Deployment Guide

Version 2.0.8

Contents

Copyright Notice **3**

Document Revision History **4**

OVA Download **5**

OVA Deployment **6**

Preparations 6

Network 7

Port Usage 7

System Requirements 8

Supported Platforms 8

Cluster Size 8

Virtual Machine Configuration 8

Browsers 8

Deploying 9

Cluster Setup **10**

Individual Node DNS Entries 10

SSL Certificates 10

OAuth Client 11

Node Setup **14**

Network Setup (DHCP) 14

Network Setup (Static IP) 15

Initialize Cluster 24

Verify DNS and SSL 33

Disable Cloud-Init 34

Content Gateway Setup **36**

Content Gateway Installer 36

SSL Certificates 36

SSL Certificates 36

Content Gateway Setup **34**

Account Creation 34

Copyright Notice

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without express written permission. Under the law, reproducing includes translating into another language or format.

The software is protected by United States copyright laws and international treaty provision. Therefore, you must treat the software like any other copyrighted material (e.g. a book or sound recording).

Document Revision History

July 18, 2017

- Initial release of documentation

August 21, 2017

- Static IP setup

May 30, 2018

- Released v1.3.4

June 04, 2018

- Released v1.3.7

September 21, 2018

- Released v2.0.3

March 8, 2019

- Released v2.0.8

OVA Download

The latest OVA file is available as a secure download hosted on Amazon S3.

Your professional services representative will provide you with a secure link to download the file when it becomes available.

OVA Deployment

Preparations

To set up Backpack, you must have:

- Backpack OVA
- Supported virtual infrastructure
- MySQL or Microsoft SQL compatible server
- Nginx compatible SSL certificate and SSL certificate key

OVA Deployment

Network

Port Usage

Protocol	Port	Direction	Purpose
HTTPS	443	Inbound	Backpack API
HTTPS	443	Outbound	VCC API
TCP	3306	Outbound	MySQL Server
TCP	1433	Outbound	Microsoft SQL Server
SSH	22	Inbound/Outbound	Cluster administration

OVA Deployment

System Requirements

Supported Platforms

VMware ESXI 5.5 and later are supported.

Cluster Size

The recommended size of a Backpack cluster is 1 node on 1 distinct physical host.

Virtual Machine Configuration

The minimum requirements for a Backpack node are:

CPU: 3 GHz dual core or 4 virtual processors
RAM: 8 GB
STORAGE: 80GB

The recommended requirements for a Backpack node are:

CPU: 3 GHz quad core or 8 virtual processors
RAM: 12 GB
STORAGE: 120GB, low-latency SATA or SSD drives

Browsers

The Backpack interface is supported on the latest versions of Firefox, Internet Explorer, Edge, Chrome, and Safari.

Backpack OVA Deployment

Deploying

Deploy the OVA on your platform as you would any other OVA. Refer to your platform's documentation for instructions on deploying OVA files.

Cluster Setup

Clusters are headless and all nodes are functionally identical.

Individual Node DNS Entries

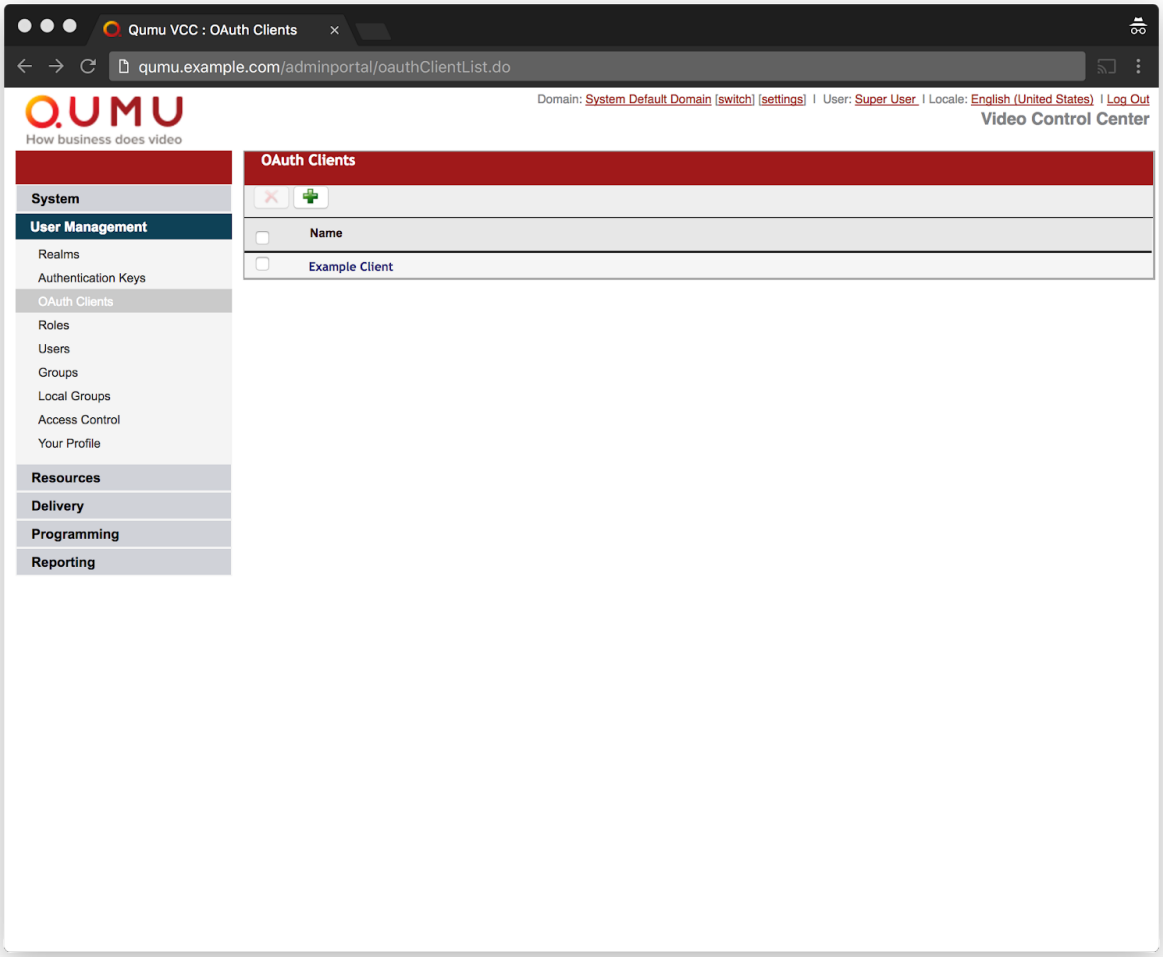
Individual nodes do not require distinct DNS entries but can be assigned one for administrative convenience.

