lilo.linux.or.jp を wheezy から jessie にあげた話

Kazuhiro NISHIYAMA

LILO&東海道らぐオフラインミーティング
2016-05-01

lilo.linux.or.jp とは?

主な用途:

- LILO の Web サーバー (apache)
- ML サーバー (mailman)

環境

- さくらの VPS
- Debian GNU/Linux

アップグレード前

- リリースノートを読む
  - https://www.debian.org/releases/jessie/amd64/release-notes/ch-upgrading.ja.html
- その他情報収集

問題点 (1/2)

- apache 2.2 から 2.4 への変更がネック
  - allow や deny の設定方法が変わっている
  - 中間証明書の設定方法が変わった
    - 証明書ファイルに結合して指定するように変わった
    - SSL/TLS を (まだ) 使っていないので影響なし

問題点 (2/2)

- denyhosts がなくなる
  - openssh 6.7 で libwrap サポートが無くなることもあって fail2ban に移行
- milter-manager を使っているが OS の更新時の手順のドキュメントがない

denyhosts から fail2ban への移行 (1/2)

- aptitude purge denyhosts
- aptitude install fail2ban
- /etc/hosts.deny の denyhosts で追加された行を削除

denyhosts から fail2ban への移行 (2/2)

- /etc/hosts.allow の「ALL: 127.0.0.1 [::1]」に「sshd: ALL」を追加
- /etc/hosts.deny の「ALL EXCEPT sshd: ALL」を削除
- /etc/hosts.deny に「ALL: ALL」を設定

ntp 削除

- systemd-timesyncd に移行するため削除

アップグレード (1/2)

- /etc/apt/sources.list と /etc/apt/sources.list.d/milter-manager.list の wheezy を jessie に変更
- apt-get update
- echo $COLUMNS $LINES が 80 25 になるように端末をリサイズ (scriptreplay を考慮して)

アップグレード (2/2)

- script -t 2>~/upgrade-jessie1.time -a ~/upgrade-jessie1.script
- apt-get upgrade
- apt-get dist-upgrade
- reboot

mailman

- 「古いキューファイルが存在します」で質問が出た
- 多少メールがロストしても大した問題はないので「かまわずに継続」で進んだ

設定ファイルのマージ

- 途中設定ファイルをどうするか聞かれた時は全て既存のファイルを使用を選んだ

rkhunter.conf (1/3)

- mv rkhunter.conf.dpkg-dist rkhunter.conf
- aptitude install unhide
- aptitude purge unhide.rb
  - 実際は後で unhide パッケージに変更した

rkhunter.conf (2/3)

反映しなかった変更:

- ALLOW_SSH_PROT_V1=1
- SCRIPTWHITELIST=/usr/bin/unhide.rb
  - unhide.rb から unhide パッケージに置き換えたため

rkhunter.conf (3/3)

反映した変更:

```
MAIL-ON-WARNING="(管理者グループ)@lilo.linux.or.jp"

# for etckeeper
ALLOWHIDDENDIR=/etc/.git
ALLOWHIDDENFILE=/etc/.etckeeper
ALLOWHIDDENFILE=/etc/.gitignore
```

/etc/etckeeper/etckeeper.conf

- mv etckeeper/etckeeper.conf.dpkg-dist etckeeper/etckeeper.conf
- GIT_COMMIT_OPTIONS="-v" を再設定

/etc/default/spamassassin

- ENABLED=1 にするだけの変更だった
- mv /etc/default/spamassassin{.dpkg-dist,}
- /lib/systemd/system/spamassassin.service に移行済みなので ENABLED は影響なし

spamassassin/local.cf

```
# diff -u /etc/spamassassin/local.cf*
--- /etc/spamassassin/local.cf  2013-11-23 20:11:16.381039020 +0900
+++ /etc/spamassassin/local.cf.dpkg-dist        2015-02-01 04:08:46.000000000 +0900
@@ -16,10 +16,7 @@
 #   modifying the original message (0: off, 2: use text/plain instead)
 #
 # report_safe 1
-report_safe 0

-remove_header ham Status
-remove_header ham Level

 #   Set which networks or hosts are considered 'trusted' by your mail
 #   server (i.e. not spammers)
@@ -85,4 +82,3 @@
 # shortcircuit BAYES_00                ham

 endif # Mail::SpamAssassin::Plugin::Shortcircuit
-
```

