Jail環境を使った仮想サーバ構築の自動化

2000MT025 稲葉 好美　　2000MT080 大矢 博子
指導教員　石崎 文雄

1　はじめに

インターネットの普及に伴い、サーバ構築、管理のコストおよびサーバ管理に対するセキュリティの問題が重要になっている。日本でもPCの浸透、マルチメディアの本格化などネットワーク･コンピューティングにおいての発展が多くの利用者を獲得することができました。またこれによってインターネットの普及には拍車がかかり、関連サービスを提供する事業者やプロバイダのさらなる急増を招いたことはよく知られている。そのような結果、サービスを提供する側は、どのような場合でも外からの攻撃にさらされるため、LAN内部向けのサーバよりも高いレベルのセキュリティが要求されている。またサービスを運用する際には安定した、セキュリティホールの発見されていないバージョンのソフトウェアを使用しなければならない。しかし、しばらく使っているうちに新たなセキュリティホールが見付かったり、不用意に実行したコマンドや不用意なCGIなどがセキュリティホールにつながる恐れがあるのが現実です。そこで注目するのが、1つのサービスを複数のコンピュータに分散処理してスループットの性能を向上を追求するブレードサーバを使用する方法がある。そして、1台の高性能サーバに複数の役割を集約させるのが仮想サーバの技術である。

本研究では、サーバ構築、管理のコスト削減とサーバのセキュリティの強化のために、仮想化技術の一つであるjailを利用した仮想サーバを取り上げ、考察を行う。仮想サーバには、Web、電子メール等の各種サーバをインストールし、汎用的に使えるサーバを構築する。そして、その構築過程を可能な限り自動化するためのシェルスクリプトの作成を行う。多数の汎用的な同質なサーバを構築する場合、サーバ構築過程の自動化は、構築過程の時間を大幅に短縮でき、人手による構築によって生ずると思われる設定段階における不具合を排除できるものと思われる。

2　仮想サーバ [3]

仮想サーバとはインストール済みの単一のサーバで、複数の企業または個人のドメイン名、IPアドレスおよびいくつかのサーバ監視機能を提供することが可能になる。これによりユーザはあたかも独自のWebサーバを持っているかのように操作できるが、実際には管理者がハードウェアを提供し仮想サーバを管理している。

仮想サーバを使う利点として、インターネットでのWebサービスなどを公開している場合に、データの改ざんやシステムの破壊に遭った場合その被害を仮想環境内に留めておける可能性が高い。また性能が劣る複数のコンピュータがいらなくなり、そのサーバに使用していた場所を新たに使用でき電気代節約、台数も少なくなる。またどのサーバにも十分に使われていない余分の容量があり、これまで見過ごされてきた容量を使うことができるようになる。

仮想サーバは下記の4つである。

- バーチャルホスティング
- jail
- 仮想OS
- 仮想マシン

4つの仮想サーバについて次節で説明する。

2.1　バーチャルホスティング

バーチャルホスティングとは、仮想ホスト・仮想ホスティングとも呼ばれ1台のサーバの中に複数のドメイン名を共有する方法である。複数のドメインを認識できる機能を持ったサーバソフトと、それを認識できるネットワークプロトコルの組み合わせの場合のみ使用でき、実際にアクセスがあった時点でそのアクセスは、預かっているドメイン名のうちのどれに対してなのかをサーバ側のプログラムで判定して振り分けている。そして専用のDNS・Webサーバを持たずに専用ドメインで仮想的にWebページを公開するもので、あたかも自前の専用サーバから独自ドメインのWebサイトを公開しているように振舞うので、このように呼ばれている。今まで構築してきたDNS・Webサーバ上にバーチャルホストを設定する。新規ドメイン取得のたびに、新たにサーバを設ける必要がなくとても経済的である。

2.2　jail

FreeBSDではchrootを強化したjailという技術がある。jailとは、1台のマシン上でユーザとユーザがお互いの存在を隠す技術のことである。これによって、1台のマシンに複数の役割を持たせることになりセキュリティが向上する。Jail環境の特徴として、1つのIPアドレスを持つネットワーク的に独立したホストとして機能させられるため、1台のマシン上で複数のサーバホストを稼動できる。これを活用すると、単一のホスト環境の安定性を高いレベルで確保しつつ、ホスティングサービスのような運用も可能である。またCGIを安全に利用する場合に優れている。

