Exium CGW On-Boarding

User Guide

Version 0.1.16

TABLE OF CONTENTS

1 INTRODUCTION

This document provides steps to install and use Exium-CGW OVA for connecting Exium SASE service. Steps mentioned in this document are applicable for virtualization environments like VirtualBox ESXi, KVM and Hyper-V.

Section (3) provides step by step guide to quickly setup CGW for first the time. Also, it includes the commands and operations supported by CGW.

Section (4) provides steps to manage Gateways. It includes steps to add, edit, delete Gateways and their respective Trust Paths.

Section (5) provides steps to manage Policies and Policy Groups. It includes steps to add, edit, delete policies or policy groups. Policy consists of rules which help user to manage the service usage.

Section (6) provides sample configuration example for local CGW. It also provides sample network diagram for users to plan the CGW deployment.

2 PREREQUISITES

Supported virtualization platforms:

- VMWare ESXi (6.5 and above)
- KVM on CentOS or Ubuntu
- Hyper-V on Windows (10 and above)
- Oracle VirtualBox (6.1 and above) on Windows (10 and above)
- Bare metal with Ubuntu 18.04 or above
- AWS Elastic Compute Cloud (EC2)

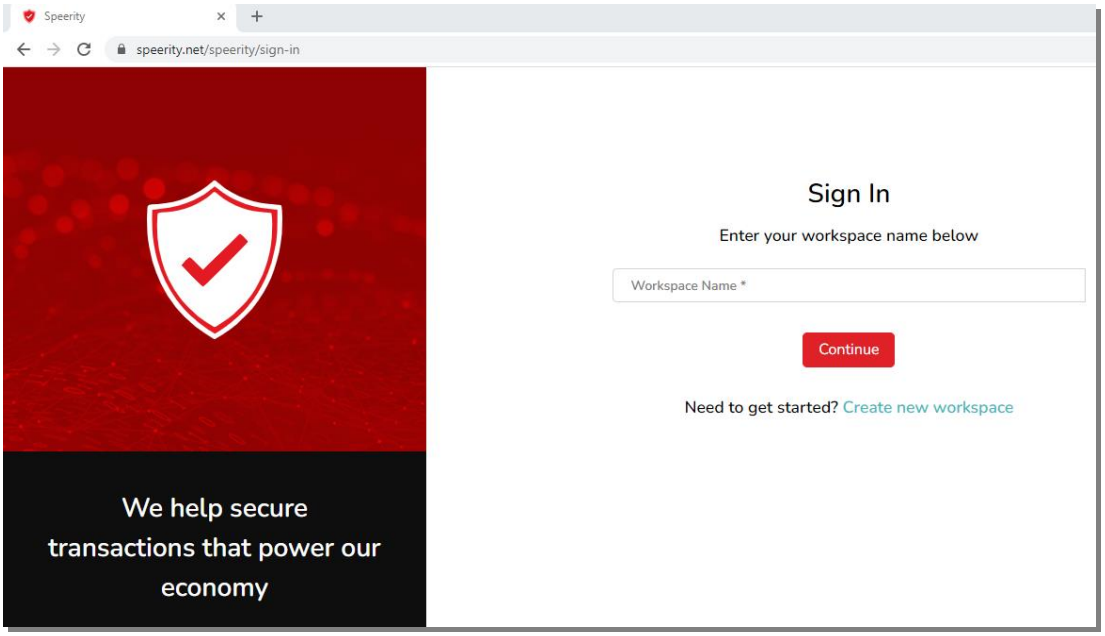
3 QUICK SETUP

This section provides step by step guide to quickly setup CGW.

- Skip section (3.1) in case user already has subscribed to Exium service.
- Skip section (3.2) in case user already has created a workspace.
- Skip section (3.3) and (3.4) in case user already has downloaded Exium CGW OVA

3.1 SUBSCRIBE TO EXIUM SERVICE

Visit https://speerity.net



3.2 MANAGE WORKSPACE

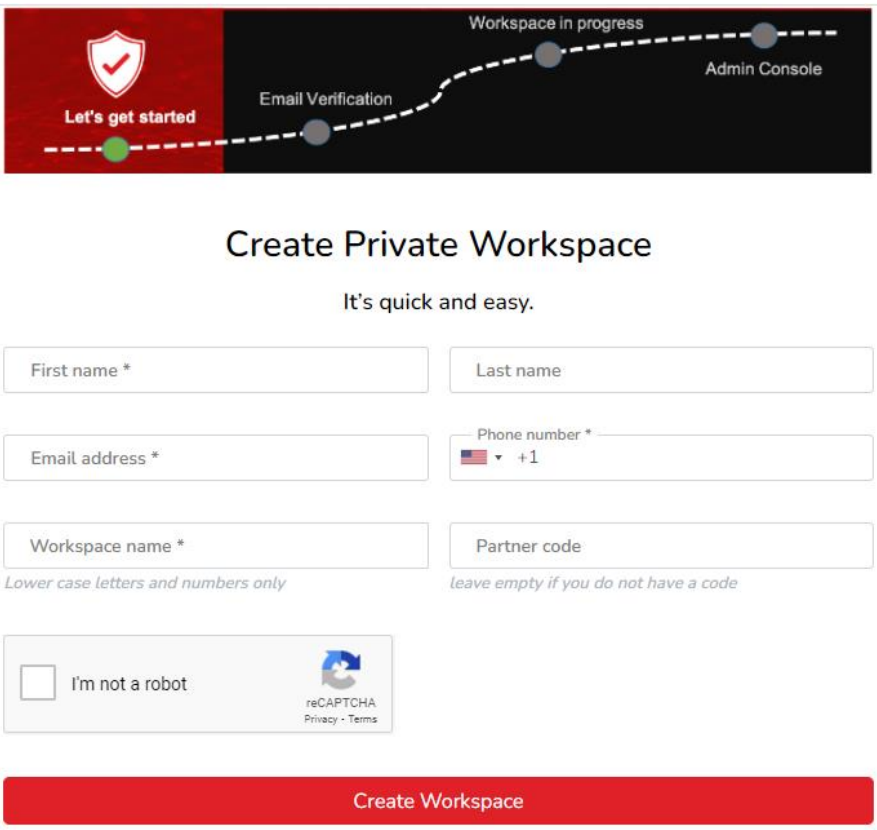
Skip this section (3.2) and navigate to section (3.3) in case user already has an active workspace.

3.2.1 Pre-requisites

A working email address (preferably work mail for enterprise workspaces) to create a workspace with Exium.

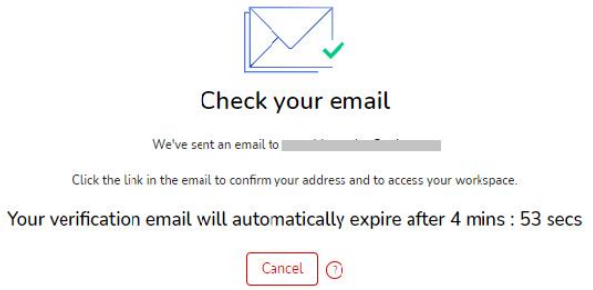
3.2.2 Create Workspace

Proceed to enter all the details like First Name (mandatory), Last Name, Email address (mandatory), Phone number (mandatory) and Workspace name (mandatory). Select checkbox for “I’m not a robot” option.
Click “Create Workspace” once finished.



3.2.3 User Verification

Check your registered email address and verify link by clicking on "CLICK to VERIFY" button. Verification link will be active only for 5 mins.

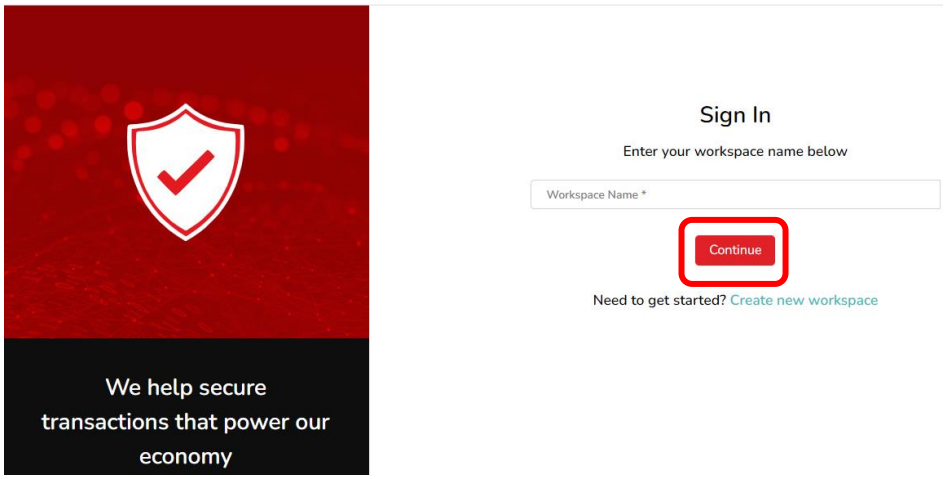


After successful verification, you will be redirected to "Admin Console" page of Exium portal.

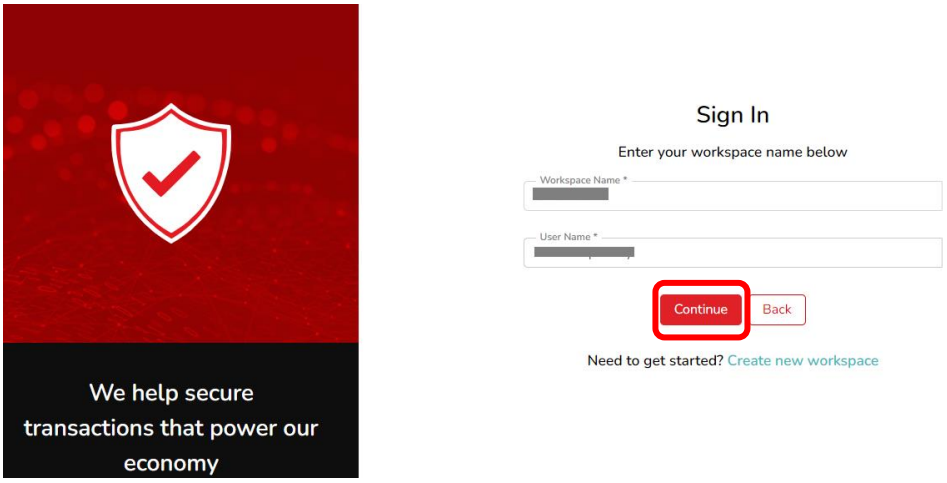
3.3 LOGIN TO WORKSPACE

Navigate to https://speerity.net

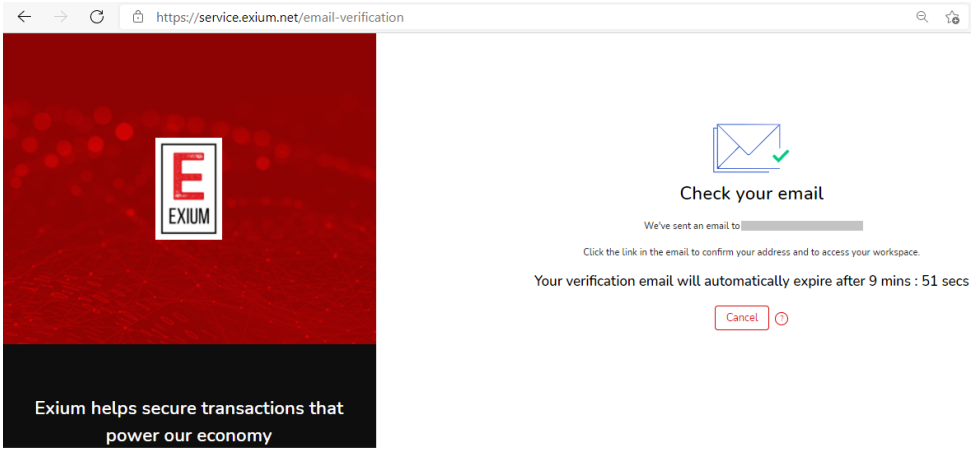
Enter "Workspace Name" and click on "Continue".



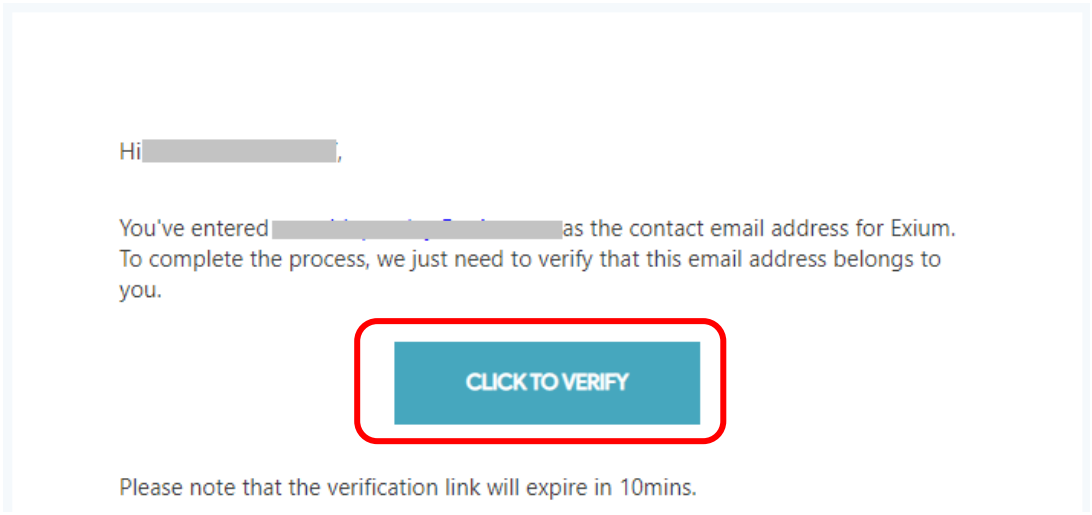
Enter “User Name” and click on “Continue”.



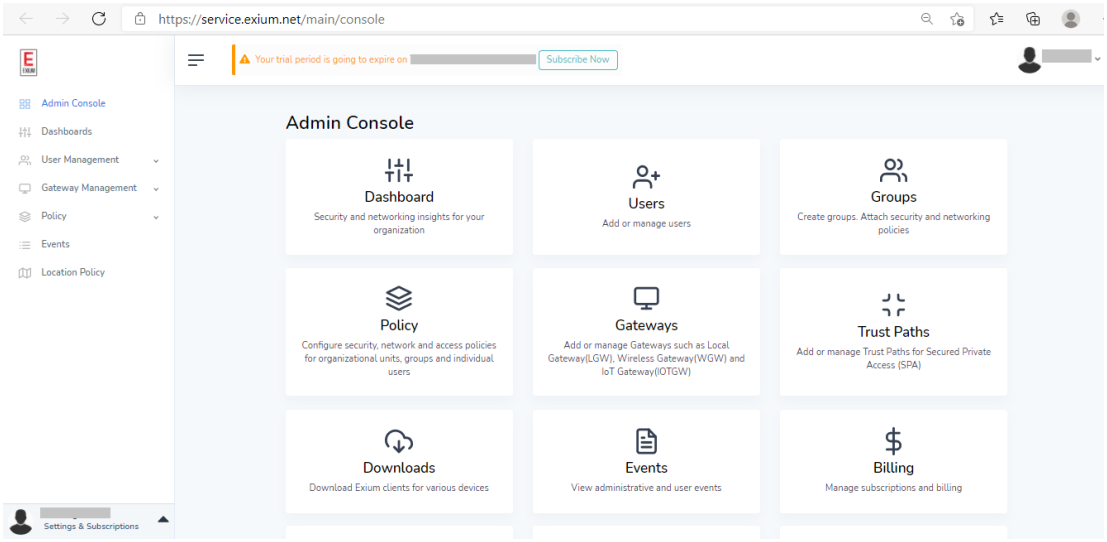
An email will be sent to user’s registered email id for user verification.



Click on “CLICK to VERIFY”.

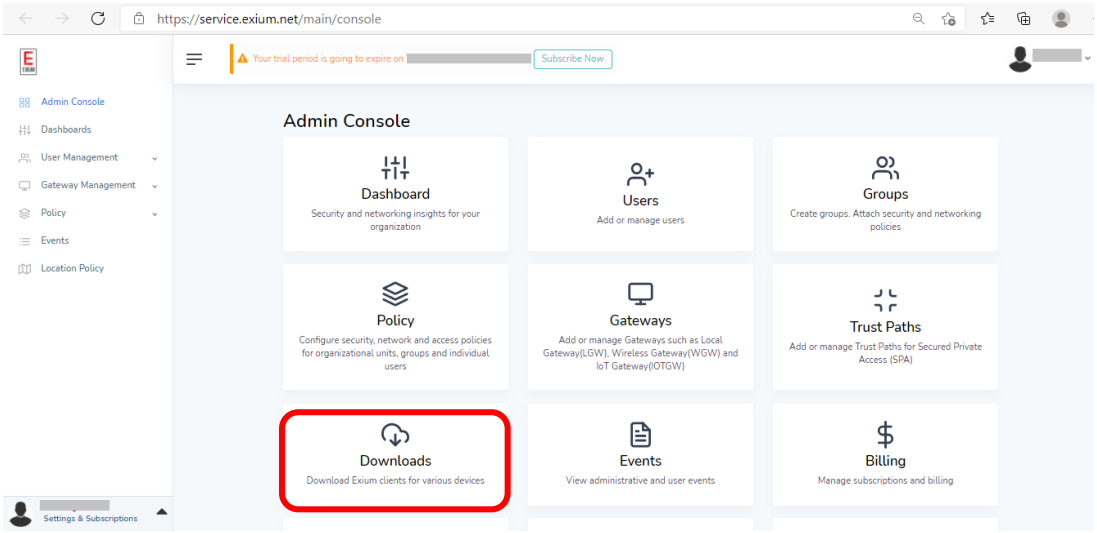


Exium Admin main console will be opened in another web page.



3.4 DOWNLOAD CGW OVA

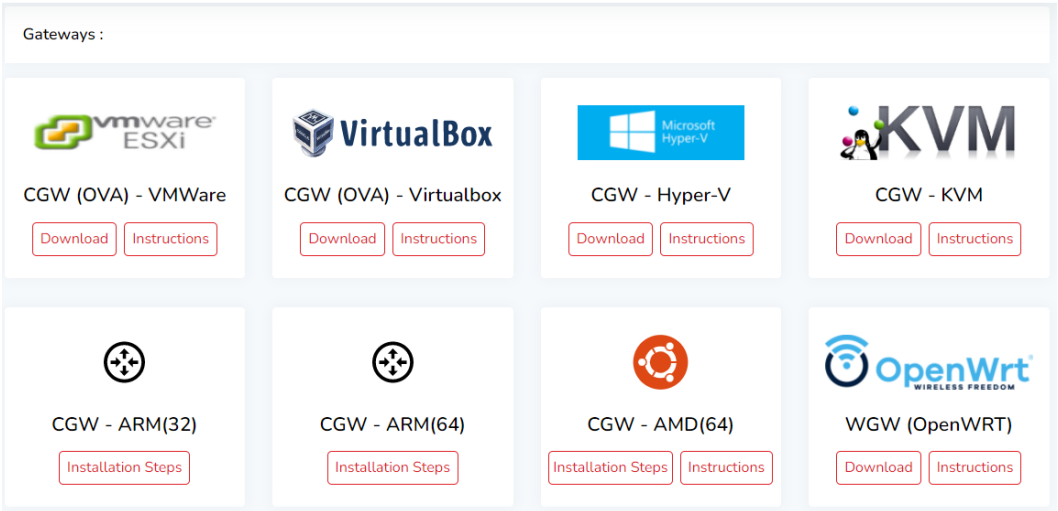
On “Admin Console” page, click on “Downloads” to access CGW (OVA) software.



New web page will open and provide various platform options to download. Platform specific CGW images are available for downloads.

- CGW (ova) for VMWare ESXi
- CGW (ova) for VirtualBox
- CGW (vhdx) for Hyper-V
- CGW (qcow2) for KVM
- CGW for bare metals

Select option according to setup requirement and click on “Downlink” link under CGW option.



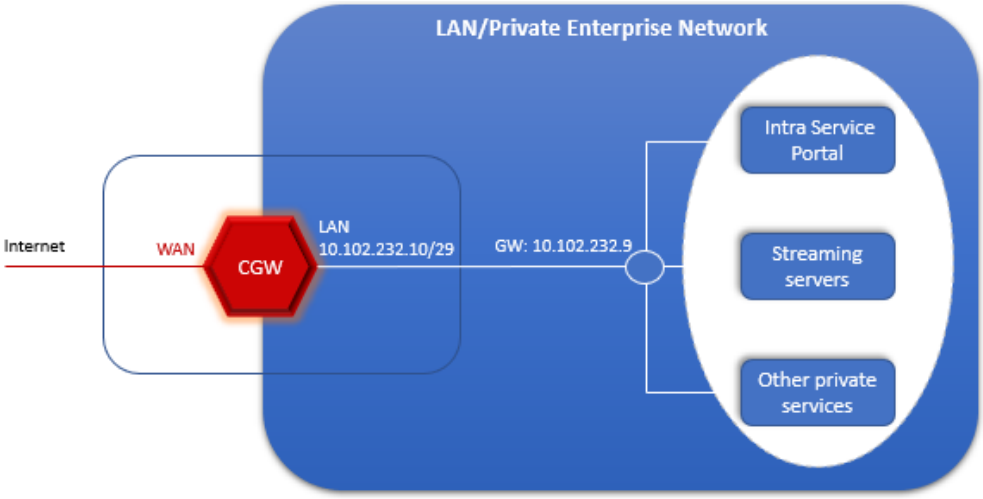
3.5 REFERENCE ARCHITECTURE

There are two ways CGW can be deployed and used for Secure Private Access (SPA):

- Two separate interfaces for WAN and LAN connectivity
- Single interface for WAN and LAN connectivity

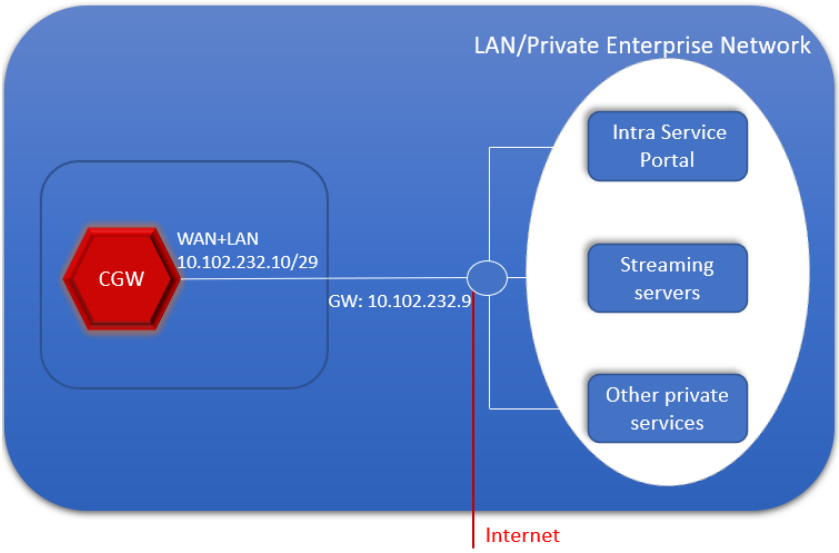
3.5.1 CGW deployment with two interfaces

User can refer below sample diagram to understand the logical network diagram with CGW on their network with two separate interfaces for LAN and WAN connectivity.



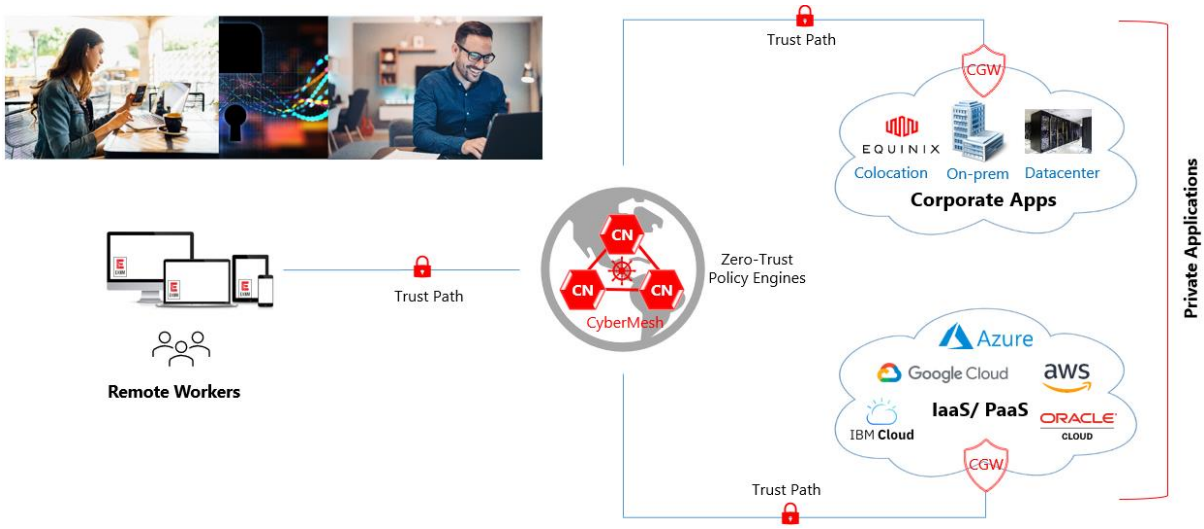
3.5.2 CGW deployment with single interface

User can refer below sample diagram to understand the logical network diagram with CGW on their network with single interface for LAN and WAN connectivity.



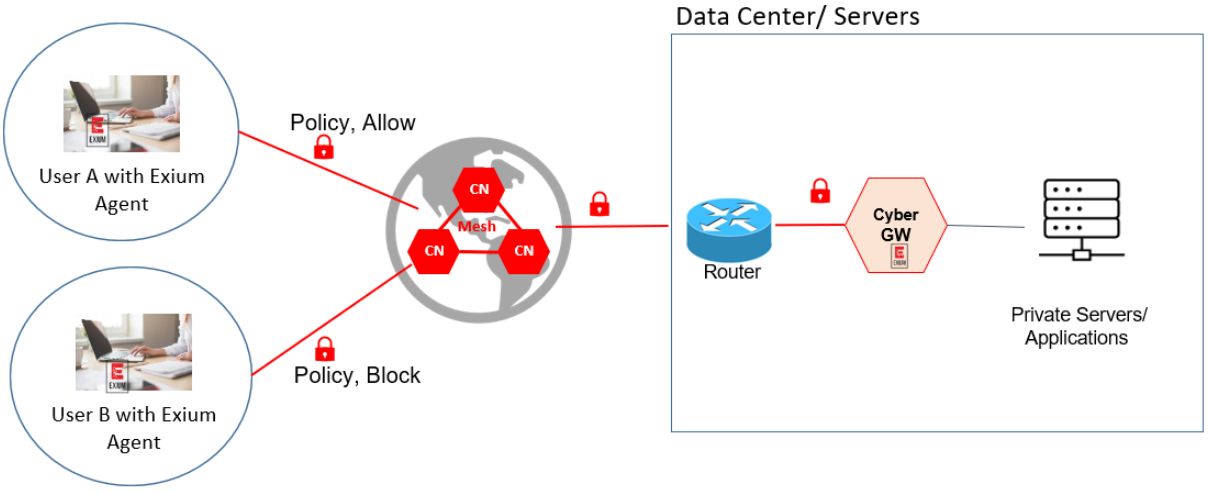
3.6 DEPLOYMENT MODELS

CGW is designed to provide fast, seamless access to private applications using cloud delivered CyberMesh.
Remote workers can connect Exium Clients on their devices and access Corporate Apps, IaaS, PaaS and other private networks.



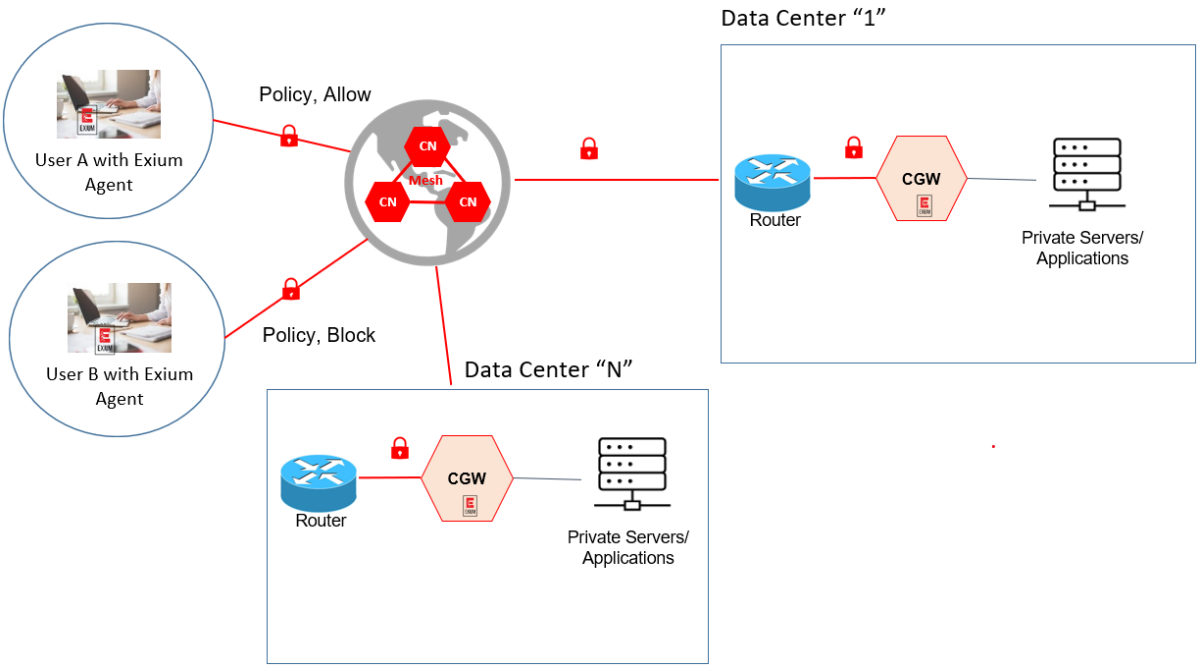
3.6.1 Securing Single Site

User can deploy CGW in one site to access secured private network which keeps sensitive data.



3.6.2 Securing Multiple Sites

User can deploy CGWs in multiple sites to secure internal information exchange which will also keep internal communication secured.
Remote users with Exium Agent connected can access both Data Centers running on different IP subnets, at the same time.
Communication among the data centers will also be secured if they deploy CGW.



3.7 INSTANTIATE VIRTUAL MACHINE

Exium CGW OVA can be deployed on different hypervisors. This deployment guide provides information on prerequisites, how to deploy a Cyber Gateway (CGW) on a VMware platform with vCenter or vSphere Hypervisor (ESXi), on a VirtualBox running on standalone windows laptop and on a KVM server. It also includes post-deployment verification checks.

3.7.1 Deploy on VMWare ESXi using Web Console/GUI

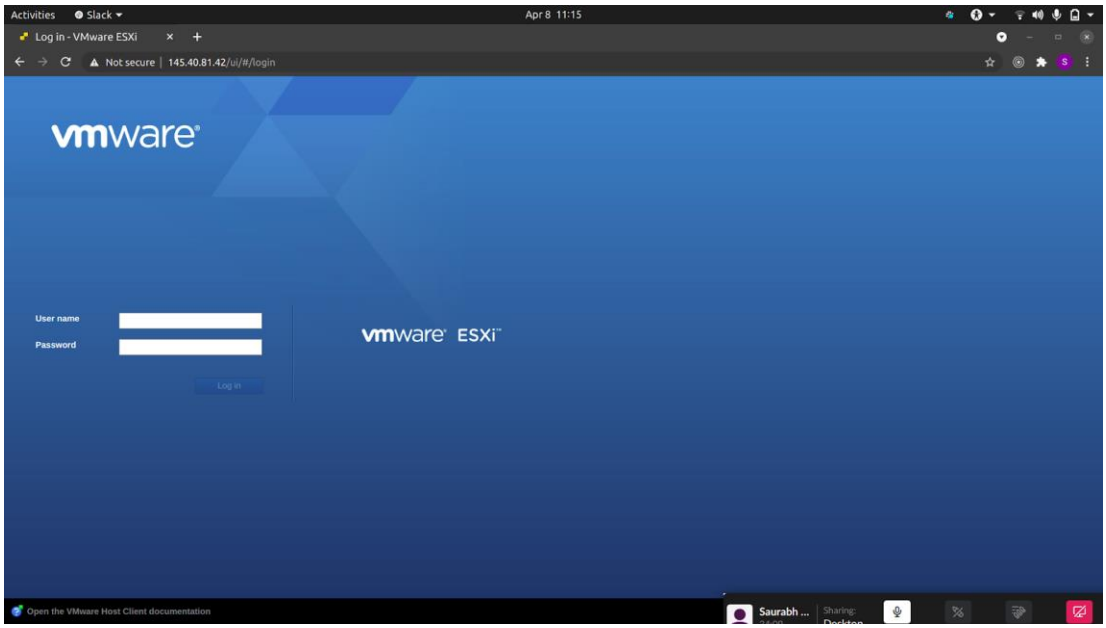
3.7.1.1 Pre-requisites

1. VMWare ESXi 6.5 or above installed and running in bare metal or customer data center.
2. Admin privilege to deploy VMs and edit network settings
3. Link to download Exium CGW OVA
   https://clientreleases.s3.us-west-1.amazonaws.com/cgw/cgw-vm-esxi.ova

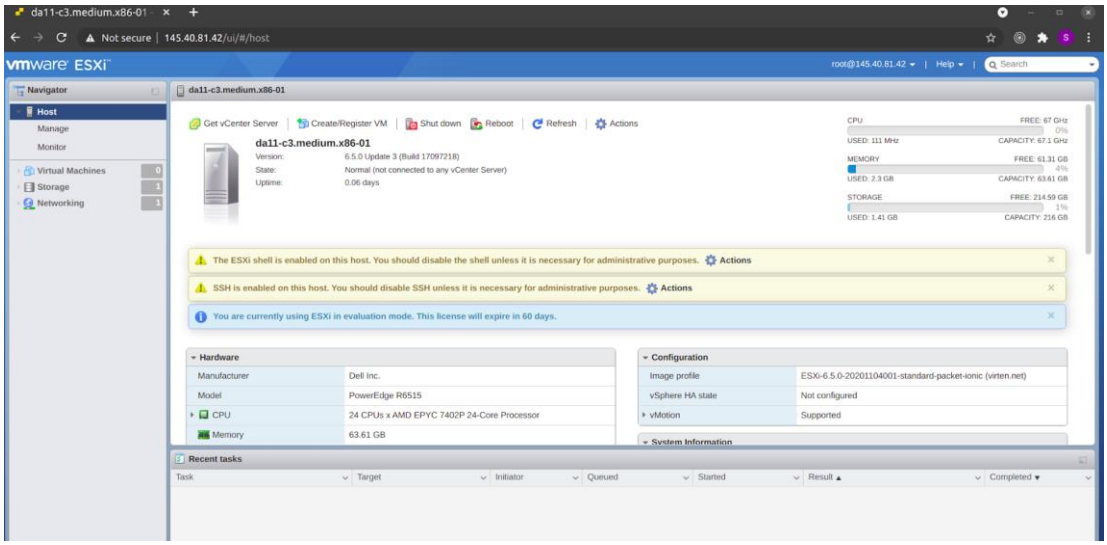
3.7.1.2 Steps to deploy

To deploy a Cyber Gateway on vSphere Hypervisor (ESXi), follow below steps:

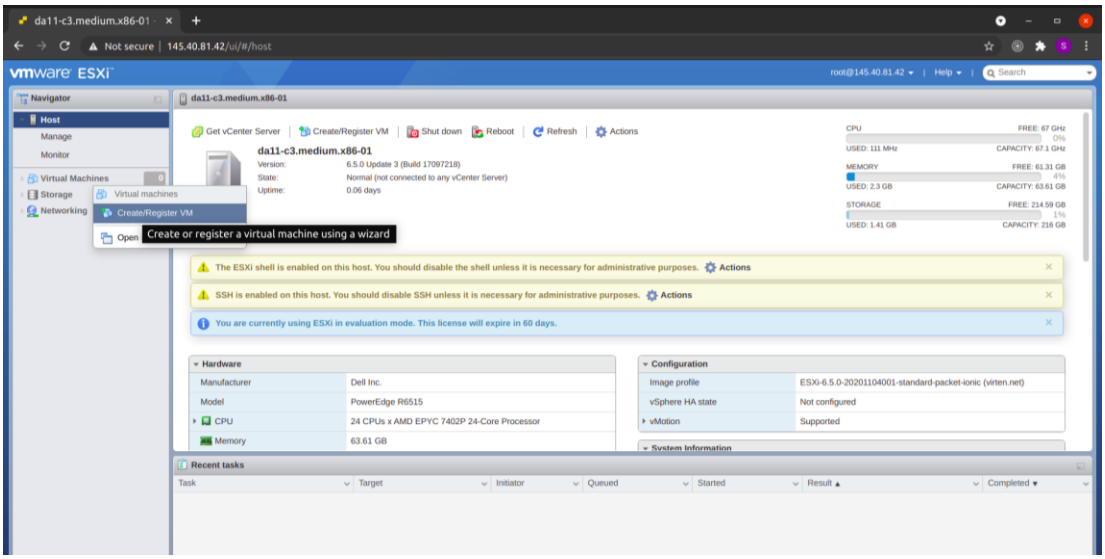
1. Log in to the vSphere Hypervisor (ESXi) Server with web browser using hostname of server for eg. http://<ip-address> or http://<domain-name> . Provide valid user credentials of ESXi host on browser to gain web access.



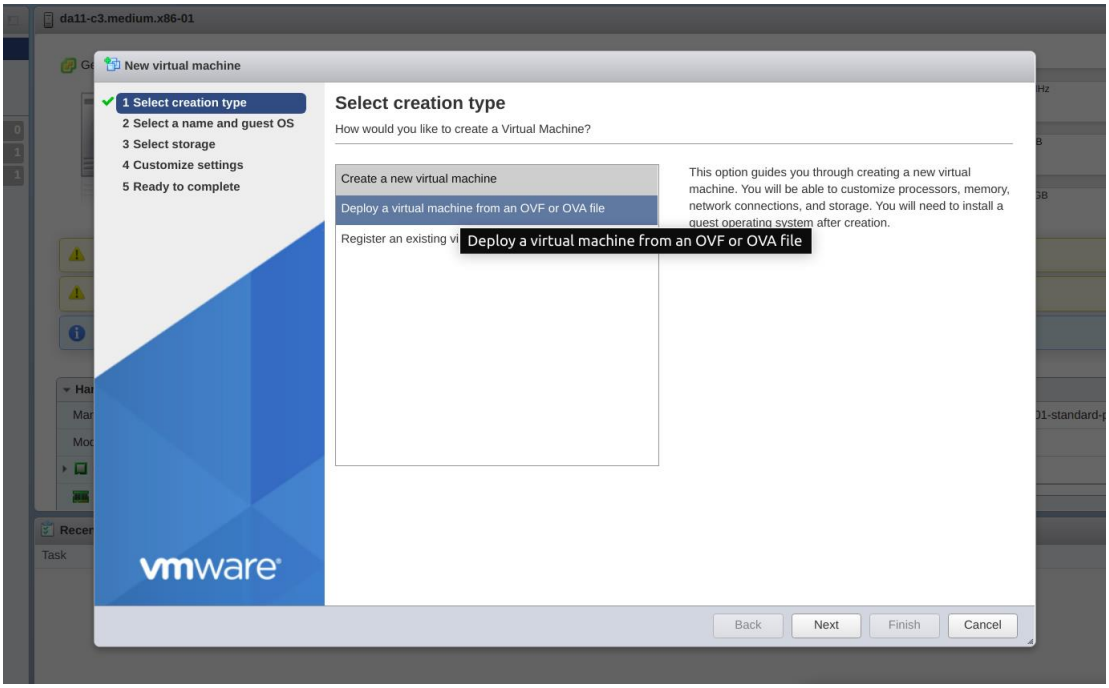
After successful login, home page will appear on screen:



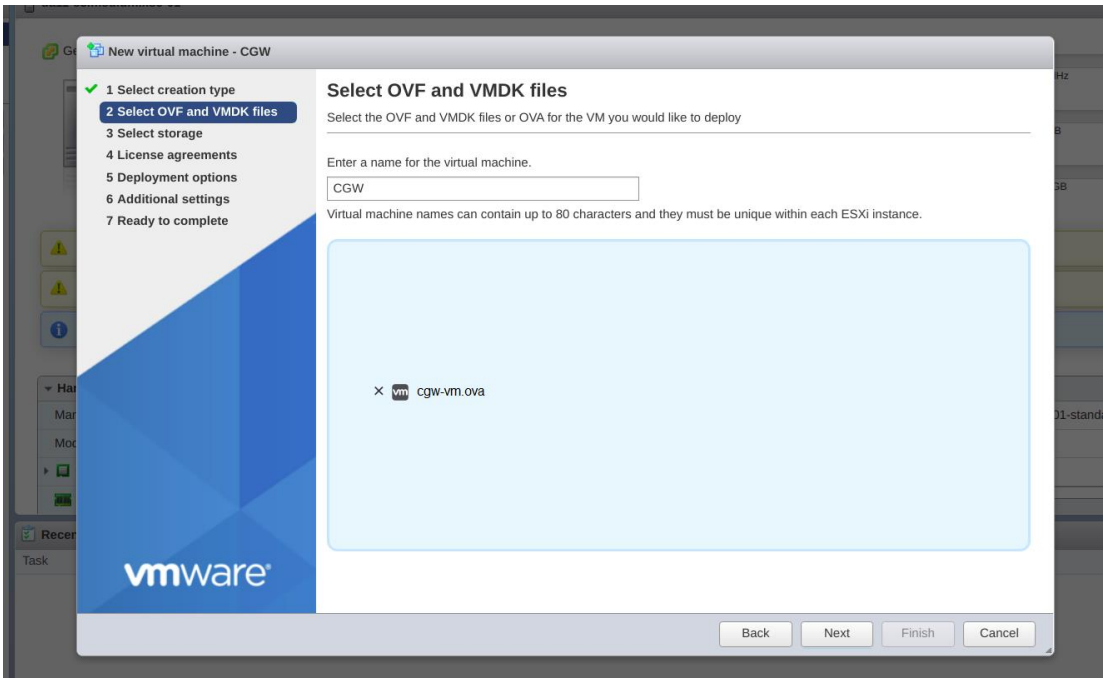
2. Right-Click on **Virtual Machines** & click on Create/Register VM:



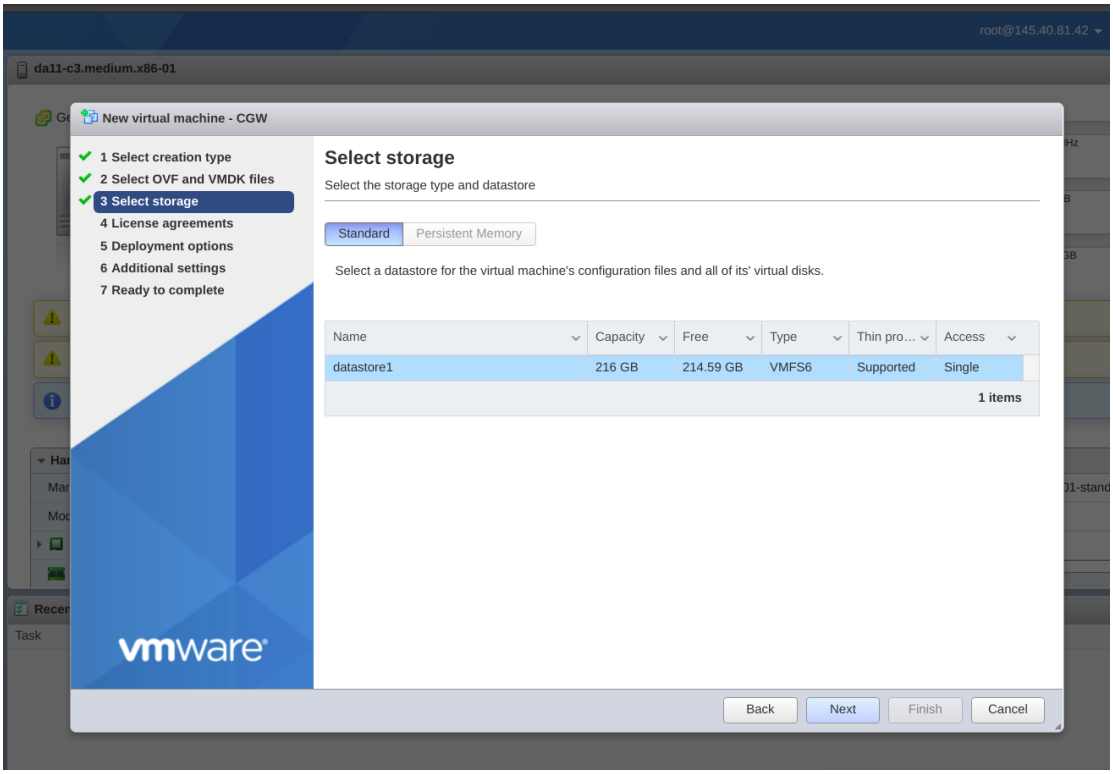
3. Select "**Deploy a virtual machine from an OVF or OVA file**" & click **Next.**



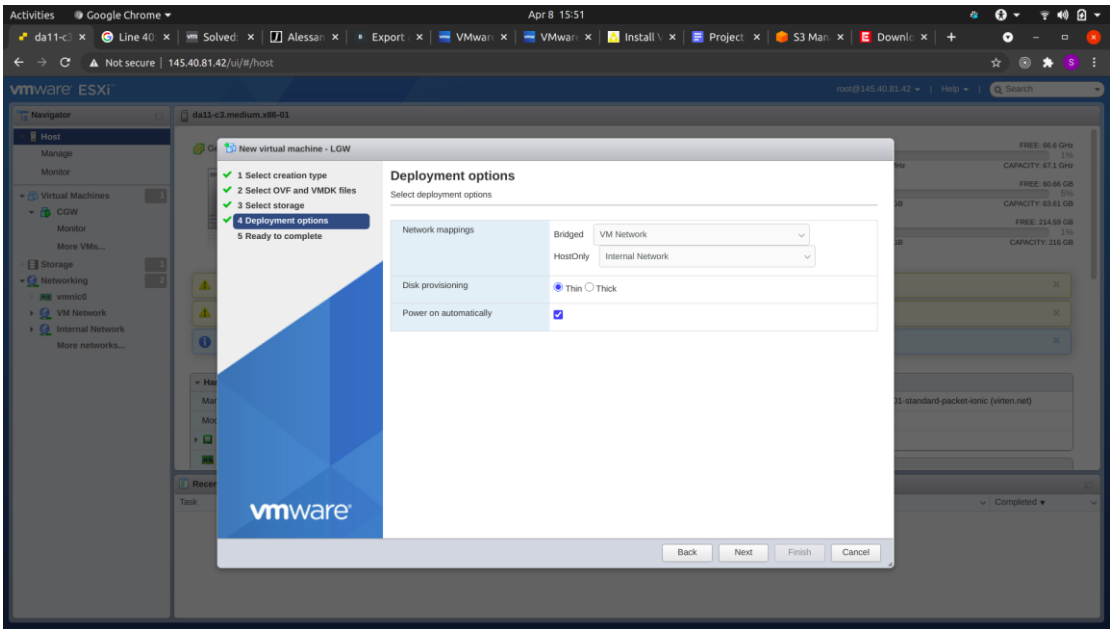
4. Provide a name for the Virtual Machine and upload the downloaded OVA file from Exium portal. Click **Next**

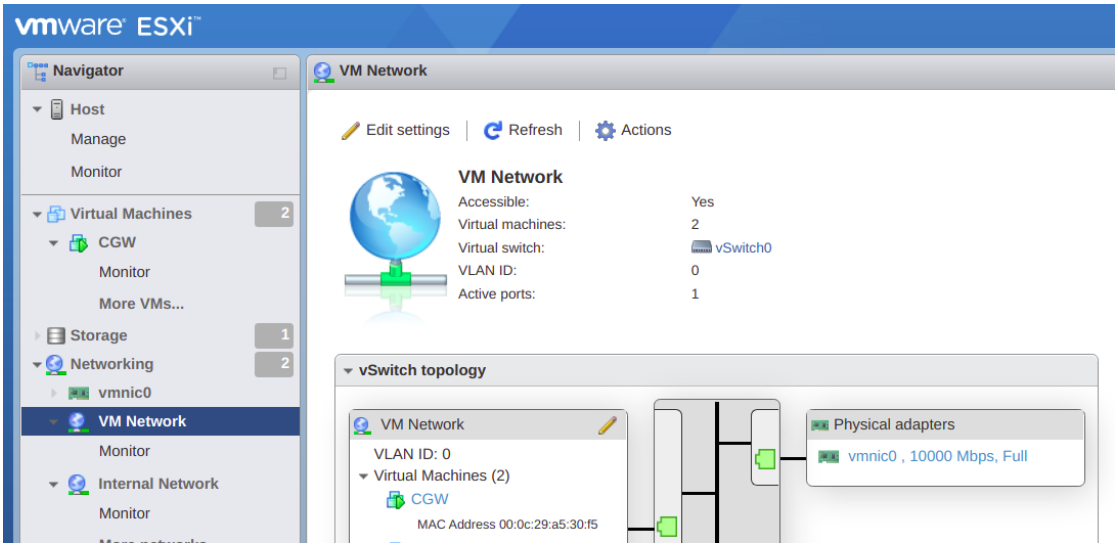


Keep default under storage setting and Click “Next”

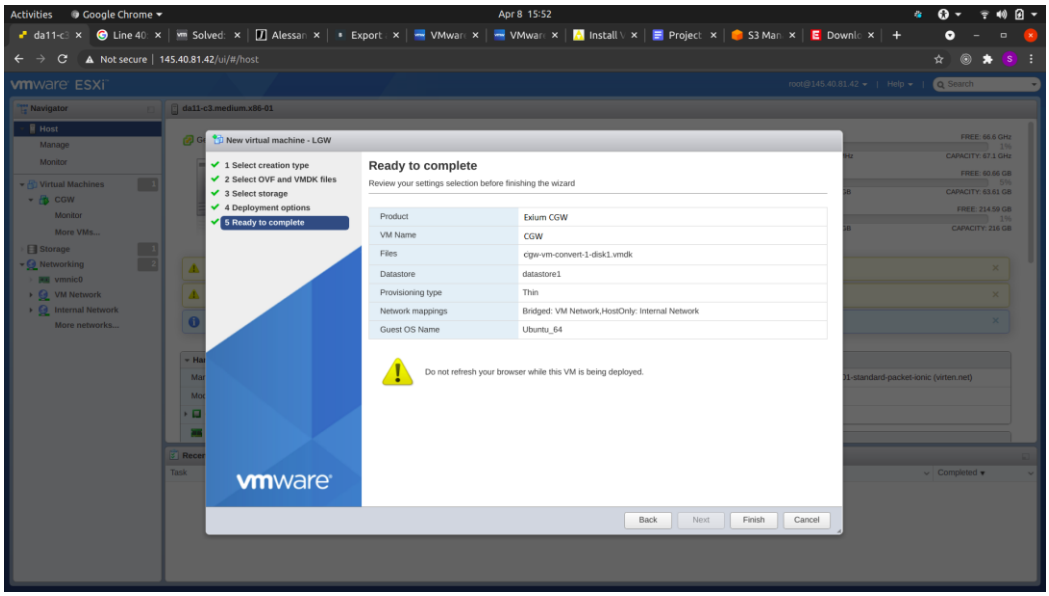


5. Under Deployment Options, Select Network Mapping for Bridged and HostOnly. They should be mapped with correct networks. Use Bridged for WAN/Internet access and HostOnly for LAN/private network

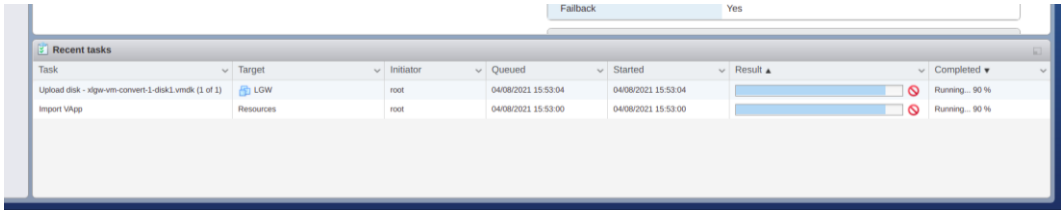




6. Select all the defaults and click **Finish**.



Watch progress Bar in Task and wait for process to complete.