- そのまま rm /etc/spamassassin/local.cf.dpkg-dist

/etc/dokuwiki/local.php

```
Auto-generated by Debian postinst script
```

ではなく

```
Auto-generated by config plugin
```

になっていたので、そのまま「rm dokuwiki/local.php.ucf-dist」した。

/etc/dokuwiki/apache.conf

- 「order allow,deny」と「Allow from ALL」を「Require all granted」に
- 「Deny from all」を「Require all denied」に
- rm dokuwiki/apache.conf.ucf-dist

/etc/milter-greylist/greylist.conf

- mv milter-greylist/greylist.conf.dpkg-dist milter-greylist/greylist.conf
- http://milter-manager.sourceforge.net/reference/ja/install-to-debian.html の設定

apache2 の sites

- rm apache2/sites-enabled/lilo.linux.or.jp
- mv apache2/sites-available/lilo.linux.or.jp{,.conf}
- a2ensite lilo.linux.or.jp.conf

apache2 のアクセス許可設定

- 「Order allow,deny」と「allow from all」を「Require all granted」に変更
- 「service apache2 reload」で反映

apache2 の conf

- dokuwiki.conf は自動で conf-available,conf-enabled に移行済みだった
- rmdir /etc/apache2/conf.d

dokuwiki の修正 (1/2)

- http://lilo.linux.or.jp/wiki/ で「A fatal error occured during compilation of the CSS files. If you recently installed a new plugin or template it might be broken and you should try disabling it again. [parse error: failed at `#line-height: 1em; ` in /lib/tpl/vector/static/css/screen.css at line 384]」

dokuwiki の修正 (2/2)

- 「#line-height: 1em; /* fix MSIE 6, 7 */」と古いサポート切れの IE 向け記述だったので削除
- 同様の修正をいくつか

ntp 設定 (1/3)

- timedatectl set-ntp true

ntp 設定 (2/3)

- /etc/systemd/timesyncd.conf の Servers 設定
  - Servers=ntp1.sakura.ad.jp
- systemctl restart systemd-timesyncd で反映

ntp 設定 (3/3)

- systemctl status systemd-timesyncd や timedatectl で確認

掃除 (1/2)

- apt-get autoremove
- aptitude purge '~c'
- aptitude search '~i!~Odebian!~Omilter' でもうインストールできない古いパッケージ一覧

掃除 (2/2)

- aptitude purge '~i!~Odebian!~Omilter'
  - ここで「rkhunter が unhide.rb | unhide を推奨」と出たので unhide.rb から unhide に移行
  - 削除後に「Invalid SCRIPTWHITELIST configuration option: Non-existent pathname: /usr/bin/unhide.rb」と出たのでコメントアウト

mailman のエラー対応 (1/4)

- 昨日さとうさんの指摘で気付いた
- lilo ML のメールが流れない状態になっていた

mailman のエラー対応 (2/4)

根本的な原因は Debian の UTF-8 対応

```
/usr/share/doc/mailman/NEWS.Debian.gz より:
mailman (1:2.1.16-1exp1) experimental; urgency=low

  This version has changed the encoding of most strings, templates
  and pages to UTF-8 to meet the Debian release goal of full UTF-8
  support in all packages. It also no longer automatically converts
  mails to ISO-8859-1.

  If you have been using any nŌn-ASCII strings in places such as
  the mailing list description, these were be stored wrongly in the
  list configuration file (config.pck), so you will need to change
  those (e.g. via the webinterface) again in order to have them be
  displayed correctly.

 -- Thorsten Glaser <tg@mirbsd.de>  Sun, 29 Dec 2013 14:35:50 +0000
```

mailman のエラー対応 (3/4)

- Web の設定画面から文字化けしていた description と info を修正

mailman のエラー対応 (4/4)

- /var/lib/mailman/qfiles/shunt/ に qrunner でエラーになったメールがたまっていた
- /var/lib/mailman/bin/unshunt コマンドを実行すると流れた

二要素認証導入

- aptitude install libpam-google-authenticator
- /etc/pam.d/sshd と /etc/ssh/sshd_config 設定
- 対象ユーザーで google-authenticator コマンド実行

