Configure SSH with key-based authentication

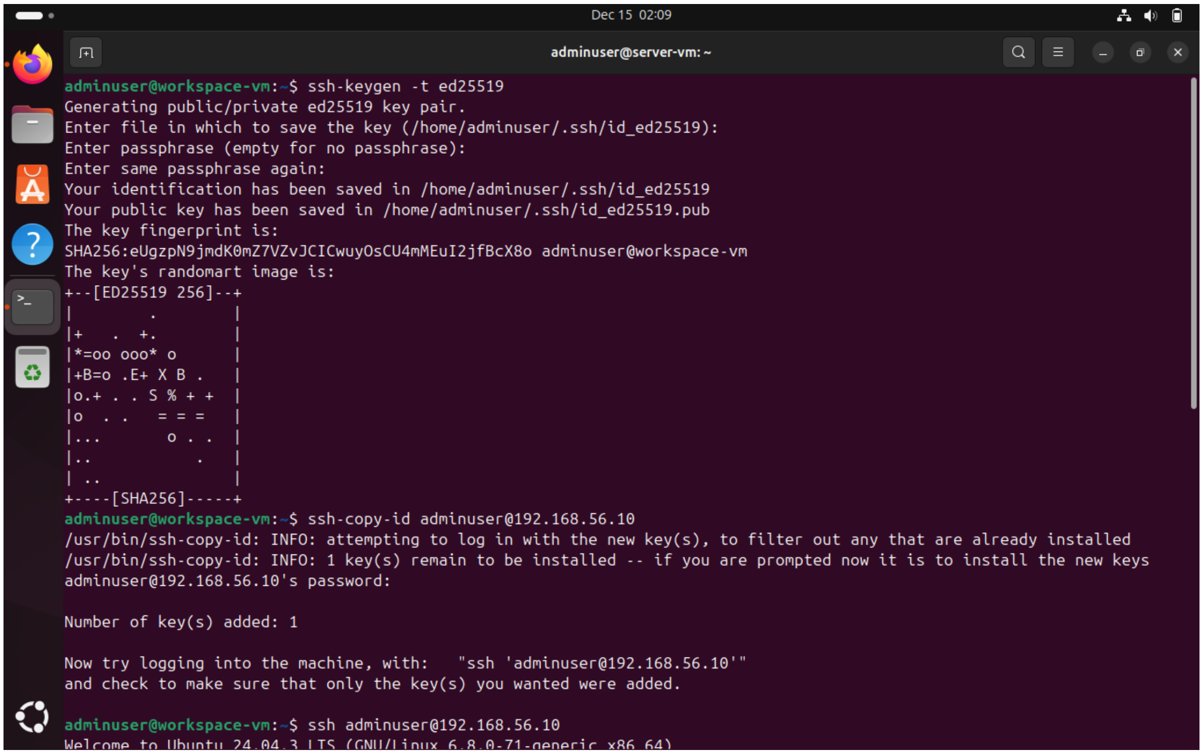
To secure access and prevent brute-force attacks on passwords, an ED25519 key pair was generated on the Workstation. The public key was transferred to the Server to enable cryptographic authentication.

Commands Executed (on Workstation):

