```
# hostnamectl set-hostname ipa-server.example.com

# vi /etc/sysconfig/network-scripts/ifcfg-enp0s3

TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=enp0s3
UUID=1113030e-357b-44ba-939b-65289cbfbccb
DEVICE=enp0s3
ONBOOT=yes
NM_CONTROLLED=no
IPADDR=192.168.100.200
PREFIX=24
GATEWAY=192.168.100.1

# vi /etc/resolv.conf
search example.com

nameserver 192.168.100.200
nameserver 192.168.100.205

# yum install bind bind-utils
# yum install rng-tools

[root@ipa-server carlos]# systemctl start rngd
[root@ipa-server carlos]# systemctl enable rngd
[root@ipa-server carlos]# systemctl status rngd
● rngd.service - Hardware RNG Entropy Gatherer Daemon
   Loaded: loaded (/usr/lib/systemd/system/rngd.service; enabled; vendor preset: enabled)
   Active: active (running) since jue 2017-02-23 12:11:20 CET; 13s ago
 Main PID: 1983 (rngd)
   CGroup: /system.slice/rngd.service
           └─1983 /sbin/rngd -f

feb 23 12:11:20 ipa-server.example.com systemd[1]: Started Hardware RNG Entropy Gatherer
Daemon.
```

feb 23 12:11:20 ipa-server.example.com systemd[1]: Starting Hardware RNG Entropy Gatherer Daemon...
feb 23 12:11:20 ipa-server.example.com rngd[1983]: Unable to open file: /dev/tpm0

[root@ipa-server carlos]# vi /etc/named.conf

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
        listen-on port 53 { 192.168.100.0/24 ; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { 192.168.100.0/24 ; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
         - If you are building a RECURSIVE (caching) DNS server, you need to enable
           recursion.
         - If your recursive DNS server has a public IP address, you MUST enable access
           control to limit queries to your legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-enable no;
        dnssec-validation no;

        //forward only;

forwarders { 8.8.8.8 ;
                8.8.4.4 ;   };

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";
```

```
        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

zone "example.com" {
type master;
file "example.com.zone";
allow-update { none; };
};