/etc/pam.d/sshd

http://blog.n-z.jp/blog/2016-04-18-libpam-google-authenticator.html 参照

```
auth [success=ignore default=2] pam_exec.so quiet /bin/sh -c [ \
 : ${HOME:=$(getent passwd "$PAM_USER" | awk -F: '{print $6}')}; \
 test -f "$HOME/.google_authenticator"]
auth [success=1 default=ignore] pam_google_authenticator.so \
 echo_verification_code
auth requisite pam_deny.so
auth required pam_permit.so

# Standard Un*x authentication.
#@include common-auth
```

ssh/sshd_config (1/3)

- ChallengeResponseAuthentication yes
- AuthenticationMethods publickey,keyboard-interactive

ssh/sshd_config (2/3)

- 設定変更後、「service ssh restart」すると sshd が起動していなかった
- LV=-c journalctl -u ssh.service で調査
  - AuthenticationMethods is not supported with SSH protocol 1

ssh/sshd_config (3/3)

- 「Protocol 2,1」を「Protocol 2」に変更
- rkhunter.conf の「ALLOW_SSH_PROT_V1=1」はこれが関係していた

TLS 導入

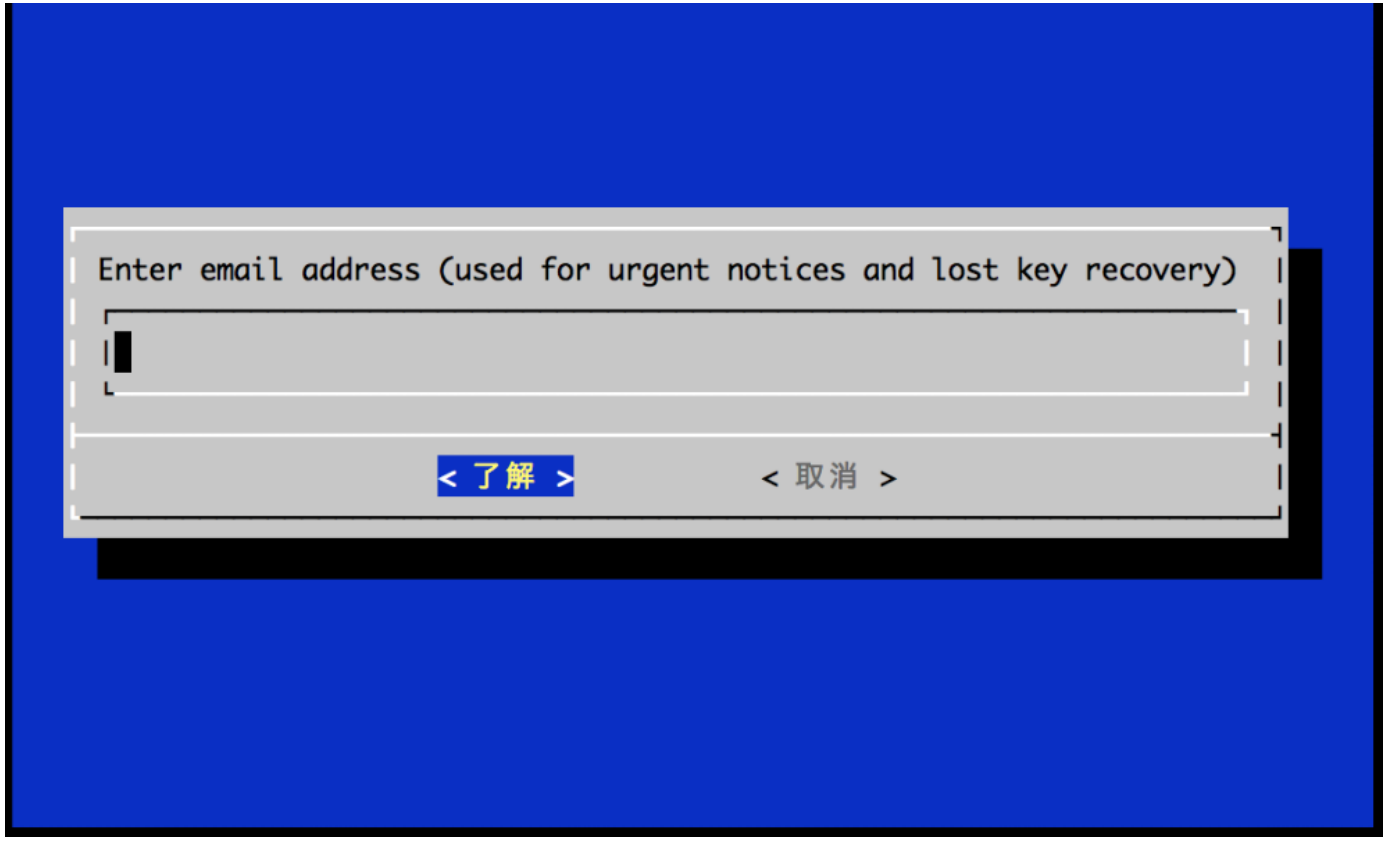
- letsencrypt の証明書導入
- 事前準備
  - JLA (linux.or.jp の管理組織) に確認
  - letsencrypt 用メールアドレス作成
- 各種サービスに設定

