COmanage Release 17040

Introduction

The packaged TIER COmanage release is a Docker container-based implementation of the COmanage Registry. The release consists of Docker containers for COmanage and its database along with a Centos Linux Virtual Machine image that is used to configure and run the containers. Release 17040 of the TIER-COmanage appliance contains the following components:

- CentOS 7.3.1611
- COmanage 2.0.0
- MariaDB 5.5
- Docker 17.04.0

At the current point in time, TIER Release 17040, we have not written documentation on how to use the containers outside of the VM environment nor have we completed the additional scripting and documentation that will make it easier to configure this COmanage release for use in a production environment. This release is primarily available for use with Oracle VirtualBox, though an Amazon AMI is available. If you are not familiar with VirtualBox, you can read the documentation and download the software from Oracle's web site.

Configuring the COmanage Release

For more information on VirtualBox and starting the VM, see the Shibboleth IdP release notes (navigation pane, left side). The basic procedure is to download the COmanage VM .ova image (1.3 GB) and then select VirtualBox's File/Import-Appliance function.

The initial login/password for the COmanage VM is: *comanage /comanage*.

1. Prerequisites
   The TIER COmanage release requires a few pieces of supporting infrastructure in order to function.
   a. An email service (authenticated SMTP server) that supports TLS.
   b. A Shibboleth IdP that can be configured to work with the Shibboleth SP running in the COmanage container.
   c. Identities from the IdP for the initial COmanage administrator and test users.
   d. The TIER Testbed can provide the Shibboleth IdP function and test user records. For email, your personal campus account may work. We have used a gmail account with POP/IMAP enabled with our internal testing.
   e. An IP address / DNS name. The VM is configured for DHCP so as long as your campus lease times are sufficiently long, DHCP will work well for testing (leave the VM running). See the notes on the Shibboleth VM page on VirtualBox testing in Bridged Mode re: some campuses requiring mac address registration in order to obtain an IP address, lack of support on Wireless Adapters, etc. NAT testing is not recommended. You do not need a public IP address in order to test COmanage.
2. Installation for Testing
   This information is ordered for use with the TIER Testbed. If you are working in a different environment, you can look at the scripting as a guide for what is needed. Changes to the Dockerfile can be made. For example, to copy a full Shibboleth SP configuration into the build.
   a. Collect all of the prerequisite information
      i. Create any TIER testbed person record(s) that you will need to work with COmanage. You will need at least one federated user for the initial administrator role. Record the full eduPersonPrincipalName (eppn) of your administrative user.
      ii. Choose/create a SMTP email account. You will need: login name, password, host, port, and an email address for the From line. The normal account email address is likely fine for the From address.
   b. Import the appliance into VirtualBox. We strongly recommend testing using the Bridged network mode configured in the VM.

Configuration Script (setup.sh) Log

```
vm>cd /home/comanage/build/comanage/work
vm>./setup.sh
Starting run at:

Welcome to the TIER COmanage Virtual Machine



Please supply the Fully Qualified Domain Name
(FQDN) of your COmanage Registry.
We will use the information you enter here to
configure the Shibboleth SP
that controls access to your COmanage Registry
Note: for testing without DNS support (a common
case), simply enter
 the IPv4 address of your VM at the prompt below
Do not enter a Shibboleth entityID - just a DNS
name or IP Address

Enter the FQDN or IP address of your server:
137.54.129.66
You entered: 137.54.129.66 Is this correct [Yes
/No]? yes


We need the eppn of initial COmanage administrative
user.
For testing now, a TIER Testbed identity will work
well.
Enter the COmanage Admin user name (i.e., admin
eppn): jaj4de@testbed.tier.internet2.edu

Enter the COmanage Admin user First Name [Jane]:

Enter the COmanage Admin user Last Name [Doe]:


Next, we need information to set up email
notifications from COmanage
 for this section to work, you will need
authentication credentials on
 a SMTP server that supports TLS encryption. We
recommend using a Gmail
 account if you don't already have something else
in place.

Enter From email address for your messages: jaj@virg
inia.edu

Enter smtp server DNS or IP address [smtp.gmail.com]:

Enter smtp server port [587]:

Enter email SMTP smtp auth user name: jaj@virginia.
edu
```

