# IPA Server

## 防火墙设置

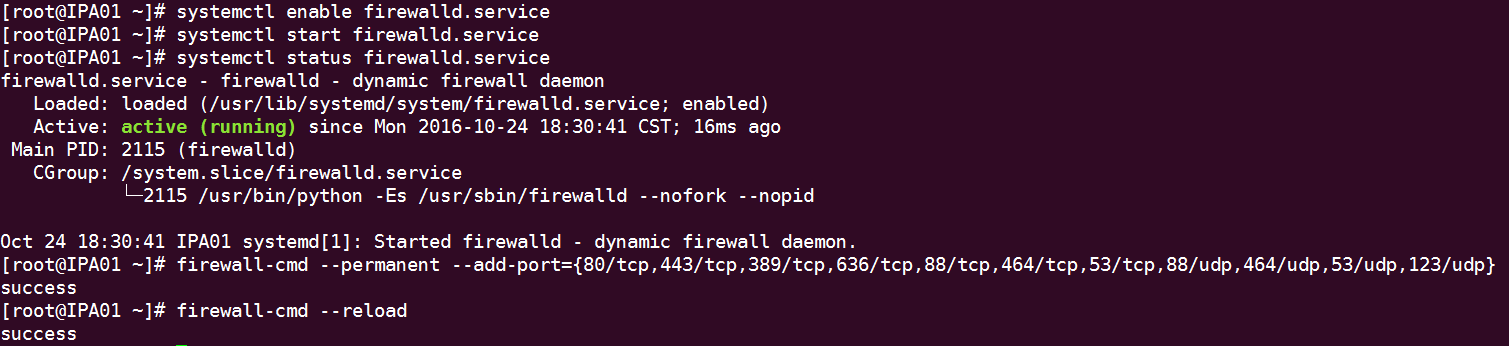
systemctl enable firewalld.service

systemctl start firewalld.service

systemctl status firewalld.service

firewall-cmd --permanent --add-port={80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,464/tcp,53/tcp,88/udp,464/udp,53/udp,123/udp}

