Alinto

Alinto Mail Server Pro

System operation guide

Alinto

Version 2.0

Index

1. Introduction

This guide will help you with basic commands on Alinto Mail Server Pro server.

As you already know, AMSP runs under Linux CentOS system.

This guide do not substituate the CentOS administration guide, but it can help you with some basic commands

2. Main services

Alinto Mail Server Pro solution consists of several services that you will want to check in order to ensure a good behavior of the system.

The most common command is the service restart or the manual stop.

You can do an action like "restart", "stop", "start" or get the "status" of a service by doing

```
service [service_name] [action]
```

Example:

```
root@v5cc:~# service postfix restart
Shutting down postfix:                                     [  OK  ]
Starting postfix:                                          [  OK  ]
```

The most susceptible services to be restarted are:

- postfix
- amavisd
- milter
- httpd
- tomcat
- mongod
- mysqld

For the Tomcat service, it's possible to run the following command after you restart, in order to verify the webapps status:

```
tom list
```

```
root@v5cc:~# tom list
OK - Applications listées pour l'hôte virtuel (virtual host) localhost
/manager:running:0:manager
/wmm:running:0:wmm
/mobile:running:0:mobile
/webdav:running:0:webdav
/host-manager:running:0:host-manager
/factory:running:0:factory
/factory-ws-v1:running:0:factory-ws-v1
/combine:running:0:combine
```

If you can't access to a web application, check if the given webapps is not "stopped" in the "tom list" command result.

Webapps can be stopped and started with the command:

```
tom {stop/start} [webapps_name]
```

```
root@v5cc:~# tom stop wmm
OK - Application arrêtée pour le chemin de contexte /wmm
root@v5cc:~# tom start wmm
OK - Application démarrée pour le chemin de contexte /wmm
```

3. Postfix

3.1. Queues analysis with searchq

Searchq is a script stored at /root/bin/.

It allows to know the pending mail queues status (active, deferral, hold) displaying their messages ID's lists, depending on the senders or addresses (can configure), or displaying their top senders or top addresses.

```
root@v5cc:~# searchq

Usage: searchq (-L [-I IP.AD.DR.ESS] [-F my@email | -T my@email] -D|-A|-H) | ( -U -S|-R)

-L ask for a complete LIST of IDs

-U ask for a TOP sender|receipt

-I ask by Sender IP use only with -L option

-F by From email use only with -L option

-T by To email use only with -L option

-S by Sender email use only with -U option

-R by Recept email use only with -U option

-D look in DEFERRAL queue

-A look in ACTIVE queue

-H look in HOLD queue

searchq with no/wrong args give a complete LIST of IDs on all queue
```

Some examples:

```
searchq –U –S –D
```

This example displays the top of the senders on the Deferral queue.

```
searchq –L –F user@domain.com -D
```

This example displays a mail-id list where the sender is "user@domain.com"

This command can be followed by a pipe. For example, with a grep, more, or even more useful, postsuper:

```
searchq –L –F domain.com –A | postsuper –h -
```

Keeps in hold queue all the emails sent from a "domain.com" from the active queue.

```
searchq –L –T domain.com –D | postsuper –d -
```

Deletes all emails that are addressed to "domain.com" from the deferral queue.

3.2. Messages size limit

To change the maximum size of the exchanged messages on the platform (mail attached files), you can change the variable "message_size_limit" in the postfix configuration file (/etc/postfix/main.cf):

```
message_size_limit = 14680064
```

To apply this changed, you need to reload or restart postfix

```
service postfix reload
```

4. Spam note

The spam part is managed at the file /etc/amavisd/amavisd.conf

```
$sa_tag_level_deflt  = undef; # add spam infor headers if at, or above that
level
$sa_tag2_level_deflt = 6.31; # add "spam detected" headers at that level
$sa_kill_level_deflt = 6.31; # triggers spam evasive actions (e.g. blocks mail)
$sa_dsn_cutoff_level = 10; # spam leve beyond wich a DSN is not send
```

If you change any value, you will need to restart the service to apply the changes.

```
service amavisd restart
```

5. Log files

The log files can be found in /var/log directory. you can check a file with the "less" command:

```
less /var/log/maillog
```

Or to read the logs in real time with the "tail" command:

```
tail –f /var/log/maillog
```

For troubleshooting, or if you need to investigate, here is the main log folders by service:

Apache logs (http / web)

/var/log/httpd/

Postfix logs (mail)

/var/log/maillog

Dovecot logs (pop/imap)

/var/log/dovecot.log

Tomcat logs (web applications)

/var/log/tomcat/

- catalina.out (generic error logs for all applications)
- webmail.log (webmail UI)
- factory.log (administration UI)
- factory-ws.log (administration API)
- mobile.log (mobile webmail UI)
- webdav.log (Dav, CalDAV, CardDAV protocols)

6. Supervision and SNMP

The supervision is up to you, but we will follow the installation step of the SNMP protocol as it is quite standard.

Install SNMP

```
yum install net-snmp
service snmpd start
```

Don't forget to launch the command

```
chkconfig snmpd on
```

to make the demon snmpd to restart and re-launch in case of reboot.

A scheduled task (cron) writes every 5 minutes on a file stored in the root (postool) the different queues values. This values that can be recovered in snmp to prepare the alerts or produce the graphs.

