細々したこと

http://d.hatena.ne.jp/bluepapa32/20101108/1289187846

■ Locale の変更

```
$ date
Thu Nov  4 14:58:50 UTC 2010
```

UTC になっている。

```
$ sudo cp -p /usr/share/zoneinfo/Japan /etc/localtime
```

```
$ date
Thu Nov  4 23:59:00 JST 2010
```

JST になった。

■ ntpd の設定

時刻がずれると色々問題なので、ntp を設定する

```
yum install ntp
/etc/init.d/ntpd start
chkconfig --level 2345 ntpd on
```

■ umask

vi .bashrc

```
umask 022
```

■ su、sudo の設定

vi /etc/pam.d/su

```
auth            required        pam_wheel.so use_uid
```

コメントイン。
visudo

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

secure_path に /usr/local/bin を追加しても良いかも。

管理者ユーザだけグループ追加

```
usermod -a -G wheel ユーザ
```

スワップ領域

http://cloudstory.in/2012/02/adding-swap-space-to-amazon-ec2-linux-micro-instance-to-increase-the-performance/

http://x68000.q-e-d.net/~68user/unix/pickup?dd
標準のままだとスワップ領域を持っていないこともある。
なくてもなんとかなるけど、作りたい時はスワップ領域をイメージファイルとして作成する

■スワップ領域のイメージファイル作成

```
dd if=/dev/zero of=/swapfile bs=1M count=1024
```

■スワップ領域の初期化

```
mkswap /swapfile
```

■スワップ領域の有効化

```
swapon /swapfile
```

もし /etc/fstab を編集後なら

```
swapon -a
```

でも良い。

■スワップ領域の確認

```
swapon -s
```

■ /etc/fstab: の編集

```
/swapfile swap swap defaults 0 0
```

SSH

パスワードログインの禁止

```
PasswordAuthentication yes
```

を

```
PasswordAuthentication no
```

に修正

ダイナミック DNS

http://b.n-at.me/archives/182
http://shikichi.ddo.jp/dice_install.html
http://www.jitaku-server.net/domain_dice.html

DiCE の設定

http://ddo.jp に登録

http://www.hi-ho.ne.jp/yoshihiro_e/dice/linux.html からダウンロード
解凍して適当なディレクトリに移動。(/usr/local/lib/DiCE とする）

```
cd /usr/local/lib/DiCE
./diced | nkf -uw
```

で起動する。 EUC で出力してくるので、文字化け対策のために nkf する。
もし ld-linux.so.2 不足でエラーが出る場合は

```
yum install glibc.i686
```

でライブラリ追加。

```
=-=-=- DiCE DynamicDNS Client -=-=-=
Version 0.19 for Japanese
Copyright(c) 2001 sarad

:?
```

? でヘルプ。

setup で DiCE の環境設定をします。

```
:setup
IP アドレスの検出方法を指定してください
(0) 自動検出
(1) ローカルのネットワークアダプタから検出
(2) 外部のスクリプトから検出
< 現在 :0>
(N) 変更しない  (P) 戻る
>n
-----------------------------------------------
プライベート IP アドレスも検出対象ですか？ (Y/N)
< 現在 : いいえ >
(P) 戻る
>n
-----------------------------------------------
IP アドレスの検出をテストしますか？ (Y/N)
(P) 戻る
>y
検出 IP アドレス >xxx.xxx.xxx.xxx
-----------------------------------------------
IP アドレスの検出をテストしますか？ (Y/N)
(P) 戻る
>n
-----------------------------------------------
IP アドレスをチェックする間隔を指定してください ( 分 )
設定可能範囲は 5 分以上です
< 現在 :10>
(N) 変更しない  (P) 戻る
>n
===============================================
DNS サーバーの負荷を軽減するために頻繁な DNS 更新を防ぐ必要があります
前回の更新から一定時間 DNS 更新処理を行わないように保護時間を設定して
ください ( 分 )  設定可能範囲は 10 分から 1440 分です
< 現在 :60>
(N) 変更しない  (P) 戻る
>30
===============================================
設定を保存しますか？ (Y/N)
(P) 戻る
>y
設定を保存しました
===============================================
```

