lilo.linux.or.jp の話 (2017年8月)

Kazuhiro NISHIYAMA

LILO&東海道らぐオフラインミーティング
2017/08/27

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

今回の話

前回以降の話

- OGP 追加
- Debian GNU/Linux 9.1 (stretch) に更新
- 更新後のログで気づいた点に対応
- clamav のパターンファイルのミラーに障害発生

OGP 追加

- <meta property="og:image" content="https://lilo.linux.or.jp/mascot/lilopen02.jpg"> などを追加
- Togetter での表示に影響するとわかったため
- Facebook のチェッカーで自動検出される内容と同じ設定
- 反映されるかどうかは未確認

stretch への更新

- 2017-06-17 Debian 9 “Stretch” released
- 2017-07-22 Updated Debian 9: 9.1 released
- リリースノート https://www.debian.org/releases/stable/amd64/release-notes/ を参考にして更新

apt line 更新

- apt line 更新: jessie から stretch へ
  - debian
  - milter-manager
- apt-get update

更新

- apt-get upgrade
- apt-get dist-upgrade
- 設定ファイルは /etc/systemd/timesyncd.conf だけ置き換え
- その他は既存のファイルを使用

後処理

- `find /etc -name '*.dpkg*'`

rkhunter.conf

新しいファイルを元に再設定:

```
UPDATE_MIRRORS=1
MIRRORS_MODE=0
MAIL-ON-WARNING="管理者ML"
UPDATE_LANG="en"
SCRIPTWHITELIST=/usr/bin/lwp-request
SCRIPTWHITELIST=/usr/sbin/unhide.rb
ALLOWHIDDENDIR=/etc/.git
ALLOWHIDDENFILE=/etc/.gitignore
ALLOWHIDDENFILE=/etc/.etckeeper
```

clamav-milter

- 不要になっていたので削除
- `sudo rm /etc/default/clamav-milter.dpkg-bak`
- systemd に対応していなくて init.d スクリプトのままなのが気になる

timesyncd.conf

/etc/systemd/timesyncd.conf.dpkg-old:

```
#Servers=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
Servers=ntp1.sakura.ad.jp
```

/etc/systemd/timesyncd.conf:

```
#NTP=
#FallbackNTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
```

timesyncd.conf の反映

- NTP=ntp1.sakura.ad.jp に変更
- sudo systemctl restart systemd-timesyncd.service

timesyncd.conf の確認

`systemctl status systemd-timesyncd.service` で

```
Status: "Synchronized to time server [2400:8500:1302:826:150:95:148:140]:123 (2.debian.pool.ntp.org)."
```

から

```
Status: "Synchronized to time server [2001:e42:0:1:210:188:224:14]:123 (ntp1.sakura.ad.jp)."
```

に変わったのを確認

etckeeper.conf

- コメントが変わっていただけ
- GIT_COMMIT_OPTIONS="-v" を再設定

/etc/ca-certificates.conf.dpkg-old

変更した覚えはないので削除

後処理2

- `find /etc -name '*.ucf*'`

ufw/before.rules

- state から conntrack に変わっていた
- FORWARD の icmp の許可が加わっていた
- COMMIT の上に追加

```
# ignore noisy igmp
-A ufw-before-input -p 2 -d 224.0.0.1 -j DROP
```

ufw/before6.rules.ucf-dist

```
# ignore noisy icmpv6(130)
-A ufw6-before-input -p icmpv6 --icmpv6-type 130 -j DROP
```

を入れていたが、

```
# MLD query
-A ufw6-before-input -p icmpv6 --icmpv6-type 130 -s fe80::/10 -j ACCEPT
```

などが加わって不要そうなので追加せずに様子見。

50unattended-upgrades

- /etc/apt/apt.conf.d/50unattended-upgrades
- ucf-dist を元に以下を再設定
- Unattended-Upgrade::Mail “root”;
- Unattended-Upgrade::Automatic-Reboot “true”;

/etc/ssh/sshd_config

- ucf-dist を元に以下を再設定
- PermitRootLogin no
- ChallengeResponseAuthentication yes
- AuthenticationMethods publickey,keyboard-interactive
- AllowUsers 許可していたユーザー