Note: Remove second interface if CGW uses single interface for WAN and LAN connectivity.

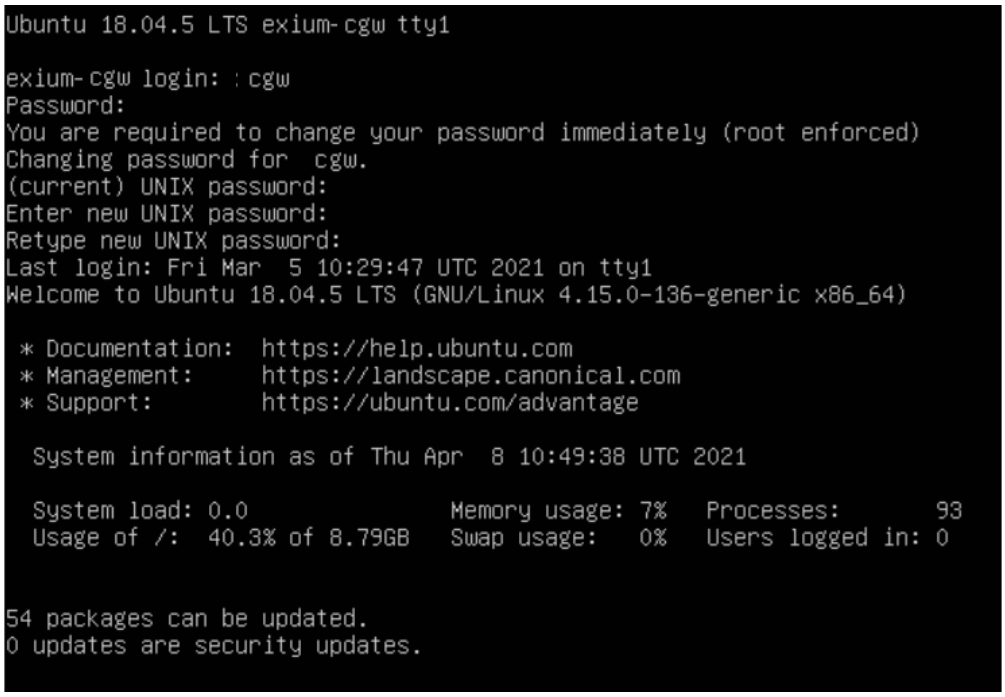
a. Click on CGW VM name
b. Click on Edit Setting
c. Remove second interface

3.7.1.3 Set VM Password

Set your own password during first login by providing default username and password mentioned below.

Login: `cgw`
Password: `cgw`

After successful login to CGW VM, switch user account and become "root" user by executing "sudo su" command.



Note: Password prompt will again appear for networking setup.

3.7.1.4 Install IP addresses on vNICs

After setting the password on the VM terminal, it will again ask to provide password to run the bootstrap script which takes care of IP address allocation using DHCP.

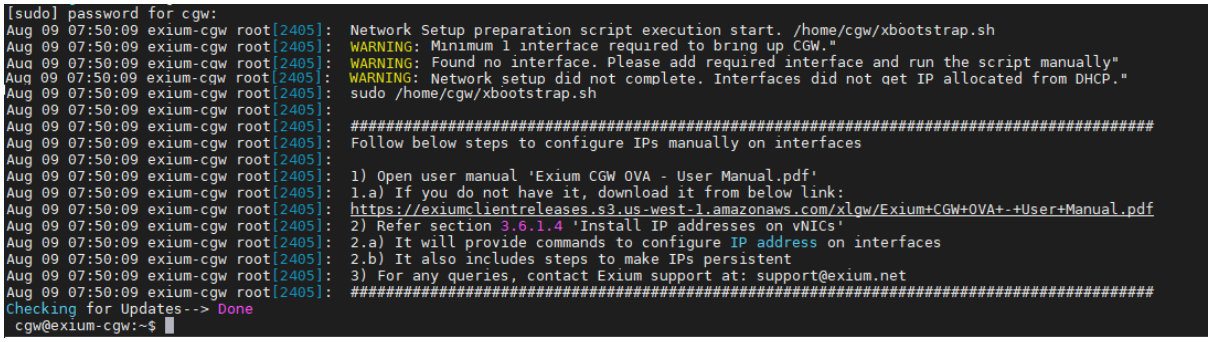
IP address allocation can be handled with below approaches:

- If interfaces on the VM are connected to DHCP enabled network, then IP will be allocated by DHCP server (see below "Bootstrap Script")
- In case of multiple interfaces, if one of the interfaces on the VM is connected to DHCP enabled network, then one interface will get IP from DHCP server, and another must be configured manually (see below "Manual IP Configuration")
- If interfaces on the VM do not have DHCP enabled network, then user must configure IP addresses manually (see below "Manual IP Configuration")

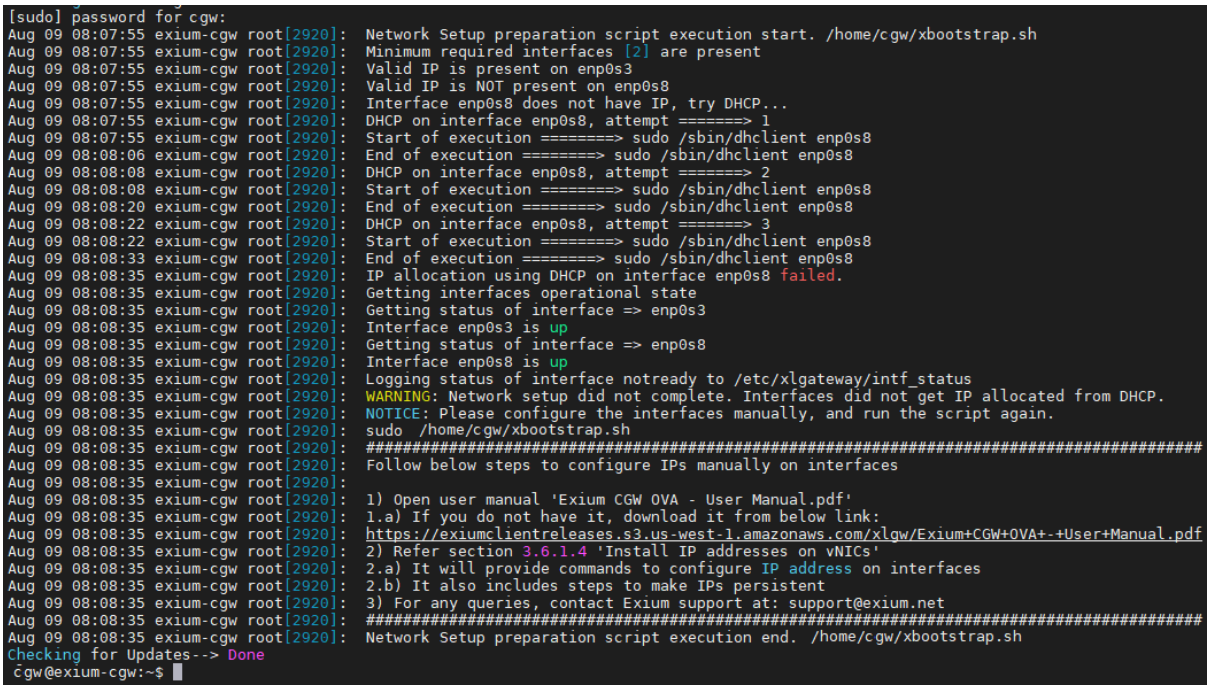
Bootstrap Script

- Script will verify minimum networking requirements and accordingly provide instructions on terminal:
  - Script will pull interface names and request DHCP allocation
    - Configured retries for each interface – 3
    - Configured timeout for each DHCP request – 30 seconds
  - **Case-1: No interface present on CGW VM**

- If minimum one interface is not available, then execution will end with warning

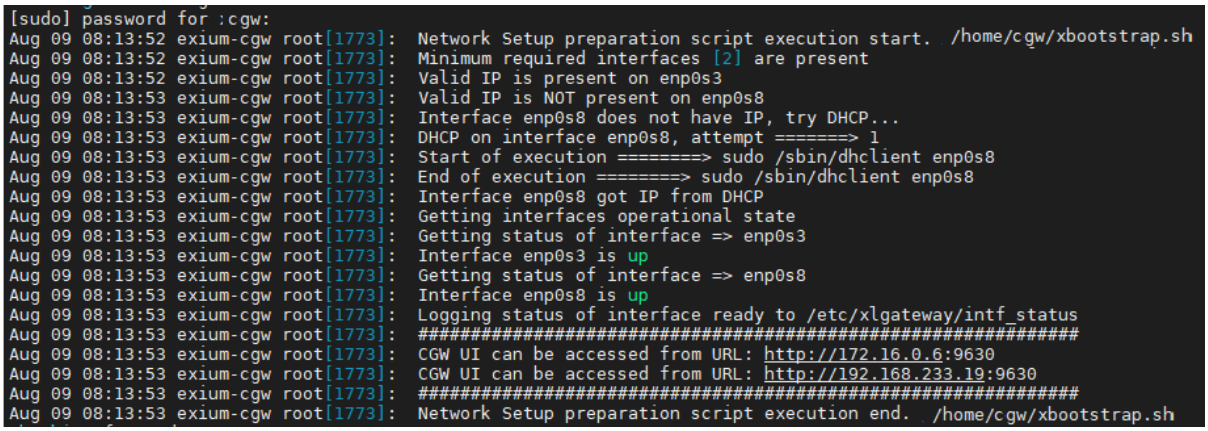


- **Case-2: DHCP on one interface only**
  - In case two interfaces are available and one of the interfaces gets IP from DHCP, but second interface does not:
    - Execution will end with warning



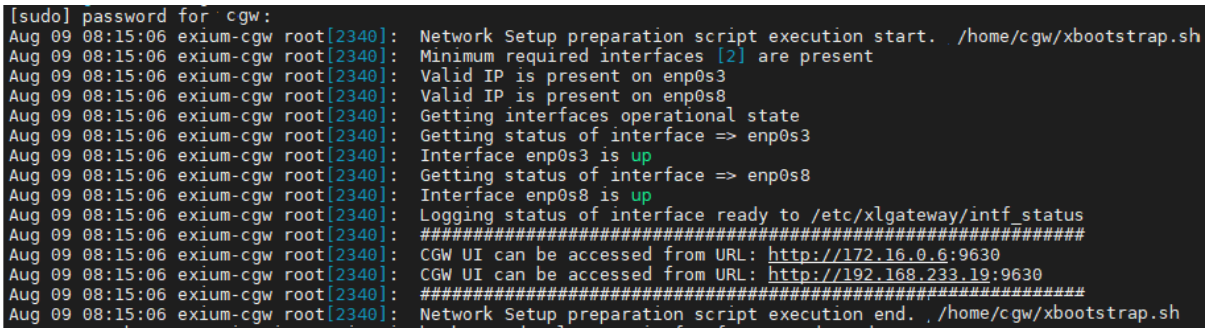
  - Refer “Manual IP Configuration” section included below
  - After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI
    `# sudo /home/cgw/xbootstrap.sh`

- **Case-3: DHCP on both interfaces**
  - If interfaces get IP addresses from DHCP and states are up:
    - Execution will end and it will show the URLs which can be used to access CGW UI



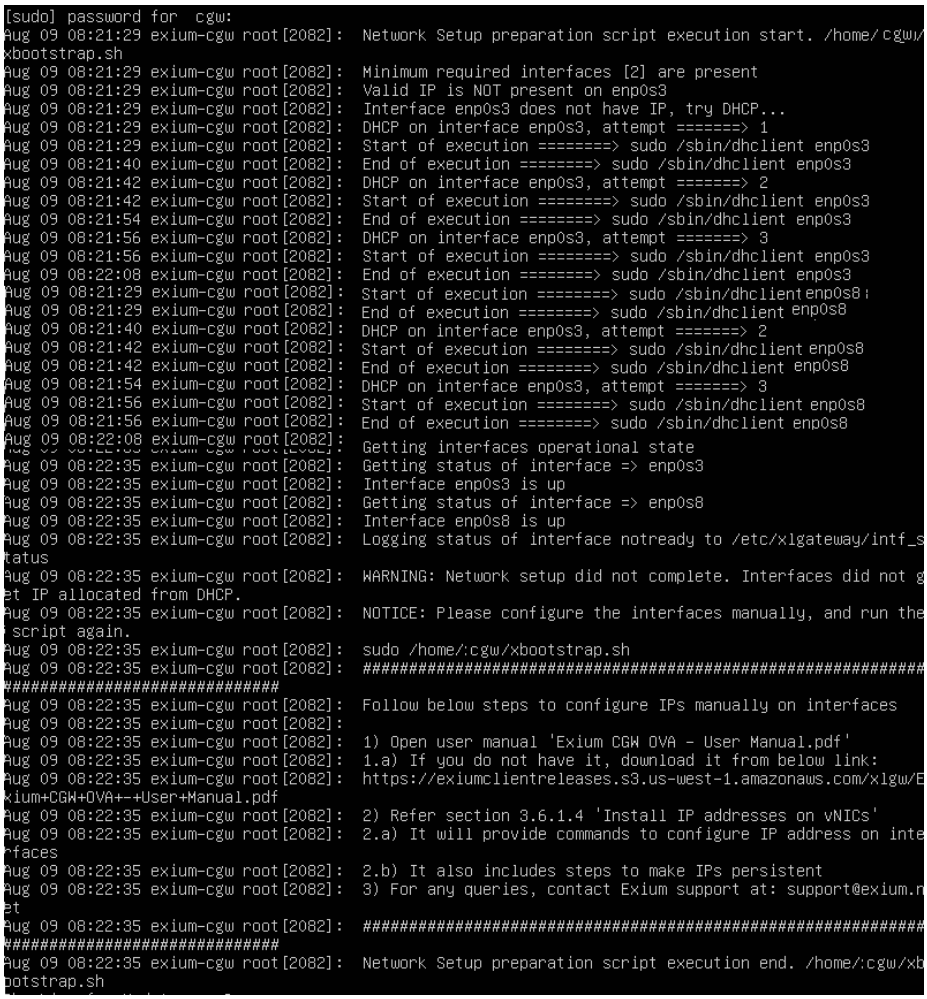
- **Case-4: IP addresses are already assigned on both interfaces**
  - If valid IP present on interface:
    - Execution will end with validations on both interface
    - Instructions will show URLs which can be used to access CGW UI
    - For eg: CGW UI access URL format would be **http://<CGW-IP>:9630**

- Each time user logs into CGW VM using "cgw" user credentials, bootstrap script will run and validate the interface IPs and states.



Manual IP configuration

- **No DHCP on interface**
  - If associated/attached network does not allocate IP address using DHCP then execution will end with warning

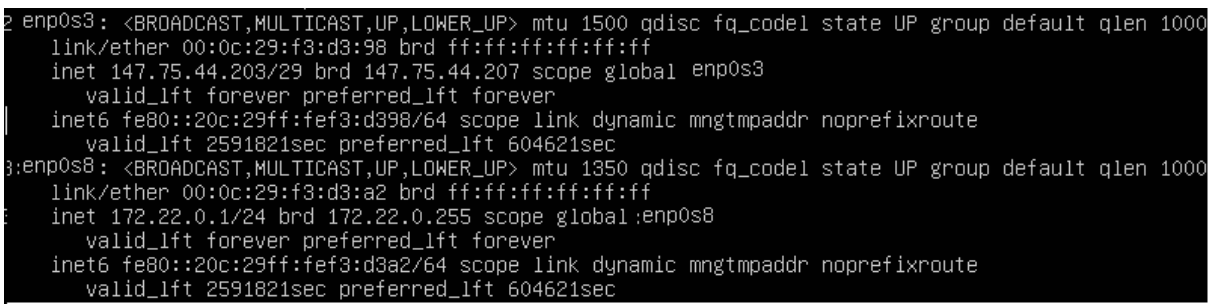


Use Command "`sudo ip addr`" to check interfaces installed:

Note: If there is only one interface then skip command/step for another interface.

Use below commands to configure IP addresses manually:

```
# sudo ifconfig enp0s3 <WAN-ip-address>/<WAN-mask> up
# sudo ifconfig enp0s8 <LAN-ip-address>/<LAN-mask> up
```

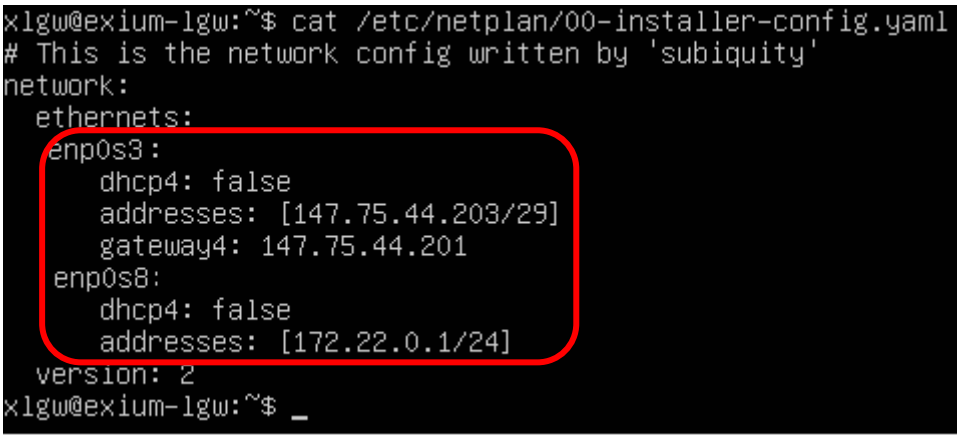


Use "netplan" utility to make IP addresses static on VM.

- Edit existing netplan and include the IP address installed manually.

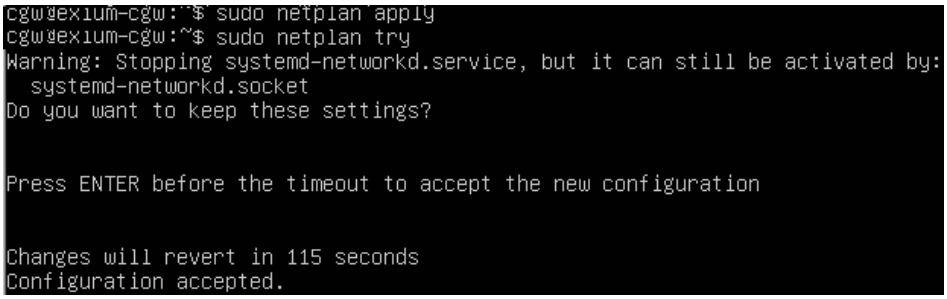
```
# sudo vim /etc/netplan/00-installer-config.yaml
```

- Add interface details:
  - Name of the interface
  - dhcpv4: false
  - addresses: IP address to be installed: Same IP which was configured manually
  - gateway4: Default gateway of the interface



- Apply the configuration:
  `# sudo netplan apply`

- Verify configuration
  `# sudo netplan try`
- Press enter, when the timer starts.
  - Configuration Accepted will be shown in case of successful scenario.



- After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI
  `# sudo /home/cgw/xbootstrap.sh`

- Verify the local time on the VMware machine is correct. If it is not, update the time using Network Time Protocol.

- Verify internet is accessible from CGW VM. If not, update the network settings accordingly.

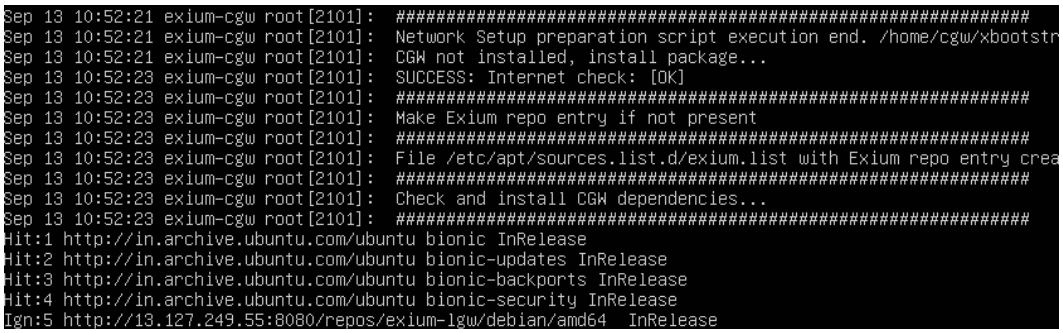
- In case Cyber Gateway (CGW) is configured with 2 separate interfaces (vNICs). One interface for internet access (WAN) and another interface connected on LAN network, then make sure both vNICs are configured with different subnets or associated to different networks.

- In case Cyber Gateway (CGW) is configured with 2 separate interfaces (vNICs), All the machines/devices behind the Cyber Gateway must be configured with Default Gateway i.e. IP address configured on the LAN interface of Cyber Gateway VM. Those machines must be reachable from CGW LAN interface.

3.7.1.5 CGW Software Installation

After IP addresses installation, bootstrap script will check internet connectivity. If internet is not accessible, then script will exit with warning, else it will continue with installation procedure.

Check default routes and verify DNS resolution and internet connection work from CGW VM. Once internet is accessible from CGW VM, run bootstrap script again to complete installation process.



Installation includes, CGW dependent packages installation, tuning parameters setting and latest CGW application software installation.

After successful installation, terminal will show below output:

Navigate to Section 3.11, to setup CGW.

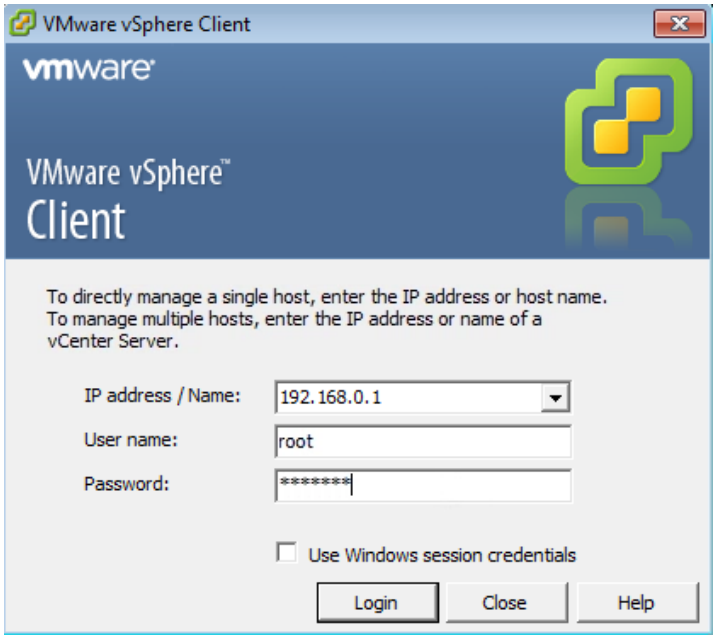
3.7.2 Deploy on VMWare ESXi using vSphere Client

3.7.2.1 Pre-requisites

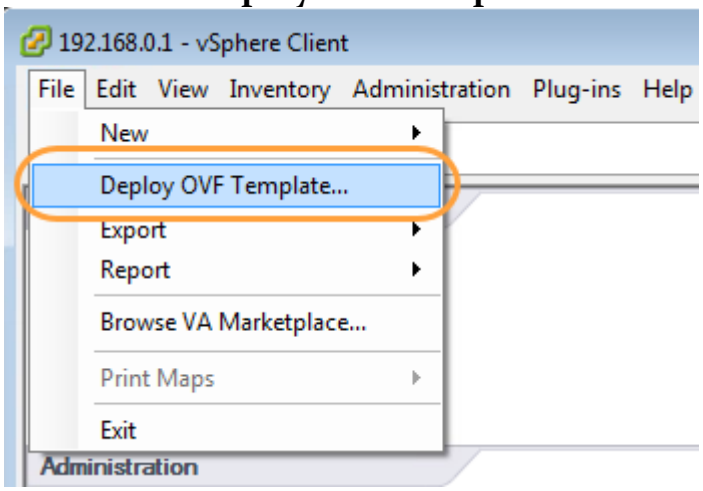
4. VMWare ESXi 6.5 or above installed and running in bare metal or customer data center.
5. Admin privilege to deploy VMs and edit network settings
6. Link to download Exium CGW OVA

3.7.2.2 Steps to deploy

To deploy a Cyber Gateway on vSphere Hypervisor (ESXi), follow below steps:
Log in to the vSphere Hypervisor (ESXi) Server with the vSphere Client.
Provide valid user credentials and management IP address of the ESXi host on VMware vSphere Client login screen.



2. Go to **File** > **Deploy OVF Template...**.



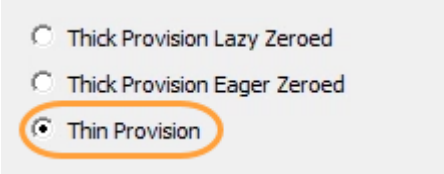
3. Complete one of the following procedures:

a. Enter the following URL for the App Connector image into the provided field: https://clientreleases.s3.us-west-1.amazonaws.com/cgw/cgw-vm-esxi.ova, then click **Next**:

If this option is selected, the image is downloaded from the URL and uploaded to the vSphere Hypervisor (ESXi) server from the local system.

If you've already downloaded the VMware image to your local system, **Browse...** to the location of the image file, then click **Next**.

4. Verify that the **OVF Template Details** are correct, then click **Next**.
5. The **Name and Location** specified in vSphere Hypervisor (ESXi) has no impact on the Exium service. So, select a name and folder that is suitable for your organization, then click **Next**.
6. After you are asked to select a **Storage** configuration, make sure that you select **Thin Provision** for the disk format, then click **Next**. This selection generally results in smaller disk space utilization.



Ensure that **Power on after deployment** is selected, then click **Finish**.

Within the **Recent Tasks** panel, you can monitor the deployment progress. After the deployment has successfully completed, ensure that the VM has powered on before proceeding to the next step.

7. Edit network settings, by clicking on Edit button available for CGW VM. Select Network Mapping for Bridged and HostOnly. They should be mapped with correct networks. Use Bridged for WAN/Internet access and HostOnly for LAN/private network.

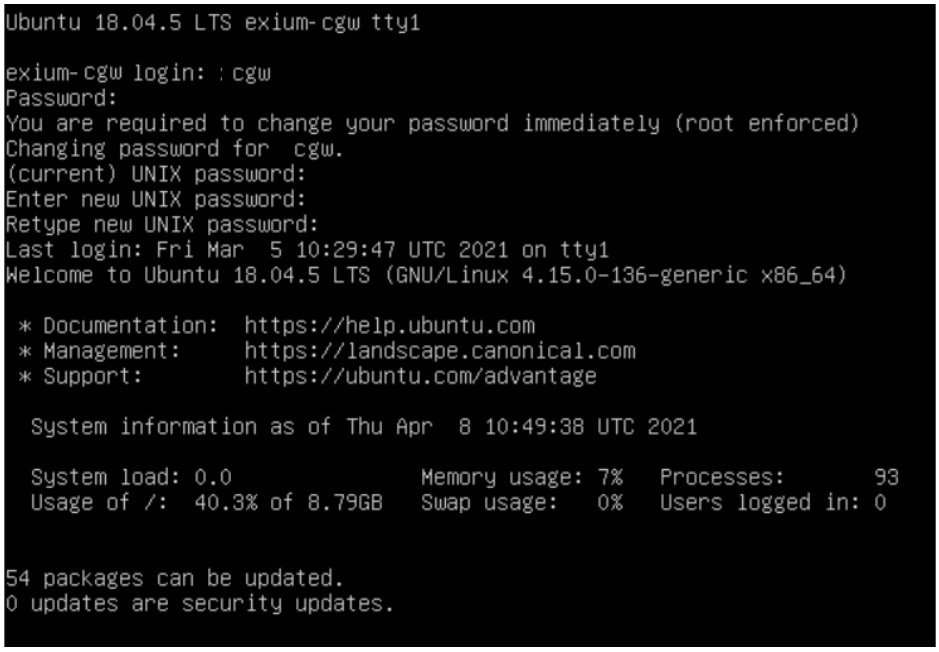
Note: Remove second interface if CGW is planned to have single interface for WAN and LAN connectivity.

3.7.2.3 Set VM Password

Set your own password during first login by providing default username mentioned below.

Login: `cgw`
Password: `cgw`

After successful login to CGW VM, switch user account and become "root" user by executing "sudo su" command.



3.7.2.4 Install IP addresses on vNICs

After setting the password on the VM terminal, it will again ask to provide password to run the bootstrap script which takes care of IP address allocation using DHCP.

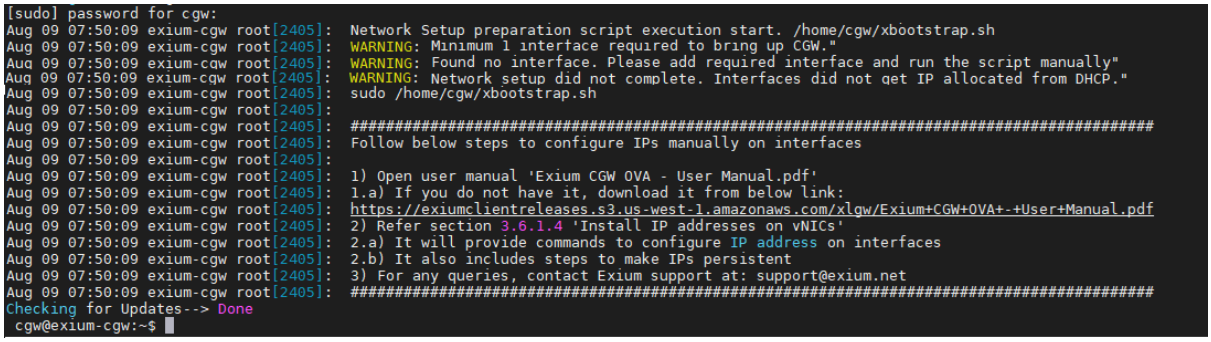
IP address allocation can be handled with below approaches:

- If interfaces on the VM are connected to DHCP enabled network, then IP will be allocated by DHCP server (see below “Bootstrap Script”)
- In case of multiple interfaces, if one of the interfaces on the VM is connected to DHCP enabled network, then one interface will get IP from DHCP server, and another must be configured manually (see below “Manual IP Configuration”)
- If interfaces on the VM do not have DHCP enabled network, then user must configure IP addresses manually (see below “Manual IP Configuration”)

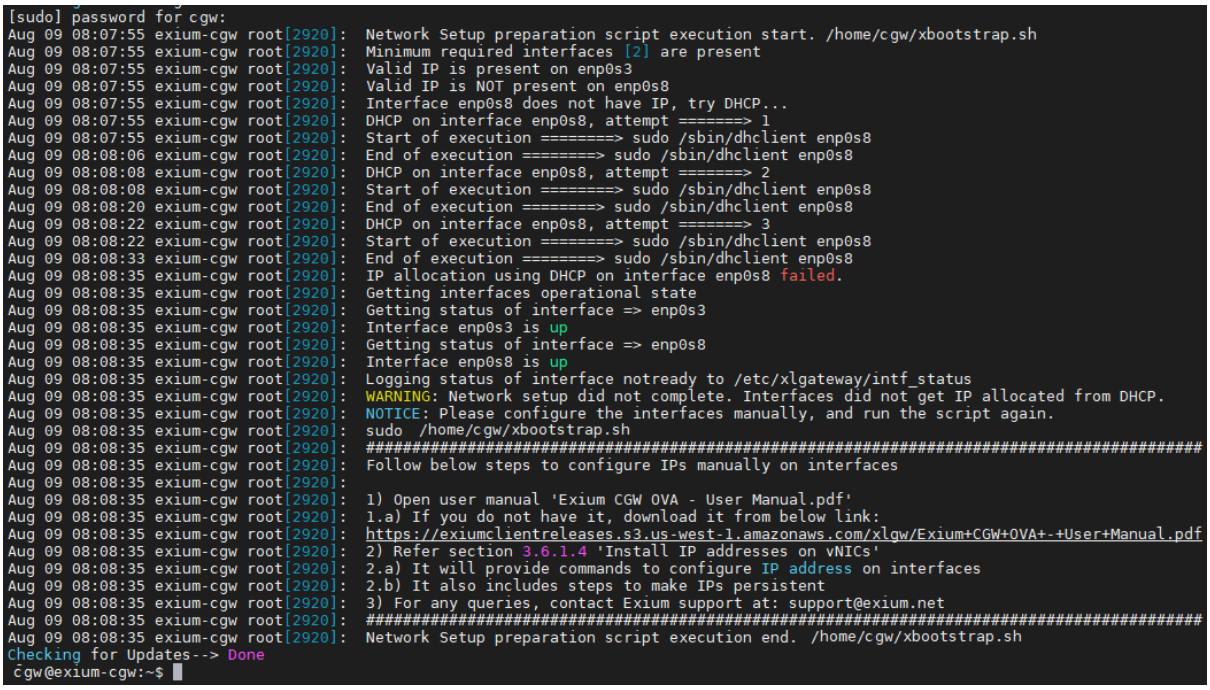
Bootstrap Script

- Script will verify minimum networking requirements and accordingly provide instructions on terminal:
  - Script will pull interface names and request DHCP allocation
    - Configured retries for each interface – 3
    - Configured timeout for each DHCP request – 30 seconds
  - **Case-1: No interface present on CGW VM**

- If minimum one interface is not available, then execution will end with warning



- **Case-2: DHCP on one interface only**
  - In case two interfaces are available and one of the interfaces gets IP from DHCP, but second interface does not:
    - Execution will end with warning



  - Refer “Manual IP Configuration” section included below
  - After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI
    `# sudo /home/cgw/xbootstrap.sh`

- **Case-3: DHCP on both interfaces**
  - If interfaces get IP addresses from DHCP and states are up:
    - Execution will end and it will show the URLs which can be used to access CGW UI

```
[sudo] password for :cgw:
Aug 09 08:13:52 exium-cgw root[1773]:  Network Setup preparation script execution start.  /home/cgw/xbootstrap.sh
Aug 09 08:13:52 exium-cgw root[1773]:  Minimum required interfaces [2] are present
Aug 09 08:13:52 exium-cgw root[1773]:  Valid IP is present on enp0s3
Aug 09 08:13:53 exium-cgw root[1773]:  Valid IP is NOT present on enp0s8
Aug 09 08:13:53 exium-cgw root[1773]:  Interface enp0s8 does not have IP, try DHCP...
Aug 09 08:13:53 exium-cgw root[1773]:  DHCP on interface enp0s8, attempt =======> 1
Aug 09 08:13:53 exium-cgw root[1773]:  Start of execution ========> sudo /sbin/dhclient enp0s8
Aug 09 08:13:53 exium-cgw root[1773]:  End of execution ========> sudo /sbin/dhclient enp0s8
Aug 09 08:13:53 exium-cgw root[1773]:  Interface enp0s8 got IP from DHCP
Aug 09 08:13:53 exium-cgw root[1773]:  Getting interfaces operational state
Aug 09 08:13:53 exium-cgw root[1773]:  Getting status of interface => enp0s3
Aug 09 08:13:53 exium-cgw root[1773]:  Interface enp0s3 is up
Aug 09 08:13:53 exium-cgw root[1773]:  Getting status of interface => enp0s8
Aug 09 08:13:53 exium-cgw root[1773]:  Interface enp0s8 is up
Aug 09 08:13:53 exium-cgw root[1773]:  Logging status of interface ready to /etc/xlgateway/intf_status
Aug 09 08:13:53 exium-cgw root[1773]:  ############################################################
Aug 09 08:13:53 exium-cgw root[1773]:  CGW UI can be accessed from URL: http://172.16.0.6:9630
Aug 09 08:13:53 exium-cgw root[1773]:  CGW UI can be accessed from URL: http://192.168.233.19:9630
Aug 09 08:13:53 exium-cgw root[1773]:  ############################################################
Aug 09 08:13:53 exium-cgw root[1773]:  Network Setup preparation script execution end.  /home/cgw/xbootstrap.sh
```

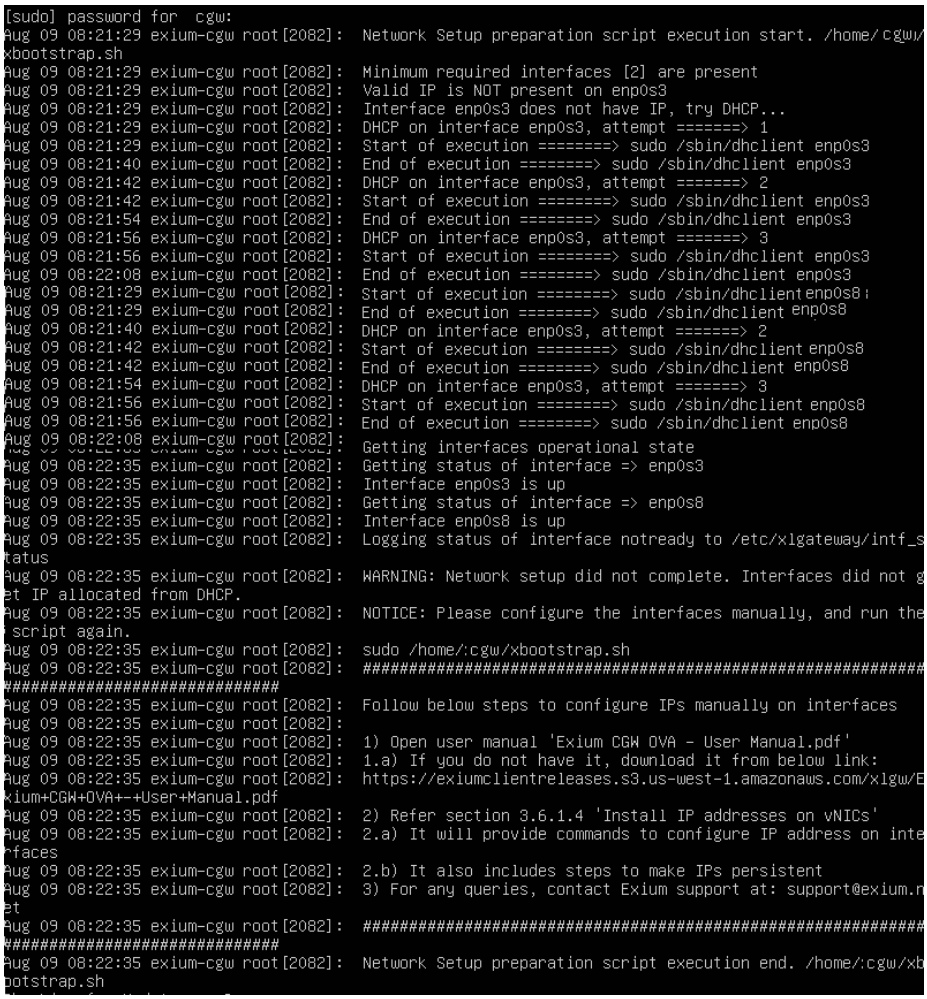
- **Case-4: IP addresses are already assigned on both interfaces**
  - If valid IP present on interface:
    - Execution will end with validations on both interface
    - Instructions will show URLs which can be used to access CGW UI
    - For eg: CGW UI access URL format would be **http://<CGW-IP>:9630**

- Each time user logs into CGW VM using “cgw” user credentials, bootstrap script will run and validate the interface IPs and states.

```
[sudo] password for cgw:
Aug 09 08:15:06 exium-cgw root[2340]:  Network Setup preparation script execution start.  /home/cgw/xbootstrap.sh
Aug 09 08:15:06 exium-cgw root[2340]:  Minimum required interfaces [2] are present
Aug 09 08:15:06 exium-cgw root[2340]:  Valid IP is present on enp0s3
Aug 09 08:15:06 exium-cgw root[2340]:  Valid IP is present on enp0s8
Aug 09 08:15:06 exium-cgw root[2340]:  Getting interfaces operational state
Aug 09 08:15:06 exium-cgw root[2340]:  Getting status of interface => enp0s3
Aug 09 08:15:06 exium-cgw root[2340]:  Interface enp0s3 is up
Aug 09 08:15:06 exium-cgw root[2340]:  Getting status of interface => enp0s8
Aug 09 08:15:06 exium-cgw root[2340]:  Interface enp0s8 is up
Aug 09 08:15:06 exium-cgw root[2340]:  Logging status of interface ready to /etc/xlgateway/intf_status
Aug 09 08:15:06 exium-cgw root[2340]:  ############################################################
Aug 09 08:15:06 exium-cgw root[2340]:  CGW UI can be accessed from URL: http://172.16.0.6:9630
Aug 09 08:15:06 exium-cgw root[2340]:  CGW UI can be accessed from URL: http://192.168.233.19:9630
Aug 09 08:15:06 exium-cgw root[2340]:  ############################################################
Aug 09 08:15:06 exium-cgw root[2340]:  Network Setup preparation script execution end.  /home/cgw/xbootstrap.sh
```

Manual IP configuration

- **No DHCP on interface**
  - If associated/attached network does not allocate IP address using DHCP then execution will end with warning

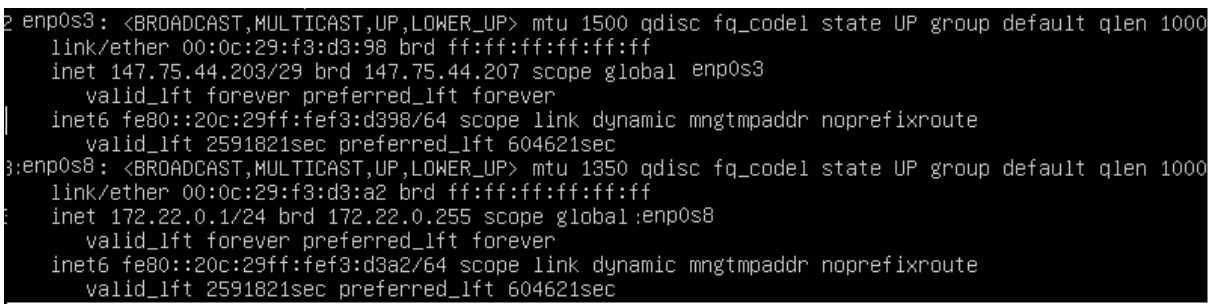


Use Command "`sudo ip addr`" to check interfaces installed:

Note: If there is only one interface then skip command/step for another interface.

Use below commands to configure IP addresses manually:

```
# sudo ifconfig enp0s3 <WAN-ip-address>/<WAN-mask> up
# sudo ifconfig enp0s8 <LAN-ip-address>/<LAN-mask> up
```

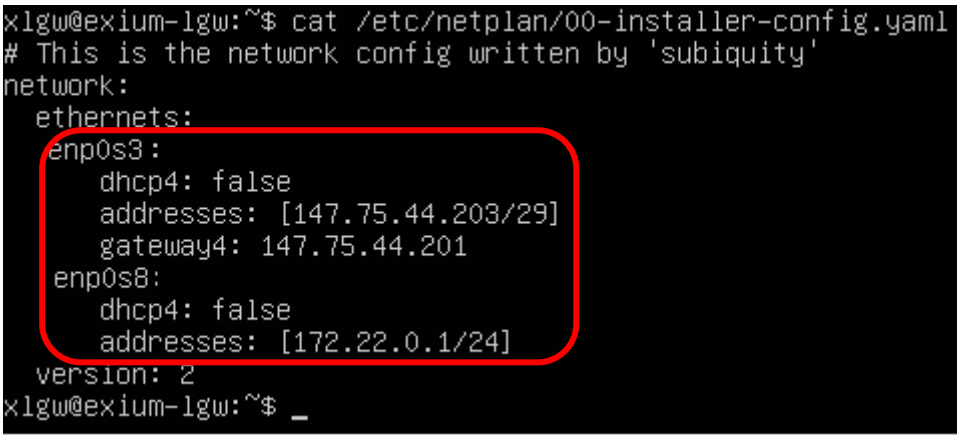


Use "netplan" utility to make IP addresses static on VM.

- Edit existing netplan and include the IP address installed manually.

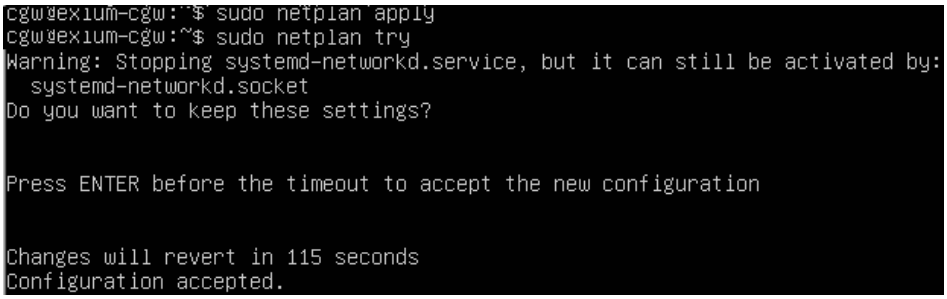
```
# sudo vim /etc/netplan/00-installer-config.yaml
```

- Add interface details:
  - Name of the interface
  - dhcpv4: false
  - addresses: IP address to be installed: Same IP which was configured manually
  - gateway4: Default gateway of the interface



- Apply the configuration:
  ```
  # sudo netplan apply
  ```

- Verify configuration
  ```
  # sudo netplan try
  ```
- Press enter, when the timer starts.
  - Configuration Accepted will be shown in case of successful scenario.



- After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI
  ```
  # sudo /home/cgw/xbootstrap.sh
  ```

- Verify the local time on the VMware machine is correct. If it is not, update the time using Network Time Protocol.

- Verify internet is accessible from CGW VM. If not, update the network settings accordingly.

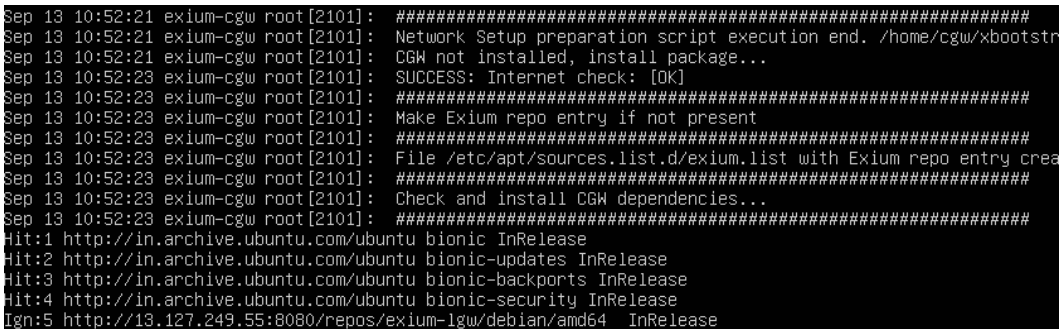
- In case Cyber Gateway (CGW) is configured with 2 separate interfaces (vNICs). One interface for internet access (WAN) and another interface connected on LAN network, then make sure both vNICs are configured with different subnets or associated to different networks.

- In case Cyber Gateway (CGW) is configured with 2 separate interfaces (vNICs), All the machines/devices behind the Cyber Gateway must be configured with Default Gateway i.e. IP address configured on the LAN interface of Cyber Gateway VM. Those machines must be reachable from CGW LAN interface.

3.7.2.5 CGW Software Installation

After IP addresses installation, bootstrap script will check internet connectivity. If internet is not accessible, then script will exit with warning, else it will continue with installation procedure.

Check default routes and verify DNS resolution and internet connection work from CGW VM. Once internet is accessible from CGW VM, run bootstrap script again to complete installation process.



Installation includes, CGW dependent packages installation, tuning parameters setting and latest CGW application software installation.

After successful installation, terminal will show below output:

Navigate to Section 3.11, to setup CGW.

