Remplacement d'Amavisd par Rspamd dans ISPConfig 3.1 sur Debian et Ubuntu

This tutorial describes the steps to replace amavis (amavisd-new) spam scanning software with Rspamd on an ISPConfig 3.1 server. The tutorial is written for Debian and Ubuntu Linux.

Prerequisites

- Root access.
- ISPConfig 3.1 must be installed. The ISPConfig version will be 3.1.15 or newer after this procedure.
- The server uses Debian 9 - 10 or Ubuntu 18.04 on an x86_64 processor (64Bit Linux). Older Debian and Ubuntu versions might work too, but I did not test them.

All commands below are run as root user. Login as root user or use '**su -**' on Debian or '**sudo -s**' on Ubuntu to become root user before you continue with this guide.

Note: This procedure will reconfigure all mailboxes and aliases to write the Rspamd config for each account (similar to an ISPConfig Tools > resync run), this may take quite some time and resources on large mail servers.

Install Redis

The Rspamd setup for ISPConfig requires Redis, so we will install it first.

```
apt-get install redis-server lsb-release
```

Install Unbound if BIND is not installed

If your server has no local DNS server installed, then a local DNS resolver like unbound should be installed.

First, check if BIND is installed by using this command:

```
which named
```

if the command returns the path to the named binary:

```
root@server1:/tmp# which named
/usr/sbin/named
```

then BIND is installed and you must skip this step. In case no path to named is returned, then install unbound:

```
apt-get install unbound
```

Install and Configure Rspamd

The first step to install Rspamd is to add the Rspamd Debian/Ubuntu package repository.

```
CODENAME=`lsb_release -c -s`
wget -O- https://rspamd.com/apt-stable/gpg.key | apt-key add -
echo "deb [arch=amd64] http://rspamd.com/apt-stable/ $CODENAME main" > /etc/apt/sources.list.d/rspamd.list
echo "deb-src [arch=amd64] http://rspamd.com/apt-stable/ $CODENAME main" >> /etc/apt/sources.list.d/rspamd.list
```

Update the Package list:

```
apt-get update
```

And Install Rspamd with apt:

```
apt-get install rspamd
```

Activate Redis in Rspamd configuration.

```
echo 'servers = "127.0.0.1";' > /etc/rspamd/local.d/redis.conf
```

Increase the Rspamd history, enable compression, and do not show the subject in the history. This step is optional.

```
echo "nrows = 2500;" > /etc/rspamd/local.d/history_redis.conf
echo "compress = true;" >> /etc/rspamd/local.d/history_redis.conf
echo "subject_privacy = true;" >> /etc/rspamd/local.d/history_redis.conf
```

Then restart Rspamd.

```
systemctl restart rspamd
```

Update ISPConfig

ISPConfig needs to be updated to enable the Rspamd configuration. When the ISPConfig updater asks you if it shall **reconfigure services**, choose '**yes**'.

