ForgeRock Accreditation L&L

Wednesday, June 5, 2024 3:13 PM

The goal is to install two ForgeRock DS instances, one on each L&L VM and make sure they are operating properly in a replica set.

Assume all steps are performed on both VMs unless specified otherwise.

- Download both L&L VMs
  - "\\nas\UT\training\LunchAndLearn\AM Accreditation"
- Set up SSH public key authentication from your host to the two L&L VMs
- Set up SSH public key authentication between each of the L&L VMs
- Disable the firewall
  - systemctl stop firewalld
  - systemctl disable firewalld
- Set up the /etc/hosts file for each VM
  - I named my VMs ds-config1 and ds-config2
  - In the hosts file, added both the unqualified and fully qualified names for each server. For example:
    172.17.2.75 am1 am1.dev.trivir.com ds-config1 ds-config1.dev.trivir.com
    172.17.2.76 am2 am2.dev.trivir.com ds-config2 ds-config2.dev.trivir.com
- Create a 'forgerock' service account (will be used to run the ForgeRock DS service under a non-privileged account… i.e. non-root account)
  - useradd -r -m -s /sbin/nologin -d {path to home dir} {username}
  - NOTE: I made the service account's home directory the following: /var/opt/forgerock
- Download and install the Azul Zulu JDK. Just use the RPM version:
  - https://www.azul.com/downloads/?version=java-17-lts&os=rhel&package=jdk#zulu
  - Make sure there is no other JVM installed when using the RPM version
- Download ForgeRock DS 7.5 from the ForgeRock Backstage site (the ZIP version)
  - https://backstage.forgerock.com/downloads/browse/ds/featured
- Install DS
  - Create deployment ID
    - https://backstage.forgerock.com/docs/ds/7.5/security-guide/pki.html#about-deployment-ids
    - You just create one deployment ID and provide the same ID to both DS instances when you install them. The deployment ID allows each DS instance in the replica set to trust each other (because they use the same deployment ID).
  - Create AND enable a systemd script that can be used for starting and stopping the DS config service you'll be setting up in the next steps
    - This was posted by Travis and Jeremiah in the Google Chat. Use it as a reference for creating the systemd script for your ds-config DS instances: https://git.trivir.com/projects/FR-ANSIBLE/repos/fr-roles/browse/trivir/forgerock_ds/install/templates/ds_service.j2
  - Unzip the DS install ZIP into /opt/forgerock/ds-config
  - Change user/group ownership to the 'forgerock' service account of all files in /opt/forgerock/ds-config. I can't remember if I changed ownership of the files before I ran the DS setup command or after, or both.
  - On the first L&L VM, set up your primary DS config instance. Feel free to change the password as desired.

cd /opt/forgerock/ds-config

```
./setup \
 --deploymentId <insert-your-deployment-id-here> \
 --deploymentIdPassword 'TriVir#1' \
 --rootUserDN uid=admin \
 --rootUserPassword 'TriVir#1' \
 --monitorUserPassword 'TriVir#1' \
 --hostname ds-config1.dev.trivir.com \
 --adminConnectorPort 1444 \
 --ldapPort 1389 \
 --enableStartTls \
 --ldapsPort 1636 \
 --httpsPort 1443 \
 --replicationPort 1989 \
 --bootstrapReplicationServer ds-config1.dev.trivir.com:1989 \
 --profile am-config \
 --set am-config/amConfigAdminPassword:TriVir#1 \
 --acceptLicense
```

- Use your systemd script to start this first DS instance before you set up your second DS instance on the other VM. Make sure 'systemctl status ds-config' shows that it is successfully running

- On the second L&L VM, set up your second DS instance. It is same command, but the 'hostname' value is changed. Also notice that you don't change the 'bootstrapReplicationServer' for this second instance setup comand. It DOES need to point to the first DS instance for replication to be set up properly. Also, feel free to change the passwords as desired.

  cd /opt/forgerock/ds-config

```
./setup \
 --deploymentId <insert-your-deployment-id-here> \
 --deploymentIdPassword 'TriVir#1' \
 --rootUserDN uid=admin \
 --rootUserPassword 'TriVir#1' \
 --monitorUserPassword 'TriVir#1' \
 --hostname ds-config2.dev.trivir.com \
 --adminConnectorPort 1444 \
 --ldapPort 1389 \
 --enableStartTls \
 --ldapsPort 1636 \
 --httpsPort 1443 \
 --replicationPort 1989 \
 --bootstrapReplicationServer ds-config1.dev.trivir.com:1989 \
 --profile am-config \
 --set am-config/amConfigAdminPassword:TriVir#1 \
 --acceptLicense
```

- Use your systemd script to start the second DS instance (on the second VM)

- Check replication status between the two DS config instances. Something along the lines of the following command:

- /dsrepl status --hostname ds-config2 --port 1444 --bindDN "uid=admin" --bindPassword 'TriVir#1' --trustAll