Piler Mailarchiv (>= 1.4.5)

Installation via zamba-lxc-toolbox (dev) auf Proxmox VE

Autor: Thorsten Spille

Supporte mich mit einem Kaffee:

git installieren (einmalig)

```
apt update
apt -y install git
```

Toolbox klonen und Piler LXC-Container erstellen

```
git clone -b dev https://github.com/bashclub/zamba-lxc-toolbox
cd zamba-lxc-toolbox
# Konfiguration erstellen
cp conf/zamba.conf.example conf/piler.conf
```

```
# Mit favorisiertem Texteditor die Datei conf/piler.conf anpassen
# Hier ist es nur notwendig, Variablen beginnend mit LXC_ zu bearbetien
# Wird vom DHCP Server im Netzwerk ein DNS-Suffix mitgegeben, so sollte der Piler Hostname eine statische IP-Konfiguration verwendet werden
# Der Piler Hostname wird aus dem FQDN Des Containers erzeugt
# Nach Anpassung der conf/piler.conf den Container erzeigen:
bash install.sh -c conf/piler.conf [-s piler] [-i <id>]
# Optional kann man den Container-Typ / Service angeben und die gewünschte LXC Container ID
```

Nach erfolgter Installation ist die Mailpiler Website über den FQDN des Containers erreichbar, dabei ist wichtig, dass der FQDN des Containers vom Client auflösbar ist.

Erstkonfiguration

Passwörter ändern (Web UI)

Standard-Logins:
- admin@local:pilerrocks
- auditor@local:auditor

Die Passwörter der Standard-Benutzer sollten auf sichere Passwörter geändert werden unter *administration -> users -> Edit/view* für den jeweiligen Benutzer.

SMTP (Smarthost), LDAP und IMAP Login Settings (CLI via pct enter oder ssh)

In der Datei */etc/piler/config-site.php* gibt es bereits vorbereitete Konfigurationsblöcke für Logins und Mailversand:
- SMTP (Smarthost mit optionaler Authentifizierung)
- IMAP (Serverdaten für User-Login am Mailarchiv)
  https://www.mailpiler.org/authenticating-against-an-imap-server/
- LDAP (für User-Login am Mailarchiv)
  https://www.mailpiler.org/authenticating-against-an-ldap-directory/
- UCS LDAP (für User-Login am Mailarchiv)
- POP3 (User-Login)

https://www.mailpiler.org/authenticating-against-a-pop3-server/

TLS-Zertifikat

Nach dem Ausrollen des Containers sind die piler Dienste mit dem snakeoil Zertifikat (Paket ssl-cert) konfiguriert. Dieses sollte durch ein Zertifikat aus einer zugehörigen PKI oder mit einem

letsencrypt Zertifikat ersetzt werden, damit es für den Client signiert ist.

Dateien:
nginx: */etc/nginx/ssl/fullchain.pem* und */etc/nginx/ssl/privkey.pem* sind jeweils Links auf das Snakeoil Zertifikat
piler: */etc/piler/piler.pem* = Kopie des Snakeoil Zertifikats, Zertifikatkette und Private Key in einer Datei

Austausch des Zertifikats

1. Links von nginx Zertifikat entfernen

```
unlink /etc/nginx/ssl/fullchain.pem
unlink /etc/nginx/ssl/privkey.pem
```

2. Zertifikat (komplette Kette nach */etc/nginx/ssl/fullchain.pem,* root:root 0640) und Private Key (nach */etc/nginx/ssl/privkey.pem*, root:root 0600) auf das Mailpiler-System (z.B. via SFTP) kopieren.
3. *renew-piler-cert* ausführen (beendet Dienste, erzeugt auf Basis des nginx Zertifikats ein piler Zertifikat, startet Dienste)

POP-/IMAP-Import via WebUI

POP-/IMAP-Postfächer können für den initialen Import via WebUI unter *administration - import* konfiguriert werden.

Mailempfang vorbereiten

Auf dem Mailpiler läuft ein integrierter SMTP-Server, der Mails für das Archiv auf TCP-Port 25 annimmt. Es muss dafür gesorgt werden, dass der Mailserver das Archiv erreichen kann.