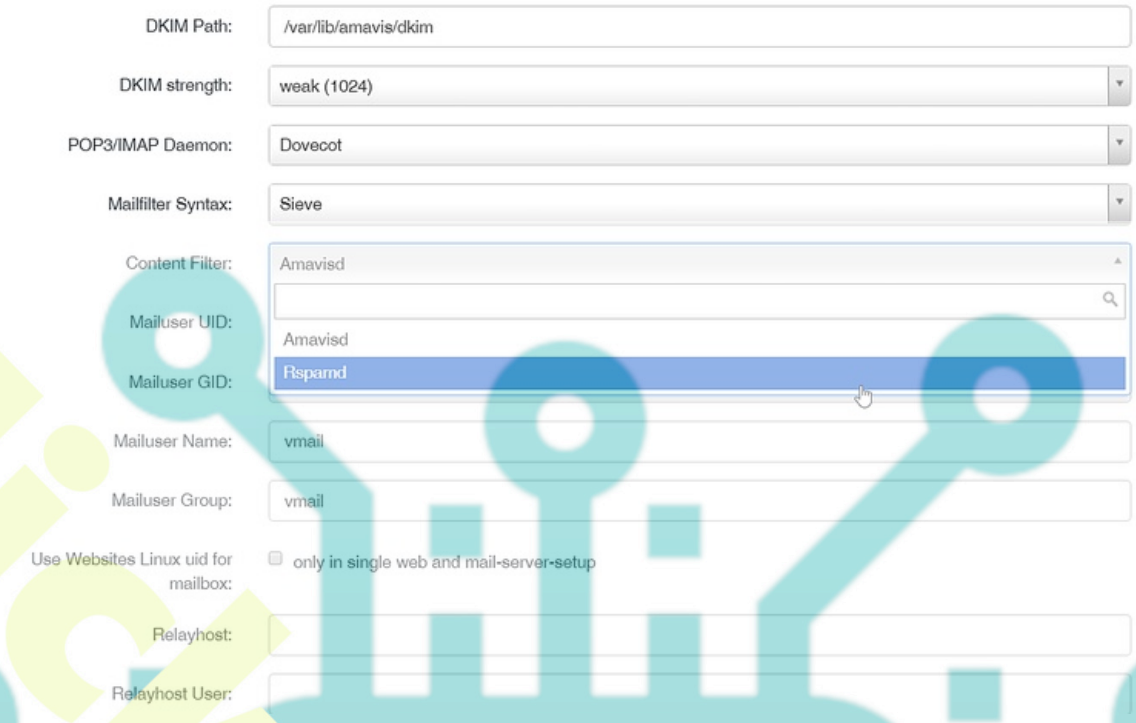
```
cd /tmp
wget http://www.ispconfig.org/downloads/ISPConfig-3-stable.tar.gz
tar xvfz ISPConfig-3-stable.tar.gz
cd ispconfig3_install/install
php -q update.php
```

You will see the line "*Configuring Rspamd*" in the output of the update script when Rspamd is detected and configured.

Enable Rspamd in ISPConfig

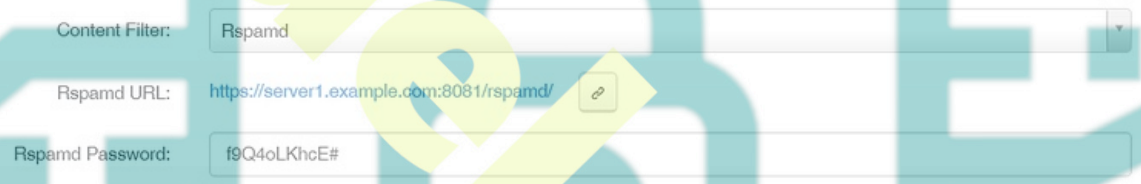
The final step requires that you log into ISPConfig as 'admin' user.

In ISPConfig navigate to ***System > Server Config > Mail***.



There you change the value of the field **Content Filter** from **Amavisd** to **Rspamd** and press the save button at the bottom of the page. ISPConfig will start to reconfigure all mailboxes for Rspamd now.

When you go back to ***System > Server Config > Mail***, then you can see some new fields where you can read and set the Rspamd password.



Make Rspamd Dashboard accessible from outside

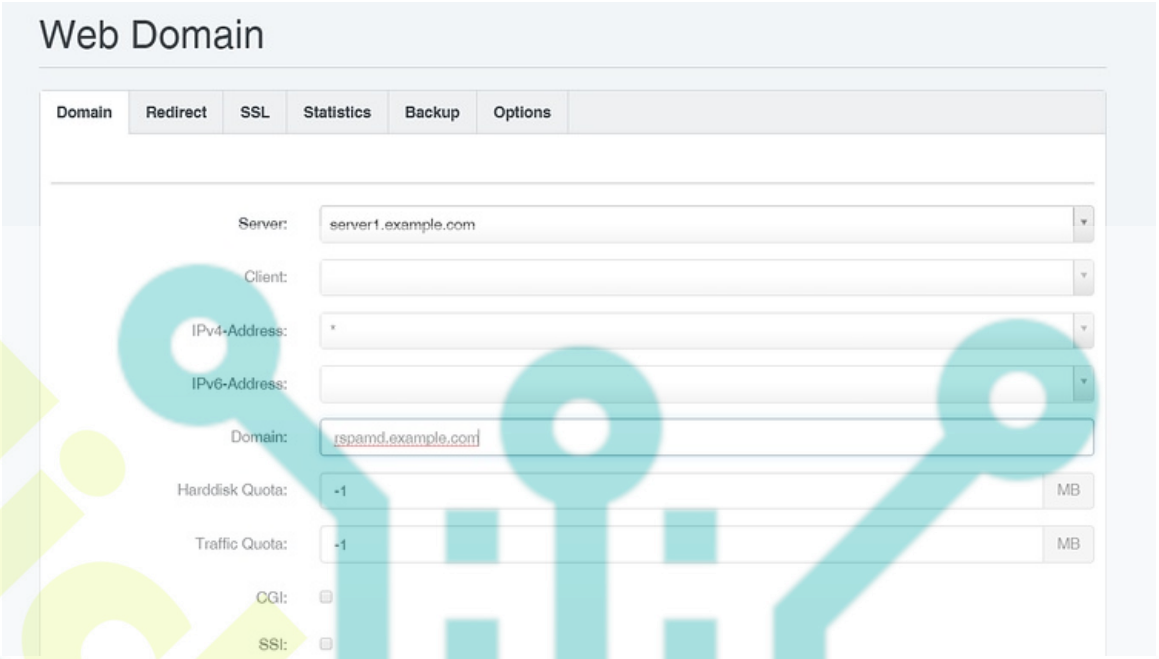
The Rspamd dashboard is on port 11334 on localhost, so it can not be accessed from outside. In this chapter, we will create a website in ISPConfig and add a proxy configuration. The configuration differs between Apache and Nginx web server, use the chapter which matches your installed web server software.

