LINUX サーバ構築演習

回答例

Ver. 1.0

リナックスアカデミー矢越昭仁

2012/01/15

目次

はじめに

この資料は Linux サーバ構築演習において、成果物として提供されるべき内容を例示したものです。当コースでは自ら問題点に気づき、調査・対策を行う事が求められ、回答というものは存在しません。この資料が、さらなるスキルアップにつながる事を期待しています。

表記について

この資料では以下の表記としています。

・フォント

コンピュータの操作および設定ファイルはクーリエフォント(タイプライター風)を用います。

```
search t123006.la.net
nameserver 10.20.123.6
```

・プロンプト

コマンド入力例がある場合は、先頭はプロンプト($または#)で始めます。

$ は一般ユーザでの操作、#はルートユーザでの操作を表します。なおユーザ切り替え(su)は省略しています。

・強調(ボールド)

コマンド入力では、キーボードから入力する場合を、設定ファイルの場合は修正箇所など特に強調したい場合に**ボールド**を使います。

・凡その作業時間

凡その作業時間とは、過去に同様の作業を経験した人が再度実行した場合にかかる時間を想定しています。つまり事前調査や試行錯誤の時間を含まない作業時間を指します。

システム仕様書

テキストにある内容をより実践的に読み換え、再度構築するシステムの仕様を定義した。

機器諸言

#	装置名	機器諸言	備考
1	筐体	DELL OptiPlex 745	
2	CPU	Intel Core2 2.14GHz	/proc/cpuinfo(5)
3	メモリ	1GBytes	free(1)
4	グラフィック	Intel 82Q963/Q965	lspci(8)
5	IDE Ctl.	Intel 82801H SATA	lspci(8)
6	HDD	Seagate Barracuda (80GB)	smartctl(8)
7	DVD	Hitachi GCC-H10N	dmesg(8)
8	NIC	Broadcom BCM5754	lspci(8)

*備考欄には、情報の入手先を記述した。

使用ソフトウエアー覧

#	構成要素	ソフトウエア名、バージョン	備考
1	OS	CentOS 5.7	LA にあるキットからアップグレード。 2012/01/04 時点での最新版にする。
2	SSH	openssh-4.3p2-72.el5_6.3	2012/01/04 時点の最新
3	ネームサーバ	bind 9.3.6-16.P1.el5_7.1	同上
4	Web サーバ	httpd-2.2.3-53.el5.centos	同上
5	メールサーバ	postfix-2.3.3-2.3.el5_6 dovecot-1.0.7-7.el5	同上
6	DBMS	MySQL 5.0.77-4.el5_6.6	同上
7	Blog ツール	MTOS 5.12	個人ライセンス版を利用

上記のうち、1～5 は必須。7(6 は 7 の前提)については十分条件とする。

アカウント情報

上記設定に関するアカウント一覧

#	ユーザ名	パスワード	備考
1	root	himitu	OS システム管理ユーザ
2	student	himitu	OS 一般ユーザ
3	staff	linux	http ベーシック認証用 http://www.t123006.la.net/staff
4	dbadm	himitu	MySQL DB ユーザ
5	student	himitu	MTOS テストユーザ http://www.t123006.la.net/cgi-bin/MT/mt.cgi より

設定要件

OS インストール仕様

1. 最新バージョンとすること。
2. 日本語環境であること。
3. 必要最小限のパッケージを導入し、ディスク容量を軽減すること。
4. ネットワークは IPv4 のみとし、IP アドレス等は別途提示された内容を用いること。
5. SELinux は不要とする。
6. 一般ユーザを作成すること(ユーザ名任意)。

SSH

1. SSH プロトコル ver. 2 のみを使用し、ver.1 は使わないこと。
2. UNIX パスワード認証は禁止とする。
3. root による直接ログインは禁止とする。

ネームサーバ

1. LAN 内での使用のため、chroot は用いない。
2. 管理するゾーン情報は以下の通り。
   ① t**xxxyyy**.la.net ドメイン(10.20.xxx.0/16)にて、主要なホストを定義する。
   なお **xxx** は自 IP の第 3、**yyy** は第 4 オクテットを 3 桁で表す。
   主要なホストは ns, smtp, h**yyy**, www が必須で、全て同一 IP(自身の IP)
   例)自 IP が 10.20.123.6 の場合、ドメインは t123006.la.net となる。
   ② 任意ドメイン (10.20.**xxx'**.0/16、第3オクテットを自 IPと変えたもの)主要なホストを定義する。
   例) 自 IP が 10.20.123.6 の場合、10.20.124.0/16 や 10.20.125.0/16 を用いる。
   ラウンドロビンを使用する場合は、ホスト名 www に対し行うこと。
   ③ 自身のドメイン①の逆引きを定義すること。
   ④ la.net のセカンダリとする。(プライマリは 10.20.250.1)