add でイベント追加

```
:add
新しくイベントを追加します
DynamicDNS サービス名を入力してください
"?" で対応しているサービスを一覧表示します
(P) 戻る
>?            <-- 対応しているサービスを検索
ZENNO.COM livedoor MyDNS.JP pcc.jp
JPN.ch MyIP.US @nifty StaticCling
MyServer ddns.ca p2p did.expoze.com
Dynamx WebReactor unicc Earth
DNS2Go EveryDNS Now.nu dynDNS.it
onamae.com DION ODN ysdn
ddo.jp Netservers todd USA
cjb Dyn.ee BIGLOBE dnip
my-domain ZoneEdit ZiVE yi
theBBS SelfHOsT No-IP nicolas
miniDNS Microtech instat ieServer
HAMMERNODE GetmyIP Dynup Dynu
dyns DynDSL DynDNSdk dyndns
DtDNS dnsQ dhs DDNS.nu
cheapnet changeIP ARTofDNS VALUEDOMAIN
ODS JSPEED IPDYN DnsTokyo
================================================
>ddo.jp           <-- 今回は ddo.jp を使用
------------------------------------------------
<< Dynamic DO!.jp >>
URL: http://ddo.jp/
*** 情報 ***
ユーザー名の入力は不要です
独自ドメインの場合はドメイン名を " ホスト " の所へ入力してください
================================================
ドメイン名を入力してください
"?" でドメイン一覧を表示します
(P) 戻る
>ddo.jp       <-- 取得したドメインが ***.ddo.jp の場合（*** を除いた部分 )
================================================
ホスト名を入力してください
(P) 戻る
>***          <-- 取得したドメインが ***.ddo.jp の場合（ddo.jp を除いた部分 )
================================================
ログインユーザ名を入力してください
(P) 戻る
>***          <-- 取得したドメインが ***.ddo.jp の場合（ddo.jp を除いた部分 )
================================================
ログインパスワードを入力してください
(P) 戻る
>??????       <-- 登録時に設定したパスワード
================================================
登録する IP アドレスを入力してください
空白にすると現在の IP アドレスを自動検出します
(P) 戻る
>               <-- 空白のまま [enter]
このイベントに題名を付けてください
(P) 戻る
>***.ddo.jp の更新              <-- わかりやすい名前を設定
================================================
このイベントを実行するスケジュールを設定します
------------------------------------------------
実行する頻度を指定してください ( 番号入力 )
(0) １回のみ (1) １日１回 (2) １週間に１回 (3) １ヵ月に１回
(4) その他の周期 (5)IP アドレス変化時 (6) 起動時
(N) 変更しない (P) 戻る
>5            <-- サーバーに負荷をかけない
------------------------------------------------
IP アドレスがあまり変化しない環境の場合、更新せずに一定期間を過ぎると
アカウントを削除されてしまうことがあります
IP アドレスの変化が無い時に実行する間隔を指定してください
(0)7 日毎 (1)14 日毎 (2)21 日毎 (3)28 日毎
(4)35 日毎 (5)56 日毎 (6)84 日毎
(N) 変更しない (P) 戻る
>0            <-- ドメインが削除されないよう短めに設定
================================================
詳細オプションを設定します
------------------------------------------------
[ サービスタイプ ]
(0) 無料 (1) 有料
```

```
番号 >0
-----------------------------------------------
[ SSL ]
(0) 使用する (1) 使用しない
番号 >1
 -----------------------------------------------
 [ オフライン ]
 (0)No (1)Yes
 番号 >0
 ===============================================
 このイベントを有効にしますか？ (Y/N)
 ( イベントの有効 / 無効は "EN/DIS" コマンドで切替えられます )
 > y            <-- イベントを有効にする
 ===============================================
 イベントを保存しますか？ (Y/N)
 ( イベントの有効 / 無効は "EN/DIS" コマンドで切替えられます )
 > y            <-- イベントを保存する
```

