BasicConfiguration

Basic Configuration

SpamAssassin allows for very flexible configuration. This page contains those configuration parameters that almost everyone will want to consider using as they install or begin using SpamAssasssin.

Server Configuration

These parameters should be placed into the server-wide local.cf configuration file.

Bayes

use_bayes (0|1)
0 = no 1 = yes

This enables using Bayes. Do you want this?, should you use it for your application?, make sure you know if you need/want this or not before installing.

Auto-Whitelist

use_auto_whitelist (0|1)

This enables using Auto-Whitelist factor. Read the description above for bayes and ask the same questions.

Network Tests

dns_available (yes|no|test)
default = test

This enables or disables using dns (disables network tests if set to no). Setting this to no has side effects of turning of a lot of helpful tests. If available always set this to yes.

User Configuration

These configuration parameters should be placed into user-specific $HOME/.spamassassin/user_prefs configuration files (or the SQL equivalents).

- required_score 5
  What score is needed to flag an email as spam (via the X-Spam-Status header)? A brand new user may want to raise this score, perhaps to 6 or 7, until you get confident that your server's parameters do not cause excessive false positives. If you server is working extremely well, you might consider dropping this required score to 4.5 or 4 (I suggest dropping it 0.1 at a time to avoid suddenly causing a lot of false positives). Note: Under version 2.5x and 2.6x, this parameter was named required_hits.
- bayes_auto_learn 1
- bayes_auto_learn_threshold_nonspam -0.001
- bayes_auto_learn_threshold_spam 9.0
  These three parameters control the Bayes auto-learn function. It's on by default, but I like including the bayes_auto_learn parameter in my user_prefs, so if I should need to turn it off, the switch is readily available (set to 0 to turn this off).
  The default non-spam auto-learn threshold is +0.1, which means that any spam that manages to miss all spam rules can be mistakenly learned as ham. I prefer to lower this to -0.1, meaning that emails are auto-learned as ham only if they hit some negative-scoring rule somewhere. Note that if you do not have the ability to create your own rules, and if your host does not have any negative scoring rules, this will effectively turn off Bayes. In that case you may want to use a threshold of 0.0 or 0.001 and hope for the best.
  The default spam auto-learn threshold is 6.0. I prefer to be more conservative, but YMMV.
- use_auto_whitelist 0
  I suggest that new users initially turn the AutoWhitelist (AWL) off. Once you've developed confidence that your ham and spam are being correctly flagged, AWL can be a very powerful tool, but a few mis-categorized emails when first starting up the system can cause emails to be mis-categorized for an extended period of time.
- # score BAYES_00 -4
- # score BAYES_05 -2
- # score BAYES_95 6
- # score BAYES_99 9
  Notice that I have "#" at the front of these lines, which will intially prevent them from rescoring the BAYES rules. However, once Bayes is working well and reliably, I strongly suggest activating these rescoring lines, which will increase the impact of Bayes on high-confidence determinations.