DebianでWOLとDropbearを組み合わせて起動する方法

暗号化LVMだがパスフレーズ省略までは頑張らない

Kentaro Hayashi

ClearCode Inc.

OSC 2021 Online/Nagoya Lightning Talks

スライドは公開済みです

- DebianでWOLとDropbearを組み合わせて起動する方法
  - https://slide.rabbit-shocker.org/authors/kenhys/-osc2021-online-nagoya-lt-20210529/

プロフィール

- ひよこDebian Developer @kenhys
- トラックポイント(ソフトドーム派)
- わさビーフ(わさっち派)

本日の内容

- リモートから比較的簡単に
  Debianマシン(Bullseye)を起動する事例紹介

なぜリモートから起動したいか

- COVID-19前
  - たまに在宅勤務するときは社内チャット(Zulip)で電源を入れてもらうようお願いするのどかな光景😊
- COVID-19後
  - 在宅勤務のためオフィスにお願いできる人がいるとは限らない🤔

前提条件

- 社内ネットワークにSSH Gatewayを経由して入れる環境あり
- リモート起動したいマシンには**社内の固定IP**がふられている
- 対象マシンのディスクの**暗号化LVMは有効**にしておきたい
  - パスフレーズの入力の省略までは頑張らなくていい

解決策

- 電源投入はWake on LANで実施
- 暗号化LVMパスフレーズはSSH経由で入力する
  - Dropbearを設定しておく
- ホスト鍵のfingerprint不一致への対策
  - DropbearとOpenSSHのホストの鍵を揃える

Wake on LANで電源投入

- 対象のマシンにマジックパケットを投げつける
- 社内の他のマシンにwakeonlanがインストールされている必要あり

```
$ sudo apt install -y wakeonlan
$ wakeonlan (対象のMACアドレス)
```

暗号化LVMのパスフレーズ入力

- Dropbearのインストール
- SSHの公開鍵を設定
- GRUBの設定
- ホスト鍵を揃える
- initramfsの更新

Dropbearのインストール

- Dropbearとは
  - https://matt.ucc.asn.au/dropbear/dropbear.html
  - リソースの制約のきびしい組み込み機器向けSSHサーバー

```
$ sudo apt install -y dropbear busybox
```

SSHの公開鍵を設定

- /etc/dropbear-initramfs/authorized_keys
  - sshで~/.ssh/authorized_keysを置くのと一緒

GRUBの設定

```
GRUB_CMDLINE_LINUX="ip=(固定IP)::192.168.10.1:255.255.255.0::eno1:none"
```

- /etc/default/grub を書き換える
- インタフェース名(eno1)等は適宜読み替えて設定する
- sudo update-grubで更新する

DropbearとOpenSSHのホストの鍵を揃える

- 初期設定ではDropbearとOpenSSHそれぞれでホストの鍵を生成する
  - 同一IPでホスト鍵が変わるとssh接続時にエラーになるので面倒

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

- dropbearconvertで鍵を変換できる

変換対象の鍵

- /etc/ssh/ssh_host_ecdsa_key
  - /etc/dropbear-initramfs/dropbear_ecdsa_host_key
- /etc/ssh/ssh_host_ed25519_key
  - /etc/dropbear-initramfs/dropbear_ed25519_host_key
- /etc/ssh/ssh_host_rsa_key
  - /etc/dropbear-initramfs/dropbear_rsa_host_key

dropbearconvertの注意 (Bullseye)

- dropbear 2020.81-3 で openssh 8.4p1-5の場合

```
$ sudo dropbearconvert openssh dropbear \
  /etc/ssh/ssh_host_ecdsa_key \
  /etc/dropbear-initramfs/dropbear_ecdsa_host_key
Error: Unsupported OpenSSH key type
Error reading key from '/etc/ssh/ssh_host_ecdsa_key'
```

あつかえる形式に前処理する

- ssh-keygen -mを指定してPEM形式に変換する

```
$ cp /etc/ssh/ssh_host_ecdsa_key /tmp
$ ssh-keygen -p -m PEM -f /tmp/ssh_host_ecdsa_key
```

前処理した鍵を変換する

```
$ sudo dropbearconvert openssh dropbear \
      /tmp/ssh_host_ecdsa_key \
      /etc/dropbear-initramfs/dropbear_ecdsa_host_key
$ sudo dropbearconvert openssh dropbear \
      /tmp/ssh_host_ed25519_key \
      /etc/dropbear-initramfs/dropbear_ed25519_host_key
$ sudo dropbearconvert openssh dropbear \
      /tmp/ssh_host_rsa_key \
      /etc/dropbear-initramfs/dropbear_rsa_host_key
```

initramfsを更新する

```
$ sudo update-initramfs -u
```

Wake on LANで起動する

```
$ wakeonlan (MACアドレス)
Sending magic packet to 255.255.255.255:9 with (MACアドレス)
```

SSHで暗号化LVMのパスワードを解除

- 暗号化LVMのパスフレーズを入力するとsshが切れて通常起動する

```
% ssh radiant-rboot
To unlock root partition, and maybe others like swap, run `cryptroot-unlock`.



BusyBox v1.30.1 (Debian 1:1.30.1-6+b1) built-in shell (ash)
Enter 'help' for a list of built-in commands.
~ # cryptroot-unlock
Please unlock disk nvme0n1p3_crypt:
cryptsetup: nvme0n1p3_crypt set up successfully
~ # Connection to 192.168.10.109 closed by remote host.
Connection to 192.168.10.109 closed.
```

まとめ

- Wake on LANとDropbearでリモートからの起動を実現できる
  - 起動時のパスフレーズ入力は許容できるならお手軽
- OpenSSHとDropbearの鍵は統一しておくと便利