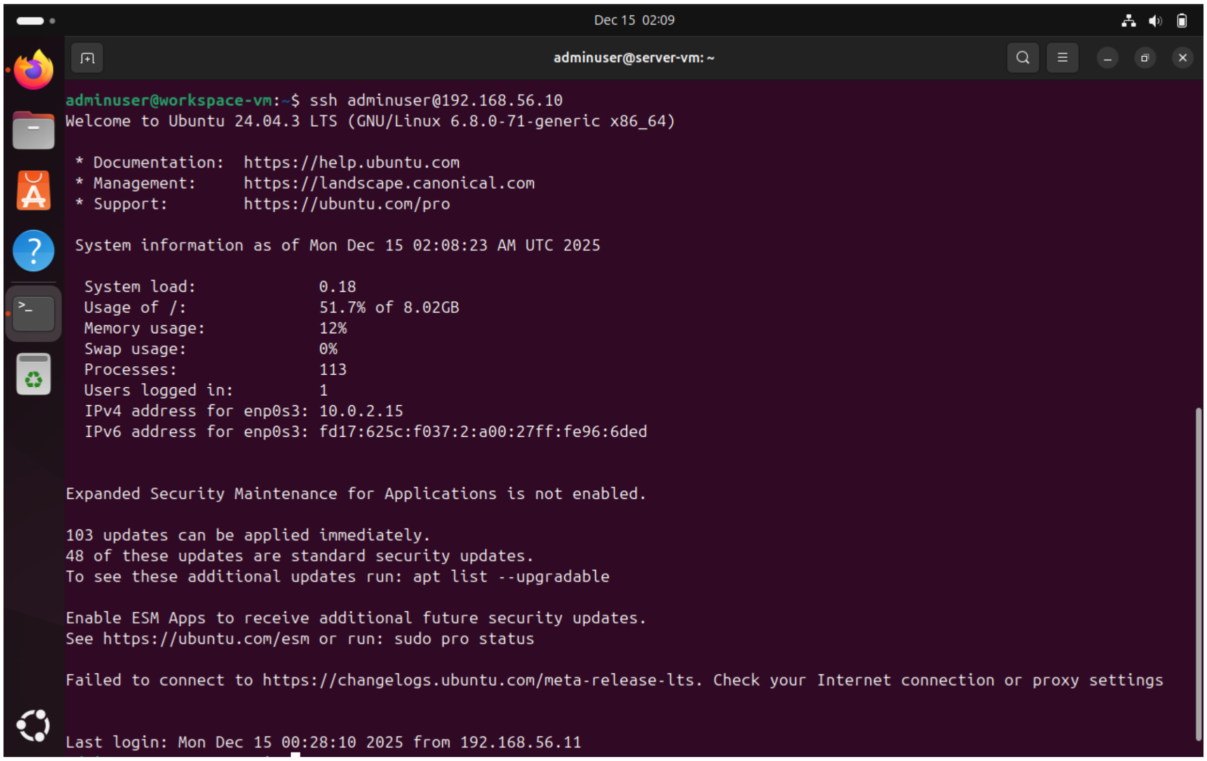
1. Generate SSH key pair
ssh-keygen -t ed25519

2. Copy public key to the server
ssh-copy-id adminuser@192.168.56.10

3. Verify password-less login
ssh adminuser@192.168.56.10



```
adminuser@workspace-vm:~$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/adminuser/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/adminuser/.ssh/id_ed25519
Your public key has been saved in /home/adminuser/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:eUgzpN9jmdK0mZ7VZvJCICwuyOsCU4mMEuI2jfBcX8o adminuser@workspace-vm
The key's randomart image is:
+--[ED25519 256]--+
|        .        |
|+   .  +.        |
|*=oo ooo* o      |
|+B=o .E+ X B .   |
|o.+ . . S % + +  |
|o  . .   = = =   |
|...       o . .  |
|..           .   |
| ..              |
+----[SHA256]-----+
adminuser@workspace-vm:~$ ssh-copy-id adminuser@192.168.56.10
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
adminuser@192.168.56.10's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'adminuser@192.168.56.10'"
and check to make sure that only the key(s) you wanted were added.

adminuser@workspace-vm:~$ ssh adminuser@192.168.56.10
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)
```



```
adminuser@workspace-vm:~$ ssh adminuser@192.168.56.10
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

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

 System information as of Mon Dec 15 02:08:23 AM UTC 2025

  System load:             0.18
  Usage of /:              51.7% of 8.02GB
  Memory usage:            12%
  Swap usage:              0%
  Processes:               113
  Users logged in:         1
  IPv4 address for enp0s3: 10.0.2.15
  IPv6 address for enp0s3: fd17:625c:f037:2:a00:27ff:fe96:6ded


Expanded Security Maintenance for Applications is not enabled.

103 updates can be applied immediately.
48 of these updates are standard security updates.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Dec 15 00:28:10 2025 from 192.168.56.11
```