SSL Certificates

The SSL certificate and certificate key should be Nginx compatible. See - http://nginx.org/en/docs/http/configuring_https_servers.html - for more information.

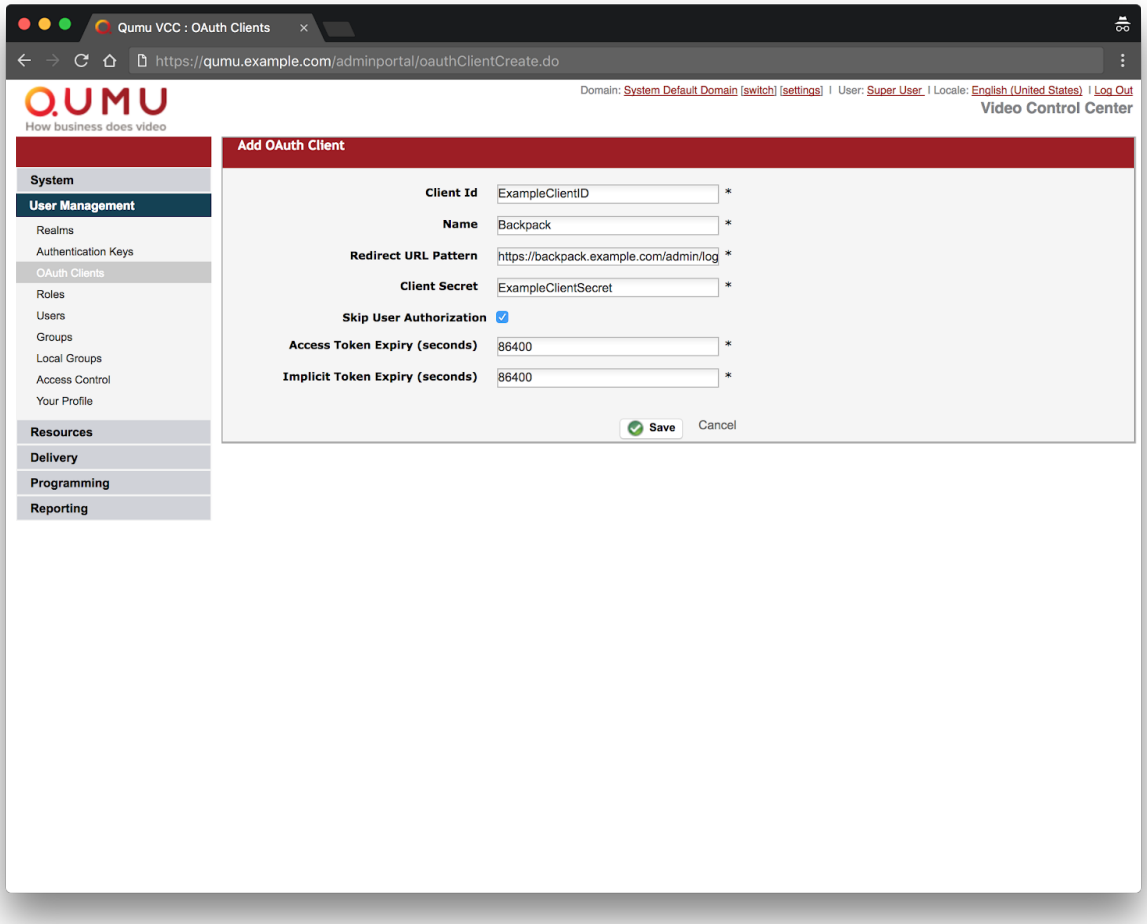
OAuth Client

1. From the Qumu Video Control Center Admin Portal, navigate to **User Management** > **OAuth Clients** and click the green + button to add a new client

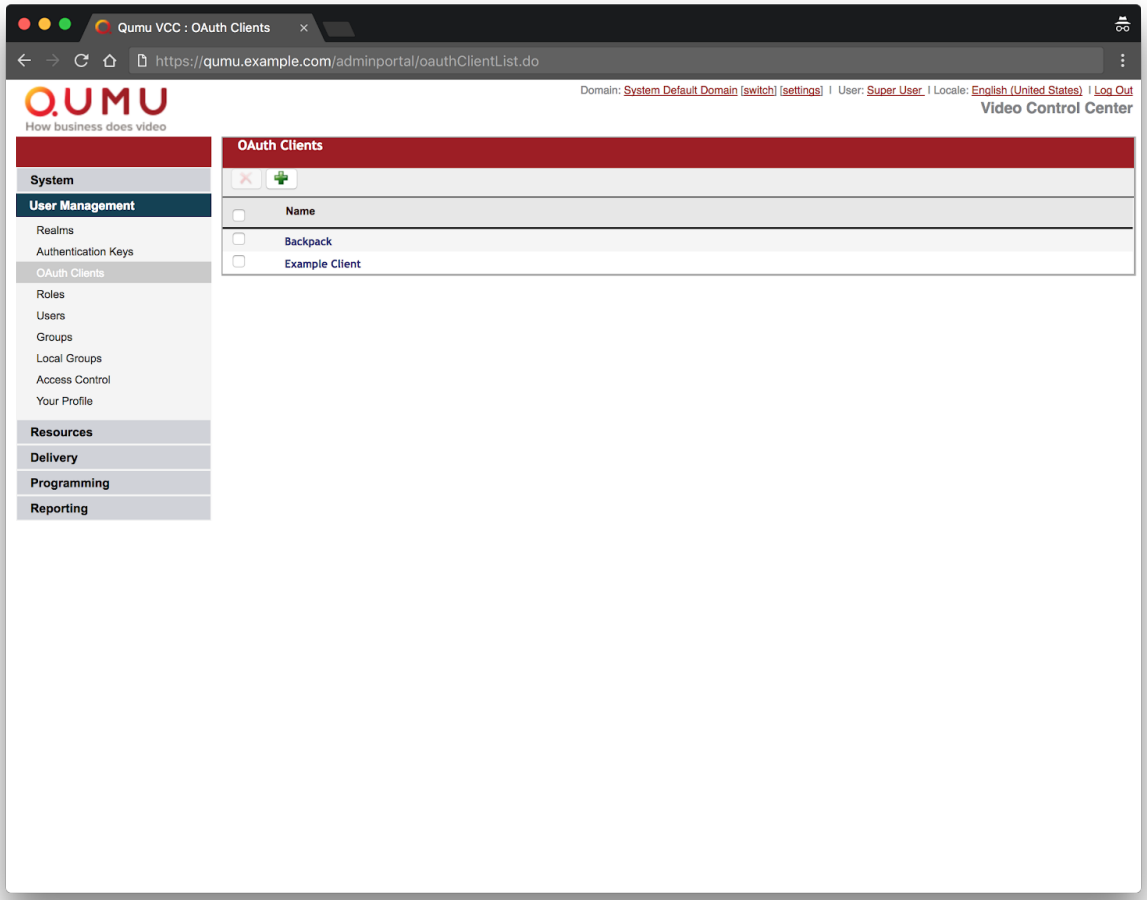


2. Enter the following values for a new OAuth Client and click **Save**. Make note of the values for use when initializing the cluster.

