

VM サービスを利用したサーバの設定

企画情報技術グループ 坂 靖範

1. はじめに

グローバル COE プロジェクトとして ARS GCOE が平成 21 年度から動き出した。このプロジェクトの運営・広報等に利用するサーバとして、独自にサーバを構築するのではなく、下記 VM サービスを利用したサーバを利用した環境整備が行われた。

以下にそこで構築・設定した内容を示す。

2. 使用したサーバ

今回、ARS GCOE のサーバは、京都大学学術情報メディアセンター(学術情報基盤グループ)の VM ホスティングサービスを利用して構築された。同ホスティングサービスは、メディアセンターで占有可能なバーチャルマシンを構築し、それをユーザである教職員に提供するサービスであり、一般的なサーバ運用と変わらない操作性がある(図 1 及び図 2)。

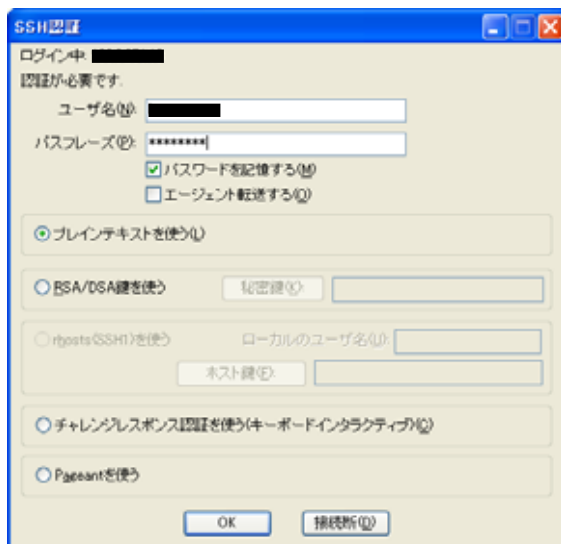


図1 vmサーバへの log in ウィンド
Tera Term を用いた一般的な log in

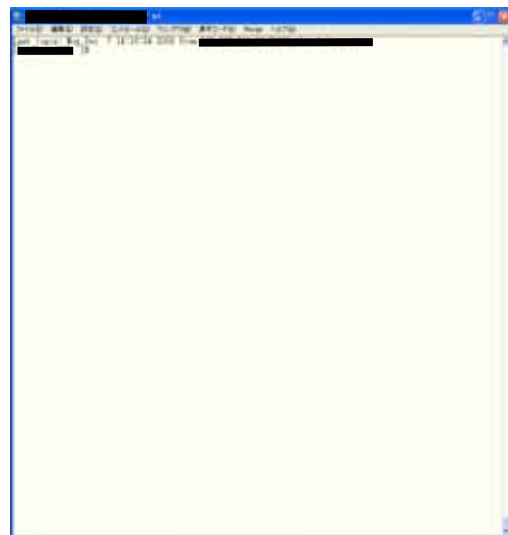


図2 log in された状態。
一般的なサーバの操作と同じ作業環境

提供されるバーチャルマシンは、VMWare を用いたものではなく、Xen を利用したものであり、

- 専用のバーチャルマシン上で Red Hat Enterprise Linux5 によるサーバ環境を提供される。
- 独自ドメイン名でサーバ環境を運用
- Web サーバ・メールサーバ（メールスプール有り）を利用可能
- 200GB のディスク容量
- 仮装ホスト利用可能

ツールとして yum が提供されているため、後述するモジュールの追加やソフトウェアの追加が非常に簡便となる。また、su-で root となり作業を行うのではなく、必要なコマンドを sudo で実行するシステムとなっている（図-4 参照）。

sudo とは、一般ユーザが特権ユーザの権限でコマンドを実行するためのコマンドである。本コマンドは、各コマンド実行を記録でき、スーパーユーザーとしてのログインの完全な代替として利用されている。これを用いることにより、限定されたメンバーのみが管理者権限でコマンドを実行することが可能となり、よりセキュアな管理が可能となる。

5. 設定方法

5.1 http

http サービスについては、GCOE にわたされた段階で既に使用可能となっていた。また、言語としては PHP・Perl・Python・Ruby が既にインストールされていた。

しかしながら、全てセキュアな方に振られたインストールの仕方だったため、必要に応じて追加でモジュールのインストールが必要となる。今回の例では、以下の CMS 利用のため、PHP の mbstring（日本語処理に必要）と mysqld（PHP と MySql の連携に必要）の追加モジュールをインストールした。

