

FreeIPA

FreeIPA

RHEL []

[1]

FreeIPA

```
[root@dlp ~]# dnf -y install freeipa-server freeipa-server-dns freeipa-client
```

[2]

DNS FreeIPA

```
# add own hostname
```

```
[root@dlp ~]# echo '10.0.0.40 dlp.ipa.srv.world dlp' >> /etc/hosts
```

```
[root@dlp ~]# ipa-server-install --setup-dns
```

The log file for this installation can be found in /var/log/ipaserver-install.log

=====

This program will set up the IPA Server.

Version 4.9.7

This includes:

- * Configure a stand-alone CA (dogtag) for certificate management
- * Configure the NTP client (chronyd)
- * Create and configure an instance of Directory Server
- * Create and configure a Kerberos Key Distribution Center (KDC)
- * Configure Apache (httpd)
- * Configure DNS (bind)
- * Configure the KDC to enable PKINIT

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

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.

```
# confirm hostname and Enter
```

```
Server host name [ dlp.ipa.srv.world ]:
```

Warning: skipping DNS resolution of host dlp.ipa.srv.world
The domain name has been determined based on the host name.

confirm domain name and Enter

Please confirm the domain name [ipa.srv.world]:

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

confirm realm name and Enter

Please provide a realm name [IPA.SRV.WORLD]:

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.

set Directory Manager password

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.

set IPA admin password

IPA admin password:

Password (confirm):

Checking DNS domain ipa.srv.world., please wait ...

if you set DNS forwarder, answer [yes]

Do you want to configure DNS forwarders? [yes]:

The following DNS servers are configured in systemd-resolved: 10.0.0.10

Do you want to configure these servers as DNS forwarders? [yes]:

All detected DNS servers were added. You can enter additional addresses now:

Enter an IP address for a DNS forwarder, or press Enter to skip:

DNS forwarders: 10.0.0.10

Checking DNS forwarders, please wait ...

DNS server 10.0.0.10 does not support DNSSEC: answer to query '. SOA' is missing DNSSEC
signatures (no RRSIG data)

Please fix forwarder configuration to enable DNSSEC support.

DNS server 10.0.0.10: answer to query '. SOA' is missing DNSSEC signatures (no RRSIG data)
Please fix forwarder configuration to enable DNSSEC support.

WARNING: DNSSEC validation will be disabled

if you search reverse zone of DNS forwarder, answer [yes]

Do you want to search for missing reverse zones? [yes]:

if you configure chrony, answer [yes]

Do you want to configure chrony with NTP server or pool address? [no]:

The IPA Master Server will be configured with:

Hostname: dlp.ipa.srv.world

IP address(es): 10.0.0.40

Domain name: ipa.srv.world

Realm name: IPA.SRV.WORLD

The CA will be configured with:

Subject DN: CN=Certificate Authority,O=IPA.SRV.WORLD

Subject base: O=IPA.SRV.WORLD

Chaining: self-signed

BIND DNS server will be configured to serve IPA domain with:

Forwarders: 10.0.0.10

Forward policy: only

Reverse zone(s): No reverse zone

confirm settings and proceed with [yes]

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.

Disabled p11-kit-proxy

Synchronizing time

No SRV records of NTP servers found and no NTP server or pool address was provided.

Using default chrony configuration.

Attempting to sync time with chronyc.

Time synchronization was successful.

Configuring directory server (dirsrv). Estimated time: 30 seconds

[1/41]: creating directory server instance

Validate installation settings ...

```
Create file system structures ...
Perform SELinux labeling ...
Create database backend: dc=ipa,dc=srv,dc=world ...
Perform post-installation tasks ...
  [2/41]: tune ldbm plugin
  [3/41]: adding default schema
  [4/41]: enabling memberof plugin
```

.....

.....

```
=====
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
- * 53: bind

UDP Ports:

- * 88, 464: kerberos
- * 53: bind
- * 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
The ipa-server-install command was successful

[3]

Kerberos

```
[root@dlp ~]# kinit admin
Password for admin@IPA.SRV.WORLD:      # IPA admin password
[root@dlp ~]# klist
```

Ticket cache: KCM: 0

Default principal: admin@IPA.SRV.WORLD

Valid starting	Expires	Service principal
11/11/2021 16: 47: 03	11/12/2021 16: 09: 58	krbtgt/IPA.SRV.WORLD@IPA.SRV.WORLD

[4]	
-----	--

```
[root@dlp ~]# firewall-cmd --add-service={freeipa-ldap, freeipa-ldaps, dns, ntp}
success
[root@dlp ~]# firewall-cmd --runtime-to-permanent
success
```

Revision #1

Created 3 March 2022 03:22:22 by

Updated 9 July 2022 19:08:53 by