

夏のDNS祭り 2014 2014-07-05

ハンズオン - 準備編

株式会社ハートビーツ 滝澤 隆史

準備

ConoHa VPS

- 会場を提供していただいているConoHa様のVPSを使用します。
- みなさん、ConoHaのアカウントは作成済みですよ。
- 電話認証も済んでいますよ。
- まだの方は美雲このはさんに叱られてください。

ConoHa VPSの作成

- ConoHaコントロールパネルにアクセス
 - <https://cp.conoha.jp/>
- ログイン
- サービス→VPS
- VPS追加
 - プラン: メモリ1GB
 - OS: [標準OS] CentOS 6.5 (64bit)
- 追加したら起動完了するまでしばらく待つ
- 起動完了したら、「コンソール」画面に遷り、「SSH Private Key」からプライベート鍵をダウンロードしてね。
 - MacOS Xの人は鍵ファイルのパーミッションを600にするのを忘れずに。

sshで接続

- 「コンソール」画面にてIPv4アドレスを確認
- IPv4のIPアドレスに対してsshで接続する。

```
$ ssh -i XXXXXX.key root@IPアドレス
```

作業ユーザーの作成

- 作業用ユーザーの作成

```
# useradd ユーザー名
```

- sudoersを編集

```
# visudo
```

```
%wheel    ALL=(ALL)        NOPASSWD:  ALL
```

↑コメントアウトを解除して有効にする。

- wheelグループに補助グループとして追加

```
# usermod -G wheel ユーザー名
```

作業ユーザーの公開鍵の配置

- VPS用のものを使い回す場合

```
# mkdir -m 700 ~ユーザー名/.ssh
```

```
# cp /root/.ssh/authorized_keys ~ユーザー名/.ssh/
```

```
# chown -R ユーザー名: ~ユーザー名/.ssh
```

- 各自が作ったものを配置する場合

```
# su - ユーザー名
```

```
$ mkdir .ssh
```

```
$ vim .ssh/authorized_keys
```

作業ユーザーでログイン

- ログアウトして、作業ユーザーでログインできることを確認する。

```
$ ssh -i XXXXXX.key ユーザー名@IPアドレス
```

- sudoができることを確認する。

```
$ sudo whoami
```

```
root
```


iptablesのルールの設定

- ルールの確認

```
$ sudo iptables -nvL INPUT --line-numbers
```

- REJECTのルールの前にUDP 53番、TCP 53番のACCEPTのルールを追加

```
$ sudo iptables -I INPUT 5 -p udp -m state \  
  --state NEW -m udp --dport 53 -j ACCEPT
```

```
$ sudo iptables -I INPUT 6 -p tcp -m state \  
  --state NEW -m tcp --dport 53 -j ACCEPT
```

- ルールの登録の確認

```
$ sudo iptables -nvL INPUT --line-numbers
```

- ルールの保存

```
$ sudo service iptables save
```

ip6tablesのルールの設定

- ルールの確認

```
$ sudo ip6tables -nvL INPUT --line-numbers
```

- REJECTのルールの前にUDP 53番、TCP 53番のACCEPTのルールを追加

```
$ sudo ip6tables -I INPUT 5 -p udp -m state \  
  --state NEW -m udp --dport 53 -j ACCEPT
```

```
$ sudo ip6tables -I INPUT 6 -p tcp -m state \  
  --state NEW -m tcp --dport 53 -j ACCEPT
```

- ルールの登録の確認

```
$ sudo ip6tables -nvL INPUT --line-numbers
```

- ルールの保存

```
$ sudo service ip6tables save
```

digコマンドが使えることを確認

- bind-utilsパッケージがインストールされていることを確認

```
$ sudo rpm -q bind-utils
```

```
bind-utils-9.8.2-0.23.rc1.el6_5.1.x86_64
```

- bind-utilsパッケージが入っていない場合

```
$ sudo yum install bind-utils
```

- 確認

```
$ dig +short . soa
```

```
a.root-servers.net. nstld.verisign-grs.com.
```

```
2014070201 1800 900 604800 86400
```

IPアドレスの登録

- VPSのIPv4アドレスを次のシートの中の自分の席に記入
 - <http://goo.gl/hYHd5U>
 - ハンズオンの後半では座席の隣同士で2人ペアになってもらう
 - ぼっちな人は手を上げてください。
スタッフがペアを組んでくれるはず
 - 残りのスタッフは適宜ペアを組んで調整

以上で準備完了

おわり