DOKUMENTASI TEKNIS EMAIL SERVER ZIMBRA

Dipersiapkan untuk : Dinas Komunikasi dan Informatika Pemerintah Kota Tangerang

DISCLAIMER

Informasi yang terkandung dalam laporan ini disediakan untuk tujuan informasi saja. Segala upaya sudah dilakukan untuk memverifikasi kelengkapan dan keakuratan informasi yang terkandung dalam dokumen ini, namun laporan ini disediakan sebagaimana adanya tanpa jaminan apapun, tersurat maupun tersirat.

DAFTAR ISI

DAFTAR ISI 2

1. Konfigurasi Reverse Proxy 3

2. Set Up the SSH Keys 3

3. Enable Server Statistics 3

4. Hardening MTA Zimbra 4

5. Setup SPF, DKIM & PTR 6

5.1. Setup SPF 6

5.2. Setup DKIM 7

5.3. Setup rDNS 8

6. Deploy SSL Certificate 8

7. Migration 9

7.1. Account Migration 9

7.2. Password Migration 14

7.2.1. Export Password 14

7.2.2. Import Password 14

7.3. Alias Migration 14

7.3.1. Export Alias 14

7.3.2. Import Alias 15

7.3. Mailbox Migration 15

1. Konfigurasi Reverse Proxy

Dikarenakan adanya perubahan hostname yang dilakukan pada server mailbox, maka harus dilakukan perubahan pula pada konfigurasi reverse proxy, karena pada saat pergantian hostname tidak otomatis merubah konfigurasi reverse proxy juga.

- Jalankan command berikut pada server ldap.

```
zmprov mcf zimbraReverseProxyAvailableLookupTargets mail1.tangerangkota.go.id
zmprov mcf zimbraReverseProxyUpstreamLoginServers mail1.tangerangkota.go.id
zmcontrol restart
```

2. Set Up the SSH Keys

SSH ini digunakan untuk management antar Zimbra. Dan SSH Keys harus diupdate secara manual pada server. Berikut langkah untuk mengupdate ssh key, lakukan pada semua server yang sudah terinstall ZCS.

- Generate SSH Keygen dan update ssh keys menggunakan command di bawah ini dengan user zimbra.

```
zmsshkeygen
zmupdateauthkeys
```

3. Enable Server Statistics

Agar statistik server ditampilkan pada admin console, konfigurasi syslog harus dimodifikasi. Men-setting konfigurasi syslog pada server untuk memungkinkan server statistic ditampilkan pada Zimbra Admin Console, dan kemudian logger dapat memonitor host. Statistik server berisi informasi tentang jumlah pesan, volume pesan, serta aktivitas antivirus dan antispam.

- **Jalankan pada server Mailbox**, login sebagai root, jalankan perintah **/opt/zimbra/libexec/zmsyslogsetup**. Fitur ini untuk mengaktifkan fungsi display statistics pada Zimbra Administration Console.

```
/opt/zimbra/libexec/zmsyslogsetup
```

- Buka file **/etc/rsyslog.conf** pada server Zimbra dengan menggunakan perintah di bawah ini :

```
vim /etc/rsyslog.conf
```

- Uncomment atau hilangkan tanda pagar pada option dibawah ini :

Sebelum

```
#$ModLoad imudp
#$UDPServerRun 514
```

Menjadi

```
$ModLoad imudp
$UDPServerRun 514
```

- Jika rsyslog sudah di konfigurasi, maka restartlah service rsyslog tersebut dengan cara seperti berikut :

```
systemctl restart rsyslog.service
```

4. Hardening MTA Zimbra

Pada bagian **Hardening MTA Zimbra** ini adalah metode-metode yang diterapkan yang berguna untuk memperketat security yang ada agar terhindar dari serangan SPAM baik dari internal maupun external.

- Jalankan command berikut dengan menggunakan user zimbra. Command berikut berguna untuk melakukan penolakan / reject apabila pengirim atau penerima tidak ada pada daftar list account.

```
zmprov mcf zimbraMtaSmtpdRejectUnlistedRecipient yes
zmprov mcf zimbraMtaSmtpdRejectUnlistedSender yes
zmmtactl restart
zmconfigdctl restart
```

- Jalankan tahapan berikut dengan menggunakan user zimbra. Command berikut berguna untuk melakukan penolakan / reject apabila pengirim email tidak melakukan otentikasi dan juga menolak apabila from address dengan sasl user login tidak sama.

```
zmprov mcf zimbraMtaSmtpdS
enderLoginMaps  proxy:ldap:/opt/zimbra/conf/ldap-slm.cf
+zimbraMtaSmtpdSenderRestrictions reject_authenticated_sender_login_mismatch
```

  - Buka file /opt/zimbra/conf/zmconfigd/smtpd_sender_restrictions.cf lalu tambahkan reject_sender_login_mismatch setelah opsi permit_mynetworks sehingga menjadi seperti berikut.

    ```
    permit_mynetworks, reject_sender_login_mismatch
    ```

- Restart service MTA

```
zmmtactl restart
```

- Jalankan tahapan berikut untuk menolak apabila terdapat email yang memalsukan from header.
  - Install repository epel-release.

```
yum install epel-release
```

  - Install package pendukung.

```
yum install python-pymilter python-ldap supervisor git-core
```

  - Download custom script dari repository git.

```
cd /opt
git clone https://github.com/iomarmochtar/zmbr_check_sender
```

  - Buat konfigurasi dan sesuaikan dengan kondisi zimbra yang ada.

```
cd zmbr_check_sender/etc
cp config_dist.ini config.ini
vim config.ini
```

```
[ldap]
url = ldap://172.16.9.135:389
bind = uid=zimbra,cn=admins,cn=zimbra
pwd = 9gQqUDLo
; optional, you can leave base search with blank (empty)
base_search = dc=tangerangkota,dc=go,dc=id
```

  - Tambahkan konfigurasi supervisord.

```
cat daemon.ini >> /etc/supervisord.conf
```

  - Jalankan service supervisord

```
service supervisord start
chkconfig supervisord on
```

