Exim+Dovecot Kerberos FreeIpa

:

- Astra Linux Special Edition .10015-01 (1.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

, FreeIPA astra.mta

:

- ;
- exim1.astra.mta;
- , , 192.168.32.3 192.168.32.0/24

, , , .

:

```
sudo apt install exim4-daemon-heavy dovecot-imapd dovecot-gssapi
```

:

- exim4-daemon-heavy – (MTA) — Exim4 ;
- dovecot-imapd – (MDA) — Dovecot;
- dovecot-gssapi – GSSAPI- MDA Dovecot;

Dovecot

dovecot **/etc/dovecot/conf.d/10-master.conf.** "service auth" :

```
unix_listener auth-client {
    mode = 0600
    user = Debian-exim
}
```

( ):

```
#default_process_limit = 100
#default_client_limit = 1000

# Default VSZ (virtual memory size) limit for service processes. This is mainly
# intended to catch and kill processes that leak memory before they eat up
# everything.
#default_vsz_limit = 256M

# Login user is internally used by login processes. This is the most untrusted
# user in Dovecot system. It shouldn't have access to anything at all.
#default_login_user = dovenull

# Internal user is used by unprivileged processes. It should be separate from
# login user, so that login processes can't disturb other processes.
#default_internal_user = dovecot
```

```
service imap-login {
  inet_listener imap {
    #port = 143
  }
  inet_listener imaps {
    #port = 993
    #ssl = yes
  }

# Number of connections to handle before starting a new process. Typically
# the only useful values are 0 (unlimited) or 1. 1 is more secure, but 0
# is faster. <doc/wiki/LoginProcess.txt>
#service_count = 1

# Number of processes to always keep waiting for more connections.
#process_min_avail = 0

# If you set service_count=0, you probably need to grow this.
#vsz_limit = $default_vsz_limit
}

service pop3-login {
    inet_listener pop3 {
    #port = 110
  }
  inet_listener pop3s {
    #port = 995
    #ssl = yes
  }
}

service lmtp {
  unix_listener lmtp {
    #mode = 0666
  }

# Create inet listener only if you can't use the above UNIX socket
#inet_listener lmtp {
# Avoid making LMTP visible for the entire internet
#address =
#port =
#}
}

service imap {
# Most of the memory goes to mmap()ing files. You may need to increase this
# limit if you have huge mailboxes.
#vsz_limit = $default_vsz_limit

# Max. number of IMAP processes (connections)
#process_limit = 1024
}

service pop3 {
# Max. number of POP3 processes (connections)
#process_limit = 1024
}

service auth {
# auth_socket_path points to this userdb socket by default. It's typically
# used by dovecot-lda, doveadm, possibly imap process, etc. Users that have
# full permissions to this socket are able to get a list of all usernames and
# get the results of everyone's userdb lookups.
#
# The default 0666 mode allows anyone to connect to the socket, but the
# userdb lookups will succeed only if the userdb returns an "uid" field that
# matches the caller process's UID. Also if caller's uid or gid matches the
# socket's uid or gid the lookup succeeds. Anything else causes a failure.
#
# To give the caller full permissions to lookup all users, set the mode to
# something else than 0666 and Dovecot lets the kernel enforce the
# permissions (e.g. 0777 allows everyone full permissions).
  unix_listener auth-userdb {
    #mode = 0666
    #user =
    #group =
  }
```

```
# Postfix smtp-auth
#unix_listener /var/spool/postfix/private/auth {
# mode = 0666
#}

# Auth process is run as this user.
#user = $default_internal_user
  unix_listener auth-client {
    mode = 0600
    user = Debian-exim
  }
}

service auth-worker {
# Auth worker process is run as root by default, so that it can access
# /etc/shadow. If this isn't necessary, the user should be changed to
# $default_internal_user.
#user = root
}

service dict {
# If dict proxy is used, mail processes should have access to its socket.
# For example: mode=0660, group=vmail and global mail_access_groups=vmail
unix_listener dict {
#mode = 0600
#user =
#group =
}
}
```

Exim:

```
sudo dpkg-reconfigure exim4-config
```

:

– : ;

– : astra.mta

– IP-, : IP-_ (, 192.168.32.3), ,

– , : astra.mta

, , " " - .