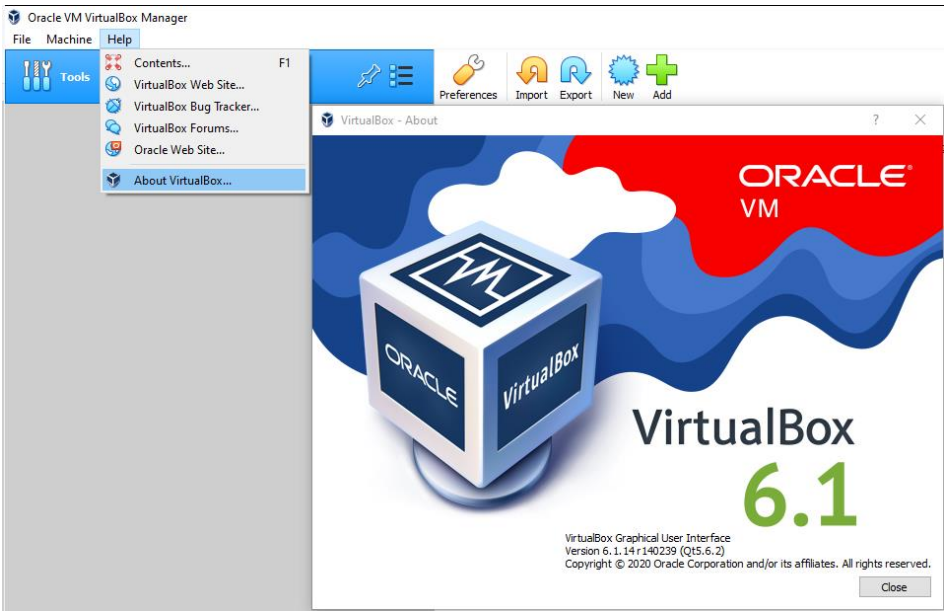
3.7.3 Deploy on Windows laptop running with VirtualBox

3.7.3.1 Pre-requisites

1. Oracle VirtualBox 6.1 (or above) must be pre-installed on user laptop (windows). Install it if already not installed to proceed further.

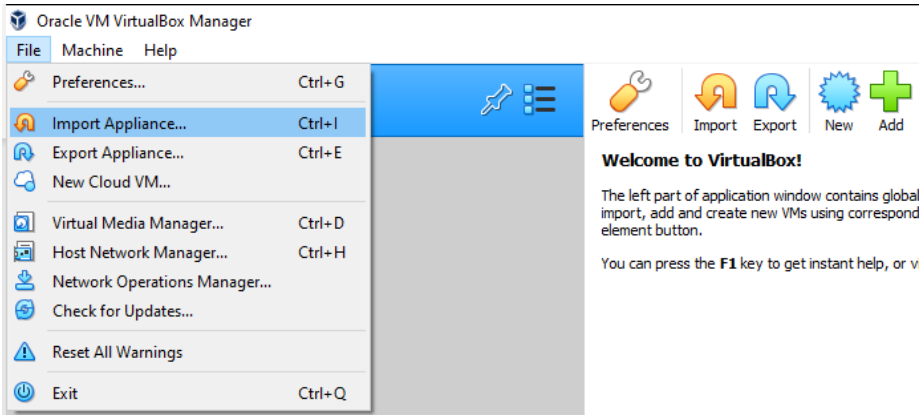
- Open VirtualBox and select “Help” on top menu bar.
- Select “About VirtualBox…” to verify the version installed on the laptop.

2. CGW OVA (cgw-vm.ova) is downloaded and saved on the user laptop.
3. Link to download ova:
   https://clientreleases.s3.us-west-1.amazonaws.com/cgw/cgw-vm.ova

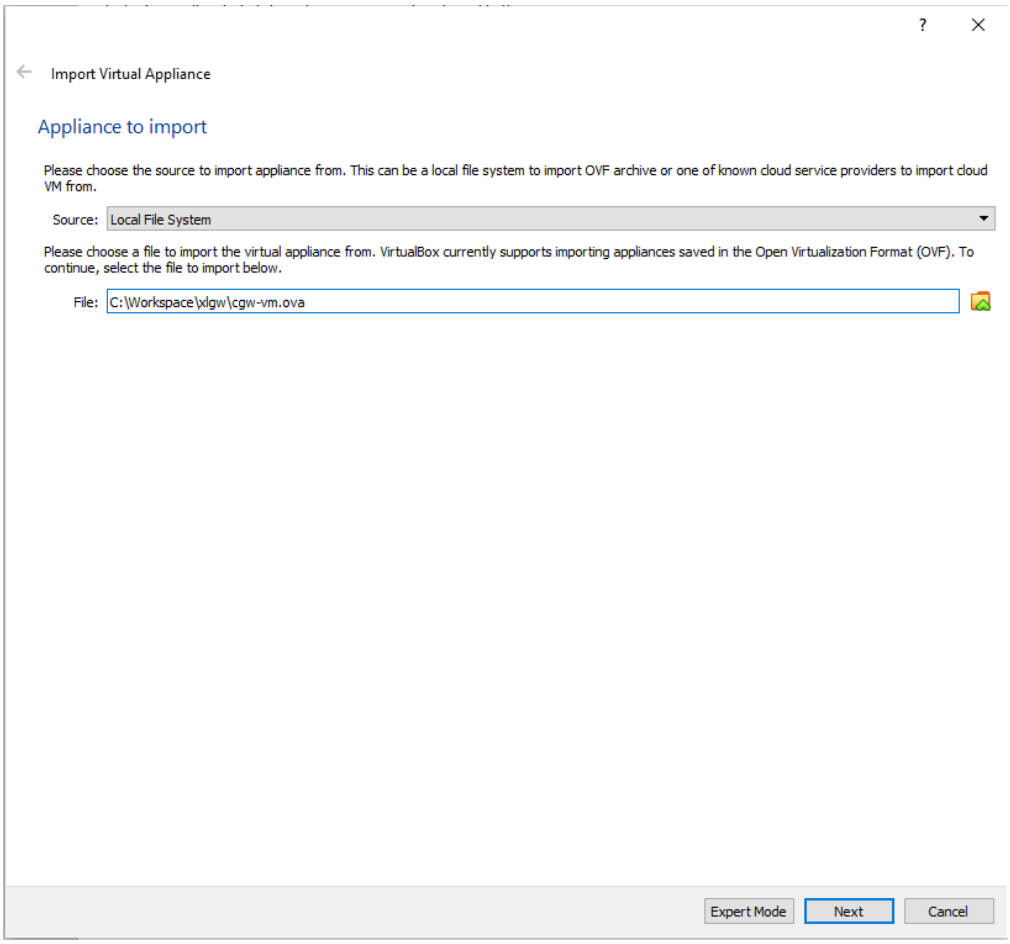


3.7.3.2 Steps to deploy

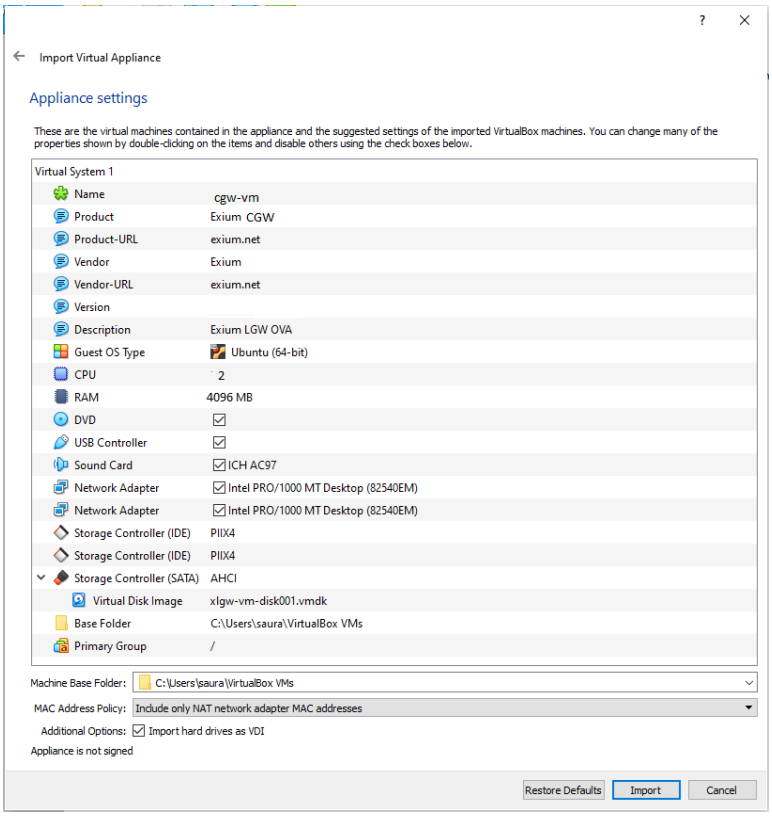
1. Import CGW virtual appliance
   a. On VirtualBox home screen, select “File” option from top menu bar
   b. Select “Import Appliance…”



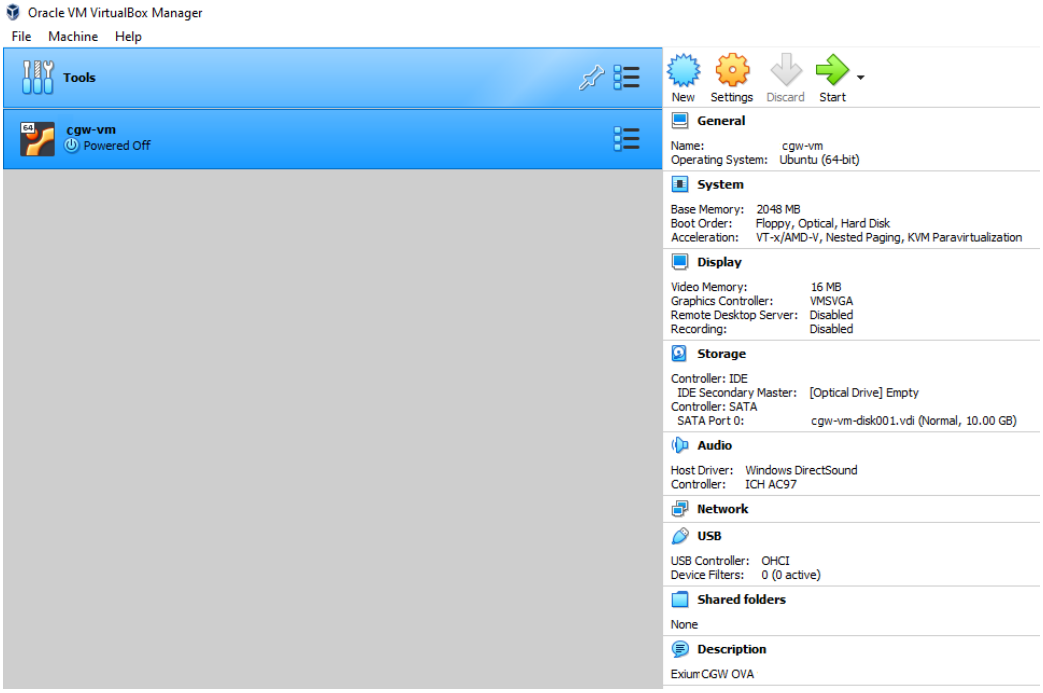
2. On new window, select the path where the cgw-vm.ova is saved on local user laptop.
   Click on “Next”.



3. New window will show all the default parameters set with cgw-vm.ova. User can modify default “CPU” and “RAM” on the same window. Those can be selected and modified according to user’s requirement.
   By default, 1 CPU and 2GB RAM is configured. Click on “Import”.



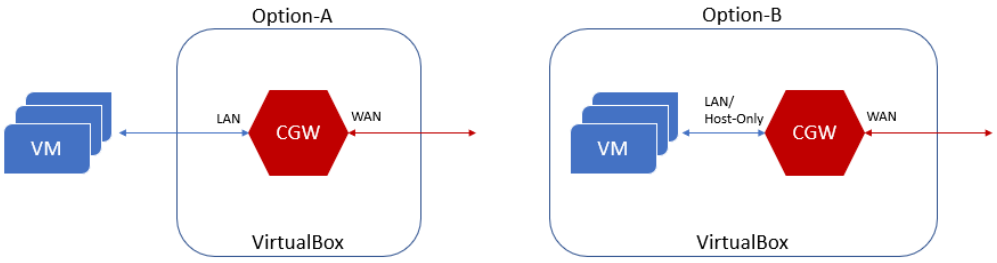
4. Once the disk is created, “cgw-vm” can be seen on left panel.



3.7.3.3 Networking Setup

Minimum two interfaces would be required on “cgw-vm”.

a. WAN interface (Bridged Network) for internet access
b. LAN interface for CGW connection to VMs/networks behind CGW



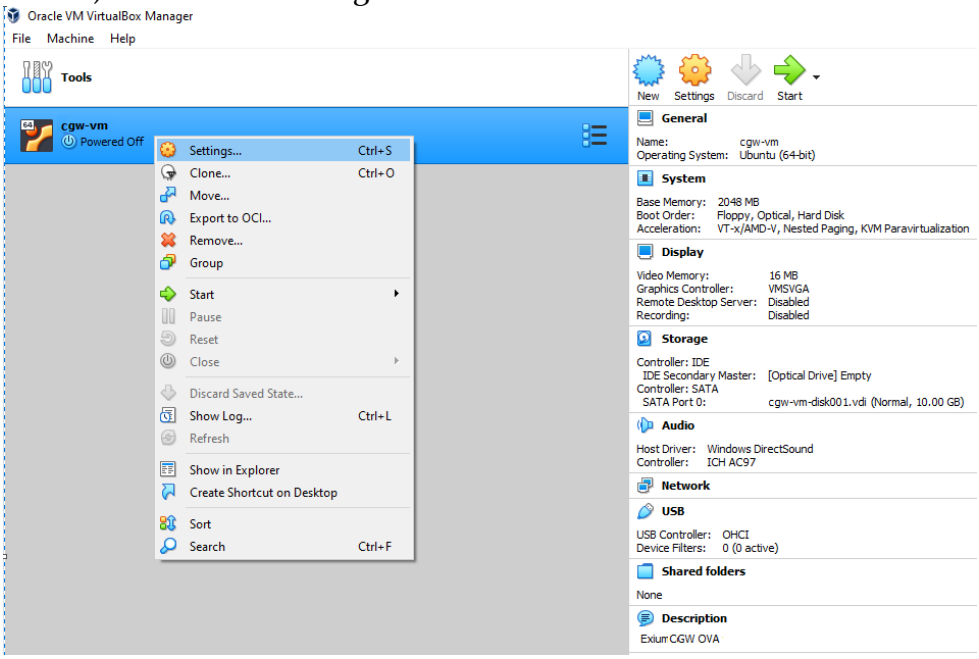
There are two options, user can setup the CGW on local laptop.

a. Option-A: Laptop hosts CGW on VirtualBox, VMs or network behind CGW are hosted outside user's laptop.
b. Option-B: Laptop is hosting CGW and other VMs/networks (which user wants to access via CGW)

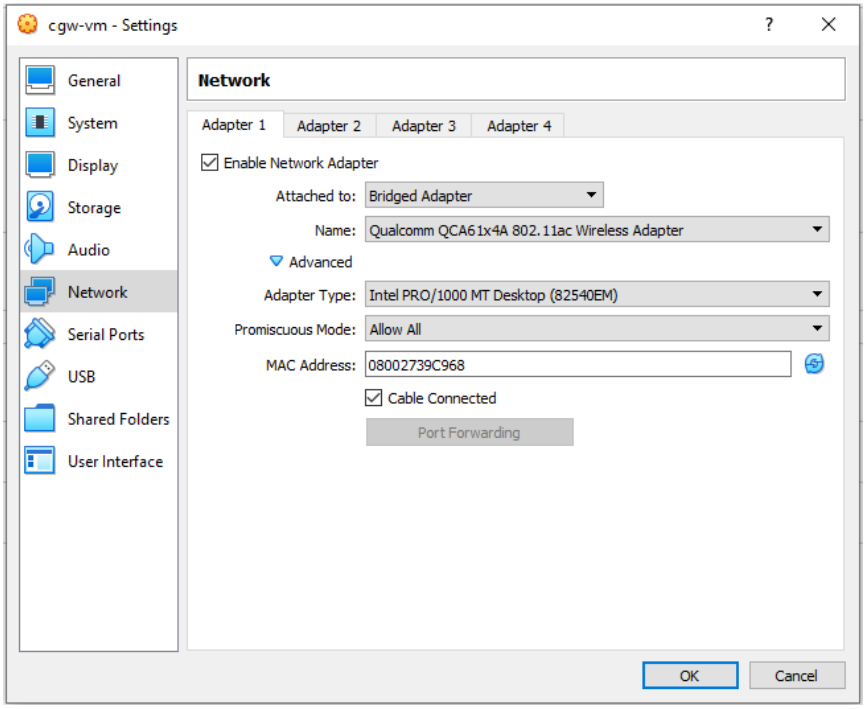
Approach mentioned in option A would require additional networking setup where user must connect another laptop/machine with ethernet cable or wifi hotspot. User will need to configure network adapter for LAN accordingly.

Refer below steps to configure network interfaces for option B approach:

1. Right click on the VM name (visible on left panel of VirtualBox home screen) and select "Settings…"



2. On settings window, select "Network" which will show Adapters (1 to 4)

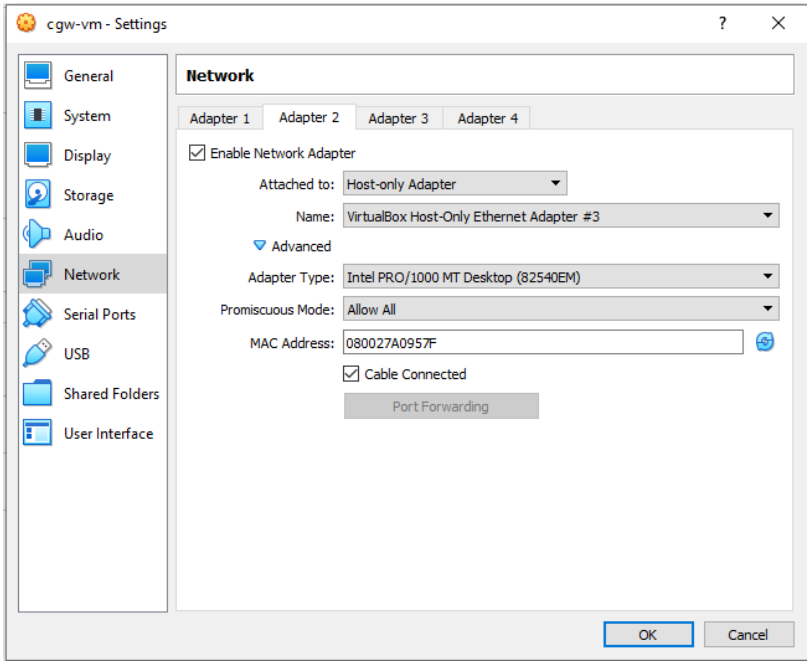


WAN Interface: Adapter 1

a. Select “Enable Network Adapter”, if it is not enabled already
b. Select “Bridged Adapter” from drop down list in “Attached to” setting
c. Name will show Wireless Adapter on laptop selected by default
d. Open up “Advanced” setting and select “Allow All” from drop down list in “Promiscuous Mode” setting
e. Click “OK” to save configuration.

Note: If CGW is planned to have single interface for WAN and LAN connectivity then skip below steps to add new Adapter.

3. On network setting window, select “Adapter 2”:
   Skip this step if CGW uses single interface for WAN and LAN connectivity.



LAN Interface: Adapter 2

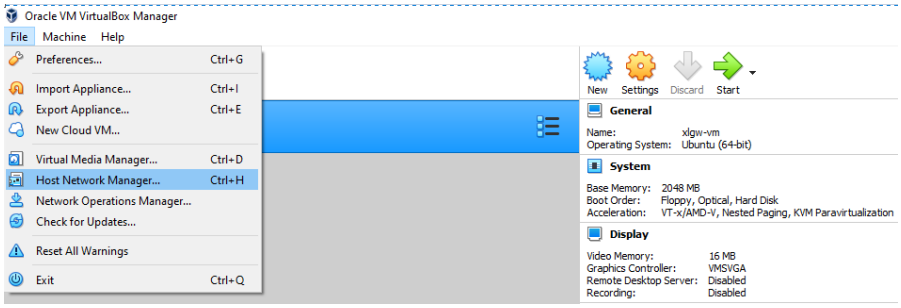
a. Select “Enable Network Adapter”, if it is not enabled already
b. Select “Host-only Adapter” from drop down list in “Attached to” setting
c. Name will show VirtualBox Host-Only Ethernet Adapter
d. Open up “Advanced” setting and select “Allow All” from drop down list in “Promiscuous Mode” setting
e. Click “OK” to save configuration.

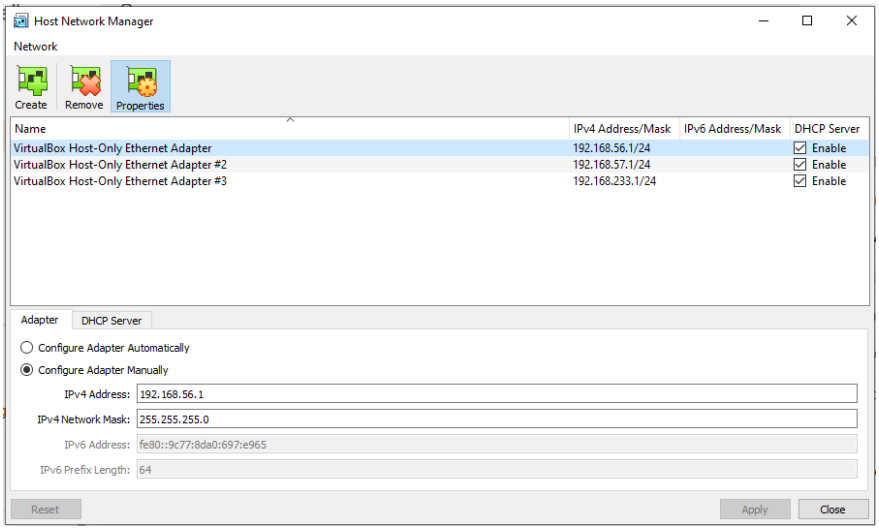
Follow below steps to find configuration of VirtualBox Host-Only Ethernet Adapter:

a. On VirtualBox home screen, select “File” option from top menu bar
b. Select “Host Network Manager…” from list, a new window will open and show available virtual network adapters.

Note: User must use “Bridged Adapter” settings in case physical machine is connected on LAN interface.

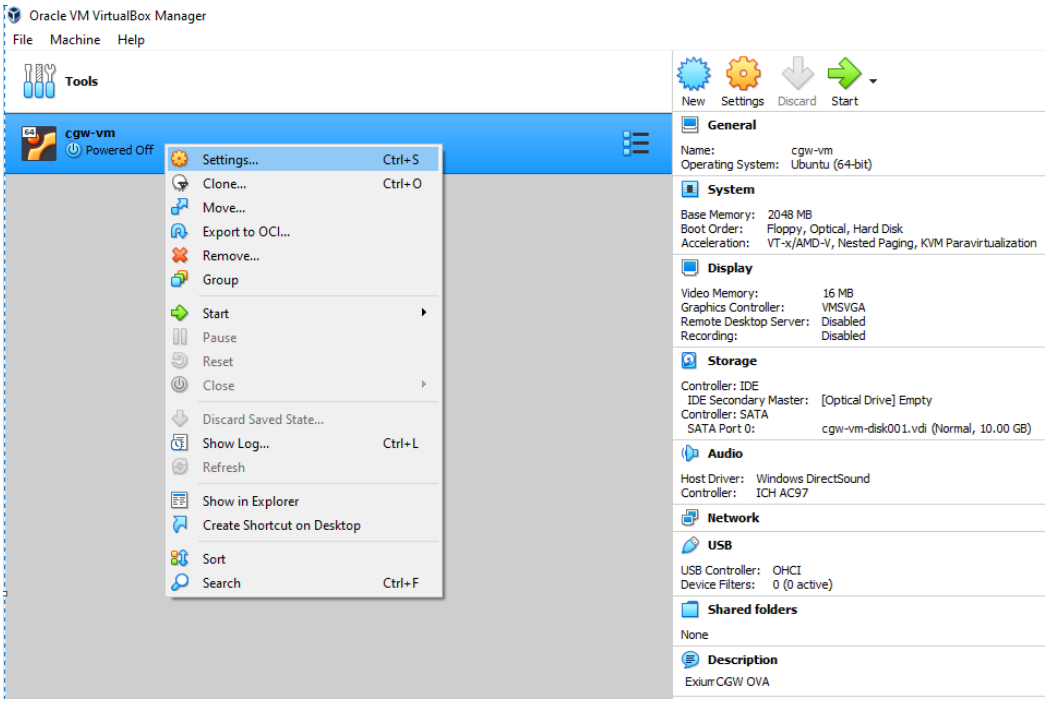
- vNIC inside VM must be configured with an IP address manually
- Physical machine connected via Lan must configure Above IP as default GW to access the internet and other services





3.7.3.4 Start Virtual Machine

Right click on the VM name (visible on left panel of VirtualBox home screen) and select “Start” from list for “Normal Start” of cgw-vm.

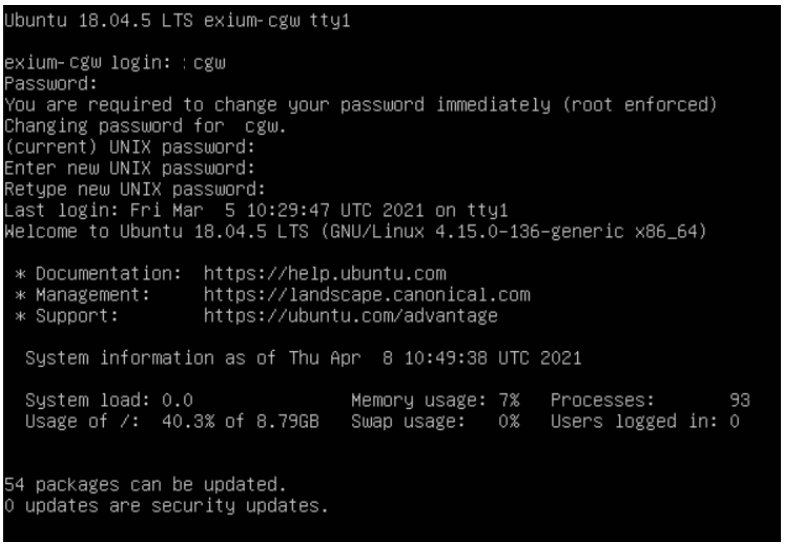


3.7.3.5 Set Password

Set your own password during first login by providing default username mentioned below.

Login: `cgw`
Password: `cgw`

After successful login to CGW VM, switch user account and become "root" user by executing "sudo su" command.



3.7.3.6 Install IP addresses on vNICs

After setting the password on the VM terminal, it will again ask to provide password to run the bootstrap script which takes care of IP address allocation using DHCP.

IP address allocation can be handled with below approaches:

- If interfaces on the VM are connected to DHCP enabled network, then IP will be allocated by DHCP server (see below “Bootstrap Script”)
- In case of multiple interfaces, if one of the interfaces on the VM is connected to DHCP enabled network, then one interface will get IP from DHCP server, and another must be configured manually (see below “Manual IP Configuration”)
- If interfaces on the VM do not have DHCP enabled network, then user must configure IP addresses manually (see below “Manual IP Configuration”)

Bootstrap Script

- Script will verify minimum networking requirements and accordingly provide instructions on terminal:
  - Script will pull interface names and request DHCP allocation
    - Configured retries for each interface – 3
    - Configured timeout for each DHCP request – 30 seconds
  - **Case-1: No interface present on CGW VM**
    - If minimum one interface is not available, then execution will end with warning

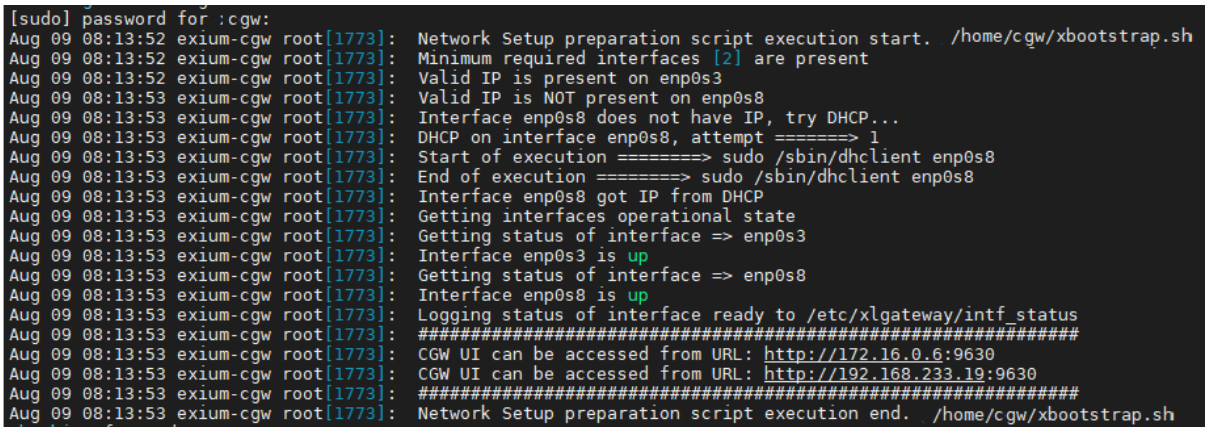
```
[sudo] password for cgw:
Aug 09 07:50:09 exium-cgw root[2405]:  Network Setup preparation script execution start. /home/cgw/xbootstrap.sh
Aug 09 07:50:09 exium-cgw root[2405]:  WARNING: Minimum 1 interface required to bring up CGW."
Aug 09 07:50:09 exium-cgw root[2405]:  WARNING: Found no interface. Please add required interface and run the script manually"
Aug 09 07:50:09 exium-cgw root[2405]:  WARNING: Network setup did not complete. Interfaces did not get IP allocated from DHCP."
Aug 09 07:50:09 exium-cgw root[2405]:  sudo /home/cgw/xbootstrap.sh
Aug 09 07:50:09 exium-cgw root[2405]:
Aug 09 07:50:09 exium-cgw root[2405]:  ################################################################################
Aug 09 07:50:09 exium-cgw root[2405]:  Follow below steps to configure IPs manually on interfaces
Aug 09 07:50:09 exium-cgw root[2405]:
Aug 09 07:50:09 exium-cgw root[2405]:  1) Open user manual 'Exium CGW OVA - User Manual.pdf'
Aug 09 07:50:09 exium-cgw root[2405]:  1.a) If you do not have it, download it from below link:
Aug 09 07:50:09 exium-cgw root[2405]:  https://exiumclientreleases.s3.us-west-1.amazonaws.com/xlgw/Exium+CGW+OVA+-+User+Manual.pdf
Aug 09 07:50:09 exium-cgw root[2405]:  2) Refer section 3.6.1.4 'Install IP addresses on vNICs'
Aug 09 07:50:09 exium-cgw root[2405]:  2.a) It will provide commands to configure IP address on interfaces
Aug 09 07:50:09 exium-cgw root[2405]:  2.b) It also includes steps to make IPs persistent
Aug 09 07:50:09 exium-cgw root[2405]:  3) For any queries, contact Exium support at: support@exium.net
Aug 09 07:50:09 exium-cgw root[2405]:  ################################################################################
Checking for Updates--> Done
 cgw@exium-cgw:~$
```

- **Case-2: DHCP on one interface only**
  - In case two interfaces are available and one of the interfaces gets IP from DHCP, but second interface does not:
    - Execution will end with warning

```
[sudo] password for cgw:
Aug 09 08:07:55 exium-cgw root[2920]:  Network Setup preparation script execution start. /home/cgw/xbootstrap.sh
Aug 09 08:07:55 exium-cgw root[2920]:  Minimum required interfaces [2] are present
Aug 09 08:07:55 exium-cgw root[2920]:  Valid IP is present on enp0s3
Aug 09 08:07:55 exium-cgw root[2920]:  Valid IP is NOT present on enp0s8
Aug 09 08:07:55 exium-cgw root[2920]:  Interface enp0s8 does not have IP, try DHCP...
Aug 09 08:07:55 exium-cgw root[2920]:  DHCP on interface enp0s8, attempt =======> 1
Aug 09 08:07:55 exium-cgw root[2920]:  Start of execution ========> sudo /sbin/dhclient enp0s8
Aug 09 08:08:06 exium-cgw root[2920]:  End of execution ========> sudo /sbin/dhclient enp0s8
Aug 09 08:08:08 exium-cgw root[2920]:  DHCP on interface enp0s8, attempt =======> 2
Aug 09 08:08:08 exium-cgw root[2920]:  Start of execution ========> sudo /sbin/dhclient enp0s8
Aug 09 08:08:20 exium-cgw root[2920]:  End of execution ========> sudo /sbin/dhclient enp0s8
Aug 09 08:08:22 exium-cgw root[2920]:  DHCP on interface enp0s8, attempt =======> 3
Aug 09 08:08:22 exium-cgw root[2920]:  Start of execution ========> sudo /sbin/dhclient enp0s8
Aug 09 08:08:33 exium-cgw root[2920]:  End of execution ========> sudo /sbin/dhclient enp0s8
Aug 09 08:08:35 exium-cgw root[2920]:  IP allocation using DHCP on interface enp0s8 failed.
Aug 09 08:08:35 exium-cgw root[2920]:  Getting interfaces operational state
Aug 09 08:08:35 exium-cgw root[2920]:  Getting status of interface => enp0s3
Aug 09 08:08:35 exium-cgw root[2920]:  Interface enp0s3 is up
Aug 09 08:08:35 exium-cgw root[2920]:  Getting status of interface => enp0s8
Aug 09 08:08:35 exium-cgw root[2920]:  Interface enp0s8 is up
Aug 09 08:08:35 exium-cgw root[2920]:  Logging status of interface notready to /etc/xlgateway/intf_status
Aug 09 08:08:35 exium-cgw root[2920]:  WARNING: Network setup did not complete. Interfaces did not get IP allocated from DHCP.
Aug 09 08:08:35 exium-cgw root[2920]:  NOTICE: Please configure the interfaces manually, and run the script again.
Aug 09 08:08:35 exium-cgw root[2920]:  sudo  /home/cgw/xbootstrap.sh
Aug 09 08:08:35 exium-cgw root[2920]:  ################################################################################
Aug 09 08:08:35 exium-cgw root[2920]:  Follow below steps to configure IPs manually on interfaces
Aug 09 08:08:35 exium-cgw root[2920]:
Aug 09 08:08:35 exium-cgw root[2920]:  1) Open user manual 'Exium CGW OVA - User Manual.pdf'
Aug 09 08:08:35 exium-cgw root[2920]:  1.a) If you do not have it, download it from below link:
Aug 09 08:08:35 exium-cgw root[2920]:  https://exiumclientreleases.s3.us-west-1.amazonaws.com/xlgw/Exium+CGW+OVA+-+User+Manual.pdf
Aug 09 08:08:35 exium-cgw root[2920]:  2) Refer section 3.6.1.4 'Install IP addresses on vNICs'
Aug 09 08:08:35 exium-cgw root[2920]:  2.a) It will provide commands to configure IP address on interfaces
Aug 09 08:08:35 exium-cgw root[2920]:  2.b) It also includes steps to make IPs persistent
Aug 09 08:08:35 exium-cgw root[2920]:  3) For any queries, contact Exium support at: support@exium.net
Aug 09 08:08:35 exium-cgw root[2920]:  ################################################################################
Aug 09 08:08:35 exium-cgw root[2920]:  Network Setup preparation script execution end. /home/cgw/xbootstrap.sh
Checking for Updates--> Done
 cgw@exium-cgw:~$
```

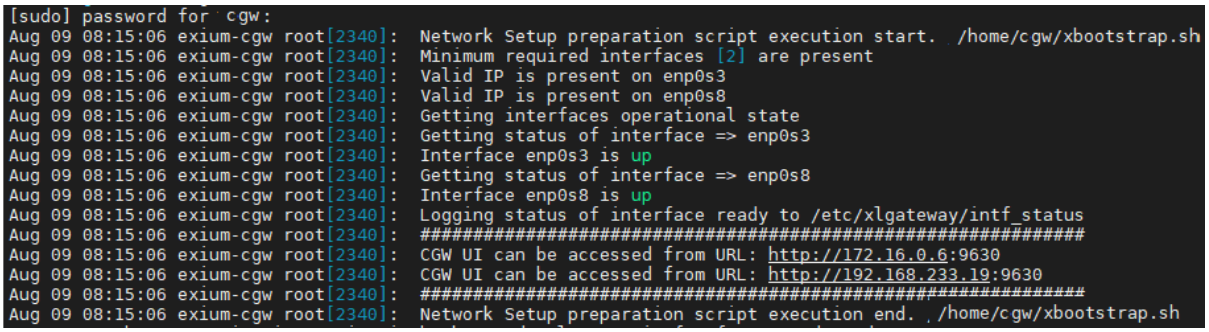
    - Refer “Manual IP Configuration” section included below
    - After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI
      `# sudo /home/cgw/xbootstrap.sh`

- **Case-3: DHCP on both interfaces**
  - If interfaces get IP addresses from DHCP and states are up:
    - Execution will end and it will show the URLs which can be used to access CGW UI



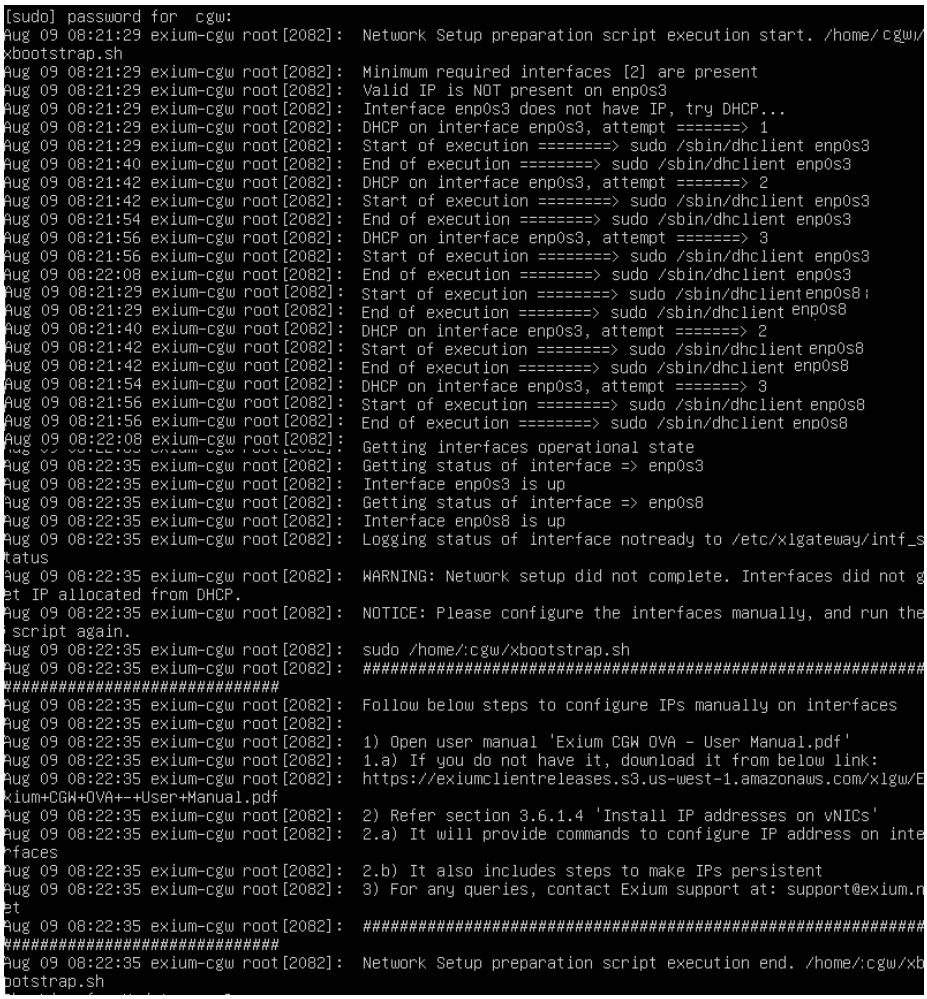
- **Case-4: IP addresses are already assigned on both interfaces**
  - If valid IP present on interface:
    - Execution will end with validations on both interface
    - Instructions will show URLs which can be used to access CGW UI
    - For eg: CGW UI access URL format would be **http://<CGW-IP>:9630**

- Each time user logs into CGW VM using "cgw" user credentials, bootstrap script will run and validate the interface IPs and states.



Manual IP configuration

- **No DHCP on interface**
  - If associated/attached network does not allocate IP address using DHCP then execution will end with warning

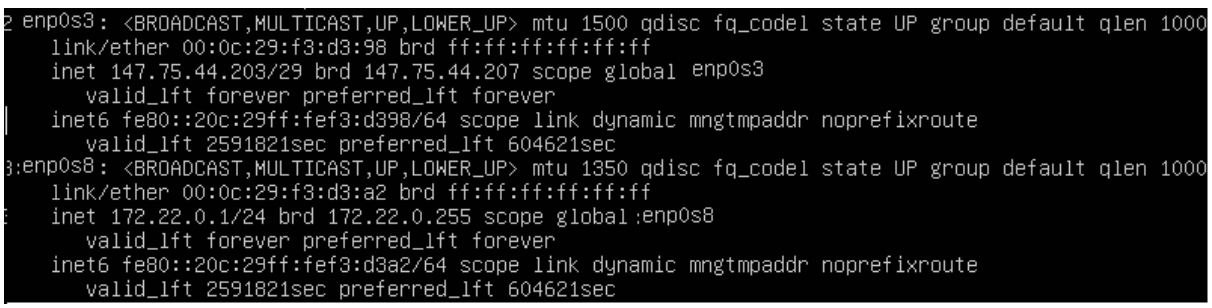


Use Command "`sudo ip addr`" to check interfaces installed:

Note: If there is only one interface then skip command/step for another interface.

Use below commands to configure IP addresses manually:

```
# sudo ifconfig enp0s3 <WAN-ip-address>/<WAN-mask> up
# sudo ifconfig enp0s8 <LAN-ip-address>/<LAN-mask> up
```

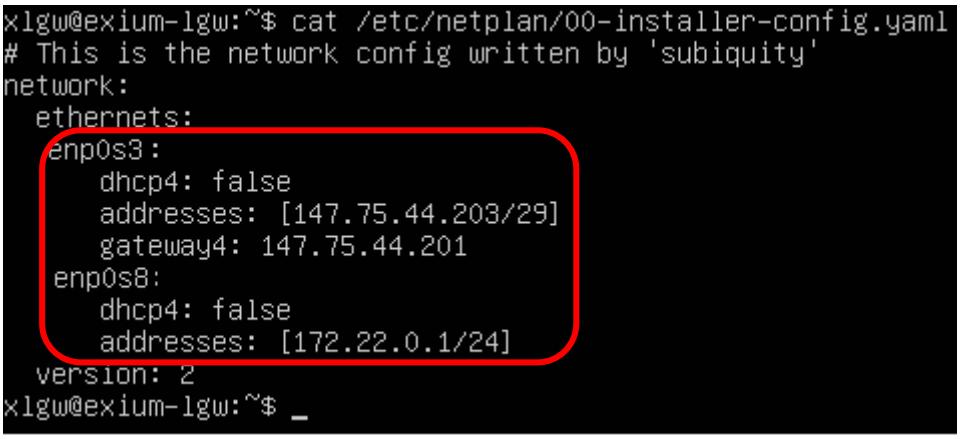


Use "netplan" utility to make IP addresses static on VM.

- Edit existing netplan and include the IP address installed manually.

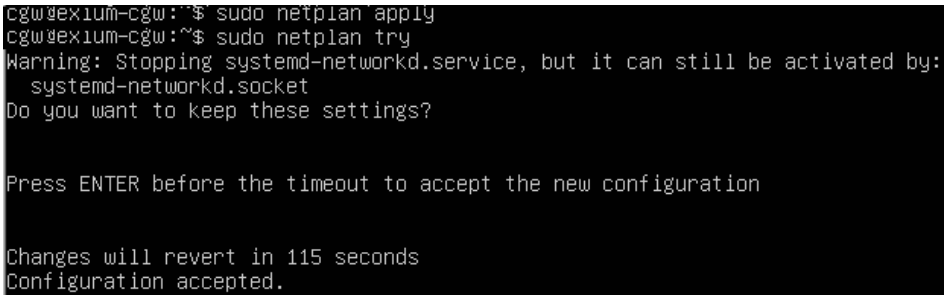
```
# sudo vim /etc/netplan/00-installer-config.yaml
```

- Add interface details:
  - Name of the interface
  - dhcpv4: false
  - addresses: IP address to be installed: Same IP which was configured manually
  - gateway4: Default gateway of the interface



- Apply the configuration:
  `# sudo netplan apply`

- Verify configuration
  `# sudo netplan try`
- Press enter, when the timer starts.
  - Configuration Accepted will be shown in case of successful scenario.

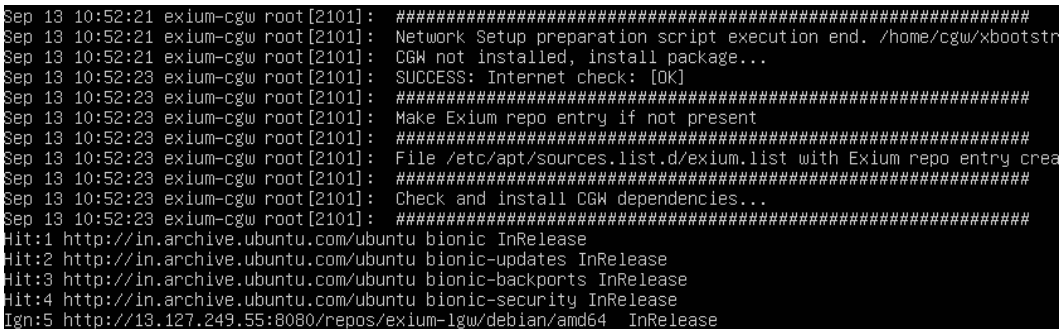


- After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI
  `# sudo /home/cgw/xbootstrap.sh`

3.7.3.7 CGW Software Installation

After IP addresses installation, bootstrap script will check internet connectivity. If internet is not accessible, then script will exit with warning, else it will continue with installation procedure.

Check default routes and verify DNS resolution and internet connection work from CGW VM. Once internet is accessible from CGW VM, run bootstrap script again to complete installation process.



Installation includes, CGW dependent packages installation, tuning parameters setting and latest CGW application software installation.

After successful installation, terminal will show below output:

Navigate to Section 3.11, to setup CGW.

3.7.4 Deploy on KVM server using console

3.7.4.1 Pre-requisites

1. QEMU emulator version 1.5.3 or above installed and running in bare metal or customer data center.
2. Admin/root privilege to deploy VMs and edit network settings
3. Link to download Exium CGW QCOW2 image
4. Virt-manager installed on KVM server to check VM health status and for management

3.7.4.2 Steps to deploy

1. Login to KVM server with root or sudo user credentials
2. Navigate to directory, where you want to store the qcow2 image, for eg:
   `# cd /var/lib/libvirt/boot/`
3. Download QCOW2 image from Exium portal using below command:
   `# wget https://clientreleases.s3.us-west-1.amazonaws.com/cgw/cgw-vm-kvm.qcow2`
4. Use below command to create CGW VM:
   `# virt-install --name CGW --ram=4096 --vcpus=2 --network=bridge=virbr1,model=virtio --`

```
network=bridge=virbr1,model=virtio --disk
/var/lib/libvirt/boot/cgw-vm-kvm.qcow2,bus=virtio --virt-
type=kvm --os-variant=ubuntu18.04 --os-type linux --graphics
vnc --noautoconsole --import --arch=x86_64 --debug --wait 1
```

Note:

- Make sure you select correct networks while creating interfaces on CGW VM. In above command sample configuration was used. (`network=bridge=virbr1,model=virtio`). Provide WAN network in first input and LAN network in second input
- If CGW is planned to have single interface for WAN and LAN connectivity, then use "`network=`" only once

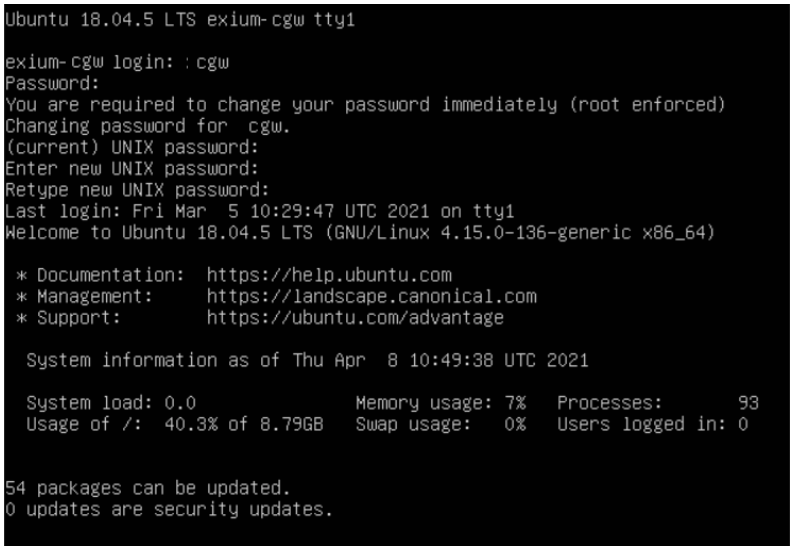
5. Open another KVM server console, and run command-virt-manager to access GUI:
   `# virt-manager`
6. Select VM on virt-manager GUI and click on "Open" to access VM console.

3.7.4.3 Set VM Password

Set your own password during first login by providing default username mentioned below.

Login: `cgw`
Password: `cgw`

After successful login to CGW VM, switch user account and become "root" user by executing "sudo su" command.



3.7.4.4 Install IP addresses on vNICs

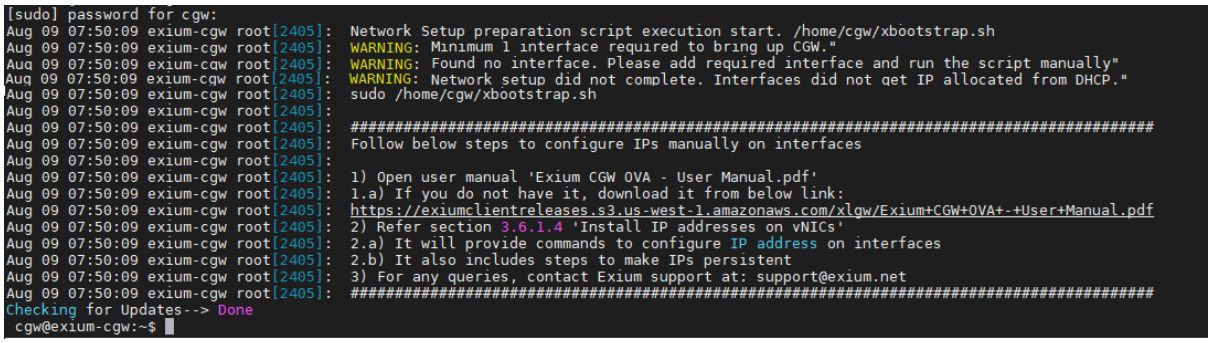
After setting the password on the VM terminal, it will again ask to provide password to run the bootstrap script which takes care of IP address allocation using DHCP.