letsencrypt パッケージインストール

- backports を有効に
  - deb http://ftp.jp.debian.org/ debian jessie-backports main
- インストール
  - apt install -t jessie-backports letsencrypt
- バージョン 0.5.0-1~bpo8+1 が入った

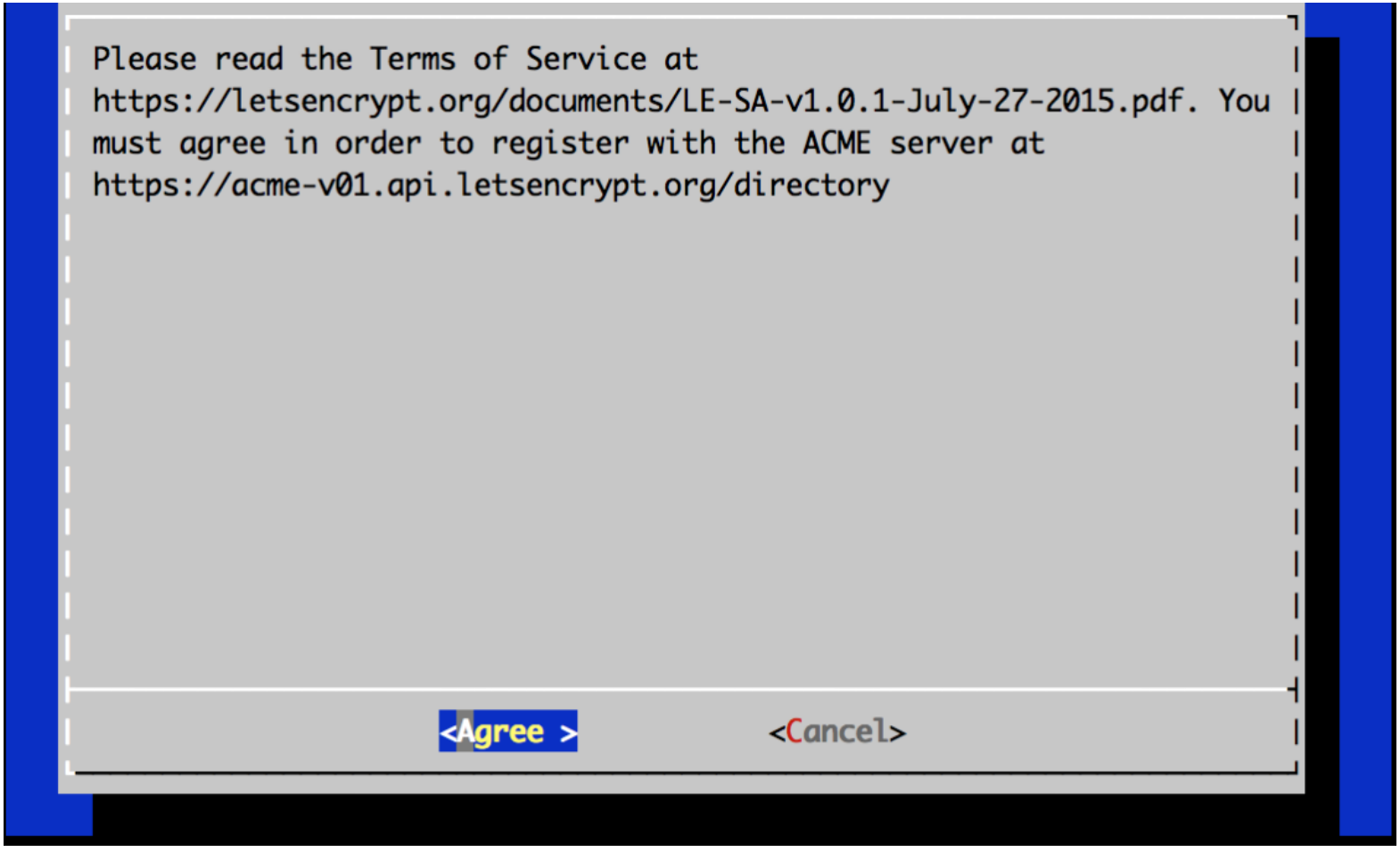
letsencrypt の証明書発行

重要やアカウントの復旧用メールアドレス設定 (初回のみ)



letsencrypt の証明書発行

Terms of Service に同意 (初回のみ)



letsencrypt の証明書発行

証明書発行完了

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/lilo.linux.or.jp/fullchain.pem. Your cert
   will expire on 2016-07-26. To obtain a new version of the
   certificate in the future, simply run Let's Encrypt again.
 - If you lose your account credentials, you can recover through
   e-mails sent to letsencrypt@lilo.linux.or.jp.
 - Your account credentials have been saved in your Let's Encrypt
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Let's
   Encrypt so making regular backups of this folder is ideal.
 - If you like Let's Encrypt, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

postfix 設定 (変更前)

```
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

postfix 設定 (変更後)

```
smtpd_tls_cert_file = /etc/letsencrypt/live/lilo.linux.or.jp/fullchain.pem
smtpd_tls_key_file = /etc/letsencrypt/live/lilo.linux.or.jp/privkey.pem
smtpd_tls_mandatory_protocols = !SSLv2,!SSLv3
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3
smtp_tls_protocols = !SSLv2, !SSLv3
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
```

postfix 設定

- snakeoil から letsencrypt の証明書に変更
- SSLv2, SSLv3 を禁止
- service postfix reload で設定反映