– , : 192.168.32.0/24

– DNS- :

– : Maildir /var/mail/

– :

Exim (/var/log/exim4/paniclog) :

```
Failed to create spool file /var/spool/exim4//input//1jb2ok-00031u-5R-D: Operation not permitted
```

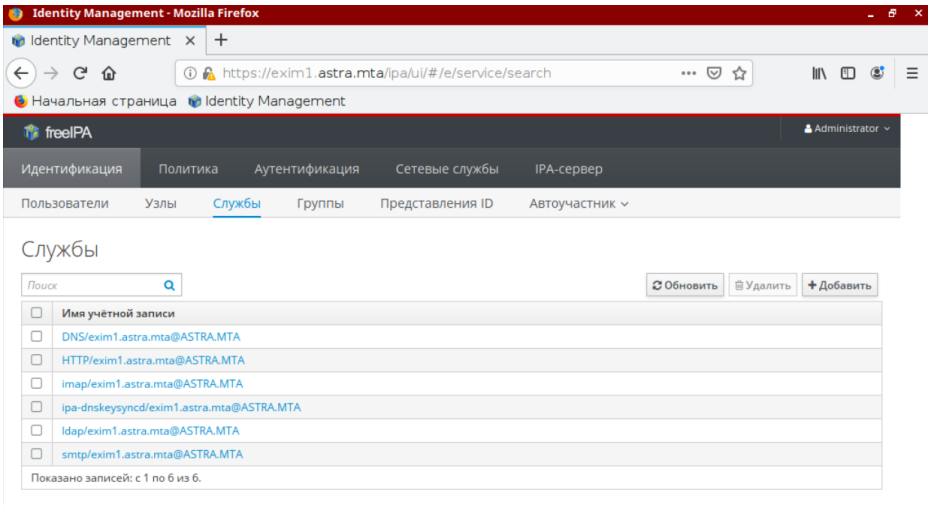
/var/spool/exim4:

```
sudo chown -R Debian-exim:Debian-exim /var/spool/exim4/
```

:

imap/exim1.astra.mta@ASTRA.MTA
smtp/exim1.astra.mta@ASTRA.MTA

FreeIPA:



:

```
kinit admin
ipa service-add imap/exim1.astra.mta@ASTRA.MTA
ipa service-add smtp/exim1.astra.mta@ASTRA.MTA
```

imap, smtp. :

```
sudo kinit admin
sudo ipa-getkeytab --principal=imap/exim1.astra.mta@ASTRA.MTA --keytab=/var
/lib/dovecot/dovecot.keytab
sudo ipa-getkeytab --principal=smtp/exim1.astra.mta@ASTRA.MTA --keytab=/var
/lib/dovecot/dovecot.keytab
```

:

```
sudo klist -k /var/lib/dovecot/dovecot.keytab
```

```
Keytab name: FILE:/var/lib/dovecot/dovecot.keytab
KVNO Principal
----
---------------------------------------------------------------------------
1 imap/exim1.astra.mta@ASTRA.MTA
1 imap/exim1.astra.mta@ASTRA.MTA
1 smtp/exim1.astra.mta@ASTRA.MTA
1 smtp/exim1.astra.mta@ASTRA.MTA
```

dovecot Kerberos:

```
sudo setfacl -m u:dovecot:x /var/lib/dovecot
sudo setfacl -m u:dovecot:r /var/lib/dovecot/dovecot.keytab
```

, **/etc/dovecot/dovecot.conf** POP3, protocols , imap:

```
protocols = imap
```

/etc/dovecot/conf.d/10-auth.conf :

- :

```
disable_plaintext_auth = yes
```

- Kerberos GSSAPI :

```
auth_gssapi_hostname = exim1.astra.mta
auth_krb5_keytab = /var/lib/dovecot/dovecot.keytab
auth_mechanisms = gssapi
```

Dovecot:

```
sudo systemctl restart dovecot
```

Exim

Exim **/etc/exim4/conf.d/auth/33_exim4-dovecot-kerberos-ipa** :

```
dovecot_gssapi:
driver = dovecot
public_name = GSSAPI
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1
```

Exim :

```
sudo systemctl start exim4
sudo systemctl enable exim4
```

Kerberos FreeIPA , ( ), (. " ", . 1, . 13 " ").