c. If you are **not** running VirtualBox in a Unix environment (e.g., Windows), uncheck Settings /System/Hardware Clock in UTC time.
d. The VM (R2-V2) defaults to using two cores and 6 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.
e. Start the VM
f. Login for the first time using the Virtual Box terminal emulator and obtain your IP address (linux: ip addr). Record the IP address. We'll call it MY-COMAN-IP-OR-DNS for the rest of this document.
g. Note: if your IP address has a reliable DNS name associated with it, you can use the DNS name instead. Some testers also prefer to use a DNS name followed by /etc/hosts modifications.
h. We recommend using SSH instead of the VirtualBox terminal emulator for the rest of this work, its much more user friendly.
ssh comanage@MY-COMAN-IP-OR-DNS; remember that the initial password is: *comanage*
i. ***Note:*** *you must change the password for the linux account* ***comanage****, 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
```

j. cd /home/comanage/build/comanage/work
k. ./setup.sh
    i. Answer the questions. This script will auto-configure several aspects of the build including the initial administrative user and email.
    ii. Note: the existing scripting **does not** yet build new certificates or keys. Be sure you understand what is needed before using this version of the distribution in production.
    iii. This setup script edits files - you can also choose to examine the script and modify appropriate files by hand.
l. cd /home/comanage/build/comanage
m. ./bin/build.sh
n. cd /home/comanage/run
o. bin/run.sh
p. wait a minute or two for COmanage to start.
q. curl -k https://172.18.0.3/Shibboleth.sso/Status (the 172.18.0.3 address is on the internal docker network - your VM is connected to this network)
r. You will need the PEM of the signing certificate (the first certificate in the output of the Step 2.o to complete the next step).
s. In a web browser, go to https://testbed.tier.internet2.edu/cgi-bin/secure/tier-process.py?function=metadata_sp
    i. Select COmanage as the Product Being Tested
    ii. Enter MY-COMAN-IP-OR-DNS (from Step 2.e above) in the Domain Name of IP address slot
    iii. Carefully copy the signing certificate PEM from Step 2.o above and paste it into the webform. Look closely at the curl output and be sure to copy/paste the whole certificate

```
Enter email server smtp auth password: PASSWORD-REDACTED
FQDN: 137.54.129.66
COMANAGE_SERVER_FQDN: 137.54.129.66
COMANAGE_MAIL_FROM: jaj@virginia.edu
COMANAGE_MAIL_HOST: smtp.gmail.com
COMANAGE_MAIL_PORT: 587
COMANAGE_MAIL_USER: jaj@virginia.edu
COMANAGE_MAIL_PASS: PASSWORD-REDACTED
COMAN_ADMIN_USERNAME: jaj4de@testbed.tier.internet2.edu
COMAN_ADMIN_NAME: Jane
COMAN_ADMIN_FAMILY: Doe


The file edit process will start in 15 seconds
Hit ctrl-C to abort the process

working ...

Updating shibboleth2.xml to match the FQDN you supplied


Updating 00-comanage-443.conf to match the FQDN you supplied


Updating email.php to match the data you supplied


Updating coman.env to match the data you supplied


Initial setup is complete

Next, cd /home/comanage/build/comanage
 bin/build.sh
Then, /home/comanage/run
 bin/run.sh
vm>
```

(without any of the leading/trailing XML) into the webform. The certificate will start with the letters: MII

iv. Press the Submit button.
v. Wait 15 minutes. The testbed needs time to process your metadata and the testbed's Shibboleth IdP needs time to load the new metadata.

Evaluating/Testing COmanage

Full testing and evaluation of COmanage is beyond the scope of this document. See the COmanage Web Site for complete information. You can, however, perform some quick initial tests to ensure that you installation is functional.

a. Browse to: https://MY-COMAN-IP-OR-DNS/registry/ and work your way past the certificate errors. Remember that you are using self-signed certificates, so these error messages are expected.
b. Press the *Login* button.
c. You will most likely want to select the testbed's Shibboleth IdP named *TIER Testbed Shibboleth IdP* to use any identities you created. If you have an IdP registered in the TIER Testbed and you feed it your COmanage SP's metadata, that should also work but complications might arise with the metadata the Testbed created for older IdP installations.
d. Enter the login name and password for the testbed user you specified as the COmanage administrator in Configuring the COmanage Release, Step 2.h above. You will now be logged in as the initial COmanage administrator.
e. Click on the wrench/Platform button, select COs, then select Add CO, and add something like *TestCO* with a description of *Just Testing*.
f. Click the *Collaborations* button (top right) and select your new CO.
g. From *Configuration*, select *Enrollment Flows,* and then click *Add/Restore Default Templates*.
h. In the *Self Signup With Approval (Template)* row, press the *Edit* button, delete the word *(Template)* from the Name and change the Status from *Template* to *Active*. Press the *Save* button at the bottom of the form. You will see a green highlighted pop up confirming the update.
i. Near the top right of the webform, you will see a *Begin* button. Copy the URL associated with this button.
j. Start a Private (Safari/Firefox), Incognito (Chrome), or InPrivate (Edge) browsing window in a new browser, paste in the URL from Step 3.i above. You must use a browser that us **not** already logged into COmanage (do not simply use a new tab or a new browser window).
k. Fill in the webform to invite a person to join the CO.
l. If everything is working properly, an email message will be sent to the address you specified in 1.k with an invitation to join the CO. As long as the recipient can reach MY-COMAN-IP-OR-DNS, clicking on the link in the message to accept the invitation will complete the process.

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.