IP address allocation can be handled with below approaches:

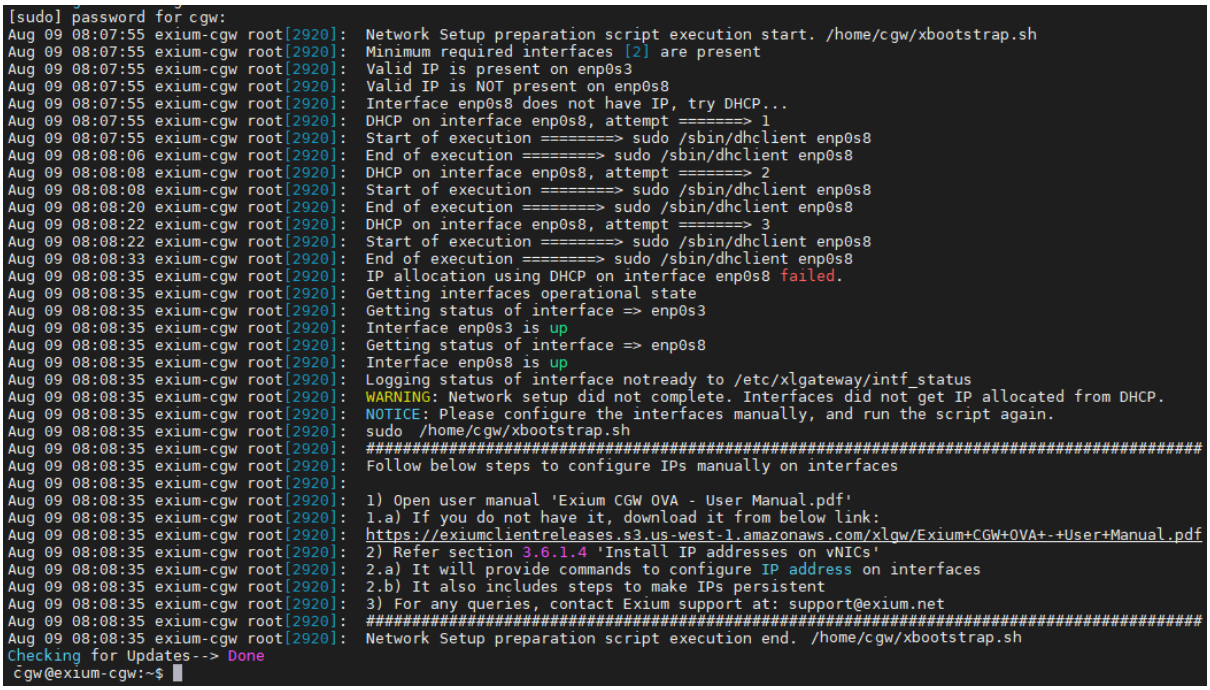
- If interfaces on the VM are connected to DHCP enabled network, then IP will be allocated by DHCP server (see below "Bootstrap Script")
- In case of multiple interfaces, if one of the interfaces on the VM is connected to DHCP enabled network, then one interface will get IP from DHCP server, and another must be configured manually (see below "Manual IP Configuration")
- If interfaces on the VM do not have DHCP enabled network, then user must configure IP addresses manually (see below "Manual IP Configuration")

Bootstrap Script

- Script will verify minimum networking requirements and accordingly provide instructions on terminal:
  - Script will pull interface names and request DHCP allocation
    - Configured retries for each interface – 3
    - Configured timeout for each DHCP request – 30 seconds
  - **Case-1: No interface present on CGW VM**
    - If minimum one interface is not available, then execution will end with warning



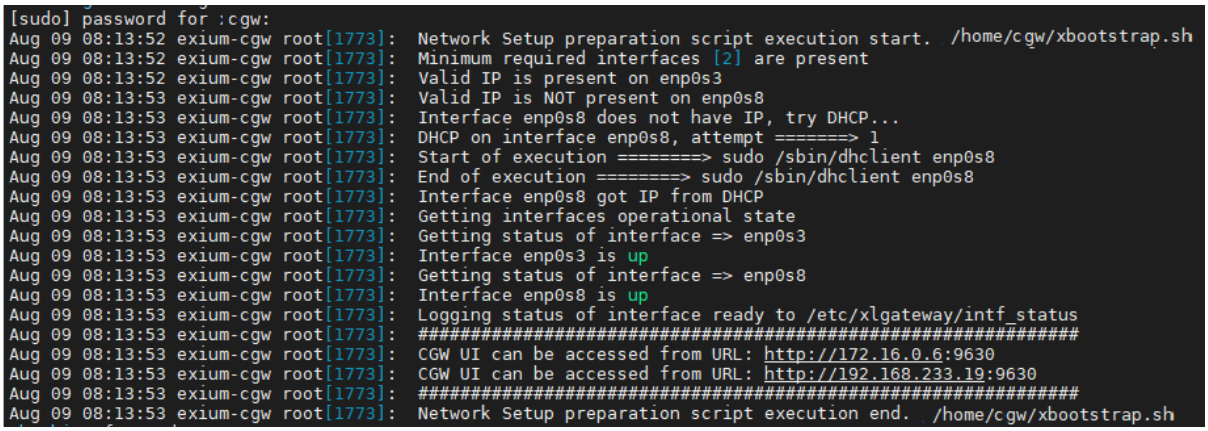
  - **Case-2: DHCP on one interface only**
    - In case two interfaces are available and one of the interfaces gets IP from DHCP, but second interface does not:
      - Execution will end with warning



- Refer “Manual IP Configuration” section included below
- After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI

```
# sudo /home/cgw/xbootstrap.sh
```

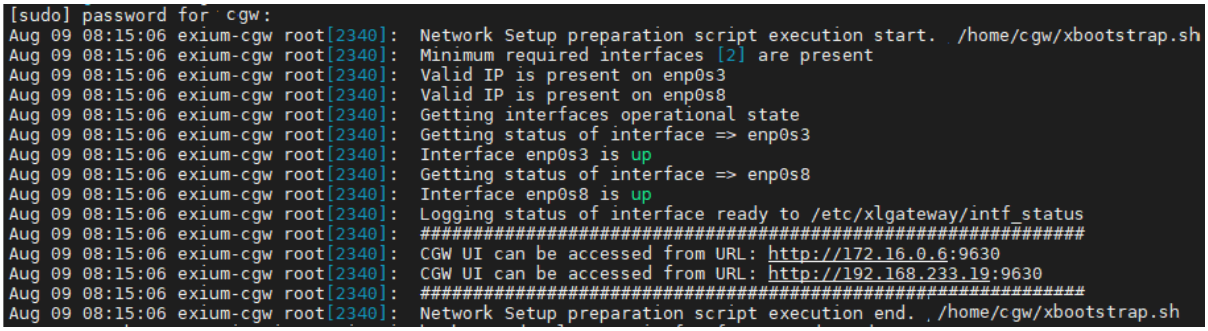
- **Case-3: DHCP on both interfaces**
  - If interfaces get IP addresses from DHCP and states are up:
    - Execution will end and it will show the URLs which can be used to access CGW UI



- **Case-4: IP addresses are already assigned on both interfaces**
  - If valid IP present on interface:
    - Execution will end with validations on both interface
    - Instructions will show URLs which can be used to access CGW UI

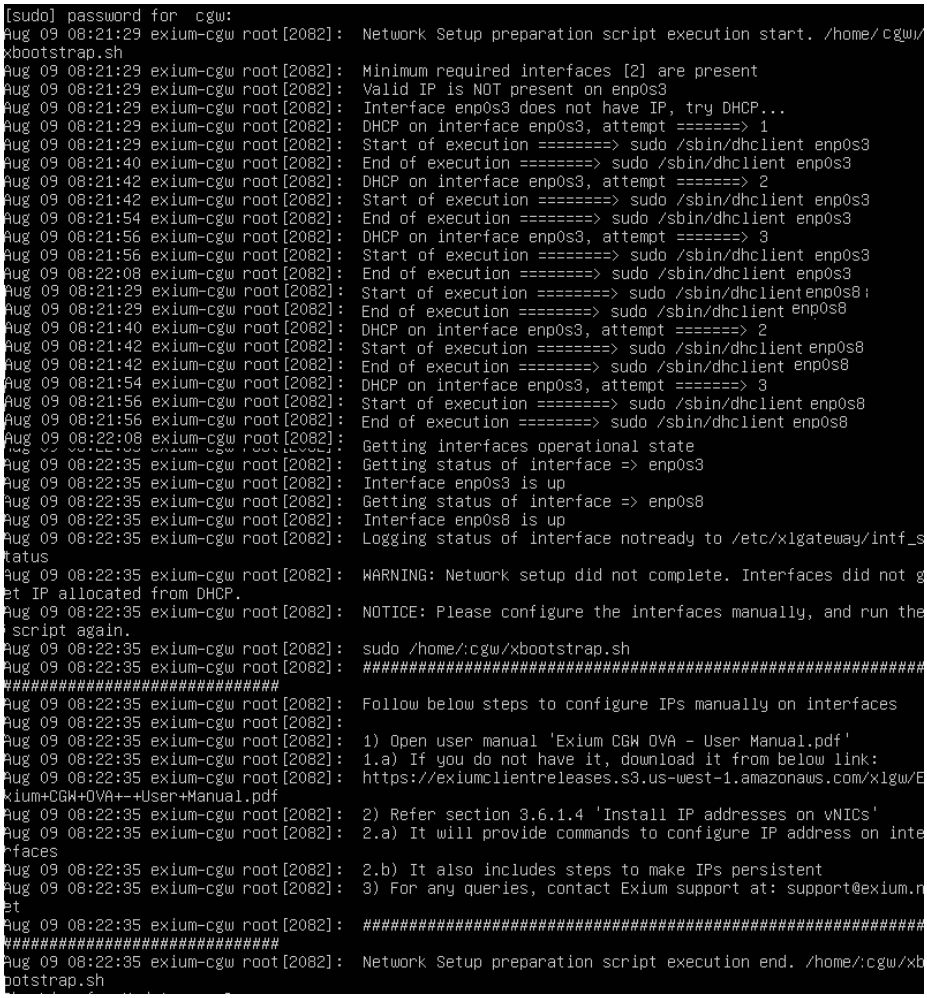
- For eg: CGW UI access URL format would be http://<CGW-IP>:9630

- Each time user logs into CGW VM using "cgw" user credentials, bootstrap script will run and validate the interface IPs and states.



Manual IP configuration

- **No DHCP on interface**
  - If associated/attached network does not allocate IP address using DHCP then execution will end with warning



Use Command "`sudo ip addr`" to check interfaces installed:

Note: If there is only one interface then skip command/step for another interface.

Use below commands to configure IP addresses manually:

```
# sudo ifconfig enp0s3 <WAN-ip-address>/<WAN-mask> up
# sudo ifconfig enp0s8 <LAN-ip-address>/<LAN-mask> up
```

```
2 enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:f3:d3:98 brd ff:ff:ff:ff:ff:ff
    inet 147.75.44.203/29 brd 147.75.44.207 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef3:d398/64 scope link dynamic mngtmpaddr noprefixroute
       valid_lft 2591821sec preferred_lft 604621sec
3:enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1350 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:f3:d3:a2 brd ff:ff:ff:ff:ff:ff
    inet 172.22.0.1/24 brd 172.22.0.255 scope global :enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef3:d3a2/64 scope link dynamic mngtmpaddr noprefixroute
       valid_lft 2591821sec preferred_lft 604621sec
```

Use "netplan" utility to make IP addresses static on VM.

- Edit existing netplan and include the IP address installed manually.
  `# sudo vim /etc/netplan/00-installer-config.yaml`

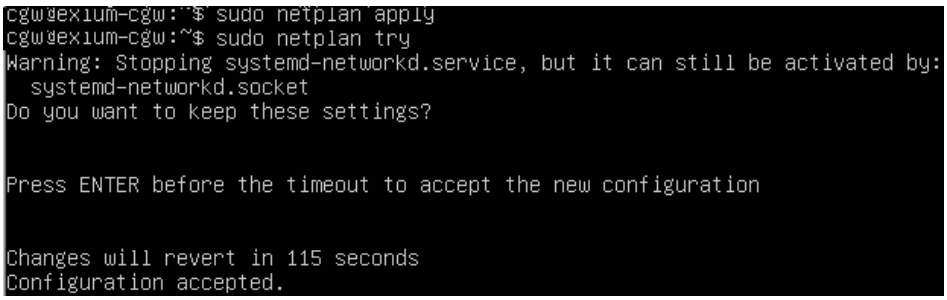
- Add interface details:
  - Name of the interface
  - dhcpv4: false
  - addresses: IP address to be installed: Same IP which was configured manually
  - gateway4: Default gateway of the interface

```
xlgw@exium-lgw:~$ cat /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  ethernets:
    enp0s3:
      dhcp4: false
      addresses: [147.75.44.203/29]
      gateway4: 147.75.44.201
    enp0s8:
      dhcp4: false
      addresses: [172.22.0.1/24]
  version: 2
xlgw@exium-lgw:~$ _
```

- Apply the configuration:
  `# sudo netplan apply`

- Verify configuration
  `# sudo netplan try`

- Press enter, when the timer starts.
    - Configuration Accepted will be shown in case of successful scenario.



- After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI

```
# sudo /home/cgw/xbootstrap.sh
```

- Verify the local time on the VMware machine is correct. If it is not, update the time using Network Time Protocol.

- Verify internet is accessible from CGW VM. If not, update the network settings accordingly.

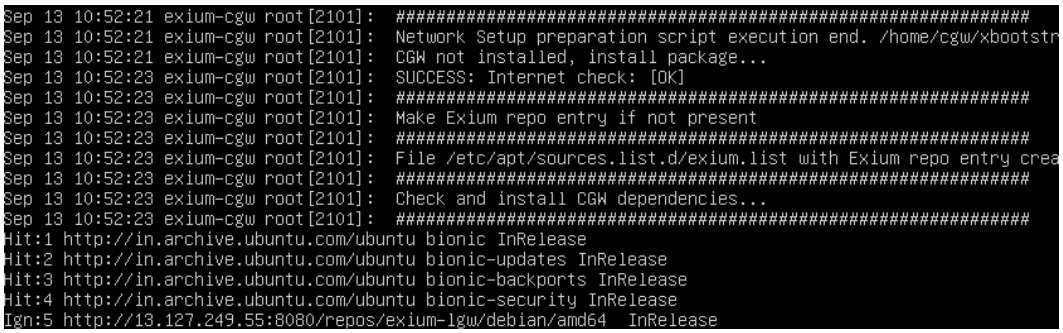
- In case Cyber Gateway (CGW) is configured with 2 separate interfaces (vNICs). One interface for internet access (WAN) and another interface connected on LAN network, then make sure both vNICs are configured with different subnets or associated to different networks.

- In case Cyber Gateway (CGW) is configured with 2 separate interfaces (vNICs), All the machines/devices behind the Cyber Gateway must be configured with Default Gateway i.e. IP address configured on the LAN interface of Cyber Gateway VM. Those machines must be reachable from CGW LAN interface.

3.7.4.5 CGW Software Installation

After IP addresses installation, bootstrap script will check internet connectivity. If internet is not accessible, then script will exit with warning, else it will continue with installation procedure.

Check default routes and verify DNS resolution and internet connection work from CGW VM. Once internet is accessible from CGW VM, run bootstrap script again to complete installation process.



Installation includes, CGW dependent packages installation, tuning parameters setting and latest CGW application software installation.

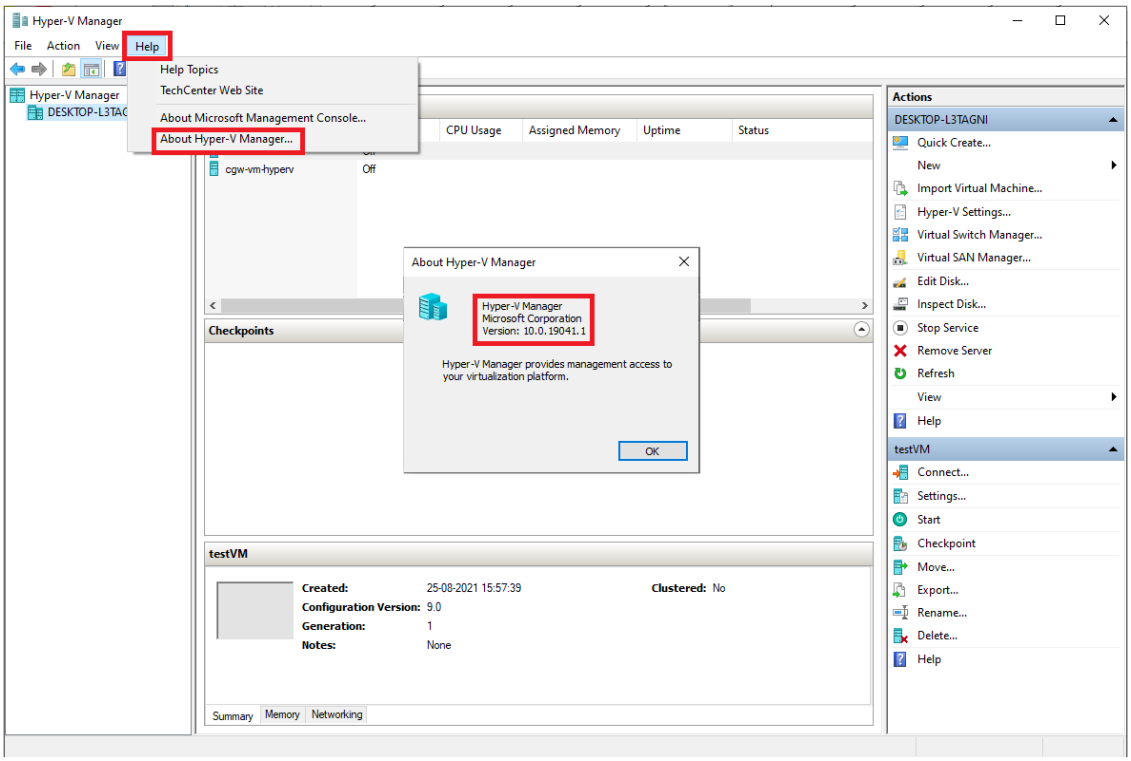
After successful installation, terminal will show below output:

Navigate to Section 3.11, to setup CGW.

3.7.5 Deploy on Hyper-V Environment using Hyper-V Manager

3.7.5.1 Pre-requisites

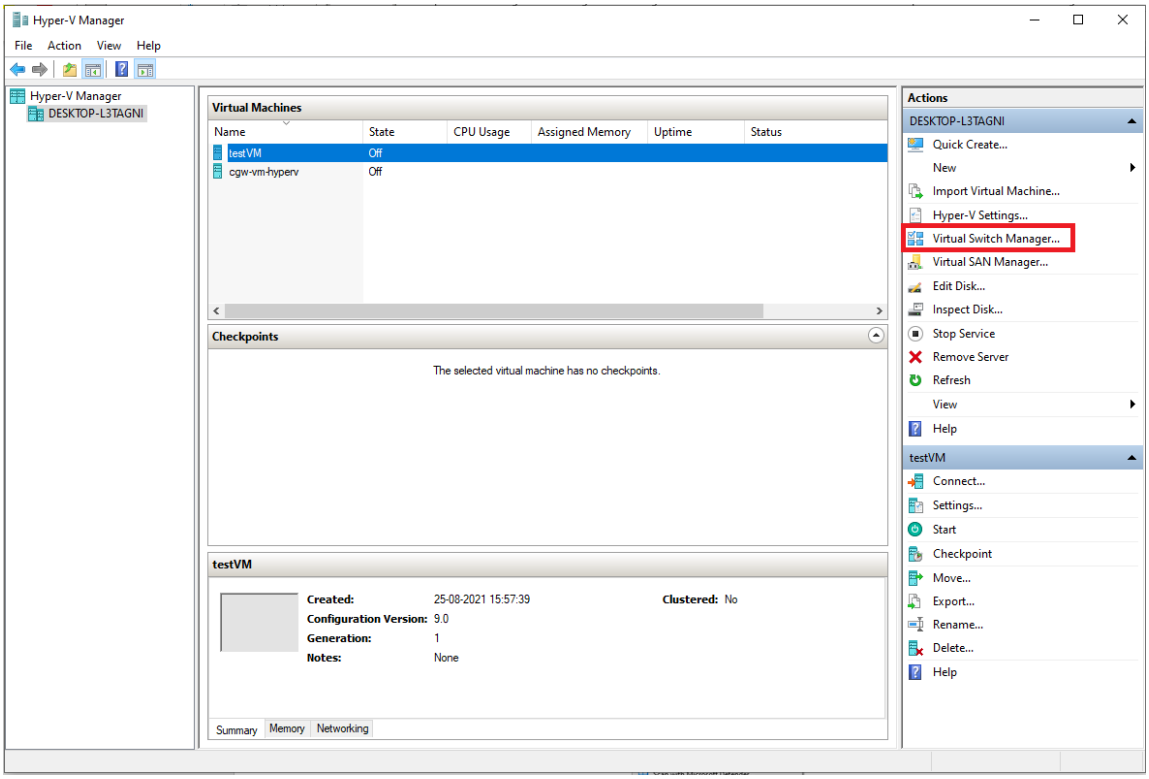
1. Windows 10 Pro or other windows version installed which supports Hyper-V Manager and virtualization.
2. Check Hyper-V version installed on server, it must be 10.0.19041.1 or later Open Hyper-V Manager, click on “Help” and select “About Hyper-V Manager…”



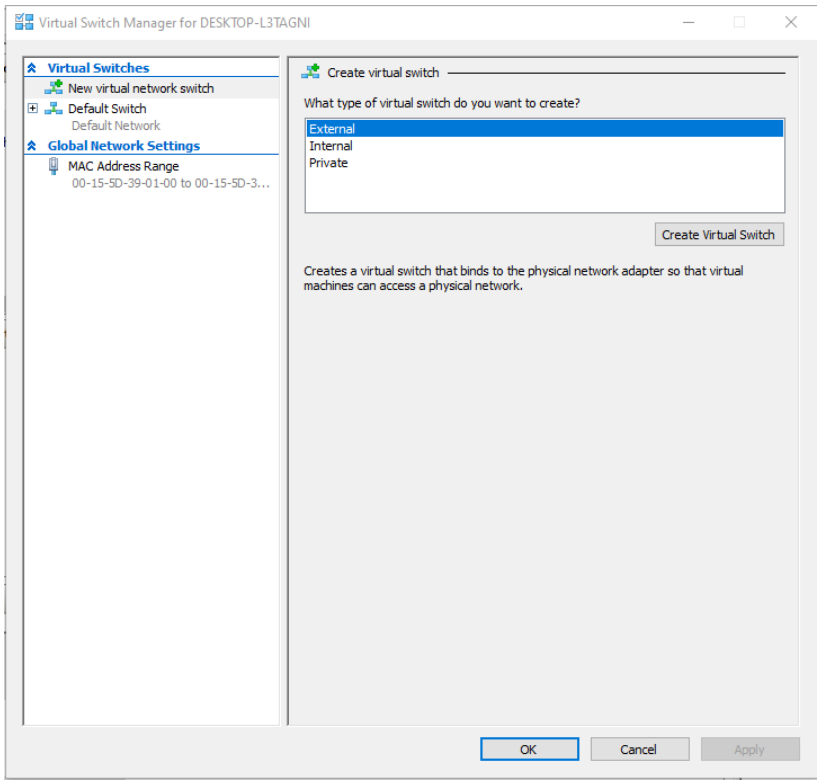
3. Admin/root privilege to deploy VMs and edit network settings
4. Link to download Exium CGW Hyper-V image zip file

3.7.5.2 Network/Virtual Switch Creation

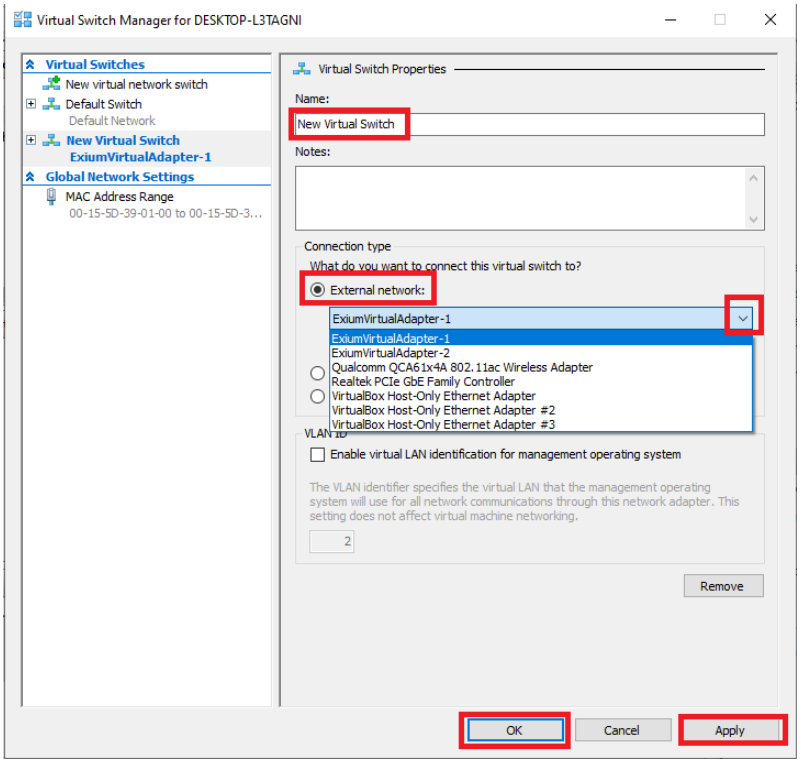
Confirm if networks/virtual switches are already present to provide WAN and LAN connectivity. WAN and LAN connectivity must be on two different virtual switches.
On Hyper-V Manager Window, click on “Virtual Switch Manager…” available on right panel



On new window, check left panel and verify WAN (external) and LAN (internal) virtual switches are already present. Skip below steps to create new virtual switches if they are already present.
On the same window (Virtual Switch Manager), virtual switch types will be displayed.
To create WAN network, click on “External” and “Create Virtual Switch”

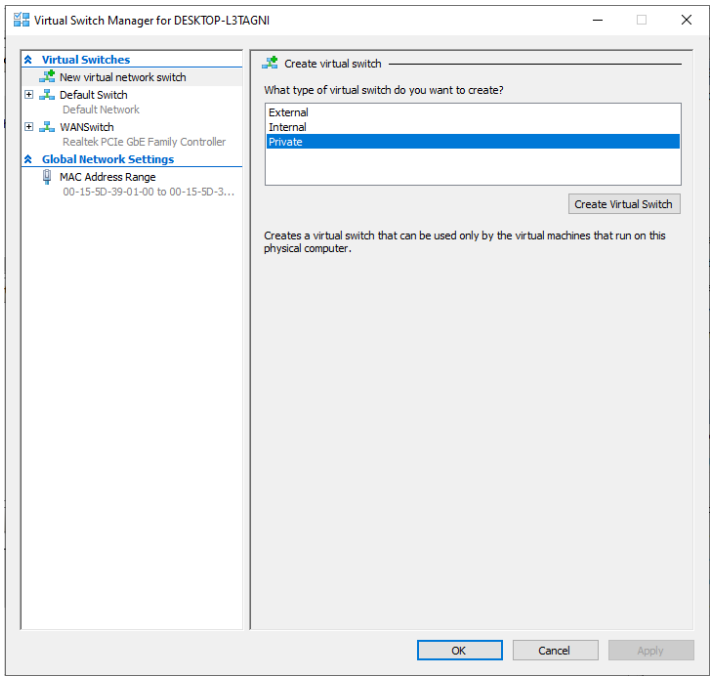


On new window, Change the name, select “External Network” option. From drop down list, select the right network adapter and click on “Apply”. A warning message may appear, click on OK to continue. After system applies changes, click on “OK” to finish.

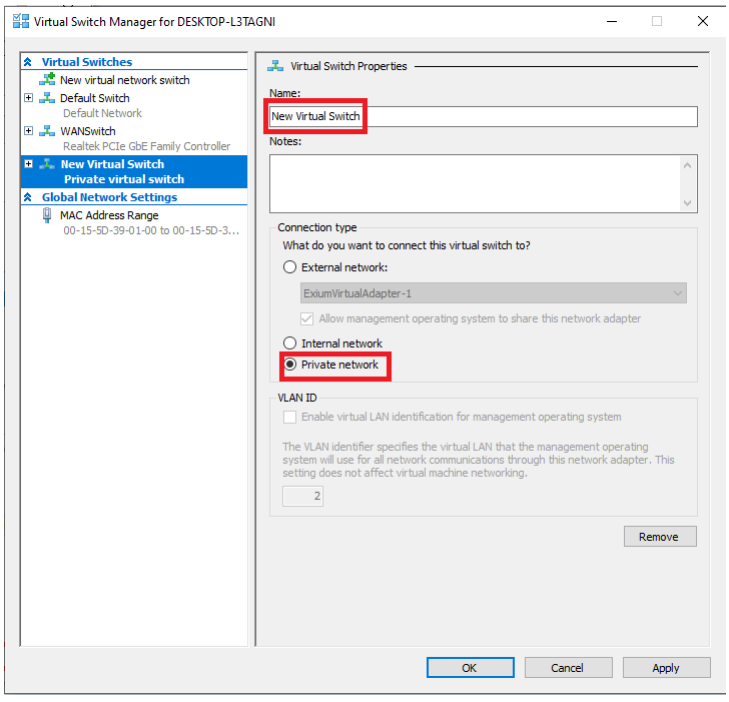


Note: If CGW is planned to have single interface for WAN and LAN connectivity then skip below steps to create LAN network.

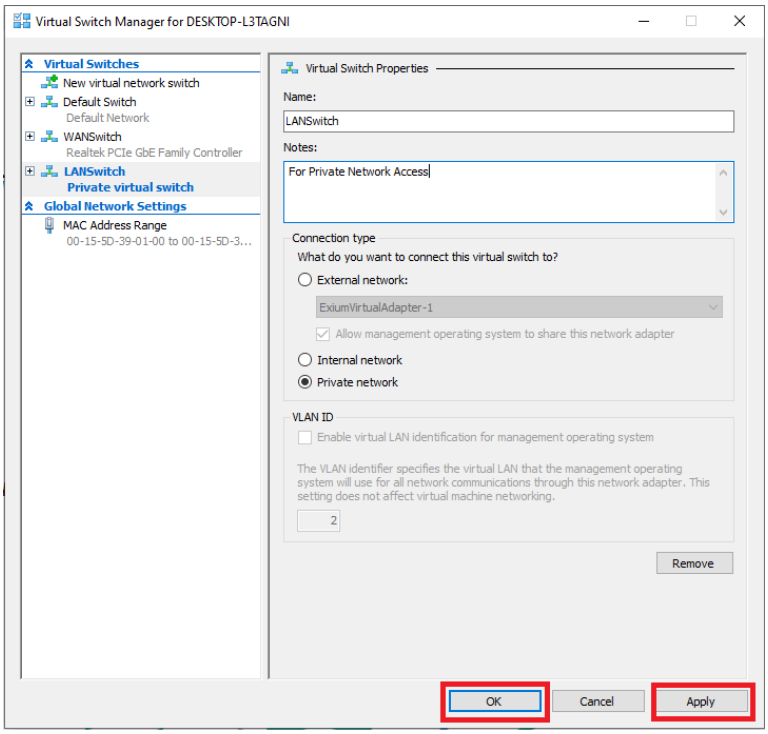
Again, on Hyper-V Manager window, click on “Virtual Switch Manager…” available on right panel to create LAN network.
On the same window, virtual switch types will be displayed.
To create WAN network, click on “Private” and “Create Virtual Switch”



On new window, change the name. Switch will not ask to select network adapter because it is a private network switch.
LAN/Private network virtual switch creation can be different on other setups (External Ethernet adapters), please follow the correct steps for configuration.

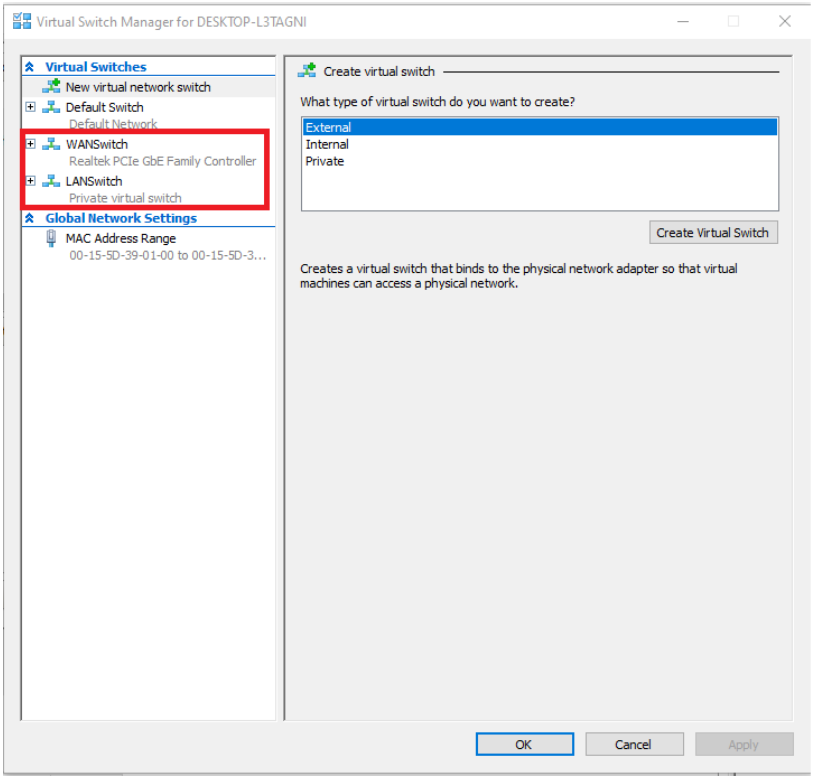


After setting the name, click on “Apply” and “OK” to finish configuration.



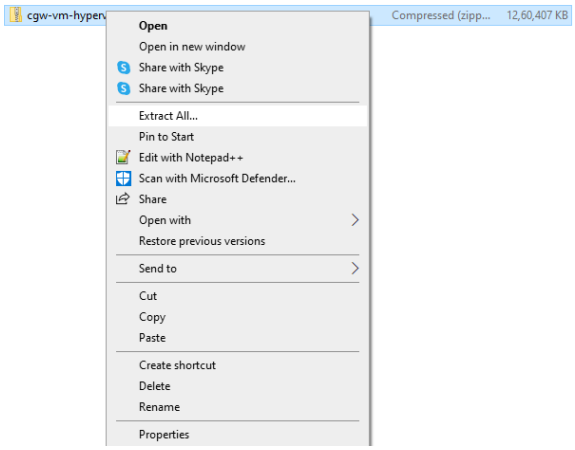
Verify virtual switches created and available on Hyper-V environment.
Open "Virtual Switch Manager..." from Hyper-V Manager window and check left panel. Both WAN and LAN switches must be visible.

It will show only one switch configuration if LAN configuration was skipped for CGW single interface deployment.

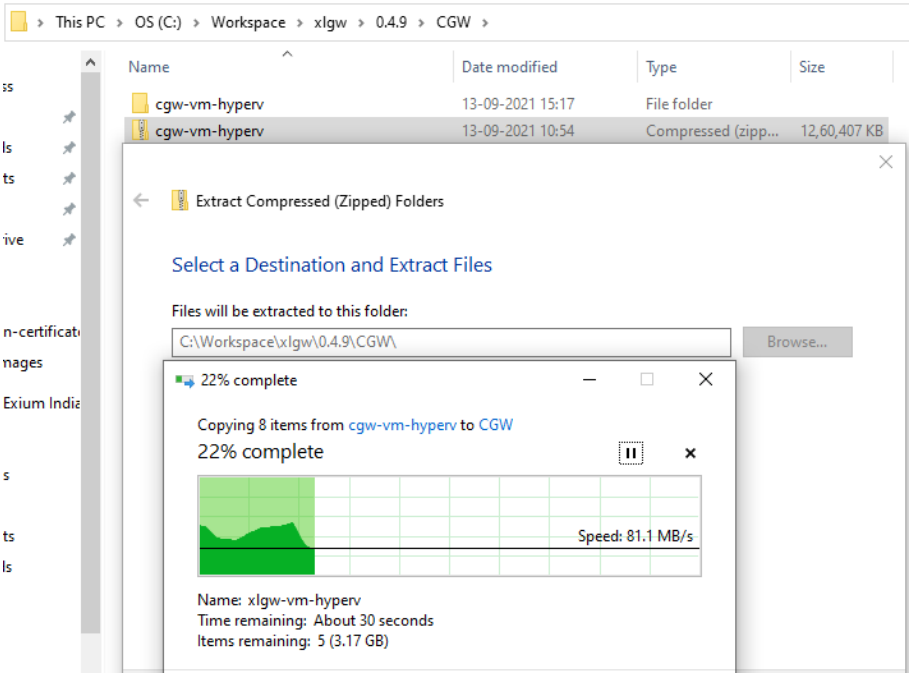


3.7.5.3 Steps to Deploy

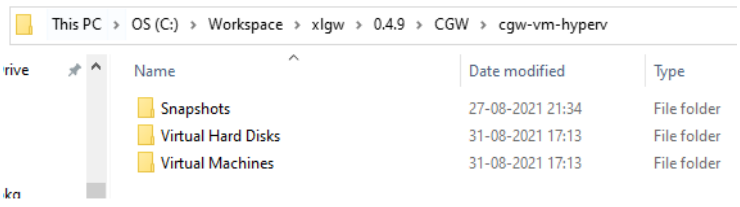
1. Use below link to download the zip file on a local laptop. Laptop should be assessable from the Hyper-V environment: https://clientreleases.s3.us-west-1.amazonaws.com/cgw/cgw-vm-hyperv.zip
2. Unzip the file and store on computer:



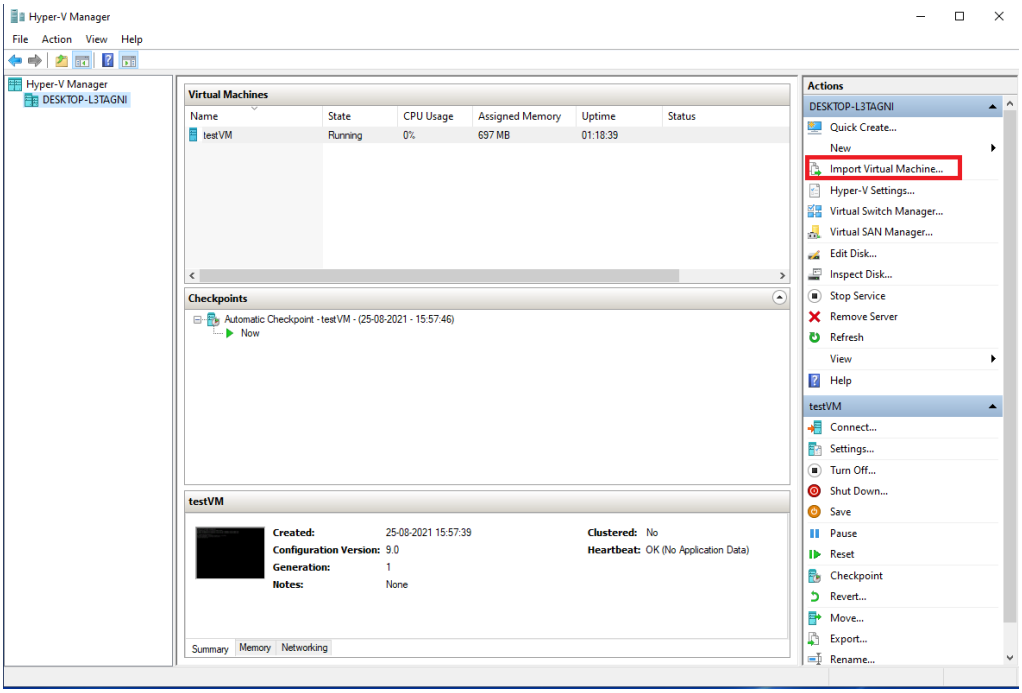
Select the folder where you want to extract the file on computer:



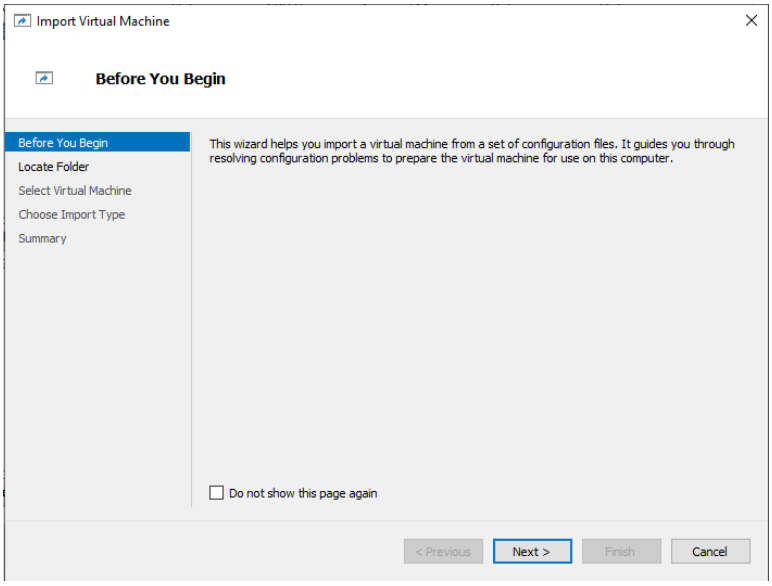
On local computer, navigate to the folder created after extracting above zip file and verify that it contains below directories:



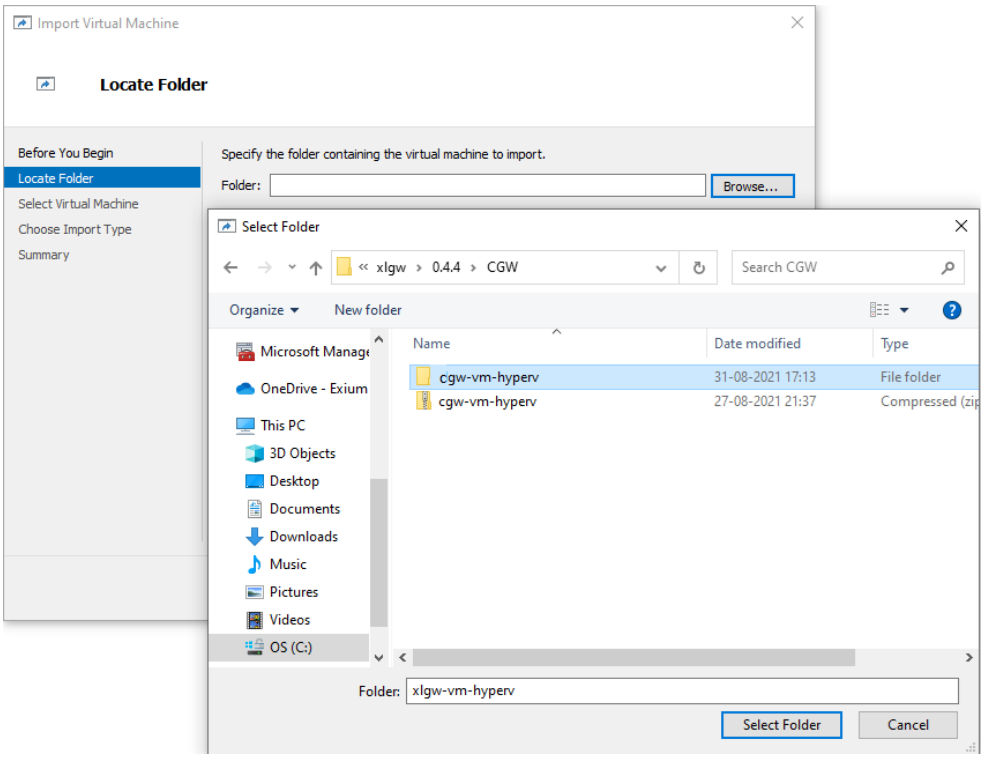
3. Open Hyper-V Manager and click on “Import Virtual Machine…” present in right panel:



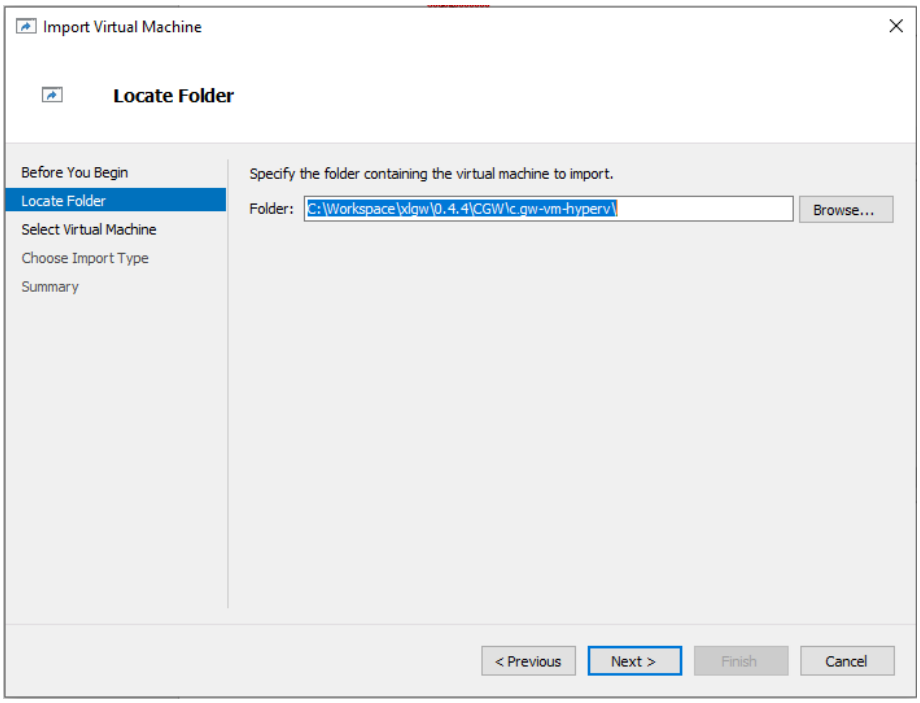
Click on “Next” on first page (Before you Begin).