firewall-cmd –reload



## Install

To install the packages required for a server with integrated DNS services：

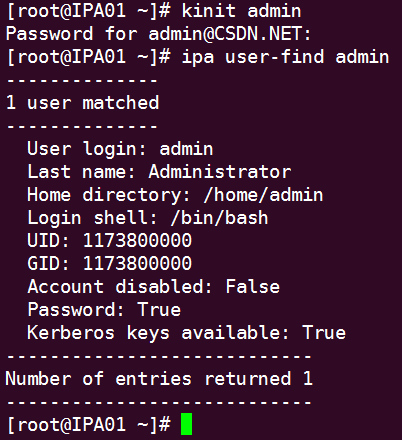
#yum install ipa-server ipa-server-dns

## 配置

# ipa-server-install



## 测试



## 启动和停止服务

ipactl start

ipactl stop

ipactl restart

## WEB UI

添加hosts

192.168.25.21 ipamaster.csdn.net

（需要使用火狐浏览器）

<https://ipamaster.csdn.net/ipa/ui/>

用户名：admin

密码：csdn.net

## 添加DNS记录

ipa dnsrecord-add csdn.net ipamaster --a-rec=192.168.25.21 --a-create-reverse

ipa dnsrecord-add csdn.net mysql --a-rec=192.168.25.22 --a-create-reverse

ipa dnsrecord-add csdn.net client01 --a-rec=192.168.25.23 --a-create-reverse

ipa dnsrecord-add csdn.net client02 --a-rec=192.168.25.24 --a-create-reverse

ipa dnsrecord-add csdn.net node01 --a-rec=192.168.25.25 --a-create-reverse

ipa dnsrecord-add csdn.net node02 --a-rec=192.168.25.26 --a-create-reverse

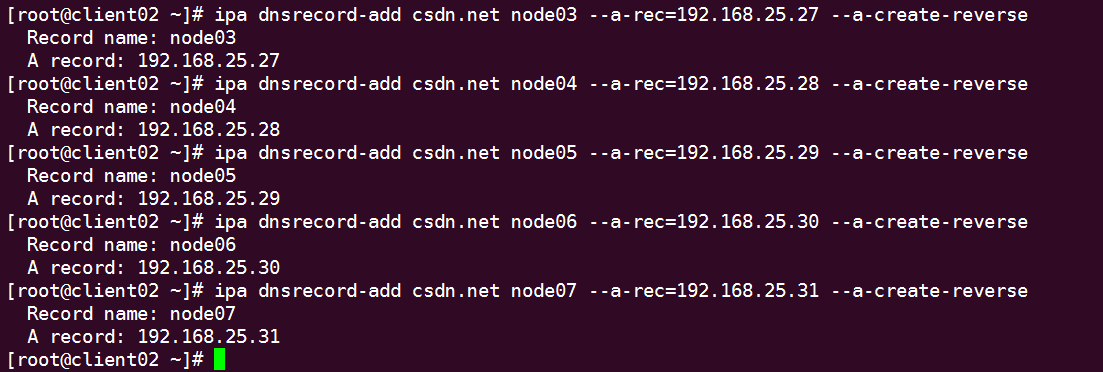
ipa dnsrecord-add csdn.net node03 --a-rec=192.168.25.27 --a-create-reverse

ipa dnsrecord-add csdn.net node04 --a-rec=192.168.25.28 --a-create-reverse

ipa dnsrecord-add csdn.net node05 --a-rec=192.168.25.29 --a-create-reverse

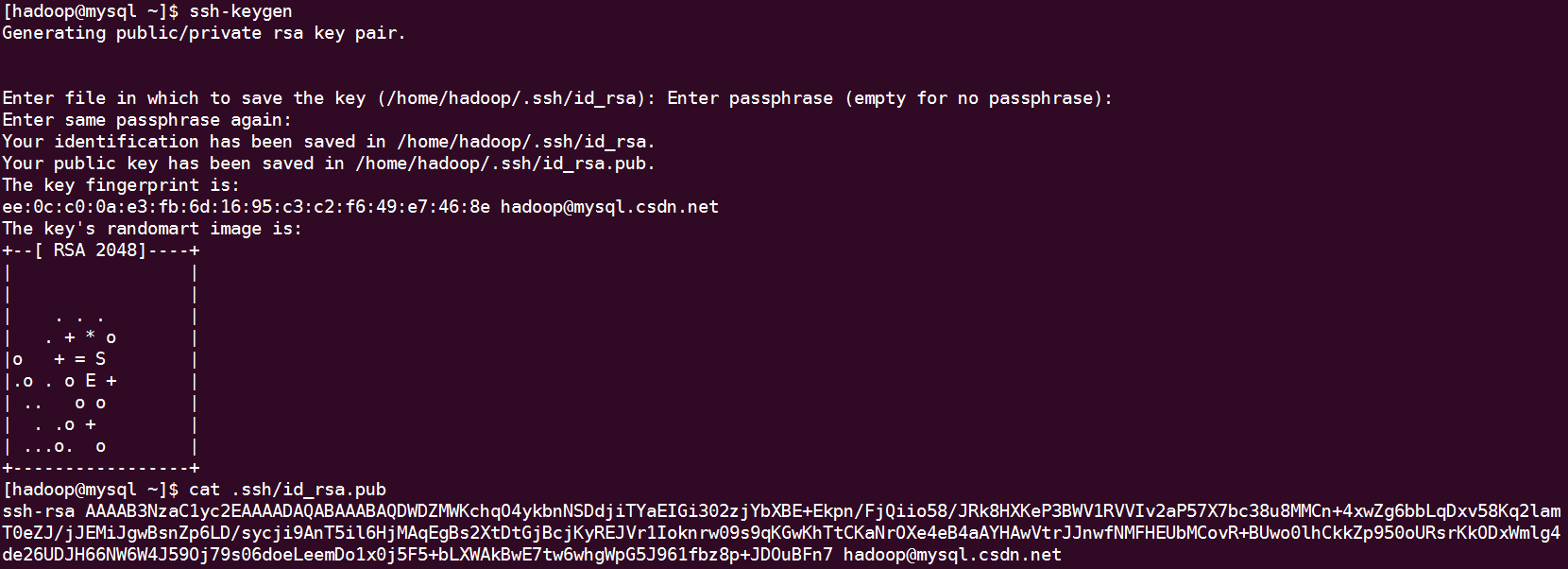
ipa dnsrecord-add csdn.net node06 --a-rec=192.168.25.30 --a-create-reverse

ipa dnsrecord-add csdn.net node07 --a-rec=192.168.25.31 --a-create-reverse

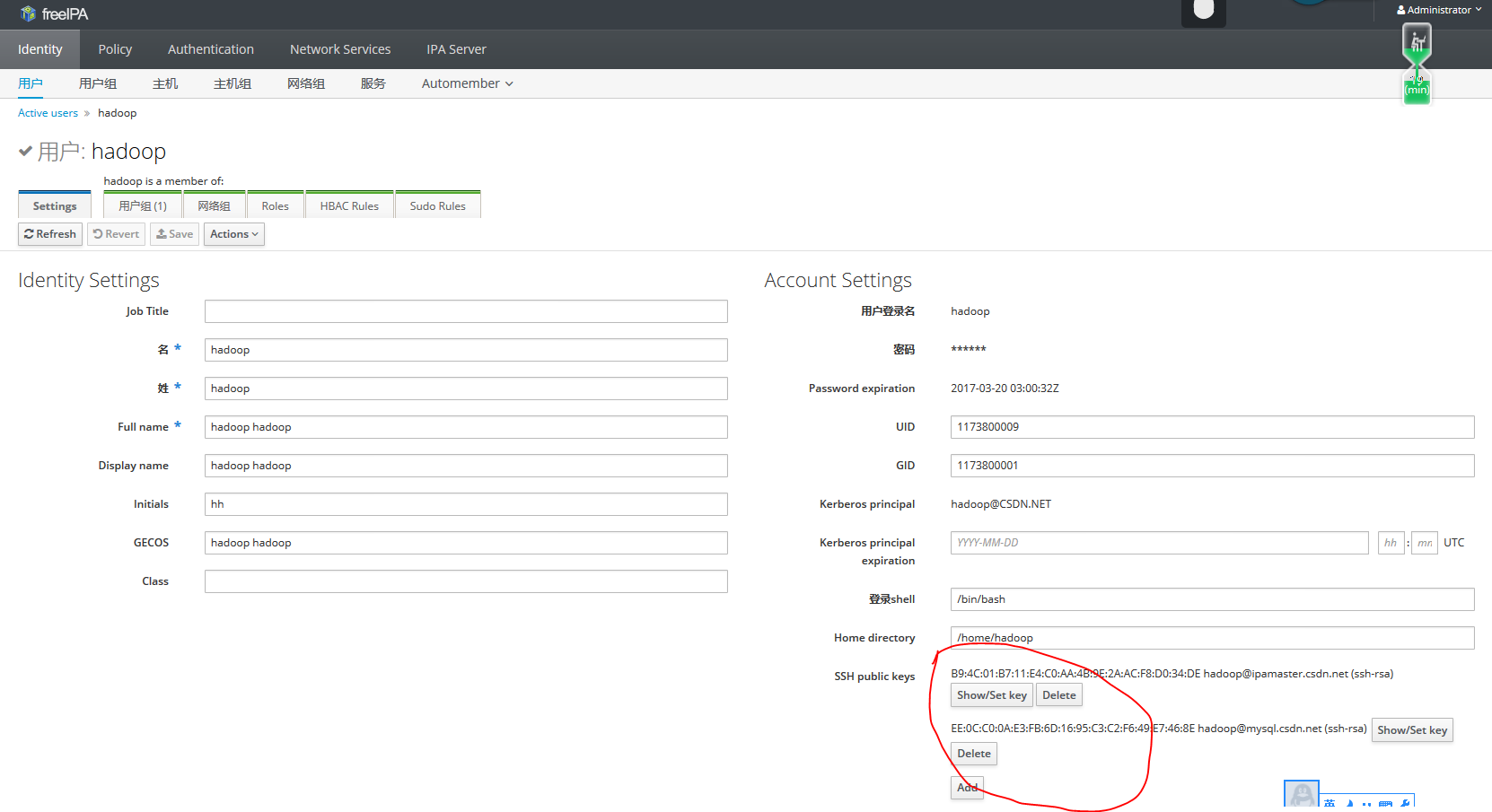


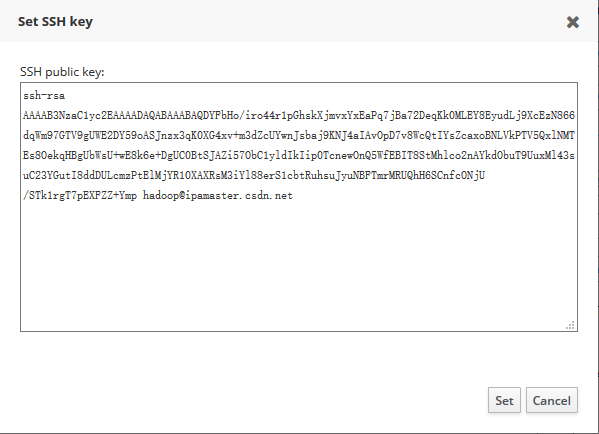
## 免密码登录

**Generat ing an SSH Key**



**Uploading User SSH Keys in the Web UI**



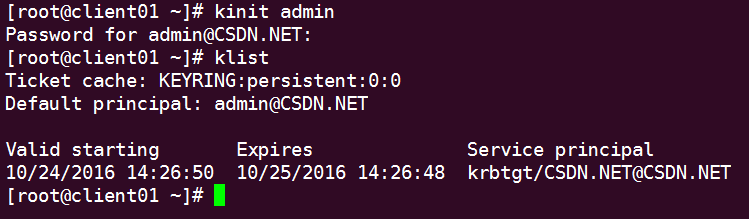