zone "100.168.192.in-addr.arpa" {
type master;
file "example.com.revzone";
allow-update { none; };
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

```
[root@ipa-server carlos]# vi /var/named/example.com.zone
$TTL 86400
@ IN SOA ipa-server.example.com. root.example.com. (
 100 ; Serial
 1d ; refresh
 2h ; retry
 4w ; expire
 1h ) ; negative min cache

@ IN NS ipa-server.example.com.
@ IN NS ipa-replica.example.com.
@ IN NS ipa-client01.example.com.
@ IN NS ipa-client02.example.com.
```

```
ipa-server      IN A    192.168.100.200
ipa-replica     IN A    192.168.100.205
ipa-client01    IN A    192.168.100.201
ipa-client02    IN A    192.168.100.202


kb-server       IN CNAME        ipa-server.example.com.
kb-replica      IN CNAME        ipa-replica.example.com.
kb-client01     IN CNAME        ipa-client01.example.com.
kb-client02     IN CNAME        ipa-client02.example.com.
```

```
[root@ipa-server carlos]# vi /var/named/example.com.revzone

$TTL 86400
@ IN SOA ipa-server.example.com. root.example.com. (
 100 ; Serial
 1d ; refresh
 2h ; retry
 4w ; expire
 1h ) ; min cache

@       IN NS ipa-server.example.com.
@       IN NS ipa-replica.example.com.
@       IN NS ipa-client01.example.com.
@       IN NS ipa-client02.example.com.

200     IN PTR ipa-server.example.com.
205     IN PTR ipa-replica.example.com.
201     IN PTR ipa-client01.example.com.
202     IN PTR ipa-client02.example.com.

[root@ipa-server carlos]# systemctl enable named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to
/usr/lib/systemd/system/named.service.
[root@ipa-server carlos]# systemctl start named
[root@ipa-server carlos]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: active (running) since jue 2017-02-23 12:42:31 CET; 2s ago
  Process: 9496 ExecStart=/usr/sbin/named -u named $OPTIONS (code=exited,
status=0/SUCCESS)
  Process: 9493 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "yes" ]; then
/usr/sbin/named-checkconf -z /etc/named.conf; else echo "Checking of zone files is disabled"; fi
(code=exited, status=0/SUCCESS)
 Main PID: 9499 (named)
   CGroup: /system.slice/named.service
           └─9499 /usr/sbin/named -u named
```

```
feb 23 12:42:31 ipa-server.example.com named[9499]: zone 1.0.0.127.in-addr.arpa/IN: loaded serial
0
feb 23 12:42:31 ipa-server.example.com named[9499]: zone 100.168.192.in-addr.arpa/IN: loaded
serial 100
feb 23 12:42:31 ipa-server.example.com named[9499]: zone localhost.localdomain/IN: loaded serial
0
feb 23 12:42:31 ipa-server.example.com named[9499]: zone
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded serial 0
feb 23 12:42:31 ipa-server.example.com named[9499]: zone example.com/IN: loaded serial 100
feb 23 12:42:31 ipa-server.example.com named[9499]: all zones loaded
feb 23 12:42:31 ipa-server.example.com named[9499]: running
feb 23 12:42:31 ipa-server.example.com systemd[1]: Started Berkeley Internet Name Domain
(DNS).
feb 23 12:42:31 ipa-server.example.com named[9499]: zone example.com/IN: sending notifies
(serial 100)
feb 23 12:42:31 ipa-server.example.com named[9499]: zone 100.168.192.in-addr.arpa/IN: sending
notifies (serial 100)
Hint: Some lines were ellipsized, use -l to show in full.

[root@ipa-server 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: 48020
;; 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       192.168.100.200
example.com.            86400   IN      A       192.168.100.205
example.com.            86400   IN      A       192.168.100.202
example.com.            86400   IN      A       192.168.100.201

;; 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 12:43:31 CET 2017
;; MSG SIZE  rcvd: 273
```

```
[root@ipa-server carlos]# dig -x 192.168.100.200

; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.2 <<>> -x 192.168.100.200
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47938
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 5

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

;; ANSWER SECTION:
200.100.168.192.in-addr.arpa. 86400 IN      PTR     ipa-server.example.com.

;; AUTHORITY SECTION:
100.168.192.in-addr.arpa. 86400    IN      NS      ipa-server.example.com.
100.168.192.in-addr.arpa. 86400    IN      NS      ipa-client01.example.com.
100.168.192.in-addr.arpa. 86400    IN      NS      ipa-client02.example.com.
100.168.192.in-addr.arpa. 86400    IN      NS      ipa-replica.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: 0 msec
;; SERVER: 192.168.100.200#53(192.168.100.200)
;; WHEN: jue feb 23 12:44:28 CET 2017
;; MSG SIZE  rcvd: 251
```

```
[root@ipa-server carlos]# dig google.com.

; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.2 <<>> google.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37456
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 1
```

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

;; ANSWER SECTION:
google.com.             299     IN      A       216.58.201.142

;; AUTHORITY SECTION:
.                       140984          IN      NS      i.root-servers.net.
.                       140984          IN      NS      f.root-servers.net.
.                       140984          IN      NS      a.root-servers.net.
.                       140984          IN      NS      c.root-servers.net.
.                       140984          IN      NS      j.root-servers.net.
.                       140984          IN      NS      b.root-servers.net.
.                       140984          IN      NS      h.root-servers.net.
.                       140984          IN      NS      k.root-servers.net.
.                       140984          IN      NS      e.root-servers.net.
.                       140984          IN      NS      m.root-servers.net.
.                       140984          IN      NS      g.root-servers.net.
.                       140984          IN      NS      l.root-servers.net.
.                       140984          IN      NS      d.root-servers.net.