2.3 仮想 OS

仮想 OS とは OS 上でアプリケーションのように OS が動く技術のことです。例えば仮想 OS には UML(User Mode Linux) がある。仮想 OS の大きな利点として、1 台のマシンを共有しているユーザ間で資源を自由に配分できることが挙げられる。また、ユーザ間でうまくピークを分散させれば、処理能力を超えたユーザを収納することも可能となる。

2.4 仮想マシン

仮想マシンとは、コンピュータにインストールされている元の OS 上で、別の複数の OS を実行できるようにするものである。特徴としては、仮想 PC 環境を構築するので実行できる OS を限定しない。またハードウェアの配置、ソフトウェアのインストール、システムのリブートや再構成の時間を短縮することができる。使用利点としては、特定の OS としか互換性のないアプリケーションを実行するために使用できたり、複数の OS 上でアプリケーションをテストする場合にも適している。欠点としては処理速度が低下することがある。

3 構築環境

まずホスト環境だけにデータベースと DNS サーバを置き、基盤の環境の設定をする。そして構築段階において、各仮想サーバである jail 環境の設定を追加するだけにしておく。最終的には作成したシェルスクリプトを実行し仮想サーバを構築する。各 jail 環境には Web サーバ (Apache1.3.27) や Mail サーバ (qmail)、FTP サーバ (proftpd) をインストール設定をし起動できるようにする。構築環境を下図に示す。

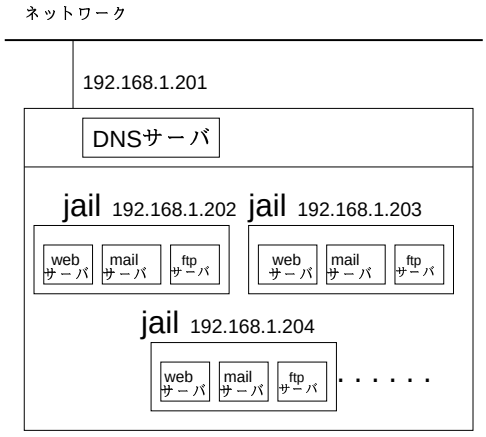

図 1 構築環境

実験環境の PC サーバの仕様を下記に示す。

CPU	インテル (R)Pentium 4(R) プロセッサ 1.8GHz/512KB キャッシュ
メモリー	512MB(1 × 512MB)PC200 DDR SDRAM
ハードディスク	73GB 10000 回転 ULTRA3 SCSI 1 インチ HDD

3.1 DNS サーバ

今回インストールする djbdns サーバとは安全、確実、高速、簡潔、設定も簡単な DNS サーバとツール群である。最近では BIND が有名であるがセキュリティの面を見て djbdns をインストールする。

djbdns サーバは外からの問い合わせを受け付ける tinydns と、キャッシュサーバである dnscache で構成されている。高速性の面からみて djbdns サーバは自分の問い合わせしか答えない。それを反復型の問い合わせと呼び、その結果をメモリにキャッシュして、次回の問い合わせに高速に答える dnscache からできている。また機能を単位のモジュール化と、root 権限実行モジュールを絞り込みするためセキュリティが向上する。

3.2 Web サーバ

また Web サーバに関してはフリーソフトウェアである Apache を使い、SSL(Secure Socket Layer) が使えるようにする。SSL とは簡単に言うとデータを暗号化してやりとりする方法であり個人情報を外部に盗み取られないようにするものである。

3.3 FTP サーバ

インストールするものは ProFTPD を使う。特徴としては、FTP を許可するアカウントを設定でき、アカウントごとにアクセス権限を指定できる。またデータベースへアクセスするためのユーザ名とパスワードが記述されたコンフィグレーションファイルで、アクセス可能なユーザを制限できる。

3.4 Mail

各 jail 環境の中で動くソフトウェアを下記に示す。

1. qmail(mail サーバ)
2. courier-imap
3. ezmlm

1.qmail [4]

