将系统用户导入FreeIPA中

1）ipa user-xxx命令报错
ipa: ERROR: did not receive Kerberos credentials
解决方案：重新执行kinit admin

参考
http://www.hadoop1024.com/2016/12/14/freeipa%E9%83%A8%E7%BD%B2%E6%AD%A5%E9%AA%A4/

系统用户导入

```
#!/bin/bash
for line in `grep "x:[5-9][0-9][0-9]:" /etc/passwd`
do
   USER=`echo $line | cut -d: -f1`
   FIRST=`echo $line | cut -d: -f5 | awk {'print $1'}`
   LAST=`echo $line | cut -d: -f5 | awk {'print $2'}`
   if [ ! "$FIRST" ]
   then
      FIRST=$USER
   fi
   if [ ! "$LAST" ]
   then
      LAST=$USER
   fi
   echo $USER | ipa user-add $USER --first=$FIRST --last=$LAST --
password
done
```

新用户自动创建家目录

修改客户端配置文件：

```
vi /etc/pam.d/system-auth
# add if you need ( create home directory automatically if it's none )
session     optional      pam_mkhomedir.so skel=/etc/skel umask=077

service oddjobd start #启动服务
```

系统组导入

```
ipa group-add hadoop
ipa group-add-member hadoop --users={yarn,knox,hdfs,atlas,mapred,druid,ranger}
```

参考 https://www.mankier.com/1/ipa#

Examples
ipa help commands
Display a list of available commands ipa help topics Display a high-level list of help topics ipa help user Display documentation and list of commands in the "user" topic.

ipa env
List IPA environmental variables and their values.

ipa user-add foo --first foo --last bar
Create a new user with username "foo", first name "foo" and last name "bar".

ipa group-add bar --desc "this is an example group"
Create a new group with name "bar" and description "this is an example group".

ipa group-add-member bar --users=foo
Add user "foo" to the group "bar".

ipa group-add-member bar --users={admin,foo}
Add users "admin" and "foo" to the group "bar". This approach depends on shell expansion feature.

ipa user-show foo --raw
Display user "foo" as (s)he is stored on the server.

ipa group-show bar --all
Display group "bar" and all of its attributes.

ipa config-mod --maxusername 20
Set maximum user name length to 20 characters.

ipa user-find foo
Search for all users with "foo" in either uid, first name, last name, full name, etc. A user with uid "foobar" would match the search criteria.

ipa user-find foo --first bar
Same as the previous example, except this time the users first name has to be exactly "bar". A user with uid "foobar" and first name "bar" would match the search criteria.

ipa user-find foo --first bar --last foo
A user with uid "foobar", first name "bar" and last name "foo" would match the search criteria.

ipa user-find
All users would match the search criteria (as there are none).

参考：https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/identity_management_guide/user-groups

```
[bjensen@server ~]$ ipa group-add groupName --desc="description" [--nonposix]
```

Additionally, there is one other configuration option, `--nonposix`. (By default, all groups are created as POSIX groups.) To enable interoperability with Windows users and groups and programs like Samba, it is possible to create non-POSIX groups by using the `--`

`nonposix`option. This option tells the script not to add the `posixGroup` object class to the entry.

For example:

```
[bjensen@server ~]$ ipa group-add examplegroup --desc="for examples" --nonposix

----------------------
Added group "examplegroup"
----------------------
  Group name: examplegroup
  Description: for examples
  GID: 855800010
```

The syntax of the `group-add-member` command requires only the group name and a comma-separated list of users to add:

```
[bjensen@server ~]$ ipa group-add-member groupName [--users=list] [--groups=list]
```

For example, this adds three users to the `engineering` group:

```
[bjensen@server ~]$ ipa group-add-member engineering --users=jsmith,bjensen,mreynolds
  Group name: engineering
  Description: for engineers
  GID: 387115842
  Member users: jsmith,bjensen,mreynolds
-------------------------
Number of members added 3
-------------------------
```

freeIPa 还不一样 要括号

ipa group-add-member hadoop --users={yarn,knox,hdfs,atlas,mapred,druid,ranger}

Likewise, other groups can be added as members, which creates nested groups:

```
[bjensen@server ~]$ ipa group-add-member engineering --groups=dev,qe1,dev2
  Group name: engineering
  Description: for engineers
  GID: 387115842
  Member groups: dev,qe1,dev2
  -------------------------
```

```
  Number of members added 3
  -------------------------
```

When displaying nested groups, members are listed as members and the members of any member groups are listed as indirect members. For example:

```
[bjensen@server ~]$ ipa group-show examplegroup
  Group name: examplegroup
  Description: for examples
  GID: 93200002
  Member users: jsmith,bjensen,mreynolds
  Member groups: californiausers
  Indirect Member users: sbeckett,acalavicci
```

It can take up to several minutes for the members of the child group to show up as members of the parent group. This is especially true on virtual machines where the nested groups have more than 500 members.

Note

When creating nested groups, be careful not to create *recursive* groups. For example, if GroupA is a member of GroupB, do not add GroupB as a member of GroupA. Recursive groups are not supported and can cause unpredictable behavior.

A group member is removed using the `group-remove-member` command.

```
[bjensen@server ~]$ ipa group-remove-member engineering --users=jsmith

  Group name: engineering
  Description: for engineers
  GID: 855800009
  Member users: bjensen,mreynolds
---------------------------
Number of members removed 1
----------------------------add-member group_name --users=user1 --users=user2 --
groups=group1
```