上記モジュールは、バイナリとして提供されていたため、yum コマンド一つでインストールすることができた。無論、同コマンドはシステムの改変を伴うこともあるため、特権ユーザでなければ操作できないが、前述の sudo コマンドを利用して一般ユーザのまま利用できる。

今回の例では、CMS サービスを導入することとなった。CMS とは、Content Management System の略で、Web コンテンツを構成するテキストや画像などのデジタルコンテンツを統合・体系的に管理し、配信などの必要な処理を行うシステムである。これを導入することにより Web サイトの管理負担を減少させ、また知識の少ない担当者であってもページの更新などが容易に行えるというメリットを享受できる。

CMS は、当初 Xoops を利用する予定であったが、使用目的や機能の面から MODx を利用することとなった。

同 CMS の利用に際しては、PHP と MySql の利用が不可欠であり、かつ文字コードの問題（サーバ側が UTF-8 を使用している）から上述のモジュールを PHP に追加した。CMS の設定そのものは外注となったが、前述のモジュールの追加、パーミッションの変更及び MODx のインストール作業はこちらで行った。

5.2 メールサーバ

メールサーバとしての利用は当初予定していなかったため、OS 上で必要なプログラムのインストールは行われておらず、メール送受信に必要なポートも塞がった状態であった。

このため、端末上から必要なプログラムのインストール及びポートの解放という作業が必要になると共に、メディアセンターに依頼して外部に対してポートを開けてもらう必要があった。

プログラムのインストール作業そのものは、前述の yum コマンド一つで実施でき、OS で必要なポートを開ける作業も iptables を用いて開けることができたが、メディアセンターの方は教員からの申請が必要であったため、寶・福岡両先生に申請をしていただき、開けていただいた。メールサーバ構築に必要なポートは、110 番 (POP) と 25 番 (smtp) のふたつである。IMAP の利用も考えたが、本サーバにメールアドレスを登録する先生方は既に防災研・京都大学のメールアドレスをお持ちであるので、あえて IMAP を利用

する必要も無いものと判断した。また、mail aliases を設定し、直接本サーバにアクセスしなくても各人がお持ちのアカウントへメールを転送する事で利用上の不都合が解消でき、セキュリティ上も有利であるとも判断した。

MTA は、qmail ではなく使い慣れた postfix を利用することとし、セキュリティに関してはサーバに登録されたユーザ以外は pop サーバにアクセスできないものとしてアクセス制限を行った。また前述のように、直接サーバにメールを取りに来る形ではなく、既に持っているメールアカウントにメールを転送する手法をとったため、パスワード等の情報が他に漏れるリスクが軽減されている。

5.3 メーリングリスト

上記メールサーバが稼働した後、メーリングリストに対する要望が教員から出てきたため、mailman を利用したサービスの構築を行った。mailman そのものは、防災研のメーリングリストでも利用されている実績のあるソフトであり、運用に関しても技術的蓄積が期待できるため、メーリングリスト構築に当たって mailman を選択した。

実際の構築に関しては、yum を用いたインストールと端末上での各種設定が比較的容易に実施でき、極短時間の作業で構築が完了した。

上述のように、渡されてすぐの状態である程度使用は可能であるが、必要に応じて様々な設定やインストールが必要となった。必要な追加ソフトのほとんどがバイナリ供給されていたため、上記設定に関してはソースからコンパイルしなければならない様な事はなかった。今後の要求内容によっては、ソースを入手しコンパイルしなければならないと言ったことも十分予想される。

その様な場合でも、極力 srpm ファイルからのリビルド等により rpm ファイルの作成を行い、rpm を用いたパッケージ管理の徹底を行いたいと考えている。

6. おわりに

今回の業務では、サーバの構築を1から実施したわけではなく、利用可能な状態にまでセッティングされた仮想サーバのセッティングを行った。このため、機器の相性やインストール作業等の初期作業の手間を大幅に減らすことができた。また、メディアセンターのサポートも仰げたため、非常に簡便に必要な機能のインストール・設定ができた。

現物のサーバが手元に無く、物理的にハードウェアの増設が難しい場合もあるが、導入・運用コストを含めた TCO の縮減や上述のメリットを考慮すると、今回のような使用目的であれば十分コストエフェクティブなサーバであると言える。

以上

参考 URL

<http://www.iimc.kyoto-u.ac.jp/services/whs/>

<http://fedorasrv.com/>

<http://gabacho-net.jp/tech-note/aliases.html>

http://www14.plala.or.jp/campus-note/vine_linux/server_ssh/sshd_config.html