MTA(Mail Transfer Agent) では sendmail ではなく qmail を使ってメールサーバを構築する。その理由として、まず第一に比較的セキュアに保ちやすいためである。sendmail は root 権限で動作する単一のプロセスからなる MTA のため、一度 sendmail のプロセスを乗っ取られてしまうと root 権限で好き放題されてしまうというセキュリティホールがよく見付かるということでも有名である。

qmail の場合の利点を下記に示す。

- MTA の機能を権限の異なる複数のプロセスの組み合わせで実現している。
- root 権限は最小限のプロセスのみが持つ。

2.courier-imap [5]

courier-imap をインストールすると IMAP サーバを構築することができる。POP サーバとの最大の違いはメールボックスを共有できるということである。具体的に言えば、ユーザがメールボックスにメールを残したままメールを読むことができ、送信も SMTP ではなく IMAP サーバで行え、送信したメールもメールボックスに残すことも可能である。

IMAP は qmail とは違いインストールするアプリケーションがいくつもあるわけではなく、基本的に courier-imap をインストールするだけで IMAP サーバを構築することができるのでインストールは qmail よりもはるかに楽である。courier-imap は MTA である qmail の maildir 形式のみサポートし、POP3/IMAP に対応しバーチャルドメインが使用可能である。

3.ezmlm(MailingList) [6]

メーリングリスト (MailingList) とは、電子メールを用いたインターネット活用法で、一回で多数の人に同じメールを送信できる仕組みのことである。普通の十、百の単位ぐらいのメーリングリストなら qmail の /etc/aliases ファイルに書き込んだほうが早いが、何千以上もの単位を扱う場合にはメーリングリストを使う方が有効である。今回、私達は qmail に対応した高速かつ設定が簡単な ezmlm を使用する。

ezmlm(MailingList) の活用法を下記に示す。

- 趣味や愛好家同士の情報交換
- ビジネスで部署内の一斉連絡
- 卒業生連絡・ＯＢ間交流や就職情報

3.5 データベース

データベースシステムとは情報データの集積であるデータベース (データバンクあるいはコンテンツと呼ばれる) と、それを管理するデータベース管理システム (DBMS：Database Management System) と呼ばれるソフトウェア、ならびに情報を格納した媒体であるハードウェアから成り立っている。

使用する PostgreSQL はフリーな RDBMS であり、特徴としてクライアントサーバ型、マルチユーザに対応し、日本語にも完全に対応（他言語にも対応）している。

4 実験の目的

実験の目的として、仮想サーバの構築過程で可能な限り自動化できるようにするためにシェルスクリプトを作成した。そして実際にシェルスクリプトを使用することによって、複数の仮想サーバをいかに時間を短縮して構築することができるか、また同質なサーバが構築できるかについて実験を行った。最終的に jail 環境上での仮想サーバを構築できる時間を計り考察する。

5 シェルスクリプトの構成

シェルスクリプトを下記の 6 つについて分けて考える。

1. jail 環境の構築
2. ホスト (実システム) 環境の変更
3. jail 内の設定とコピー
4. jail 環境の起動
5. 各ソフトウェアのインストールと設定
6. データベースと dns の設定

○ jail 環境の構築 [2]

基本的に man jail に従って構築する。今回はディレクトリ名と IP アドレスを一緒にしたために、入力引数が少なくて済むようにしてある。また複数の jail 環境を構築するため make world するのは時間かかる。そこで jail を tar で固めて新たなディレクトリを作り、作成するディレクトリ配下に展開を名前を変更するようにするようにし、最後にデバイスを作成する。また各ソフトウェアをインストールするには FreeBSD の特徴である ports からインストールするが、ports でも同じように tar で固めて jail 環境内で展開をする。

○ ホスト (実システム) 環境の変更

ホストでは jail 環境の IP アドレスの割り当てを /etc/rc.conf に書き設定をする。また jail 環境内で実行するシェルスクリプトは全てホスト環境からコピーを済ませておく。

○ jail 内の設定

ユーザ名やパスワードの設定はシェルスクリプトで自動化できないために手動で設定をする。また jail 環境内でスーパーユーザになるためには仮想サーバ内の/etc/group のファイルにユーザ名を書き込みする。ここで一旦リブートをする。

○ jail 環境の起動

次に jail をマウントしそして仮想サーバ内に入る。jail 環境に入るにはユーザのパスワード入力が必要であり手動で入力する。その後、su でスーパユーザになり各ソフトウェアのインストールを開始するシェルスクリプトを実行する。

○ 各ソフトウェアのインストールと設定

インストールは簡単にできるが各サーバの設定については、ファイルを書き換えるとこがあり、それはシェルスクリプトでは記述することはできないので手動で書き換えをする。
下記の 6 つのソフトウェアをインストールをする。