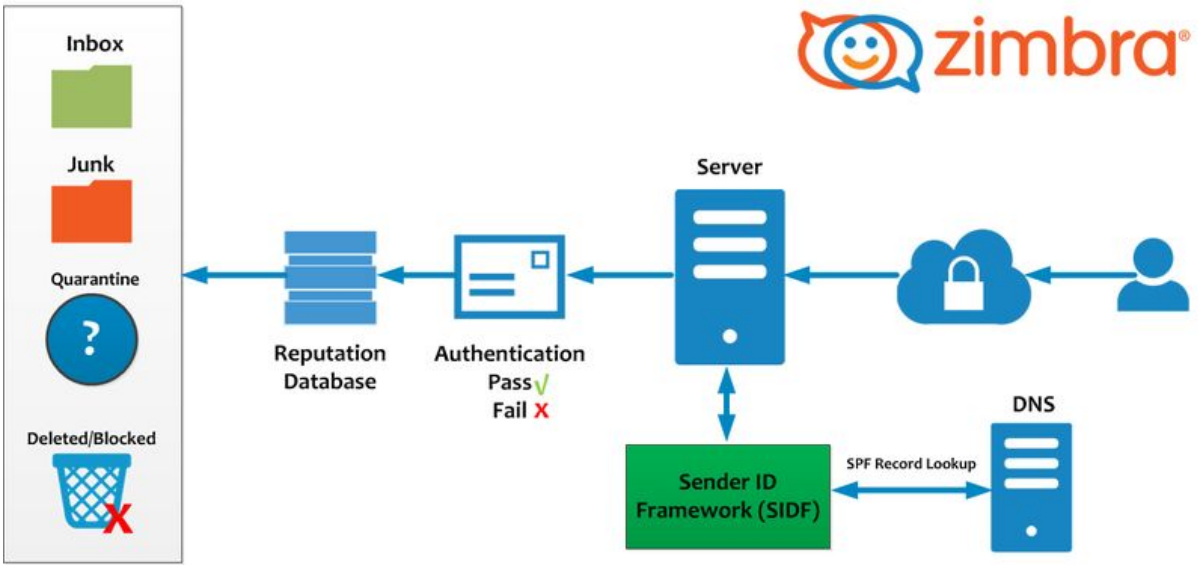
  - Integrasi supervisord dengan Zimbra

```
su - zimbra
zmprov ms `zmhostname` zimbraMtaSmtpdMilters inet:127.0.0.1:5000
zmprov ms `zmhostname` zimbraMilterServerEnabled TRUE
zmmtactl restart
```

5. Setup SPF, DKIM & PTR

5.1. Setup SPF

SPF atau Sender Policy Framework adalah sistem validasi email yg didesain untuk mencegah spam dengan cara mendeteksi spoofing, dengan memverifikasi alamat IP pengirim. Dengan SPF kita bisa tahu bahwa sebuah email terkirim dari sebuah alamat IP (email server) yang memang diizinkan untuk mengirim email tsb dari domain si sender.



Teknisnya, anda harus membuat sebuah entri DNS pada domain anda, berupa SPF record atau TXT Record dan memasukan list valid dari alamat2 IP (hosts) yg diijinkan untuk mengirim atau menghantarkan email atas nama domain anda. Setiap email terkirim yg bukan dari list tsb di atas, bisa dipastikan palsu atau spoof dan anda bisa mengatur DNS anda, supaya MX penerima (external MTA) bisa mengecek incoming mail memang benar terkirim dari daftar valid hosts yg tertera di DNS anda.

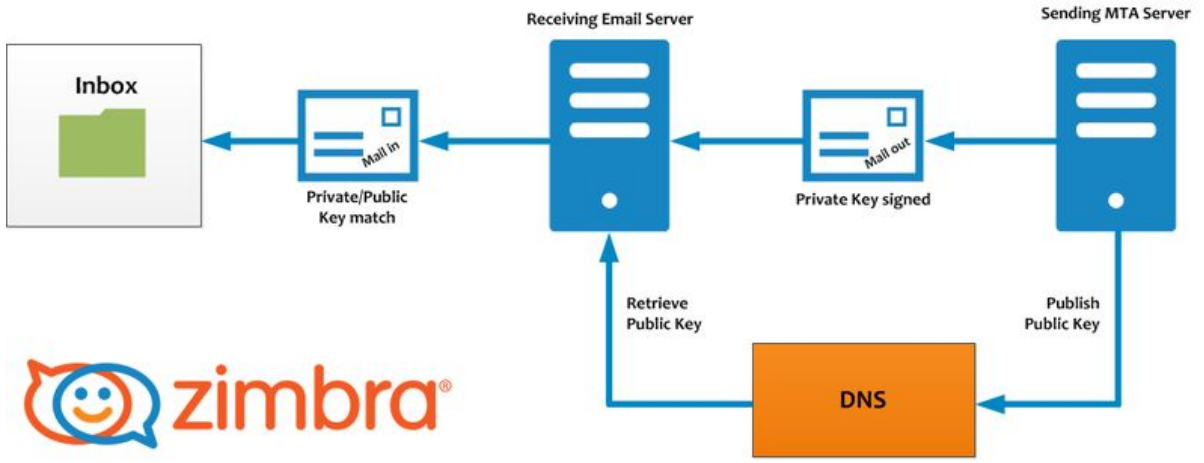
Meski simple, akan tetapi setiap admin DNS harus menambahkan SPF record, dan MX server anda juga harus mendukung SPF (aktif mengecek atau memverifikasi sumber dari sebuah incoming mail)

- Berikut record SPF yang sudah diterapkan pada DNS public tangerangkota.go.id.

```
Domain : tangerangkota.go.id
Type   : TXT
Value  : v=spf1 a mx ip4:103.50.218.254/32 -all
```

5.2. Setup DKIM

DKIM (DomainKeys Identified Mail) adalah cara agar mail server tujuan bisa memverifikasi apakah ini email yang valid yang berasal dari nama domain tertentu. Jadi fungsinya mencegah spoofing dan phising email. Dan sama dengan SPF ini nanti dipasangkan pada DNS record untuk nama domainnya.



DKIM menggunakan pasangan kunci private/publik untuk men“sign” semua email keluar secara otomatis.

Dengan membuat kunci publik domain Anda tersedia melalui DNS setiap mail server di internet dapat memeriksa apakah signature tsb berlaku untuk domain Anda dan tidak ada yang spoofed email terkait. Meskipun SPF lebih tersebar luas daripada DKIM, namun SPF memiliki desain flaw karena SPF akan gagal ketika Anda mem-forward email (disebabkan alamat IP pengirim berubah dan mungkin saja alamat tsb menjadi tidak valid lagi – karena mungkin tidak tercantum dalam entri SPF).

