[root@ipa-client01 carlos]# vi /etc/hosts

```
192.168.100.200     ipa-server.example.com      ipa-server
192.168.100.205     ipa-replica.example.com     ipa-replica
192.168.100.201     ipa-client01.example.com    ipa-client01
192.168.100.202     ipa-client02.example.com    ipa-client02
```

[root@ipa-client01 carlos]# vi /etc/resolv.conf

```
search example.com

nameserver 192.168.100.200
nameserver 192.168.100.205
```

[root@ipa-client01 carlos]# dig example.com.

```
; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.2 <<>> example.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13059
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;example.com.                   IN      A

;; ANSWER SECTION:
example.com.            86400   IN      A       192.168.100.201
example.com.            86400   IN      A       192.168.100.202
example.com.            86400   IN      A       192.168.100.200
example.com.            86400   IN      A       192.168.100.205

;; AUTHORITY SECTION:
example.com.            86400   IN      NS      ipa-client01.example.com.
example.com.            86400   IN      NS      ipa-client02.example.com.
example.com.            86400   IN      NS      ipa-replica.example.com.
example.com.            86400   IN      NS      ipa-server.example.com.

;; ADDITIONAL SECTION:
ipa-server.example.com.       86400   IN      A       192.168.100.200
ipa-replica.example.com. 86400        IN      A       192.168.100.205
ipa-client01.example.com. 86400       IN      A       192.168.100.201
ipa-client02.example.com. 86400       IN      A       192.168.100.202

;; Query time: 1 msec
;; SERVER: 192.168.100.200#53(192.168.100.200)
;; WHEN: jue feb 23 18:18:01 CET 2017
;; MSG SIZE  rcvd: 273
```

[root@ipa-client01 carlos]# dig -x 192.168.100.201

```
; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.2 <<>> -x 192.168.100.201
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6508
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;201.100.168.192.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
201.100.168.192.in-addr.arpa. 86400 IN      PTR     ipa-client01.example.com.

;; AUTHORITY SECTION:
100.168.192.in-addr.arpa. 86400     IN      NS      ipa-client01.example.com.
100.168.192.in-addr.arpa. 86400     IN      NS      ipa-server.example.com.
100.168.192.in-addr.arpa. 86400     IN      NS      ipa-replica.example.com.
100.168.192.in-addr.arpa. 86400     IN      NS      ipa-client02.example.com.

;; ADDITIONAL SECTION:
ipa-server.example.com.       86400 IN      A       192.168.100.200
ipa-replica.example.com. 86400      IN      A       192.168.100.205
ipa-client01.example.com. 86400     IN      A       192.168.100.201
ipa-client02.example.com. 86400     IN      A       192.168.100.202

;; Query time: 1 msec
;; SERVER: 192.168.100.200#53(192.168.100.200)
;; WHEN: jue feb 23 18:19:11 CET 2017
;; MSG SIZE  rcvd: 251
```

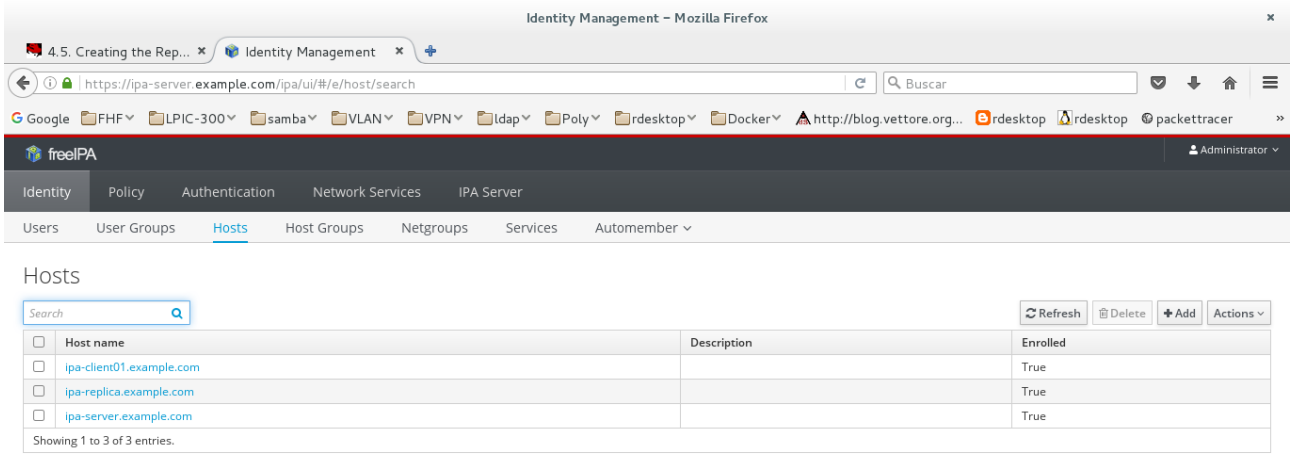
[root@ipa-client01 carlos]# yum install ipa-client ipa-admintools

```
[root@ipa-client01 carlos]# ipa-client-install --enable-dns-updates
DNS discovery failed to determine your DNS domain
Provide the domain name of your IPA server (ex: example.com): example.com
Provide your IPA server name (ex: ipa.example.com): ipa-server.example.com
The failure to use DNS to find your IPA server indicates that your resolv.conf file is not properly
configured.
Autodiscovery of servers for failover cannot work with this configuration.
If you proceed with the installation, services will be configured to always access the discovered
server for all operations and will not fail over to other servers in case of failure.
Proceed with fixed values and no DNS discovery? [no]: yes
Client hostname: ipa-client01.example.com
Realm: EXAMPLE.COM
```