サービス登録

/etc/init.d/ に移動

```
cd /etc/init.d/
```

起動スクリプトの作成

```
vi diced
```

```
#!/bin/sh
#
# chkconfig: 35 99 99
# description: DiCE
#
# diced: /usr/local/bin/DiCE/diced

diced="/usr/local/bin/DiCE/diced"

[ -f "$diced" ] || exit 0

case "$1" in
  start)
        # Start daemons.
        if [ ! -f /var/lock/diced ] ; then
            echo "Starting DiCE."
            "$diced" -d -l > /dev/null
            touch /var/lock/diced
        else
            echo "DiCE is Already Started."
        fi
        ;;
  stop)
        # Stop daemons.
        echo "Shutting down DiCE."
        PID=`/bin/ps -aefw | grep "$diced" | awk '{print $2}'`
        if [ ! -z "$PID" ] ;  then
            /bin/kill ${PID} 1> /dev/null 2>&1
        fi
        rm -f /var/lock/diced
        ;;
   *)
        echo "Usage: /etc/init.d/diced {start|stop}"
        exit 1
esac

exit 0
```

登録する

```
chkconfig --add diced
```

確認する

```
chkconfig --list | grep diced
```

パーミッションの変更

```
chmod 754 diced
```

サービススタート

```
service diced start
```

ログ確認

```
nkf -Ew /usr/local/lib/DiCE/log/events.log
```

cron 登録

普通は必要ないと思うのだけど、一週間に一度の更新が正常に動作していないことがある。
とりあえず、cron で一週間に一度の更新をする。

```
sudo crontab -e
00 02 * * 5 /usr/local/lib/DiCE/diced -e 0 > /dev/null
```

毎週金曜日の 2:00 に IP 更新をする。

Apache

インストール

```
yum install httpd
chkconfig --level 2345 httpd on
```

設定

■サーバの設定

vi /etc/httpd/conf/httpd.conf

```
KeepAlive On ← on が良いような気がするが、 off のままで運用してみる。
ServerTokens Prod ←  余計な情報を出さない
ServerSignature Off ←  余計な情報を出さない
```

メモリを食いつぶさないようにプロセス数を制御する
http://www.happyquality.com/2012/02/01/1905.htm
http://9ensan.com/blog/server/sakura-vps-httpd-confi/

```
<IfModule prefork.c>
StartServers       2
MinSpareServers    2
MaxSpareServers    5
ServerLimit       32
MaxClients        32
MaxRequestsPerChild 100
```

```
</IfModule>
```

ちなみに、httpd が prefork なのか worker なのかは

```
httpd -V | grep MPM
```

でわかる

■ public_html の設定

```
UserDir public_html ← public_html を有効
<Directory /home/*/public_html>
   AllowOverride FileInfo AuthConfig Limit Options
   Options MultiViews SymLinksIfOwnerMatch IncludesNoExec
```

AllowOverride All
Options All
は避けたい。ディレクティブの詳細は
http://httpd.apache.org/docs/2.2/ja/mod/core.html

■ Welcome 非表示

vi /etc/httpd/conf.d/welcome.conf

```
<LocationMatch "^/+$">
    Options -Indexes
#    ErrorDocument 403 /error/noindex.html
</LocationMatch>
```