## 添加用户及用户组

要在ipamaster上或安装有*ipa-admintools的客户端上执行*

#yum install ipa-admintools

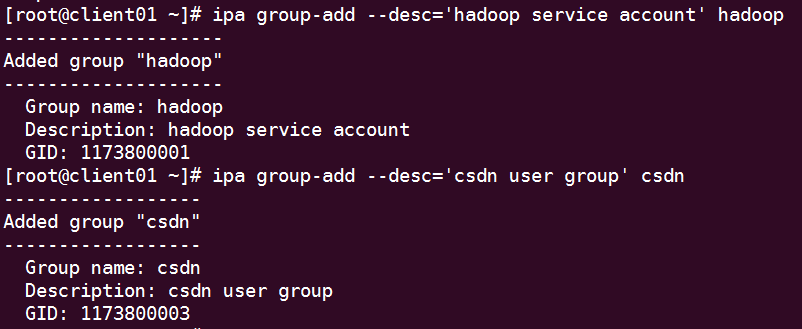
执行前要通过管理员认证：



### 添加用户组

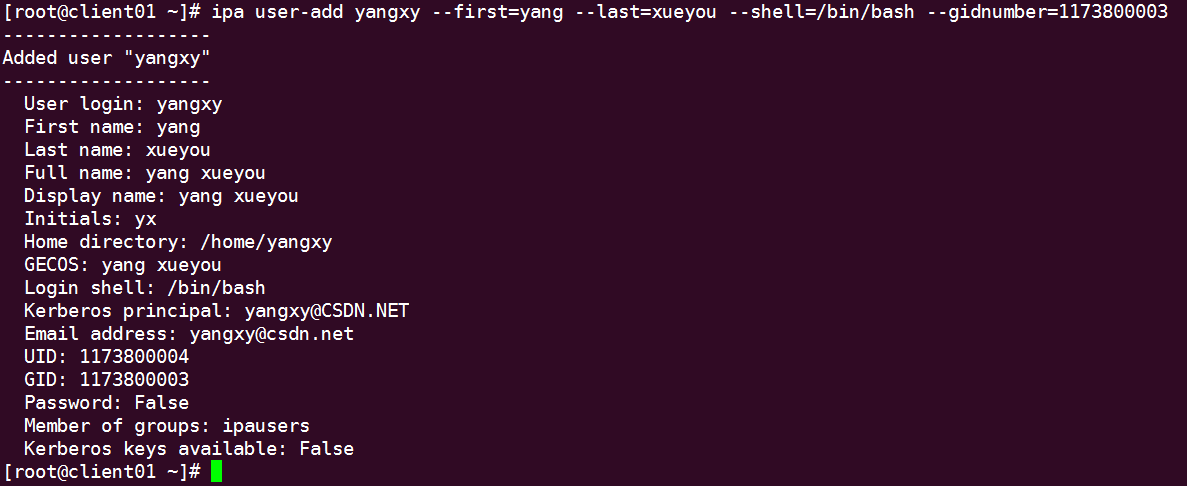
#ipa group-add --desc='hadoop service account' hadoop #添加hadoop组

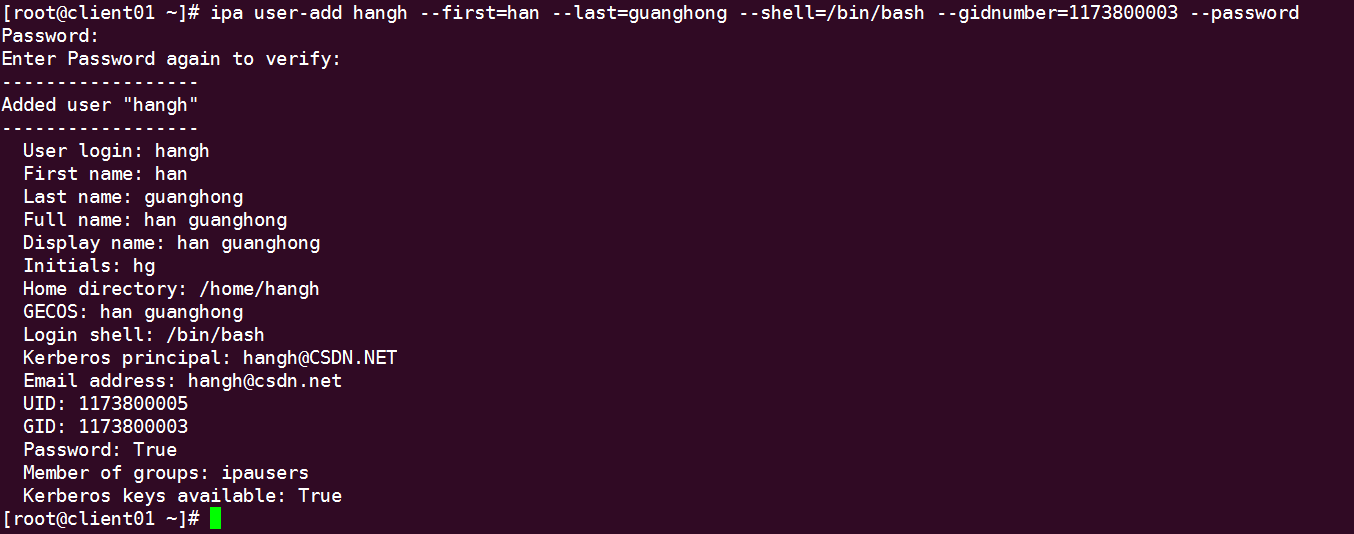
#ipa group-add --desc='csdn user group' csdn #添加csdn组



### 添加用户

ipa user-add yangxy --first=yang --last=xueyou --shell=/bin/bash --gidnumber=1040900500 --password



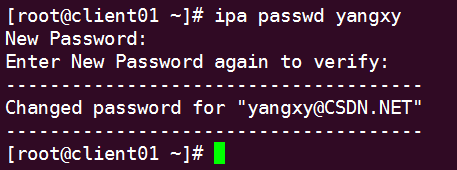


不添加私有用户组

ipa user-add hadoop --first=hadoop --last=hadoop --shell=/bin/bash --noprivate --gidnumber=1173800001 --password

