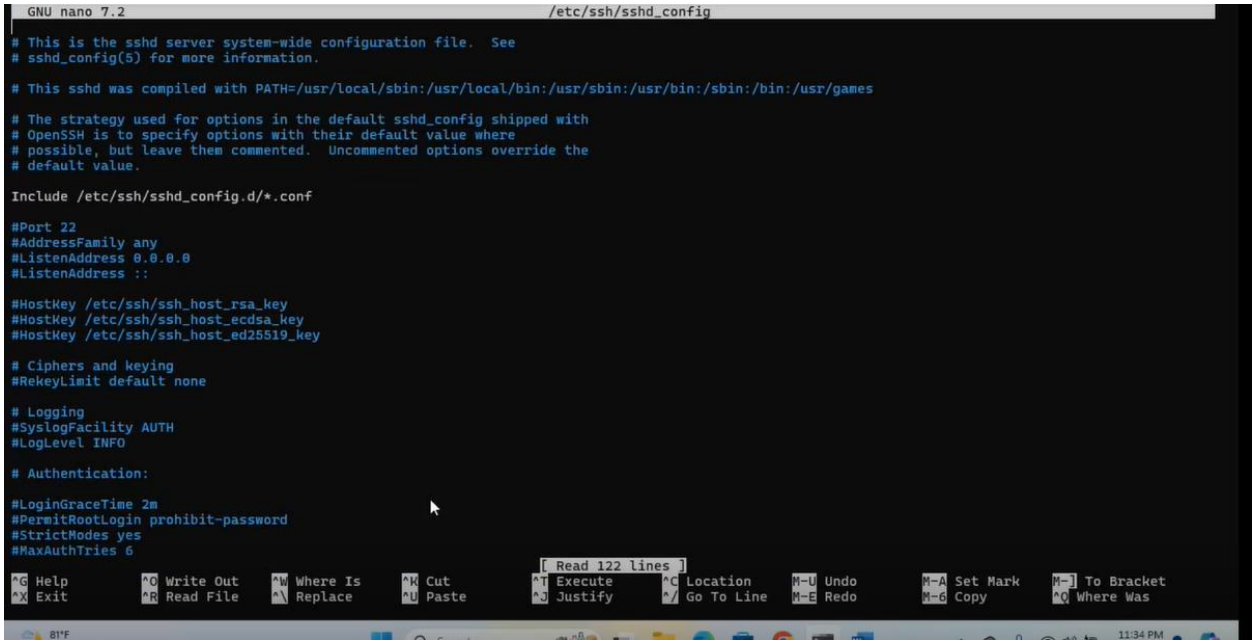
1. **Create an NSG**:
    - In the Azure portal, search for **Network security groups** and select it.
    - Click on **Create**.

- Fill in the required details such as **Subscription**, **Resource group**, **Name**, and **Region**.
- Click on **Review + create** and then **Create**.

2. **Add Inbound Security Rules**:
   - Go to your newly created NSG.
   - Under **Settings**, select **Inbound security rules**.
   - Click on **Add**.
   - Configure the rule to allow SSH (port 22) from specific (Public) IP addresses:
     - **Source**: IP Addresses
     - **Source IP addresses/CIDR ranges**: Enter the specific IP addresses or ranges.
     - **Destination**: Any
     - **Destination port ranges**: 22
     - **Protocol**: TCP
     - **Action**: Allow
     - **Priority**: Set a priority (e.g., 100).
     - **Name**: Give the rule a name (e.g., Allow-SSH).
3. **Associate NSG with VM's Network Interface**:
   - Go to your VM's **Networking** settings.
   - Under **Network interface**, select the network interface associated with your VM.
   - Under **Settings**, select **Network security group**.
   - Click on **Associate** and select the NSG you created.

Step 3: Disable Password-Based Logins

1. **Edit SSH Configuration**:
   - Connect to your VM:
   - ssh username@your_vm_public_ip
   - Open the SSH configuration file:
   - sudo nano /etc/ssh/sshd_config
   - Find the line #PasswordAuthentication yes and change it to:
   - PasswordAuthentication no
   - Save and exit the editor.



2. **Restart SSH Service**:
    - Restart the SSH service to apply the changes:
    - sudo systemctl restart ssh

6. *Test Remote Access:*

- Each group member should test remote access to the Linux VM using SSH.

- Troubleshoot and resolve any connection issues.

7. *Monitoring and Logging: *

- Enable and configure logging on the Linux VM to track remote access attempts (syslog or other logging service).

- Monitor the logs for any unauthorized access attempts and document the findings.