;; Query time: 81 msec
;; SERVER: 192.168.100.200#53(192.168.100.200)
;; WHEN: jue feb 23 12:46:06 CET 2017
;; MSG SIZE  rcvd: 266

[root@ipa-server carlos]# cat /proc/sys/kernel/random/entropy_avail
2978

[root@ipa-server carlos]#  dig +short ipa-server.example.com A
192.168.100.200
[root@ipa-server carlos]#  dig +short ipa-server.example.com AAA
192.168.100.200

[root@ipa-server carlos]# dig +short -x 192.168.100.200
ipa-server.example.com.

[root@ipa-server carlos]# dig +dnssec @8.8.8.8 . SOA

; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.2 <<>> +dnssec @8.8.8.8 . SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36435
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;.                              IN      SOA

;; ANSWER SECTION:
.                       51505   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2017022202
1800 900 604800 86400
.                       51505   IN      RRSIG           SOA 8 0 86400 20170307210000
20170222200000 61045 .
WgAyTNiyMeAzagyqtPitqC+6R0TQI4tE9mNLKvp5Uxa9/oKYL7Ajlb0Y
NlP2TWuifOQtIRWN9wKPfQVvsNGs0AwpsLeCHxtxDELDZ3hQg+BZlw6b
CVoKgwhN9IBpXWAi4/8Gmy+sytwoF+nGpcTeMBvDt7VnoBG+15ZTcDPb
qFbpKc3Mm7wzdkAVgIsY9pLIhXD6GpBze+lUQmK1jquVXMafk8Apvc41
3kVBpnTsXf4jJh4E70PoKYWVAClG9WxP+XuBIsZ3bG5qb09bORzasAzj
YtJN8uEmCYLlPBP+6trmAGx0dlhaFBr47ovGXidKV0P/tGVlJWZG2ucG Otigtw==

;; Query time: 56 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: jue feb 23 12:51:49 CET 2017
;; MSG SIZE  rcvd: 389

[root@ipa-server carlos]# dig +dnssec @8.8.4.4 . SOA

; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.2 <<>> +dnssec @8.8.4.4 . SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23563
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;.                              IN      SOA

;; ANSWER SECTION:
.                       40921   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2017022202
1800 900 604800 86400
.                       40921   IN      RRSIG           SOA 8 0 86400 20170307210000
20170222200000 61045 .
WgAyTNiyMeAzagyqtPitqC+6R0TQI4tE9mNLKvp5Uxa9/oKYL7Ajlb0Y
NlP2TWuifOQtIRWN9wKPfQVvsNGs0AwpsLeCHxtxDELDZ3hQg+BZlw6b
CVoKgwhN9IBpXWAi4/8Gmy+sytwoF+nGpcTeMBvDt7VnoBG+15ZTcDPb
qFbpKc3Mm7wzdkAVgIsY9pLIhXD6GpBze+lUQmK1jquVXMafk8Apvc41
3kVBpnTsXf4jJh4E70PoKYWVAClG9WxP+XuBIsZ3bG5qb09bORzasAzj
YtJN8uEmCYLlPBP+6trmAGx0dlhaFBr47ovGXidKV0P/tGVlJWZG2ucG Otigtw==
```

```
;; Query time: 64 msec
;; SERVER: 8.8.4.4#53(8.8.4.4)
;; WHEN: jue feb 23 12:52:39 CET 2017
;; MSG SIZE  rcvd: 389
```

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

```
192.168.100.200        ipa-server.example.com  ipa-server
```

```
[root@ipa-server carlos]# dig example.com. any
```

```
; <<>> DiG 9.9.4-RedHat-9.9.4-38.el7_3.2 <<>> example.com. any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9107
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 9, AUTHORITY: 0, ADDITIONAL: 5

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

;; ANSWER SECTION:
example.com.            86400   IN      SOA     ipa-server.example.com. root.example.com. 100 86400
7200 2419200 3600
example.com.            86400   IN      NS      ipa-client02.example.com.
example.com.            86400   IN      NS      ipa-client01.example.com.
example.com.            86400   IN      NS      ipa-server.example.com.
example.com.            86400   IN      NS      ipa-replica.example.com.
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
example.com.            86400   IN      A       192.168.100.201

;; 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 13:05:52 CET 2017
;; MSG SIZE  rcvd: 314
```