    a. **Client ID:** [A recognizable value of your choice.]
    b. **Name:** Backpack
    c. **Redirect URL Pattern:** https://[BACKPACK_HOSTNAME]/admin/login
    d. **Client Secret:** [A random value of your choice. https://www.uuidgenerator.net/ helps create these.]
    e. **Skip User Authorization:** Checked
    f. **Access Token Expiry (seconds):** 86400
    g. **Implicit Token Expiry (seconds):** 86400



3. Confirm the OAuth client was created and exit the Qumu Video Control Center Admin Portal.



Node Setup

Network Setup (DHCP)

By default, nodes use dynamic host configuration protocol (DHCP) on network device eth0. No additional network setup is required on DHCP systems.

Network Setup (Static IP)

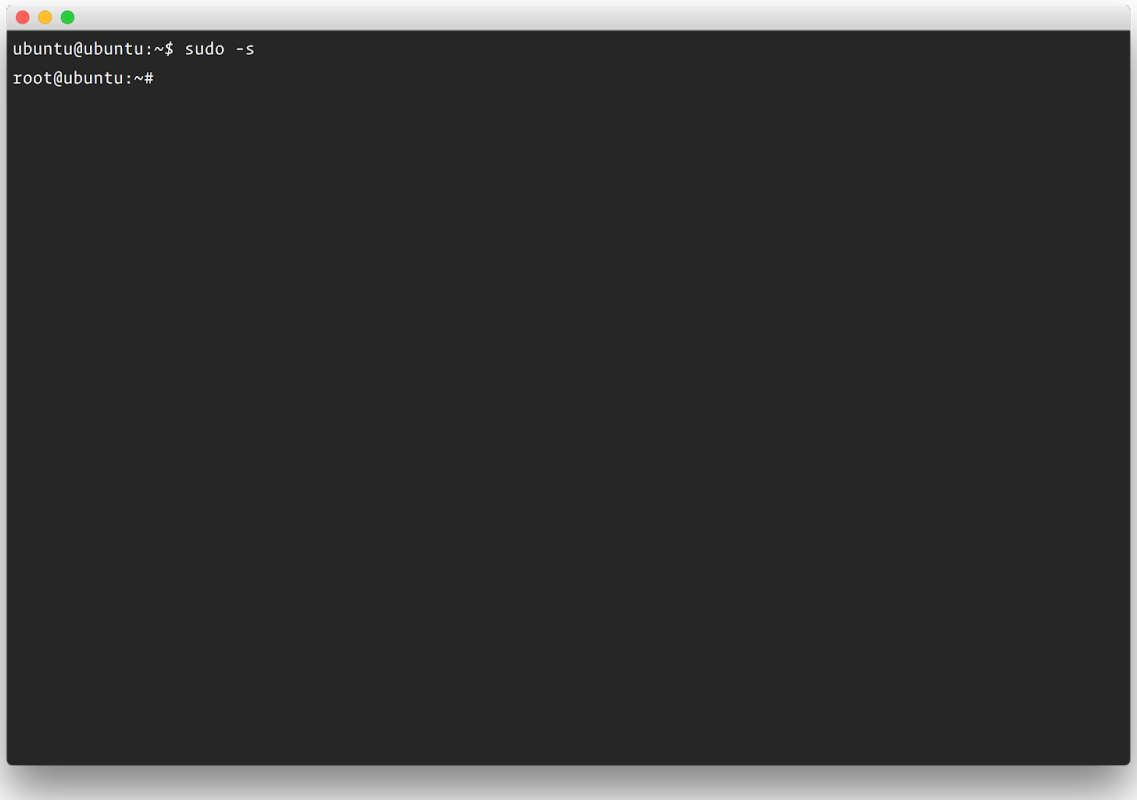
For systems with statically allocated IP addresses:

1. Access the virtual machine terminal.
2. At the login prompt, enter:

```
username: ubuntu
password: ubuntu
```

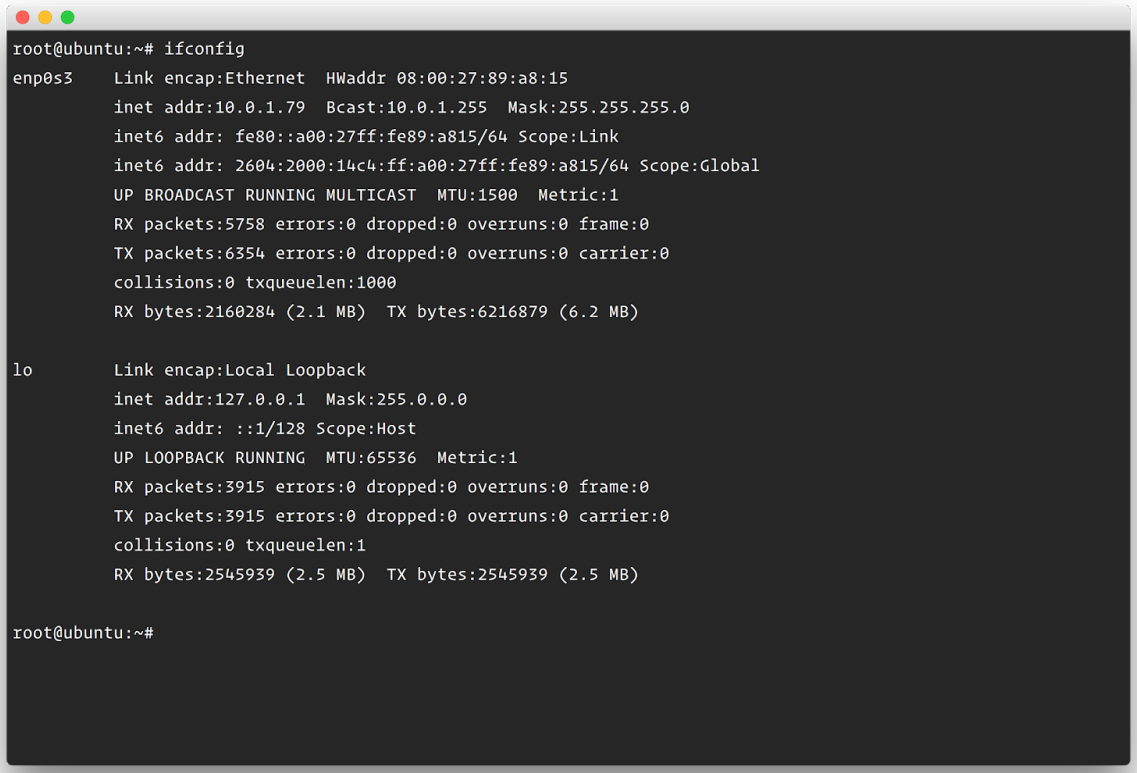
3. Run the following command to switch to ‘root’ user:

```
sudo -s
```