Prinsip kerja DKIM similar dengan SPF, dimana ada informasi yang diletakan di public DNS, perbedaanya adalah DKIM melibatkan pasangan kunci private/public untuk men-sign setiap email keluar. Persamaan lainnya, baik SPF maupun DKIM, lebih diarahkan untuk menjaga reputasi domain perusahaan, sehingga spammer tidak bisa menggunakan teknis spoofed atau phising email ke MX target, namun tidak berarti incoming email ke system menjadi lebih aman dari spammer. Signing dan verifying mail bisa dimanfaatkan sebagai mekanisme whitelist yang lebih bisa diandalkan, untuk misalnya email2 yg berasal dari partner atau clients.

- Berikut command untuk melakukan generate DKIM

```
/opt/zimbra/libexec/zmdkimkeyutil -q -d ilmuzimbra.com
```

- Dari hasil generate DKIM, maka record yang harus dimasukkan pada DNS public adalah sebagai berikut.

```
Domain : BEEFE20C-183B-11EA-9D4F-5C82DC51F88D._domainkey.tangerangkota.go.id
Type   : TXT
Value  : v=DKIM1; k=rsa;
         p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0j0jHAO145rnI3yTe6wkyXMzoX2+A2ABd
         vWH6SvoubX1lnqXURJBzdU6+d9W1dJjZtWmO6B35IizUK74WfnaZhWUqqtQZ/4ShZ3x/Rf/3OnZ9zKA
         0p6eDnz+If54WnchTLzmhDrUEOdqke/a4CtHD2Ez9xsQs4JaErB6ePfOgi0OzkXfP7uWP+tVglQWQeY
         aDKlFRqug+DJFEsF1h7TUU6vD96KMJDAHFADe3VMUwGRlqWjxVG2rzVeuC8dXjSUGZlLe/4BimPv5Eg
         HlDfLnWFdc+PYpVbngSWiXBP5qUx5tpb0yrB+5l4i+iMM2FQpybXxEcg4U0ziNwoY6tNd2pwIDAQAB
```

5.3. Setup rDNS

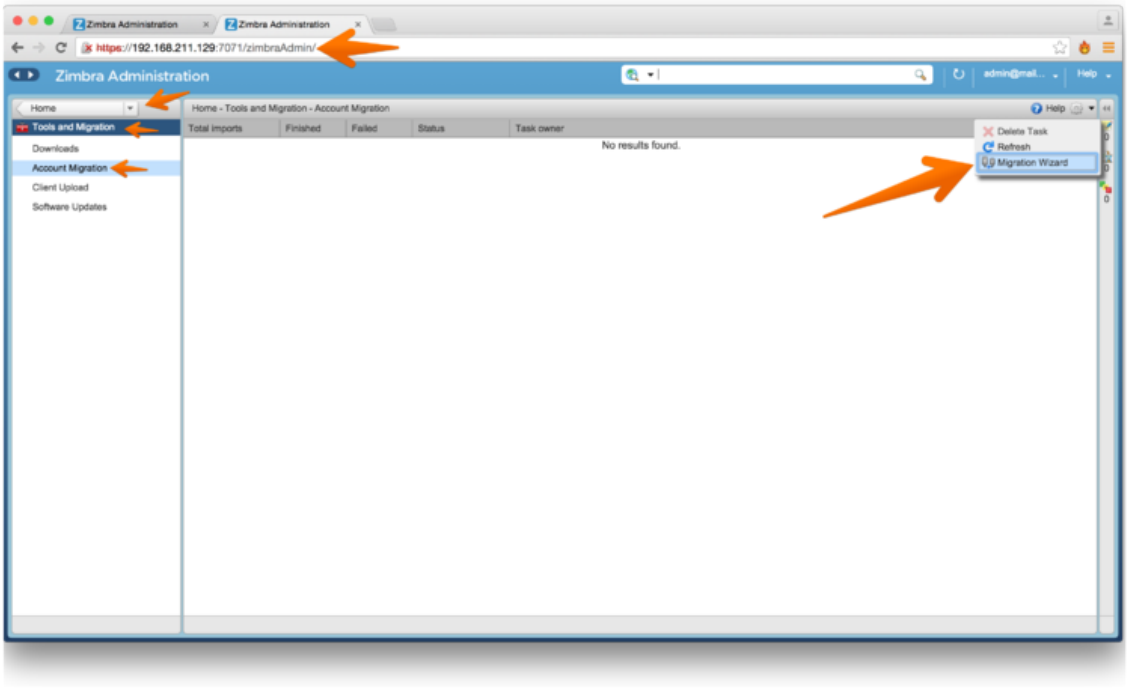
Berikut adalah reverse DNS atau PTR record yang sudah ditambahkan pada DNS public tangerangkota.go.id