- nc localhost 25 で EHLO localhost で動作確認 (STARTTLS が含まれる)

apache2 設定 (1/2)

- /etc/apache2/sites-available/ の default-ssl.conf などを元に設定作成
- a2ensite lilo.linux.or.jp_ssl.conf で有効に

apache2 設定 (2/2)

- a2enmod ssl で SSL を有効に
- service apache2 restart で反映
- ufw allow 443/tcp でポート開放
- https://lilo.linux.or.jp/ で表示確認

mailman 設定変更

- /etc/mailman/mm_cfg.py の DEFAULT_URL_PATTERN を変更
  - 'http://%s/cgi-bin/mailman/' を
  - 'https://%s/cgi-bin/mailman/' に変更

自動更新設定 (1/2)

/etc/cron.daily/local-letsencrypt に以下のスクリプトを設置

```
#!/bin/sh
LOGFILE=/var/log/letsencrypt/renew.log
if [ -f "$LOGFILE" ]; then
    savelog -c 90 -q "$LOGFILE"
fi
if ! letsencrypt renew > "$LOGFILE" 2>&1 ; then
    echo Automated renewal failed:
    cat "$LOGFILE"
    exit 1
fi
if [ -f "$LOGFILE".0 ]; then
    diff -u "$LOGFILE".0 "$LOGFILE"
fi
apachectl graceful
service postfix reload
```

自動更新設定 (2/2)

- スクリプトについて
  - 基本部分は https://letsencrypt.org/getting-started/ 由来
  - ログの保存回数 (日数) の 90 は letsencrypt の証明書の有効期限から
  - savelog コマンドは debianutils パッケージ由来
  - 失敗した時以外でも差分があればメールが飛ぶ

まとめ (1/3)

- wheezy から jessie へのアップグレードしました。
  - apache の移行で少しの間 Web が見えない時間が発生しました。
  - dokuwiki も雑に対処しました。
  - mailman で問題が起きました。
  - 他は大きな問題はなさそうでした。

まとめ (2/3)

- 二要素認証を導入しました。
  - 今は google-authenticator コマンドを実行して ~/.google_authenticator が存在するユーザーだけ
  - 移行期間として１ヶ月くらい余裕を見て、6月になったら ~/.google_authenticator の存在チェックを外す予定

まとめ (3/3)

- letsencrypt の証明書を導入
- postfix (SMTP over TLS) と apache2 (https) の設定
- mailman の設定も変更
- cron で自動更新の設定