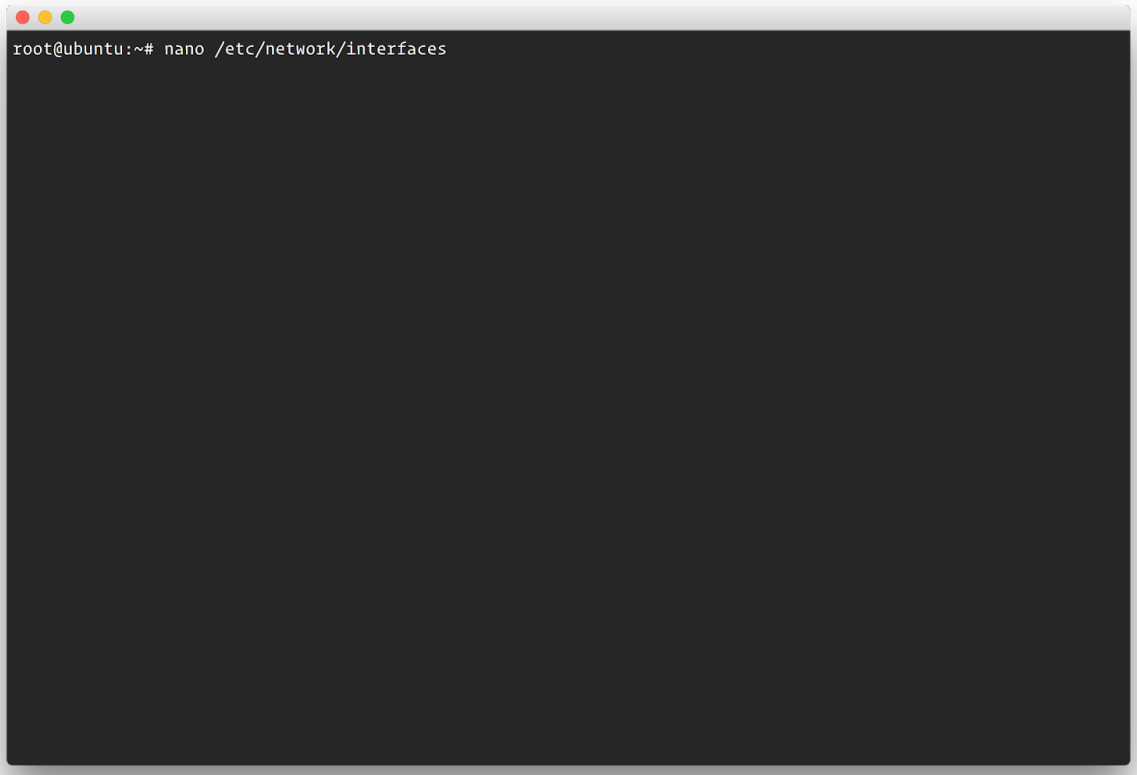
4. Verify the network interface, In this case it's **enp0s3**

```
ifconfig
```