Web サーバ

1. http://自サーバ/staff で、BASIC 認証を行うこと。
   ユーザ名は staff で、パスワードは任意
2. CGI は ScriptAlias および各ディレクトリに配置した .cgi ファイルで実行できること。
3. ホスト名によりアクセスするディレクトリが異なるよう仮想ホストを行う(*)
4. www.(任意ドメイン)のラウンドロビンに対応するよう IP ベースの仮想ホストを行う(*)

上記 3,4 については何れか一方が実装できればよい。

メールサーバ

1. ユーザ名@t**xxxyyyy**.la.netドメインでのメール発信(From)とする。
2. 送信サーバでは 10.20.123.0 以外からのリレーを禁止する。
3. postmaster 宛のメールは一般ユーザへ転送すること。
4. 受信サーバは POP3 のみを使用する。
5. MUA は特に指定しないが、GUI 対応の物を導入すること。

Blog ツール

1. Blog ツールとして MTOS を導入すること。
2. 上記 DBMS として MySQL を導入すること。
3. DBMS は Blog ツールからの利用のみとする。
4. オプションモジュール(Perl)については、可能な限り全て導入すること。

セキュリティ

1. パケットフィルターにより当該サービス以外へのアクセスを禁止すること。
2. 不要なサービスは起動しないこと。
3. その他、セキュリティに関し強化策をとること。

設定手順

上記作業について、どのように設定したか手順書を残すこと。

設定手順書

OS インストール

LA 環境にある CentOS DVD よりインストーラを起動、以下主だった指定内容を記載。

1. インストール言語: 日本語
   [Language Selection]にて Japanese を選択

2. キーボード: OADG106 キーボード
   [Keyboard Selection]にて jp106 を選択

3. ディスクパーティション関連
   特にパーティション分割は行わず、内蔵 HDD の全領域を LVM(デフォルト)で使用

4. NIC 設定
   Static 設定 IPv4 10.20.123.6/16
   デフォルトゲートウエイは 10.20.0.1
   DNS 1 は 10.20.250.1
   DNS 2 は 10.20.0.1
   ホスト名は h006.t123.la.net　　(h<第 4 オクテット 3 桁>. t<第 3 オクテット>. la. net)

5. タイムゾーン
   システムクロックは UTC を使わず、ローカル時刻(日本)を用いる。

6. パッケージ選定
   以下のパッケージ**のみ**選択。これ以外は選択しない。
   - Administration Tools
   - Base
   - DNS Server
   - Development Libraries (MTOS 導入用、オプション)
   - Editors
   - GNOME Desktop Environment (オプション)
   - Graphical Internet (Firefox、動作確認を自サーバで行わない場合は不要)
   - MySQL(MTOS オプション)
   - Web Server
   - X Software Development (MTOS オプション)
   - X Window System(オプション)

7. インストール後処理(Setup Agent)
   Firewall configuration にて、Security Level および SELinux を無効(Disable)

8. 一般ユーザ追加
   student を追加
   # useradd student
   # passwd student
   (パスワード 2 回入力)

9. OS バージョンアップ
   # yum –y update
   により全パッケージを最新にする。
   $ cat /etc/redhat-release
   CentOS release 5.7 (Final)
   である事を確認する。

凡その作業時間 30 分

SSH 設定手順

1. /etc/ssh/sshd_conf を修正(以下修正箇所のみ抜粋)し、再起動。

```
# ycos change 2012/01/04
PermitRootLogin no
# ycos change 2012/01/04
PasswordAuthentication no
```

＊外部からのアクセスを許容する場合は、設定変更前に公開鍵を配布しておくこと。

2. 動作確認
一般ユーザでキーペアを作成し、authorized_keys を作成しパーミッションを調整。

```
$ cd .ssh
$ cat id_dsa.pub >> authorized_keys
$ chmod 600 authorized_keys
```

パスワードによるログイン不能を確認。

```
 $ ssh student@localhost
 Enter passphrase for key '/home/student/.ssh/id_dsa': ←パスフレーズ入力（有効）
 Last login: Wed Jan  4 10:28:20 2012

$ ssh student@localhost
Enter passphrase for key '/home/student/.ssh/id_dsa': ←パスフレーズ入力（無効）
Permission denied (publickey,gssapi-with-mic).     ←パスワード認証なし
```

3. root によるログイン不能を確認。

```
$ ssh root@localhost
```

凡その作業時間 20 分

ネームサーバ設定手順

1. bind-chroot の削除

```
#  rpm -e  bind-chroot
```

2. /etc/named.conf の作成(巻末資料参照)

```
#  named-checkconfig /etc/name.conf
```

にて文法エラーをチェック

3. localhost の正引き、逆引きゾーンファイルの作成
サンプルをコピー

```
# cd /var/named
# cp /usr/share/doc/bind-9.3.6/sample/var/named/localhost.zone   .
# cp /usr/shaKshar/doKare/doc/bind-9.3.6/sample/var/named/named.local   .
```