```
[root@ipa-server carlos]# yum install firewalld
```

```
[root@ipa-server carlos]# systemctl start firewalld.service
[root@ipa-server carlos]# systemctl enable firewalld.service
[root@ipa-server carlos]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since jue 2017-02-23 13:06:27 CET; 17s ago
     Docs: man:firewalld(1)
 Main PID: 9848 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─9848 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

feb 23 13:06:27 ipa-server.example.com systemd[1]: Starting firewalld - dynamic firewall
daemon...
feb 23 13:06:27 ipa-server.example.com systemd[1]: Started firewalld - dynamic firewall daemon.

[root@ipa-server carlos]# 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}
success
[root@ipa-server carlos]# firewall-cmd --reload
success

[root@ipa-server carlos]# firewall-cmd --list-ports
443/tcp 80/tcp 464/tcp 88/udp 464/udp 88/tcp 123/udp 389/tcp 53/tcp 53/udp 636/tcp
[root@ipa-server carlos]# yum install ipa-server ipa-server-dns

[root@ipa-server carlos]# ipa-server-install

The log file for this installation can be found in /var/log/ipaserver-install.log
==============================================================================
=======
This program will set up the IPA Server.

This includes:
  * Configure a stand-alone CA (dogtag) for certificate management
  * Configure the Network Time Daemon (ntpd)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)

To accept the default shown in brackets, press the Enter key.

Do you want to configure integrated DNS (BIND)? [no]: no

Enter the fully qualified domain name of the computer
on which you're setting up server software. Using the form
<hostname>.<domainname>
Example: master.example.com.
```

Server host name [ipa-server.example.com]:

The domain name has been determined based on the host name.

Please confirm the domain name [example.com]:

The kerberos protocol requires a Realm name to be defined.
This is typically the domain name converted to uppercase.

Please provide a realm name [EXAMPLE.COM]:
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and has full access
to the Directory for system management tasks and will be added to the
instance of directory server created for IPA.
The password must be at least 8 characters long.

Directory Manager password:
Password (confirm):

The IPA server requires an administrative user, named 'admin'.
This user is a regular system account used for IPA server administration.

IPA admin password:
Password (confirm):

The IPA Master Server will be configured with:
Hostname: ipa-server.example.com
IP address(es): 192.168.100.200
Domain name: example.com
Realm name: EXAMPLE.COM

Continue to configure the system with these values? [no]: yes

The following operations may take some minutes to complete.
Please wait until the prompt is returned.

Configuring NTP daemon (ntpd)
[1/4]: stopping ntpd
[2/4]: writing configuration
[3/4]: configuring ntpd to start on boot
[4/4]: starting ntpd
Done configuring NTP daemon (ntpd).
Configuring directory server (dirsrv). Estimated time: 1 minute
[1/47]: creating directory server user
[2/47]: creating directory server instance
[3/47]: updating configuration in dse.ldif

```
  [4/47]: restarting directory server
  [5/47]: adding default schema
  [6/47]: enabling memberof plugin
  [7/47]: enabling winsync plugin
  [8/47]: configuring replication version plugin
  [9/47]: enabling IPA enrollment plugin
  [10/47]: enabling ldapi
  [11/47]: configuring uniqueness plugin
  [12/47]: configuring uuid plugin
  [13/47]: configuring modrdn plugin
  [14/47]: configuring DNS plugin
  [15/47]: enabling entryUSN plugin
  [16/47]: configuring lockout plugin
  [17/47]: configuring topology plugin
  [18/47]: creating indices
  [19/47]: enabling referential integrity plugin
  [20/47]: configuring certmap.conf
  [21/47]: configure autobind for root
  [22/47]: configure new location for managed entries
  [23/47]: configure dirsrv ccache
  [24/47]: enabling SASL mapping fallback
  [25/47]: restarting directory server
  [26/47]: adding sasl mappings to the directory
  [27/47]: adding default layout
  [28/47]: adding delegation layout
  [29/47]: creating container for managed entries
  [30/47]: configuring user private groups
  [31/47]: configuring netgroups from hostgroups
  [32/47]: creating default Sudo bind user
  [33/47]: creating default Auto Member layout
  [34/47]: adding range check plugin
  [35/47]: creating default HBAC rule allow_all
  [36/47]: adding sasl mappings to the directory
  [37/47]: adding entries for topology management
  [38/47]: initializing group membership
  [39/47]: adding master entry
  [40/47]: initializing domain level
  [41/47]: configuring Posix uid/gid generation
  [42/47]: adding replication acis
  [43/47]: enabling compatibility plugin
  [44/47]: activating sidgen plugin
  [45/47]: activating extdom plugin
  [46/47]: tuning directory server
  [47/47]: configuring directory to start on boot
Done configuring directory server (dirsrv).
Configuring certificate server (pki-tomcatd). Estimated time: 3 minutes 30 seconds
  [1/31]: creating certificate server user
  [2/31]: configuring certificate server instance
```