5. Open the network configuration file for editing:

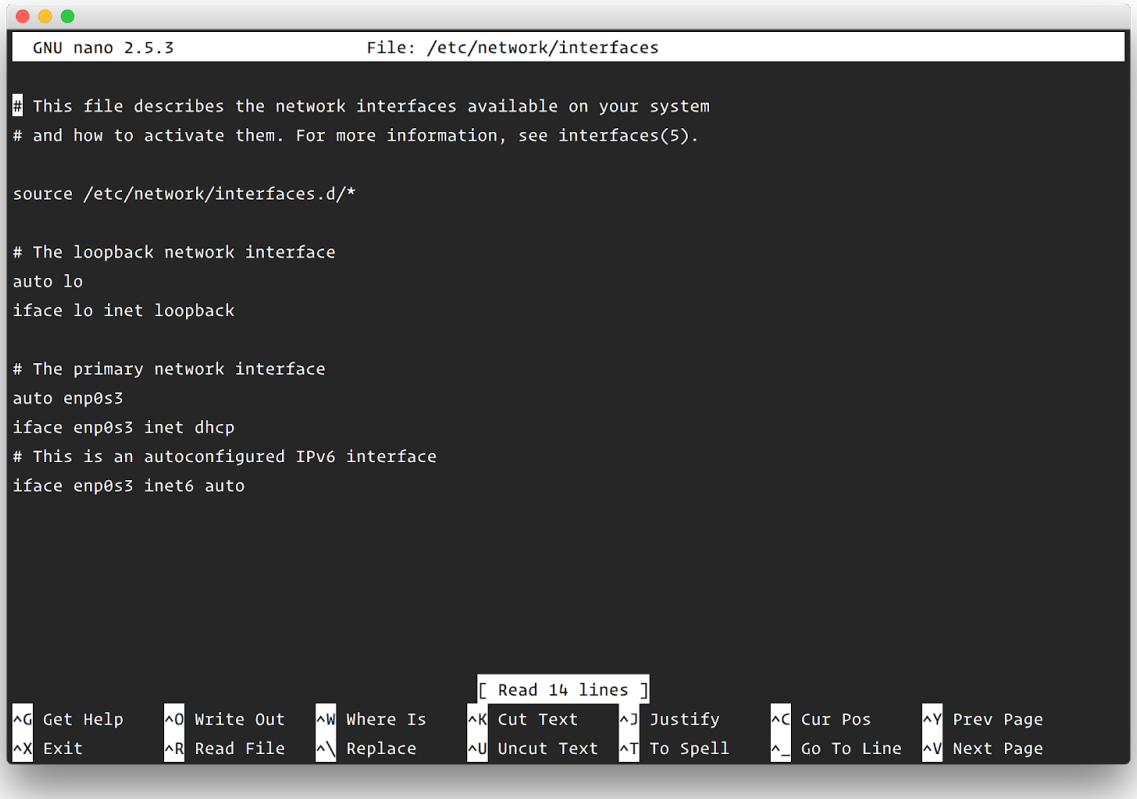
```
nano /etc/network/interfaces
```



6. Review and modify the settings as needed.

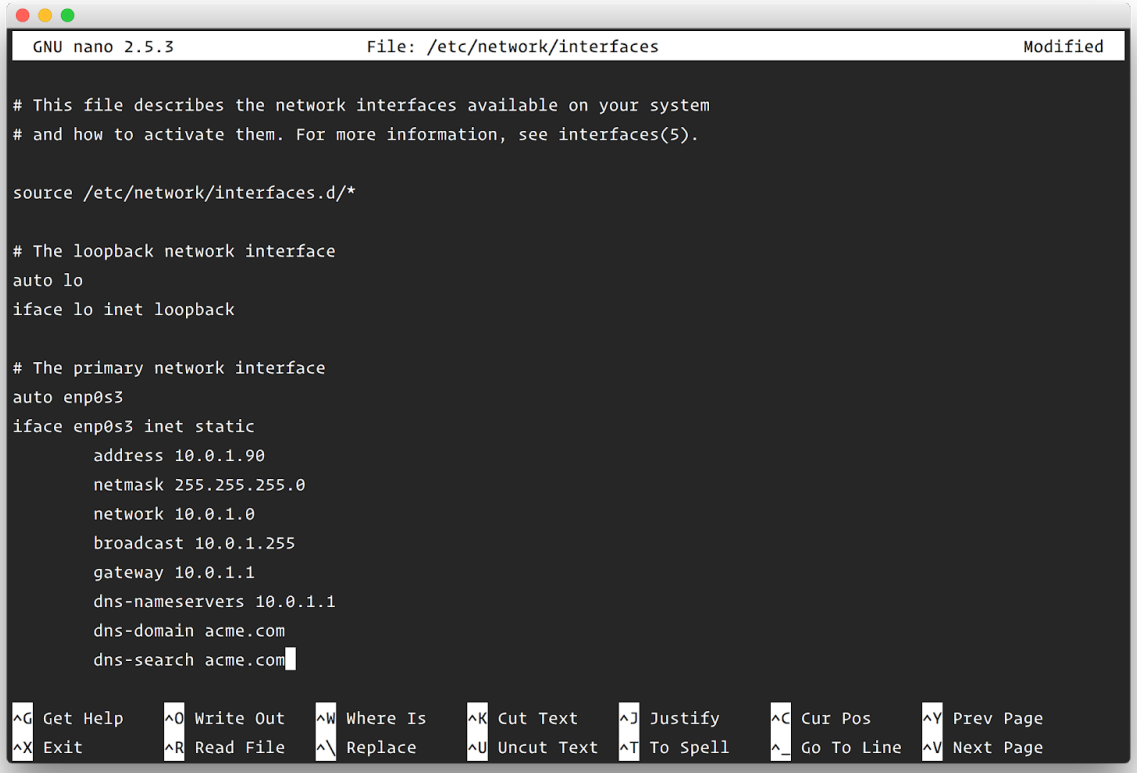
    - If the primary network interface has a different name, the /etc/network/interfaces file may look little different.
    - The file will look similar to:

```
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto enp0s3
iface enp0s3 inet dhcp
# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto
```

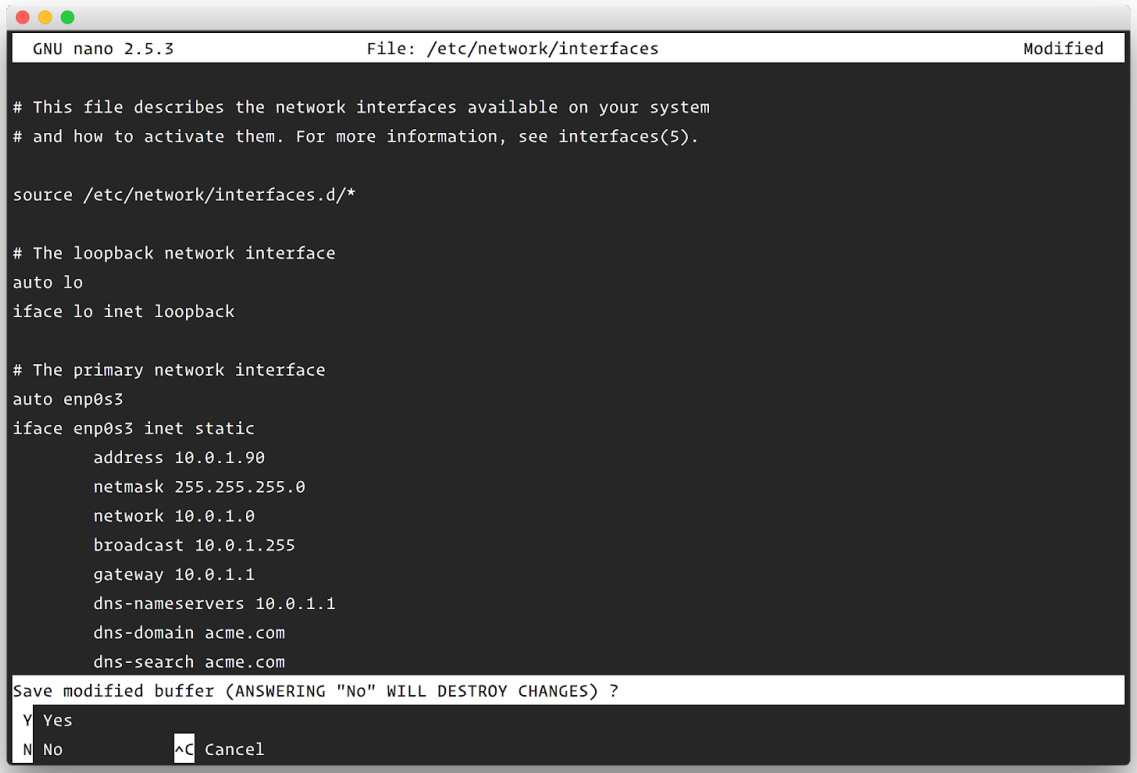


- Your changes will most likely look similar to:

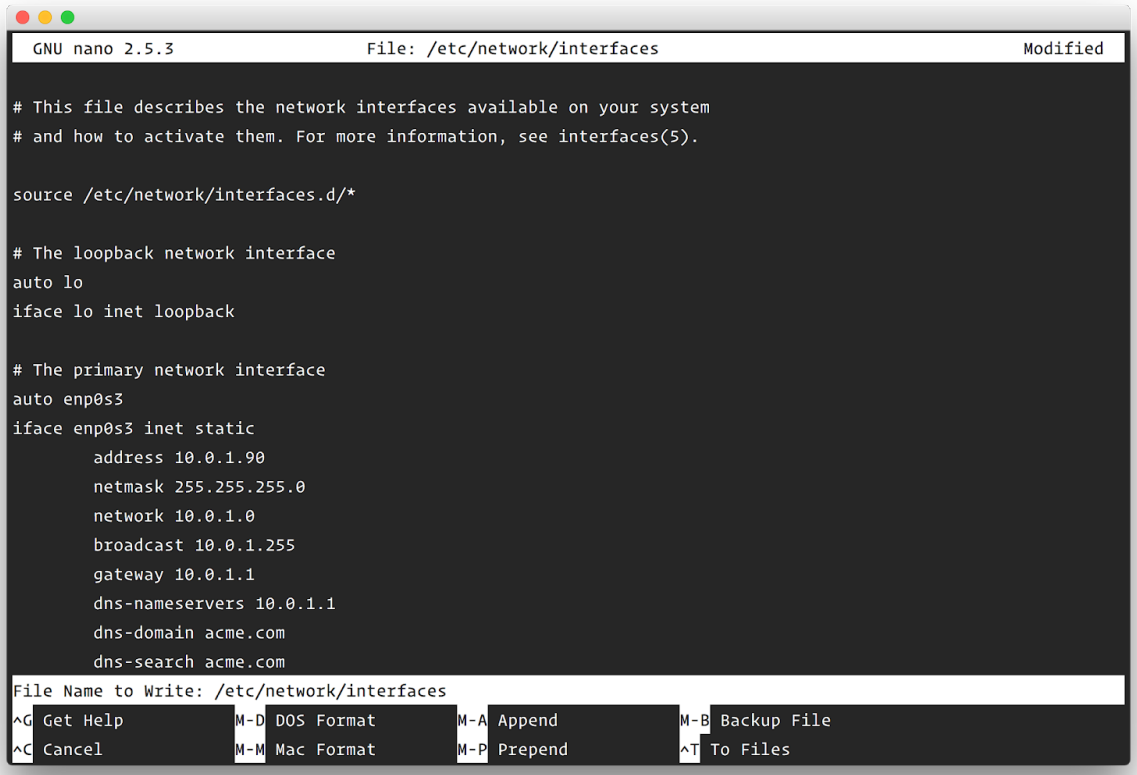
```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto enp0s3
iface enp0s3 inet static
    address 10.0.1.90
    netmask 255.255.255.0
    network 10.0.1.0
    broadcast 10.0.1.255
    gateway 10.0.1.1
    dns-nameservers 10.0.1.1
    dns-domain acme.com
    dns-search acme.com
```