Solution

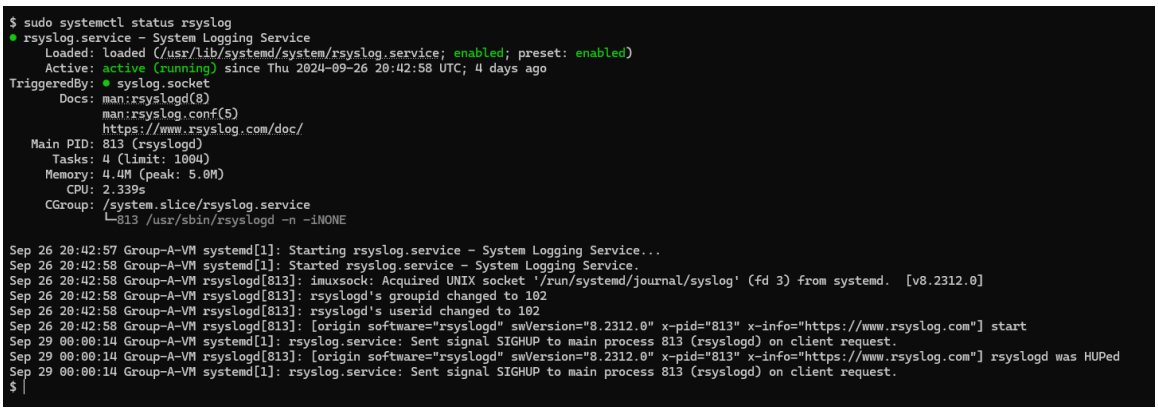
Enable and Configure Syslog for SSH Logging

The default logging system on most Linux distributions is syslog, which logs system events, including remote access attempts via SSH.

Step 1. Check if rsyslog is installed

Run the following command to check if rsyslog is installed and running:

```
sudo systemctl status rsyslog
```



If it's not installed, you can install it using:

```
sudo apt update
sudo apt install rsyslog
```