The configuration file is stored on: **/etc/snmpd/snmpd.conf**

We just need to authorize the machines who will ask the program snmp:

We need to add a line changing localhost for the IP of the machine before ask the oid snmp.

For the postfix queues, here you have the corresponding oid and how to ask them:

- .1.3.6.1.4.1.8072.1.3.2.3.1.1.6.97.99.116.105.118.101 → oid queue active
- .1.3.6.1.4.1.8072.1.3.2.3.1.1.8.100.101.102.101.114.114.101.100 → oid queue deferral
- .1.3.6.1.4.1.8072.1.3.2.3.1.1.4.104.111.108.100 → oid queue hold
- .1.3.6.1.4.1.8072.1.3.2.3.1.1.8.109.97.105.108.100.114.111.112 → oid maildrop

The command that allows to ask is:

```
snmpwalk –c your_community IP.ADD.RE.SS –v 2c asked_oid
```

For example:

```
snpmwalk –c private 192.168.0.1 –v 2c
.1.3.6.1.4.1.8072.1.3.2.3.1.1.6.97.99.116.105.118.101
```

7. File system

Your server should have 2 disks:

- sda : with sda1 for the system and sda2 for the swap
- sdb: over a partition xfs is mounted via LVM. This is the IMAP (mails) volume, The IMAP storage is the volume which will be probably extended as we will see.

To extend your data volume, start add more space in your virtualization hypervisor.

After you got the supplementary space, you have to create a new partition. Launch the command cfdisk and in the part free space do:

```
[New] -> [Primary].
```

Then go to your new partition and do:

```
[Type] and enter 8E (Linux LVM) and press enter to validate.
Finally do: [Write] -> [Quit].
```

For this extension, we will add a physical volume at volume group origin with the command vgextend:

```
vgextend volume_existing_group the_name_of new_volume
```

Example:

```
vgextend imap_vg /dev/sdc1
```

Once it's done, we'll have to make the same operation for the logical volume. For that, depending on your needs, you will have 3 different extensions:

- Increase thee logical volumes until a determined size:

```
lvextend –L50G /dev/imap_vg/imap
```

⇒ logical volume 50GB

- Increase the logical volume with some determined size:

```
lvextend -L +50G /dev/imap_vg/imap
```

⇒ Will increase the logical volume in 50GB

-Increase the logical volume depending on a group volume:

```
lvextend –l 100%VG /dev/imap_vg/imap
```

⇒ The logical volume will be 100% of the volume group

Once we understand the logical volume, we need to increase the size of the file system. By default, the great part of the file systems resizing tools will increase the size following the size of the logical volume. Then you don't need to specify the same size.

The file system XFS must be built in order to be resized and the build point must be given instead of the device name:

```
xfs_grows /imap
```

8. Updating AMSP modules

Once Alinto releases an update to one of AMSP modules, you will be informed via email by Alinto

Technical Support.

In order to install the different updates, you only have to follow the next instructions:

1. Connect to your server via SSH:

```
ssh root@<your_hostname_or_ip>
```

2. Stop the web application server:

```
service tomcat stop
```

3. Launch the update command

```
yum update alinto-* --disablerepo=* --enablerepo=alinto
```

Do not upgrade your distribution version to CentOS 7. It's currently not supported

4. The updates are OK, we need to launch the next command :

```
symlinks -d /var/alinto/webapps/*/WEB-INF/lib
```

5. Restart web application server

```
service tomcat start
service httpd reload
```

9. How to change AMSP default certificates

Alinto Mail Server Pro comes by default with an auto-signed SSL certificate. If you have your own SSL certificate it's possible to update your services.

We have 2 different possibilities here:

1. Wildcard certificate: If we have a wildcard certificate for, for example: *.amsp.alinto.net, we would be able to use this certificate for all your services. For example, for https we can call it by webmail.amsp.alinto.net.
2. Domain certificate: With this, we will have to configure the access to all your services pointing them through amsp.alinto.net.

Once we have introduced the two options, you only have to follow the next steps in order to install it correctly in your system:

1. Overwrite the next 3 files:

a. /etc/pki/tls/private/localhost.key (Private key of the certificate)

b. /etc/pki/tls/certs/localhost.crt (Your certificate)

c. /etc/pki/tls/certs/server-chain.crt (File that contains all your certificate's chain, which is provided by your certificate's issuer)

2. Run the next command on your server console:

a. reload your SMTP service

```
service postfix reload
```

b. reload your HTTP service

```
service httpd reload
```

c. reload your IMAP/POP service

```
service dovecot reload
```

10. How to modify the IP for your services

There is the possibility of changing the IP assigned for AMSP services. In order to make this, you only have to follow this easy steps:

1. First you have to add the IP to the server with the help of CentOS commands
2. After this, we have to modify the file "/etc/postfix/main.cf" by adding the next line: "smtp_bind_address=xxx.xxx.xxx.xxx"
3. Once we have this, we already defined the default IP, we will only need to reload the postfix service with the command: "service postfix reload"

By default AMSP assign one IP, by adding this line we will order our postfix service to use the IP we want it to assign.

11. Maintaining your system up to date

As a system administrator you must keep your system up to date by doing regularly

```
yum update
```

Do not upgrade your distribution version to CentOS 7. It's currently not supported