4. ルートキャッシュの作成
dig によりルートネームサーバに問い合わせ、最新の情報を得る。

```
# dig . @192.58.128.30 > named.root
```

5. ゾーンファイルの作成(巻末資料参照)
t123006.la.net ゾーンのファイル名は t123006.zone
yakoshi.la.net ゾーンのファイル名は yakozhi.zone
10.20.123.逆引きゾーンのファイル名は 123.zone
la.net のゾーンファイル名は slaves/la.zone とした
なお、t123006.zone は絶対表記、yakoshi.zone は省略表記(@を用いたパターン)とした。

6. 動作確認
以下の手順にて問題ない事を確認
dig/nslookup にて h006.t123006.la.net が問題なく引けること(回答サーバは localhost)

```
    $ dig h006.t123006.la.net  @localhost
```

上記同様に主要サーバ、他ゾーンも確認
www.yakoshi.la.net については、ラウンドロビンを確認

10.20.123.xx の逆引きができること。

```
$ dig -x 10.20.123.200
```

NS, MX レコードの確認、上位ドメインの確認（抜き打ちテスト可）
スレーブファイルを削除し、DNS 再起動でゾーン転送が行われている事を確認。

7. /etc/resolv.conf の切り替え
先頭に自信の IP アドレス（10.20.123.6）を指定、省略時のドメインは t123006.la.net とした。

凡その作業時間 40 分、スレーブサーバ、逆引き等拡張部分で 40 分

Web サーバ設定（１）基本部分

1. ドキュメントルートは標準設定ではシステムログ等と共有となりセキュリティ上好ましくない。よって、今回は/www 以下に配置することとした。
httpd.conf 当該変更箇所

```
# ycos change 2012/01/04
#DocumentRoot "/var/www/html"
DocumentRoot "/www"
```

2. 基本的な情報を修正
（Not found などのエラー発生時に表示されるメッセージに影響する）

```
#ServerAdmin root@localhost
# ycos change 2011/01/08
ServerAdmin webmaster@t123006.la.net

#ServerName www.example.com:80
# ycos change 2011/01/04
ServerName www.t123006.la.net
```

3. Basic 認証定義を追加

```
# ycos add 2012/01/04
<Directory "/www/staff">
        AuthType Basic
        AuthName "Staff only"
        AuthUserFile "/www/staff/.htpasswd"
        Require user staff
</Directory>
```

4. AuthUserFIle の作成
ユーザは staff のみ作成

```
# htpasswd /www/staff/.htpasswd  staff
New password:
Re-type new password:
Updating password for user staff
# cat /www/staff/.htpasswd
staff:rL2P8wJOqrJVQ
```

http://www.t123006.la.net/staff にアクセスし BASIC 認証が有効であることを確認。

5. CGI 設定（1） ScriptAlias 設定

```
#ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
# ycos change 2012/01/04
ScriptAlias /cgi-bin/ "/www/cgi-bin/"
```

date.cgi(巻末参照) を作成し、正常に動作する事を確認。
http://www.t123006.la.net/cgi-bin/date.cgi

6. CGI 設定(2) .cgi ファイル
CGI による実行の有効化(Directory ディレクティブ内)

```
# ycos change 2012/01/04
#   Options Indexes FollowSymLinks
Options Indexes FollowSymLinks +ExecCGI
```

.cgi ファイルの読み替え

```
# ycos change 2012/01/04  .cgi enable
AddHandler cgi-script .cgi
```

test.cgi（巻末参照）により動作を確認。
http://www.t123006.la.net/test.cgi

凡その作業時間 40 分

Web サーバ設定（２）ホストベースによる仮想ホスト

1. h006 と www.t123006.la.net によるホストベースの仮想ホストを定義。
予め DNS のゾーン情報として以下を定義しておく。

```
h006.t123006.la.net     IN      A       10.20.123.6
www.t123006.la.net      CNAME           h006.s123006.la.net
```

2. VirtualHost 定義を追加。

```
# ycos add 2011/01/04 +++
<VirtualHost *:80>
    Servername www.t123006.la.net
    DocumentRoot /www/www
</VirtualHost>
<VirtualHost *:80>
    Servername h006.t123006.la.net
    DocumentRoot /www/h006
</VirtualHost>
# ycos add 2011/01/04 ---
```

3. 各ドキュメントルートディレクトリを作成し index.html を作成。
（下記の例では 2 つを同時に操作）

```
# mkdir /www/www  /www/h006
# vi  /www/www/index.html  /www/h006/index.html
```

(index.html はディレクトリ名が分かるよう工夫)

4. 動作確認
http://www.t123006.la.net/と http://h006.t123006.la.net/で表示内容が異なる事を確認。

凡その作業時間 20 分

Web サーバ設定（３）IP ベースによる仮想ホスト

1. 予め www.yakoshi.la.net として、10.20.125.1～3 を DNS でラウンドロビン定義。

```
www         IN      A       10.20.125.1
www         IN      A       10.20.125.2
www         IN      A       10.20.125.3
```