DNS Domain: example.com
IPA Server: ipa-server.example.com
BaseDN: dc=example,dc=com

Continue to configure the system with these values? [no]: yes
Synchronizing time with KDC...
Attempting to sync time using ntpd. Will timeout after 15 seconds
Unable to sync time with NTP server, assuming the time is in sync. Please check that 123 UDP port is opened.
User authorized to enroll computers: admin
Password for admin@EXAMPLE.COM:
Successfully retrieved CA cert
    Subject: CN=Certificate Authority,O=EXAMPLE.COM
    Issuer: CN=Certificate Authority,O=EXAMPLE.COM
    Valid From: Thu Feb 23 12:21:12 2017 UTC
    Valid Until: Mon Feb 23 12:21:12 2037 UTC

Enrolled in IPA realm EXAMPLE.COM
Created /etc/ipa/default.conf
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm EXAMPLE.COM
trying https://ipa-server.example.com/ipa/json
Forwarding 'schema' to json server 'https://ipa-server.example.com/ipa/json'
trying https://ipa-server.example.com/ipa/session/json
Forwarding 'ping' to json server 'https://ipa-server.example.com/ipa/session/json'
Forwarding 'ca_is_enabled' to json server 'https://ipa-server.example.com/ipa/session/json'
Systemwide CA database updated.
Failed to update DNS records.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
Forwarding 'host_mod' to json server 'https://ipa-server.example.com/ipa/session/json'
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
No SRV records of NTP servers found. IPA server address will be used
NTP enabled
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring example.com as NIS domain.
Client configuration complete.



[root@ipa-client01 carlos]# vi /etc/sssd/sssd.conf

```
[domain/example.com]

cache_credentials = True
krb5_store_password_if_offline = True
ipa_domain = example.com
id_provider = ipa
auth_provider = ipa
access_provider = ipa
ipa_hostname = ipa-client01.example.com
chpass_provider = ipa
dyndns_update = True
ipa_server = _srv_, ipa-server.example.com
dyndns_iface = enp0s3
ldap_tls_cacert = /etc/ipa/ca.crt
[sssd]
services = nss, sudo, pam, ssh

domains = example.com
[nss]
homedir_substring = /home

[pam]

[sudo]

[autofs]
```

[ssh]

[pac]

[ifp]

[root@ipa-client01 carlos]# getent passwd admin
admin:*:794400000:794400000:Administrator:/home/admin:/bin/bash

[root@ipa-client01 carlos]# getent group admins
admins:*:794400000:admin

[root@ipa-server carlos]# kadmin.local
Authenticating as principal carlos/admin@EXAMPLE.COM with password.
kadmin.local: list_principals
admin@EXAMPLE.COM
K/M@EXAMPLE.COM
krbtgt/EXAMPLE.COM@EXAMPLE.COM
kadmin/ipa-server.example.com@EXAMPLE.COM
kadmin/admin@EXAMPLE.COM
kadmin/changepw@EXAMPLE.COM
kiprop/ipa-server.example.com@EXAMPLE.COM
ldap/ipa-server.example.com@EXAMPLE.COM
host/ipa-server.example.com@EXAMPLE.COM
dogtag/ipa-server.example.com@EXAMPLE.COM
HTTP/ipa-server.example.com@EXAMPLE.COM
host/ipa-replica.example.com@EXAMPLE.COM
ldap/ipa-replica.example.com@EXAMPLE.COM
HTTP/ipa-replica.example.com@EXAMPLE.COM
aurora@EXAMPLE.COM
host/ipa-client01.example.com@EXAMPLE.COM
kadmin.local:

[root@ipa-client01 carlos]# ktutil
ktutil: read_kt /etc/krb5.keytab
ktutil: l
slot KVNO Principal
---- ---- ---
   1   1 host/ipa-client01.example.com@EXAMPLE.COM
   2   1 host/ipa-client01.example.com@EXAMPLE.COM
ktutil: