

## 1. Установка hostname

```
admin@ubuntu-tms-3:~$ sudo hostnamectl set-hostname ububuntu  
[sudo] password for admin:
```

```
admin@ububuntu:~$
```

## Установка даты и времени

```
admin@ububuntu:~$ timedatectl  
Local time: Mon 2026-02-09 10:58:59 UTC  
Universal time: Mon 2026-02-09 10:58:59 UTC  
RTC time: Mon 2026-02-09 10:56:27  
Time zone: Etc/UTC (UTC, +0000)  
System clock synchronized: yes  
NTP service: active  
RTC in local TZ: no  
admin@ububuntu:~$ sudo timedatectl set-timezone Europe/Minsk  
[sudo] password for admin:  
admin@ububuntu:~$ timedatectl  
Local time: Mon 2026-02-09 13:59:26 +03  
Universal time: Mon 2026-02-09 10:59:26 UTC  
RTC time: Mon 2026-02-09 10:56:34  
Time zone: Europe/Minsk (+03, +0300)  
System clock synchronized: yes  
NTP service: active  
RTC in local TZ: no
```

## Настройка NTP

```
[Time]  
NTP=0.pool.ntp.org 1.pool.ntp.org  
FallbackNTP=ntp.ubuntu.com
```

```
admin@ububuntu:~$ sudo nano /etc/systemd/timesyncd.conf  
admin@ububuntu:~$ sudo systemctl restart systemd-timesyncd  
admin@ububuntu:~$ timedatectl  
Local time: Mon 2026-02-09 14:05:42 +03  
Universal time: Mon 2026-02-09 11:05:42 UTC  
RTC time: Mon 2026-02-09 10:57:53  
Time zone: Europe/Minsk (+03, +0300)  
System clock synchronized: yes  
NTP service: active  
RTC in local TZ: no
```

## 2. Настройка сети через Netplan

```
network:
  version: 2
  ethernet:
    enp0s3:
      dhcp4: false
      addresses:
        - 192.168.1.50/24
      routes:
        - to: default
          via: 192.168.1.1
      nameservers:
        addresses:
          - 1.1.1.1
          - 8.8.8.8
```

```
admin@ubuntu:/etc/netplan$ sudo netplan apply
```

```
** (generate:4358): WARNING **: 14:12:11.075: Permissions for /etc/netplan/01-net-work-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
```

```
** (process:4356): WARNING **: 14:12:11.486: Permissions for /etc/netplan/01-net-work-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
```

```
** (process:4356): WARNING **: 14:12:11.575: Permissions for /etc/netplan/01-net-work-manager-all.yaml are too open. Netplan configuration should NOT be accessible by others.
```

### 3. Добавление пользователей:

```
admin@ubuntu:/etc/netplan$ sudo useradd -m -s /bin/bash -c "Full Name" newuser
admin@ubuntu:/etc/netplan$ sudo useradd -m -s /bin/bash -c "Full Name" newuser2
admin@ubuntu:/etc/netplan$ whoami
admin
admin@ubuntu:/etc/netplan$ sudo groupadd dev1
admin@ubuntu:/etc/netplan$ sudo groupadd dev2
admin@ubuntu:/etc/netplan$ sudo usermod -aG dev1 newuser
admin@ubuntu:/etc/netplan$ sudo usermod -aG dev2 newuser2
```

Выдача прав группе dev1 и пользователю newuser:

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

# Allow newuser to execute 'systemctl status'
%newuser ALL=(ALL) NOPASSWD: /bin/systemctl status *

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# Allow members of group dev1 to update/upgrade system
%dev1   ALL=(ALL) NOPASSWD: /usr/bin/apt update, /usr/bin/apt upgrade
```

Настройка доступа по ssh:

```
admin@ubuntu:~$ sudo mkdir /home/newuser2/.ssh
mkdir: cannot create directory '/home/newuser2/.ssh': File exists
admin@ubuntu:~$ sudo chmod 700 /home/newuser2/.ssh
admin@ubuntu:~$ sudo chown newuser2:newuser2 /home/newuser2/.ssh
admin@ubuntu:~$ sudo nano /home/newuser2/.ssh/authorized_keys
admin@ubuntu:~$ sudo chmod 600 /home/newuser2/.ssh/authorized_keys
chmod: cannot access '/home/newuser2/.ssh/authorized_keys': No such file or directory
admin@ubuntu:~$ sudo mkdir /home/newuser2/.ssh/authorized_keys
admin@ubuntu:~$ sudo chmod 600 /home/newuser2/.ssh/authorized_keys
admin@ubuntu:~$ sudo chown newuser2:newuser2 /home/newuser2/.ssh/authorized_keys
```

Изменение доступа по паролю:

```
admin@ubuntu: ~
GNU nano 7.2 /etc/ssh/sshd_config
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
GNU nano 7.2 /etc/ssh/sshd_config
# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
# the setting of "PermitRootLogin prohibit-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and KbdInteractiveAuthentication to 'no'.
UsePAM no

admin@ubuntu:~$ sudo systemctl restart sshd
```

Резы:

```
newuser@ububuntu:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab
   Active: active (running) since Mon 2026-02-09 16:07:48 +03; 11min ago
   TriggeredBy: ● ssh.socket
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 1097 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 1106 (sshd)
       Tasks: 1 (limit: 4603)
      Memory: 2.1M (peak: 2.5M)
         CPU: 44ms
        CGroup: /system.slice/ssh.service
                └─1106 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Feb 09 16:07:48 ububuntu systemd[1]: Starting ssh.service - OpenBSD Secure Shel
Feb 09 16:07:48 ububuntu sshd[1106]: Server listening on 0.0.0.0 port 22.
Feb 09 16:07:48 ububuntu sshd[1106]: Server listening on :: port 22.
Feb 09 16:07:48 ububuntu systemd[1]: Started ssh.service - OpenBSD Secure Shell
lines 1-18/18 (END)
newuser@ububuntu:~$ sudo systemctl restart ssh
[sudo] password for newuser:
Sorry, user newuser is not allowed to execute '/usr/bin/systemctl restart ssh' as root on ububuntu.
```



Доступ по ssh с другой ubuntu:

```
admin@ubuntu-tms-2:~/.ssh$ ssh 'newuser2@192.168.100.50'
Warning: Permanently added '192.168.100.50' (ED25519) to the list of known hosts.
newuser2@192.168.100.50's password:
newuser2@ububuntu:~$

admin@ubuntu-tms-2:~/.ssh$ ssh 'newuser@192.168.100.50'
Warning: Permanently added '192.168.100.50' (ED25519) to the list of known hosts.
Last login: Mon Feb 9 21:17:26 2026 from 192.168.100.80
newuser@ububuntu:~$
```

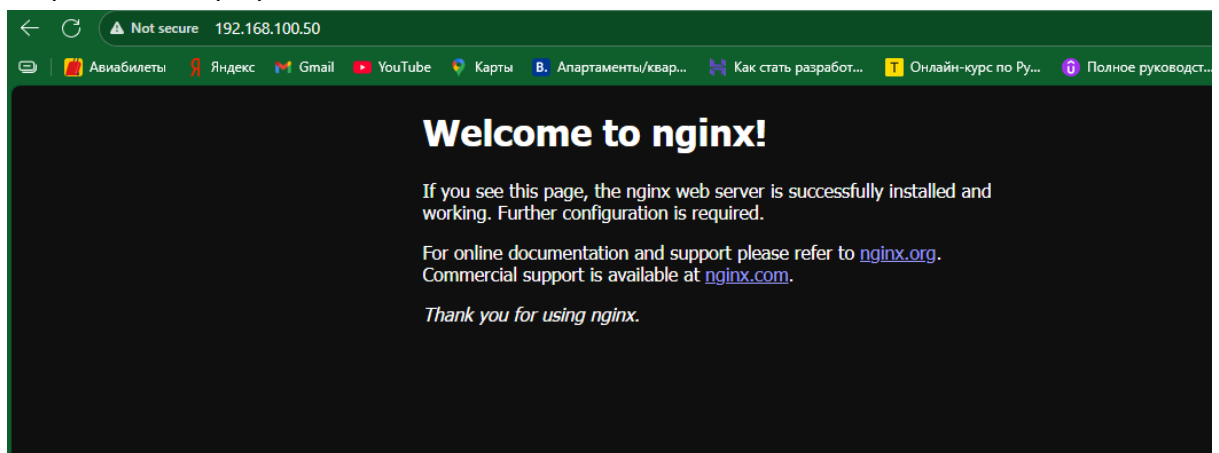
4. Настройка каталога для работы группы пользователей:

```
admin@ububuntu:/$ sudo mkdir /opt/dev1
[sudo] password for admin:
admin@ububuntu:/$ sudo chown :dev1 /opt/dev1
admin@ububuntu:/$ sudo chmod 770 /opt/dev1
admin@ububuntu:/$ sudo chmod g+s /opt/dev1
admin@ububuntu:/$ sudo -u newuser touch /opt/dev1/sometext.txt
admin@ububuntu:/$ sudo chmod 600 /opt/dev1/sometext.txt
admin@ububuntu:/$
```

5. Настройка:

```
admin@ubuntu:/home$ sudo ufw allow 22/tcp
adding existing rule
skipping adding existing rule (v6)
admin@ubuntu:/home$ sudo ufw allow 80/tcp
skipping adding existing rule
skipping adding existing rule (v6)
admin@ubuntu:/home$ sudo ufw enable
firewall is active and enabled on system startup
admin@ubuntu:/home$ sudo apt install nginx
Reading package lists... Done
Building dependency tree... Done
```

Разрешенный трафик:



Запрещенный трафик:

