Objetivo:

→ ***Instalar** server1.example.com **como** IPA Server.*
  ↘ ***Parámetros de conexión:***
  192.168.1.150 server1.example.com server1
  192.168.1.151 station1.example.com station1
→ ***Crear usuarios:** ldapuser{1..3}*
→ ***Instalar** station1.example.com **como** IPA Client*
→ ***Autenticación ssh con:** ldapuser{1..3} **desde:** station1**con shell:** → /bin/bash **y home:** → /home/ldapuser{1..3}*

++
(Tiempo máximo estimado → 20 minutos)...
++

[root@server1 ~]# yum install ipa-server
[root@server1 ~]# 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)
  * Configure the KDC to enable PKINIT

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

WARNING: conflicting time&date synchronization service 'chronyd' will be disabled
in favor of ntpd

Do you want to configure integrated DNS (BIND)? [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 [server1.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: server1.example.com
IP address(es): 192.168.1.150
Domain name: example.com
Realm name: EXAMPLE.COM

Continue to configure the system with these values? [no]: yes
…
==========
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@server1 ~]# ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
httpd Service: RUNNING
ipa-custodia Service: RUNNING
ntpd Service: RUNNING
pki-tomcatd Service: RUNNING
ipa-otpd Service: RUNNING
ipa: INFO: The ipactl command was successful

[root@server1 ~]# firewall-cmd --permanent --add-
port={80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,464/tcp,88/udp,464/udp,123/udp}
success
[root@server1 ~]# firewall-cmd --reload
success
[root@server1 ~]# firewall-cmd --list-ports
80/tcp 443/tcp 389/tcp 636/tcp 88/tcp 464/tcp 88/udp 464/udp 123/udp

[root@server1 ~]# kinit admin
Password for admin@EXAMPLE.COM:
[root@server1 ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@EXAMPLE.COM

Valid starting     Expires            Service principal
26/04/18 11:57:24  27/04/18 11:57:20  krbtgt/EXAMPLE.COM@EXAMPLE.COM

[root@server1 ~]# ipa config-mod --defaultshell=/bin/bash
  Largo máximo para nombre de usuario: 32
  Base del directorio principal: /home
  Shell predeterminada: /bin/bash
  Grupo de usuarios predeterminado: ipausers
  Dominio de correo electrónico por defecto: example.com
  Buscar límite de tiempo: 2
  Límite del tamaño de la búsqueda: 100
  Campos de búsqueda de usuario: uid,givenname,sn,telephonenumber,ou,title
  Group search fields: cn,description
  Habilitar modo migración: FALSE
  Base de certificado de asunto: O=EXAMPLE.COM
  Notificación de Expiración de Contraseña (días): 4
  Funciones del complemento de contraseña: AllowNThash, KDC:Disable Last Success
  SELinux user map order: guest_u:s0$xguest_u:s0$user_u:s0$staff_u:s0-
        s0:c0.c1023$unconfined_u:s0-s0:c0.c1023
  Default SELinux user: unconfined_u:s0-s0:c0.c1023
  Default PAC types: MS-PAC, nfs:NONE
```

IPA masters: server1.example.com
IPA CA servers: server1.example.com
IPA NTP servers: server1.example.com
IPA CA renewal master: server1.example.com
IPA master capable of PKINIT: server1.example.com

[root@server1 ~]# ipa user-add ldapuser1 --first=ldapuser1 --last=ldapuser1 --password
Contraseña:
Ingrese Contraseña nuevamente para verificar:

Ha sido agregado el usuario "ldapuser1"

Ingreso de usuario: ldapuser1
Nombre: ldapuser1
Apellido: ldapuser1
Nombre y apellidos: ldapuser1 ldapuser1
Mostrar nombre: ldapuser1 ldapuser1
Iniciales: ll
Directorio principal: /home/ldapuser1
GECOS: ldapuser1 ldapuser1
Shell de ingreso: /bin/bash
Nombre principal: ldapuser1@EXAMPLE.COM
Principal alias: ldapuser1@EXAMPLE.COM
Dirección de correo electrónico: ldapuser1@example.com
UID: 938600001
GID: 938600001
Contraseña: True
Miembros de los grupos: ipausers
Claves Kerberos disponibles: True

[root@server1 ~]# ipa user-add ldapuser2 --first=ldapuser2 --last=ldapuser2 --password
Contraseña:
Ingrese Contraseña nuevamente para verificar:

Ha sido agregado el usuario "ldapuser2"

…

[root@server1 ~]# ipa user-add ldapuser3 --first=ldapuser3 --last=ldapuser3 --password
Contraseña:
Ingrese Contraseña nuevamente para verificar:

Ha sido agregado el usuario "ldapuser3"

...
[root@server1 ~]# ipa user-find
---
4 usuarios coincidentes

Ingreso de usuario: **admin**
Apellido: Administrator
Directorio principal: /home/admin
Shell de ingreso: /bin/bash
Principal alias: admin@EXAMPLE.COM
UID: 938600000
GID: 938600000
Cuenta inhabilitada : False

Ingreso de usuario: **ldapuser1**
Nombre: ldapuser1
Apellido: ldapuser1
Directorio principal: /home/ldapuser1
Shell de ingreso: /bin/bash
Nombre principal: ldapuser1@EXAMPLE.COM
Principal alias: ldapuser1@EXAMPLE.COM
Dirección de correo electrónico: ldapuser1@example.com
UID: 938600001
GID: 938600001
Cuenta inhabilitada : False

Ingreso de usuario: **ldapuser2**
Nombre: ldapuser2
Apellido: ldapuser2
Directorio principal: /home/ldapuser2
Shell de ingreso: /bin/bash
Nombre principal: ldapuser2@EXAMPLE.COM
Principal alias: ldapuser2@EXAMPLE.COM
Dirección de correo electrónico: ldapuser2@example.com
UID: 938600003
GID: 938600003
Cuenta inhabilitada : False

Ingreso de usuario: **ldapuser3**
Nombre: ldapuser3
Apellido: ldapuser3
Directorio principal: /home/ldapuser3
Shell de ingreso: /bin/bash
Nombre principal: ldapuser3@EXAMPLE.COM
Principal alias: ldapuser3@EXAMPLE.COM
Dirección de correo electrónico: ldapuser3@example.com
UID: 938600004
GID: 938600004
Cuenta inhabilitada : False

Cantidad de entradas devueltas 4

```
[root@server1 ~]# ipa host-find
--------------------
1 equipo coincidente
--------------------
  Nombre del equipo: server1.example.com
  Nombre principal: host/server1.example.com@EXAMPLE.COM
  Principal alias: host/server1.example.com@EXAMPLE.COM
  SSH public key fingerprint: SHA256:hsoJrtGbcaFIIIhtN2eSk2z4rTx25vlheKDxJjERa6w (ssh-
rsa), SHA256:tKrxWBBgusdB247Qs9CTfhQdhKro4etkZi3O+WGFK0I (ecdsa-sha2-    nistp256),
   SHA256:E4yLQHOqh1Ua9xMHU8NlfjA8Tjiq0A+jHBCAwpH1WBo (ssh-ed25519)
----------------------------
Cantidad de entradas devueltas 1
----------------------------

[root@server1 ~]# authconfig --enablemkhomedir  --update
```

↘station1

```
[root@station1 ~]# yum install ipa-client
[root@station1 ~]# firewall-cmd --permanent –add-port=123/udp
[root@station1 ~]# firewall-cmd --reload
[root@station1 ~]# ipa-client-install --force-ntpd

[root@station1 ~]# authconfig --enablemkhomedir --update
[root@station1 ~]# authconfig --winbindtemplateshell=/bin/bash --update

[root@server1 ~]# getent passwd ldapuser{1..3}
ldapuser1:*:938600001:938600001:ldapuser1 ldapuser1:/home/ldapuser1:/bin/bash
ldapuser2:*:938600003:938600003:ldapuser2 ldapuser2:/home/ldapuser2:/bin/bash
ldapuser3:*:938600004:938600004:ldapuser3 ldapuser3:/home/ldapuser3:/bin/bash

[root@station1 ~]# ssh ldapuser2@server1
Password:
Password expired. Change your password now.
Current Password:
New password:
Retype new password:
Creating home directory for ldapuser2.
[ldapuser2@server1 ~]$ pwd
/home/ldapuser2

[ldapuser2@server1 ~]$ kinit ldapuser1
Password for ldapuser1@EXAMPLE.COM:
[ldapuser2@server1 ~]$ klist
Ticket cache: KEYRING:persistent:938600003:krb_ccache_Jjp363Q
Default principal: ldapuser1@EXAMPLE.COM
```

Valid starting Expires Service principal
01/05/18 09:28:13 02/05/18 09:28:09 krbtgt/EXAMPLE.COM@EXAMPLE.COM

[ldapuser2@server1 ~]$ ipa host-find

---
2 equipos coincidentes

Nombre del equipo: **server1.example.com**
Nombre principal: host/server1.example.com@EXAMPLE.COM
Principal alias: host/server1.example.com@EXAMPLE.COM
SSH public key fingerprint: SHA256:hsoJrtGbcaFIIIhtN2eSk2z4rTx25vlheKDxJjERa6w (ssh-rsa), SHA256:tKrxWBBgusdB247Qs9CTfhQdhKro4etkZi3O+WGFK0I (ecdsa-sha2-nistp256), SHA256:E4yLQHOqh1Ua9xMHU8NlfjA8Tjiq0A+jHBCAwpH1WBo (ssh-ed25519)

Nombre del equipo: **station1.example.com**
Nombre principal: host/station1.example.com@EXAMPLE.COM
Principal alias: host/station1.example.com@EXAMPLE.COM
SSH public key fingerprint: SHA256:hsoJrtGbcaFIIIhtN2eSk2z4rTx25vlheKDxJjERa6w (ssh-rsa), SHA256:tKrxWBBgusdB247Qs9CTfhQdhKro4etkZi3O+WGFK0I (ecdsa-sha2-nistp256), SHA256:E4yLQHOqh1Ua9xMHU8NlfjA8Tjiq0A+jHBCAwpH1WBo (ssh-ed25519)

Cantidad de entradas devueltas 2
