Hostnames:

- Server1: **srv1.rhce.local**
- Server2: **srv2.rhce.local**

IP addresses and networking:

- Server1: **10.8.8.71/24**
- Server2: **10.8.8.72/24**
- Name server: **10.8.8.70**
- Gateway: **10.8.8.70**

Once you configure networking with the details above, you will be able to resolve the following domains successfully (as they're set up on the FreeIPA/DNS server):

- ipa.rhce.local
- srv1.rhce.local
- srv2.rhce.local
- vhost1.rhce.local
- dynamic1.rhce.local

The following LDAP (FreeIPA) users are available for testing:

- alice
- vince

Before you begin, reset the root user password to **pass** on both servers, **server1** and **server2**.

1. Configure SELinux

Configure **server1** and **server2** to have SELinux running in enforcing mode.

2. Configure Repository

Configure a repository on **server1** and **server2**. Use the RHEL 7 DVD that's available on `/dev/cdrom` on both machines. The changes should persist after reboot.

3. Link Aggregation

Configure **server1** and **server2** for link aggregation, which watches for link changes and selects an active port for data transfers. The **server1** should use the address of 10.8.8.71/24. The **server2** should use the address 10.8.8.72/24. The gateway and the name server address is 10.8.8.70. The changes should persist after reboot.

Configure the "dmz" firewalld zone to be the default zone on both servers **server1** and **server2**, and ensure that the the aggregated network connection uses to the default zone.

4. IPv6 Network

Configure previously configured aggregated network links with static IPv6 addresses. The changes should persist after reboot.

Configure a static IPv6 address on the **server1** as fc00::a:b:c:71/64. Configure a static IPv6 address on the **server2** as fc00::a:b:c:72/64.

5. NTP

Configure **server1** and **server2** to synchronise time with the NTP server ipa.rhce.local.

6. SMTP Configuration

Configure **server1** as a null client to relay email from local system through **ipa.rhce.local**. All outgoing mail have their sender domain as rhce.local.

7. Kernel Parameters

Configure **server1** to be a router. Also ensure that the **server1** reboots automatically after 300 seconds in case of a kernel panic. The changes should persist after reboot.

8. Kerberos Authentication

Configure **server1** and **server2** for Kerberos authentication.

Use the following LDAP authentication details:

- Server: **ipa.rhce.local**
- Base DN: **dc=rhce,dc=local**
- LDAP cacert is available on **ftp://ipa.rhce.local/pub/cacert.p12**

There is an LDAP user alice created on the FreeIPA server, use it for testing.

Use the following Kerberos authentication details:

- Realm: **RHCE.LOCAL**
- KDC: **ipa.rhce.local**
- Admin Server: **ipa.rhce.local**

To test, you can obtain a Kerberos ticket for the user alice.

9. NFS Server

Configure **server1** to provide a Kerberised NFSv4 share.
Set up a Kerberised NFSv4 share `/srv/nfssec` in a read-write mode and share it to the client **srv2.rhce.local** only. Enable krb5p security to secure access to the NFS share from URI **ftp://ipa.rhce.local/pub/srv1.keytab**. The owner of the share must be LDAP user alice.

10. NFS Mount

Configure **server2** to mount a Kerberised NFSv4 share.
Mount Kerberised NFSv4 share `/srv/nfssec` on `/mnt/protected` directory persistently at boot time provided with the keytab **ftp://ipa.rhce.local/pub/srv2.keytab**. LDAP user alice should be able to write to the share.

11. MariaDB Server

Configure **server2** to meet the following requirements.
Set up a default secure MariaDB database called **shop** with a user john with all privileges. The user john must be identified by “pass”. In this database, create one simple table with the name **products** that allows to store names varchar(20) and their prices int(10). Enter two products. Backup the database with mysqldump to `/root/shop.sql`.
MariaDB must listen on a TCP port 5555 with a dataroot on `/srv/mariadb`. Firewall should allow access to port 5555 from **srv1.rhce.local** only. The MariaDB root password must be “pass”.

12. Samba Server

Configure **server1** to provide a Samba share. Share `/srv/smb_docs` directory via SMB**.** The SMB server must be a member of the DEVOPS workgroup. The share name must be docs. Only the host **srv2.rhce.local** should be allowed to connect to the docs share. The docs share must be browseable but not writable nor printable. User vince must have read-write access to the docs share, authenticating with the password “pass”.
Ensure that SELinux allows sharing of home directories.