CGI を使う

```
yum install perl
yum install php
```

.htaccess

```
Options +ExecCGI -Indexes
AddHandler cgi-script cgi pl
```

perl の実行権限は suExec によりホーム以下の場合は各ユーザの権限で実行される。
php での実行は、apache ユーザで実行されるので注意。
所有者を apache にするか、sgid と apache の umask の設定で対処する

vsftpd

```
 yum -y install vsftpd
chkconfig --level 2345 vsftpd on
```

vi /etc/vsftpd/vsftpd.conf

```
anonymous_enable=NO    ←  anonymous ユーザ ( 匿名ユーザ ) のログイン禁止
chroot_local_user=YES ←  デフォルトでホームディレクトリより上層へのアクセスを禁止する
userlist_deny=NO ←  user_list に書かれているユーザのみを許可する
```

```
use_localtime=YES ←　タイムスタンプ時間を日本時間にする
pasv_addr_resolve=YES　←　PASV モード接続先 IP アドレスをホスト名から取得する
pasv_address=hogehoge.ddo.jp　←　PASV モード接続先 IP アドレスが牽けるホスト名※
pasv_min_port=60000 ←　PASV モード接続時の最小ポート番号
pasv_max_port=60030 ←　PASV モード接続時の最大ポート番号
force_dot_files=YES ← .htaccess のような隠しファイルも表示する
```

この場合は 60000 ～ 60030 も Security Group の設定で通信を許可する

メール送信設定

sendmail コマンドで外部へメールを送る。
ただし、メールサーバは建てない。
なので、他のメールサーバにリレーしてもらう。

具体的な方法は、sendmail コマンドの smtp サーバの設定参照。

バックアップジョブ

EC2 API tools を使って cron でスナップショットを取得してバックアップを取る。

EC2 API tools をインストールする

Amazon EC2 に EC2 API tools をインストール

スナップショットによるバックアップ

Amazon EC2 を snapshot でバックアップ

メンテナンス記録

2014/10/25

中国を中心に大量アクセスがあったため、日本国内からのみアクセス可能とした

■流したスクリプト

```
#!/bin/sh

IPLIST=cidr.txt

# 初期化をする
iptables -F                    # Flush
iptables -X                    # Reset
#iptables -P INPUT DROP        # 受信はすべて破棄
iptables -P OUTPUT ACCEPT      # 送信はすべて許可
iptables -P FORWARD DROP       # 通過はすべて破棄

# サーバーから接続を開始した場合の応答を許可する。
iptables -A INPUT -i eth0 -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A INPUT -s 127.0.0.1 -j ACCEPT

if [ -z "$1" ]; then
  date=`date -d '1 day ago' +%Y%m%d`
else
  date="$1"
fi

if [ -e $IPLIST ]; then
    mv $IPLIST "${IPLIST}_${date}"
fi

# 最新の IP リストを取得する
wget http://nami.jp/ipv4bycc/$IPLIST.gz
gunzip -d $IPLIST.gz

# ダウンロードしてきた IP リストで日本の IP だけを許可するようにする
```

```
sed -n 's/^JP\t//p' $IPLIST | while read ipaddress; do
    iptables -A INPUT -s $ipaddress -j ACCEPT
done

# Amazon EC2 の Asia Pacific (Tokyo) に割り振られている IP レンジを許可する
iptables -A INPUT -s 46.51.224.0/19 -j ACCEPT
iptables -A INPUT -s 54.248.0.0/15 -j ACCEPT
iptables -A INPUT -s 103.4.8.0/21 -j ACCEPT
iptables -A INPUT -s 175.41.192.0/18 -j ACCEPT
iptables -A INPUT -s 176.34.0.0/18 -j ACCEPT
iptables -A INPUT -s 176.32.64.0/19 -j ACCEPT
iptables -A INPUT -s 54.250.0.0/16 -j ACCEPT


# iptables によって DROP されたアクセスのログを取る
#iptables -A INPUT -m limit --limit 1/s -j LOG --log-prefix '[IPTABLES INPUT DROP] : '
iptables -P INPUT DROP          # 受信はすべて破棄

# 設定を保存する場合はコメントを外す
#/etc/init.d/iptables save
```