# OzLabs.org:
## Administering a system for “smart people”

Martin Schwenke
<martin@meltin.net>

Stephen Rothwell
<sfr@canb.auug.org.au>

# What have we got?

- Debian testing
- Hosts about 100 domains
- Most of domains are used for web server virtual hosts using Apache and email using Postfix
- Also runs git, rsyncd, MySQL, PostgreSQL and all of the other usual services

# So what's the big deal?

- No real big deal...  :-)
- Users are free software hackers
- All of our users are power users
- Nearly all can get a root shell
- Administration via interactive shell

- Goal: Minimise the potential damage...  ;-)

# Principles

- Invent as little as possible
- /etc/ is well known – mimic it in ~/etc/
- Use include files or symlinks
- Offer restricted sudo when useful
- Allow unrestricted sudo too...

# Example: ~martins/etc/

```
martins@bilbo:~$ tree -F -L 1 etc/
etc/
├── apache2/
├── bind/
├── cron.daily/
├── cron.hourly/
├── cron.monthly/
├── cron.weekly/
├── crontab
├── dovecot/
├── drupal/
├── mysql/
├── postfix/
├── rsync/
├── spamassassin/
├── wordpress/
└── zenphoto/

14 directories, 1 file
```

# Example: BIND

- Global BIND configuration:

```
martins@bilbo:~$ grep martins /etc/bind/named.conf.local
include "/home/martins/etc/bind/named.conf";
```

- User's BIND configuration:

martins@bilbo:~$ cat ~martins/etc/bind/named.conf
include "/home/martins/etc/bind/update-keys";

```
zone "meltin.net" {
        type master;
        file "/home/martins/etc/bind/db.meltin";
        allow-transfer {
                ...
        };
};
...
```

- martins is in the “bind” group:

```
martins@bilbo:~$ /usr/sbin/rndc reload meltin.net
```

# Example: Postfix (virtuals)

- Global Postfix configuration:

```
martins@bilbo:~$ cat /etc/postfix/main.cf
virtual_alias_maps =
    hash:/home/martins/etc/postfix/virtual
    ...
```

- User's Postfix configuration:

```
martins@bilbo:~$ cat ~martins/etc/postfix/virtual
meltin.net .

martin@meltin.net  martins@bilbo.ozlabs.org
...
```

- No special permissions needed:

```
martins@bilbo:~$ /usr/sbin/postmap ~martins/etc/postfix/virtual
```

# Example: Apache (VirtualHosts)

- Global Apache configuration:

```
martins@bilbo:~$ readlink /etc/apache2/sites-available/martins
/home/martins/etc/apache2/httpd.conf
```

- User's Apache configuration:

```
martins@bilbo:~$ cat ~martins/etc/apache2/httpd.conf
<VirtualHost *:80>
        ServerName      meltin.net
        ServerAlias     www.meltin.net
        ...
</VirtualHost>
...
```

- Reload via passwordless restricted sudo:

```
martins@bilbo:~$ sudo /usr/sbin/apache2ctl graceful
```

  Possibly safer via this?

```
martins@bilbo:~$ sudo /etc/init.d/apache2 reload
```

# Example: Dovecot/Postfix (virtual domains/users)

- Goals:
  - Virtual Dovecot users
  - Mail delivered from Postfix
  - Per virtual user spamassassin configuration
  - Per virtual user sieve configuration

# Example: Dovecot/Postfix (virtual domains/users)

- Global Dovecot configuration:

```
martins@bilbo:~$ cat /etc/dovecot/conf.d/auth-local.conf.ext
passdb {
  args = username_format=%n /etc/dovecot/passdb.d/%d
  driver = passwd-file
}
userdb {
  args = username_format=%n /etc/dovecot/passdb.d/%d
  driver = passwd-file
}

martins@bilbo:~$ readlink /etc/dovecot/passdb.d/meltin.net
/home/martins/etc/dovecot/passdb.d/meltin.net
```

# Example: Dovecot/Postfix (virtual domains/users)

- User's Dovecot configuration:

```
martins@bilbo:~$ awk -F: '$1 == "mel" { OFS=":" ; $2 = "x" ; print $0
}' \
> ~martins/etc/dovecot/passdb.d/meltin.net
mel:x:1004:1004::/home/martins/var/mail/meltin.net/mel::userdb_mail=m
aildir:~/Maildir
```

- Password can be “set” with “`doveadm pw`”
- That's all that's needed for each Dovecot virtual user to be able to read mail.

# Example: Dovecot/Postfix (virtual domains/users)

- Global Postfix/spamassassin configuration:

```
martins@bilbo:~$ cat /etc/postfix/main.cf
dovecot_destination_recipient_limit = 1
virtual_mailbox_domains =
        ...
        meltin.net.virtual
        ...
virtual_transport = dovecot

martins@bilbo:~$ cat /etc/postfix/master.cf
...
dovecot   unix  -       n       n       -       -
  pipe flags=DORhu user=vmail:vmail
  argv=/usr/local/sbin/vmail ${sender} ${recipient} ${user} ${domain}
...

martins@bilbo:~$ sudo grep vmail /etc/sudoers.d/local
vmail  ALL=(ALL) NOPASSWD: /usr/lib/dovecot/dovecot-lda

martins@bilbo:~$ readlink /etc/spamassassin/virtual/meltin.net
/home/martins/var/mail/meltin.net
```

# Example: Dovecot/Postfix (virtual domains/users)

- That vmail script...

```
martins@bilbo:~$ cat /usr/local/sbin/vmail
#!/bin/bash -f
EX_TEMPFAIL=75

# Some error checking elided...  :-)
sender="$1" ; recipient="$2" ; user="$3" ; orig_domain="$4"

domain="${orig_domain%.virtual}"
[ "$domain" = "$orig_domain" ] && {
    echo "Not a valid virtual user" 1>&2 ; exit $EX_TEMPFAIL
}

no_virt="${recipient%.virtual}"
[ "$recipient" = "$no_virt" ] && {
    echo "Not a valid virtual user" 1>&2 ; exit $EX_TEMPFAIL
}

spam_filter ()
{
    local d="/etc/spamassassin/virtual/$domain/$user/.spamassassin"
    if [ -d "$d" -a -w "$d" ] ; then
        spamc -p 10783 -u "$user@$domain"
    else
        cat
    fi
}

spam_filter | exec sudo /usr/lib/dovecot/dovecot-lda -f "$sender" -d "$user@$domain" -a "$no_virt"
```

# Example: Dovecot/Postfix (virtual domains/users)

- User's Postfix virtual user configuration:

```
martins@bilbo:~$ grep  '^mel@meltin.net' ~martins/etc/postfix/virtual
mel@meltin.net          mel@meltin.net.virtual
```

# Other

- Use gitkeeper to keep track of /etc/
- One dynamic DNS zone "`dyn.ozlabs.org`" – users can use CNAMEs to keep things simple

# Conclusions

- We have invented as little as possible
- /etc/postfix/main.cf modified 3 times in 2012 for user-related changes
- /etc/apache2/site-available – 1 new link added for a new user in 2012
- /etc/bind/named.conf.local – modified 1 time in 2012 for user-related changes
- None of our users have ever done anything really stupid... ;-)

# Legal Statement

- This work represents the view of the authors and does not necessarily represent the view of IBM.
- IBM is a registered trademark of International Business Machines Corporation in the United States and/or other countries.
- Linux is a registered trademark of Linus Torvalds.
- Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Other company, product, and service names may be trademarks or service marks of others.