

Step2: OS初期設定 (RockyLinux 9)

1. 管理ユーザーの作成

root 直ログインは避け、管理者ユーザーを作成します。

- ・新規ユーザー作成（例：**admin**）

```
sudo adduser admin
```

- ・パスワード設定

```
sudo passwd admin
```

- ・wheelグループに追加 (**sudo**権限付与)

```
sudo usermod -aG wheel admin
```

2. SSH鍵認証設定

- 公開鍵を表示（ホスト側で実行）

```
cat ~/.ssh/id_rsa.pub
```

- 出力された文字列をコピー

例:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQ...
```

- VMにSSHログインして、`~/.ssh/authorized_keys` を作成

```
mkdir -p ~/.ssh chmod 700
```

```
vi ~/.ssh/authorized_keys
```

コピーした公開鍵の内容を貼り付けて保存。

```
chmod 600 ~/.ssh/authorized_keys
```

- パーミッションを設定

3. SSHセキュリティ設定

- SSH設定を編集

`sudo vi /etc/ssh/sshd_config`

修正例:

`PermitRootLogin no`

`PasswordAuthentication no`

- SSH再起動

`sudo systemctl restart sshd`

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

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

4. パッケージ更新

常に最新のセキュリティパッチを適用します。

```
sudo dnf update -y
```

```
Installed:
```

```
kernel-5.14.0-570.37.1.el9_6.x86_64
```

```
kernel-modules-5.14.0-570.37.1.el9_6.x86_64
```

```
kernel-core-5.14.0-570.37.1.el9_6.x86_64
```

```
kernel-modules-core-5.14.0-570.37.1.el9_6.x86_64
```

```
Complete!
```

```
██████████@vbox ~]$ |
```

5. 時刻同期

システム時刻を日本標準時に設定します。

- ・タイムゾーンを東京に設定

`sudo timedatectl set-timezone Asia/Tokyo`

- ・chrony（NTPクライアント）が有効か確認

`sudo systemctl enable --now chronyd`

`timedatectl status`

```
@vbox ~]$ sudo systemctl enable --now chronyd
[vbox ~]$
[vbox ~]$
[vbox ~]$ timedatectl status
          Local time: Wed 2025-09-03 00:24:36 JST
          Universal time: Tue 2025-09-02 15:24:36 UTC
              RTC time: Tue 2025-09-02 15:24:36
          Time zone: Asia/Tokyo (JST, +0900)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
[vbox ~]$
```

6. firewalld 設定

SSHと必要なサービスのみ許可します。

- ・ firewalld起動

```
sudo systemctl enable --now firewalld
```

- ・ SSH許可

```
sudo firewall-cmd --permanent --add-service=ssh
```

```
sudo firewall-cmd --reload
```

- ・ 許可ルール確認

```
sudo firewall-cmd --list-all
```

```
@vbox ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: 
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

7. SELinux 確認

- getenforce
- Enforcing → 推奨設定（そのままOK）
- 実務では SELinux を有効にした状態で動作確認することが重要。

8. 動作確認

- 新しいユーザーで鍵認証ログインできるか確認
- `dnf update` でエラーがないか確認
- `timedatectl` で時刻同期が正しいか確認
- `firewall-cmd --list-all` で不要ポートが開いていないか確認

9.本Stepの学び

- Virtualboxからコマンド投入を行うと、コピペが使えず不便だが、PowerShellからssh接続することでコピペを使用し作業が行えることに気づき、効率が上がった。
- 鍵情報をサーバー側で保存し、パスワードログインを禁止することで、よりセキュアにログイン管理できることを学んだ。