SMTP Acl List

Ist der SMTP des Mailarchivs öffentlich erreichbar, sollte eine ACL mit erlaubten Mailservern für den Mailempfang am Archiv definiert werden. Hierzu wird die Datei */etc/piler/smtp.acl* erstellt und darin IP-Netze im CIDR Format und einem permit / reject dehinter. Beispiel:

```
# MS 365 Server
40.92.0.0/15 permit
40.107.0.0/16 permit
52.100.0.0/14 permit
104.47.0.0/17 permit
```

Ist die Liste vollständig, wird die Datei gespeichert, die ACL aktiviert und der piler-smtp neu gestartet:

```
sed -i -e "s|smtp_access_list=.*|smtp_access_list=1|g" /etc/piler/piler.conf
systemctl restart piler-smtp
```

Konfiguration des Mailservers

Auf dem Mailserver sollte nun BCC-Maps definiert werden, damit alle eingehende Mails (der zu archivierenden Domains) an die Adresse archive@<fqdn-des-archivservers> gesendet werden.

Postfix

Ein Beispiel ist in der Installationsanleitung zu finden: https://www.mailpiler.org/installation/

To archive emails, piler must receive them somehow. So you have to configure your mail server to send a copy of each received emails to piler via smtp. Since piler is actually an SMTP server, you should not put postfix, exim, ... on the archive itself. If you need it for some reason, then put it to 127.0.0.1:25/tcp, and set the listen_addr variable in piler.conf to listen on eth0 or similar.

If you have MS Exchange, then turn on journaling.

If you have postfix (including zimbra), then add the following to main.cf:

/etc/postfix/main.cf:

```
  smtpd_recipient_restrictions = reject_non_fqdn_recipient, ..., \
                check_recipient_access pcre:$config_directory/x-add-envelope-to, ...

  always_bcc = archive@piler.yourdomain.com
```

/etc/postfix/x-add-envelope-to:

```
  /(.*)/   prepend X-Envelope-To: $1
```

Note that such configuration might reveal Bcc addresses to the recipients in the To/Cc fields. To prevent it happening piler features the HEADER_LINE_TO_HIDE config.php variable to automatically hide the X-Envelope-To: line.

When set (and the default is as seen below) it will hide such header lines from regular users on the GUI, only auditors are allowed to see all recipients, including the Bcc addresses.

```
$config['HEADER_LINE_TO_HIDE'] = 'X-Envelope-To:';
```

If you have Exim, then add the following at the beginning of the routers-section:

```
begin routers

mailarchive:
  debug_print = "R: mailarchive for $local_part@$domain"
  driver = manualroute
  domains = *
  transport = remote_smtp
  # piler listening on port 25:
  route_list = * "piler.yourdomain.com::25"
  self = send

  unseen
```

Mailcow

Im Mailcow WebUI unter *E-Mail - Konfiguration - Addressumschreibung* können pro Domain BCC-Maps für eingehende und ausgehende Mails definiert werden.
Sollte eine DNS-Auflösung des Mailarchivs nicht verfügbar, das Archiv aber über die IP-Adresse erreichbar sein, so kann unter *System - Konfiguration - Routing* ein Transport Mapping angelegt werden.

Weitere Mailserver

Mehr gibts in der offiziellen Doku: https://www.mailpiler.org/docs.html

Angepasste Pfade im LXC-Container

Konfigurations-Verzeichnis: */etc/piler*
Piler-Cronjobs: */etc/cron.d/piler*
Piler CLI-Tools: */usr/bin* (ausführbar ohne Pfadangabe)
Piler-Dienste (systemd units):
- */etc/systemd/system/piler.service (Hauptprozess)*
- */etc/systemd/system/pilersearch.service (Suchdienst)*
- */etc/systemd/system/piler-smtp.service (Piler SMTP)*
Verzeichnis für vom WebUI genutzte Skripte: */usr/libexec/piler*

Datenverzeichnis und Home-Directory des piler Users: */var/piler*
Mountpoint *mp0* ist ein separates Dataset mit sparsamer *recordsize=16K*, welches auf */var/piler* eingehängt wird.

Supportkontakt

Spille IT Solutions

Thorsten Spille <thorsten@spille-edv.de>

Version #9
Erstellt: 5 Mai 2024 16:55:01 von Thorsten Spille
Zuletzt aktualisiert: 13 Mai 2024 17:41:40 von Thorsten Spille