```
  [3/31]: stopping certificate server instance to update CS.cfg
  [4/31]: backing up CS.cfg
  [5/31]: disabling nonces
  [6/31]: set up CRL publishing
  [7/31]: enable PKIX certificate path discovery and validation
  [8/31]: starting certificate server instance
  [9/31]: creating RA agent certificate database
  [10/31]: importing CA chain to RA certificate database
  [11/31]: fixing RA database permissions
  [12/31]: setting up signing cert profile
  [13/31]: setting audit signing renewal to 2 years
  [14/31]: restarting certificate server
  [15/31]: requesting RA certificate from CA
  [16/31]: issuing RA agent certificate
  [17/31]: adding RA agent as a trusted user
  [18/31]: authorizing RA to modify profiles
  [19/31]: authorizing RA to manage lightweight CAs
  [20/31]: Ensure lightweight CAs container exists
  [21/31]: configure certmonger for renewals
  [22/31]: configure certificate renewals
  [23/31]: configure RA certificate renewal
  [24/31]: configure Server-Cert certificate renewal
  [25/31]: Configure HTTP to proxy connections
  [26/31]: restarting certificate server
  [27/31]: migrating certificate profiles to LDAP
  [28/31]: importing IPA certificate profiles
  [29/31]: adding default CA ACL
  [30/31]: adding 'ipa' CA entry
  [31/31]: updating IPA configuration
Done configuring certificate server (pki-tomcatd).
Configuring directory server (dirsrv). Estimated time: 10 seconds
  [1/3]: configuring ssl for ds instance
  [2/3]: restarting directory server
  [3/3]: adding CA certificate entry
Done configuring directory server (dirsrv).
Configuring Kerberos KDC (krb5kdc). Estimated time: 30 seconds
  [1/9]: adding kerberos container to the directory
  [2/9]: configuring KDC
  [3/9]: initialize kerberos container
  [4/9]: adding default ACIs
  [5/9]: creating a keytab for the directory
  [6/9]: creating a keytab for the machine
  [7/9]: adding the password extension to the directory
  [8/9]: starting the KDC
  [9/9]: configuring KDC to start on boot
Done configuring Kerberos KDC (krb5kdc).
Configuring kadmin
  [1/2]: starting kadmin
```