掃除

- sudo aptitude purge ‘~i!~Odebian!~Omilter’

```
$ sudo aptitude purge '~i!~Odebian!~Omilter'
以下のパッケージが削除されます:
  acl{u} cpp-4.9{pu} docutils-common{u} docutils-doc{u} dokuwiki{p} gamin{u} gcc-4.9{p} gcc-4.9-base{p}
  imagemagick{u} imagemagick-6-common{u} imagemagick-6.q16{u} imagemagick-common{u} libalgorithm-c3-perl{u}
  libapache2-mod-php5{pu} libapache2-mod-php7.0{u} libapt-inst1.5{p} libapt-pkg4.12{p} libarchive-extract-perl{u}
  libasan1{pu} libasprintf0c2{pu} libb-hooks-endofscope-perl{u} libbind9-90{pu} libboost-iostreams1.55.0{pu}
  libcgi-fast-perl{u} libcgi-pm-perl{u} libclass-c3-perl{u} libclass-c3-xs-perl{u}
  libclass-method-modifiers-perl{u} libclass-xsaccessor-perl{u} libcloog-isl4{u} libcpan-changes-perl{u}
  libcpan-meta-perl{u} libdata-optlist-perl{u} libdata-perl-perl{u} libdata-section-perl{u} libdevel-caller-perl{u}
  libdevel-globaldestruction-perl{u} libdevel-lexalias-perl{u} libdjvulibre-text{u} libdjvulibre21{u}
  libdns-export100{pu} libdns100{pu} libept1.4.12{p} libexiv2-13{pu} libexiv2-14{u} libexporter-tiny-perl{u}
  libfcgi-perl{u} libfftw3-double3{u} libfile-slurp-perl{u} libgamin0{u} libgcc-4.9-dev{p} libgd3{u}
  libgetopt-long-descriptive-perl{u} libgnutls-deb0-28{pu} libgnutls-openssl27{u} libhogweed2{pu} libicu52{pu}
  libilmbase12{u} libilmbase6{pu} libimport-into-perl{u} libintl-perl{u} libintl-xs-perl{u} libio-stringy-perl{u}
  libirs-export91{pu} libisc-export95{pu} libisc95{pu} libisccc90{pu} libisccfg-export90{pu} libisccfg90{pu}
  libisl10{pu} libjasper1{pu} libjs-jquery-cookie{u} libjs-jquery-ui{u} libjson-c2{pu} libjxr-tools{u} libjxr0{u}
  liblensfun-data{pu} liblensfun-data-v1{u} liblensfun0{pu} liblensfun1{u} liblist-moreutils-perl{u} libllvm3.5{pu}
  liblog-message-perl{u} liblog-message-simple-perl{u} liblognorm1{pu} liblqr-1-0{u} liblua5.1-0{u} liblwres90{pu}
  libmagickcore-6.q16-3{u} libmagickcore-6.q16-3-extra{u} libmagickwand-6.q16-3{u} libmodule-build-perl{u}
  libmodule-implementation-perl{u} libmodule-load-conditional-perl{u} libmodule-pluggable-perl{u}
  libmodule-runtime-perl{u} libmodule-signature-perl{u} libmoo-perl{u} libmoox-handlesvia-perl{u}
  libmro-compat-perl{u} libnamespace-autoclean-perl{u} libnamespace-clean-perl{u} libnetpbm10{u} libnettle4{pu}
  libonig2{pu} libopendkim9{pu} libopenexr22{u} libopenexr6{pu} libpackage-constants-perl{u}
  libpackage-stash-perl{u} libpackage-stash-xs-perl{u} libpadwalker-perl{u} libparams-classify-perl{u}
  libparams-util-perl{u} libparams-validate-perl{u} libpath-tiny-perl{u} libperl4-corelibs-perl{u}
  libphp-simplepie{u} libpng12-0{pu} libpod-latex-perl{u} libpod-markdown-perl{u} libpod-readme-perl{u}
  libprocps3{pu} libpsl0{pu} libpth20{u} libqdbm14{u} libreadline6{p} libregexp-common-perl{u} librole-tiny-perl{u}
  libruby2.1{pu} libsoftware-license-perl{u} libssl1.0.0{p} libstrictures-perl{u} libsub-exporter-perl{u}
  libsub-exporter-progressive-perl{u} libsub-identify-perl{u} libsub-install-perl{u} libsub-name-perl{u}
  libterm-ui-perl{u} libtext-soundex-perl{u} libtext-template-perl{u} libtry-tiny-perl{u} libtype-tiny-perl{u}
  libtype-tiny-xs-perl{u} libunicode-utf8-perl{u} libuuid-perl{u} libvariable-magic-perl{u} libvpx1{pu}
  libwebp5{pu} libwebp6{u} libwebpdemux1{pu} libwebpdemux2{u} libwebpmux1{pu} libwebpmux2{u} libwmf0.2-7{u}
  libxapian22{p} libxpm4{u} libxtables10{pu} linux-image-3.16.0-4-amd64{p} netpbm{u} php{u} php-common{u}
  php-curl{u} php-geshi{u} php-intl{u} php-seclib{u} php5{pu} php5-cli{p} php5-common{p} php5-curl{pu} php5-gd{p}
  php5-intl{pu} php5-json{pu} php5-ldap{pu} php5-readline{pu} php7.0{u} php7.0-cli{u} php7.0-common{u}
  php7.0-curl{u} php7.0-intl{u} php7.0-json{u} php7.0-opcache{u} php7.0-readline{u} python-debian{u}
  python-debianbts{u} python-defusedxml{u} python-docutils{u} python-gamin{u} python-httplib2{u}
  python-ndg-httpsclient{u} python-pil{u} python-pycurl{u} python-pygments{u} python-pyinotify{u}
  python-pysimplesoap{u} python-reportbug{p} python-roman{u} python-soappy{u} python-support{p} python-wstools{u}
  ruby2.1{p} sysvinit{p} ufraw-batch{u} zlib1g-dev{u}
以下の、インストールが完了していないパッケージが設定されます:
  spamass-milter
更新: 0 個、新規インストール: 0 個、削除: 204 個、保留: 0 個。
アーカイブの 0 B を取得する必要があります。展開後に 427 MB のディスク領域が解放されます。
先に進みますか? [Y/n/?]
```