Configure a firewall permitting SSH from one specific workstation only

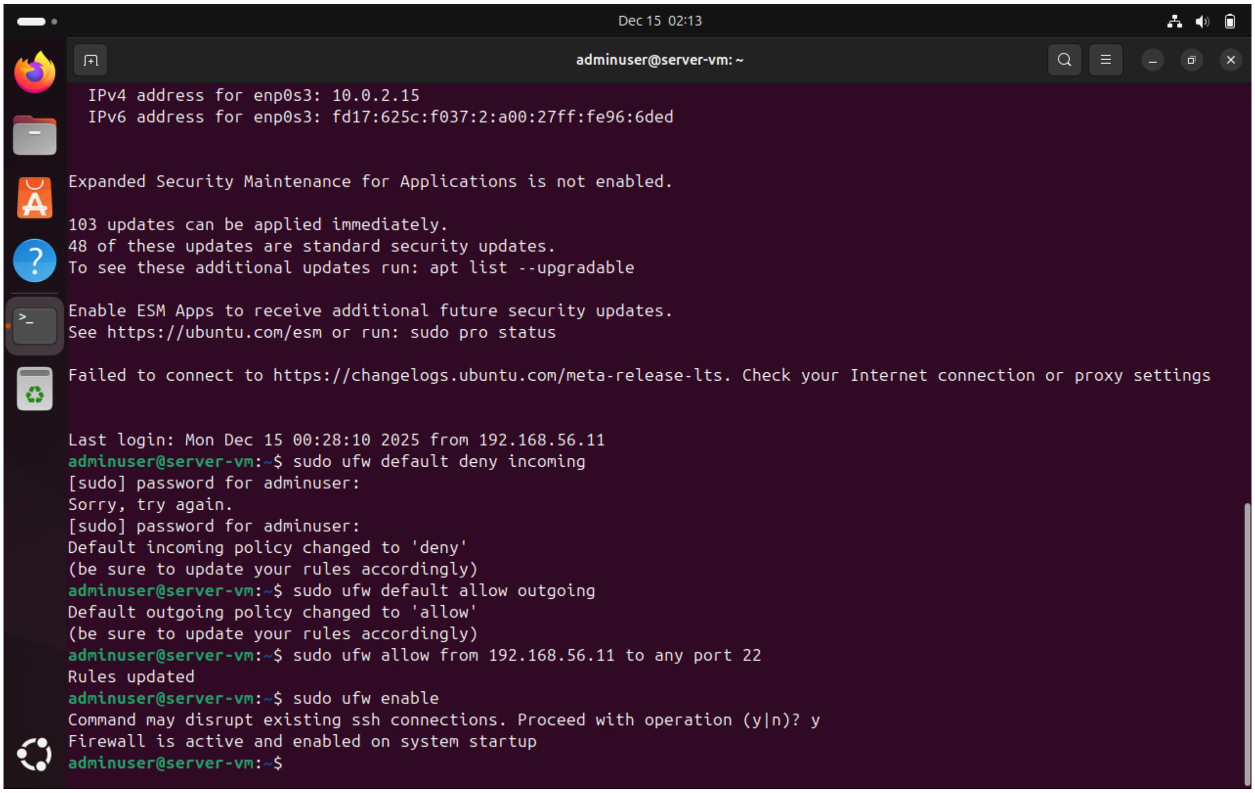
The Uncomplicated Firewall (UFW) was configured to deny all incoming traffic by default. A specific exception was made to allow SSH (port 22) connections only from the Workstation's IP address (192.168.56.11), effectively isolating the server from other network traffic.

Commands Executed:

1. Set default policies
sudo ufw default deny incoming
sudo ufw default allow outgoing

2. Allow SSH strictly from Workstation IP
sudo ufw allow from 192.168.56.11 to any port 22

3. Enable the firewall
sudo ufw enable



```
  IPv4 address for enp0s3: 10.0.2.15
  IPv6 address for enp0s3: fd17:625c:f037:2:a00:27ff:fe96:6ded


Expanded Security Maintenance for Applications is not enabled.

103 updates can be applied immediately.
48 of these updates are standard security updates.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Dec 15 00:28:10 2025 from 192.168.56.11
adminuser@server-vm:~$ sudo ufw default deny incoming
[sudo] password for adminuser:
Sorry, try again.
[sudo] password for adminuser:
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
adminuser@server-vm:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
adminuser@server-vm:~$ sudo ufw allow from 192.168.56.11 to any port 22
Rules updated
adminuser@server-vm:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
adminuser@server-vm:~$
```