- Apache1.3.29 の設定

- proftpd の設定
- qmail の設定
- tcpserver の設定
- courier-imap の設定
- ezmlm の設定

○データベースと DNS サーバの設定

最後にホストにあるデータベースと DNS サーバについて、jail 環境の設定をし仮想サーバの構築終了である。

6 実験結果

まず最初に、予め用意する jail と ports についての圧縮時間と展開時間を計った。通常の make world するのに 22 分かかり、make world したものを tar で固めるのに 18 秒、それを展開するのに 13 秒かかった。その後 make distribution に 7 秒かかった。その結果を表 1 にまとめる。

またサーバを作成するための CUP タイムと設定にかかる時間を計った。jail を作成し起動するまでの時間を 5 分 36 秒、またその後 jail 環境内に入り各ソフトウェアをインストールし実行するまでの時間は 45 分 5 秒になった。そして 1 つのサーバを構築するのに 50 分 41 秒かかり、その後 5 つ、10 つとサーバを構築させるのにかかる時間は 4 時間 11 分 20 秒、9 時間 38 分 10 秒になった。その結果を表 2 にまとめる。

表 1

jail を make world する	22m
jail を固める	18s
jail を展開する	13s
distribution	7s

表 2

jail を起動するまで	5m36s
jail を起動しインストール	45m5s
仮想サーバを 1 つ作成するまでの時間	50m41s
仮想サーバを 5 つ作成するまでの時間	4h11m20s
仮想サーバを 10 つ作成するまでの時間	9h38m10s

7 考察

使用した実験環境において、仮想サーバを 1 つ作り上げるのに 50 分 41 秒かかった。これは jail 環境のディレクトリ作成からサーバとしての機能を果たすところまでを示している。しかし表 1 と表 2 の 1 行目から jail を起動させるのには 5 分 36 秒かかっていて、jail 環境を起動しインストールの作業をするのには 45 分 5 秒かかっている。そのため仮想サーバを作成するのに大幅な時間がかかっている部分は、各ソフトウェアのインストールすることに費すことになっていることがわかる。

そのほか、シェルスクリプトで効率化を図ること以上に jail と ports を tar で固めて展開することにした。それは make world を実行するたびに、その都度コンパイルを繰り返していては時間がかかり過ぎてしまうためである。その結果表 1 からわかるように、1 つの jail を作成するのに対して jail を make world する時間から jail を展開するまでの差、21 分 47 秒の時間短縮することができた。

最終的にシェルスクリプトを作成したことによって、当然多くのコマンドを手作業で実行することが省けたが、ユーザ作成やパスワード設定については各サーバでそれぞれ設定するようになっている。ドメイン名やパスワード設定は重要なので、ユーザ側がきちんと手動で設定するようになっている。本研究の実験を行うことにあたっては、ディレクトリと IP アドレスを同じにし複雑さを回避した。その他、シェルスクリプト中に条件分岐がないことも時間の短縮に繋がっている。

8 おわりに

本研究ではサーバ構築、管理のコスト削減とサーバのセキュリティの強化のために、仮想化技術の一つである jail を利用した仮想サーバを取り上げた。その構築過程を可能な限り自動化するためのシェルスクリプトを作成し、結果的に手動設定より構築過程の時間を大幅に短縮できた。また、正確性に関してもシェルスクリプトを使用したのでどの仮想サーバも同質であり、手動で設定するより不具合がなく安定した構築ができた。

本研究で開発したシェルスクリプトでは種々の設定ファイルの書き換えには対応しておらず、今後この作業については他の言語でプログラムを書く必要がある。この点では、さらなる自動化が課題となるであろう。また他の課題としては、jail 環境上の仮想サーバの性能評価を行うことが必要である。例えば Mail を多量に送ったり、ファイルの転送を行ったりした場合の処理時間の評価を行うことが考えられる。

参考文献

[1] 衛藤敏寿ほか : FreeBSD 徹底入門 [改訂版]
株式会社翔泳社 (2002)

[2] 小坂浩史：FreeBSD Expert,
評論技術社出版 (2002)

[3] アットマークアイティ,
サーバの仮想化技術とビジネス展開の可能性
http://www.atmarkit.co.jp/flinux/special/vserver/vserver01.html

[4] The qmail home page
http://www.qmail.org/top.html

[5] Courier-IMAP
http://www.inter7.com/courierimap/INSTALL.html

[6] ezmlm
http://cr.yp.to/ezmlm.html