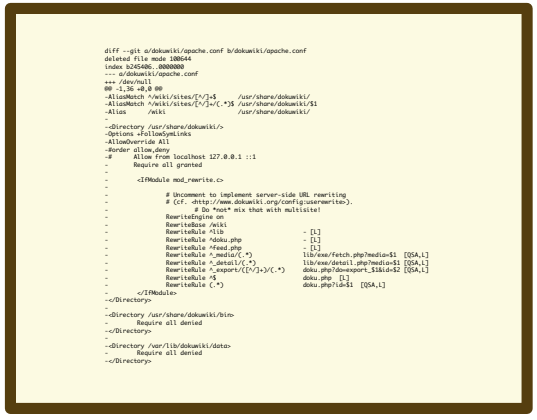
dokuwiki 復旧 (1)

- dokuwiki が消えてしまった。
- とりあえず https://packages.debian.org/dokuwiki から buster (testing) の 0.0.20160626.a-2: all をダウンロードしてきて入れた。

```
$ wget -N http://ftp.jp.debian.org/debian/pool/main/d/dokuwiki/dokuwiki_0.0.20160626.a-2_all.deb
$ sudo dpkg -i dokuwiki_0.0.20160626.a-2_all.deb
$ sudo apt-get -f install
```

dokuwiki 復旧 (2)