2. 上記状態でラウンドロビン動作を確認。

```
$ nslookup www.yakoshi.la.net
Server:         10.20.123.6
Address:        10.20.123.6#53

Name:   www.yakoshi.la.net

Address: 10.20.125.3
Name:   www.yakoshi.la.net
```

```
Address: 10.20.125.1
Name:   www.yakoshi.la.net
Address: 10.20.125.2

$ nslookup www.yakoshi.la.net
Server:         10.20.123.6
Address:        10.20.123.6#53

Name:   www.yakoshi.la.net
Address: 10.20.125.2                ←表示順がかわっている（ラウンドロビン）
Name:   www.yakoshi.la.net
Address: 10.20.125.3
Name:   www.yakoshi.la.net
Address: 10.20.125.1
```

3. 10.20.125.1～3をそれぞれ、/etc/sysconfig/network-scripts/ifcfg-eth0:1～3としてエイリアスを作成。（以下は代表して ifcfg-eth0:1、10.20.125.1 の定義内容）

```
DEVICE=eth0:1
BOOTPROTO=static
BROADCAST=10.20.255.255
IPADDR=10.20.125.1
NETMASK=255.255.0.0
NETWORK=10.20.0.0
ONBOOT=yes
```

4. IP ベース仮想ホスト定義の追加

```
<VirtualHost 10.20.125.1:80>
    Servername h006.t123006.la.net
    DocumentRoot /www/web1
</VirtualHost>
<VirtualHost 10.20.125.2:80>
    Servername h006.t123006.la.net
    DocumentRoot /www/web2
</VirtualHost>
<VirtualHost 10.20.125.3:80>
    Servername h006.t123006.la.net
    DocumentRoot /www/web3
</VirtualHost>
```

5. ディレクトリおよび index.html の作成（ホストベース参照、割愛）
6. 動作確認
   http://www.yakoshi.la.net でアクセスし、毎回表示内容が異なる事を確認。

凡その作業時間 40 分

メールサーバ

1. Postfix を使うため、/etc/postfix/main.cf を修正する。基本部分は以下の通り。

```
# ycos add 2012/01/04
myhostname = h006.t123006.la.net
# ycos add 2012/01/04
mydomain = t123006.la.net
# ycos change 2012/01/04 - select 'all'
inet_interfaces = all
# ycos add 2012/01/04
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
```

2. 課題の From 欄については、origin を修正。

```
# ycos add 2012/01/04
myorigin = $mydomain
```

3. リレー禁止は以下の要領。

```
# ycos add 2012/01/04
mynetworks = 10.20.123.0/28, 127.0.0.0/8
```

4. 修正後、postconf –n にて非デフォルト値を確認。

 # postconf –n

5. 動作確認(1)From 欄の設定

```
 $ date | mail student
 $ mail
Mail version 8.1 6/6/93.  Type ? for help.
"/var/spool/mail/student": 2 messages 1 new 2 unread
 U  1 logwatch@t123006.la.  Sun Jan  8 10:27  42/1409  "Logwatch for h006.
>N  2 student@t123006.la.n  Sun Jan  8 13:51  13/473
& 2
Message 2:
From student@t123006.la.net  Sun Jan  8 13:51:33 2012
X-Original-To: student
Delivered-To: student@t123006.la.net
To: student@t123006.la.net
Date: Sun,  8 Jan 2012 13:51:33 +0900 (JST)
From: student@t123006.la.net                ← From のドメイン部が設定されている。

2012 年  1 月  8 日 日曜日 13:51:33 JST

&q
```

動作確認(2)リレー禁止
(異なるセグメントのマシンから)

```
$ telnet 10.20.123.6 25
Trying 10.20.123.6...
Connected to 10.20.123.6 (10.20.123.6).
Escape character is '^]'.
220 h006.t123006.la.net ESMTP Postfix
ehlo test
250-h006.t123006.la.net
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from:student@la.net
250 2.1.0 Ok
rcpt to:ycos001@yahoo.co.jp
554 5.7.1 <ycos001@yahoo.co.jp>: Relay access denied
```

6. 転送設定は /etc/aliases を修正し、newaliases(8)を実行する。
当該個所(/etc/aliases)

```
    # ycos add 2011/01/04
    root:          student
```

7. エイリアス動作確認

```
    $ date | mail postmaster
    $ date | mail webmaster (課題にないが、Web 設定と整合させるため)
```

上記2つの送信結果がユーザ student で確認した。

8. 受信サーバ設定は/etc/dovecot.conf を修正する。

```
# ycos add 2012/01/04
protocols = pop3
```

9. 動作確認および MUA のインストール。今回は時間省略のため RPM の Thunderbird を使用。
   # yum –y install thunderbird
   Thunderbird による送受信を確認（但し LA の外からのメールは受信できない）

