BetterDocumentation LdapReadme

ldap/README

The following is the text of ldap/README, based off of revision 170078.

Please feel free to edit it as much as you like to make it more useful. Periodically the version in Subversion will be updated to incorporate some of the changes.

To see the latest version in Subversion, click here

Feel free to write comments about your changes in the Comments section (at the bottom).

```
Using SpamAssassin With An LDAP Server
--------------------------------------

SpamAssassin can now load users' score files from an LDAP server.  The concept
here is to have a web application (PHP/perl/ASP/etc.) that will allow users to
be able to update their local preferences on how SpamAssassin will filter their
e-mail.  The most common use for a system like this would be for users to be
able to update the white list of addresses (whitelist_from) without the need
for them to update their $HOME/.spamassassin/user_prefs file.  It is also quite
common for users listed in /etc/passwd to not have a home directory,
therefore, the only way to have their own local settings would be through a
database or LDAP server.

SpamAssassin will check the global configuration file (ie. any file matching
/etc/mail/spamassassin/*.cf) for the following settings:

  user_scores_dsn ldap://host:port/dc=basedn,dc=de?attr?scope?uid=__USERNAME__
  user_scores_ldap_username        bind dn
  user_scores_ldap_password        password

The first option, user_scores_dsn, describes the data source name that will be
used to create the connection to your LDAP server. You have to write the DSN as
an LDAP URL, the components being the host and port to connect to, the base DN
for the search, the scope of the search (base, one or sub), the single
attribute being the multivalued attribute used to hold the configuration data
(space separated pairs of key and value, just as in a file) and finally the
filter being the expression used to filter out the wanted username. Note that
the filter expression uses the literal text __USERNAME__ as a placeholder for
the username (SpamAssassin will use a s///g statement to replace it with the
actual username).

Examples:

  ldap://localhost:389/dc=koehntopp,dc=de?spamassassin?sub?uid=__USERNAME__
  ldap://localhost:389/o=stooges?spamassassin?sub?uid=__USERNAME__


If the user_scores_dsn option does not exist, SpamAssassin will not attempt
to use an LDAP server for retrieving users' preferences. Note that this will
NOT look for test rules, only local scores, whitelist_from(s), and
required_score.

Requirements
------------

In order for SpamAssassin to work with your LDAP database, you must have
the perl Net::LDAP module installed. You'll also need the URI module.

In order for spamd to use the LDAP driver, you will have to start spamd
with the additional parameters '--ldap-config -x'.

Each user that wants to utilise the SpamAssassin LDAP driver must add
the 'spamassassin' attribute in their object (either manually or via the
web interface of your making/choice) like this (see the file sa_test.ldif
in this directory for a full database example):

  spamassassin: add_header all Foo LDAP read
```

```
Database Schema
---------------

You can use any schema extension to your user entries with SpamAssassin,
as long as the attribute is multivalued and correctly named in your LDAP url.
We are currently using a <customername>spamassassin field that is part of
our inetOrgPerson subclass.

Here's an example for openldap's /etc/openldap/schema/inetorgperson.schema :

  # SpamAssassin
  # see http://SpamAssassin.org/ .
  attributetype ( 2.16.840.1.113730.3.1.217
          NAME 'spamassassin'
          DESC 'SpamAssassin user preferences settings'
          EQUALITY caseExactMatch
          SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

(don't forget to add "$ spamassassin" to the objectclass MAY clause.)


Testing SpamAssassin/LDAP
-------------------------

To test your LDAP setup, and debug any possible problems, you should start
spamd with the -D option, which will keep spamd in the foreground, and will
output debug message to the terminal. You should then test spamd with a
message by calling spamc.  You can use the sample-spam.txt file with the
following command:

  cat sample-spam.txt | spamc

Watch the debug output from spamd and look for the following debug line:

  retrieving LDAP prefs for <username>: <value>

If you do not see the above text, then the LDAP query was not successful, and
you should see any error messages reported. <username> should be the user
that was passed to spamd and is usually the user executing spamc.

If you need to set up LDAP, a good guide is here:
http://yolinux.com/TUTORIALS/LinuxTutorialLDAP.html

To test LDAP support using the SpamAssassin test suite, you need to
perform a little bit of manual configuration first.  See the file
"ldap/README.testing" for details.


******
NB:  This should be considered BETA, and the interface or overall
operation of LDAP support may change at any time with future releases of SA.
******

Please send any comments to <kris at koehntopp.de> and file bugs via
<http://bugzilla.spamassassin.org/>.

Kristian Köhntopp
```

Comments

Please enter comments here. You can type @"SIG@ to insert your signature. – DuncanFindlay <<DateTime(2005-08-22T02:52:47Z)>>