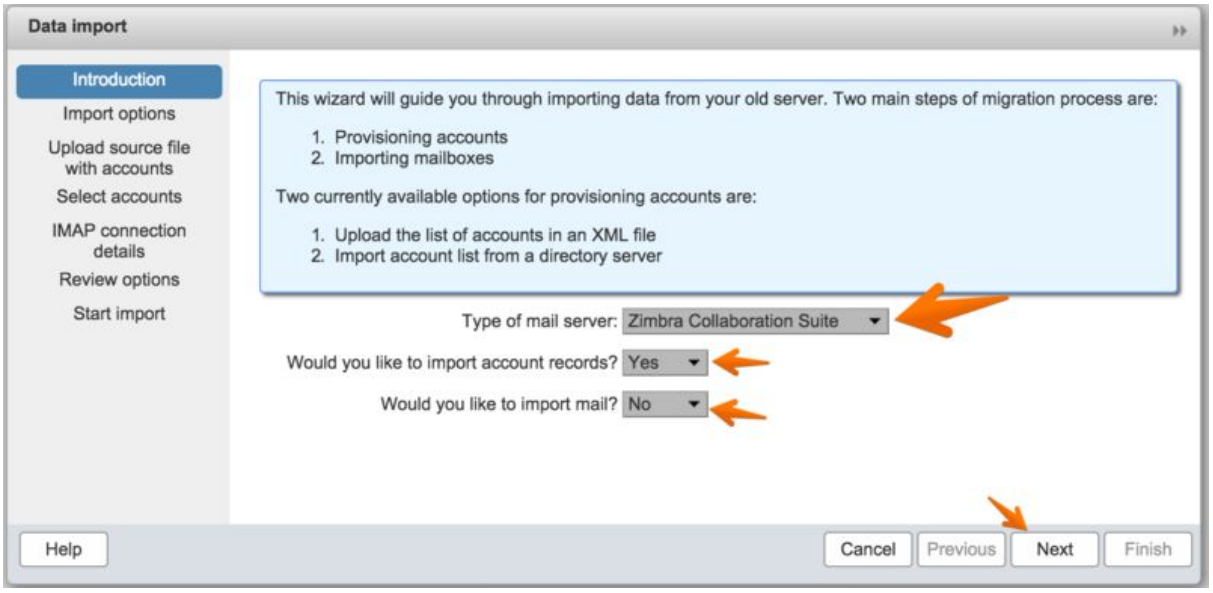
6. Migration

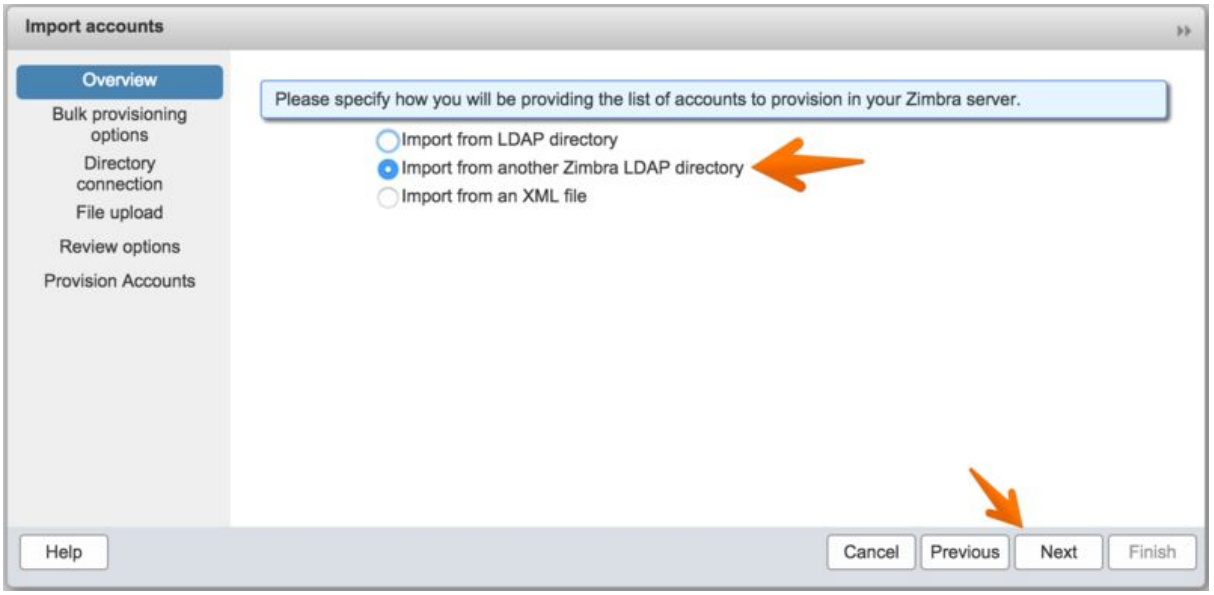
6.1. Account Migration

Berikut adalah langkah-langkah untuk melakukan migration account dari Zimbra lama ke Zimbra baru. Screenshot ini tidak menggunakan data yang sebenarnya, harap disesuaikan dengan environment yang ada.

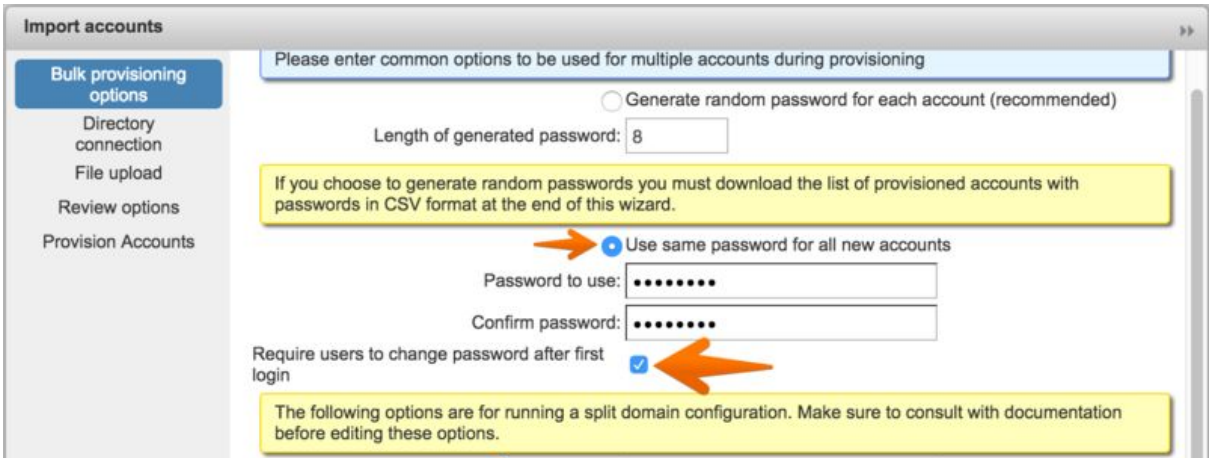
- Login ke Zimbra Admin Console server yang baru. Lalu masuk ke menu Tools & Migration > Account Migration > Migration Wizard


Zimbra Administration
Zimbra Administration
https://192.168.211.129:7071/zimbraAdmin/
Zimbra Administration
admin@mail...
Help
Home
Tools and Migration
Downloads
Account Migration
Client Upload
Software Updates
Home - Tools and Migration - Account Migration
Help
Total imports
Finished
Failed
Status
Task owner
No results found.
Delete Task
Refresh
Migration Wizard


Data import
Introduction
Import options
Upload source file with accounts
Select accounts
IMAP connection details
Review options
Start import
This wizard will guide you through importing data from your old server. Two main steps of migration process are:
1. Provisioning accounts
2. Importing mailboxes
Two currently available options for provisioning accounts are:
1. Upload the list of accounts in an XML file
2. Import account list from a directory server
Type of mail server: Zimbra Collaboration Suite
Would you like to import account records? Yes
Would you like to import mail? No
Help
Cancel
Previous
Next
Finish