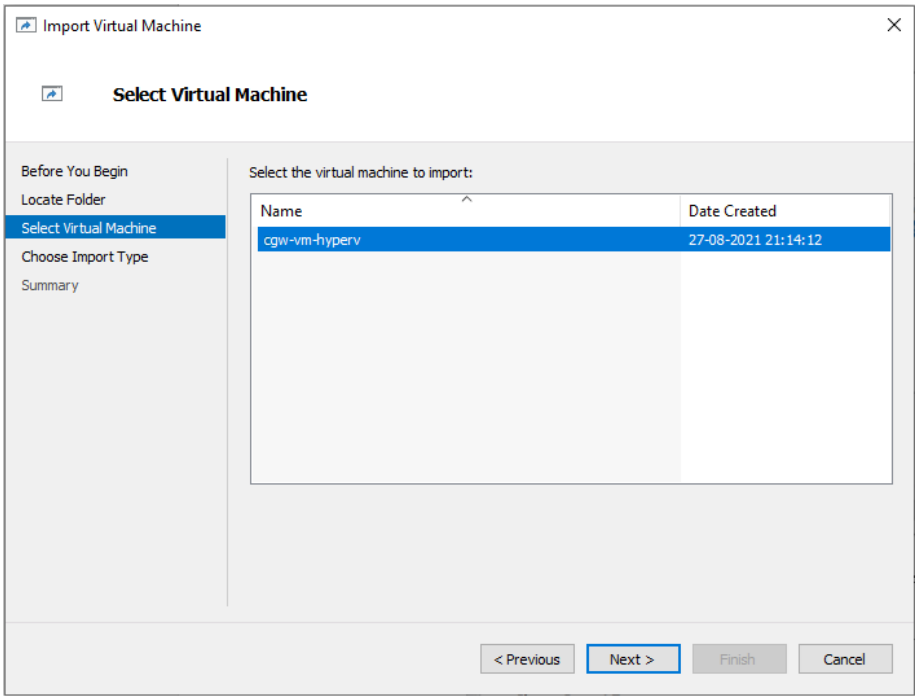


4. Click on “Browse” and select the folder which was created after extracting the zip file (cgw-vm-hyperv.zip)

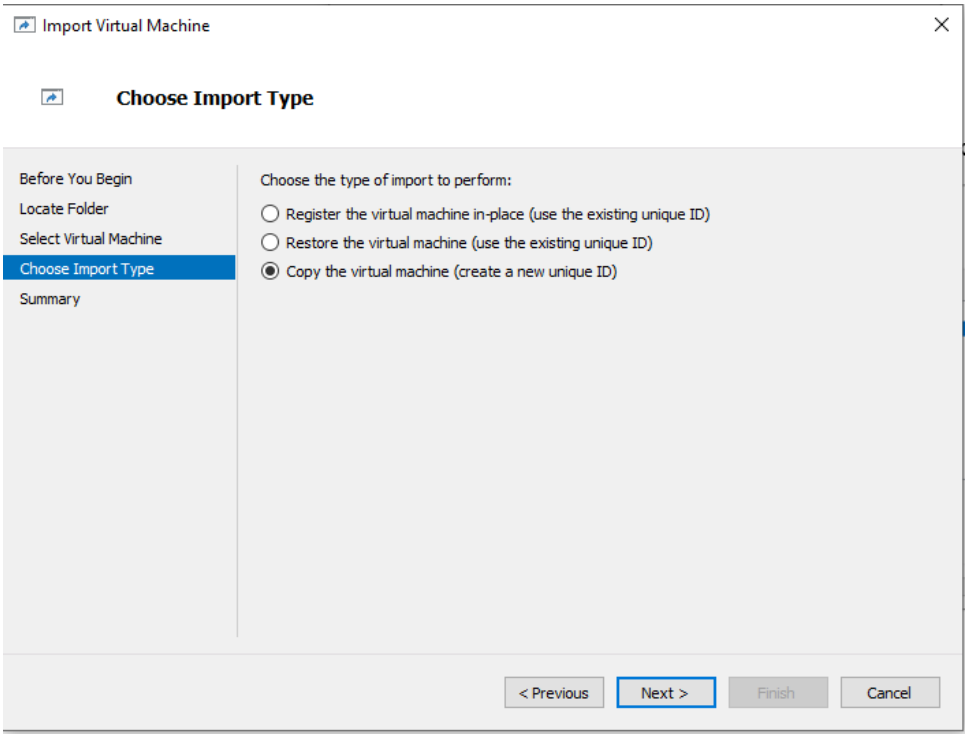


Click on “Next” button after folder is selected. Select the VM “cgw-vm-hyperv” and click on “Next”:

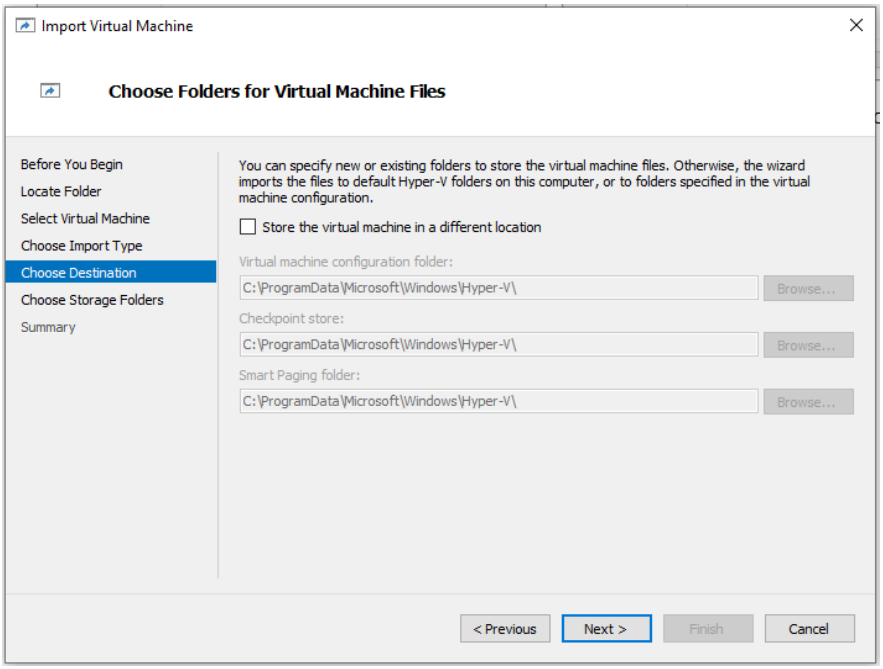




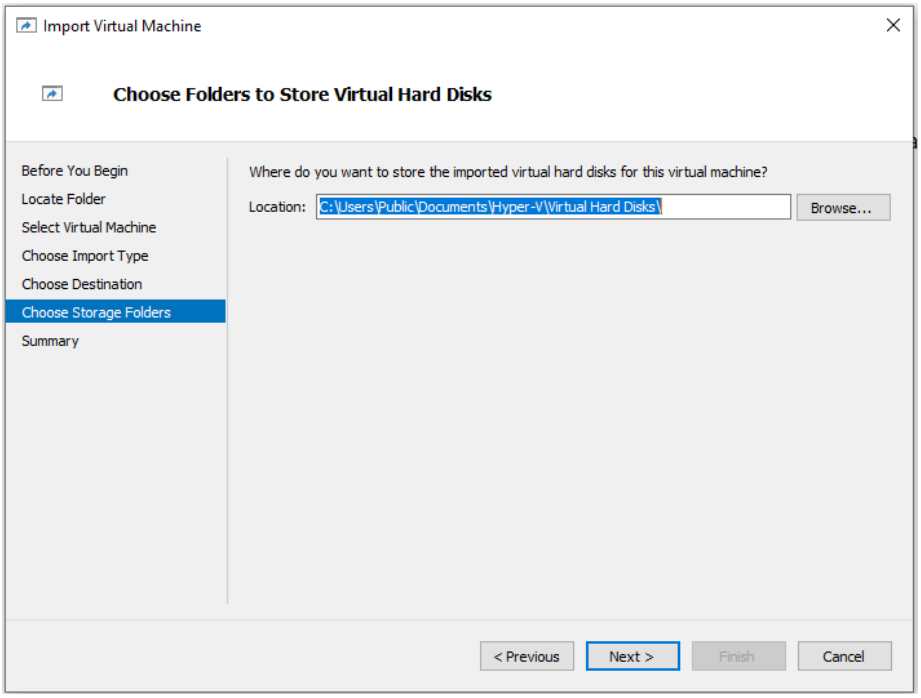
Choose import type “Copy the Virtual Machine (create a new unique ID)” option and click on “Next”:



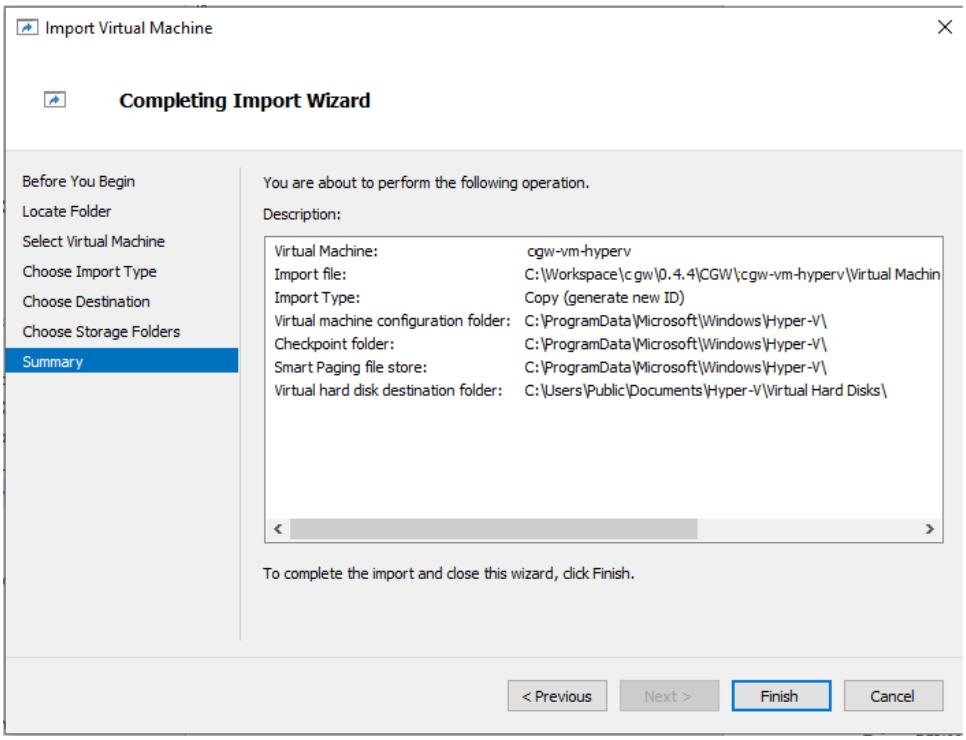
Select a specific folder to store VM files or it will take default path. Click on “Next” if changes are not required in path



Select a specific folder to store VM Hard disks. Click on “Next” if changes are not required in path

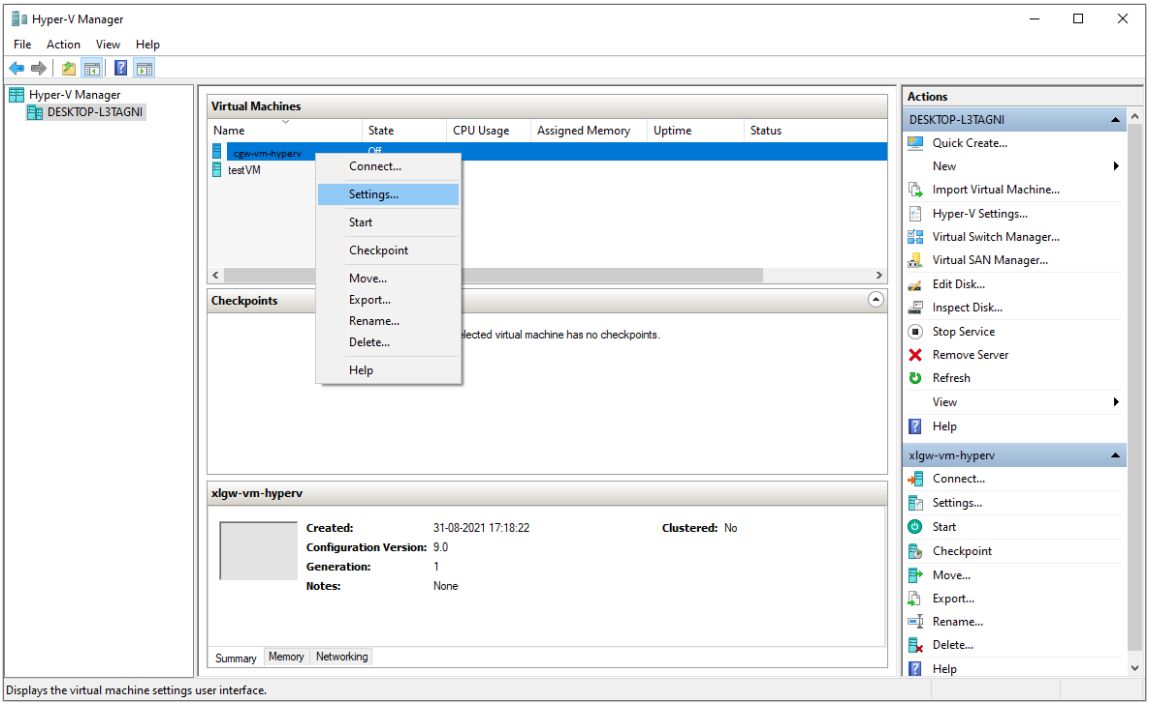


On page “Completing Import Wizard”, check the paths and other details. Click on “Finish” to complete the on-boarding.
Message will be displayed while files are being copied and import action completes.

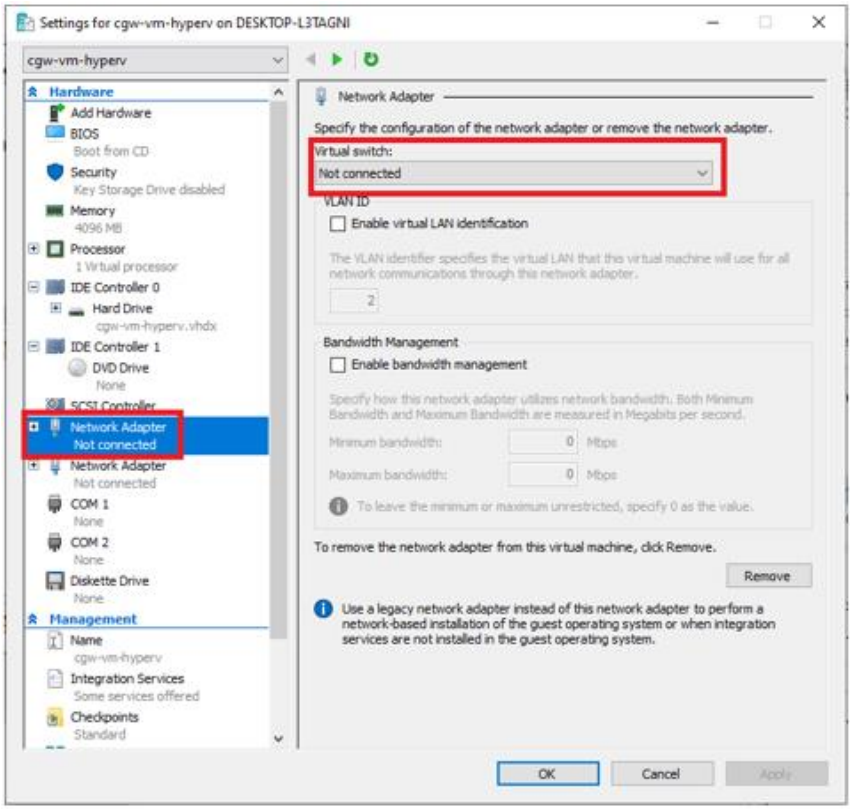


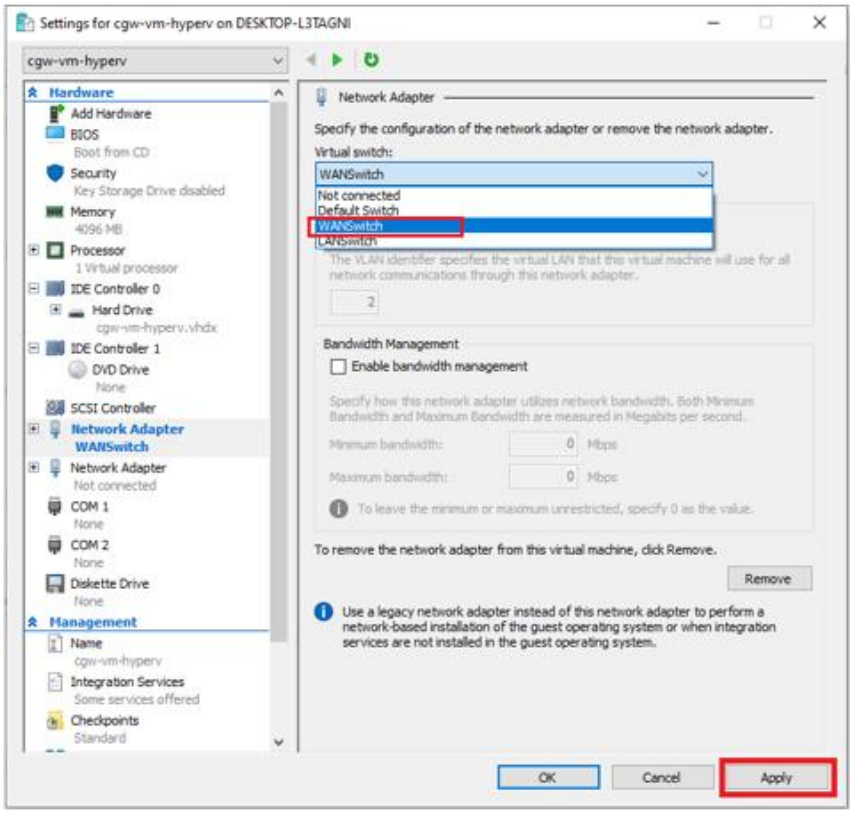
3.7.5.4 Networking Setup

Assuming WAN and LAN networks are already present on Hyper-V.
CGW requires minimum two interfaces, one for internet access and another to access private network on LAN.
On Hyper-V Manager window, select CGW VM “cgw-vm-hyperv”, right click and select “Settings…”:



On Settings window, click on the first Network Adapter and select the virtual switch from drop down list, which provides access to internet/WAN. Click on “Apply”.

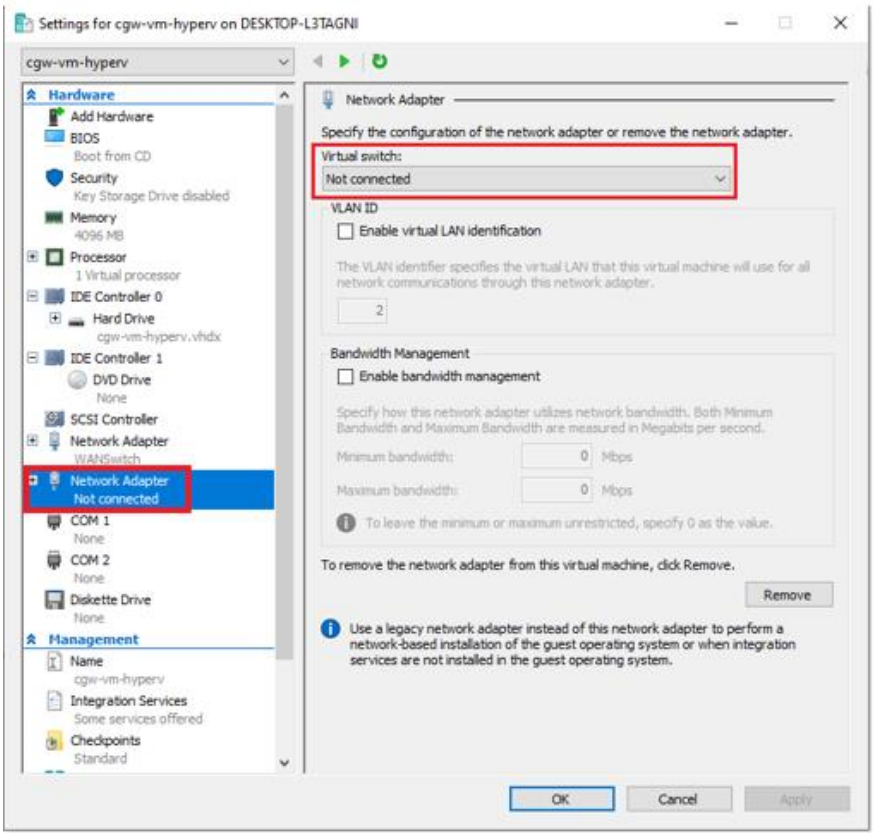


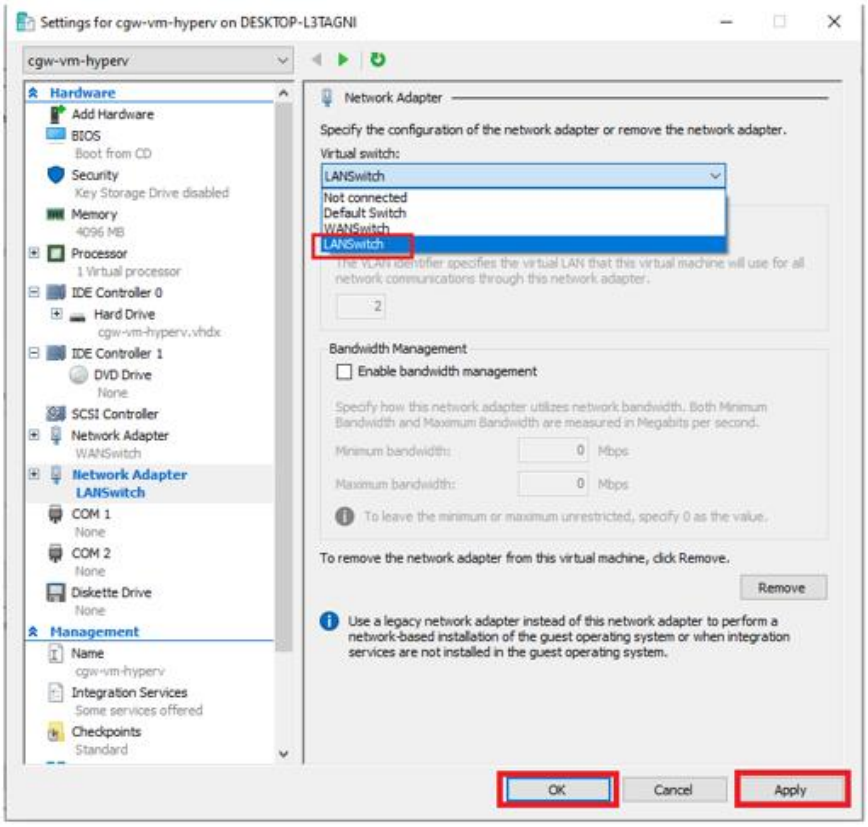


Remove second interface from CGW VM, if single interface is planned for WAN and LAN connectivity.

- In left panel select second adapter
- Click on remove
- Skip below steps for switch selection for separate LAN network

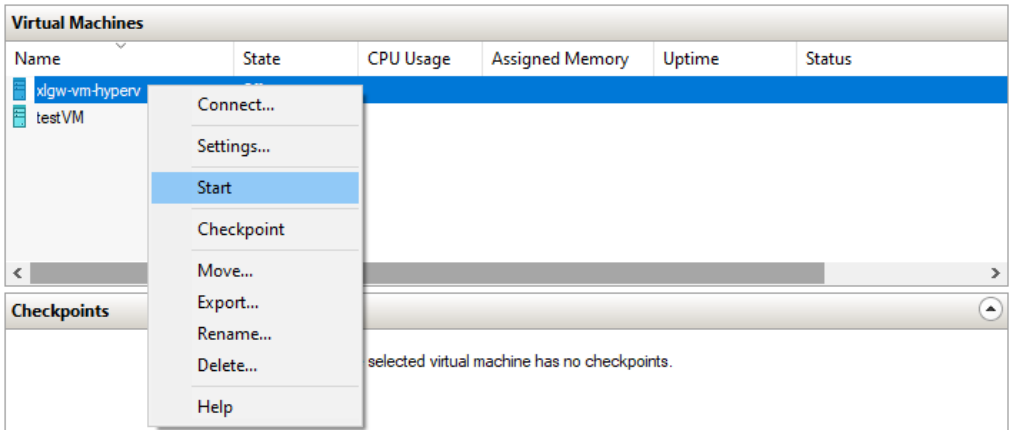
On same Settings window, click on the second Network Adapter and select the virtual switch from drop down list, which provides access to private network/LAN. Click on “Apply” and “OK” to finish.



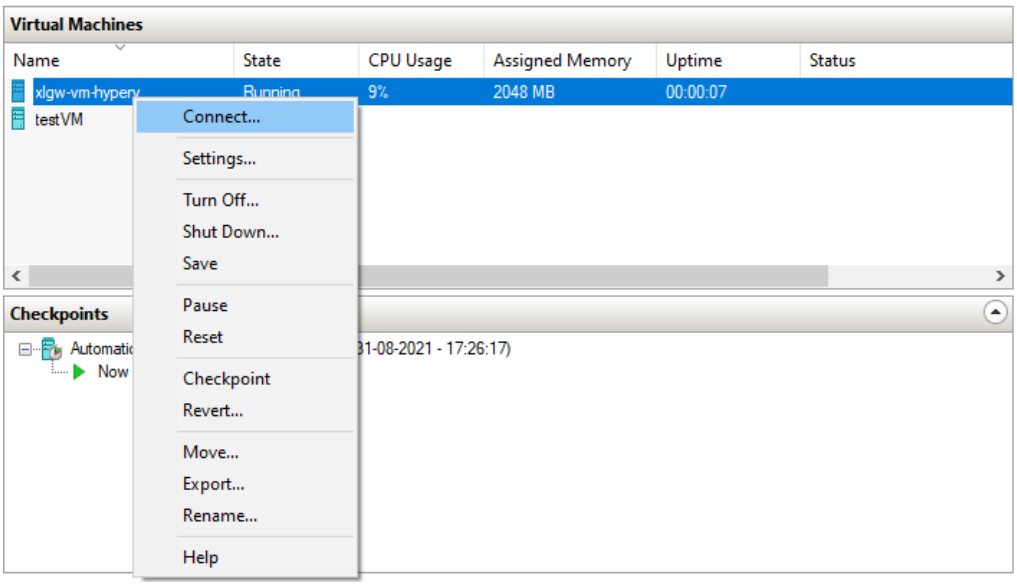


3.7.5.5 Start CGW VM and Access VM Console

a. On Hyper-V manager, click on the CGW virtual machine, right click, and select “Start” to start the VM.

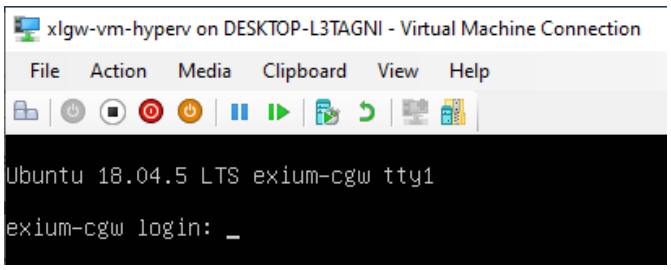


b. After VM starts, it will not open console automatically. Again, right click on CGW VM and click on “Connect”. It will open VM console

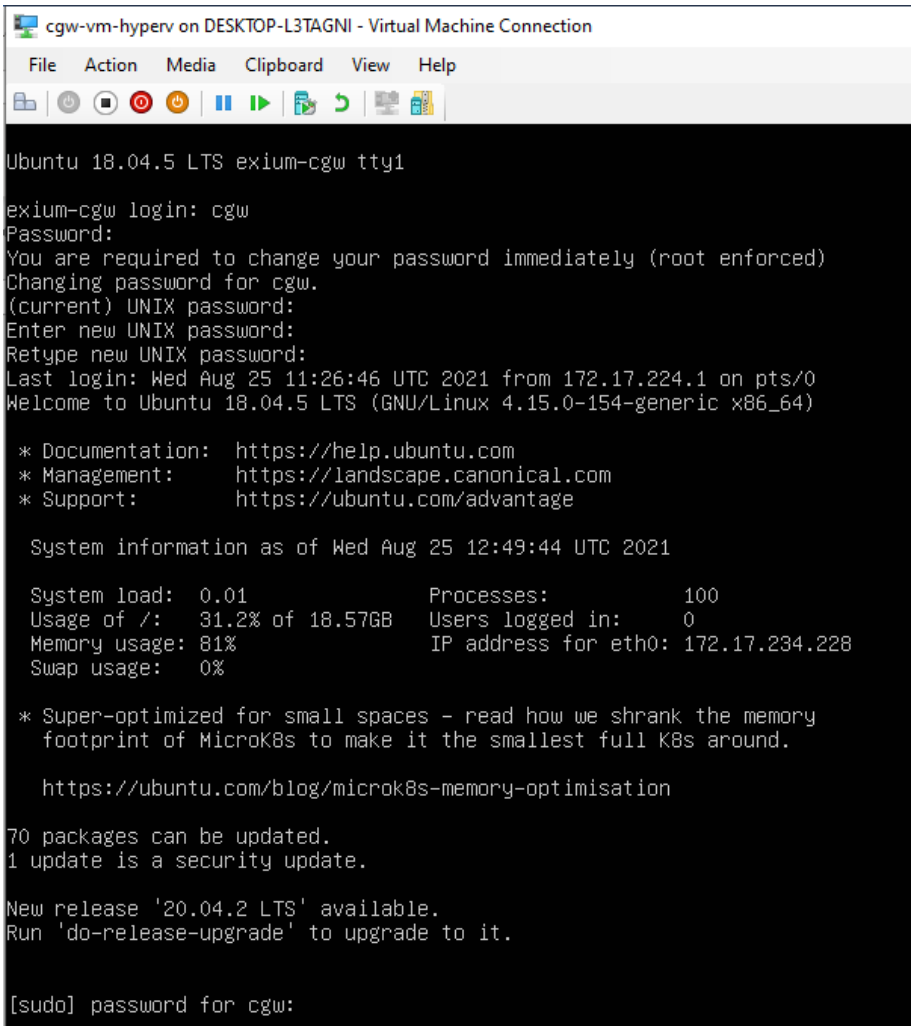


3.7.5.6 Set VM Password

VM console will ask user to enter login details, use default username and password to set your own password:



Username: cgw
Password: cgw
After entering default password, VM will ask again to enter default password “cgw” to initiate password change procedure. Provide your own password by following instructions on console.



3.7.5.7 Install IP addresses on vNICs

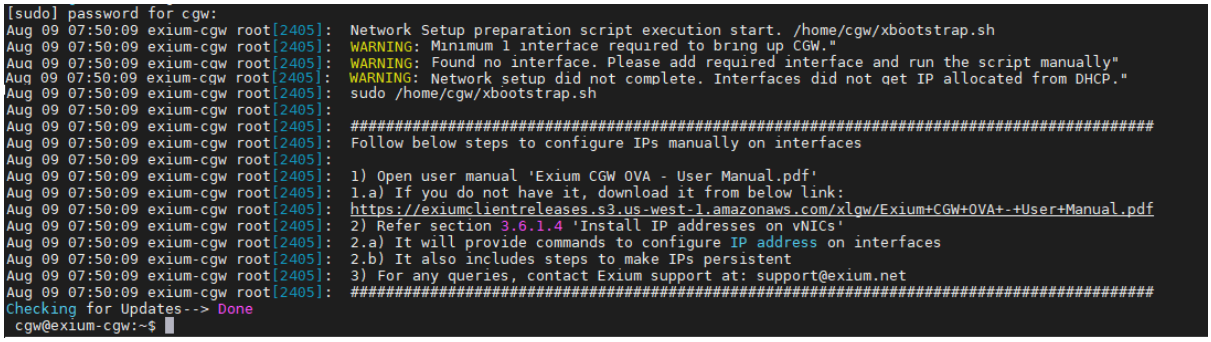
After setting the password on the VM terminal, it will again ask to provide password to run the bootstrap script which takes care of IP address allocation using DHCP.

IP address allocation can be handled with below approaches:

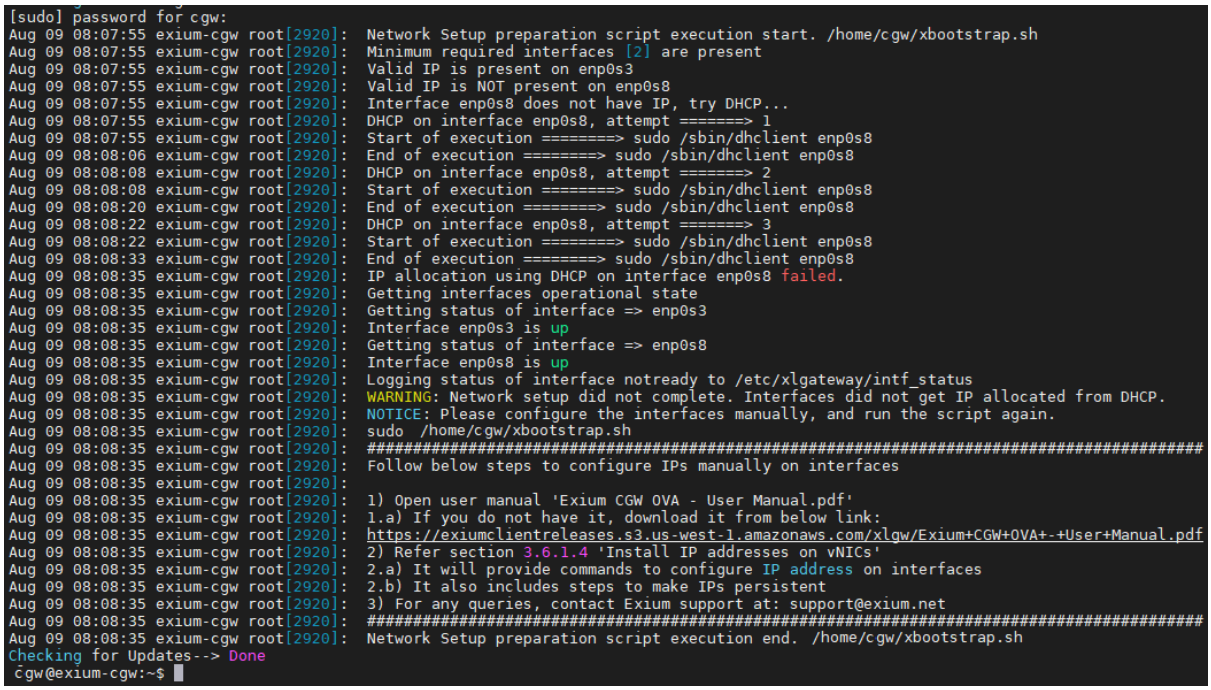
- If interfaces on the VM are connected to DHCP enabled network, then IP will be allocated by DHCP server (see below “Bootstrap Script”)
- In case of multiple interfaces, if one of the interfaces on the VM is connected to DHCP enabled network, then one interface will get IP from DHCP server, and another must be configured manually (see below “Manual IP Configuration”)
- If interfaces on the VM do not have DHCP enabled network, then user must configure IP addresses manually (see below “Manual IP Configuration”)

Bootstrap Script

- Script will verify minimum networking requirements and accordingly provide instructions on terminal:
  - Script will pull interface names and request DHCP allocation
    - Configured retries for each interface – 3
    - Configured timeout for each DHCP request – 30 seconds
  - **Case-1: No interface present on CGW VM**
    - If minimum one interface is not available, then execution will end with warning



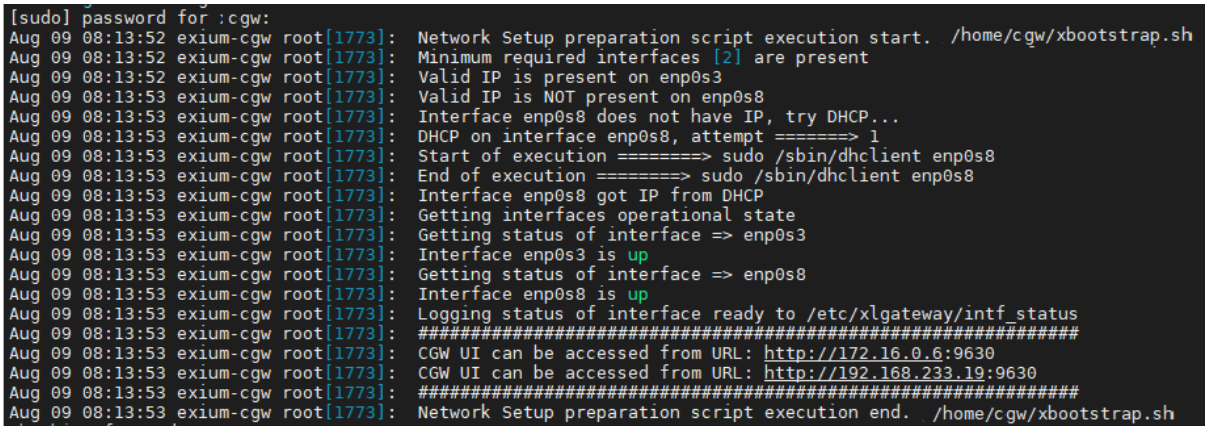
  - **Case-2: DHCP on one interface only**
    - In case two interfaces are available and one of the interfaces gets IP from DHCP, but second interface does not:
      - Execution will end with warning



- Refer “Manual IP Configuration” section included below
- After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI

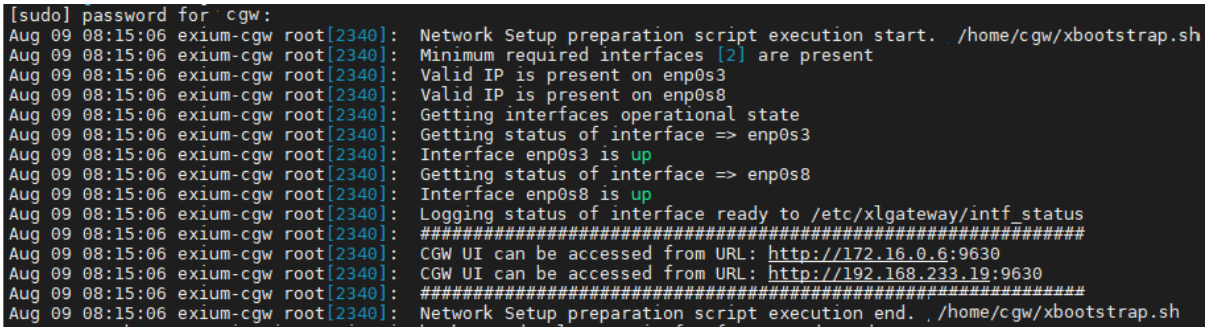
```
# sudo /home/cgw/xbootstrap.sh
```

- **Case-3: DHCP on both interfaces**
  - If interfaces get IP addresses from DHCP and states are up:
    - Execution will end and it will show the URLs which can be used to access CGW UI



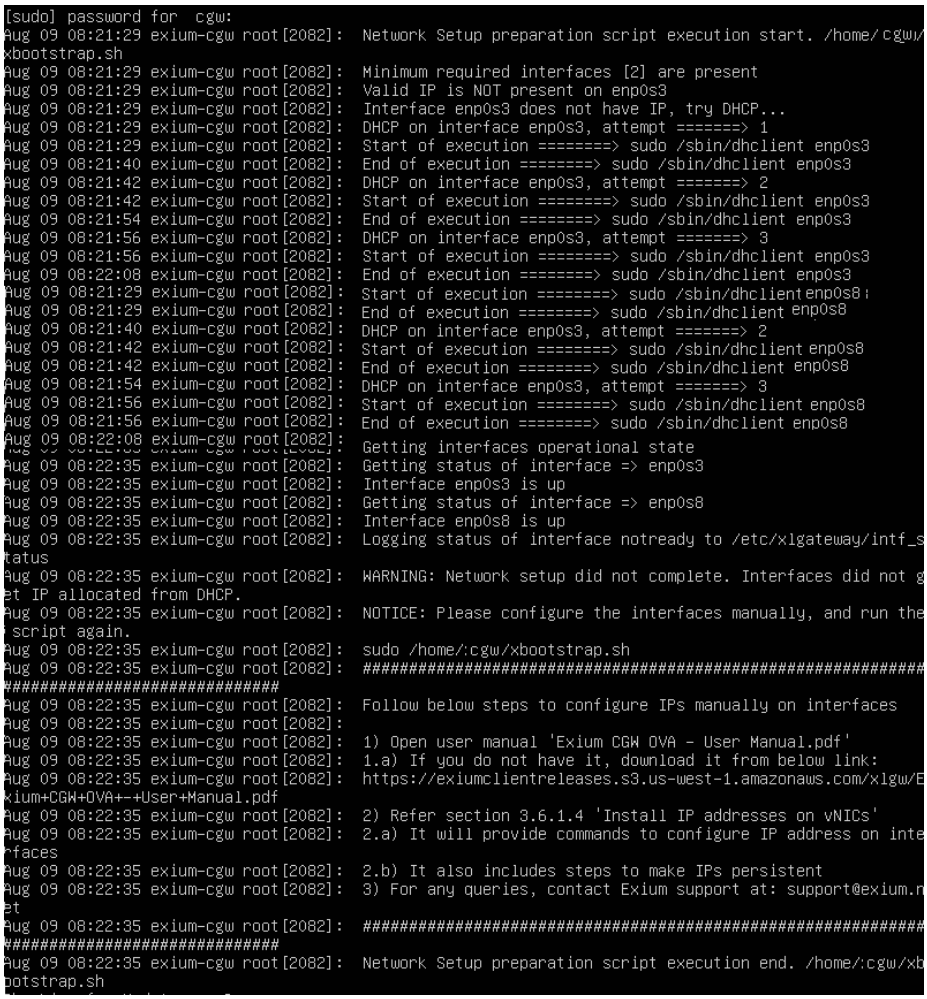
- **Case-4: IP addresses are already assigned on both interfaces**
  - If valid IP present on interface:
    - Execution will end with validations on both interface
    - Instructions will show URLs which can be used to access CGW UI
    - For eg: CGW UI access URL format would be **http://<CGW-IP>:9630**

- Each time user logs into CGW VM using “cgw” user credentials, bootstrap script will run and validate the interface IPs and states.



Manual IP configuration

- **No DHCP on interface**
  - If associated/attached network does not allocate IP address using DHCP then execution will end with warning

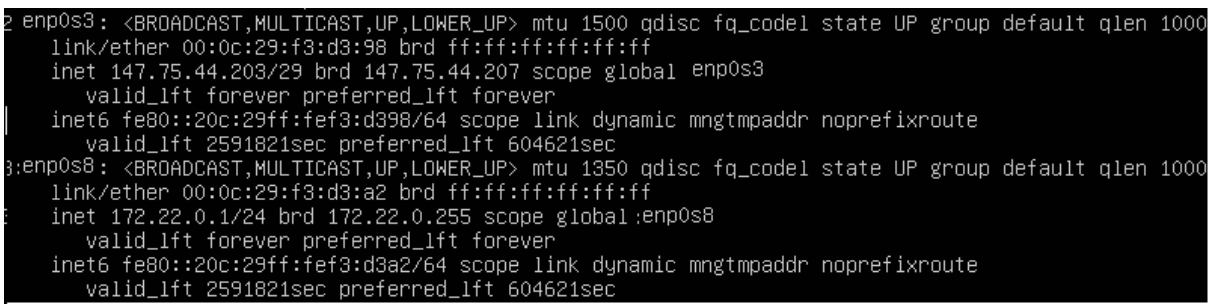


Use Command "`sudo ip addr`" to check interfaces installed:

Note: If there is only one interface then skip command/step for another interface.

Use below commands to configure IP addresses manually:

```
# sudo ifconfig enp0s3 <WAN-ip-address>/<WAN-mask> up
# sudo ifconfig enp0s8 <LAN-ip-address>/<LAN-mask> up
```

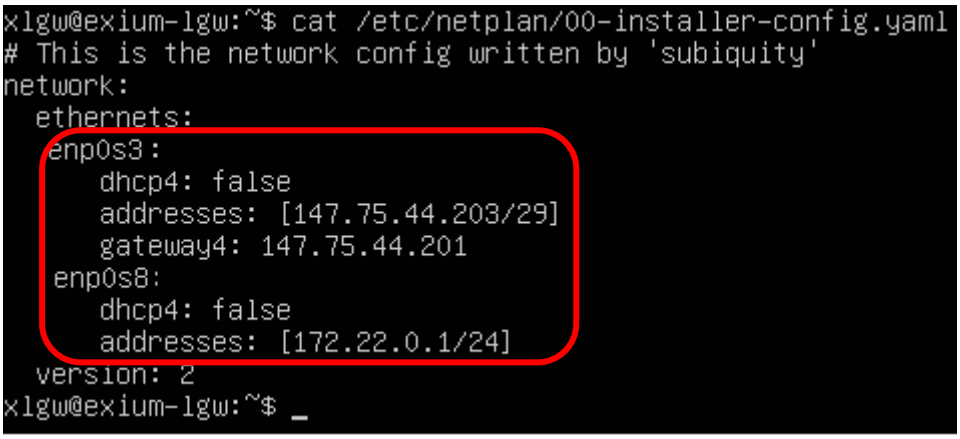


Use "netplan" utility to make IP addresses static on VM.

- Edit existing netplan and include the IP address installed manually.

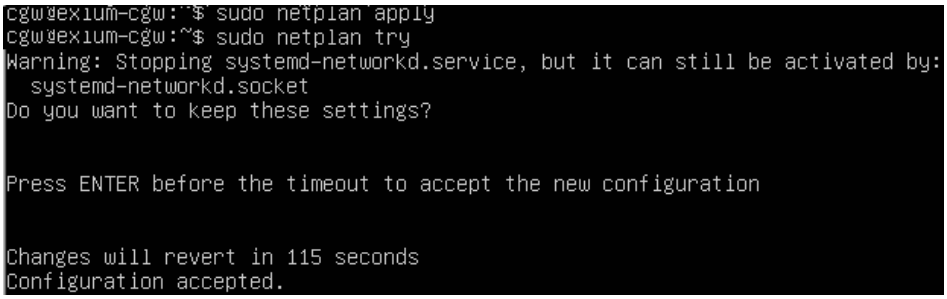
```
# sudo vim /etc/netplan/00-installer-config.yaml
```

- Add interface details:
  - Name of the interface
  - dhcpv4: false
  - addresses: IP address to be installed: Same IP which was configured manually
  - gateway4: Default gateway of the interface



- Apply the configuration:
  `# sudo netplan apply`

- Verify configuration
  `# sudo netplan try`
- Press enter, when the timer starts.
  - Configuration Accepted will be shown in case of successful scenario.



- After configuring IP addresses manually on VM, user can run below script to get URLs to access CGW UI
  `# sudo /home/cgw/xbootstrap.sh`

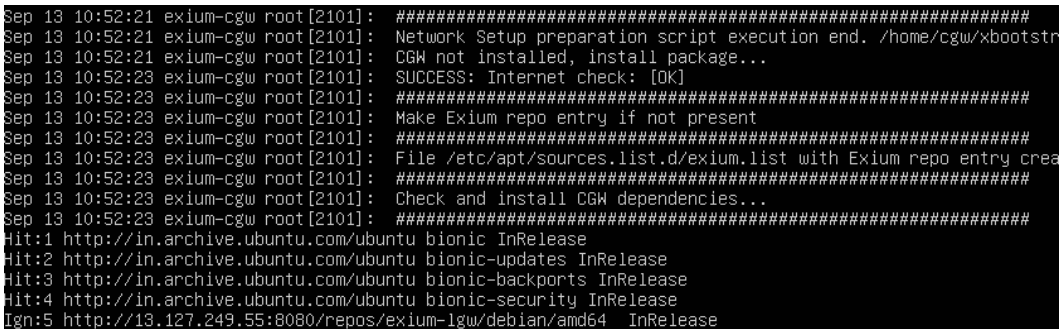
- Verify the local time on the VMware machine is correct. If it is not, update the time using Network Time Protocol.

- Verify internet is accessible from CGW VM. If not, update the network settings accordingly.

3.7.5.8 CGW Software Installation

After IP addresses installation, bootstrap script will check internet connectivity. If internet is not accessible, then script will exit with warning, else it will continue with installation procedure.

Check default routes and verify DNS resolution and internet connection work from CGW VM. Once internet is accessible from CGW VM, run bootstrap script again to complete installation process.



Installation includes, CGW dependent packages installation, tuning parameters setting and latest CGW application software installation.

After successful installation, terminal will show below output:

Navigate to Section 3.11, to setup CGW.

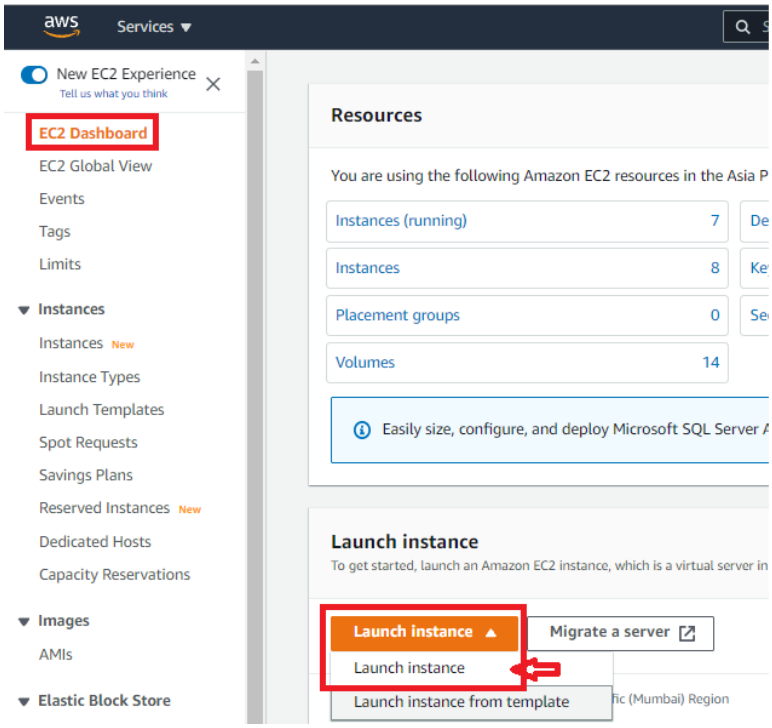
3.7.6 Deploy AWS Elastic Compute Cloud (EC2)

3.7.6.1 Pre-requisites

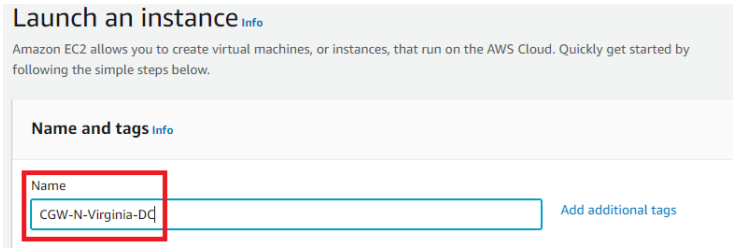
1. Valid login and privileged access to AWS EC2 to launch instance
2. Virtual Private Cloud (VPC) on AWS EC2
3. Network/Subnet defined to access Internet for WAN connectivity in the same VPC where VM will be created
4. Network/Subnet defined to access private cloud services for LAN connectivity in the same VPC where VM will be created
5. Security groups defined with rules to allow:
    a. ICMP (For reachability checks)
    b. TCP port 9630 (For CGW UI access)
    c. TCP port 22 (For SSH access)

3.7.6.2 Launch CGW AMI

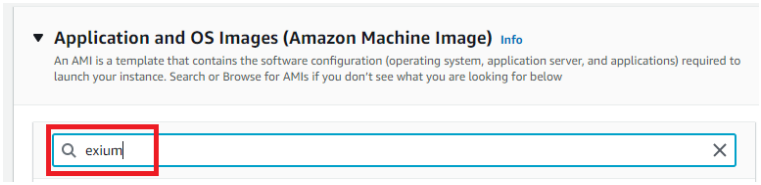
1. Login to AWS Elastic Compute Cloud (EC2) using valid user credentials
2. Navigate to “EC2 Dashboard” on left panel and click on “Launch Instance”:



3. Provide the name of the instance



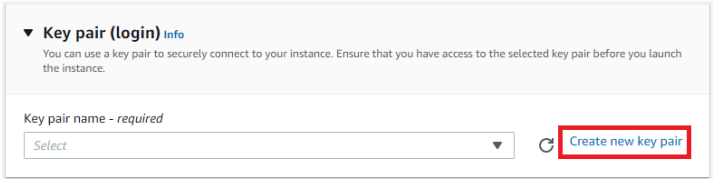
4. Type “exium” in “Application and OS Images (Amazon Machine Image)” search box and press enter.



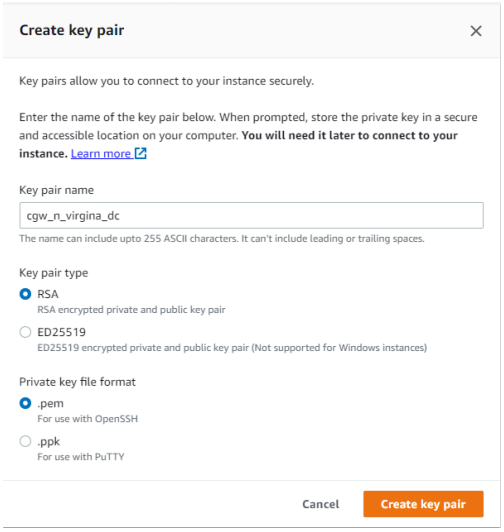
5. Select “Community AMIs” tab and CGW AMI would be visible. Click on select (first AMI) to continue.

On next page, if user wants, instance type can be modified.

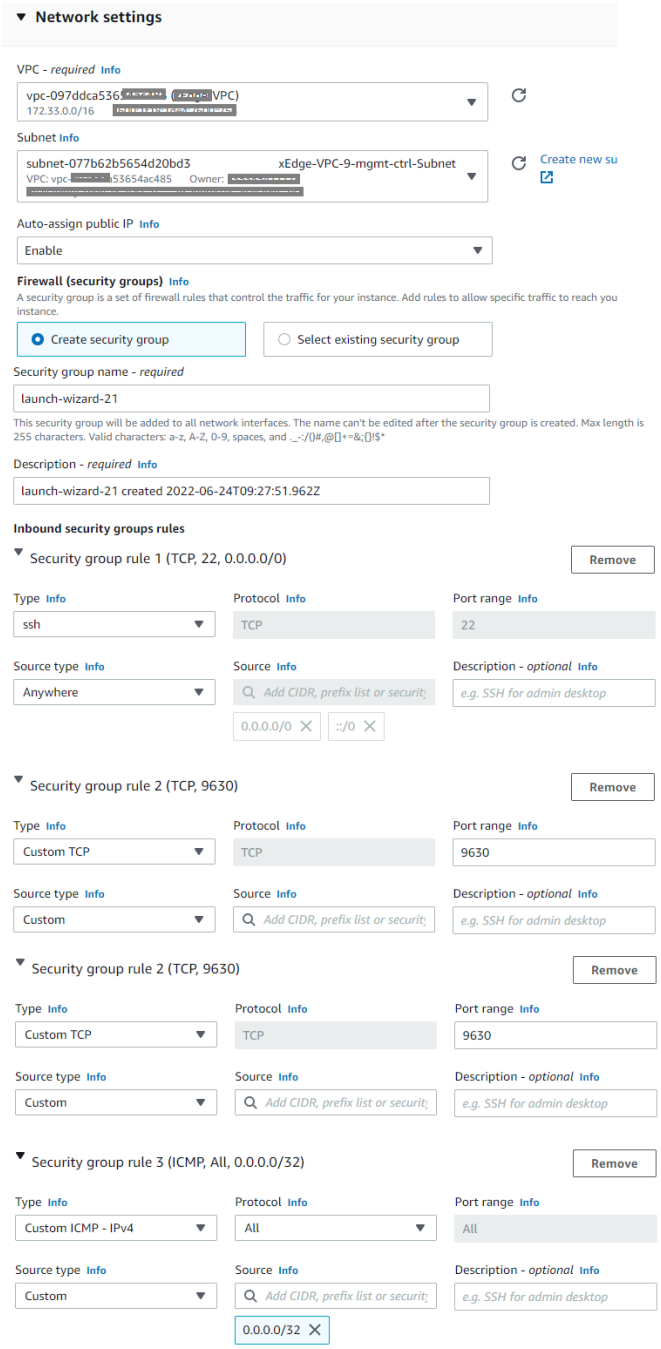
6. Click on “Create new key pair” in section “Key pair (login)”



7. On pop up page, provide key pair name, select the key pair type and private key format according to your requirements. Or follow the selection mentioned in the snapshot below.
   Click on “Create key pair”. Key file will be downloaded on your laptop/machine. Save it for SSH access in future

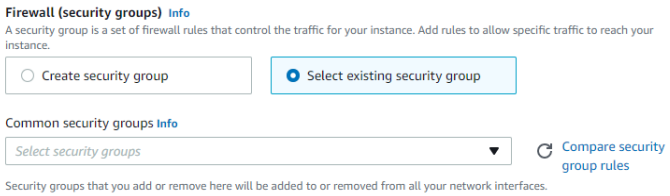


8. Configure network by selecting “Edit” option in “Network settings” section:
   a. VPC – Check and select the VPC (Virtual Private Cloud) from drop down list
   b. Subnet – Select the subnet which provides connectivity to WAN/Internet
   c. Auto-assign Public IP – Select Enable from drop down list
   d. Security group – Select “Create security group” if you do not have existing security groups to use. Or select “Select existing security group”

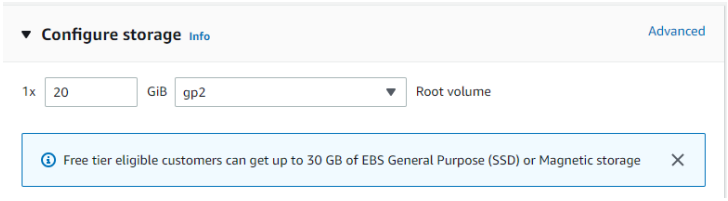


By default, inbound security rule for SSH access will be configured. User can add new security group rule if required. Security rules can also be managed later when instance is deployed and running. Above example shows to add custom TCP rule for CGW UI port 9630 and ICMP.

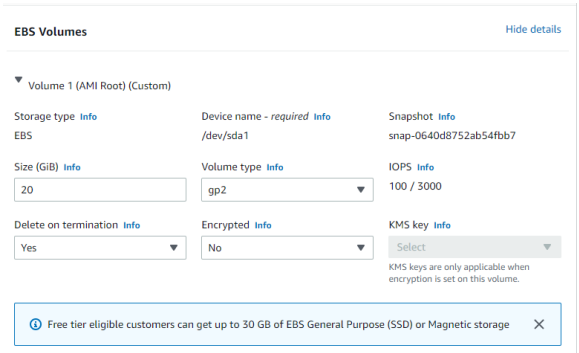
i. In case existing security groups are available, user will get drop down list to select.



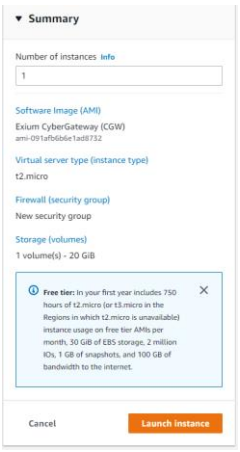
9. Configure storage, by modifying the root volume as per requirement. We recommend having minimum 20GB root volume.



   a. User can change Encryption type by selecting keys from drop down list.
      i. Click on “Advanced” option to open other configuration parameters. If Encryption is not selected or set as “Not Encrypted”, but Encryption is mandatory in customer’s AWS VPC, then VM will not up after it launched.

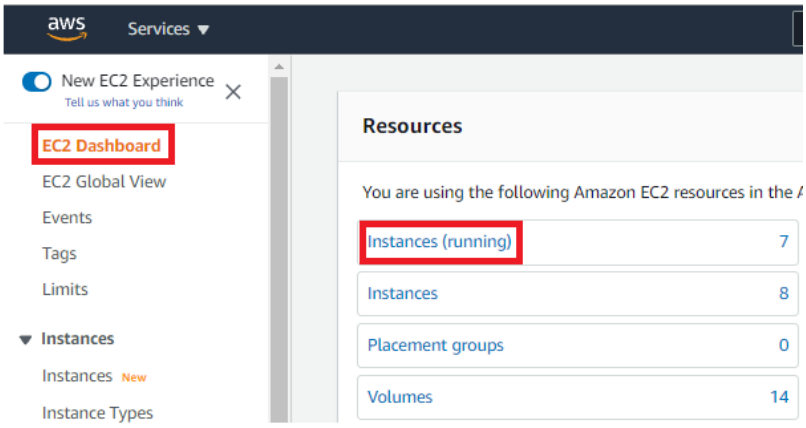


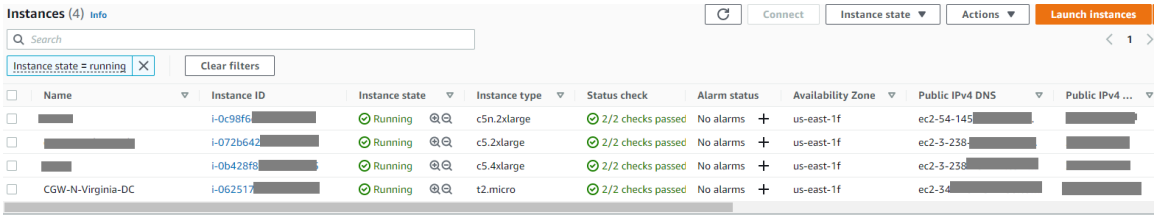
10. Review and Launch
    Click on “Launch instance” button at bottom right corner



3.7.6.3 CGW Software Installation

1. Access EC2 Dashboard and click on “Instances (running)”





2. Note Public IPv4 address of CGW VM
3. Login to CGW VM using the key pair file download in above step
    a. Use any SSH client
    b. Navigate to key pair file location
    c. Change the file permission:
        # chmod 600 cgw_n_virginia_dc.pem
    d. Use below ssh command to login to CGW VM:
        # ssh -i cgw_n_virginia_dc.pem ubuntu@<CGW-public-ip-address>
4. Bootstrap script will automatically execute and check following points:
    a. Valid IP address on interface
    b. DNS resolution

Script will install CGW latest application software from Exium cloud repository.

```
24/06/2022  10:21.33  /drives/c/Workspace/Login/PEM-files  ssh -i cgw_n_virgina_dc.pem ubuntu@[redacted]
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-1045-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Jun 24 04:51:52 UTC 2022

  System load:  0.01              Processes:             109
  Usage of /:   10.7% of 19.32GB  Users logged in:       0
  Memory usage: 25%               IPv4 address for eth0: 172.33.5.110
  Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

101 updates can be applied immediately.
1 of these updates is a standard security update.
To see these additional updates run: apt list --upgradable


*** System restart required ***
Last login: Fri Jun 24 04:49:40 2022 from [redacted]
Jun 24 04:51:53 ip-172-33-5-110 root[82855]:  Network Setup preparation script execution start. /home/ubuntu/xbootstrap.sh
Jun 24 04:51:53 ip-172-33-5-110 root[82855]:  Minimum required interfaces [1] are present
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  IP address validation for interface eth0
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  Valid IP is present on eth0
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  Getting interfaces operational state
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  Getting status of interface => eth0
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  Interface eth0 is up
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  Logging status of interface ready to /etc/xlgateway/intf_status
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  ############################################################
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  CGW UI can be accessed from URL: http://172.33.5.110:9630
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  ############################################################
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  Network Setup preparation script execution end. /home/ubuntu/xbootstrap.sh
Jun 24 04:51:54 ip-172-33-5-110 root[82855]:  CGW not installed, install package...
Jun 24 04:51:56 ip-172-33-5-110 root[82855]:  SUCCESS: Internet check: [OK]
Jun 24 04:51:56 ip-172-33-5-110 root[82855]:  ############################################################
Jun 24 04:51:56 ip-172-33-5-110 root[82855]:  Make Exium repo entry if not present
Jun 24 04:51:56 ip-172-33-5-110 root[82855]:  ############################################################
Jun 24 04:51:56 ip-172-33-5-110 root[82855]:  File /etc/apt/sources.list.d/exium.list with Exium repo entry created
Jun 24 04:51:56 ip-172-33-5-110 root[82855]:  ############################################################
Jun 24 04:51:56 ip-172-33-5-110 root[82855]:  Check and install CGW dependencies...
Jun 24 04:51:56 ip-172-33-5-110 root[82855]:  ############################################################
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1935 kB]
Get:6 http://debrepo.exium.net/repos/exium-lgw/debian/amd64  InRelease
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [924 kB]
```

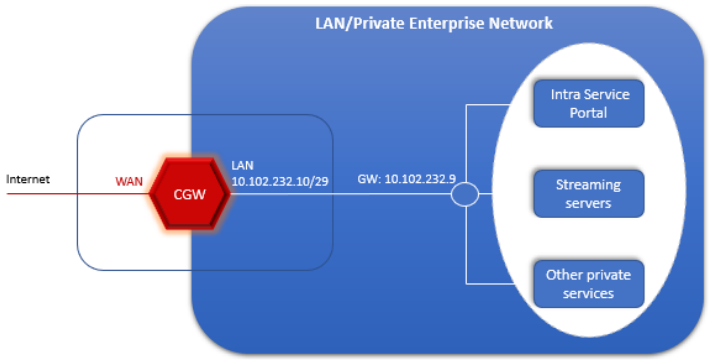
After installation completes, below message will be displayed on screen:

```
Sep 29 11:37:36 ip-172-31-47-249 root[933]:  ############################################################
Sep 29 11:37:36 ip-172-31-47-249 root[933]:  CGW application package installed successfully
Sep 29 11:37:36 ip-172-31-47-249 root[933]:  Use command 'sudo xlgateway setup' to start CGW configuration
Sep 29 11:37:36 ip-172-31-47-249 root[933]:  OR Access CGW UI for setup and connection
Sep 29 11:37:36 ip-172-31-47-249 root[933]:  CGW UI can be accessed from URL: http://172.31.47.249:9630
Sep 29 11:37:36 ip-172-31-47-249 root[933]:  ############################################################
ubuntu@ip-172-31-47-249:~$
```

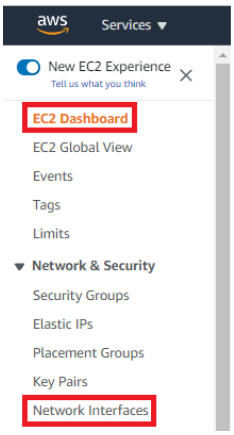
3.7.6.4 CGW LAN Interface

Create LAN Interface

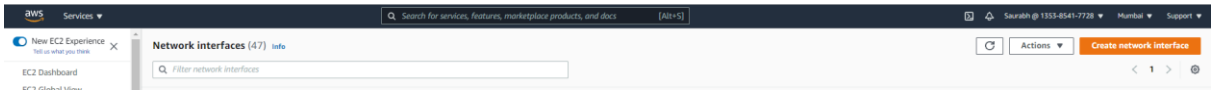
CGW requires 2 interfaces, one for WAN and another for LAN. Single interface is not supported for CGW on AWS environment.
WAN interface already gets created during launch. User needs to create another interface to access Private network.
Refer sample diagram below:



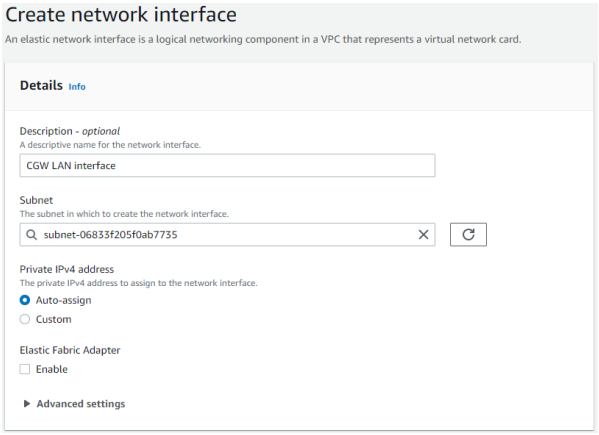
1. Login to CGW VM using SSH (For more details, refer Section CGW Application Installation, point 3). Keep terminal open to check interface state.
2. Access EC2 Dashboard and click on “Network Interfaces” in left panel

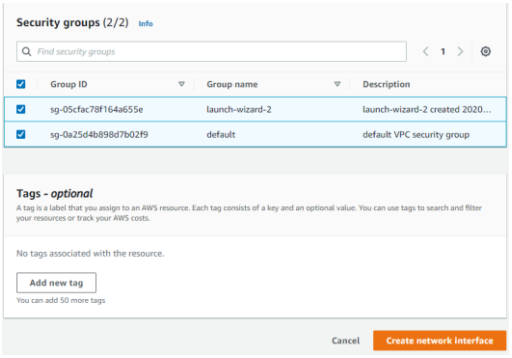


3. Click on “Create Network Interface”:

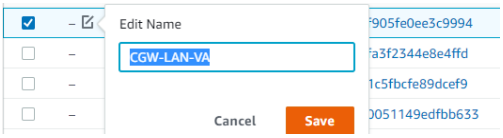


4. Provide description to identify interface later. Select the “Subnet” from drop down list.
    a. Make sure selected subnet belongs to same VPC which was selected during AMI launch.
    b. Make sure selected subnet is different than primary interface subnet which was selected during AMI launch
    c. Click on “Create network interface”

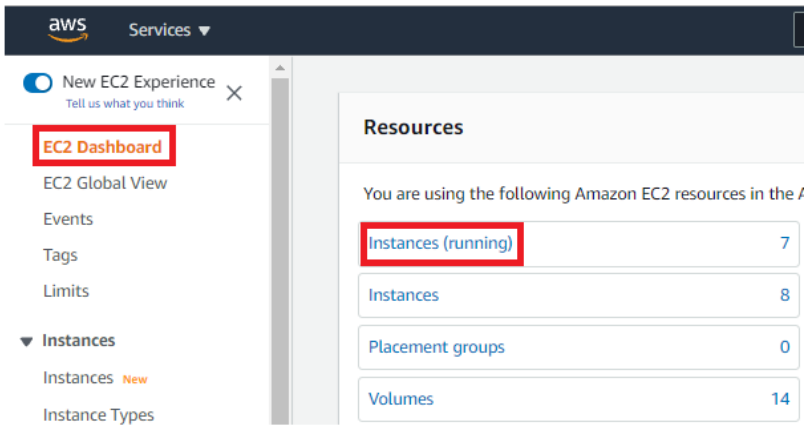




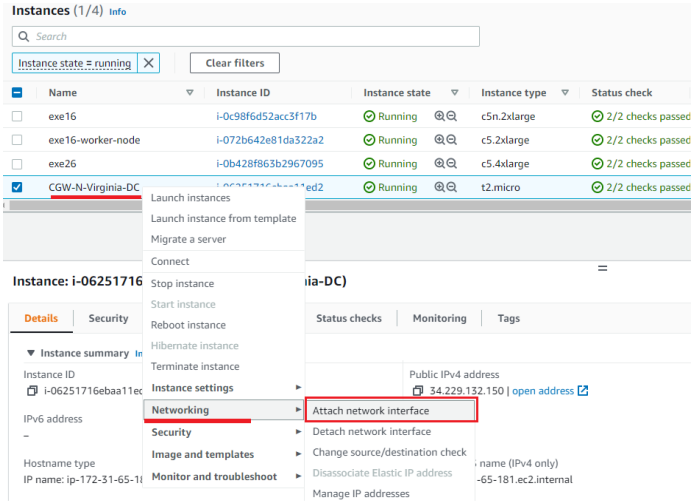
d. Make sure you note the network interface ID which was created in above step. LAN interface will be attached to CGW instance in next step.
e. Navigate to “Network interface” link in left panel again, identify the interface created and provide name to CGW LAN interface.



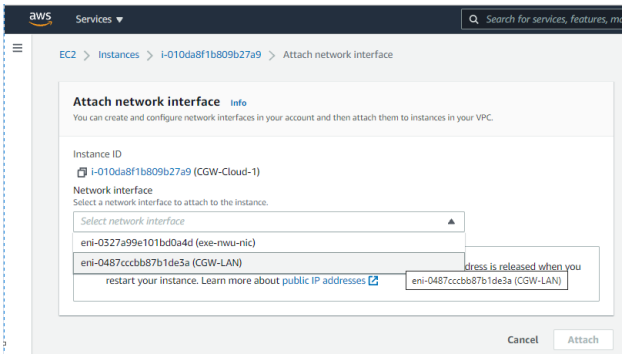
5. Access EC2 Dashboard and click on “Instances (running)”



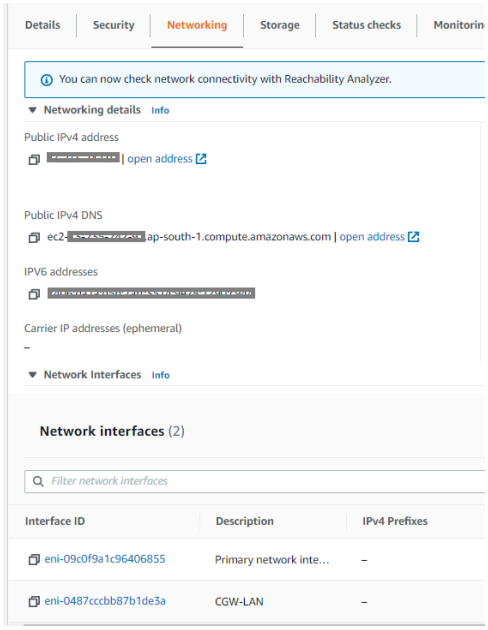
6. Right click on CGW VM and in Networking option select “Attach network interface”



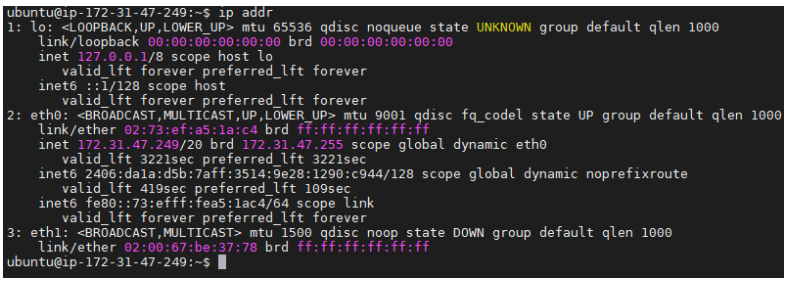
7. Select the interface which was created for CGW LAN to access private network. Click on “Attach”



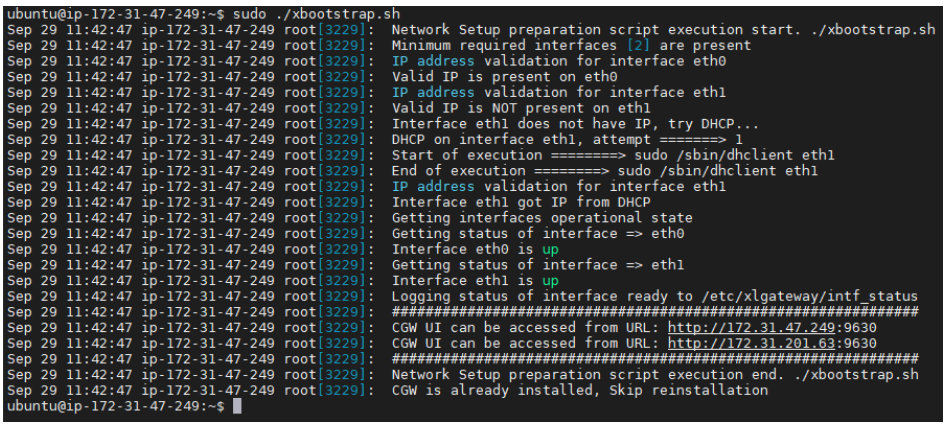
8. On “Instances” page, select CGW VM and check Network Interfaces. It should show both primary and new interface:



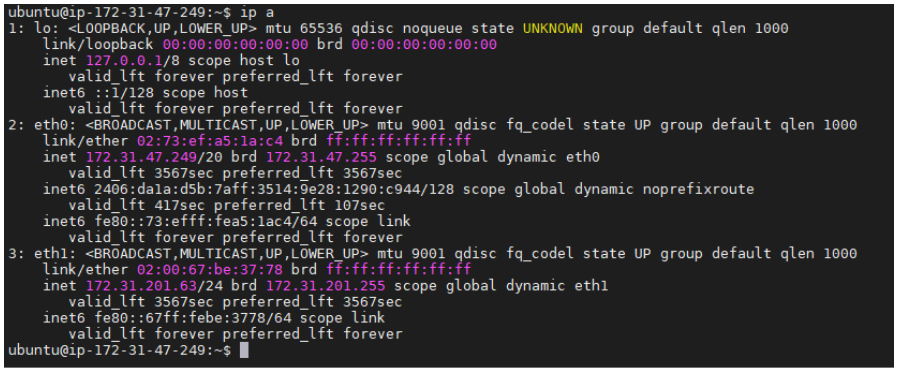
9. Additional interface may not have IP installed automatically. Execute “ip addr” command to see interface state:



10. Run xbootstrap.sh script available in user’s home directory.
Script will install IP using DHCP and validate the state of both interfaces.



11. Check IP addresses are properly installed using “ip addr” command
Below example shows:
    - WAN: `eth0`
    - LAN: `eth1`

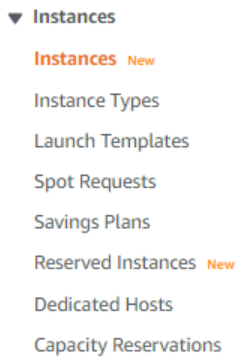


Now CGW VM is ready for setup and configuration.

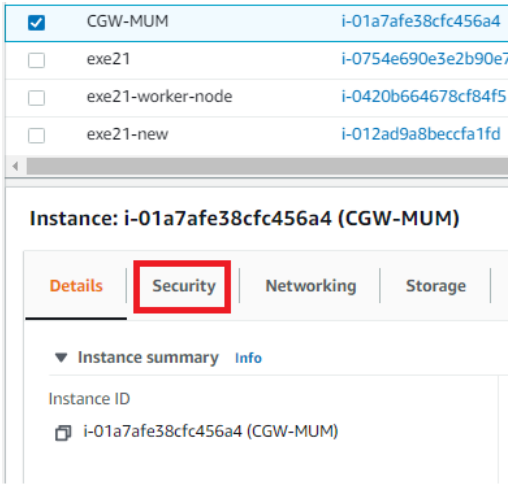
Outbound Rule Check

Allow all traffic on the LAN interface by modifying the outbound rules.

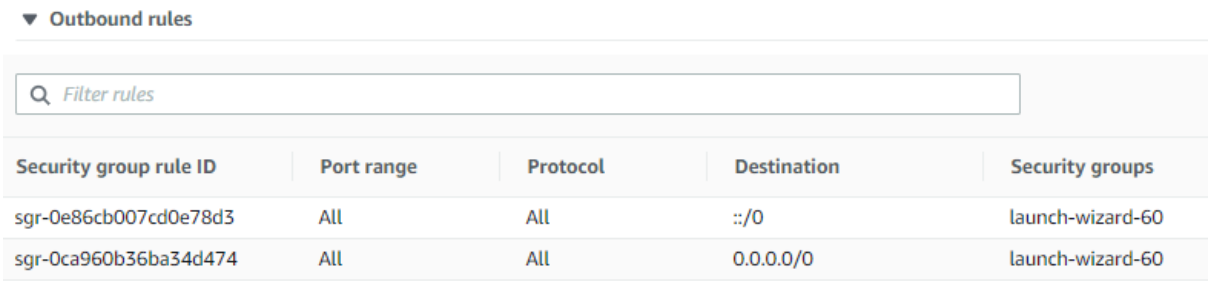
Click on the “Instances” in left panel of EC2 portal



Select CGW instance and click on “Security”:



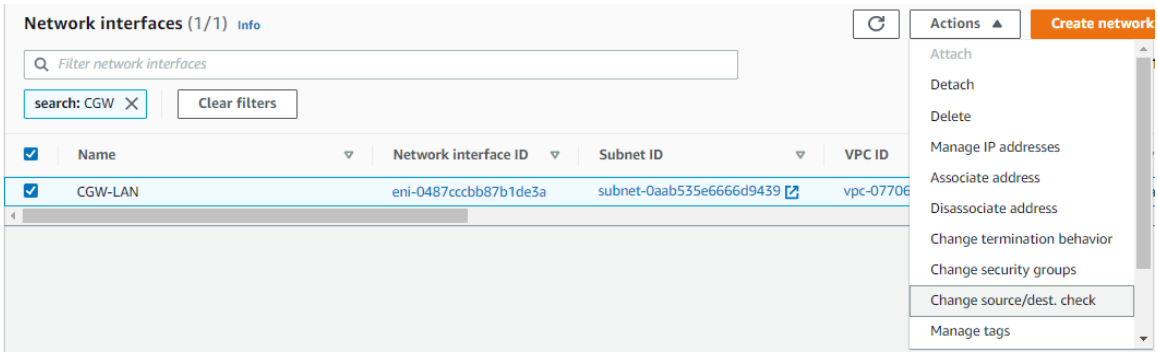
Scroll down and check for existing outbound rules. If all the traffic not allowed then modify outbound rules as mentioned below:



Source / Destination Check

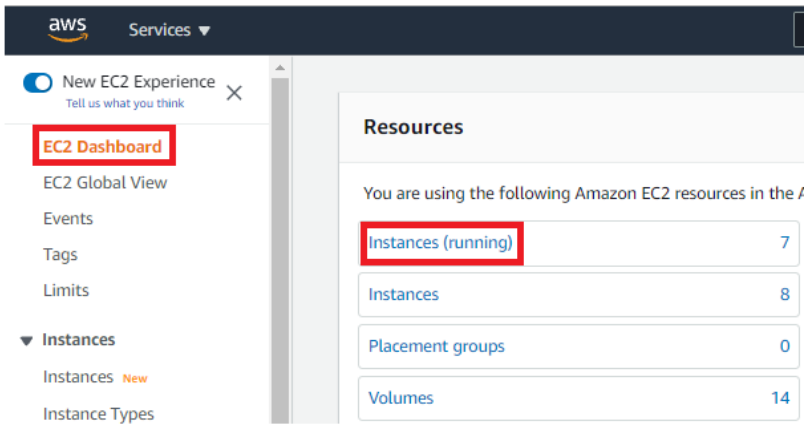
Disable Source / Destination check on LAN interface attached to CGW VM.
Select “Network Interfaces” from left panel on EC2 portal:

In search bar, write interface name which was created in earlier step and select it.
Click on “Actions” button on top right corner.
Click on “Change source/dest. check”. Disable it if found enabled.

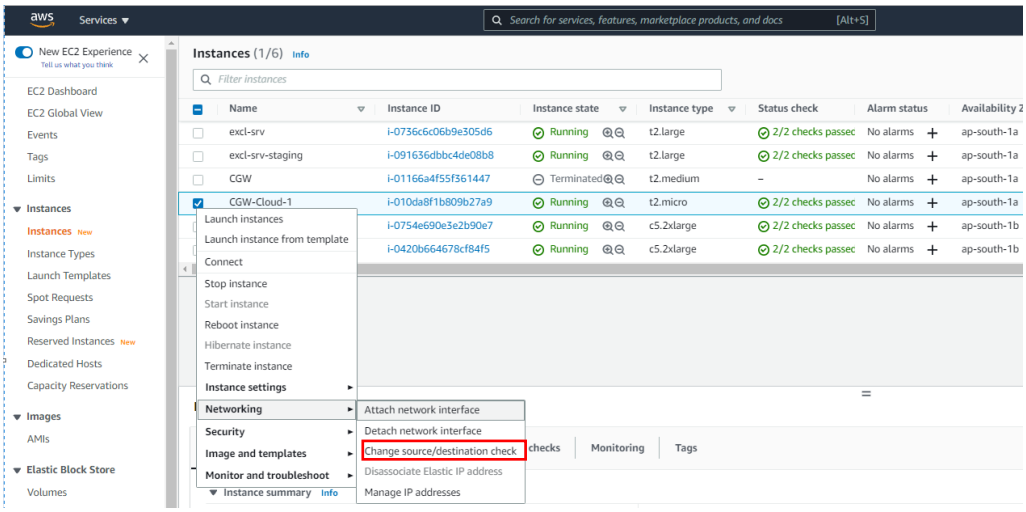


3.7.6.5 Disable Source / Destination Check

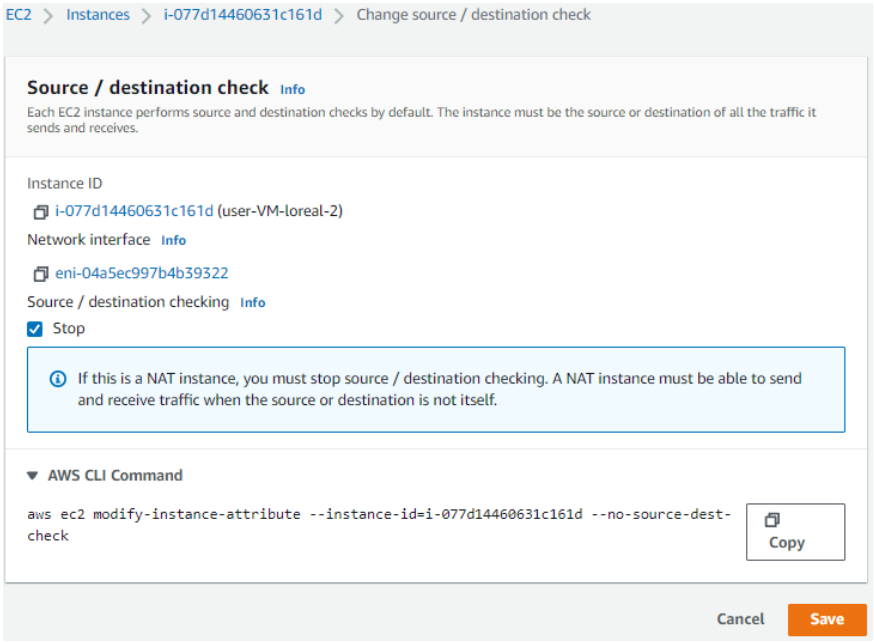
1) Access EC2 Dashboard and click on “Instances (running)”



2) Right click on CGW VM and in Networking option select “Change source/destination check”:



3) Disable source/destination check by selecting stop option on the configuration page. Click on Save.



Navigate to Section 3.11, to setup CGW.

3.8 CGW ON BARE METAL

3.8.1.1 Pre-requisites

1. Internet connectivity from WAN interface
2. Private network connectivity from LAN interface. If there is only one interface, then WAN and LAN connectivity from same interface will be required.
3. Sudoer access on the machine

3.8.1.2 Steps to install

Pre-requisite validation script can be downloaded to check if machine is ready for CGW installation. It shows missing commands and packages required for CGW along with the sysctl parameters which are required to tune CGW performance. User must proceed with choice "yes" to continue CGW installation and tuning.

To install Cyber Gateway on Ubuntu bare metal, follow below steps:

User must be part of sudoer group on Ubuntu machine.

1. Login to machine and confirm internet is accessible. Ping "google.com" to confirm DNS resolution is working.
2. Download script to check and install pre-requisites:

```
# wget https://clientreleases.s3.us-west-1.amazonaws.com/cgw/xpre-req.sh
```

3. Provide executable permissions to script:

```
# chmod +x xpre-req.sh
```

4. Execute pre-requisite script:

```
# sudo ./xpre-req.sh -i
```

   Note: After successful validation and installation of pre-requisites, further instructions will be displayed on the console.

5. Make apt entry for Exium cloud repository:

```
# sudo echo 'deb [trusted=yes] http://debrepo.exium.net/repos/exium-lgw/debian/amd64 /' > /etc/apt/sources.list.d/exium.list
```

6. Update the machine's package lists with latest repository addition

```
# sudo apt-get update
```

7. Check latest available versions of CGW:

```
# sudo apt-cache policy exium-lgw
```

8. Install CGW software:

```
# sudo apt-get install exium-lgw
```

Navigate to Section 3.11, to setup CGW.

3.8.1.3 Steps to Uninstall

CGW software can be uninstalled by following below steps:

1. Execute below command to uninstall CGW application:

```
# sudo apt-get remove --purge exium-lgw
```

2. Navigate to the path where the pre-requisite script is present.
3. Uninstall the additional packages and tuning parameters set for CGW:

```
# sudo ./xpre-req.sh -u
```

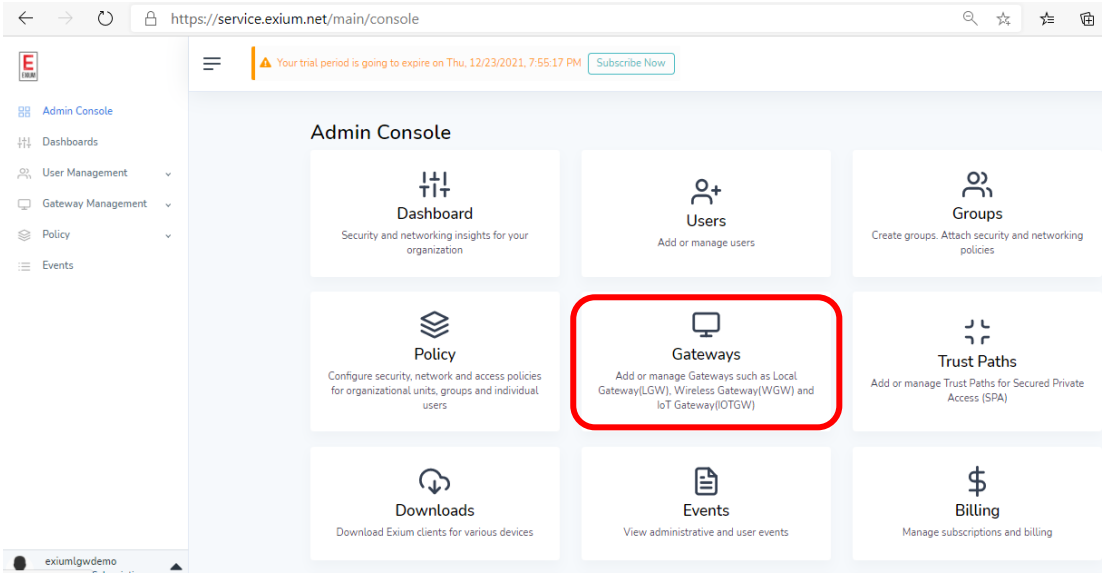
3.8.1.4 Steps to Rollback Tuning Parameters

CGW tuning parameters are additional configuration changes required to achieve better performance. They will be setup before CGW installation as a pre-requisite. It is not recommended to modify those if CGW is installed on the machine.
In case sysctl parameters rollback is indeed required, below command can be used:

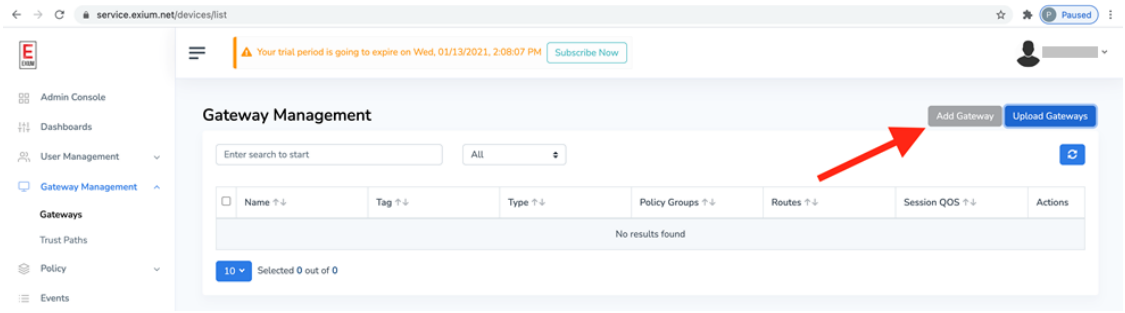
```
# sudo ./xpre-req.sh -r
```

3.9 ADD GATEWAY

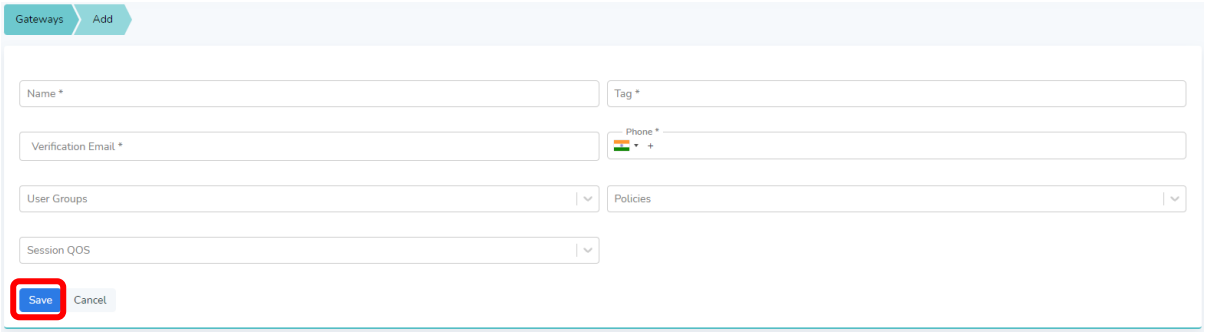
If user is already logged in on Exium portal, then access “Admin Console” from left panel of web page and click on “Gateways” tab. Otherwise, follow instructions mentioned in section (3.3) to access “Admin Console” on Exium portal and click on “Gateways” tab.



On Gateway Management page, click on “Add Gateway”.

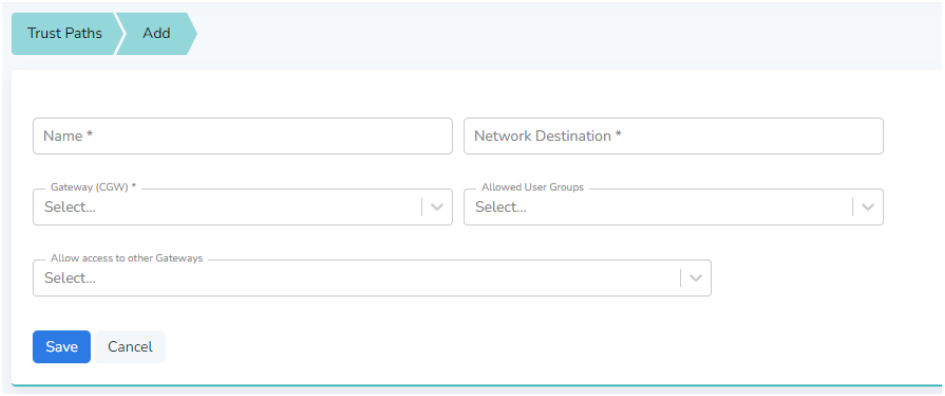


Proceed to enter all the details like Name (mandatory), Email & mobile number (auto filled), Tag (editable) and Session QoS. Click “Save” once finished.



3.10 ADD TRUST PATH

Once Gateway is added successfully, Trust Path Management page will open. Fill the mandatory fields, “Name” and “Network Destination” (LAN Subnet to allow).



Trust path is the private network subnet which will be allowed for remote users to access.
Users can add and associate multiple trust paths to CGW.

Refer Below example, which explains trust paths.

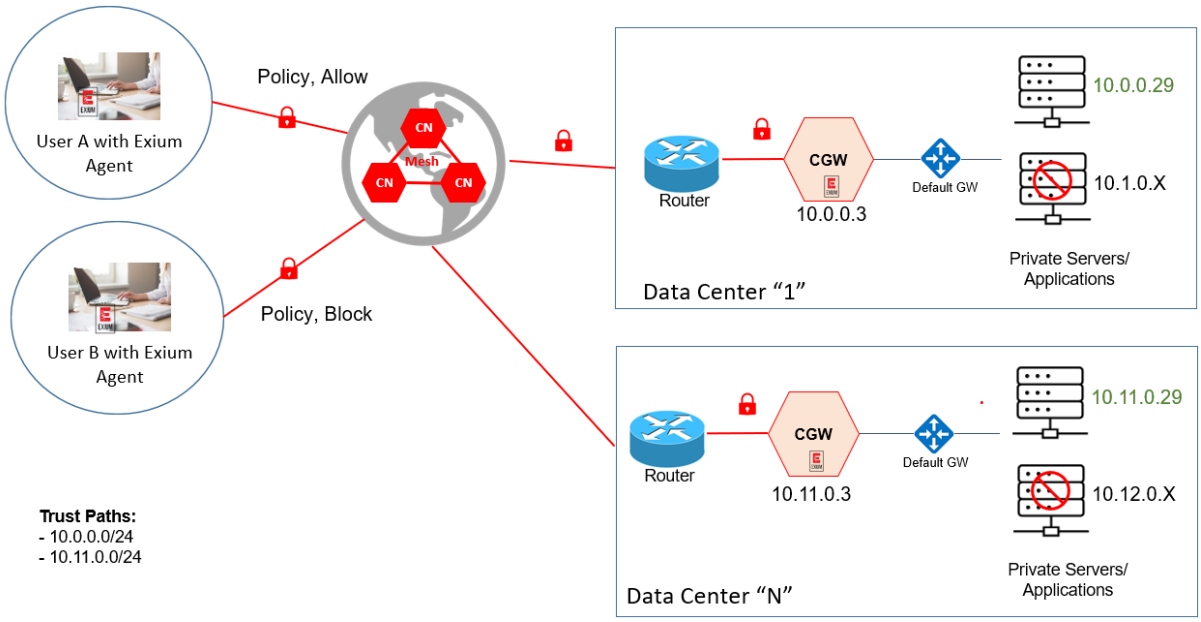
Data Center-1:

- CGW-1:
  - Trust Path: 10.0.0.0/24

Data Center-N:

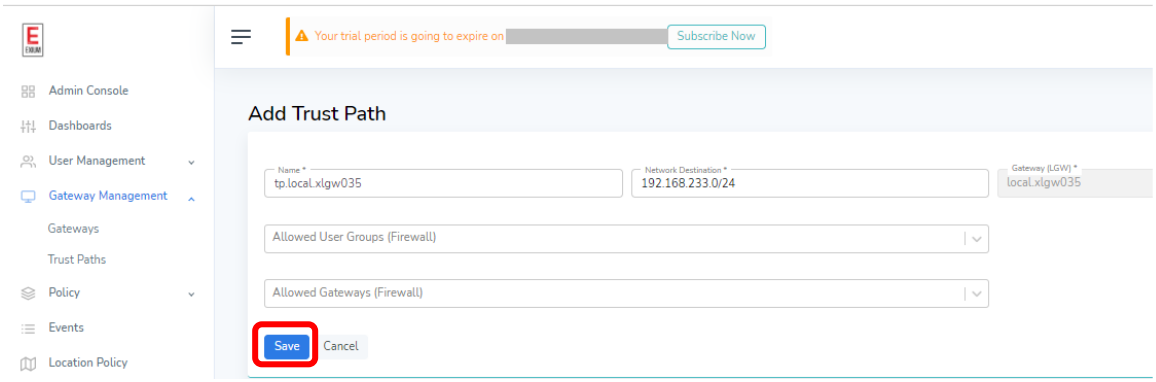
- CGW-2:
  - Trust Path: 10.11.0.0/24

Remote users will be allowed to access the private networks 10.0.0.0/24 and 10.11.0.0/24 at the same time. They will not be able to access the private networks 10.1.0.X or 10.12.0.X which are also available in Data Centers behind CGW.

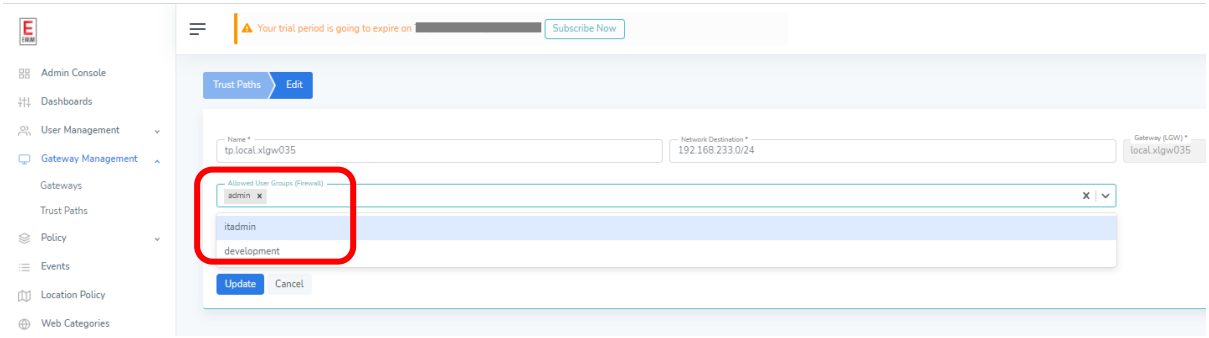


3.10.1 Associate User Group with Trust Path

Create new user group if different set of users require Private Mesh or Secure Private Access. Or identify the group name from existing user groups and select them from drop down list available in option "Allowed User Groups (Firewall)". Admin can also update "Allowed User Groups (Firewall)" setting in existing Trust Path later. Below picture shows an example of trust path, Name will show the trust path user has created.
Click on "Save" once finished.
Sample configuration page where Admin did not select the user group:



Sample configuration page where Admin is selected "admin" user group from drop down list: (Click on Update once finished.)


Your trial period is going to expire on
Subscribe Now
Admin Console
Dashboards
User Management
Gateway Management
Gateways
Trust Paths
Policy
Events
Location Policy
Web Categories
Trust Paths
Edit
tp.local.xlgw035
192.168.233.0/24
local.xlgw035
admin
itadmin
development
Update
Cancel

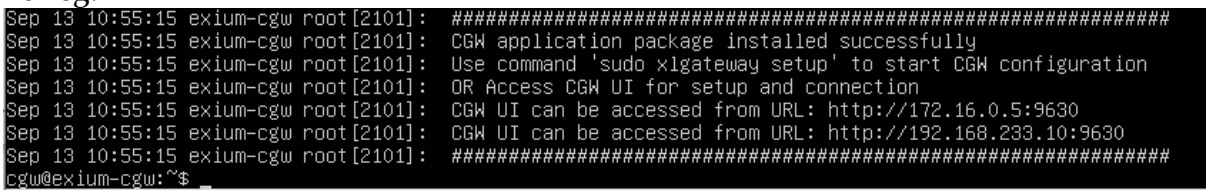
3.11 SETUP CGW

There are two ways user can complete CGW setup procedure:

- CGW Web UI (User Interface)
- CGW VM Console (Command Line Interface / CLI)

3.11.1 CGW Setup using Web UI

Once CGW installation completes, it will show the URLs to access CGW UI.
For eg:



If single interface is present on VM, then one URL link will be displayed in above output.

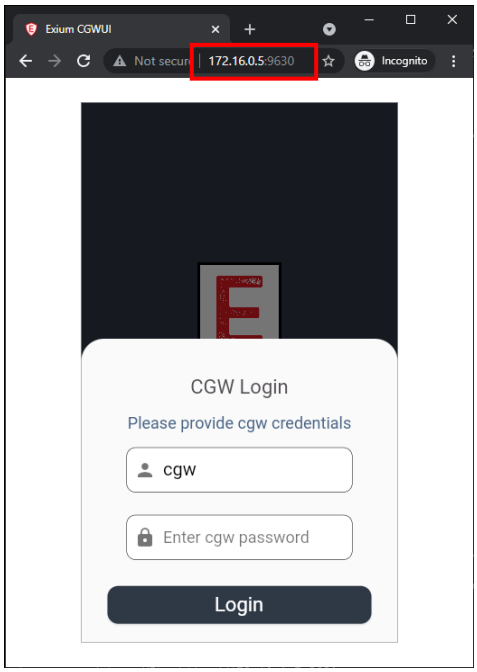
3.11.1.1 CGW Web UI Access

Select the machine/laptop which is accessible from CGW VM/machine. Open internet browser (recommended: chrome) on laptop and type one of the URL shown on terminal (http://172.16.0.5:9630).

