Active Spam Killer
Installation and Configuration

Marco Paganini <paganini@paganini.net>

Contents

Copyright and Legal Information

1 Installation and Configuration

1.1 Requirements

- A Unix or Linux system. Some report success running ASK under OS X but we could not verify it.
- Python 2.2 or later.
- Any mail system capable of forwarding incoming mails to a program, such as:
  - Sendmail
  - Qmail
  - Exim
  - Postfix

ASK supports, but doesn't require procmail. If you use procmail, make sure you have version 3.22 or later. Older versions of procmail contain bugs that may cause mailbox corruption.

Supervisory access (root) is not required, but may help under some circumstances.

1.2 Initial Steps

If you're upgrading, don't forget to read the Upgrade Instructions in Section 4. The upgrade instructions must be followed carefully. A misconfigured system will not only make you miss important emails but also send confirmations to mailing lists and such. Those things will make you a very unpopular person and that's generally a bad idea.

1.3 Installation Instructions

ASK comes pre-packaged in three different formats: an RPM file for RedHat users, a DEB file for Debian users and a compressed tar file that can be used under any unix variant. Usually, you should opt for the pre-packaged file (RPM or DEB) if you have one of those systems and root access. If that's not the case, follow the tarball installation instructions.

1.4 RPM-based Installation

If you have a RPM based system (RedHat, Conectiva, etc), just download the respective RPM file, login as root and type:

```
rpm -ivh ask-X.XX-X.noarch.rpm
```

1.5 DEB-based Installation

If your system uses the Debian packaging format, just download the respective DEB file, login as root and type:

```
dpkg -i ask_X.XX-X_all.deb
```

1.6 Tarball Installation

Use this method if you're just a regular user trying to use ASK or if you don't want to use the pre-packaged files. In this case, all you have to do is unpack ASK somewhere, like this:

```
tar zxvf ask-X.XX.tar.gz
```

This command creates a directory named "ask-x.xx", where "x.xx" is the current ASK version.

This method is the only alternative for those without root access. In this case, just unpack the tarball under your home directory.

1.7 Common Installation Procedures

The rest of the installation is the same regardless of the method chosen.

First, run `asksetup` to create the `.ask` directory under your home directory and install a basic configuration file named `$HOME/.askrc`. This step is required for every user that uses ASK (even if you installed using the RPM or DEB installation options).

Next, edit the `$HOME/.askrc` file and change the variables accordingly. There are some important points to note:

- The `rc_askdir` parameter points to the directory where ASK's data files and lists are kept. You may think of it as the program's "work directory". The default is `$HOME/.ask`.
- Change the `rc_mymails` parameter to contain your email addresses. Add all email addresses where you receive email, separated by commas.

  Example:

  ```
  rc_mymails = mymail@domain.com, myothermail@otherdomain.com
  ```

- Change `rc_mymailbox` to point to your mailbox. Most installations set the default mailbox to a file named with your username under "/var/mail" or "/var/spool/mail".

  If you use a mail-directory instead of a mailbox (Qmail), just append a "/" (slash) to the mailbox name. A very common approach under Qmail for example, is to use a Maildir called "Maildir" under the user's home directory. In this case, the `rc_mymailbox` parameter should be set to something like:

  ```
  rc_mymailbox = /home/yourloginname/Mailbox/
  ```

  The slash at the end tells ASK to use this directory as a Maildir-style mailbox.

- Change `rc_md5_key` to any string. This key is used to generate a unique MD5 signature. This string doesn't appear anywhere and should be unique. Make sure you change it! This parameter does not need to be changed after the initial installation.

- Your `rc_mailkey` can be any string, but it must appear on all emails you send. A good idea is to pick an unusual word or combination of characters from your signature. Make sure every email message you send contains this string. Try to pick something without spaces as some mailers tend to break phrases in mysterious ways and that could cause your mailkey not to be recognized. Do not use your name as the mailkey! This would case a lot of spam to be delivered as some spammers know not only your address but also your name.

The default for the remaining options should be appropriate for most users.

Make sure that your signature contains your mailkey. Send yourself an email and double check it.

2 Configuration

2.1 Configuring Your Lists

ASK uses three lists, stored as text files, under the directory specified by the `rc_askdir` parameter. These text files are named "whitelist.txt", "ignorelist.txt" and "blacklist.txt" for the white, ignore and black lists respectively. The lists contain a set of rules that determine the fate of a message that reaches the system. A match in the whitelist will cause immediate delivery of the message. A match in the ignorelist will cause the message to be discarded and a match in the blacklist will not only discard the message but also send a "nastygram" back to the sender.

There are no default list files in the installation package. If ASK cannot find a list file, it assumes "empty" as the default. This means that confirmation messages will be sent to everybody.

ASK uses regular expressions to match incoming emails to the lists. It's important to get acquainted with some basic regular expression concepts. We present below a sample whitelist with some common cases:

```
from friend@bla\.org
crazy-people@yahoogroups\.com
from resume
to @lists\.sourceforge.net
from \.gov$
from ^info@
subject job offer
header ^X-Spam-Status: no
```

We now discuss each rule in more detail:

- `from friend@bla\.org`: Immediately accept any emails coming from "friend@bla.org". Note that dots are "escaped" with a backslash. This indicates that we want to match a real dot. Without the backslash, a dot means "any character".

  Observe that without extra treatment, this rule would also match "friend@bla.org.br", but ASK knows that this is an email address and internally adjusts the regular expression to match only "friend@bla.org".

- `crazy-people@yahoogroups\.com`: This entry does not contain the "from" qualifier, so ASK adds it internally. Entries like "from x@y and "x@y" are completely equivalent, but you should always use the "from" qualifier as it makes the lists more readable.

- `from resume`: This entry matches the word "resume" anywhere in the sender's email address. Addresses like "resume@domain.com", "test@resume.com", "whatever@yourresume.com" will be gladly accepted. Use with care.

- `to @lists\.sourceforge\.net`: Emails going to any address at "lists.sourceforge.net" are accepted immediately. This is a good way to handle mailing-lists that put the mailing list address in the "To:" field.

  Email addresses are composed of two parts: The "username" part to the left of the "@" sign and the "domain" part to the right of the "@" sign. In this case, no username part exists, causing ASK to employ a substring match. Fully formed emails cause ASK to match an email address exactly.

- `from \.gov$`: Matches anything coming from a ".gov" domain. The dollar sign at the end of the rule means "Match the end of the line here". Without it, this regular expression would match any addresses with ".gov", like "whatever@bla.gov.mx" and "jose.gove@test.com".

  Observe that when a full email is used in the regexp, ASK internally appends the "$" sign to it. That's why "from test@domain.com" is equivalent to "from ^test@domain.com$".

- `from ^info@`: The caret sign (^) matches the beginning of the line. This regular expressions matches any email addresses beginning with "info@", like "info@domain.com". It will not match "info" in any other part of the email address, like "mailinfo@domain.com".

- `subject job offer`: it's also possible to match the message subject. This rule will match the words "job offer" anywhere in the subject. Use with care.

- `header ^X-Spam-Status: no`: this rule will match a header called "X-Spam-Status" with "no" anywhere in its contents. This allows ASK to be cascaded with other anti-spam solutions like SpamAssassin.

ASK never sends confirmations to mailing-lists. If ASK detects a message from a mailing-list it queues the message with the status of "Bulk", unless a match happens in the whitelist. ASK uses some heuristics to determine wether a message is coming from a mailing-list or not.

If you are subscribed to a mailing-list make sure you have the list address in your whitelist. Add a "from mailing-list-address" if your mailing list sends out emails with the mailing-address in the "From:" (or "Reply-To:") field. Add "to mailing-list-address" if your mailing-list sends out emails with the original sender name in the "From:" field and the email list address in the "To:" field.

Do not publish your whitelist or someone may use one of its addresses to deliver spam to your mailbox.

The other lists follow the same rules. See below for a blacklist example:

```
from boss@boringcompany\.com
from @spam
from exwife@bloodsuckinglawyers.com
```

These people will not only be ignored but will also receive a nastygram back. Be careful about who you put here! You don't want to send unnecessary nastygrams. In most cases, you should add people you don't want to receive emails to `ignorelist.txt`. In that case, the email will be silently ignored.

2.2 Generating the Initial Whitelist

ASK comes with a program called `asksenders` that can be used to create an initial whitelist.

`asksenders` reads an mbox formatted mailbox on the standard input and outputs the rules to whitelist all email addresses found on the mailbox. The list can be saved as the whitelist, immediately granting access to past correspondents.

For more information, type `asksenders --help` at the command prompt.

2.3 Final Configuration Steps

The final configuration step is to configure your Mail Transfer Agent to pipe every incoming mail into ASK for processing. This procedure varies according to your MTA and other factors. The following sections contain installation details for popular MTAs and mail filters.

2.3.1 Sendmail, Exim and Postfix Users

Create a file named `$HOME/.forward` with the following line:

```
"|/path/askfilter --loglevel=5 --logfile=/your_home/ask.log --home=/your_home"
```

Make sure you substitute "path" for the correct location where the `askfilter` executable is installed, and make sure that you copy the quotes (") to your file - they are part of it.

Now, change the file permissions with:

```
chmod 600 $HOME/.forward
```

This configuration causes ASK to monitor your emails and generate log messages to a file named "ask.log" under your home directory.

Send yourself some emails (make sure your email signature contains your mailkey). ASK some friends not yet in your whitelist to send you some emails and see if they receive the confirmation message. Ask them to reply to the confirmation message and watch in awe as their email addresses magically appear in your whitelist!

Monitor your log files for a while, to make sure no confirmation messages are being sent to mailing lists or other places where they shouldn't. When you are satisfied with ASK's operation, reduce the logging level to 1 to save disk space.