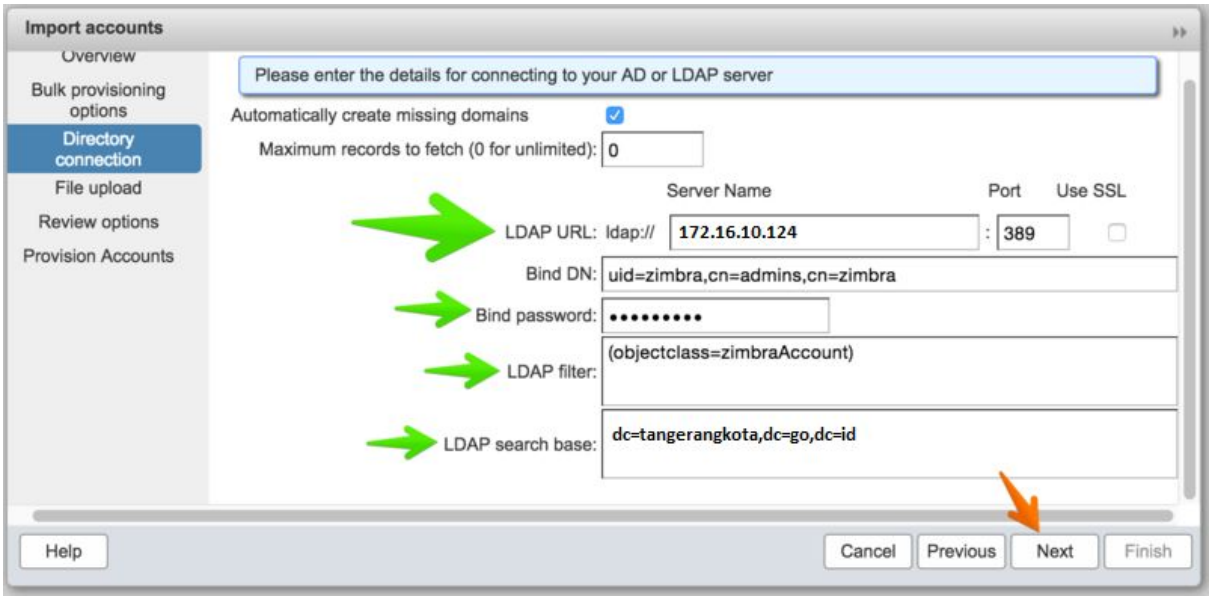
- Pada bagian di bawah ini kita akan diminta memasukkan password yang akan digunakan oleh user. Pada tahapan ini masukkan saja password sembarang, karena nantinya kita akan melakukan migrasi password, sehingga user masih dapat melakukan login dengan username dan password yang lama.

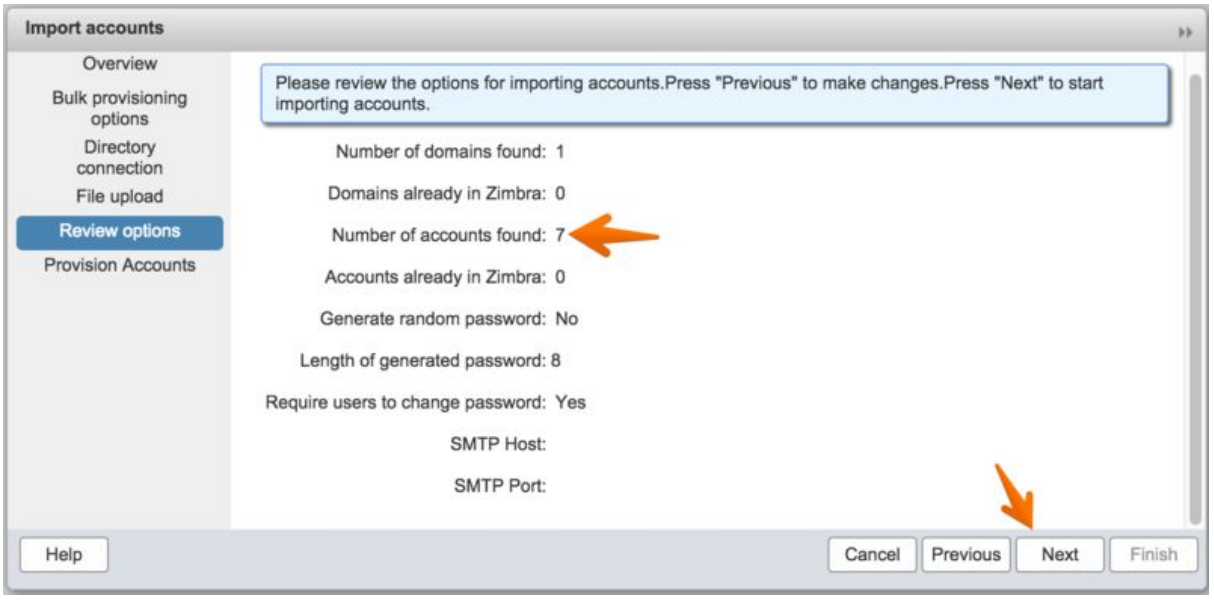


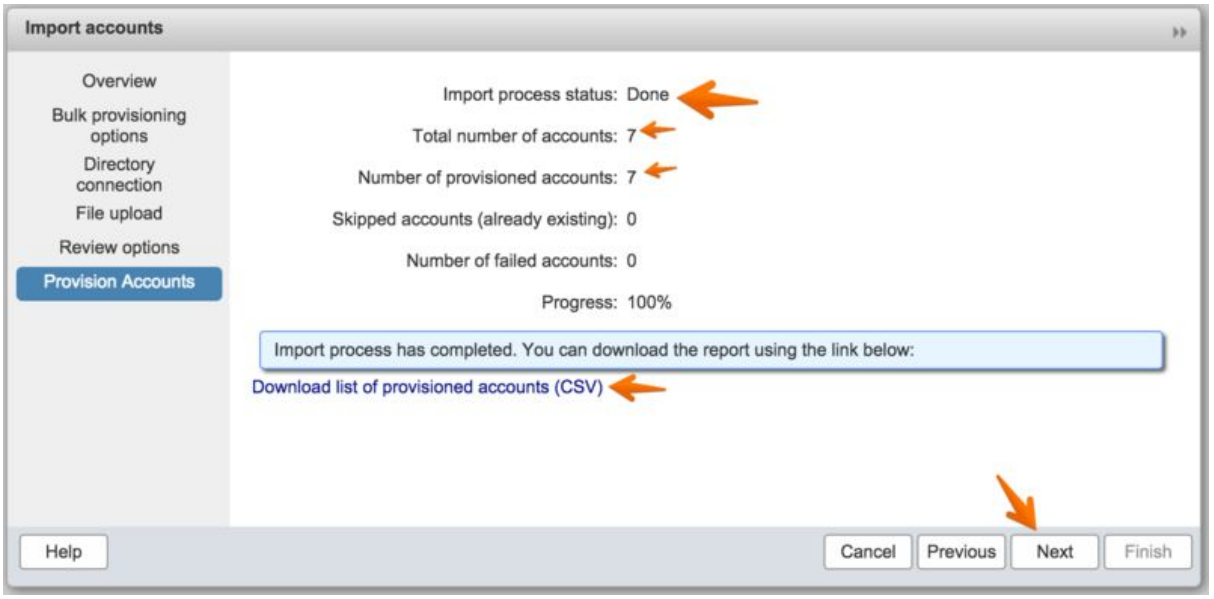
- Pada bagian ini masukkan opsi yang sesuai dengan environment zimbra yang ada.
  - LDAP URL : 172.16.10.124
  - Bind DN : uid=zimbra,cn=admins,cn=zimbra
  - Bind Password :
    - Untuk mengetahui Bind Password yang ada, jalankan command berikut pada server Zimbra lama.