凡その作業時間 40 分

Blog ツールの導入

1. 導入先の決定
   今回は Apache の DocumentRoot を変更しているため、以下のディレクトリへ変更

アプリケーション格納用	/www/cgi-bin/MT
スタティック配置用	/www/www/mt-static
ブログ書込み用	/www/www/MT
データベース格納用	/www/mysql/MT

2. MySQL の導入（詳細はテキスト参照のこと）
   /etc/my.cnf のデータ格納先を変更

```
datadir=/www/mysql/MT
```

   環境の整備

```
# mkdir  /www/mysql/MT
# mysql_install_db  -user=dbadm
# /etc/init.d/mysqld start
# mysqladmin –root password 'himitu'
# mysqladmin  -u  root  create  MT
Enter password:      （パスワード入力）
# mysqlshow –p
Enter password:      （パスワード入力）
    （ MT データベースの存在を確認）
# mysql –u root –p
Enter password:      （パスワード入力）
mysql> gran all privileges on MT.* to dbadm@localhost identified by 'himitu';
mysql>quit
```

3. キットの入手。MTOS の個人ライセンス版をダウンロードし展開。
   http://www.sixapart.jp/movabletype/personal.html
   (ユーザ登録が義務付けられているため、適当なメールアドレスを用意)
   2012 年 1 月 4 日現在、MT-5_12-ja.zip が最新版。

```
# cd /www/cgi-bin
# unzip ~student/Desktop/MT-5_12-ja.zip      （ダウンロード先のファイルを指定）
Archive:  Desktop/MT-5_12-ja.zip
   creating: MT-5.12-ja/
   creating: MT-5.12-ja/tools/
  inflating: MT-5.12-ja/tools/rebuild-benchmark
             （後略）
# mv MT-5.12-ja/  MT
# mv MT/mt-static  /www/www/
# mkdir /www/ww/MT
# chown –R apache:apache  /www/
# chmod –R 775 /www/cgi-bin/MT  /www/www/mt-static  /www/www/MT
```

4. MTOS の管理画面を表示し、不足するモジュールを追加してゆく。
   http://www.t123006.la.net/cgi-bin/MT.mt-check.cgi
   *注：mt-config.cgi があると、チェックをしなくなるため、先に確認すること。

5. 不足モジュールの追加
   必須 Perl モジュールは以下で、それ以外はオプション。余力によって追加する。
   CGI::Cookie、File::Spec、Image::Size、DBI、DBD::mysql (DBMS の中から選択)

ImageMagick の最新版は以下の手順にてインストール

```
# yum install  ImageMagick  ImageMagick-perl  ImageMagick-devel
```

他に Perl モジュールをインストールする際に必要となる Linux のパッケージは yum でインストール。

GD　<　gd, gd-devel
XML::Parser　<　expat-devel,　libxml2-devel

6. MTOS 設定ファイルの修正 mt-config.cgi-original をコピーし mt-config.cgi を作成後それを修正。

```
# cp /www/cgi-bin/MT/mt-config.cgi-original   /www/cgi-bin/MT/mt-config.cgi
```

mt-config.cgi を修正

```
# ycos change 2012/01/04
Database MT
DBUser dbadm
DBPassword himitu
DBHost localhost
```

7. 動作確認
http://www.t123006.la.net/cgi-bin/MT/mt.cgi にアクセスしブログを作成する。
また、再度ログイン時に「パスワード忘れ」を実施し再設定 URL のメールが届く事を確認。

作業時間凡そ 1 時間 30 分
（オプションモジュール取り込みを含め 2 時間強）

セキュリティ

1. パケットフィルターは以下の設定とした。sport については自分自身で確認するためのクライアント設定であるため、本来は不要。

```
# Policy
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
# common rule
iptables -A INPUT -d localhost -j ACCEPT
iptables -A INPUT -p icmp -d 10.20.123.6 -j ACCEPT
iptables -A INPUT -p icmp -d 10.20.125.1 -j ACCEPT
iptables -A INPUT -p icmp -d 10.20.125.2 -j ACCEPT
iptables -A INPUT -p icmp -d 10.20.125.3 -j ACCEPT
# Server side
iptables -A INPUT -p tcp -d 10.20.123.6 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.125.1 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.125.2 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.125.3 --dport 80 -j ACCEPT
iptables -A INPUT -p udp -d 10.20.123.6 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.123.6 --dport 25 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.123.6 --dport 110 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.123.6 --dport 22 -j ACCEPT
# Client side
iptables -A INPUT -p tcp -d 10.20.123.6 --sport 80 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.125.1 --sport 80 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.125.2 --sport 80 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.125.3 --sport 80 -j ACCEPT
iptables -A INPUT -p udp -d 10.20.123.6 --sport 53 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.123.6 --sport 25 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.123.6 --sport 110 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.123.6 --sport 22 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.123.6 --sport 53 -j ACCEPT
iptables -A INPUT -p tcp -d 10.20.123.6 --sport 443 -j ACCEPT
```