Manage users and implement privilege management

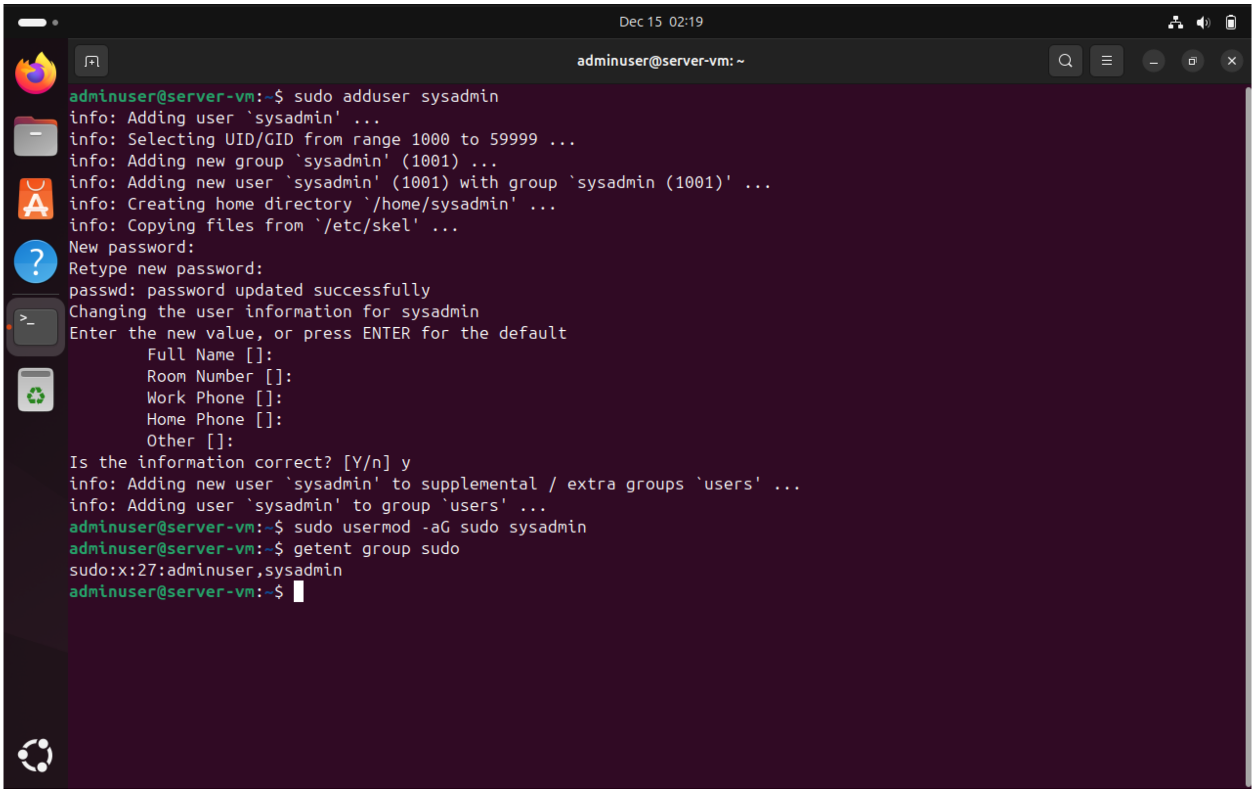
To adhere to the principle of least privilege, a dedicated administrative user (sysadmin) was created. This user was added to the sudo group to perform administrative tasks, removing the need to log in as the root user.

Commands Executed:

1. Create new administrative user
sudo adduser sysadmin

2. Grant sudo privileges
sudo usermod -aG sudo sysadmin

3. Verify group membership
getent group sudo



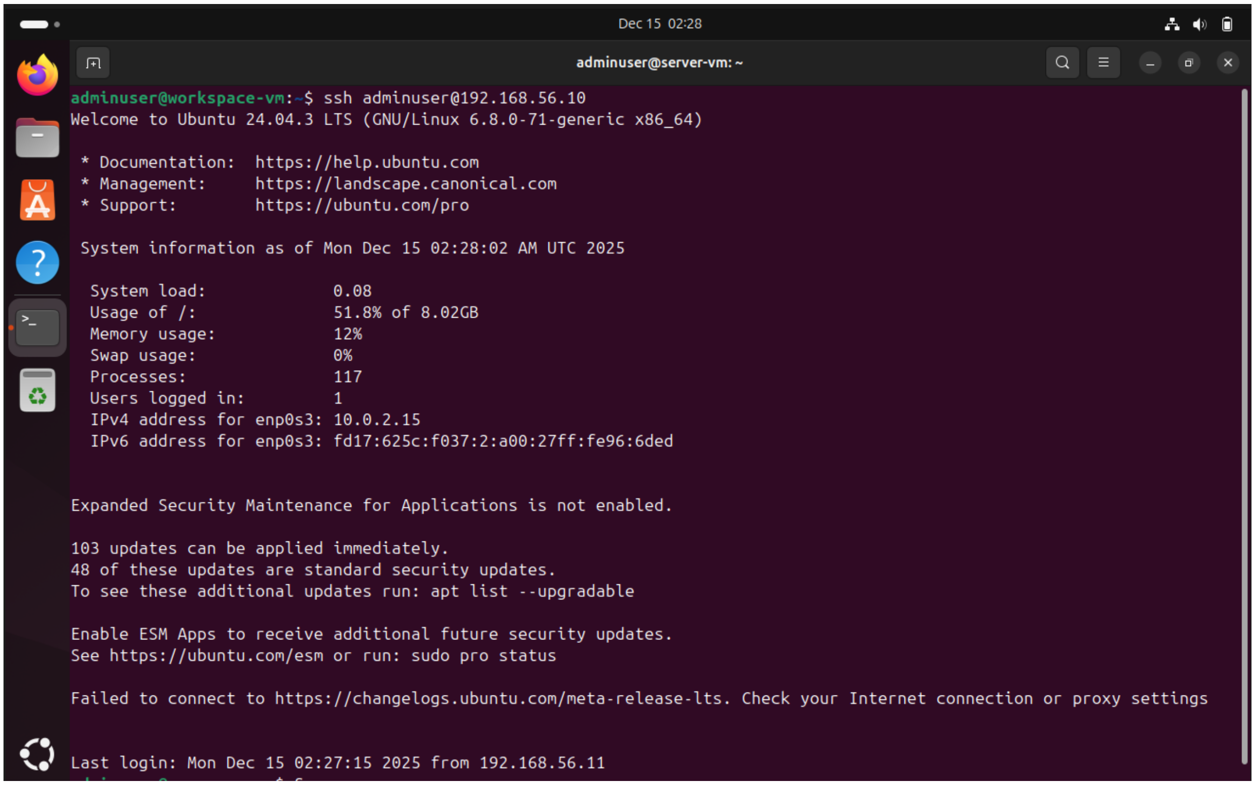
```
adminuser@server-vm:~$ sudo adduser sysadmin
info: Adding user `sysadmin' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `sysadmin' (1001) ...
info: Adding new user `sysadmin' (1001) with group `sysadmin (1001)' ...
info: Creating home directory `/home/sysadmin' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for sysadmin
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `sysadmin' to supplemental / extra groups `users' ...
info: Adding user `sysadmin' to group `users' ...
adminuser@server-vm:~$ sudo usermod -aG sudo sysadmin
adminuser@server-vm:~$ getent group sudo
sudo:x:27:adminuser,sysadmin
adminuser@server-vm:~$ 
```

SSH Access Evidence

This section provides evidence of a successful connection to the server using the new adminuser user and key-based authentication, confirming that the setup in Task 1 is functional.

Verification Command:

ssh adminuser@192.168.56.10



```
adminuser@workspace-vm:~$ ssh adminuser@192.168.56.10
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

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

 System information as of Mon Dec 15 02:28:02 AM UTC 2025

  System load:             0.08
  Usage of /:              51.8% of 8.02GB
  Memory usage:            12%
  Swap usage:              0%
  Processes:               117
  Users logged in:         1
  IPv4 address for enp0s3: 10.0.2.15
  IPv6 address for enp0s3: fd17:625c:f037:2:a00:27ff:fe96:6ded


Expanded Security Maintenance for Applications is not enabled.

103 updates can be applied immediately.
48 of these updates are standard security updates.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Mon Dec 15 02:27:15 2025 from 192.168.56.11
```

Configuration Files with before and after comparisons

The SSH daemon configuration (/etc/ssh/sshd_config and /etc/ssh/sshd_config.d/*.conf) was hardened. The root account login and password authentication were explicitly disabled to force the use of SSH keys.

Changes applied:

PermitRootLogin changed from yes to no

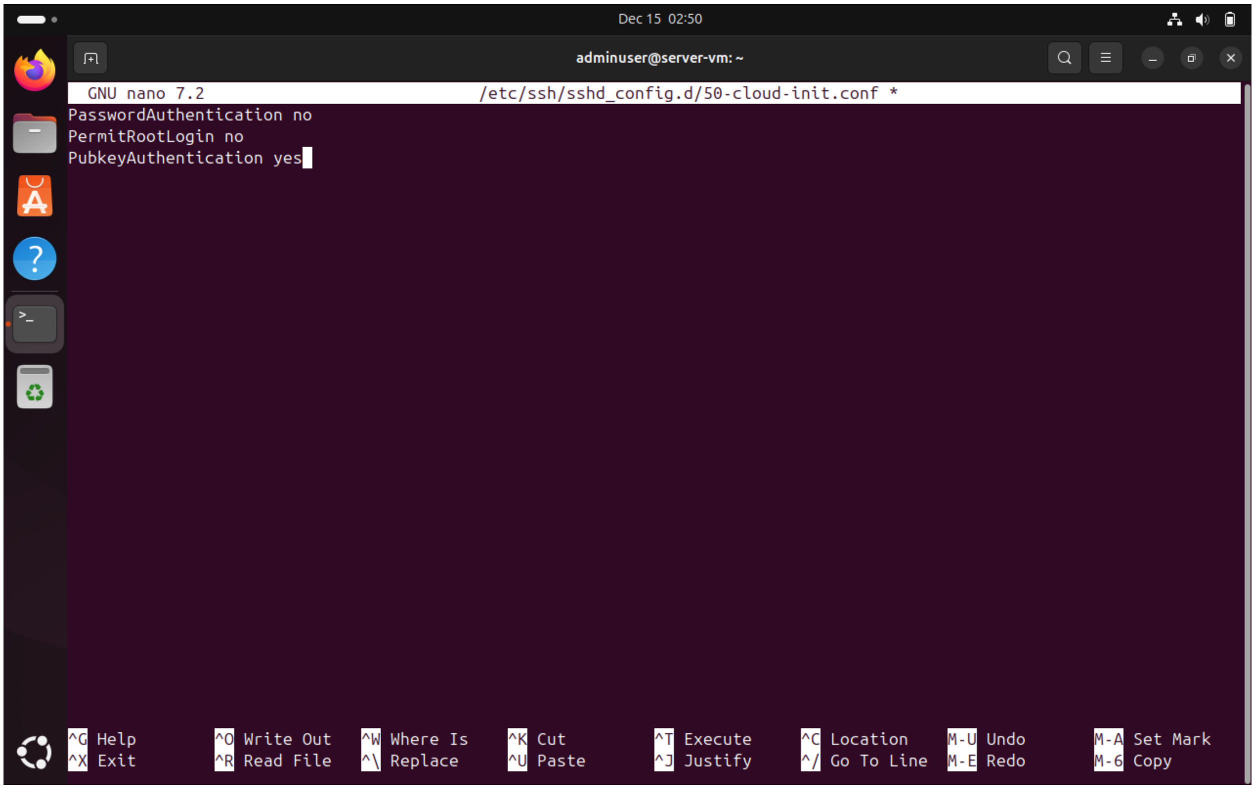
PasswordAuthentication changed from yes to no

PubkeyAuthentication set to yes

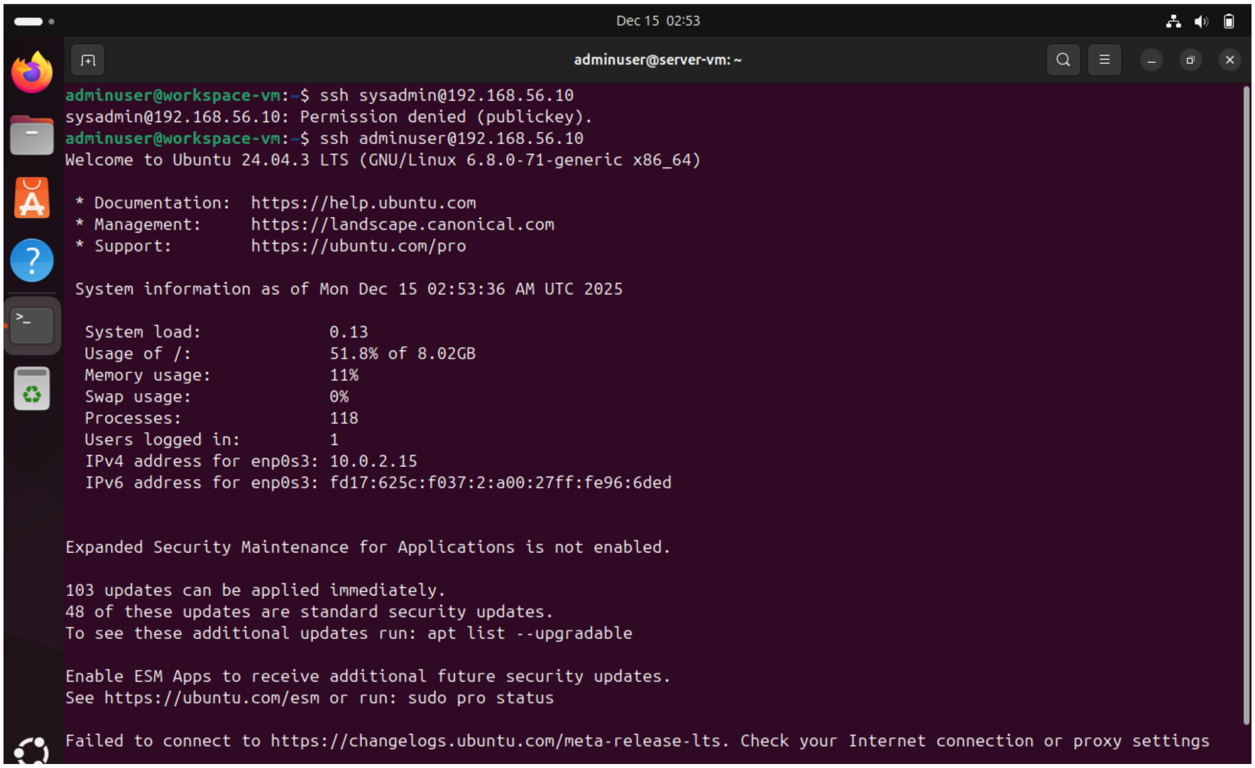
Commands to Apply & Verify:

1. Edit configuration
sudo nano /etc/ssh/sshd_config.d/*.conf

2. Restart SSH service to apply changes
sudo systemctl restart ssh



```
  GNU nano 7.2                     /etc/ssh/sshd_config.d/50-cloud-init.conf *
PasswordAuthentication no
PermitRootLogin no
PubkeyAuthentication yes
```



```
adminuser@workspace-vm:~$ ssh sysadmin@192.168.56.10
sysadmin@192.168.56.10: Permission denied (publickey).
adminuser@workspace-vm:~$ ssh adminuser@192.168.56.10
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-71-generic x86_64)

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

 System information as of Mon Dec 15 02:53:36 AM UTC 2025

  System load:             0.13
  Usage of /:              51.8% of 8.02GB
  Memory usage:            11%
  Swap usage:              0%
  Processes:               118
  Users logged in:         1
  IPv4 address for enp0s3: 10.0.2.15
  IPv6 address for enp0s3: fd17:625c:f037:2:a00:27ff:fe96:6ded


Expanded Security Maintenance for Applications is not enabled.

103 updates can be applied immediately.
48 of these updates are standard security updates.
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

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings
```

For sysadmin cannot login because user does not have publickey

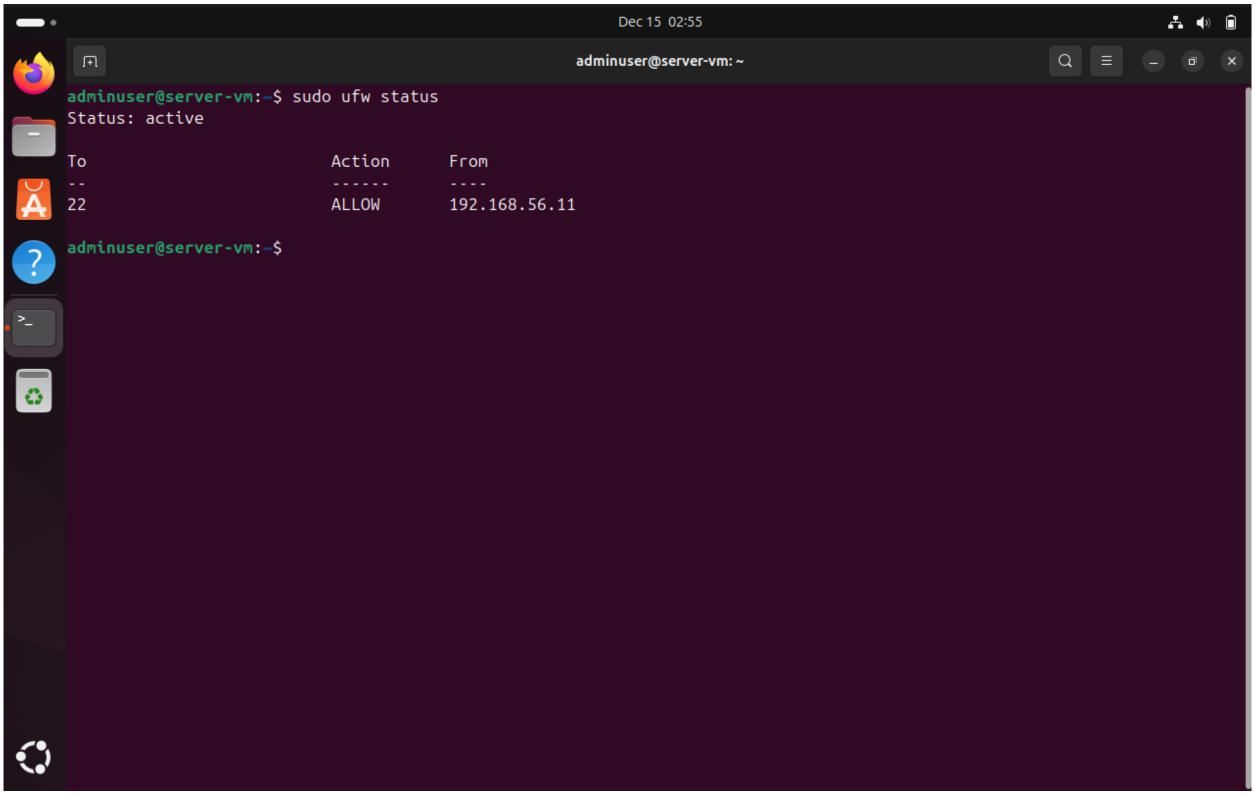
For adminuser can login because user have publickey