Apache

Enable the Proxy Module and restart apache.

```
a2enmod proxy
systemctl restart apache2
```

Then log into ISPconfig and create a website which will get used to access the Rspamd GUI. You are free to choose the domain name, I will use *rspamd.example.com* here. You don't have to enable any programming language or other options in that site, just leave everything at the defaults. Enabling SSL and Let's encrypt is highly recommended though.



Go to the Options tab of the website and enter the following configuration into the **Apache Directives** field. For Apache 2.2, use:

```
<Location /rspamd>
Order allow,deny
Allow from all
</Location>
RewriteEngine On
RewriteRule ^/rspamd$ /rspamd/ [R,L]
RewriteRule ^/rspamd/(.*) http://127.0.0.1:11334/$1 [P]
```

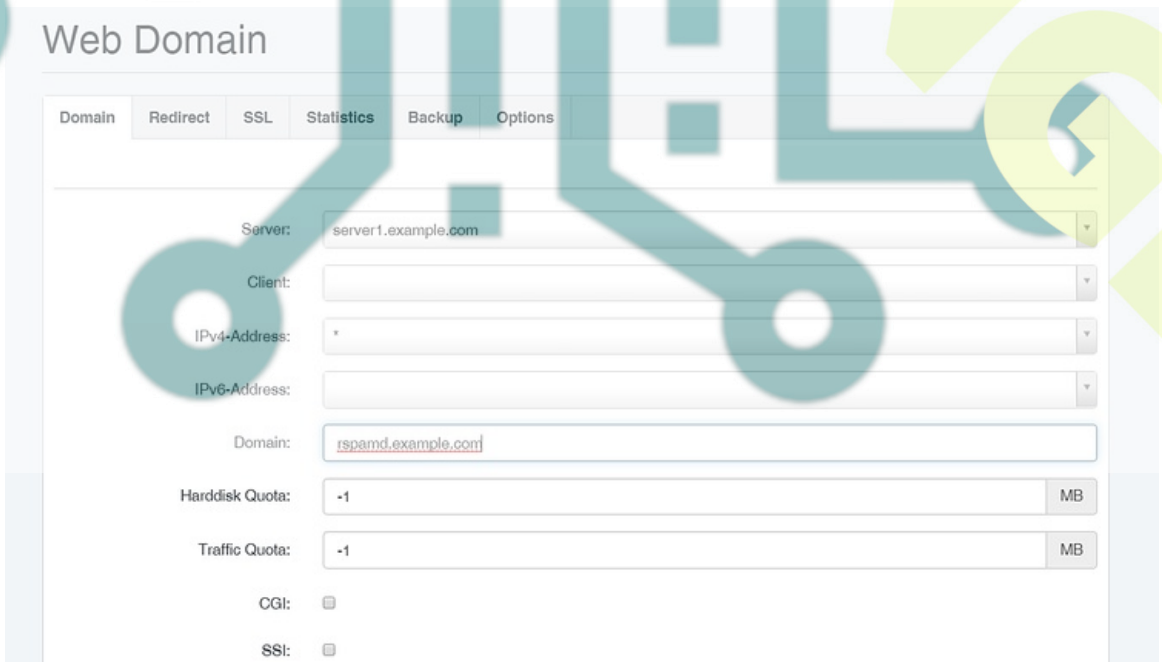
For Apache 2.4, use this instead:

```
<Location /rspamd>
Require all granted
</Location>
RewriteEngine On
RewriteRule ^/rspamd$ /rspamd/ [R,L]
RewriteRule ^/rspamd/(.*) http://127.0.0.1:11334/$1 [P]
```