```
  [2/2]: configuring kadmin to start on boot
Done configuring kadmin.
Configuring ipa_memcached
  [1/2]: starting ipa_memcached
  [2/2]: configuring ipa_memcached to start on boot
Done configuring ipa_memcached.
Configuring ipa-otpd
  [1/2]: starting ipa-otpd
  [2/2]: configuring ipa-otpd to start on boot
Done configuring ipa-otpd.
Configuring ipa-custodia
  [1/5]: Generating ipa-custodia config file
  [2/5]: Making sure custodia container exists
  [3/5]: Generating ipa-custodia keys
  [4/5]: starting ipa-custodia
  [5/5]: configuring ipa-custodia to start on boot
Done configuring ipa-custodia.
Configuring the web interface (httpd). Estimated time: 1 minute
  [1/21]: setting mod_nss port to 443
  [2/21]: setting mod_nss cipher suite
  [3/21]: setting mod_nss protocol list to TLSv1.0 - TLSv1.2
  [4/21]: setting mod_nss password file
  [5/21]: enabling mod_nss renegotiate
  [6/21]: adding URL rewriting rules
  [7/21]: configuring httpd
  [8/21]: configure certmonger for renewals
  [9/21]: setting up httpd keytab
  [10/21]: setting up ssl
  [11/21]: importing CA certificates from LDAP
  [12/21]: setting up browser autoconfig
  [13/21]: publish CA cert
  [14/21]: clean up any existing httpd ccache
  [15/21]: configuring SELinux for httpd
  [16/21]: create KDC proxy user
  [17/21]: create KDC proxy config
  [18/21]: enable KDC proxy
  [19/21]: restarting httpd
  [20/21]: configuring httpd to start on boot
  [21/21]: enabling oddjobd
Done configuring the web interface (httpd).
Applying LDAP updates
Upgrading IPA:
  [1/9]: stopping directory server
  [2/9]: saving configuration
  [3/9]: disabling listeners
  [4/9]: enabling DS global lock
  [5/9]: starting directory server
  [6/9]: upgrading server
```

```
  [7/9]: stopping directory server
  [8/9]: restoring configuration
  [9/9]: starting directory server
Done.
Restarting the directory server
Restarting the KDC
Please add records in this file to your DNS system: /tmp/ipa.system.records.QXgIgR.db
Restarting the web server
Configuring client side components
Using existing certificate '/etc/ipa/ca.crt'.
Client hostname: ipa-server.example.com
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: ipa-server.example.com
BaseDN: dc=example,dc=com

Skipping synchronizing time with NTP server.
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
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.
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
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring example.com as NIS domain.
Client configuration complete.

==============================================================================
=======
Setup complete

Next steps:
        1. You must make sure these network ports are open:
                TCP Ports:
                  * 80, 443: HTTP/HTTPS
                  * 389, 636: LDAP/LDAPS
                  * 88, 464: kerberos
```

UDP Ports:
  * 88, 464: kerberos
  * 123: ntp

2. You can now obtain a kerberos ticket using the command: 'kinit admin'
   This ticket will allow you to use the IPA tools (e.g., ipa user-add)
   and the web user interface.

Be sure to back up the CA certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these
files is the Directory Manager password

```
[root@ipa-server carlos]# ipa-backup
Preparing backup on ipa-server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Backed up to /var/lib/ipa/backup/ipa-full-2017-02-23-14-04-03
Starting IPA service
The ipa-backup command was successful
[root@ipa-server carlos]# ls /var/lib/ipa/backup/
ipa-full-2017-02-23-14-04-03

[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
kadmin.local:

[root@ipa-server carlos]# klist -k /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   2 host/ipa-server.example.com@EXAMPLE.COM
```

```
   2 host/ipa-server.example.com@EXAMPLE.COM
   2 host/ipa-server.example.com@EXAMPLE.COM
   2 host/ipa-server.example.com@EXAMPLE.COM
   2 host/ipa-server.example.com@EXAMPLE.COM
   2 host/ipa-server.example.com@EXAMPLE.COM
[root@ipa-server carlos]# ktutil
ktutil:  read_kt /etc/krb5.keytab
ktutil:  list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
   1    2  host/ipa-server.example.com@EXAMPLE.COM
   2    2  host/ipa-server.example.com@EXAMPLE.COM
   3    2  host/ipa-server.example.com@EXAMPLE.COM
   4    2  host/ipa-server.example.com@EXAMPLE.COM
   5    2  host/ipa-server.example.com@EXAMPLE.COM
   6    2  host/ipa-server.example.com@EXAMPLE.COM
ktutil:

[root@ipa-server carlos]# kinit admin
Password for admin@EXAMPLE.COM:
[root@ipa-server carlos]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@EXAMPLE.COM

Valid starting     Expires            Service principal
23/02/17 14:07:42  24/02/17 14:07:38  krbtgt/EXAMPLE.COM@EXAMPLE.COM

[root@ipa-server 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
```