If you are using Sendmail and the message "xxx not available for sendmail programs" appears in your logs, you need to create a symlink from `smrsh`'s (Sendmail's restricted shell utility) directory for restricted programs to the actual `askfilter` executable. Under RedHat Linux, this directory is normally `/etc/smrsh` but it changes from Unix to Unix. For more details on this issue (and exact instructions on how to create the symlink), please visit The Sendmail FAQ, Section 3.34 at http://www.sendmail.org/faq/section3.html#3.34.

2.3.2 Alternative Exim Installation

Joe Vaughan was kind enough to supply an alternative way of installing ASK with Exim. This method requires some modifications to be performed on Exim's configuration file (`/etc/exim.conf`), so root access (and some familiarity with Exim 3) are required.

You don't need to use this method to make ASK work with Exim. You can use the `.forward` mechanism as described in previous sections.

First, edit your `/etc/exim.conf` file and locate the "Transports" section. Add the following lines:

```
ask_pipe:
  driver = pipe
  command="/usr/bin/askfilter --loglevel=10 --logfile=/home/$local_part/ask.log"
  return_path_add
  delivery_date_add
  envelope_to_add
  check_string = "From "
  escape_string = ">From "
  user = $local_part
  group = mail
```

Install ASK from the RPM or DEB packages if use this configuration. This will guarantee that the `askfilter` script is installed under `/usr/bin`.

The next step is to locate locate the "Directors" section. Add a new director with the lines:

```
ask:
  driver = localuser
  transport = ask_pipe
  require_files = ${local_part}:+${home}:+${home}/.askrc:+/usr/bin/askfilter
  no_verify
```

Change the directories to suit your needs

The new director is called "ask". Order matters. You can put it before or after your "procmail" director, depending which one you want executed first. Don't forget to restart exim after you finish the changes.

This will provide ASK to all users on the system. Note that individual users must still run `asksetup` to create the `.askrc` directory, copy the template `.askrc` file, etc.

2.3.3 Qmail Users

If you're using Qmail, edit the `.qmail` file under your home directory and add the following line:

```
| preline /path_to_ask/askfilter --loglevel=5 --logfile=/your_home/ask.log
```

Make sure this file is not readable by anyone else. At the command prompt, type:

```
chmod 600 $HOME/.qmail
```

Monitor the log file and change the logging level to 1 when you're satisfied with ASK's operation.

2.3.4 Procmail Users

ASK supports procmail directly through the "--procmail" switch. In this mode, ASK works as a mail filter and returns an error code telling procmail whether a message should be delivered or not. If a message needs to be de-queued, stdin is substituted and the appropriate code is returned to procmail.

To use ASK in this fashion, your first procmail rules should be:

```
--- cut here ---
:0 fW
|/path_to_ask/askfilter --procmail --loglevel=5 --logfile=/your_home/ask.log

:0 e
/dev/null
--- cut here ---
```

Pay special attention to the blank line between the rules. They are important. Any rules coming after this block will receive email "sanitized" by ASK.

The second rule above instructs procmail to deliver the message to `/dev/null` if ASK returns a fail code. If you're truly paranoid, you can save those messages to a file instead for later inspection. Keep in mind however, that doing so will not alter the fact that "they" are after you. It will not stop the voices from talking to you either.

As usual, set the logging level to one when you're satisfied with ASK's operation. This will help conserve disk space.

3 Remote Commands

ASK checks the "Subject" line of incoming mails, looking for special strings called "Remote Commands". By sending emails to your own account using these strings, it is possible to manage the queue, edit the lists and others.

ASK understand two flavors of remote commands: HTML mode and Text Mode. You can select the desired mode by locating editing your `.askrc` file and changing the `rc_remote_cmd_htmlmail` parameter to "on" or "off". HTML mode requires an HTML capable mail reader. Text Mode can be used with any mail reader.

To find out about the available remote commands, send yourself a message with "ASK HELP" in the subject. ASK will reply with the list of commands.

3.1 Queue Management

When ASK sends a confirmation message, it stores the original message under the `$HOME/.ask/queue` directory. The original message remains "queued" until the sender replies to the confirmation. As most spammers send their emails using forged return addresses, it is impossible for them to reply to the confirmation, causing the original message to remain queued forever.

It is recommended to check the contents of the queue periodically, removing old messages and delivering any messages of interest. You can remotely control the contents of your queue by sending yourself an email with the string "ASK PROCESS QUEUE" in the subject line. ASK will reply with all the queued files. You will be able to delete messages, add the message sender to one of your lists, dequeue messages, etc. Note that if you're using HTML mode, you will be able to click on certain links inside the email to process the messages. Text mode users need to edit the message and send it back to ASK for processing (A "Reply" usually works well).

3.2 List Management

It is also possible to edit the lists (whitelist, ignorelist and blacklist) via email. To that purpose, just send yourself a message with "ASK EDIT *list*", where list is one of "WHITELIST", "IGNORELIST", or "BLACKLIST." ASK will send you back an email with the contents of your list and further instructions.

4 Upgrade Instructions

4.1 From version 2.2 to version 2.4.x

No special procedures should be necessary, but you may want to take a look at the `sample_askrc` file included in the package as it contains instructions on how to activate the new features.