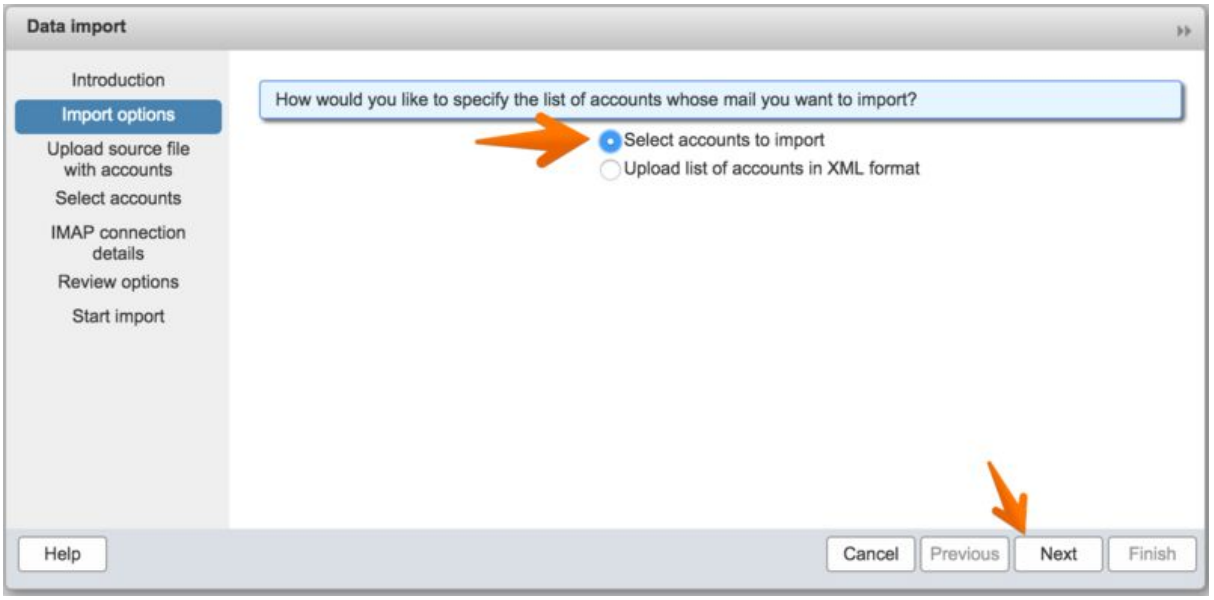
```
zmlocalconfig -s zimbra_ldap_password
```

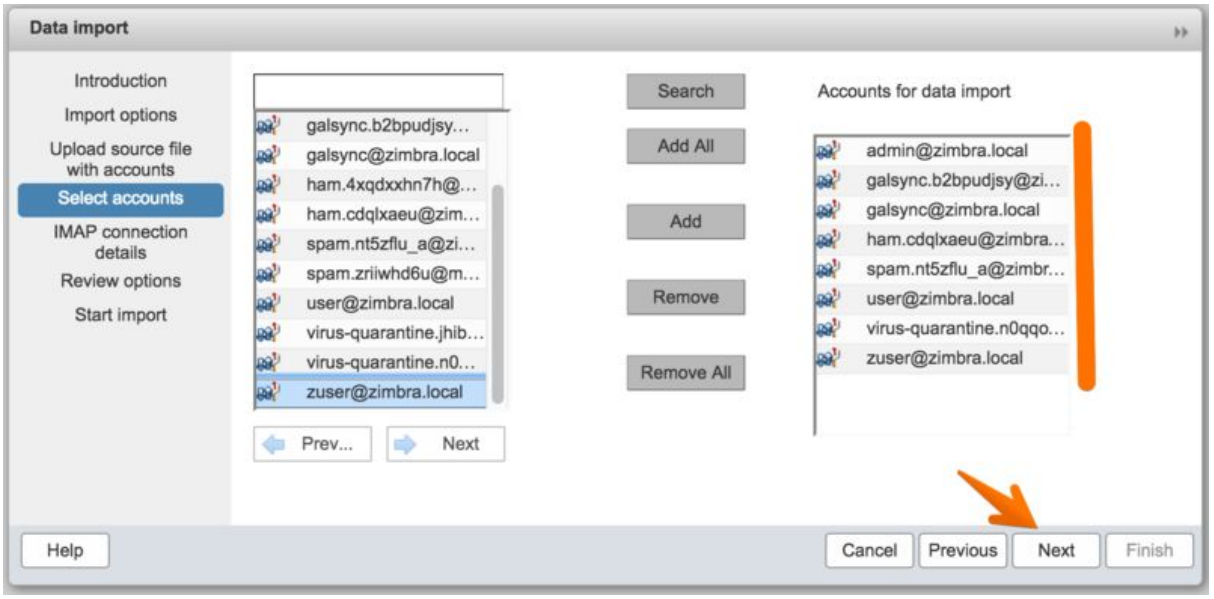
  - LDAP filter : (objectclass=zimbraAccount)
  - LDAP search base: dc=tangerangkota,dc=go,dc=id