Use the same password (for cgw username) which was set during CGW VM on-boarding.

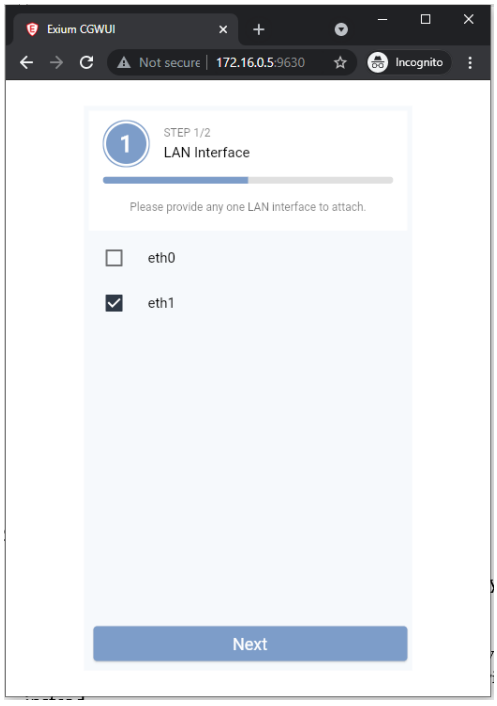
To get the UI access details again, login to CGW VM and run bootstrap script again:

```
# sudo /home/cgw/xbootstrap.sh
```

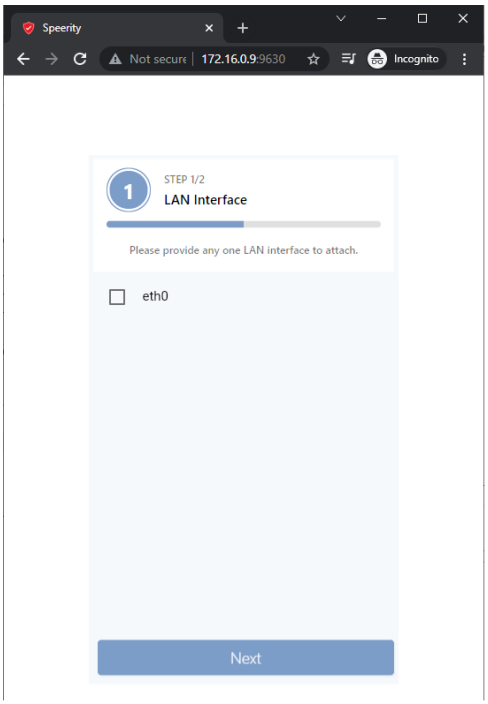


3.11.1.2 LAN Interface Selection

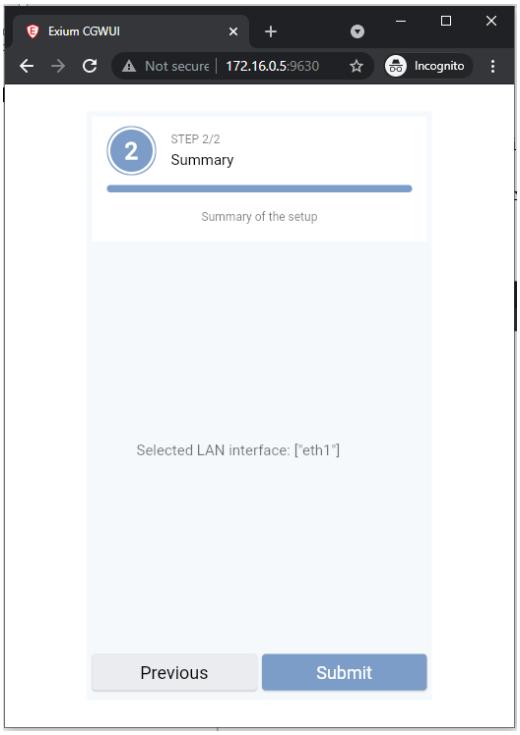
After successful login, new screen will appear with the interface names present on CGW VM.
Select one of the interfaces from list which provides access to data center or private network (LAN).
Click on the checkbox and “Next”.



Single interface entry will be displayed if CGW is deployed with single interface. Refer below example:

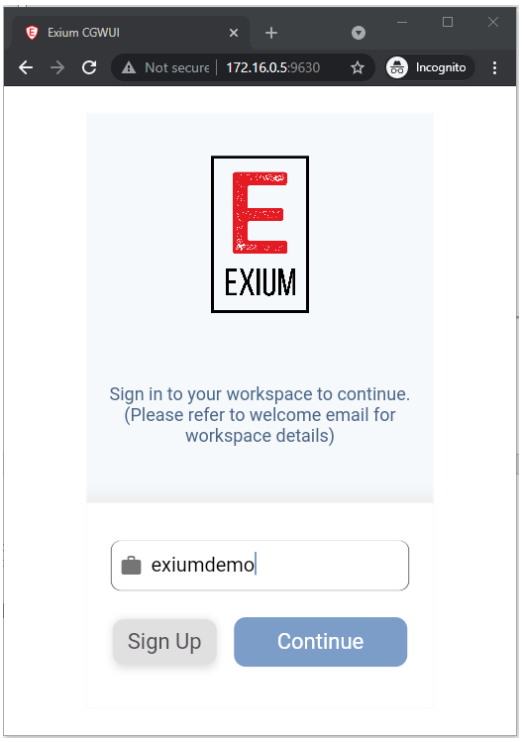


On summary page, verify selected LAN interface and click on “Submit” button.

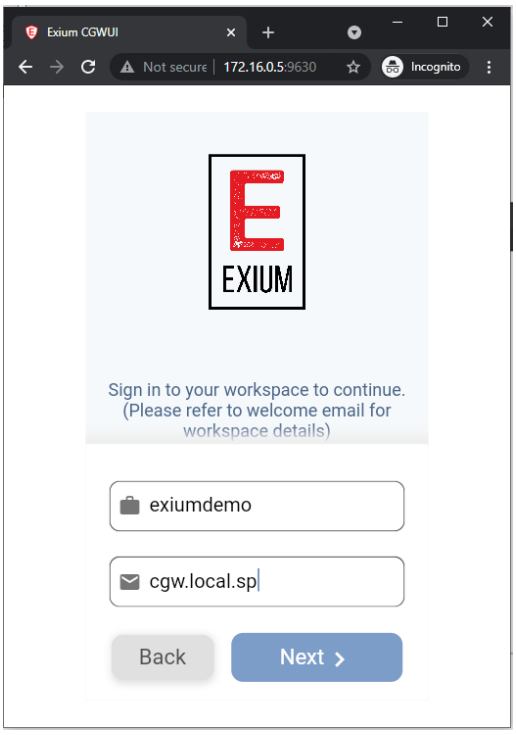


3.11.1.3 CGW Login

After successful setup, login screen will appear.
Provide workspace name and click on “Continue”:



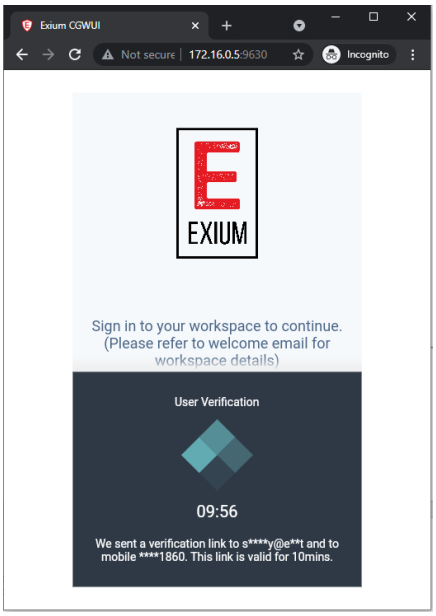
Provide username/gateway name and click on “Next”:

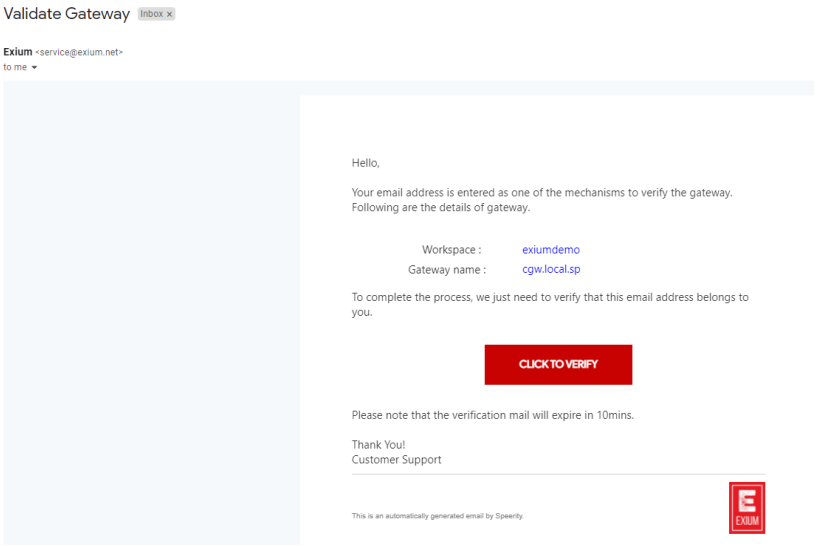


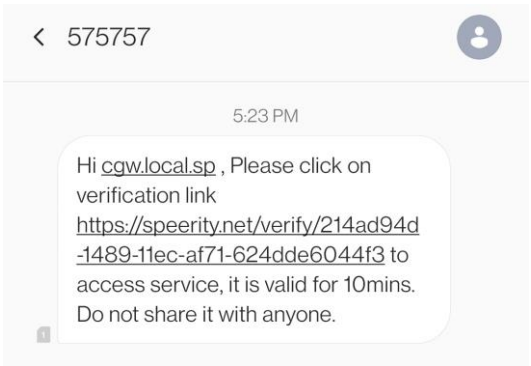
3.11.1.4 CGW Login Verification

A verification link will be sent to the registered email ID and an SMS will be sent to the registered mobile number.

User can click on the link (either from SMS or email) to complete the verification procedure.



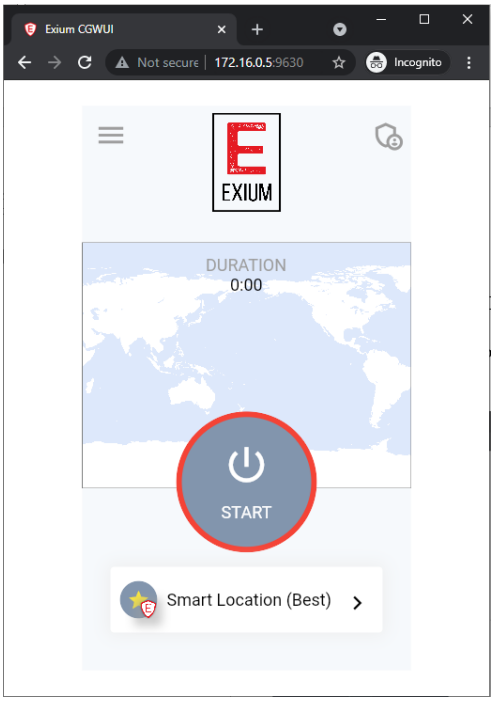




3.11.1.5 CGW Home Screen

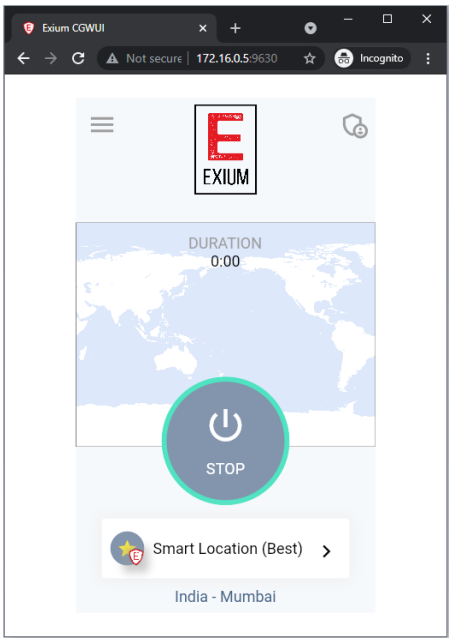
After successful verification, home screen will appear.

Click on “Start” to connect the service.



3.11.1.6 CGW Service Connection

Once the service is connected, it will show “Stop” button.
Now users can use Secure Private Access feature and login from their remote Exium Clients to access private network/servers.



3.11.2 CGW Setup using CLI

Users can choose to complete login and connection procedures during setup, or login and connection can be done later are per requirement.

During setup procedure, user will be required to provide below inputs:

- WAN & LAN interface names (in case CGW is deployed with 2 separate interfaces)
- Workspace name
- Gateway name

Verification email will be sent to registered email during login procedure. Please click on verification link to complete login process.

Note: If internet is not accessible from the WAN interface provided, setup will exit with warning. User will need to check the routing for internet connection to retry setup again.

Example:

- CGW setup with two separate interfaces for WAN and LAN
- User does not choose login and connection during setup
- Later user can use “sudo xlgateway login” to login and connect service

```
$  sudo xlgateway setup
   ###########################################################
   Starting CGW installation...
   ###########################################################
   Validate Internet Connection : [OK]
   Check for user requirements...
   Notification: Multicast support disabled on CGW
   Notification: NAT support enabled on CGW
   Reloading services and daemons : [OK]
   Available interfaces: ['eth0', 'eth1']
   Provide LAN interface to attach: eth1
   Provide WAN interface to attach: eth0
   Validate WAN connectivity from WAN interface [eth0] : [OK]
   LAN interface [eth0] attached successfully with CGW
   Logout from current account
   Notification: Not logged in
   Login and connect the cyber gateway now [y/n]?: n
   CGW login incomplete...
   Use 'sudo xlgateway login' to login, verify the account and connect service
   ***********************************************************
   Use 'sudo xlgateway help' to get list of supported commands
   ***********************************************************
```

Example:

- CGW setup with single interface for WAN and LAN
- User chooses login and connection during setup

```
$  sudo xlgateway setup
   ########################################################
   Starting CGW installation...
   ########################################################
   Validate Internet Connection : [OK]
   Check for user requirements...
   Notification: Multicast support disabled on CGW
   Notification: NAT support enabled on CGW
   Reloading services and daemons : [OK]
   Available interfaces: ['eth0']
   Setting LAN and WAN on same interface [eth0]
   Validate WAN connectivity from WAN interface [eth0] : [OK]
   LAN interface [eth0] attached successfully with CGW
   Logout from current account
   Notification: Not logged in
   Login and connect the cyber gateway now [y/n]?: y
   ************************************************
   Provide inputs to login...
   Workspace: eiumdemo
   Gateway Name: cgw.local.sp
   Checking Credentials--------> Done
   Notification: Please check your email
   Notification: We sent a verification link to s****y@e**t and to mobile ****1860.
   This link is valid for 10mins.
   Verifying User--------> Verified
   Creating User Certificates--------> Success
   ********************************************************
   Service connection is in progress...
   Connection In Progress--------------> SessionConnected
   Exium CGW connected successfully
   ******************* Dashboard ******************
            Username:  cgw.local.sp@exiumdemo
             Version:  v0.5.6
    Server Connected:  India - Mumbai
   Connection Status:  Active
     Connected Since:  Wed 2021-10-13 13:11:33 UTC; 1 sec ago
                Date:  Wed 2021-10-13 13:11:33 UTC
          WebUI URL:  http://172.16.0.7:9630
   ************************************************
```

Example:

- CGW setup with two separate interfaces for WAN and LAN
- User chooses login and connection during setup

```
$  sudo xlgateway setup
   ########################################################
   Starting CGW installation...
   ########################################################
   Validate Internet Connection : [OK]
   Check for user requirements...
```

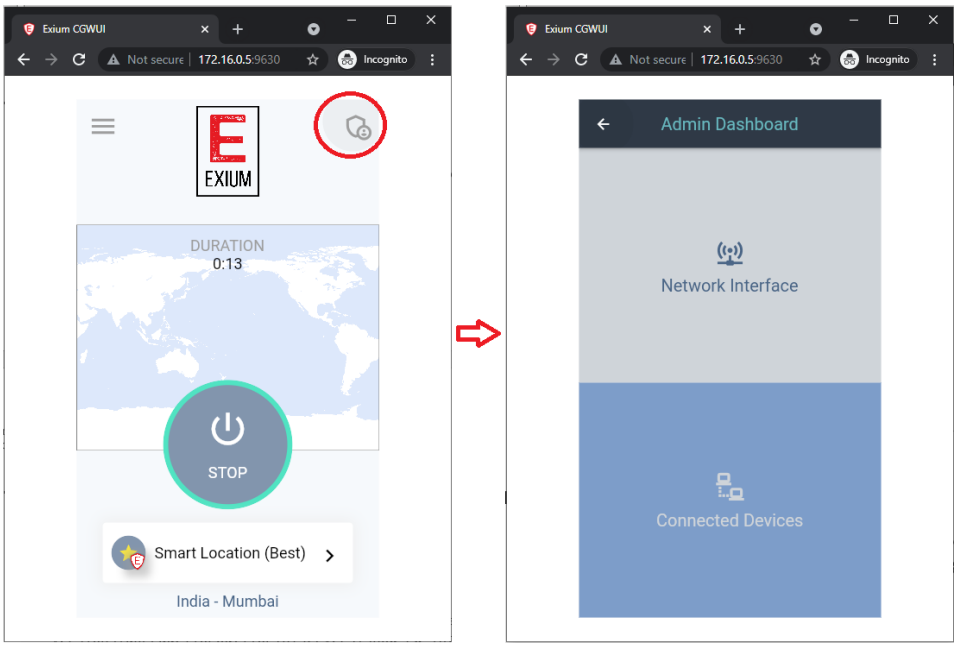
```
Notification: Multicast support disabled on CGW
Notification: NAT support enabled on CGW
Reloading services and daemons : [OK]
Available interfaces: ['eth0', 'eth1']
Provide LAN interface to attach: eth1
Provide WAN interface to attach: eth0
Validate WAN connectivity from WAN interface [eth0] : [OK]
LAN interface [eth0] attached successfully with CGW
Logout from current account
Notification: Not logged in
Login and connect the cyber gateway now [y/n]?: y
************************************************
Provide inputs to login...
Workspace: eximdemo
Gateway Name: cgw.local.sp
Checking Credentials--------> Done
Notification: Please check your email
Notification: We sent a verification link to s****y@e**t and to mobile ****1860.
This link is valid for 10mins.
Verifying User-------> Verified
Verifying User Certificates-----> Success
************************************************************
Service connection is in progress...
Connection In Progress--------------> SessionConnected
Exium CGW connected successfully
****************** Dashboard ******************
         Username:  cgw.local.sp@eximdemo
          Version:  v0.5.6
 Server Connected:  India - Mumbai
Connection Status:  Active
  Connected Since:  Wed 2021-10-13 13:11:33 UTC; 1 sec ago
             Date:  Wed 2021-10-13 13:11:33 UTC
       WebUI URL:  http://172.16.0.7:9630
************************************************
```

Note: By default, NAT on CGW LAN interface is enabled and Multicast is disabled.
Navigate to Section 3.11.2 to connect CGW service.

3.12 CGW UI FEATURES

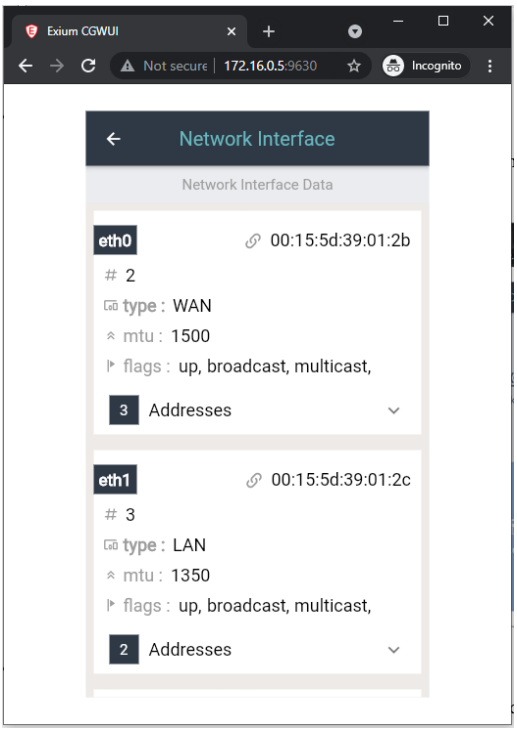
3.12.1 CGW Admin Dashboard

On CGW UI screen, click on the admin icon on top right corner.
It will open Admin Dashboard.



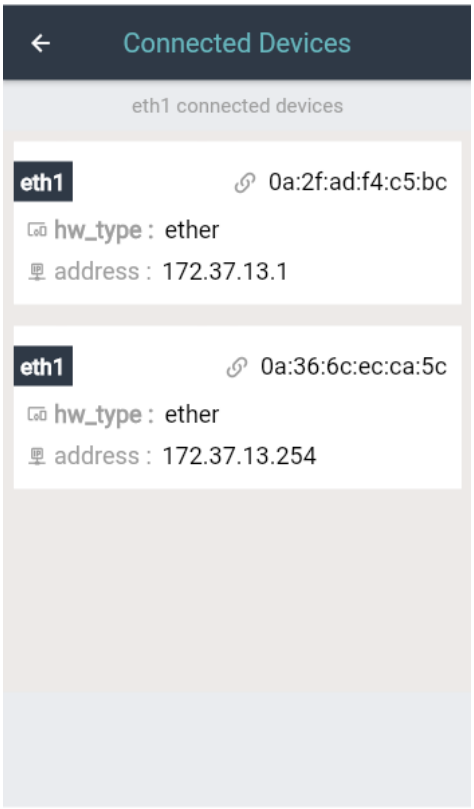
3.12.2 Display CGW Network Interfaces

On Admin Dashboard, click on “Network Interface” to display CGW interfaces: It will show “WAN”, “LAN”, “tuno”, “par-gre” and other interfaces available on CGW.



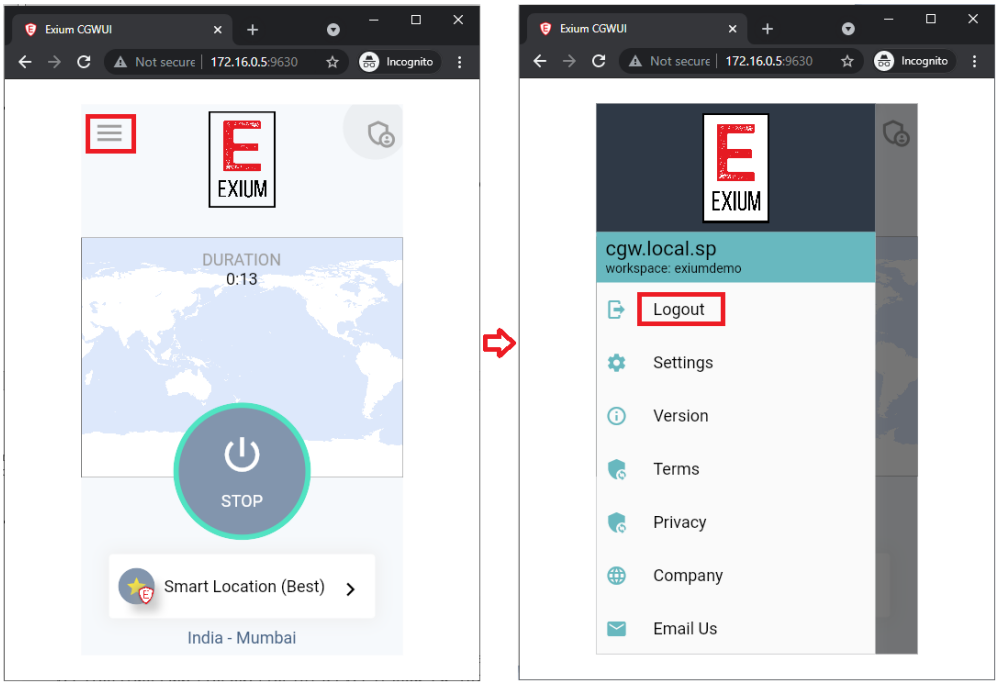
3.12.3 Display Connected Devices

On Admin Dashboard, click on “Connected Devices” to display the devices connected to CGW on LAN interface:



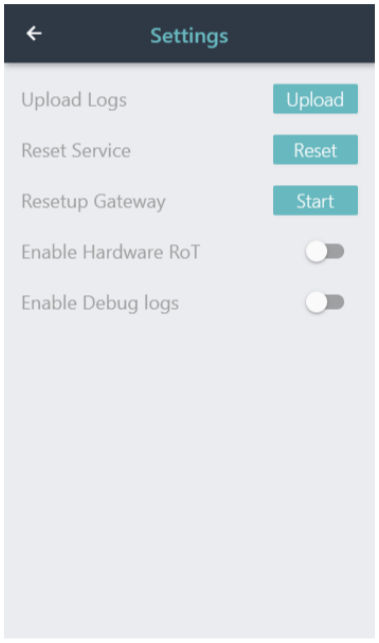
3.12.4 Logout

On CGW UI Home screen, click on three lines available on top left corner to show available options:
Click on “Logout” button to logout from CGW:



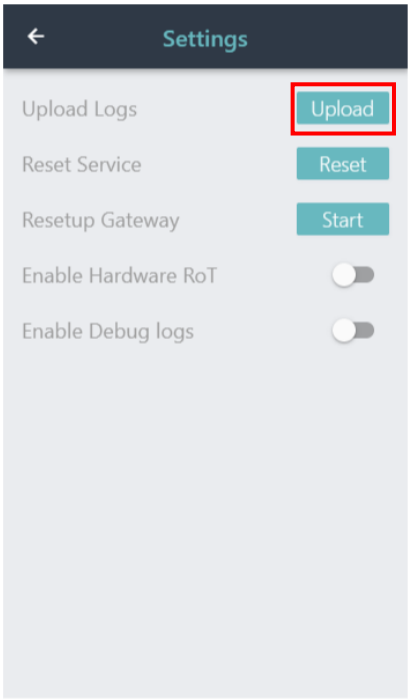
3.12.5 CGW Settings

On CGW UI Home screen, click on three lines available on top left corner to show available options.
Click on “Settings” to display available settings/parameters:



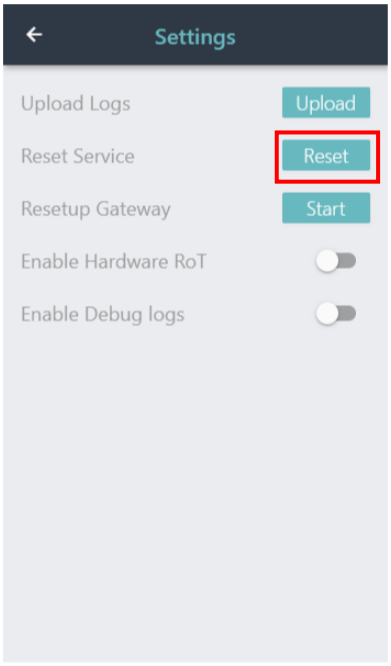
3.12.6 Upload Logs

On CGW UI Home screen, click on three lines available on top left corner to show available options.
Click on “Settings” to get access to button to upload logs.
Click on “Upload” button. After uploading logs, successful message will be displayed.



3.12.7 Service Reset

On CGW UI Home screen, click on three lines available on top left corner to show available options.
Click on “Settings” to get access to button to reset service.
Service Reset is recommended when CGW service or UI is not working properly.



3.13 CGW CLI COMMANDS

CGW command line interface supports below commands for service operations.

3.13.1 CGW Commands Help

Display supported commands:

```
$  sudo xlgateway
   usage:
       xlgateway {setup|servers|connect|disconnect|status|login|logout|show-gw-
   interface|attach-gw-interface|change-lan-interface|enable-multicast|disable-
   multicast|show-multicast-config|enable-nat|disable-nat|recover|available-
   versions|upload-log|show-upload-log-config|enable-auto-upload-log|disable-
   auto-upload-log|set-upload-log-duration|upgrade|show-auto-upgrade-
   config|enable-auto-upgrade|disable-auto-upgrade|set-auto-upgrade-
   duration|reset|version|set-static-cyber-node|unset-static-cyber-node|show-
   static-cyber-node|speedtest|set-lan-next-hop|unset-lan-next-hop|show-lan-
   next-hop|setup-ha|unset-ha|enable-cgw-bypass|disable-cgw-bypass}

   Command description:
```

```
      setup                       : Do CGW setup, login and verification
      servers                     : Get Exium Cyber Nodes List
      connect                     : Connect CGW to Smart Location
      connect <cyber-node>        : Connect CGW to provided Cyber Node
      disconnect                  : Disconnect CGW
      status                      : Check CGW connection status
      login                       : Login to CGW service
      logout                      : Logout from CGW service
      show-gw-interface           : Show attached LAN interface
      attach-gw-interface         : Attach interfaces to CGW
      change-lan-interface        : Change attached LAN interface
      enable-multicast            : Enable Multicast
      disable-multicast           : Disable Multicast
      show-multicast-config       : Show Multicast Configuration
      enable-nat                  : Enable NAT on LAN interface
      disable-nat                 : Disable NAT on LAN interface
      recover                     : Recover CGW service
      available-versions          : Show latest available versions
      upload-log                  : Upload logs for debugging
      show-upload-log-config      : Show log upload config
      enable-auto-upload-log      : Enable auto upload log
      disable-auto-upload-log     : Disable auto upload log
      set-upload-log-duration     : Set duration to auto upload log in seconds
      upgrade                     : Upgrade CGW application manually
      show-auto-upgrade-config    : Show auto upgrade config
      enable-auto-upgrade         : Enable auto upgrade of CGW
      disable-auto-upgrade        : Disable auto upgrade of CGW
      set-auto-upgrade-duration   : Set duration to auto upgrade CGW in seconds
      reset                       : Reset CGW service
      version                     : Show CGW version
      set-static-cyber-node       : Select a Cyber Node to connect always
      unset-static-cyber-node     : Disable Static Cyber Node
      show-static-cyber-node      : Show Static Cyber Node Config
      speedtest                   : Show speedtest results
      set-lan-next-hop            : Configure single next-hop on LAN
      unset-lan-next-hop          : Remove single next-hop on LAN
      show-lan-next-hop           : Show configured LAN next hop
      setup-ha                    : Setup High Availability
      unset-ha                    : Remove High Availability configuration/setup
      enable-cgw-bypass           : Enable traffic to bypass CGW tunnel
      disable-cgw-bypass          : Disable traffic to bypass CGW tunnel
```

3.13.2 Service Connect

Use below command to connect CGW service.

```
$ sudo xlgateway connect
  Service connection is in progress...
  Connection In Progress--------------> SessionConnected
  CGW connected successfully
  ****************** Dashboard ******************
           Username:  cgw.local.sp@eximdemo
            Version:  v0.6.3
   Server Connected:  Mumbai, India
  Connection Status:  Active
    Connected Since:  Tue 2021-11-09 07:34:36 UTC; 1 sec ago
               Date:  Tue 2021-11-09 07:34:37 UTC
```

```
         WebUI URL:  http://172.16.0.5:9630
**********************************************
```

User can also connect to a specific server by selecting it from the list. Use command “sudo xlgateway servers” to get the list of the Cyber Nodes and pass it with connect command:

```
$  sudo xlgateway connect exe21mum.exium.net
   Service connection is in progress...
   Connection In Progress--------------> SessionConnected
   CGW connected successfully
   ****************** Dashboard ******************
            Username:  cgw.local.sp@eximdemo
             Version:  v0.6.3
    Server Connected:  Mumbai, India
   Connection Status:  Active
     Connected Since:  Tue 2021-11-09 07:34:36 UTC; 1 sec ago
                Date:  Tue 2021-11-09 07:34:37 UTC
           WebUI URL:  http://172.16.0.5:9630
   **********************************************
```

3.13.3 Service Disconnect

Use below command in case user wants to disconnect service:

```
$  sudo xlgateway disconnect
   Service disconnection is in progress...
   CGW disconnected successfully
```

3.13.4 Service Status

Use below command to check Exium CGW connection status:

```
$  sudo xlgateway status
   ****************** Dashboard ******************
            Username:  cgw.local.sp@eximdemo
             Version:  v0.6.3
    Server Connected:  Mumbai, India
   Connection Status:  Active
     Connected Since:  Tue 2021-11-09 07:34:36 UTC; 1 mins ago
                Date:  Tue 2021-11-09 07:36:09 UTC
           WebUI URL:  http://172.16.0.5:9630
   **********************************************
           CGW State: Connected
   Multicast Support: Disabled
         NAT Support: Enabled
        Auto upgrade: Disabled
      LAN Interfaces: eth1
      WAN Interfaces: eth0
   **********************************************
```

WAN and LAN interface names will be same in above output if CGW is deployed with single interface.

3.13.5 Multicast Support Enable/Disable

Use below commands to enable or disable Multicast support on CGW.

- By default, Multicast support is disabled.
- Below example shows commands to enable Multicast support on CGW:
  - To enable, provide input 'y' else 'n' to disable
  - Provide LAN interface name
  - Provide subnets which will originate Multicast streaming
    - Multiple entries can be configured

```
$ sudo xlgateway enable-multicast
  Configure Multicast parameters...
  Provide inputs to configure Multicast support...
  Multicast traffic originator or source subnet(format: 10.101.0.0/16):
  10.101.0.0/16
  ['10.101.0.0/16']
  Do you want to configure another Multicast traffic originator subnet:(y/n) y
  Multicast traffic originator or source subnet(format: 10.101.0.0/16):
  10.102.0.0/16
  ['10.101.0.0/16', '10.102.0.0/16']
  Do you want to configure another Multicast traffic originator subnet:(y/n) n
  Multicast configuration completed successfully
  Reloading services and daemons...

$ sudo xlgateway disable-multicast
  Notification: Multicast support disabled on CGW
  Reloading services and daemons...
```

Note: CGW will disconnect and reconnect automatically after enabling Multicast support.

3.13.6 Cyber Node List

Use below command to get the list of all the Exium Cyber nodes available to connect: [It is recommended to use "Smart Location" in case there is no specific requirement to use other Cyber Node]

```
$ sudo xlgateway servers
  Name                              Address
  Smart Location(SPA)               exe.exium.net
  Ohio, USA                         exe15oho.exium.net
  Virginia, USA                     exe16va.exium.net
  California, USA                   exe18ca.exium.net
  Mumbai, India                     exe21mum.exium.net
  Dallas, TX (EQ)                   exe51eqtx.exium.net
  Dallas, TX (IBM Lab-2)            170.226.21.114
```

3.13.7 Change of Cyber Node

Use below command to connect to specific Exium Cyber Node:

```
$  sudo xlgateway connect exe15oho.exium.net
   ****************** Dashboard ******************
            Username:  cgw.local.sp@exiumdemo.exium.net
             Version:  v0.5.5
    Server Connected:  US East - Ohio
   Connection Status:  Active
     Connected Since:  Mon 2021-10-11 12:17:31 UTC; 42 sec ago
                Date:  Mon 2021-10-11 12:17:12 UTC
          WebUI URL:  http://172.16.0.5:9630
   ***********************************************
   CGW State : Connected
```

3.13.8 Logout

Use below command to logout:

```
$  sudo xlgateway logout
   User logged out successfully
```

3.13.9 Login

Use below command to login:

```
$  sudo xlgateway login
   Provide inputs to login...
   Workspace: exiumdemo
   Gateway Name: cgw.local.sp
   Checking Credentials-------> Done
   Notification: Please check your email
   Notification: We sent a verification link to s****y@e**t and to mobile ****1860.
   This link is valid for 10mins.
   Verifying User--------> Verified
   Verifying User Certificates-----> Success
   ******************************************************
   Service connection is in progress...
   Connection In Progress-------------> SessionConnected
   Exium CGW connected successfully
   ****************** Dashboard ******************
            Username:  cgw.local.sp@exiumdemo
             Version:  v0.5.6
    Server Connected:  India - Mumbai
   Connection Status:  Active
     Connected Since:  Wed 2021-10-13 13:21:06 UTC; 1 sec ago
                Date:  Wed 2021-10-13 13:21:07 UTC
          WebUI URL:  http://172.16.0.7:9630
   ***********************************************
```

3.13.10 Show Attached LAN Interface

Use below command to check current attached LAN interface:

```
$  sudo xlgateway show-gw-interface
   Attached Interfaces: [eth1]
```

3.13.11 Change of LAN Interface

User can check current interface attached to CGW and decide to change LAN interface.
Press “y” when asked to disconnect service.
Provide LAN interface when prompted:

```
$  sudo xlgateway show-gw-interface
   Attached Interfaces: [eth1]

$  sudo xlgateway change-lan-interface
   Existing LAN interface attached: eth1
   Service will disconnect Do you want to change attached LAN interface [y/n]: y
   Detach interface eth1 which is attached to Exium CGW
   Detached interface eth1 successfully
   CGW is in connected state. Disconnecting, before attaching interface...
   Service disconnection is in progress...
   Exium CGW disconnected successfully
   Provide LAN interface to attach: eth1
   LAN interface attached successfully with Exium CGW
   Connecting service with new LAN interface changes...
   Service connection is in progress...
   Connection In Progress------------> SessionConnected
   Exium CGW connected successfully
   ******************** Dashboard ********************
            Username:  cgw.local.sp@eximdemo.exium.net
             Version:  v0.5.5
    Server Connected:  India - Mumbai
   Connection Status:  Active
     Connected Since:  Mon 2021-10-11 12:17:31 UTC; 42 sec ago
                Date:  Mon 2021-10-11 12:17:12 UTC
             UI Link:  http://172.16.0.5:9630
   ************************************************
```

3.13.12 Show Multicast Configuration

If Multicast is enabled, use below command to show Multicast related configuration:

```
$  sudo xlgateway show-multicast-config
   ********************************************************
      Multicast Support: Enabled
     Upstream Interface: eth1
       Upstream Subnets:
                   10.102.0.0/16
                   10.101.0.0/16
   Downstream Interface: par-gre
     Downstream Subnets:
                   100.121.0.0/16
   ********************************************************
```

3.13.13 Upload Logs

Use below command to upload logs for debugging:

```
$  sudo xlgateway upload-log
   Uploading Logs--> Done
```

3.13.14 Show Latest Available CGW Versions

Use below command to upload logs for debugging:

```
$  sudo xlgateway available-versions
   exium-lgw:
     Installed: 0.4.9
     Candidate: 0.4.9
     Version table:
    *** 0.4.9 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
           100 /var/lib/dpkg/status
        0.4.8 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
        0.4.7 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
        0.4.6 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
        0.4.5 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
        0.4.4 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
        0.4.3 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
        0.4.2 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
        0.4.1 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
        0.4.0 500
           500 http://13.127.249.55:8080/repos/exium-lgw/debian/amd64  Packages
```

3.13.15 CGW Upgrade

Use below command to upgrade CGW:

```
$  sudo xlgateway upgrade
```

If latest version is already installed, then command will exit after displaying information on screen.

3.13.16 CGW Auto Upgrade Enable/Disable

Use below command to enable/disable auto upgrade of CGW:

```
$  sudo xlgateway enable-auto-upgrade
   ******************************************************
   Updating setting--> Done

$  sudo xlgateway disable-auto-upgrade
   ******************************************************
```

```
   Updating setting--> Done
```

3.13.17 Show Auto Upgrade Configuration Settings

Use below command to show CGW auto upgrade configuration settings:

```
$  sudo xlgateway show-auto-upgrade-config
   ********************************************************
   upgrade_config =>
           next_trigger = Wed 2021-11-10 06:51:24 UTC
           running = true
           auto = false
           candidate = 0.6.3
           duration = 86400
           installed = 0.6.3
           last_trigger =
   ********************************************************
```

3.13.18 Set Auto Upgrade Duration

Use below command to set duration for auto upgrade:

```
$  sudo xlgateway set-auto-upgrade-duration 3600
   ********************************************************
   Updating setting--> Done
   ********************************************************
```

Note:
- Duration is in seconds
- By default, duration is set to 24 Hours

3.13.19 Auto Log Upload Enable/Disable

Use below command to enable/disable auto log upload from CGW:

```
$  sudo xlgateway enable-auto-upload-log
   ********************************************************
   Updating setting--> Done
   ********************************************************

$  sudo xlgateway disable-auto-upload-log
   ********************************************************
   Updating setting--> Done
   ********************************************************
```

3.13.20 Show Auto Log Upload Configuration Settings

Use below command to show CGW auto log upload configuration settings:

```
$  sudo xlgateway show-upload-log-config
   ********************************************************
```

```
   log_rotation_config =>
           last_log_cleanup_time = 2021-10-18 12:32:09.308700632 +0000 UTC
           log_rotate_duration = 12h0m0s
           log_rotate_next_trigger = 1.049449555s
           log_rotate_size = 1.048576e+07
           last_log_rotate_time = 2021-10-18 12:52:01.327107645 +0000 UTC
   m=+840.093164647
           log_cleanup_active = true
           log_cleanup_next_trigger = 22h18m10.722340475s
           log_cleanup_older_than = 168h0m0s
           log_rotation_active = true
           max_num_files = 30
   log_upload_config =>
           next_trigger = Mon 2021-10-18 12:56:46 UTC
           running = true
           auto = true
           duration = 240
           last_trigger = Mon 2021-10-18 12:52:46 UTC
   last_log_file_creation_time = 2021-10-18T12:38:01.256276022Z
   log_cleanup_enabled = true
   log_dir = /var/log/exium
   log_file = /var/log/exium/exium.log
   log_level = error
   log_rotate_enabled = true
   ************************************************************
```

3.13.21 Set Auto log Upload Duration

Use below command to set duration for auto log upload:

```
$  sudo xlgateway set-upload-log-duration 3600
   ************************************************************
   Updating setting--> Done
   ************************************************************
```

Note:
- Duration is in seconds
- By default, duration is set to 24 Hours

3.13.22 Reset

Use below command to reset CGW.
Service be disconnected and automatically reconnect after some time.

```
$  sudo xlgateway reset
   ************************************************************
   Resetting CGW, service will reconnect incase already connected...
   Do you want to continue service reset? (y/n): y
   Disconnection In Progress----------------> Success
   Reset in Progress-------> Success
   Checking Service status-------> OK
   Notification: Service is UP and running
   ******************* Dashboard ******************
            Username:  cgw.local.sp@eximdemo
             Version:  v0.6.3
```

```
  Server Selected:  Smart Location
Connection Status:  Not Active
             Date:  Tue 2021-11-09 10:50:06 UTC
        WebUI URL:  http://172.16.0.5:9630
************************************************
        CGW State: Disconnected
Multicast Support: Disabled
      NAT Support: Enabled
     Auto upgrade: Disabled
   LAN Interfaces: eth1
   WAN Interfaces: eth0
************************************************
```

3.13.23 Version

Use below command to check CGW version:

```
$  sudo xlgateway version
   ********************************************************
   CGW Version: v0.6.3
   ********************************************************
```

3.13.24 Set Static Cyber Node

Use below command to set static cyber node for CGW to connect always.
It will show available Cyber Nodes which user can select. User will be prompted for option to disconnect. It will ask for reconnection to configured static cyber node if CGW is already in connected state.

```
$  sudo xlgateway set-static-cyber-node
   ============ Available Cyber Nodes ===============
   Name                                Address
   Smart Location(SPA)                 exe.exium.net
   Ohio, USA                           exe15oho.exium.net
   Virginia, USA                       exe16va.exium.net
   California, USA                     exe18ca.exium.net
   Mumbai, India                       exe21mum.exium.net
   Dallas, TX (EQ)                     exe51eqtx.exium.net
   Dallas, TX (IBM Lab-2)              170.226.21.114
   OCN - exiumdemo - ex-test           exe185exiumdemo.exium.net
   London, UK                          158.175.97.142
   Dallas, TX (Innovate5G)             206.126.56.58
   ================================================
   Provide Cyber Node Address: exe16va.exium.net
   SUCCESS: Static Cyber Node set to : exe16va.exium.net
   NOTICE: CGW connected to other Cyber Node.
   Service will disconnect and reconnect CGW to static Cyber Node?
   Do you want to continue? [y/n]: y
   CGW will be connected to static Cyber Node: exe16va.exium.net
   Service disconnection is in progress...
   CGW disconnected successfully
   Service connection is in progress...
   NOTICE: Static Cyber Node: exe16va.exium.net
   Config Update in progress--> ConfigUpdated
   Connection In Progress------------> SessionConnected
```

```
CGW connected successfully
******************** Dashboard ********************
         Username:  cgw.local.sp@exiumdemo
          Version:  v0.6.9
 Server Connected:  Virginia, USA
Connection Status:  Active
  Connected Since:  Wed 2021-12-08 14:29:30 UTC; 1 sec ago
             Date:  Wed 2021-12-08 14:29:30 UTC
        WebUI URL:  http://172.16.0.5:9630
***************************************************
```

Note: It is not recommended to set static cyber node if user does not have any specific reason. Once set, CGW will always try to connect to static cyber node which will not allow it to choose any other cyber node using Smart Location concept.

3.13.25 Unset Static Cyber Node

Use below command to unset static cyber node configured on CGW. If CGW is in connected state then notification will be prompted.

```
$  sudo xlgateway unset-static-cyber-node
   ********************************************************
   Notification: Static Cyber Node disabled
   NOTICE: CGW is in connected state. Reconnect CGW to select Cyber Node using
   Smart Location
   ********************************************************
```

3.13.26 Show Static Cyber Node

Use below command to show static cyber node configured on CGW. It will show “Not Configured” if static cyber node entry is not configured.

```
$  sudo xlgateway show-static-cyber-node
   ********************************************************
   Static Cyber Node: exe16va.exium.net
   ********************************************************
```

3.13.27 Set LAN Next Hop

Next hop configuration on LAN interface is required to avoid configuration of individual routes of different subnets on CGW VM.
For eg. –

- CGW LAN interface is on subnet 192.168.10.0/24 and default gateway is 192.168.10.1.
- Other private subnets are 192.168.11.0/24 and 192.168.12.0/24 which are accessible from gateway 192.168.10.1

- Trustpaths configured will be required for all three subnets 192.168.10.0/24, 192.168.11.0/24 and 192.168.12.0/24
- CGW must be configured with next hop 192.168.10.1 on LAN interface to avoid individual routes of subnet 192.168.11.0/24 via 192.168.10.1 and 192.168.12.0/24 via 192.168.10.1

Use below command to set the next hop IP address on CGW towards LAN interface.

```
$  sudo xlgateway set-lan-next-hop 192.168.10.1
   ********************************************************
   LAN next hop configure success: [192.168.10.1]
   ********************************************************
```

Note: LAN next hop must be accessible from the LAN interface. Make sure other subnets are accessible from the next hop.

3.13.28 Unset LAN Next Hop

Use below command to unset the next hop IP address on CGW towards LAN interface, if already configured.

```
$  sudo xlgateway unset-lan-next-hop
   ********************************************************
   Removing configured LAN next hop...
   ********************************************************
```

3.13.29 Show LAN Next Hop

Use below command to show the next hop IP address on CGW towards LAN interface, if already configured.

```
$  sudo xlgateway show-lan-next-hop
   ********************************************************
   LAN Next Hop: [192.168.10.1]
   ********************************************************
```

3.13.30 Setup High Availability

Two machines must be available to setup CGW with high availability.

- Primary CGW
- Secondary CGW

Note:

1. High Availability on CGW with two interfaces (WAN and LAN on

separate interfaces) is currently not supported.
2. HA setup is not supported using CGW UI.

In case one CGW is already running in data center then it can be treated as Primary Node. Below steps will be required to setup CGW HA:

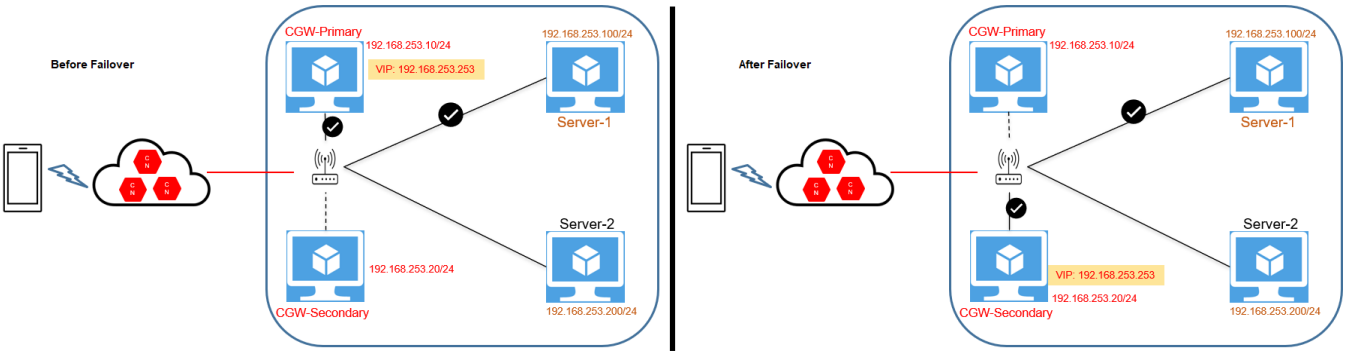
I. Create another CGW VM by referring section 3.7 or refer section 3.8 in case machine is a bare metal.
II. Both CGWs (Primary and Secondary) must be reachable to each other. IPs on both CGW machines must be from same subnet.
III. Multicast traffic must be allowed between CGW machines.

Virtual IP

CGW failover / health monitor utility will require additional IP address from the same subnet configured on interface which will be used as VIP (Virtual IP).

- VIP will be installed only on Active node
- CGW will be in connected state only on Active node
- VIP will be switched over to other node and CGW will connect automatically if current Active node fails

Sample Network Diagram



Primary Node

On primary node, install and setup CGW (refer section 3.11) or skip installation and setup if one CGW is already running in data center.