* ログについては大量に出力されるため、今回は使わず。

2. 動作確認
Web、メール、SSH 等の接続確認。またサーバとクライアント側で構成が異なるゾーン転送が正しく動作するか確認。

```
# rm /var/named/slaves/la.zone
# /etc/init.d/named restart
# ls -l /var/named/slaves
```

(再起動時にゾーン転送が行われ la.zone が生成されていること)

また、クライアント側の設定の大部分は本来サーバ専用とする場合は不要。
・各サービスの動作確認用(http、named/UDP、SMTP、POP)
・ゾーン転送用(named/TCP)は、必須
・情報検索用(https)は、Web でログインを伴う場合に必要。

3. chkconfig により、不要と思われるサービスは停止。主な不要サービスは以下の通り。
「HW 構成にない」は PC に搭載されていないハードウエアの機能、「構成にない」は課題として提示されていないサービスかつ停止しても問題のないもの。

サービス名	用途・理由
avahi-daemon,avahi-dnsconfd	LAN 上のサービス検索(構成にない)
bluetooth, dund, hidd	BT 用デーモン(HW 構成にない)
cups	プリンタースプーラ(HW 構成にない)
ip6tables	IPv6 用パケットフィルタ(構成にない。IPv4 のみ)
apmd	無停電電源用デーモン(HW 構成にない)
autofs	NFS 自動マウント(構成にない)
ibmsam	IBM 提供のシステム管理ツール(構成にない)
netfs	Windows ファイル共有(構成にない)
nfs, nfslock, portmap, rpcgssd, rpcidmapd	NFS 用デーモン(構成にない)
pcscd	PC カードデーモン(HW 構成にない)
rawdevices	Oracle DB 用(構成にない)
irda	赤外線通信(HW 構成にない)
mcstrans, setrobuleshoot	SELinux 用(構成にない)
mdmonitor, mdmpd, multipathd	RAID 制御用(HW 構成にない)
xfs	X フォントサーバ(構成にない)

chkconfig –level 0123456 サービス名 off で停止。また必要なサービスは 345 で on。

4. セキュリティ強化(例)バナーの削除。
各サーバに対し TELNET 等で直接アクセスした際に、バージョンや OS といった詳細情報が表示されるため、それを無効化する。

① コンソールのディストリビューション詳細表示
/etc/issue, /etc/issue.net の表示内容からバージョン、ディストリビューションに関わる記述を削除。

② DNS のバージョン表示
以下のコマンドにより詳細な BIND のバージョンが表示されるため、それを修正。

```
$ dig @localhost chaos txt version.bind    (バージョンの確認)
```

/etc/named.conf を以下のように修正。

```
options {
        directory "/var/named";
        version  "bind9";
};
```

③ Web サーバの接続時のメッセージと、Not Found 時のコメント。
/etc/httpd/conf/httpd.conf を修正

```
ServerTokens  Prod       (デフォルトは OS)
ServerSignature Email    (デフォルトは On)
```

④ メールサーバ接続時のバージョン
/etc/postfix/main.cf を修正

```
smtpd_banner = stmp.t123006.la.net ESMTP smtp-server
```

作業時間凡そ 40 分（iptables 部分）

ドキュメンテーション

作業手順書および考察は必須、箇条書きでよい。
作業時間凡そ 3 時間

補足

作業にかかった時間を記録しておくと、次回同様の作業を行う際の見積もり根拠となる。またその時のノウハウを形として蓄積しておく事も大事。
ノウハウとしては、

- 設定ファイル群
  作成・修正したファイルはネット上のファイルサーバやメールサーバに保存しておくと、次回流用できる。
- 手順書
  自分で分かるように設定した内容を記録しておく。2 回目以降はそれを見ながら行えば間違いが少なく、作業時間も短縮できる。
- ルール化
  手順の中で間違いやすい点を抜き出し、後でチェックできるようチェックリストを作る。コメントの書き方を決める、確認方法を決めるといった品質を担保する仕組みを考え文書化する。
- ツール
  良く使うコマンドのエイリアス、シェルスクリプトの作成をしておくと、さらに効率があがる。

想定される作業時間は以下の通り、

(単位分)	Day 1	Day 2	Day3
OS インストール	60	30	30
SSH 設定	40	20	20
DNS 設定（基本）	80	40	40
DNS 拡張	N/A	40	
Web 基本	80	40	60
Web 拡張	N/A	40～80	
Mail	40	20	20
Blog	N/A	N/A	160
セキュリティ	80	40	20
（自由研究）	N/A	N/A	140
合計	380	310	490

この値は、自分が設定したゴール（Day1～3）を振り返り、自習にて再挑戦する際の目安として活用するとよい。
なお同じ項目を実施する場合には、前回のノウハウ（成果物の活用、設定ファイルを流用するなど）を生かす事で半分の時間になるような想定となっている。
例） SSH のインストールは初回（Day 1）では、60 分だが 2 回目以降は 30 分に短縮されている。

