Problemas a la hora de montar tu servidor de correo con Zimbra? el smtp te envía a algunas direcciones el correo y a otras no?? pues no desesperes... aqui la solucion de la mano de la wiki de Zimbra

fuente: http://wiki.zimbra.com/index.php?title=Outgoing_SMTP_Authentication

Outgoing SMTP Authentication

From Zimbra :: Wiki

Jump to: navigation , search

Contents

[hide]

- 1 Overview
- 2 Setting a relay host
- 3 Enabling SMTP authentication
- 4 Enable TLS
- 5 Troubleshooting
- 6 AT&T Yahoo DSL Specific
- 7 Persistence across Zimbra upgrades

if (window.showTocToggle) { var tocShowText = "show"; var tocHideText = "hide"; showTocToggle(); }

Overview

When you need to route all outgoing mail through your ISP's MTA, and that MTA requires that you authenticate, certain settings in postfix are required.

For this example, we will use *mailrelay.example.com* as the outgoing relay The authentication user will be *username* The password will be *password*

The outbound destination should be the canonical address. postfix will resolve CNAMEs to canonical addresses and then use that to lookup the username and password .

Godaddy example:

smtpout.secureserver.net is really smtp.starfieldtech.com, so make sure you enter smtp.starfieldtech.com

nslookup smtpout.secureserver.net
...
Non-authoritative answer:
smtpout.secureserver.net canonical name = smtp.starfieldtech.com.
Name: smtp.starfieldtech.com
Address: 64.202.165.58

Run all commands as the zimbra user

Setting a relay host

Set the relay host in the admin console, MTA tab to point to your ISPs outgoing mail server. Your ISP can tell you the proper value for this.

You may have to set the port, as well. From the command line:

zmprov ms server.domain.com zimbraMtaRelayHost external.relay.com:#

Enabling SMTP authentication

Create a text file mapping which name/password should be used for each given outbound destination:

echo mailrelay.example.com *username:password* > /opt/zimbra/conf/relay_password

Create a postfix lookup table:

postmap hash:/opt/zimbra/conf/relay_password

To test that the lookup table is correct, the following should return *username:password*:

postmap -q mailrelay.example.com /opt/zimbra/conf/relay_password

Configure postfix to use the new password map:

```
postconf -e smtp_sasl_password_maps=hash:/opt/zimbra/conf/relay_password
```

Configure postfix to use SSL authentication:

```
postconf -e smtp_sasl_auth_enable=yes
```

Configure postfix to use the outgoing servername rather than the canonical server name:

```
postconf -e smtp_cname_overrides_servername=no
```

smtp_cname_overrides_servername=no is used because many smtp servers forward the connection different server than the one set in the smtp_sasl_password_maps file.

Example of the problem :

/opt/zimbra/conf/relay_password :

```
smtp.gmail.com username@gmail.com:password
```

but postfix connects to gmail-smtp.l.google.com

Postfix will not send the authentication info contained in smtp_sasl_password_maps file because it as no entry for the server gmail-smtp.l.google.com but has one for smtp.gmail.com

If you apply smtp_tls_per_site settings then smtp_cname_overrides_servername may become obsolete.

Restart postfix:

```
postfix reload
```

Enable TLS

As Zimbra user:

```
 postconf -e smtp_use_tls=yes
postfix reload
```

Troubleshooting

After sending a test message, check the Log Files for the error:

(Authentication failed: cannot SASL authenticate to server ...: no mechanism available)

You can fix this problem by tweaking the auth mechanisms that postfix is willing to use. First check what auth mechanism postfix is configured to use - by default, you will see:

```
 postconf smtp_sasl_security_options
smtp_sasl_security_options = noplaintext, noanonymous
```

Since noplaintext is present, postfix will refuse to use a mechanism that sends passwords in the clear. If your upstream relay host only supports PLAIN or LOGIN mechanisms (both of which send password in the clear), you have to remove noplaintext from smtp_sasl_security_options:

```
 postconf -e smtp_sasl_security_options=noanonymous
postfix reload
```

If you are concerned about password-in-the-clear and your upstream relay host offers TLS, you might be interested in this smtp_use_tls variable.

See also [1] .

Don't use brackets [] around the server name definition as seen in many places.
Exp.:[smtp.gmail.com]

AT&T Yahoo DSL Specific

If outgoing mail is not being delivered and /var/log/mail.log shows:

(lost connection with smtp.att.yahoo.com while receiving the initial server greeting)

Some ISP's SMTP servers do not implement TLS properly on port 465 (AT&T Yahoo DSL in particular); mail clients handle this when making an SSL connection, however Postfix loses the server connection in this case. Port 587, the standard secondary SSL SMTP port, does work properly with TLS.

The proper commands for AT&T DSL customers in the above setup are:

Change:

zmprov ms server.domain.com zimbraMtaRelayHost external.relay.com:#

To:

zmprov ms server.domain.com zimbraMtaRelayHost smtp.att.yahoo.com:587

And add:

postconf -e smtp_sasl_mechanism_filter=plain,login
postconf -e smtp_sasl_security_options=noanonymous
postconf -e smtp_tls_security_level=may

With those changes the connection works properly. Source [2]

Persistence across Zimbra upgrades

I just did an upgrade of Zimbra 5.0.5 to 5.0.8 after doing the above - and all of the relay smtp auth changes stayed - they were not wiped out by the upgrade.

Retrieved from " http://wiki.zimbra.com/index.php?title=Outgoing_SMTP_Authenticatio

n "

Categories : MTA | Troubleshooting