Execute below command to setup HA on primary node:
Provide input “1”, when prompted for node type and provide Virtual IP address.

```
$  sudo xlgateway setup-ha
   ********************************************************
   Setup CGW High Availability...
   Check CGW failover and monitoring utility...
   WARNING: failover/monitoring utility is missing
   Update system repository...
   System repository update: [OK]
```

```
Installing Linux Headers...
Linux Headers installation: [OK]
Installing failover/monitoring utility package...
CGW failover and monitoring utility: [OK]
Choose node type:
1. Primary
2. Secondary
Node type (provide choice 1 or 2): 1
Selected Node type: [Primary]
CGW application configuration as primary
HA health monitoring interface: [enp0s3]
Provide virtual IP to install on above interface: 192.168.253.253
Start HA monitoring utility: [OK]
Synchronizing state of keepalived.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable keepalived
*******************************************************
```

Verify CGW HA on primary node has been setup successfully.

```
$  sudo xlgateway status
   ****************** Dashboard ******************
            Username:  cgw.local.sp@eximdemo
             Version:  v0.7.8
    Server Connected:  Mumbai, India
   Connection Status:  Active
     Connected Since:  Wed 2022-03-23 07:14:19 UTC; 4 sec ago
                Date:  Wed 2022-03-23 07:14:23 UTC
           WebUI URL:  http://192.168.253.142:9630
   ***********************************************
           CGW State: Connected
   Multicast Support: Disabled
         NAT Support: Enabled
        Auto upgrade: Disabled
       LAN Interface: enp0s3
       WAN Interface: enp0s3
        LAN Next Hop: Not configured
   ***********************************************
   High Availability: Enabled
           Node Type: ACTIVE
          Virtual IP: 192.168.253.253
   ***********************************************
```

If CGW is configured with two interfaces (WAN and LAN separately), then command will exit with error.

```
$  sudo xlgateway setup-ha
   *******************************************************
   ERROR: LAN and WAN are on different interfaces.
   ERROR: Currently High Availability is supported on CGW with single interface
   *******************************************************
```

Secondary Node

On secondary node, first complete CGW installation.
Refer section 3.7 to install CGW using Exium provided virtual appliance or refer section 3.8 if user wants to install software manually on a VM or bare metal.

Make sure Primary CGW is reachable from current secondary CGW node.

Execute below command to setup secondary node:
Provide input “n”, when prompted to login and connect CGW.

```
$  sudo xlgateway setup
   ########################################################
   Starting CGW installation...
   ########################################################
   Validate Internet Connection : [OK]
   Check for user requirements...
   Notification: Multicast support disabled on CGW
   Notification: NAT support enabled on CGW
   Reloading services and daemons : [OK]
   Detach interface enp0s3 which is attached to CGW
   Detached interface enp0s3 successfully
   Available interfaces: ['enp0s3']
   Setting LAN and WAN on same interface [enp0s3]
   Validate WAN connectivity from WAN interface [enp0s3] : [OK]
   LAN interface [enp0s3] attached successfully with CGW
   Logout from current account
   Notification: Not logged in
   Login and connect the cyber gateway now [y/n]?: n
   CGW login incomplete...
   Use 'sudo xlgateway login' to login, verify the account and connect the
   service
   ************************************************************
   Use 'sudo xlgateway help' to get list of supported commands
   ************************************************************
```

Setup high availability on secondary node

Execute below command to setup HA on secondary node:
Provide input “2”, when prompted for node type and provide Virtual IP address.

```
$  sudo xlgateway setup-ha
   ********************************************************
   Setup CGW High Availability...
   Check CGW failover and monitoring utility...
   WARNING: failover/monitoring utility is missing
   Update system repository...
   System repository update: [OK]
   Installing Linux Headers...
   Linux Headers installation: [OK]
   Installing failover/monitoring utility package...
   CGW failover and monitoring utility: [OK]
   Choose node type:
   1. Primary
   2. Secondary
```

```
   Node type (provide choice 1 or 2): 2
   Selected Node type: [Secondary]
   CGW application configuration as secondary
   HA health monitoring interface: [enp0s3]
   Provide virtual IP to install on above interface: 192.168.253.253
   Start HA monitoring utility: [OK]
   Synchronizing state of keepalived.service with SysV service script with
   /lib/systemd/systemd-sysv-install.
   Executing: /lib/systemd/systemd-sysv-install enable keepalived
   ********************************************************
```

Login

Use same credentials which were used on primary CGW and complete account verification. Service will try to connect automatically but will fail because current machine is configured as secondary node. Please refer below example with sample inputs.

```
$  sudo xlgateway login
   ***********************************************
   Provide inputs to login...
   Workspace: exiumdemo
   Gateway Name: cgw.local.sp
   Checking Credentials---------> Done
   Notification: Please check your email
   Notification: We sent a verification link to s****y@e**t and to mobile
   ****1860. This link is valid for 10mins.
   Verifying User--------> Verified
   Creating User Certificates--------> Success
   Start HA monitoring utility: [OK]
   ********************************************************
   ********************************************************
   ERROR: CGW HA is enabled and current node is in STANDBY mode
   ERROR: Connection is not allowed in STANDBY mode, Exiting...
   ********************************************************
```

Verify CGW HA on secondary node has been setup successfully.

```
$  sudo xlgateway status
   ****************** Dashboard ******************
            Username:  cgw.local.sp@exiumdemo
             Version:  v0.7.8
     Server Selected:  Smart Location
   Connection Status:  Not Active
                Date:  Wed 2022-03-23 13:04:44 IST
           WebUI URL:  http://192.168.253.59:9630
   ***********************************************
           CGW State: Disconnected
   Multicast Support: Disabled
         NAT Support: Enabled
        Auto upgrade: Disabled
       LAN Interface: enp0s3
       WAN Interface: enp0s3
        LAN Next Hop: Not configured
```

```
   ***********************************************
   High Availability: Enabled
           Node Type: STANDBY
         Virtual IP: 192.168.253.253
   ***********************************************
```

If CGW is configured with two interfaces (WAN and LAN separately), then command will exit with error.

```
$  sudo xlgateway setup-ha
   *********************************************************
   ERROR: LAN and WAN are on different interfaces.
   ERROR: Currently High Availability is supported on CGW with single interface
   *********************************************************
```

3.13.31 Disable High Availability

Below commands will disable CGW HA on CGW VMs.

Secondary Node

CGW will be logged out if application is in standby state.

```
$  sudo xlgateway unsetup-ha
   *********************************************************
   CGW HA configuration will be removed, do you want to continue? [y/n]: y
   Purge CGW HA configuration. CGW will work in standalone mode
   Synchronizing state of keepalived.service with SysV service script with
   /lib/systemd/systemd-sysv-install.
   Executing: /lib/systemd/systemd-sysv-install disable keepalived
   Removed /etc/systemd/system/multi-user.target.wants/keepalived.service.
   Disabling HA utility...
   Remove HAEanable and NodeType entries: [OK]
   Stop HA monitoring utility: [OK]
   Reload HA monitoring configuration: [OK]
   Logging out application running in backup node
   User logged out successfully
   *********************************************************
```

Note: Same workspace and gateway names cannot be used simultaneously on different VMs.

Primary Node

CGW will remain connected even after HA support is disabled if current node is in active state.

```
$  sudo xlgateway unsetup-ha
   *********************************************************
```

```
CGW HA configuration will be removed, do you want to continue? [y/n]: y
Purge CGW HA configuration. CGW will work in standalone mode
Synchronizing state of keepalived.service with SysV service script with
/lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install disable keepalived
Disabling HA utility...
Remove HAEanable and NodeType entries: [OK]
Stop HA monitoring utility: [OK]
Reload HA monitoring configuration: [OK]
**********************************************************
```

3.13.32 Enable CGW Internet Bypass

It is possible in rare conditions that CGW disconnects and loses connection with Cyber Nodes. In such conditions, Secure Private Access (SPA) and Secure Internet Access (SIA) will be impacted. Machines behind CGWs will lose the internet access if CGW is not in connected state.
To avoid even minimum downtime, bypass feature can be enabled. It provides uninterrupted internet access to machine behind CGW. Traffic will pass without IpSec tunnel and configured policies.
Once CGW connects automatically, bypass rules will be disabled automatically. If CGW disconnects, bypass rules will be enforced automatically.

```
$  sudo xlgateway enable-cgw-bypass
   **********************************************************
   Traffic bypass: [Enabled]
   **********************************************************
```

Verify bypass is enabled but not enforced if CGW is in connected state:

```
$  sudo xlgateway status
   ******************** Dashboard ******************
            Username:  cgw.local.sp@exiumdemo
             Version:  v0.7.8
    Server Connected:  Mumbai, India
   Connection Status:  Active
     Connected Since:  Wed 2022-03-23 09:11:04 UTC; 22 mins ago
                Date:  Wed 2022-03-23 09:33:28 UTC
           WebUI URL:  http://192.168.253.142:9630
   ************************************************
           CGW State: Connected
   Multicast Support: Disabled
         NAT Support: Enabled
        Auto upgrade: Enabled
       LAN Interface: enp0s3
       WAN Interface: enp0s3
        LAN Next Hop: Not configured
   ************************************************
      Traffic Bypass: Enabled, [NOT ENFORCED]
   ************************************************
```

Verify bypass is enabled and enforced if CGW is in disconnected state:

```
$  sudo xlgateway status
   ****************** Dashboard ******************
            Username:  cgw.local.sp@exiumdemo
             Version:  v0.7.8
      Server Selected:  Smart Location
   Connection Status:  Not Active
                Date:  Wed 2022-03-23 09:38:34 UTC
           WebUI URL:  http://192.168.253.142:9630
   ***********************************************
           CGW State: Disconnected
   Multicast Support: Disabled
         NAT Support: Enabled
        Auto upgrade: Enabled
       LAN Interface: enp0s3
       WAN Interface: enp0s3
        LAN Next Hop: Not configured
   ***********************************************
      Traffic Bypass: Enabled, [ENFORCED]
   ***********************************************
```

Note: CGWs are already configured to recover themselves automatically in case of abnormal scenarios.

3.13.33 Disable CGW Internet Bypass

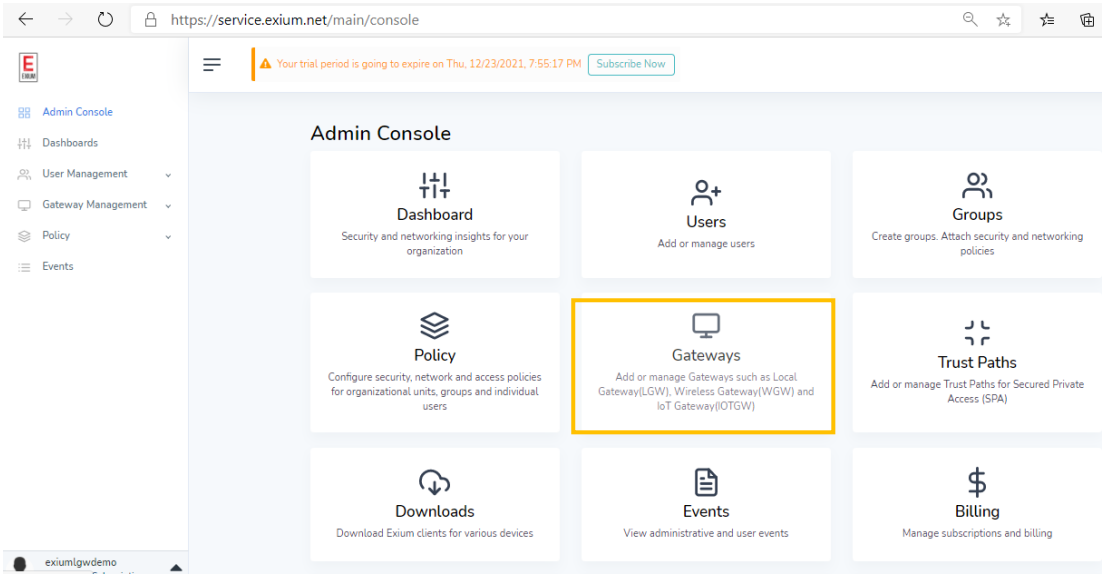
Use below command to disable Internet bypass. If internet bypass is disabled, machines behind CGW will observe interruption if CGW loses connection with Cyber Node/Mesh.

```
$  sudo xlgateway disable-cgw-bypass
   ********************************************************
   Traffic by-passing: [Disabled]
   ********************************************************
```

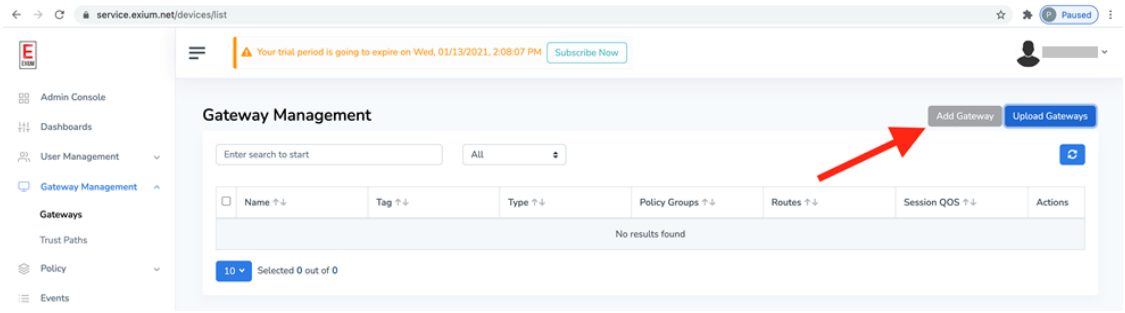
4 GATEWAY MANAGEMENT

4.1 ADD GATEWAY

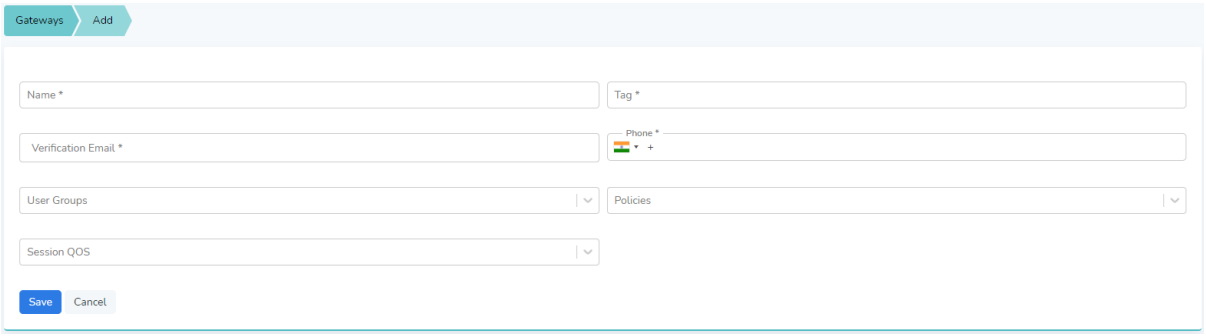
Follow instructions mentioned in section (3.3) “Admin Console” on Exium portal. Click on “Gateways” tab.
If you are already logged in, then access “Admin Console” from left panel of web page and click on “Gateways” tab.



On Gateway Management page, click on “Add Gateway”.

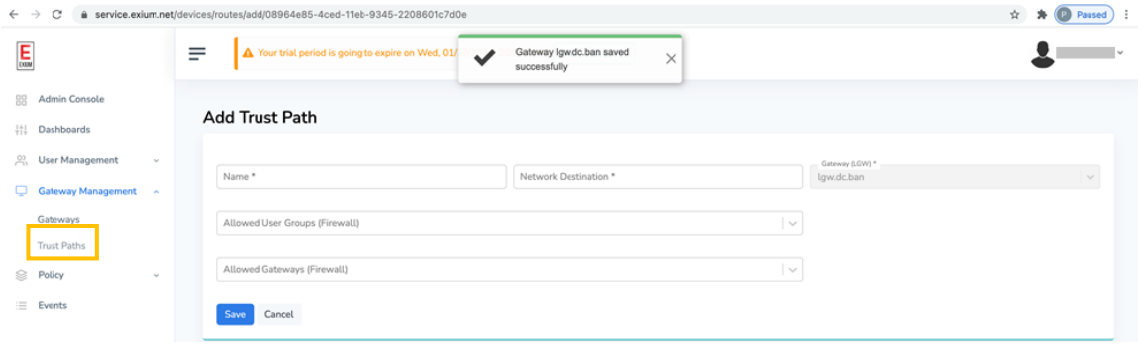


Proceed to enter all the details like Name (mandatory), Email (auto filled), Tag (editable), Session QoS, Policy groups. Click “Save” once finished.

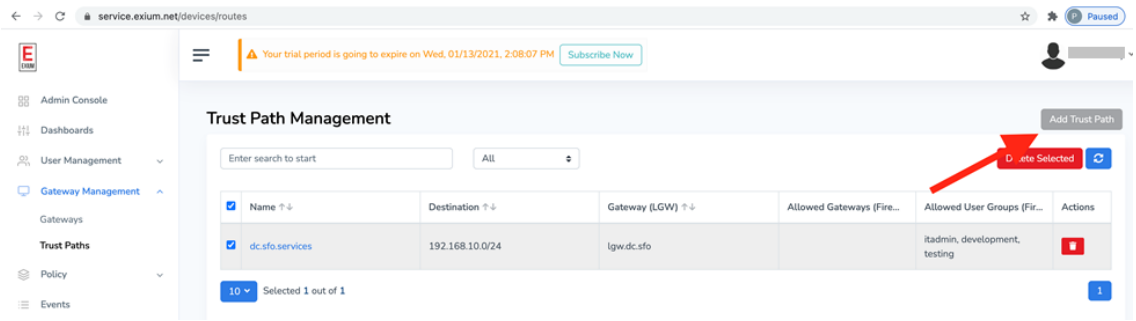


4.2 ADD TRUST PATH

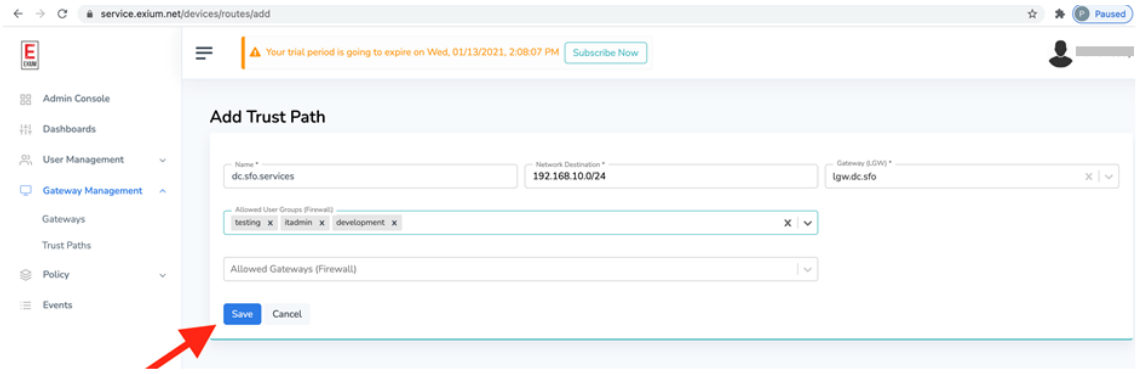
Once Gateway is added successfully, you will be redirected to next page to add trust path.
In case user wants to add trust path later, “Trust Paths” page can be accessed from “Admin Console” on the portal or left panel on the web page under “Gateway Management”.



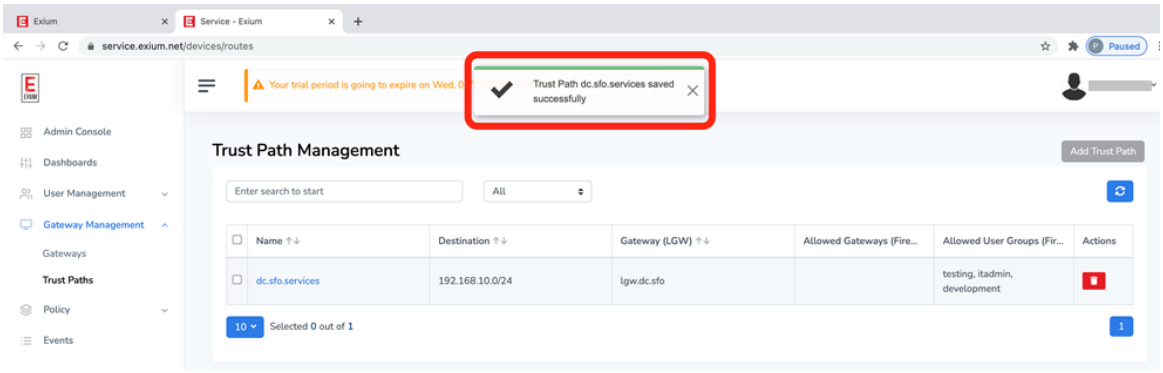
Click on “Add Trust Path” on “Trust Path Management” page:



Proceed to enter all the details like Group Name (mandatory), Network Destination (mandatory), Gateway (mandatory), Allowed User Groups (multiple – user groups which can access these services/servers). Click “Save” once finished.

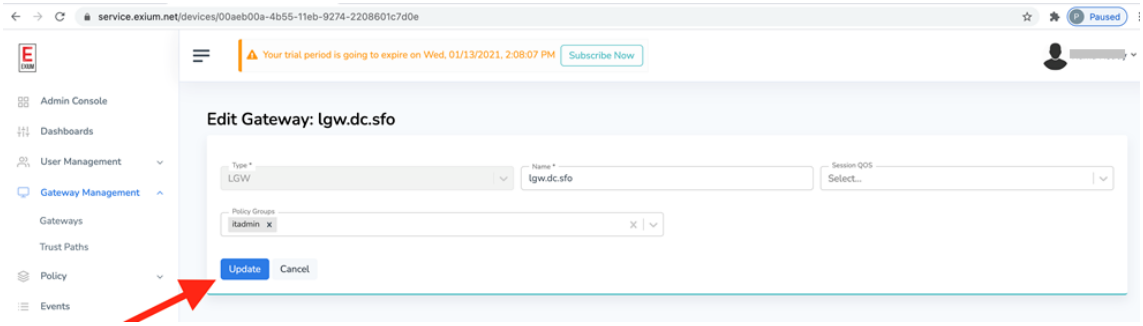


Notification will be displayed after trust path is added successfully.



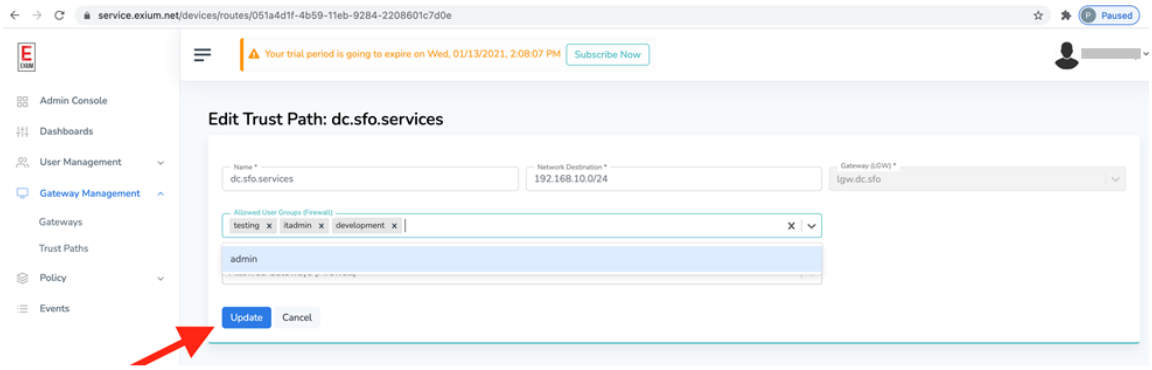
4.3 EDIT GATEWAY

User can edit existing Gateway by clicking on name visible on “Gateway Management” page. It will display gateway details and fields which can be updated or modified.



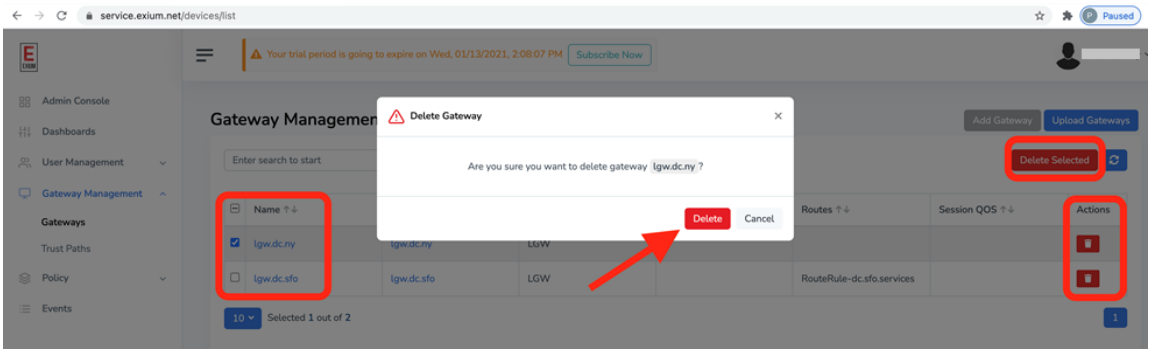
4.4 EDIT TRUST PATH

User can edit a trust path by clicking its name visible on “Trust Paths” page. User can add or remove allowed user groups (by default only admin group will be present).



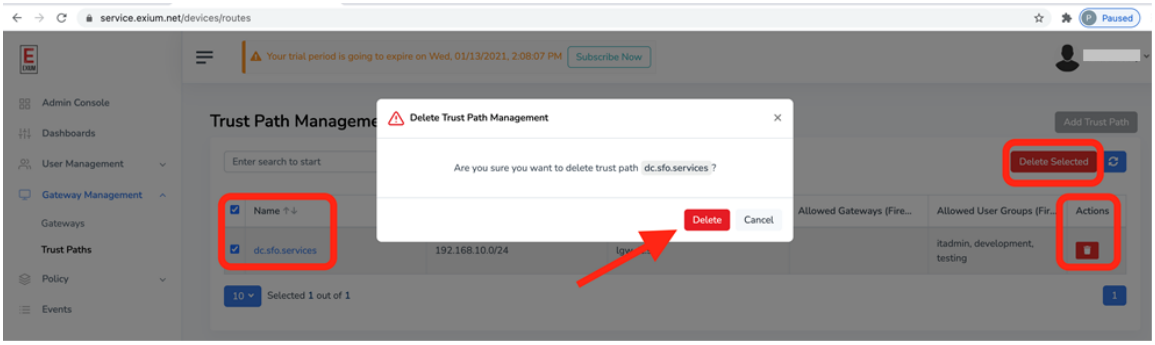
4.5 DELETE TRUST PATH

User can delete a trust path by individually clicking on delete icon. Multiple trust paths can also be selected and deleted by single delete operation.



4.6 DELETE GATEWAY

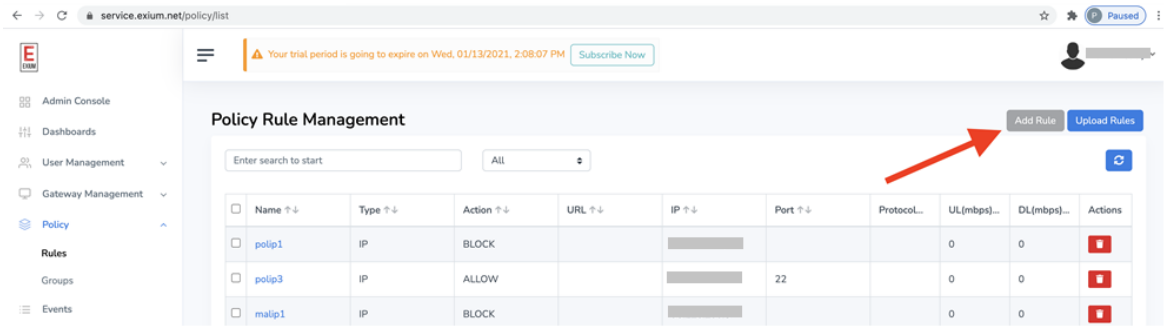
User can delete a Gateway by individually clicking on delete icon. Multiple Gateways can also be selected and deleted by single delete operation.



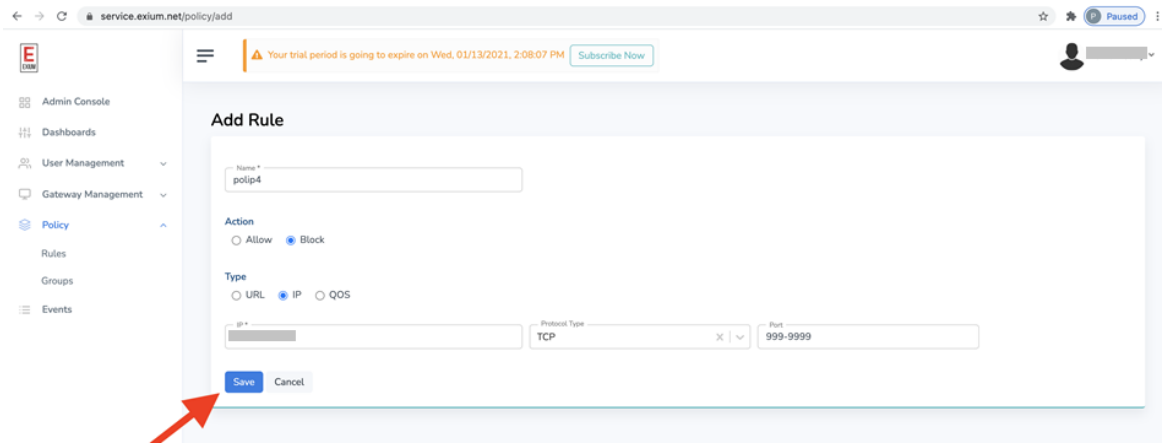
5 POLICY MANAGEMENT

5.1 ADD POLICY

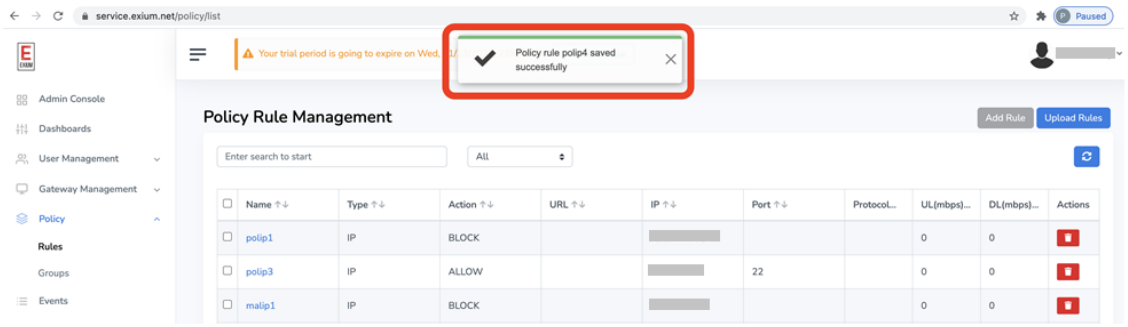
Follow instructions mentioned in section (3.3) to access “Admin Console” on Exium portal. Click on “Policy” tab.
If you are already logged in, then access “Policy” tab from left panel of web page and click on “Rules” tab.
On Policy Rule Management page, click on “Add Rule”:



Proceed to enter all the details like Name (mandatory), Action (mandatory), Type (mandatory). Based on Type, enter details like IP, Port, Protocol etc.
Click “Save” once configuration is completed.

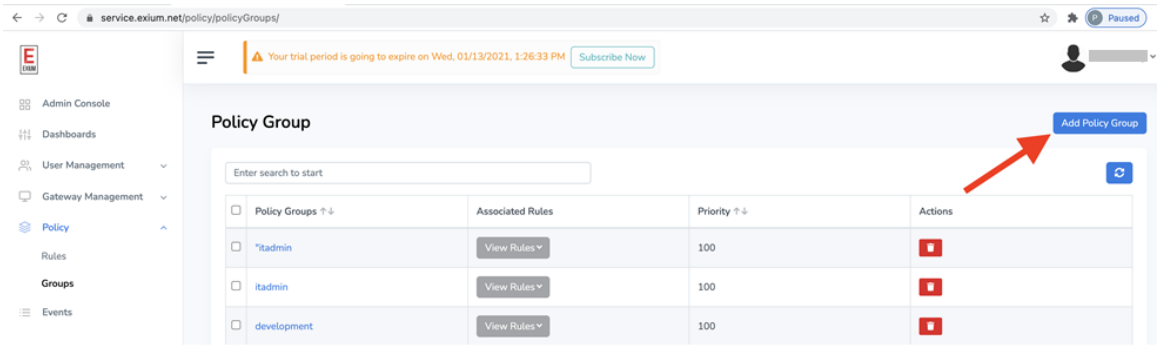


Notification will be displayed after policy is added successfully.

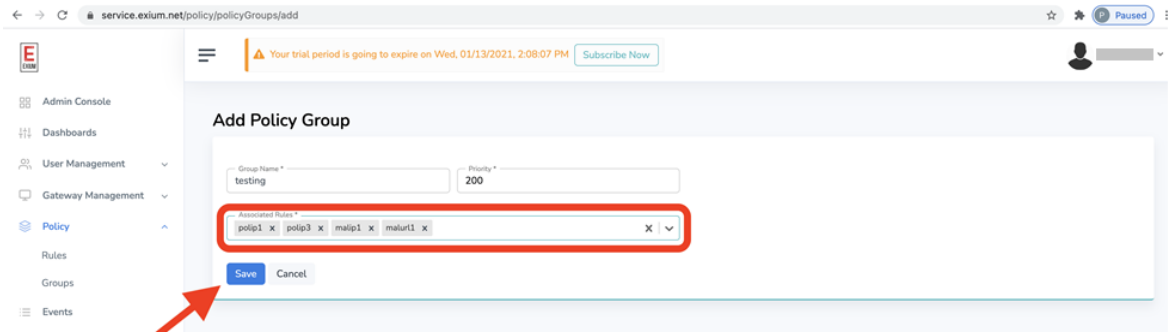


5.2 ADD POLICY GROUP

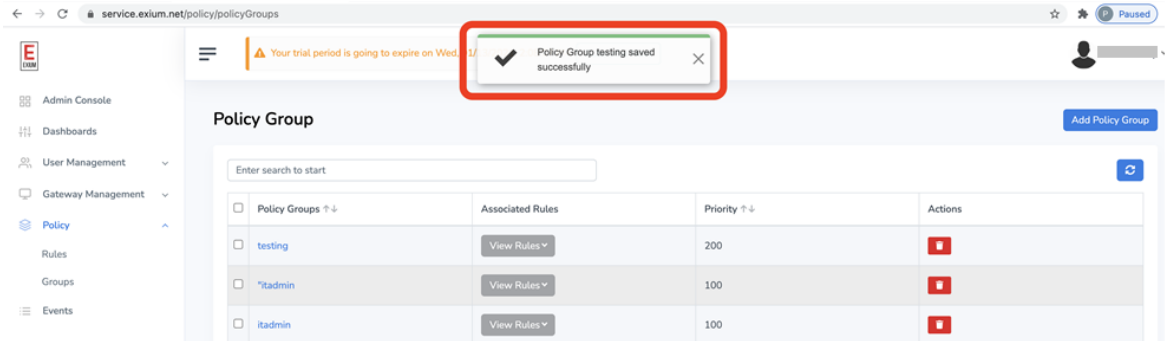
Navigate to “Groups” page by clicking on the tab present under “Policy” section on left panel of the web page.
On Groups page, click on “Add Policy Group”:



Proceed to enter all the details like Group Name (mandatory), Priority (mandatory), Rules (multiple).
Click “Save” to complete configuration.

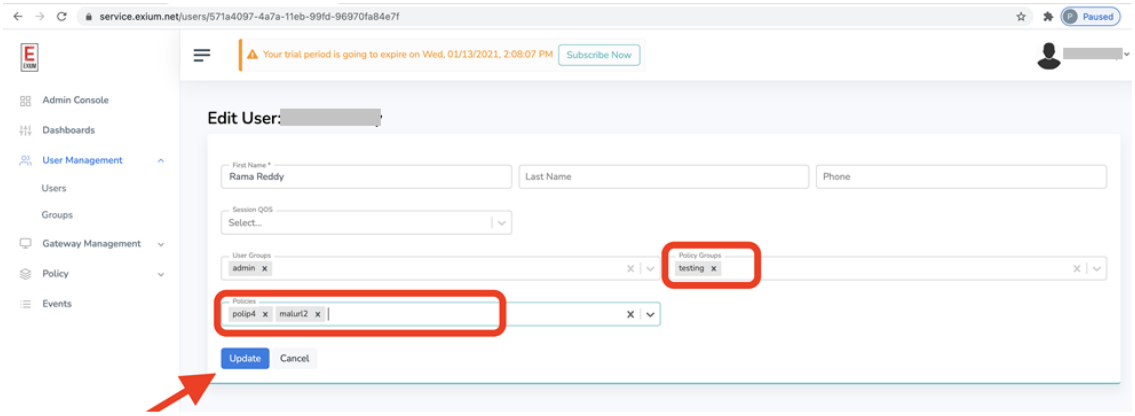


Notification will be displayed after policy group is added successfully.

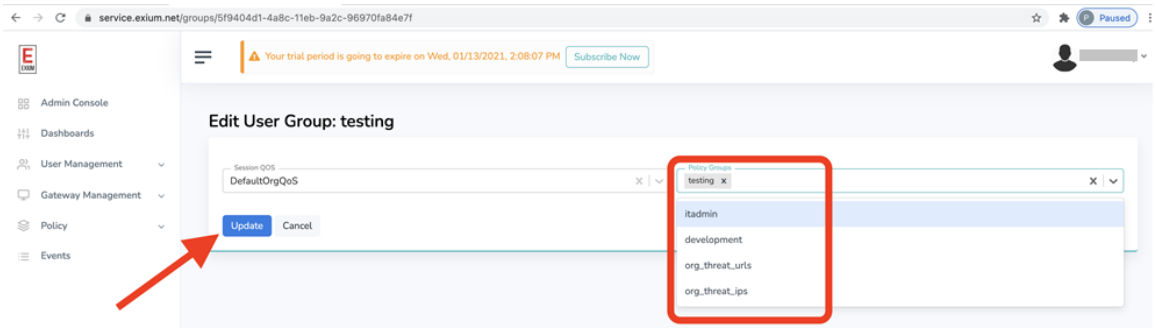


5.3 POLICY ASSIGNMENT

User can assign policies and groups to registered users.
Navigate to “User Management” page and click on a username to assign policies and groups.

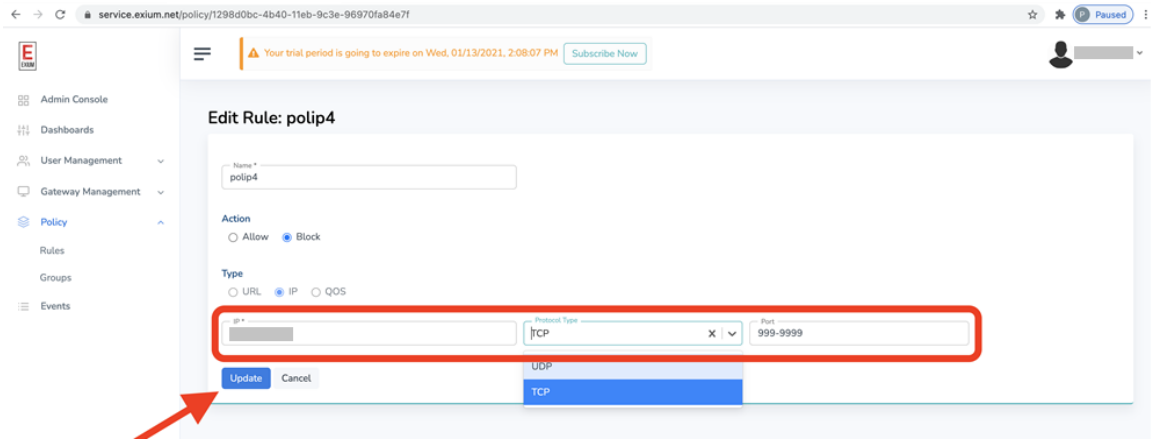


User can assign policy groups to registered user group.
Click On edit User under User Groups page to assign policy group.



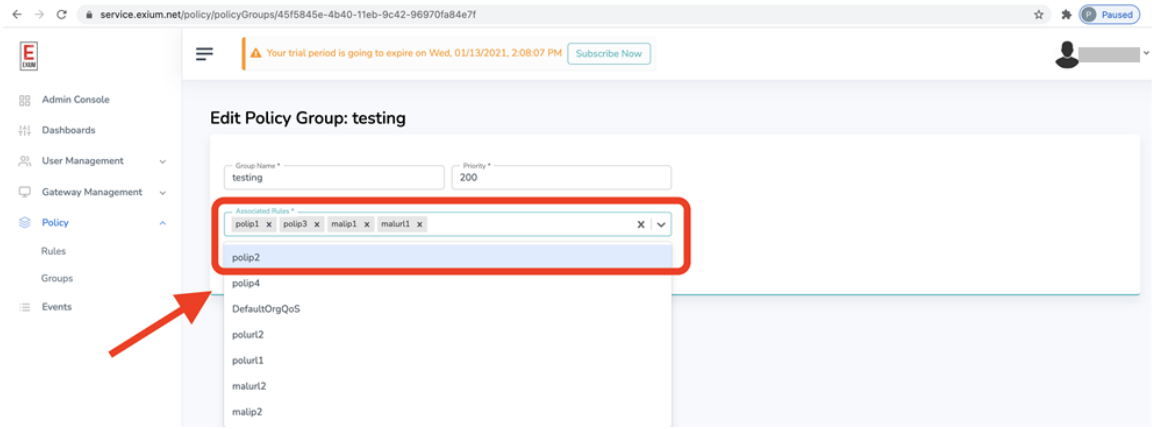
5.4 EDIT POLICY

User can edit a rule/policy by clicking on an individual policy name visible on "Rules" page.
It will display policy details and fields which can be updated or modified.
Click on "Update" to save changes.



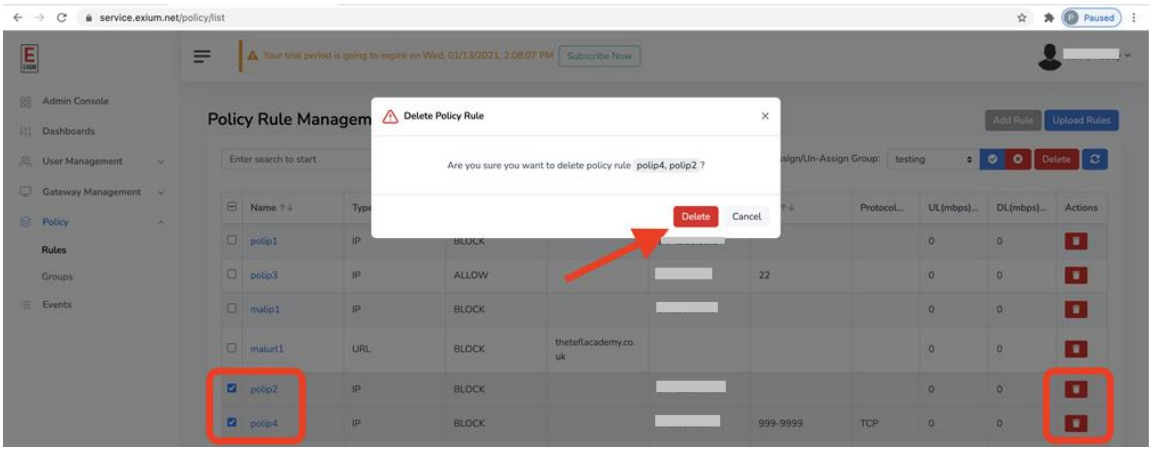
5.5 EDIT POLICY GROUP

User can edit a policy group by clicking on an individual policy group name visible on "Groups" page.
It will display policy group details and fields which can be updated or modified.
Click on "Update" to save changes.



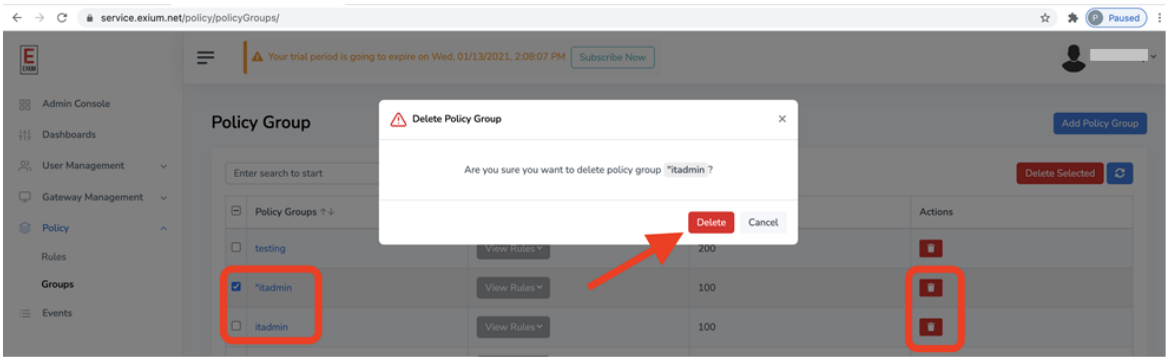
5.6 DELETE POLICY

User can delete a rule/policy by individually clicking on delete icon. Multiple rules/policies can also be selected and deleted by single delete operation.



5.7 DELETE POLICY GROUP

User can delete a policy group by individually clicking on delete icon. Multiple policy groups can also be selected and deleted by single delete operation.



6 APPENDIX

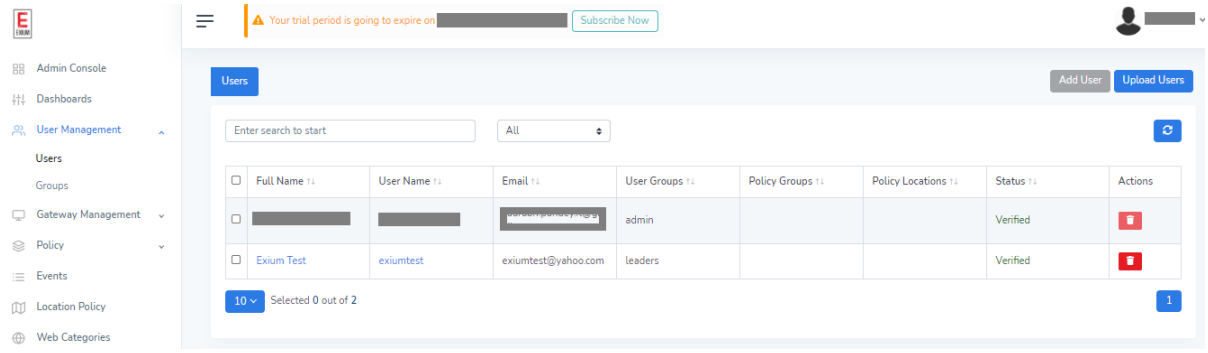
The purpose of this section it to provide users working configuration example of CGW.
It includes following configuration examples:

- Exium Client User Configuration
- CGW Configuration
- Trust Path Configuration
- Sample setup diagram

6.1 EXIUM CLIENT USER CONFIGURATION

Refer below example configuration with the details:

- "Enterprise Admin" is Full Name of "admin" user present in first row of below snapshot.
- "Exium Test" is Full Name of the non-admin user present in second row of below snapshot. It is part of "leaders" user group.

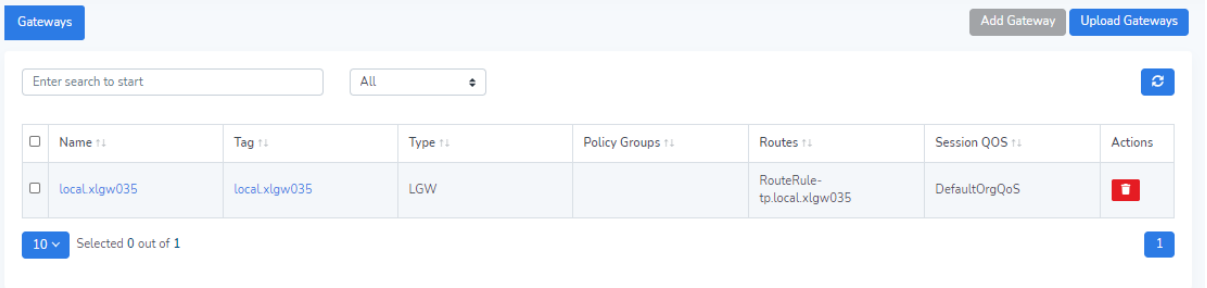


- Users present under "User Management", must be used on Exium clients for login and not on CGW VM.

6.2 CGW CONFIGURATION

Refer below example configuration with the details:

- Gateway name: local.xlgw035

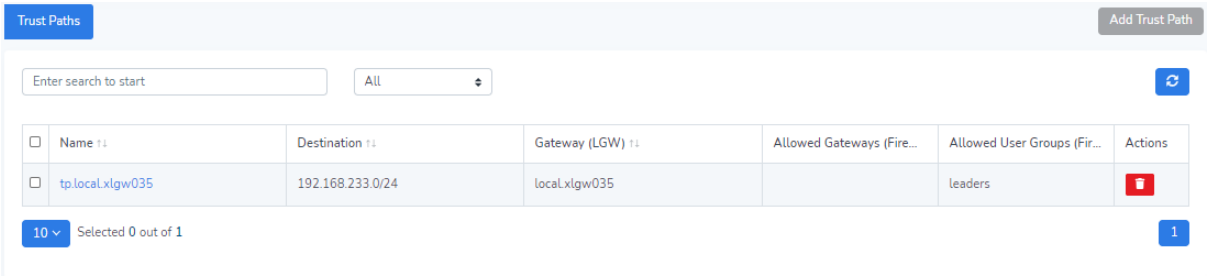


- Gateway names must be used as username on the CGW VMs during setup procedure (Section 3.6).
- To avail "Secure Private Access", CGW and Exium client usernames must be part of same Workspace.

6.3 TRUST PATH CONFIGURATION

Refer below example for policy configuration:

- Trust Path name: tp.local.xlgw035
- Associated gateway name: local.xlgw035
- Allowed user groups: leaders
- Subnet: "192.168.233.0/24"



6.4 SAMPLE DIAGRAM FOR LOCAL CGW SETUP WITH 2 INTERFACES

Note: Below example show sample CGW setup with gateway name and trust path.

1) Workspace : lgwsetup1
   Gateway name : local.xlgw035
   LAN subnet : 192.168.233.0/24
   Exium Client (non LGW) username : eximtest
   User group allowed for secure access : leaders