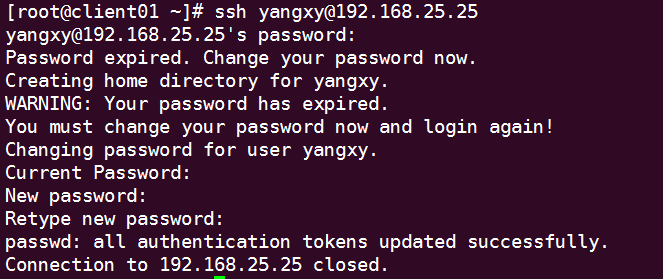
### 修改用户密码

[root@client01 ~]# ipa passwd yangxy



### 用户首次登录

用户首次登录需要修改密码



## Sudo

## 副本

# IPA Client

## 安装

#yum install ipa-client

## 配置

添加ipamaster到hosts

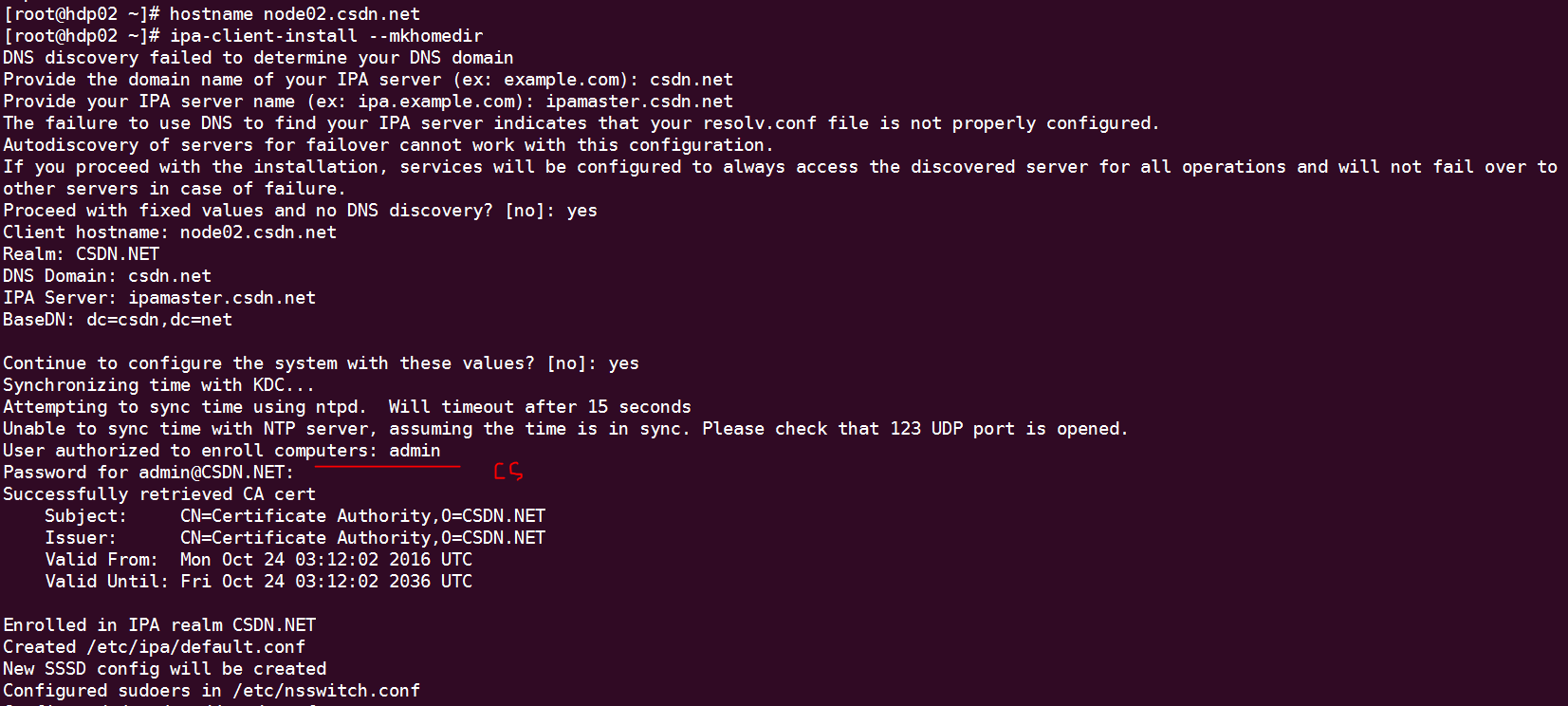
192.168.25.21 ipamaster.csdn.net

[root@hdp03 ~]# ntpdate 192.168.25.21 #如果和ipamaster时间差别比较大，kerberos会报错

[root@client01 ~]# hostnamectl --static set-hostname client01.csdn.net

[root@client01 ~]# ipa-client-install --mkhomedir

User authorized to enroll computers:用户名admin ，密码csdn.net



## 开机启动nis

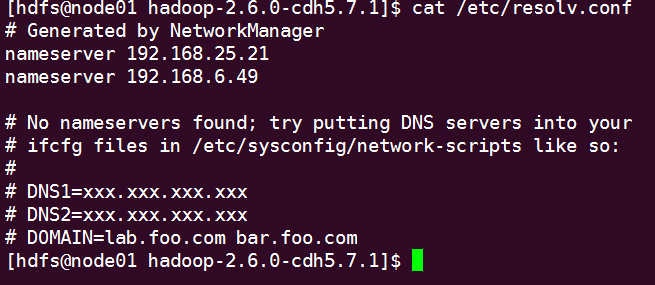
[root@node01 yangxy]# systemctl enable rhel-domainname.service