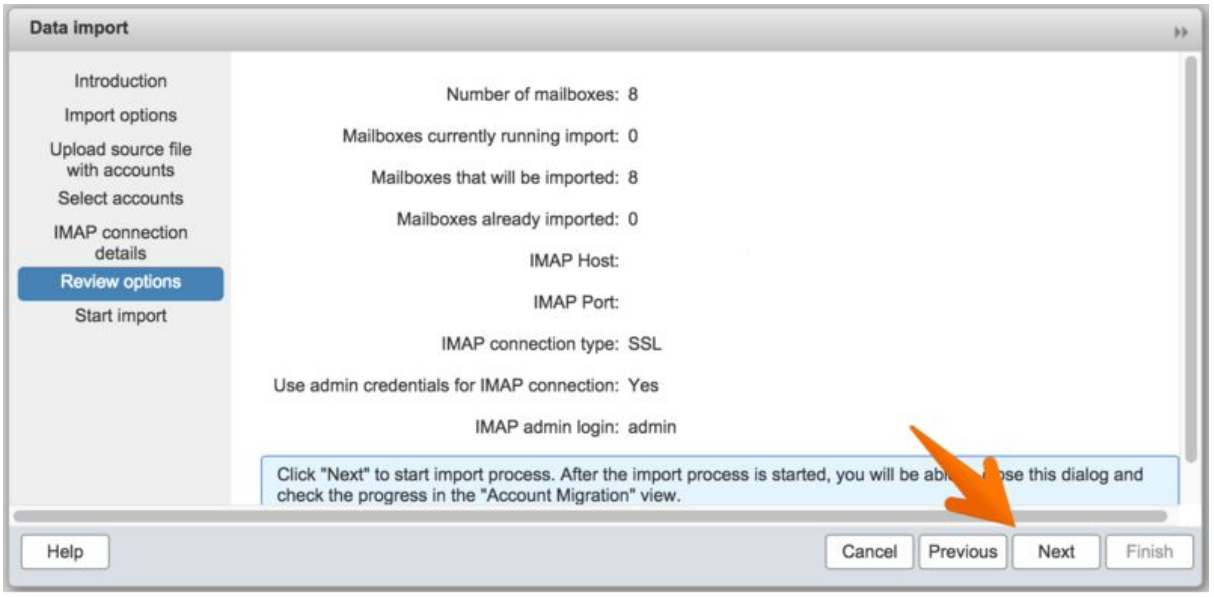


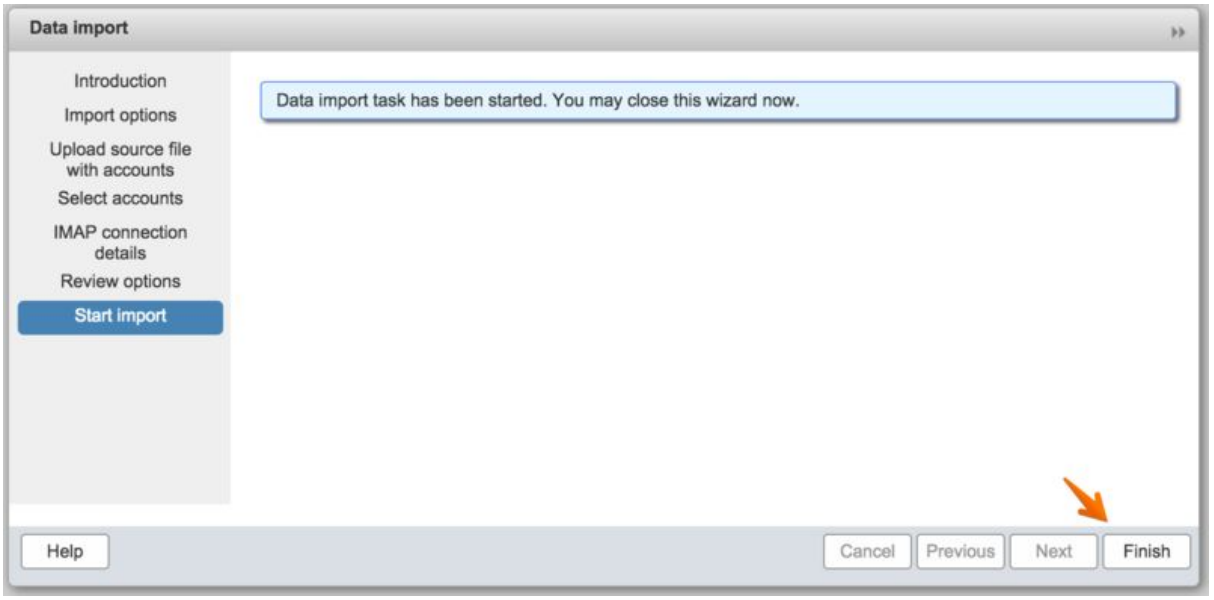


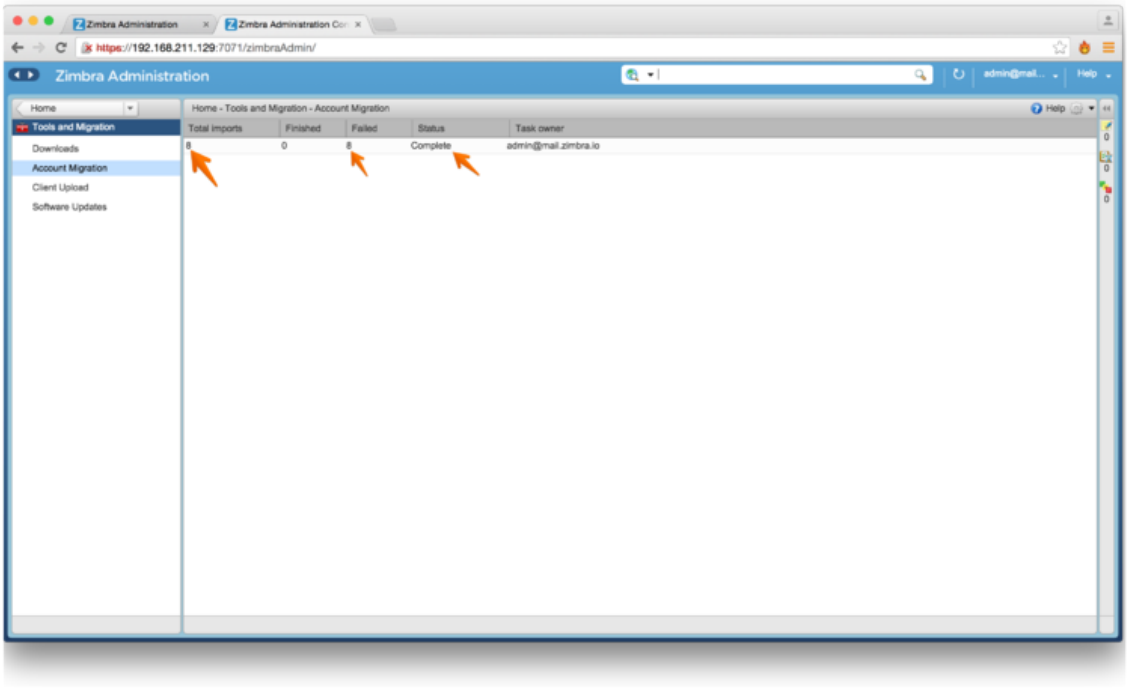

Import accounts
Overview
Bulk provisioning options
Directory connection
File upload
Review options
Provision Accounts
Import process status: Done
Total number of accounts: 7
Number of provisioned accounts: 7
Skipped accounts (already existing): 0
Number of failed accounts: 0
Progress: 100%
Import process has completed. You can download the report using the link below:
Download list of provisioned accounts (CSV)
Help
Cancel
Previous
Next
Finish