考察

ワーニングのない設定

ログファイルに多くのワーニングが出力されている事に気付かなかった。完全に削除は時間の関係で出来なかったが、細かい設定やマニュアルにない事が多いと感じた。

DNS(/var/log/messages):

・the working directory is not writable

→ # **chmod g+w /var/named**

なおゾーン転送のファイルの格納場所は /var/named/slaves にする事でエラーを回避

Web(/var/log/httpd/error_log):

・File does not exist: /www/web1/favicon.ico

→ 各仮想ホストの DocumentRoot に/var/www/manual/images/favicon.ico をリンク

バナーの影響

システムのセキュリティを向上させるためには、不必要なシステムの情報を公開しない事が重要であると考え、インターネット上からサーバのバージョン情報を削除する事例を調査、実装した。

（詳細は本文中に記載）

その他

チェックツール使用の徹底

慣れにより、システム設定確認ツールによる確認を怠り動作不良になる場合が散見された。チェックツールによる確認を徹底したい。

例）

named-checkconfig /etc/named.conf
named-checkzone t123006.la.net /var/named/t123006.zone
apachectl –t
postconf –n

不足モジュール

導入モジュールの削減で、GNOME を導入しなかったところ X で日本語が表示できない事に気づく。後で gnome-term をインストールしたが、それまでは毎回言語設定を LANG=C としていた。root のプロファイルを LANG=C にしておく方が確実かもしれない。

もしくは藪蛇になるので、そもそもデスクトップ環境をインストールすべきだったと考えられる。

またチェックのために、nmap をインストールした。

コメント

修正箇所を後で検証できるよう、すべてコメントを付与した。ただしオリジナルのファイルを xxx.org といった別名で保存するか、変更する度にバージョン管理する方がより確実である。

設定ファイル類

SSH 関連

/etc/ssh/sshd_config（変更箇所のみ抜粋）

```
#       $OpenBSD: sshd_config,v 1.73 2005/12/06 22:38:28 reyk Exp $
        （中略）
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
# ycos change 2012/01/04
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
        （中略）
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
# ycos change 2012/01/04
PasswordAuthentication no
        （中略）
# no default banner path
#Banner /some/path

# override default of no subsystems
Subsystem       sftp    /usr/libexec/openssh/sftp-server
```

DNS 関連

/etc/named.conf（新規作成全文）

```
// Simple named.conf
options {
        directory "/var/named";
        version  "bind9";
};

zone "." IN {
        type hint;
        file "named.root";
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "t123006.la.net" IN {
        type master;
        file "t123006.zone";
};

zone "yakoshi.la.net" IN {
        type master;
        file "yakoshi.zone";
};
```

```
zone "123.20.10.in-addr.arpa." IN {
        type master;
        file "123.zone";
};

zone "la.net" IN {
        type slave;
        file "slaves/la.zone";
        masters { 10.20.250.1; };
};
```

/var/named/t123006.zone（新規作成全文）

```
$TTL    1D
t123006.la.net. IN SOA  ns.t123006.la.net. root.t123006.la.net. (
        2012010401 8H 4H 1000H 1D )
        IN      NS      ns.t123006.la.net.
        IN      MX      100     smtp.t123006.la.net.
ns.t123006.la.net.      IN      A       10.20.123.6
smtp.t123006.la.net.    IN      A       10.20.123.6
h006.t123006.la.net.    IN      A       10.20.123.6
www.t123006.la.net.     CNAME   h006.t123006.la.net.
ftp.t123006.la.net.     IN      A       10.20.123.6
```

/var/named/yakoshi.zone（新規作成全文）

```
$TTL    1D
$ORIGIN yakoshi.la.net.
@       IN      SOA     ns      root (
        2012010402 8H 4H 1000H 1D )
        IN      NS      ns
        IN      MX      100     smtp
ns      IN      A       10.20.125.6
smtp    IN      A       10.20.125.6
h006    IN      A       10.20.125.6
ftp     IN      A       10.20.125.6
www     IN      A       10.20.125.1
www     IN      A       10.20.125.2
www     IN      A       10.20.125.3
```

/var/named/123.zone（新規作成全文）

```
$TTL    1D
@       IN      SOA     ns.t123006.la.net. root.t123006.la.net. (
        2012010401 8H 4H 1000H 1D )
        IN      NS      ns.t123006.la.net.
$GENERATE 1-9   $.123.20.10.in-addr.arpa.       IN PTR h00$.t123006.la.net.
$GENERATE 10-99 $.123.20.10.in-addr.arpa.       IN PTR h0$.t123006.la.net.
$GENERATE 100-255       $.123.20.10.in-addr.arpa.       IN PTR h$.t123006.la.net.
```

/etc/resolv.conf（全文）

```
search t123006.la.net
nameserver 10.20.123.6
nameserver 10.20.250.1
nameserver 10.20.0.1
```