7. When your modifications are completed press **CTRL-X** to exit.
8. Press the **Y** key to save your changes.

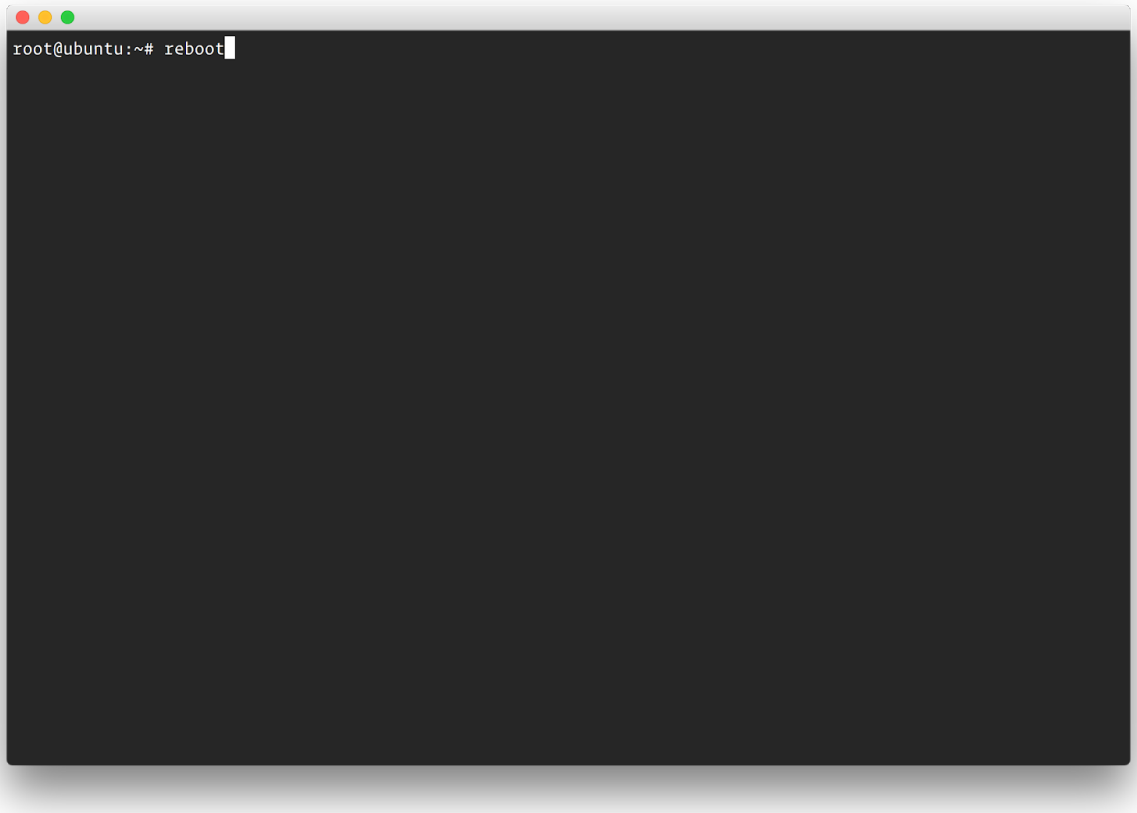


9. Press **ENTER** to save the file.



10. Reboot the machine:

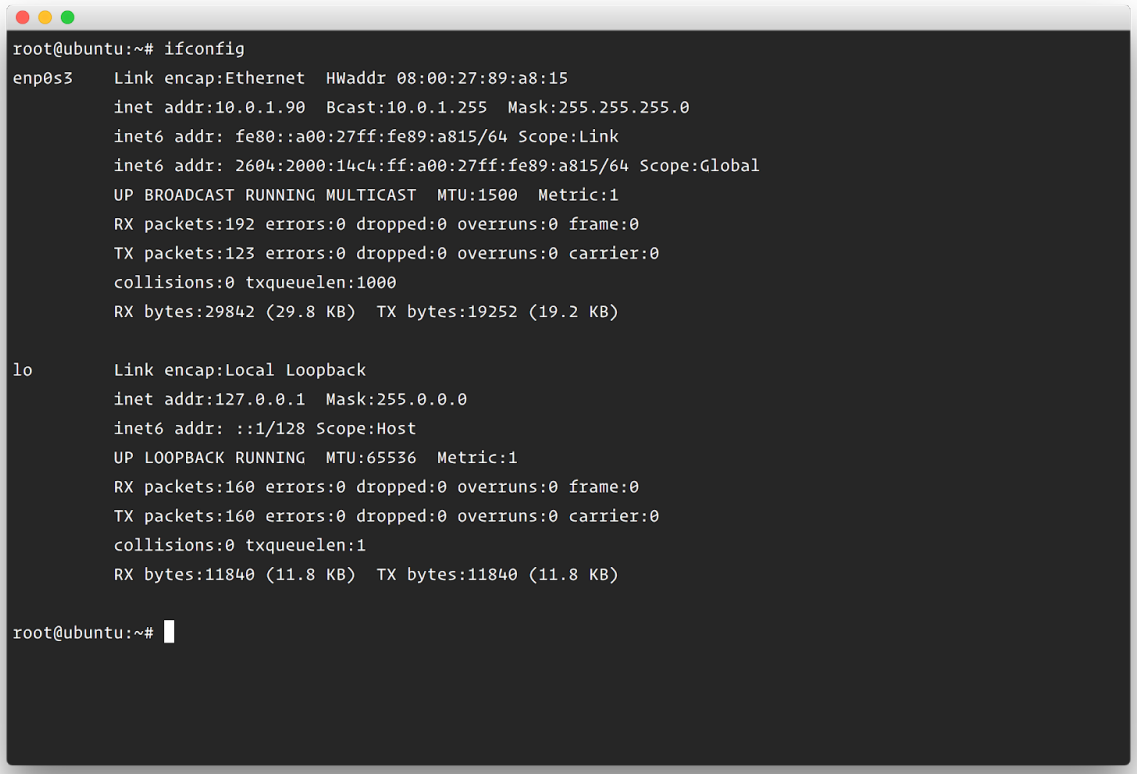
```
reboot
```



11. After the system restarts, confirm that it was configured successfully.
    - Lookup ip address of the machine by running,

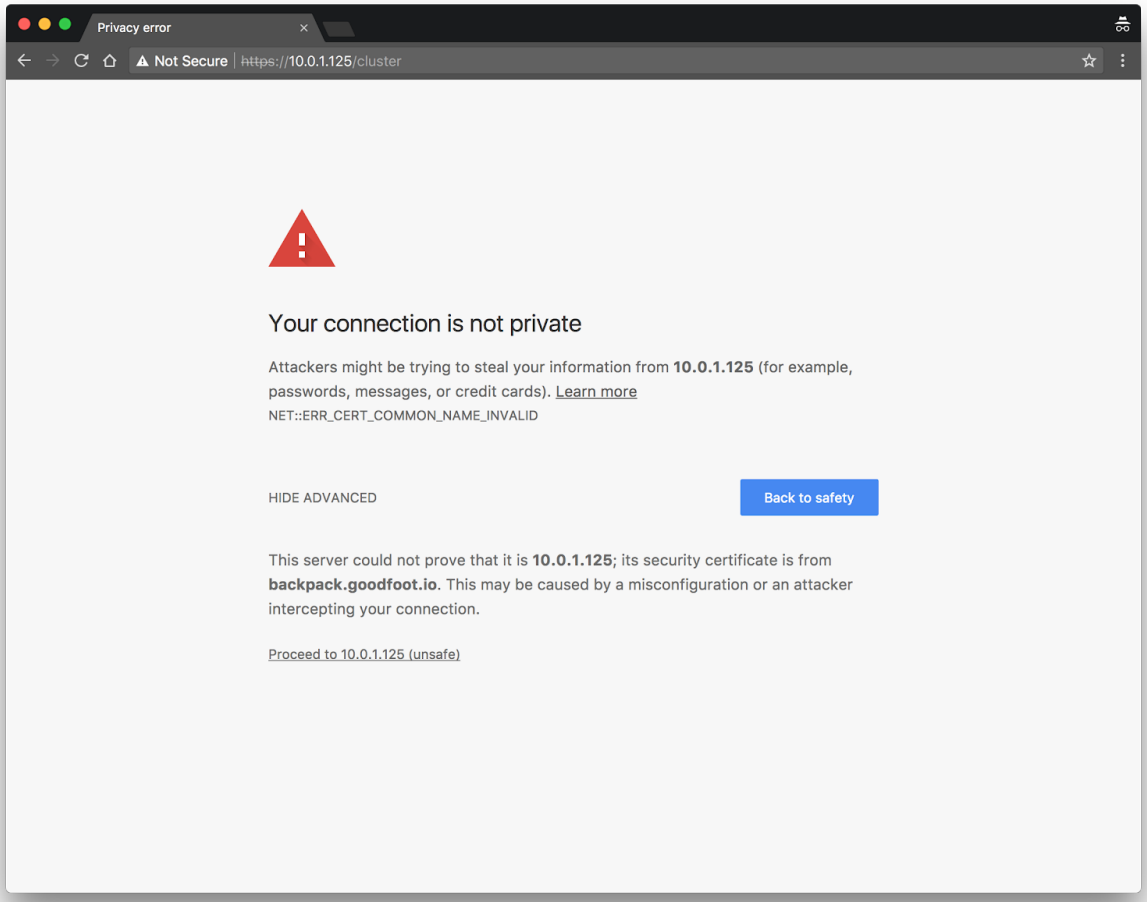
      ```
      ifconfig
      ```
    - Ping the configured IP address:

      ```
      ping [configured IP address]
      ```
    - Access **https://[configured IP address]/cluster** in a web browser and check for the cluster setup screen.