Step 2. Check SSH Logging in Syslog

By default, SSH logs are sent to `/var/log/auth.log` on Debian-based systems (e.g., Ubuntu). You can monitor this log for SSH access attempts:

```
sudo tail -f /var/log/auth.log
```

```
$ sudo tail -f /var/log/auth.log
2024-10-01T10:01:49.101947+00:00 Group-A-VM sshd[38859]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:01:50.920140+00:00 Group-A-VM sshd[38859]: Failed password for root from 119.249.51.221 port 37128 ssh2
2024-10-01T10:01:53.713967+00:00 Group-A-VM sshd[38859]: Connection closed by authenticating user root 119.249.51.221 port 37128 [preauth]
2024-10-01T10:01:58.661169+00:00 Group-A-VM sshd[38861]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:02:00.715188+00:00 Group-A-VM sshd[38861]: Failed password for root from 119.249.51.221 port 17440 ssh2
2024-10-01T10:02:03.190069+00:00 Group-A-VM sshd[38861]: Connection closed by authenticating user root 119.249.51.221 port 17440 [preauth]
2024-10-01T10:02:08.691063+00:00 Group-A-VM sshd[38863]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:02:10.785155+00:00 Group-A-VM sshd[38863]: Failed password for root from 119.249.51.221 port 14628 ssh2
2024-10-01T10:02:13.306234+00:00 Group-A-VM sshd[38863]: Connection closed by authenticating user root 119.249.51.221 port 14628 [preauth]
2024-10-01T10:02:16.763293+00:00 Group-A-VM sudo:  matthew : TTY=pts/0 ; PWD=/home ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2024-10-01T10:02:16.769276+00:00 Group-A-VM sudo: pam_unix(sudo:session): session opened for user root(uid=0) by matthew(uid=1005)
2024-10-01T10:02:18.408074+00:00 Group-A-VM sshd[38865]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:02:20.206397+00:00 Group-A-VM sshd[38865]: Failed password for root from 119.249.51.221 port 40748 ssh2
2024-10-01T10:02:22.762317+00:00 Group-A-VM sshd[38865]: Connection closed by authenticating user root 119.249.51.221 port 40748 [preauth]
2024-10-01T10:02:27.037806+00:00 Group-A-VM sshd[38870]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:02:29.071945+00:00 Group-A-VM sshd[38870]: Failed password for root from 119.249.51.221 port 25984 ssh2
2024-10-01T10:02:31.663557+00:00 Group-A-VM sshd[38870]: Connection closed by authenticating user root 119.249.51.221 port 25984 [preauth]
2024-10-01T10:02:36.603154+00:00 Group-A-VM sshd[38872]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:02:38.205757+00:00 Group-A-VM sshd[38872]: Failed password for root from 119.249.51.221 port 11692 ssh2
2024-10-01T10:02:39.536929+00:00 Group-A-VM sshd[38872]: Connection closed by authenticating user root 119.249.51.221 port 11692 [preauth]
2024-10-01T10:02:44.179089+00:00 Group-A-VM sshd[38874]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:02:46.213331+00:00 Group-A-VM sshd[38874]: Failed password for root from 119.249.51.221 port 26804 ssh2
2024-10-01T10:02:48.620490+00:00 Group-A-VM sshd[38874]: Connection closed by authenticating user root 119.249.51.221 port 26804 [preauth]
2024-10-01T10:02:53.331390+00:00 Group-A-VM sshd[38876]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:02:55.601025+00:00 Group-A-VM sshd[38876]: Failed password for root from 119.249.51.221 port 19964 ssh2
2024-10-01T10:02:57.732406+00:00 Group-A-VM sshd[38876]: Connection closed by authenticating user root 119.249.51.221 port 19964 [preauth]
2024-10-01T10:03:02.460171+00:00 Group-A-VM sshd[38878]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:03:04.298672+00:00 Group-A-VM sshd[38878]: Failed password for root from 119.249.51.221 port 36296 ssh2
2024-10-01T10:03:07.178638+00:00 Group-A-VM sshd[38878]: Connection closed by authenticating user root 119.249.51.221 port 36296 [preauth]
2024-10-01T10:03:11.950572+00:00 Group-A-VM sshd[38881]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:03:14.025031+00:00 Group-A-VM sshd[38881]: Failed password for root from 119.249.51.221 port 24128 ssh2
2024-10-01T10:03:16.557631+00:00 Group-A-VM sshd[38881]: Connection closed by authenticating user root 119.249.51.221 port 24128 [preauth]
2024-10-01T10:03:21.811057+00:00 Group-A-VM sshd[38883]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:03:23.925655+00:00 Group-A-VM sshd[38883]: Failed password for root from 119.249.51.221 port 15456 ssh2
2024-10-01T10:03:26.259681+00:00 Group-A-VM sshd[38883]: Connection closed by authenticating user root 119.249.51.221 port 15456 [preauth]
2024-10-01T10:03:31.466634+00:00 Group-A-VM sshd[38885]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
2024-10-01T10:03:32.953749+00:00 Group-A-VM sshd[38885]: Failed password for root from 119.249.51.221 port 36984 ssh2
2024-10-01T10:03:34.176593+00:00 Group-A-VM sshd[38885]: Connection closed by authenticating user root 119.249.51.221 port 36984 [preauth]
2024-10-01T10:03:39.023855+00:00 Group-A-VM sshd[38887]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=119.249.51.221  user=root
```

```
*** System restart required ***
Last login: Fri Sep 27 21:57:14 2024 from 102.89.23.157
$ sudo nano /etc/ssh/sshd_config
[sudo] password for temitope:
$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
     Active: active (running) since Thu 2024-09-26 20:42:58 UTC; 1 day 1h ago
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
   Main PID: 813 (rsyslogd)
      Tasks: 4 (limit: 1004)
     Memory: 3.7M (peak: 5.0M)
        CPU: 732ms
     CGroup: /system.slice/rsyslog.service
             └─813 /usr/sbin/rsyslogd -n -iNONE

Sep 26 20:42:57 Group-A-VM systemd[1]: Starting rsyslog.service - System Logging Service...
Sep 26 20:42:58 Group-A-VM systemd[1]: Started rsyslog.service - System Logging Service.
Sep 26 20:42:58 Group-A-VM rsyslogd[813]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3) from systemd.  [v8.2312.0]
Sep 26 20:42:58 Group-A-VM rsyslogd[813]: rsyslogd's groupid changed to 102
Sep 26 20:42:58 Group-A-VM rsyslogd[813]: rsyslogd's userid changed to 102
Sep 26 20:42:58 Group-A-VM rsyslogd[813]: [origin software="rsyslogd" swVersion="8.2312.0" x-pid="813" x-info="https://www.rsyslog.com"] start
$ sudo tail -f /var/log/auth.log
2024-09-27T22:32:00.387318+00:00 Group-A-VM (systemd): pam_unix(systemd-user:session): session opened for user temitope(uid=1004) by temitope(uid=0)
2024-09-27T22:34:21.077447+00:00 Group-A-VM sudo: temitope : TTY=pts/2 ; PWD=/home/temitope ; USER=root ; COMMAND=/usr/bin/nano /etc/ssh/sshd_config
2024-09-27T22:34:21.077815+00:00 Group-A-VM sudo: pam_unix(sudo:session): session opened for user root(uid=0) by temitope(uid=1004)
2024-09-27T22:35:01.394513+00:00 Group-A-VM CRON[15237]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
2024-09-27T22:35:01.398061+00:00 Group-A-VM CRON[15237]: pam_unix(cron:session): session closed for user root
2024-09-27T22:37:44.457467+00:00 Group-A-VM sudo: pam_unix(sudo:session): session closed for user root
2024-09-27T22:38:56.436275+00:00 Group-A-VM sudo: temitope : TTY=pts/2 ; PWD=/home/temitope ; USER=root ; COMMAND=/usr/bin/systemctl status rsyslog
2024-09-27T22:38:56.438944+00:00 Group-A-VM sudo: pam_unix(sudo:session): session opened for user root(uid=0) by temitope(uid=1004)
2024-09-27T22:38:56.455485+00:00 Group-A-VM sudo: pam_unix(sudo:session): session closed for user root
2024-09-27T22:43:04.724571+00:00 Group-A-VM sudo: temitope : TTY=pts/2 ; PWD=/home/temitope ; USER=root ; COMMAND=/usr/bin/tail -f /var/log/auth.log
2024-09-27T22:43:04.730251+00:00 Group-A-VM sudo: pam_unix(sudo:session): session opened for user root(uid=0) by temitope(uid=1004)
```

This log file will show all SSH login attempts, including both successful and unsuccessful logins.