Now you can access the Rspamd GUI with a web browser ***https://rspamd.example.com/rspamd***. You will get asked for a password, use the password that you generated during Rspamd installation.

Nginx

Log into ISPconfig and create a website which will get used for accessing the Rspamd GUI. You are free to choose the domain name, I will use *rspamd.example.com* here. You don't have to enable any programming language or other options in that site, just leave everything at the defaults. Enabling SSL and Let's encrypt is highly recommended though.



Go to the Options tab of the website and enter the following configuration into the Nginx **Directives** field.

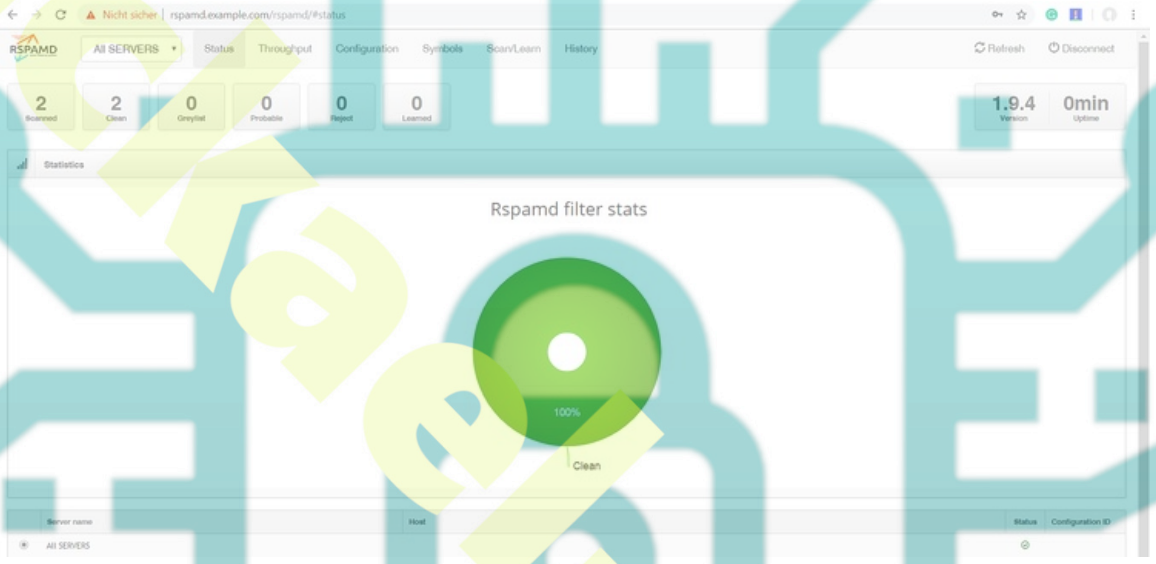
```
location / {
 root /usr/share/rspamd/www/;
 try_files $uri @proxy;
}

location @proxy {
 proxy_pass http://127.0.0.1:11334;
 proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
 proxy_set_header Host $http_host;
}
```

Now you can access the Rspamd GUI with a web browser ***https://rspamd.example.com/***. You will get asked for a password, use the password that you have set for Rspamd in ISPConfig.

Rspamd GUI

Now you can access the Rspamd GUI with a browser and get detailed statistics about the spam filter rate and throughput.



ISPConfig has been reconfigured to use Rspamd instead of Amavis to scan for spam emails. Rspamd is also used for Dkim Signing.

Disable Amavis

Finally, we stop and disable amavisd service:

```
systemctl stop amavisd-new
systemctl disable amavisd-new
```

Conclusion

Rspamd is a modern high-performance spam scan software for Linux servers which delivers very accurate filter results. ISPConfig supports Rspamd as spam scan unit since version 3.1.15. This tutorial shows how to replace amavisd.new with Rspamd on an ISPConfig 3.1 server.