Web 関連

/etc/httpd.conf(修正箇所のみ抜粋)

```
#
# This is the main Apache server configuration file.  It contains the
#
        (中略)
```

```
#ServerTokens OS
# ycos change 2011/01/04
ServerTokens Prod
        (中略)
#
#ServerAdmin root@localhost
# ycos change 2011/01/08
ServerAdmin webmaster@t123006.la.net
        (中略)
#ServerName www.example.com:80
# ycos change 2011/01/04
ServerName www.t123006.la.net
        (中略)
# ycos change 2012/01/04
#DocumentRoot "/var/www/html"
DocumentRoot "/www"
        (中略)
# This should be changed to whatever you set DocumentRoot to.
#
# ycos change 2012/01/04  /var/www/html --> /www
<Directory "/www">
        (中略)
# ycos change 2012/01/04
#    Options Indexes FollowSymLinks
    Options Indexes FollowSymLinks +ExecCGI
        (中略)
#
# Controls who can get stuff from this server.
#
    Order allow,deny
    Allow from all
</Directory>
# ycos add 2012/01/04
<Directory "/www/staff">
        AuthType Basic
        AuthName "Staff only"
        AuthUserFile "/www/staff/.htpasswd"
        Require user staff
</Directory>
        (中略)
#ServerSignature On
# ycos change 2012/01/04
ServerSignature Email
        (中略)
#ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
# ycos change 2012/01/04
ScriptAlias /cgi-bin/ "/www/cgi-bin/"
        (中略)
# ycos change 2012/01/04  .cgi enable
AddHandler cgi-script .cgi
        (中略)
#    CustomLog logs/dummy-host.example.com-access_log common
#</VirtualHost>
# ycos add 2011/01/04 +++
<VirtualHost *:80>
        Servername www.t123006.la.net
        DocumentRoot /www/www
</VirtualHost>
<VirtualHost *:80>
        Servername h006.t123006.la.net
        DocumentRoot /www/h006
</VirtualHost>
<VirtualHost 10.20.125.1:80>
        Servername h006.t123006.la.net
        DocumentRoot /www/web1
```

```
</VirtualHost>
<VirtualHost 10.20.125.2:80>
        Servername h006.t123006.la.net
        DocumentRoot /www/web2
</VirtualHost>
<VirtualHost 10.20.125.3:80>
        Servername h006.t123006.la.net
        DocumentRoot /www/web3
</VirtualHost>
# ycos add 2011/01/04 ---
```

/www/cgi-bin/date.cgi（新規作成全文）

```
#! /bin/bash
cat <<EOD
Content-type: text/plain

`date`
EOD
```

/www/www/test.cgi（新規作成全文）

```
#! /bin/bash
cat <<EOD
Content-type: text/html

<html>
<head><title>CGI sample</title>
</head>
<body>
<h2>CGI sampel</h2>
Environment valiables list
<table border=1>
<tr><th>Name</th><th>Value</tr>
<tr>
EOD

env | sed -e 's,^,<tr><td>,' -e 's,=,</td><td>,' -e 's,$,</tr>,'

cat <<EOD
</table>
</body>
</html>
EOD
```

/etc/sysconfig/network-scripts/ifcfg-eth0:1（新規作成全文）

```
# Broadcom Corporation NetXtreme BCM5754 Gigabit Ethernet PCI Express
DEVICE=eth0:1
BOOTPROTO=static
BROADCAST=10.20.255.255
IPADDR=10.20.125.1
NETMASK=255.255.0.0
NETWORK=10.20.0.0
ONBOOT=yes
```

/www/web1/index.html（新規作成全文）

```
<html>
<body>
<h1>Welcom WWW(1) site</h1>
</body></html>
```

MTOS 関連

/etc/my.cnf（修正箇所のみ抜粋）

```
[mysqld]
# datadir=/var/lib/mysql
# ycos change 2012/01/04
datadir=/www/mysql/MT
socket=/var/lib/mysql/mysql.sock
user=mysql
        （後略）
```

/www/cgi-bin/mt-config.cgi（修正箇所のみ抜粋）

```
        （中略）
# The CGIPath is the URL to your Movable Type directory
#CGIPath   http://www.example.com/cgi-bin/mt/
# ycos change 2012/01/04
CGIPath   http://www.t123006.la.net/cgi-bin/MT/

# The StaticWebPath is the URL to your mt-static directory
# Note: Check the installation documentation to find out
# whether this is required for your environment.  If it is not,
# simply remove it or comment out the line by prepending a "#".
#StaticWebPath   http://www.example.com/mt-static
# ycos change 2012/01/04
StaticWebPath   http://www.t123006.la.net/mt-static

#================ DATABASE SETTINGS ==================
#   CHANGE setting below that refer to databases
#   you will be using.

##### MYSQL #####
ObjectDriver DBI::mysql
# Database DATABASE_NAME
# DBUser DATABASE_USERNAME
# DBPassword DATABASE_PASSWORD
# ycos change 2012/01/04
Database MT
DBUser dbadm
DBPassword himitu
DBHost localhost

DefaultLanguage ja
```