TIER-Grouper Release 180401

Introduction

The TIER Grouper Virtual Machine software release is a Docker container-based virtual machine distribution that includes the ability both build the appropriate set of Docker containers and run the containers to provide a Grouper service. The operating environment includes appropriate Grouper an d MariaDB containers networked together to build the Grouper service. The current distribution is based on Oracle VirtualBox, though an Amazon AMI is available which can easily be shared, but is not yet public. The VirtualBox VM can be downloaded here.

These notes are for TIER-Grouper Release 180401. Release 180401 of the TIER-Grouper appliance contains the following components:

- CentOS: 7.4.1708
- Grouper: 2.3
- Tomcat: 8.5.12
- Java: 1.8.0_162-b12
- MariaDB: 5.5.50-1
- Docker: 18.03.0.ce

A few words on VirtualBox:

- If you are not familiar with VirtualBox, you can read the documentation and download the software from Oracle's web site.
- Once VirtualBox is installed and running, you import the .ova distribution image using the File / Import Appliance function.
- The default network connection for the Grouper packaged Virtual Machine is *Bridged*. With a bridged network connection, the VM will use dhcp to obtain its IP address from your local network. If you have a network registration process in place on your campus network, you may need to register the MAC address of your VM before you obtain an IP address. You can change the VirtualBox network configuration to NAT mode to look at the VM and its components this way but it is not recommended for general testing. *Remember, if you are on a public network, the VM will be exposed to the world and we publish the password on this web site (So please change it immediately!).* Note that Virtual Box bridge mode can not work with many wireless network adapters since the don't support promiscuous mode. A wired network connection is generally better for use with Bridge Mode. Note that is *possible* to do some testing in NAT mode, but involves the inclusion of port numbers into the process. This works e.g. https://127.0.0.1:8443 but remember that only one person can use a URL at a time in the TIER Testbed, if you will be using the TIER testbed.
- If you choose to connect this VM to the TIER Testbed, upon success you will see a set of attributes supplied by your Shibboleth IdP VM being displayed by the TIER testbed Shibboleth SP.
- The VM may default to using two cores and 4 GB of RAM. If your machine does not have the resources to support this environment, you should be able to successfully operate with a singe core and down to approximately 2 GB of RAM. You can make these changes by clicking on the Settings button and then selecting the System options after you import the VM into VirtualBox.

Setup Process

When you complete the process itemized below, you'll be able to see and login to the Grouper management page.

Once you have started the VM, login to the account *grouper* with a password of *grouper*. You can then use the Linux *ip addr* command to determine the IP address that has been assigned to your virtual machine. You will need this address (or its matching DNS name, if any) later in the process. We also recommend that you use a ssh client (e.g. ssh, putty, or securecrt) to login to the vm instead of using the terminal emulator provided by VirtualBox. The VirtualBox terminal emulator is very limiting.

Note: *You should change the password for the linux account **grouper**, especially before placing the VM on a public network. If you fail to change this passwords, your VM might be compromised. The user comanage has sudo capability. We recommend that you **change this password now by issuing the following command:***

```
passwd
```

Issue the following command to configure Grouper:

```
vm> /home/grouper/work/setup.sh
```

Setup.sh Log Example

vm> /home/grouper/work/setup.sh

Welcome to the TIER Grouper Virtual Machine

Note: if you are running this script to set up a production Grouper instance, please be sure that you have had this VM running for a sufficiently long period of time, with network traffic reaching reaching the VM in order to build entropy before keys are generated.

Grouper requires that you use Oracle Java. This VM is configured to download it for you as part of the Docker image build process, but, before we proceed, you must agree to the Oracle Binary Code License Agreement for Java SE ("Oracle License"). Please review:

http://www.oracle.com/technetwork/java/javase/terms/license/index.html

By agreeing to the Oracle License, you acknowledge that Internet2 is not distributing the Java software and, to the extent an issue arises related to your use of Oracle Java in the TIER software package, you and Internet2 agree to hold each other harmless from any third party claims.

Do you agree to the terms of the Oracle license [Yes/No]? Yes

Please supply the Fully Qualified Domain Name (FQDN) of your Grouper IdP.

We will use the information you enter here to configure your IdP. Note: for testing without DNS support (a common case), simply enter the IPv4 address of your VM at the prompt below

The setup.sh script generates a new key-pair, a certificate signing request, and a self-signed certificate. The script installs the self-signed certificate into */home/grouper/build/grouper/certs* where it will later be built into the Docker container. For a production environment, you must take the certificate signing request from */home/grouper/work/crypto /server.csr*, have it signed by a commercial CA, and place the resulting certificate in */home/grouper/build/grouper/certs* before moving on to the next step.

Notewell: Virtual machines start will little to no entropy for the random number generator. If your build is for a production environment, be sure to run the VM for a while, moving data, typing, causing randomness, etc., before running the setup.sh script.

Issue the following command to build the containers:

```
/home/grouper/build/grouper/bin/build.sh
```

Issue the following command to run the containers:

```
/home/grouper/run/bin/run.sh
```

Enter the FQDN or IP address of your server: 137.54.129.75

You entered: 137.54.129.75 Is this correct [Yes/No]? yes

SSL certificate: enter value for country: US

SSL certificate: enter value for State of Province: Michigan

SSL certificate: enter value for Locality: Ann Arbor

SSL certificate: enter name of your organization: Internet2

Hit ctrl-C in the next 10 seconds to abort the process.

Please do not abort the script is doing work, you can rerun when its complete if needed

Configuring for the download of Oracle Java

Generating certificates for Grouper

A self-signed certificate for Grouper is stored in: /home /grouper/etc/certs For production use, replace this certificate with one signed by a commercial CA the Certificate Signing Request for the commercial CA is located at: /home/grouper /work/crypto/server.csr

Preliminary setup is complete

For production use, please review the files in: /home/grouper /run/conf The common.env and grouper.env files contain passwords that need to be site secrets for production use

Once you have made any other needed edits, cd to /home /grouper/build/grouper and execute bin/build.sh

When the build is complete, cd to /home/grouper/run/ and execute bin/run.sh

***** Wait for grouper to start. This can take a couple of minutes the first time**

Then browse to: https://137.54.129.75/grouper/

Note: your first connection to this URL will be very slow and may time out - try again - be patient.

Verification Process

The first step is to be patient and wait. The first-time startup of Grouper can take a couple of minutes. Wait two minutes before starting on the next step.

- Browse to: https://YOUR-IP-OR-DNS/grouper/
  - Note: your first connection to this URL will be very slow (minutes are not unusual)
  - If your browser times our, just retry the connection,
- Login as the Grouper Administrator
  - Login Name: GrouperSystem
  - Password: XXXXXXXXXX

If you are not familiar with Grouper, please review the on-line Grouper Training, Grouper Administration Guides, TIER Grouper Deployment Guide, and Community Contributions/Adopter Sketches.

Some Useful Docker Commands

While the normal idea is that you should never need to look inside a container, it is possible and is sometimes useful for debugging unusual issues. These commands may be helpful.

1. docker ps
   Shows the names and status of any running containers.

2. docker exec
   Run a command inside a running docker container. You will find **docker exec -it comanage bash** a handy command for debugging issues. This command will open a root shell inside the container and map the output back to your VM session. Inside the container you will find the familiar files and directories, including access to the configuration and logs.
3. docker start
   To start the COmanage container after rebooting the VM, run **docker start comanage mariadb**
4. docker stop
   To stop the COmanage container, run **docker stop comanage**
5. docker cp
   Used to copy files in to or out of a running container. The syntax is similar to scp.