Data import
Introduction
Import options
Upload source file with accounts
Select accounts
IMAP connection details
Review options
Start import
How would you like to specify the list of accounts whose mail you want to import?
Select accounts to import
Upload list of accounts in XML format
Help
Cancel
Previous
Next
Finish


Data import
Introduction
Import options
Upload source file with accounts
Select accounts
IMAP connection details
Review options
Start import
galsync.b2bpudjsy...
galsync@zimbra.local
ham.4xqdxxhn7h@...
ham.cdqlxaeu@zim...
spam.nt5zflu_a@zi...
spam.zriiwhd6u@m...
user@zimbra.local
virus-quarantine.jhib...
virus-quarantine.n0...
zuser@zimbra.local
Prev...
Next
Search
Add All
Add
Remove
Remove All
Accounts for data import
admin@zimbra.local
galsync.b2bpudjsy@zi...
galsync@zimbra.local
ham.cdqlxaeu@zimbra...
spam.nt5zflu_a@zimbr...
user@zimbra.local
virus-quarantine.n0qqo...
zuser@zimbra.local
Help
Cancel
Previous
Next
Finish


Data import
Introduction
Import options
Upload source file with accounts
Select accounts
IMAP connection details
Review options
Start import
Number of mailboxes: 8
Mailboxes currently running import: 0
Mailboxes that will be imported: 8
Mailboxes already imported: 0
IMAP Host:
IMAP Port:
IMAP connection type: SSL
Use admin credentials for IMAP connection: Yes
IMAP admin login: admin
Click "Next" to start import process. After the import process is started, you will be ab se this dialog and check the progress in the "Account Migration" view.
Help
Cancel
Previous
Next
Finish


Data import
Introduction
Import options
Upload source file with accounts
Select accounts
IMAP connection details
Review options
Start import
Data import task has been started. You may close this wizard now.
Help
Cancel
Previous
Next
Finish



6.2. Password Migration

6.2.1. Export Password

Berikut adalah command untuk melakukan export password pada seluruh account yang ada pada server Zimbra lama.

```
for i in `zmprov -l gaa`;do echo "$i,`zmprov -l ga $i userPassword |grep userPassword |
sed 's/userPassword: //'`" >> /tmp/password.txt; done;
```

Script di atas akan menghasilkan berupa file dengan nama password.txt pada directory /tmp dan nantinya file tersebut akan ditransfer ke server Zimbra Baru.

6.2.2. Import Password

Jika file password.txt sudah ditransfer ke Zimbra baru, maka letakkan file tersebut pada directory /tmp dan jalankan command berikut.

```
for i in `cat /tmp/password.txt`; do zmprov ma `echo $i | awk -F, '{print $1 "
userPassword " $2}'`;done
```

6.3. Alias Migration

6.3.1. Export Alias

Sebelum kita menjalankan export alias, buat terlebih dahulu directory dengan nama backupalias pada directory /tmp yang berguna menyimpan hasil export. Berikut adalah

command untuk melakukan export alias pada seluruh account yang ada pada server Zimbra lama.

```
for email in `zmprov -l gaa; do zmprov ga  $email | grep zimbraMailAlias |awk '{print
$2}' > /tmp/backupalias/$email.txt done
```

Jika proses export sudah selesai, maka transfer directory backupalias ke server Zimbra baru.

6.3.2. Import Alias

Jika directory backupalias sudah ditransfer dan diletakkan pada directory /tmp, maka jalankan command berikut untuk melakukan import alias.

```
for email in `zmprov -l gaa`; do if [[ -f "/tmp/backupalias/$email.txt" ]]; then for
alias in $(grep '@' /tmp/backupalias/$email.txt); do zmprov aaa $email $alias echo "  ->
$email has alias $alias" done fi done
```

6.3. Mailbox Migration

Langkah terakhir dalam proses migrasi adalah melakukan migrasi data email atau mailbox. Proses migrasi menggunakan tool yang disediakan oleh Zimbra. Jalankan proses migrasi pada server Zimbra lama.

- Buka file /opt/zimbra/conf/zmztozmig.conf dan sesuaikan opsi-opsi seperti berikut.

```
#Source ZCS server IP/name,admin user name and password, server port
SourceZCSServer=172.16.10.124
SourceAdminUser=admin
SourceAdminPwd=PASSADMIN
SourceAdminPort=7071
#Destination/Target ZCS server IP/name,admin user name and password, server port
TargetZCSServer=172.16.9.136
TargetAdminUser=admin
TargetAdminPwd=PASSADMIN
TargetAdminPort=7071
Threads=3
WorkingDirectory=/tmp/ztozmig/mailboxdumps/
FailedDirectory=/tmp/ztozmig/mailboxfailures/
SuccessDirectory=/tmp/ztozmig/successes/
LogDirectory=/opt/zimbra/log/ztozmiglogs
KeepSuccessFiles=FALSE
Domains=tangerangkota.go.id
Accounts=all
```

- Jalankan command berikut untuk memulai proses migrasi.

```
/opt/zimbra/libexec/zmztozmig
```

- Jika proses sudah selesai, maka akan terlihat ringkasan atau summary report dari hasil proses migrasi.

```
[INFO|main:1| 03/18/2015 20:34:57]: ***************SUMMARY*************************
[INFO|main:1| 03/18/2015 20:34:57]: Total Accounts processed         :    7
[INFO|main:1| 03/18/2015 20:34:57]: Successfull Accounts             :    7
[INFO|main:1| 03/18/2015 20:34:57]: Failed accounts                  :    0
```

```
[INFO|main:1| 03/18/2015 20:34:57]: Total Migration Time(seconds)    :    157.949
[INFO|main:1| 03/18/2015 20:34:57]: ***********************************************
```