[root@node01 yangxy]# nisdomainname

csdn.net

## 配置DNS

将IPA Server 添加到DNS中



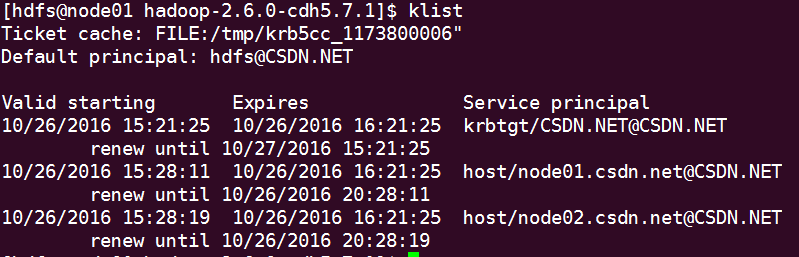
## 配置/etc/krb5.conf

修改default\_ccache\_name = FILE:/tmp/krb5cc\_%{uid}

重启SSSD服务

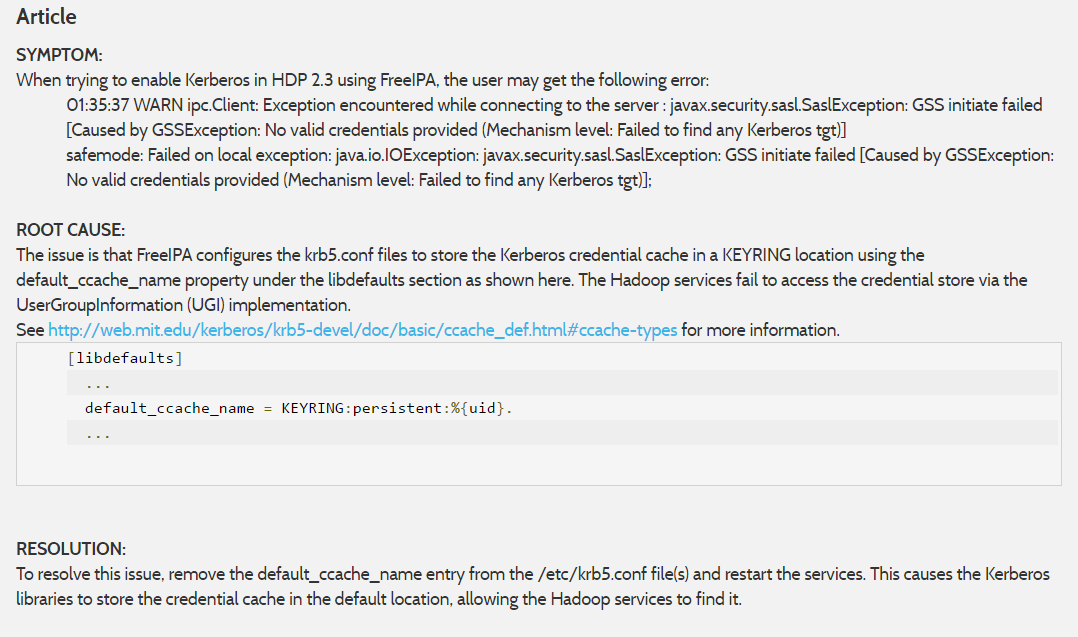
Systemctl restart sssd

确保Ticket cache: FILE（否则kerberos报错）



Exception encountered while connecting to the server : javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt)]

safemode: Failed on local exception: java.io.IOException: javax.security.sasl.SaslException: GSS initiate failed [Caused by GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos tgt)];



<https://community.hortonworks.com/questions/11288/kerberos-cache-in-ipa-redhat-idm-keyring-solved.html>

<http://ec2-52-89-10-2.us-west-2.compute.amazonaws.com/articles/49095/problem-enabling-kerberos-in-hdp-23-centos-7-using.html>

# Bug

<https://bugzilla.redhat.com/show_bug.cgi?id=1373427>