Firewall Documentation showing complete ruleset

Verification that the firewall is active, and the rules are correctly applied to restrict traffic to the management workstation only.

Verification Command:

sudo ufw status

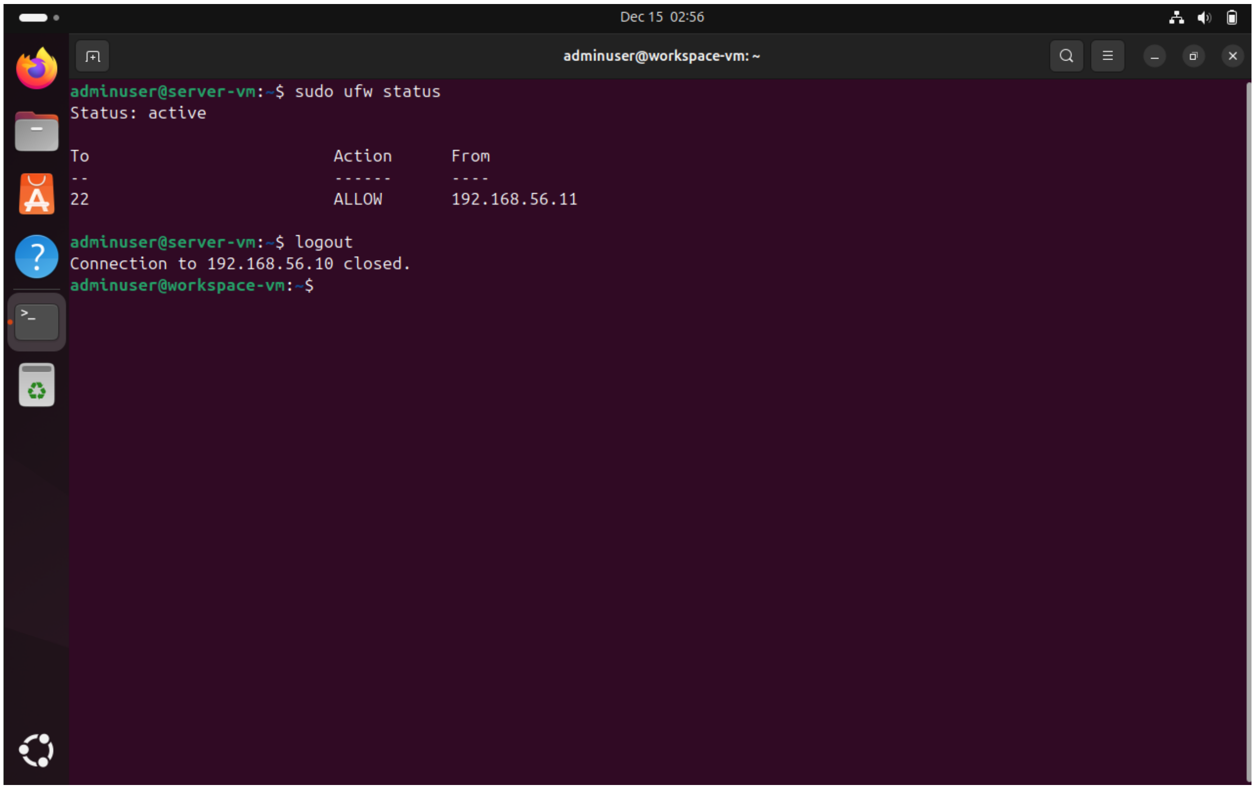


```
adminuser@server-vm:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       192.168.56.11

adminuser@server-vm:~$
```

Remote Administration Evidence

This section demonstrates that all commands referenced above were executed via a remote connection, complying with the assessment's administrative constraints.

1. sudo ufw status
2. logout



```
adminuser@server-vm:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       192.168.56.11

adminuser@server-vm:~$ logout
Connection to 192.168.56.10 closed.
adminuser@workspace-vm:~$
```