APPENDIX D

Setting Up Identity Management

To prepare for the RHCSA and RHCE exams, you need to use a server that provides Lightweight Directory Access Protocol (LDAP) and Kerberos services. The configuration of these services, by itself, is not an exam topic; however, it isn't hard to do either using the Red Hat Identity Management (IdM) solution, which implements the free IPA server. This appendix describes how to set up a free IPA server that can be used to provide services that are described in Chapter 6, "User and Group Management;" Chapter 24, "Configuring Time Services;" and Chapter 35, "Configuring a MariaDB Database," of this book.

WARNING FreeIPA conflicts with many other services. For that reason, make sure to use a clean (virtual) machine where nothing has been installed yet.

Performing the Base Installation

To create the IPA server that is needed for several exercises throughout this book, install a (virtual) machine that matches the following criteria:

- Ensure your server has 2 GB RAM and 10 GB available disk space.
- Use Red Hat Enterprise Linux 7 or CentOS 7.
- Name set to ipa.example.com.
- IP address set to 192.168.122.200, default gateway to 192.168.122.1, and DNS temporarily to 8.8.8.8. (You need to change that later.)
- Choose the server with graphical interface installation pattern.
- Use default partitioning on the servers hard disk.
- Switch off SELinux.
- Make sure that you have access to installation repositories.
- Add an entry to /etc/hosts to enable hostname resolution for the hostname. The line should read as follows:

```
192.168.122.200 ipa.example.com ipa
```

Installing FreeIPA

To install FreeIPA, follow these steps:

1. Open a root shell and type **yum -y install ipa-server bind-dyndb-ldap**.
2. Start the installation program for the IPA server by running **ipa-server-install --setup-dns**. (Type **ipa-server --help** for a complete list of all options.)

> **TIP** There is also a command **ipa-dns-install**. This command is useful if you have configured FreeIPA without DNS first and later on you decide that you want to change that and add DNS support.

3. When asked whether you want to configure integrated DNS (BIND), answer yes.
4. The installer will now tell you that it has found an existing BIND configuration and asks if you want to overwrite it. Answer yes to this question.
5. At this point, the installer should detect the hostname that has been set and prompt for the hostname, which according to the earlier instructions should be set to ipa.example.com. If the installer shows anything else, stop the installation now, using **Ctrl+C** and use **hostnamectl set-hostname ipa.example.com** to set the hostname. You should *not* go on and install IPA if the hostname has not been set correctly!
6. At this point, the installer asks you to confirm the DNS domain name, which should be set to example.com. If all went well, the DNS name has been correctly identified earlier in this procedure. Press **Enter** to confirm.
7. At this point, the installer should ask you to confirm the Kerberos realm name EXAMPLE.COM. If it does not, you haven't created a line in /etc/hosts that allows for resolution of this hostname. If that is the case, stop the configuration script and add this line to /etc/hosts. After adding it, you can start this script again to work through all steps of the configuration. Confirm the Kerberos realm name EXAMPLE.COM by pressing **Enter**.
8. The installer now prompts for the Directory Manager password. As you are setting up the IPA server for use in a course / test environment, I recommend using the password **password**.
9. After setting the password for the Directory Manager (which is an LDAP administrative account), you need to set a password for the IPA admin user as well. This is the account that you typically use to accomplish all IPA management tasks. Set this to **password** also.

10. At this point, you are prompted as to whether you want to set an IP address for a DNS forwarder. It is a good idea to forward all DNS requests that cannot be resolved locally to an external DNS server, but you do not have to. Enter the IP address of your external DNS server, or a common external DNS server such as 8.8.8.8, and press **Enter**.

11. The installer prompts once more for the IP address of a DNS forwarder. This is because multiple DNS forwarders can be configured. Press **Enter** without entering anything else here.

12. You are now asked if you want to configure the (DNS) reverse zone. For full functionality, it is important that you do this. Press **Enter** to access the default suggestion and start configuring it. This will allow you to not only resolve hostnames to IP addresses but also to resolve IP addresses to hostnames.

13. You are now prompted to specify the reverse zone name. According to the preceding instructions, it should be set to 122.168.192.in-addr.arpa. (The reverse zone name contains the network part of the IP address, but reversed, followed by the fixed part in-addr.arpa. Press **Enter** to accept.

14. You will now see a summary of all installation settings. Check if it looks okay. If it does, type **yes** and press **Enter** to start the installation. Go have a cup of coffee; this will take a couple of minutes to complete. After successful completion, the installer shows the following message:

```
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 certificate stored in /root/cacert.p12
This file is required to create replicas. The password for this
file is the Directory Manager password
```

15. At this point, you need to finalize the installation. First, you need to open the firewall to allow all services that FreeIPA is offering to be accessed. Do this by typing **for i in http https ldap ldaps kerberos kpasswd dns ntp; do firewall-cmd --permanent --add-service $i; done**. Next type **firewall-cmd --reload** to reload the configuration.

16. Now you can obtain a Kerberos ticket for the Kerberos admin user by using **kinit admin**. Enter the password **password** that you've set for this user previously and you'll have a Kerberized session that is established.

17. Type **klist** to verify the contents of the Kerberos ticket. You'll see that your session is valid for 24 hours. This completes the primary part of the setup.

You now have a working IPA service that provides LDAP, Kerberos, DNS, and time services. Notice that the time services are offered by using the **ntp** service, and not the **chronyd** service that you will learn about in this book. From a functionality perspective, that does not really matter.

Preparing Your IPA Server for User Authentication

Now that you have a functional IPA server, it is time to prepare it for the labs where you need to authenticate on the IPA server using LDAP or Kerberos credentials. This includes the creation of an FTP server to make the certificate and keytab files available:

1. Install the vsftpd FTP server by using **yum install -y vsftpd**.

2. Type **systemctl enable vsftpd; systemctl start vsftpd** to enable and start the FTP service.

3. From a root shell, type **cp ~/cacert.p12 /var/ftp/pub** to copy the CA certificate of the IPA server to the FTP site. This ensures that the certificate is available for the exercises where users need to authenticate.

4. Type **firewall-cmd --permanent --add-service ftp; firewall-cmd --reload**.

5. Type **klist** to see whether you are still in a Kerberized session. If not, type **kinit admin**.

6. Now that you are authenticated on the IPA server, type **ipa user-add lisa**. Enter **lisa** as the first name and **jones** as the last name. You'll see that the user lisa is added to the IPA server. Repeat this procedure to create a user **linda thomsen**.

7. For both users, set the IPA password. Use **ipa passwd lisa**; **ipa passwd linda** to do this. Enter the password **password** for both users.

Your IPA server is now ready for all exercises in Chapters 6 and 24 of this book.

Preparing Your IPA Server for Kerberized NFS

To prepare for the labs in Chapter 36, "Configuring NFS," you need to create Kerberos principals for the NFS server you are going to create on server1. After creating the Kerberos credentials for the NFS server, you need to make them available on the NFS server also. To do this, in this procedure you need access to server1 and server2 (which are going to be used in Chapter 36).

1. To start, you need to create DNS entries on the IPA server. From ipa.example.com, start Firefox and enter httpd://labipa.example.com. On the certificate warning, click **I Understand the Risks and Add Exception**. Next, click **Confirm Security Exception**. You'll now see the IPA login window. From this window, enter the username admin and the password **password** to authenticate.

2. Before continuing, you need DNS records for the hosts. Possibly you do not have to do this, but in case you do not have DNS resource records, this is how you can create them. Click the **Hosts** link, and from there, click **Add**. Enter the hostname **server1**, verify that the DNS zone is set to example.com, and enter the IP address **192.168.122.210**. Repeat this procedure for server2.example.com with IP address 192.168.122.220. You now have DNS records and reverse DNS records for all of your hosts in the test environment.

3. You now need to join the NFS server server1.example.com to the IPA Kerberos realm. Open a root shell on the NFS server and type **yum install -y ipa-client**. All the following steps need to be executed on server1 also.

4. Use **nmtui** to set the IP address of the DNS server to 192.168.122.200. Type **systemctl restart NetworkManager**. This sets the nameserver to be used to 192.168.122.200, which is essential for the success of the following steps.

5. Type **ipa-client-install --mkhomedir --enable-dns-updates --force-ntpd**. When asked which user is authorized to enroll computers, type **admin**, and when prompted for a password for admin@EXAMPLE.COM, type **password**. The procedure should complete telling you that the client configuration is complete.

6. Still on ipa.example.com, create the service principals for the NFS server that you are going to install on server1. Type **ipa service-add**, and when asked

for the principal, enter **nfs/server1.example.com**. This returns the following information.

```
[root@ipa ~]# ipa service-add
Principal: nfs/server1.example.com
---------------------------------------------------
Added service "nfs/server1.example.com@EXAMPLE.COM"
---------------------------------------------------
  Principal: nfs/server1.example.com@EXAMPLE.COM
  Managed by: server1.example.com
```

7. Type **klist -k** on server1. You will see that you have a host principal, which is needed for single sign-on and host authentication for Kerberos.

8. On server1, type **ipa-getkeytab -s ipa.example.com -p nfs/server1.example.com -k /etc/krb5.keytab**.

9. Verify that you now have the NFS principal on server1 by using **kinit -k nfs/server1.example.com**, followed by **klist**.

10. On server2, repeat Step 6 of this procedure to enter the client into the IPA domain. Next, from the client, type **ipa-getkeytab -s ipa.example.com -k /etc/krb5.keytab -p host/server2.example.com@EXAMPLE.COM**. Copy the keytab from server2 to the IPA server by using **scp /etc/krb5.keytab ipa.example.com:/var/ftp/pub/server2.keytab**.