- データは残ってそうだったのでこれ以上の被害が出る前にバックアップ
- `etckeeper vcs log -p --stat` から dokuwiki/apache.conf を復元



```
diff --git a/dokuwiki/apache.conf b/dokuwiki/apache.conf
deleted file mode 100644
index b245406..0000000
--- a/dokuwiki/apache.conf
+++ /dev/null
@@ -1,36 +0,0 @@
-AliasMatch ^/wiki/sites/[^/]+$      /usr/share/dokuwiki/
-AliasMatch ^/wiki/sites/[^/]+/(.*)$ /usr/share/dokuwiki/$1
-Alias      /wiki                    /usr/share/dokuwiki/
-
-<Directory /usr/share/dokuwiki/>
-Options +FollowSymLinks
-AllowOverride All
-#order allow,deny
-#       Allow from localhost 127.0.0.1 ::1
-       Require all granted
-
-       <IfModule mod_rewrite.c>
-
-               # Uncomment to implement server-side URL rewriting
-               # (Cf. <http://www.dokuwiki.org/config:userewrite>).
-                 # Do *not* mix that with multisite!
-               RewriteEngine on
-               RewriteBase /wiki
-               RewriteRule ^lib                        - [L]
-               RewriteRule ^doku.php                   - [L]
-               RewriteRule ^feed.php                   - [L]
-               RewriteRule ^_media/(.*)                lib/exe/fetch.php?media=$1  [QSA,L]
-               RewriteRule ^_detail/(.*)               lib/exe/detail.php?media=$1 [QSA,L]
-               RewriteRule ^_export/([^/]+)/(.*)       doku.php?do=export_$1&id=$2 [QSA,L]
-               RewriteRule ^$                          doku.php  [L]
-               RewriteRule (.*)                        doku.php?id=$1  [QSA,L]
-       </IfModule>
-</Directory>
-
-<Directory /usr/share/dokuwiki/bin>
-       Require all denied
-</Directory>
-
-<Directory /var/lib/dokuwiki/data>
-       Require all denied
-</Directory>
```

dokuwiki 復旧 (3)

まだ dokuwiki/apache.conf しかみていないので、他の設定ファイルも見直した方が良いかも

DKIM

- sudoedit /etc/mailman/mm_cfg.py
- REMOVE_DKIM_HEADERS = Yesを
  REMOVE_DKIM_HEADERS = 2 に変更
- sudo systemctl restart
  mailman.service

/usr/lib/mailman/Mailman/Defaults.py

- jessie の時点で Yes の意味が変わっていたらしいが気づいていなかった

```
# Some list posts and mail to the -owner address may contain DomainKey or
# DomainKeys Identified Mail (DKIM) signature headers <http://www.dkim.org/>.
# Various list transformations to the message such as adding a list header or
# footer or scrubbing attachments or even reply-to munging can break these
# signatures.  It is generally felt that these signatures have value, even if
# broken and even if the outgoing message is resigned.  However, some sites
# may wish to remove these headers.  Possible values and meanings are:
# No, 0, False -> do not remove headers.
# Yes, 1, True -> remove headers only if we are munging the from header due
#                 to from_is_list or dmarc_moderation_action.
# 2 -> always remove headers.
# 3 -> always remove, rename and preserve original DKIM headers.
REMOVE_DKIM_HEADERS = No
```

ssh_host_ed25519_key

Logwatch のメールで

```
error: Could not load host key: /etc/ssh/ssh_host_ed25519_key
```

と出ていたので生成:

```
$ sudo ssh-keygen -A
ssh-keygen: generating new host keys: ED25519
```

dpkg-reconfigure openssh-server の方がよかったかも

CVD Download issues for August 23, 2017

- WARNING: getpatch: Can't download daily-23697.cdiff from database.clamav.net
- 全ミラーが一時的におかしかったらしい
- [clamav-jp 281] ウィルスDB更新の異常について（解決済）

clamav 続き

- 2017-08-26 (土) の Logwatch では直っていなかったが 2017-08-27 (日) の Logwatch では直っていた

postfix

```
Postfix is running with backwards-compatible default settings
http://www.postfix.org/COMPATIBILITY_README.html for details
To disable backwards compatibility use "postconf compatibility_level=2" and "postfix reload"
```

Qiita の Postfix 2.12 の compatibility_level という記事を参考にして問題がなさそうなのを確認して compatibility_level=2 に設定

まとめ

- OGP 追加しました
- Debian GNU/Linux 9.1 (stretch) への更新
- dokuwiki が消えたので設定確認が必要そう
- 他は大きな問題はなさそうだった
- clamav も特に対応は必要なかった