13. Samba Mount

Configure **server2** to mount a Samba share. Mount the Samba share docs permanently on `/mnt/samba` as a multi-user mount. The share should be mounted with the credentials of vince.

14. Port Forwarding

Configure **server2** to forward incoming traffic on port 8080/tcp to 10.8.8.71:80 (srv1.rhce.local:80).
Also configure **server2** for firewalld SSH logging with a prefix of “SSH_” and a debug level, limit to 2 log entries per minute. The changes should persist after reboot.

15. iSCSI Target

Configure **server1** to provide iSCSI LUNs. Set up an iSCSI target with CHAP authentication (username=client/password=client) based on a fileio backstore `/srv/iscsifile` of 200MB. The logical block name should be file1. A local file system cache must be disabled to reduce the risk of data loss.
Also set up an LVM based block backstore of 100MB called lv_iscsi (use a volume group of your choice). The logical block name should be block1.

Use the IQN of **iqn.2003-01.local.rhce:srv1** for the iSCSI server, apply standard firewall configuration. Create LUNs for both backstores, ensure the LUNs are available to the client iqn.2003-01.local.rhce:srv2.

16. iSCSI Initiator

Configure **server2** as an iSCSI initiator. Use the IQN of **iqn.2003-01.local.rhce:srv2** for it.
The datastore block1 should be formated as ext4 and mounted permanently on `/mnt/san1`.
The datastore file1 should be added to a new LVM volume group vg_san, a new 50MB logical volume lv_lun1 should be created, formatted as xfs, and mounted permanently on `/mnt/san2`.

17. Webserver

Configure **server1** to meet all of the following requirements.

17.1 Secure Webserver

Configure a webserver for the site **http://srv1.rhce.local**. The webpage should say “hello”.
Also configure website **http://srv1.rhce.local** with TLS. Generate a self-signed certificate, the only requirement for the certificate is to match the webserver name srv1.rhce.local. Make sure that SSLv2 and SSLv3 protocols are disabled.
The content of the websites should be visible to everyone browsing from the localhost but should not be accessible from any other location.

17.2 Webpage Content Modification

Implement a website for **http://srv1.rhce.local/group**. Create a directory “group” under the document root used for the website. The webpage should say “group”.
The webpage must be configured for group-based authentication and require users to login. Only user alice, who is a member of the devops group, should be allowed to access the website with a password “password”.

17.3. Virtual Hosting

Setup a virtual host **http://vhost1.rhce.local** with the alternate document root under `/srv/www/vhost1`. The webpage should say “vhost1”. The webpage must be configured for user-based authentication. Only user alice should be allowed to login with a password “password”.
Note: the other websites configured on the **server1** must still be accessible.

17.4. Dynamic Content Configuration

Configure website **http://dynamic1.rhce.local:8888/** with the document root `/srv/www/scripts` to serve a PHP application. The site should execute index.php. The PHP application is provided on **ftp://ipa.rhce.local/pub/index.php**. Content of the script should **not be modified**.
Note: the PHP application won’t work until you have a MariaDB server configured as per task **#11**.

18. Name Server

Configure **server1** as a caching-only DNS server to forward DNS queries. Forward all requests (zone for the root . domain) to another DNS server 10.8.8.70. External access to the DNS server should only be allowed from **srv2.rhce.local**.

19. SSH Configuration

Configure **server1** to meet the following requirements.
SSH should listen on ports 22 and 2222. Firewall should allow access to port 2222 from **srv2.rhce.local** only. Client **ipa.rhce.local** must not have access to SSH at all. Enable password and key authentication. The changes should persist after reboot.
Configure **server2** for passwordless root authentication against the server1.

20. Scripting

Create a script on the **server1** called `/root/newusers`. When the script is called with an argument users.txt, it should add all the users from the file. Download the file from **ftp://ipa.rhce.local/pub/users.txt**.

All users should have the login shell as /sbin/nologin, password is not required. When this script is called with any other argument, it should print the message as “Input File Not Found”. When this script is run without any argument, it should display “Usage: /root/newusers users.txt”