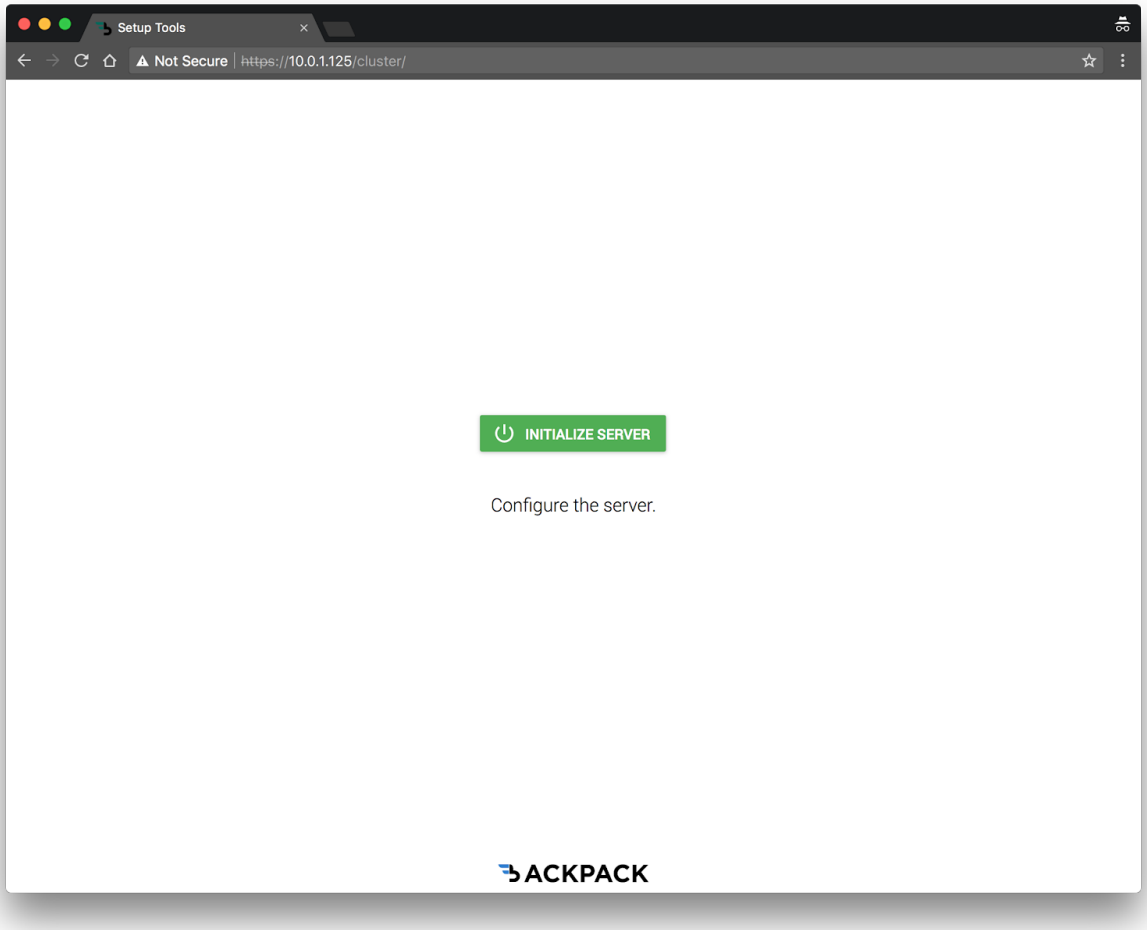


Initialize Cluster

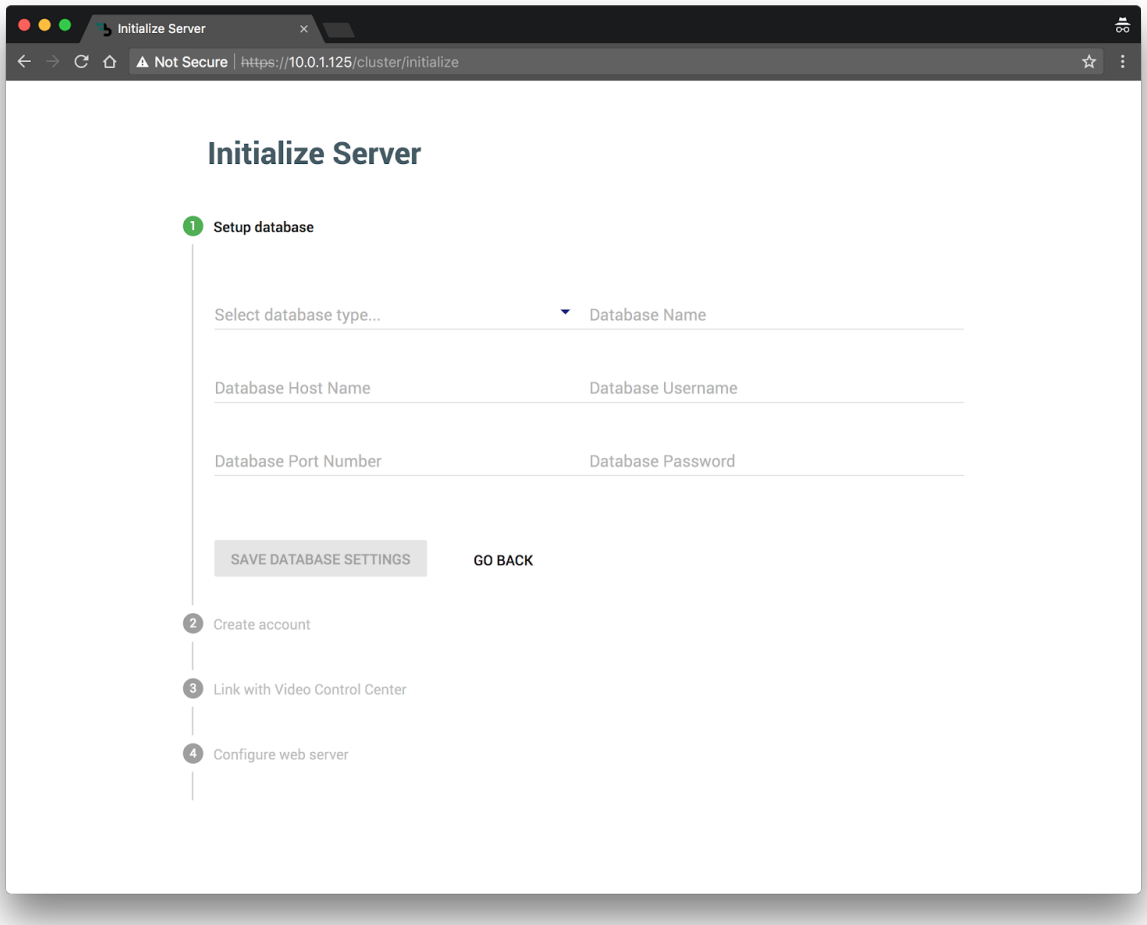
Visit the HTTPS **/cluster** path of the first node. If the node IP were **10.0.1.125,** the address would be **https://10.0.1.125/cluster**. Proceed through the SSL certificate warnings.

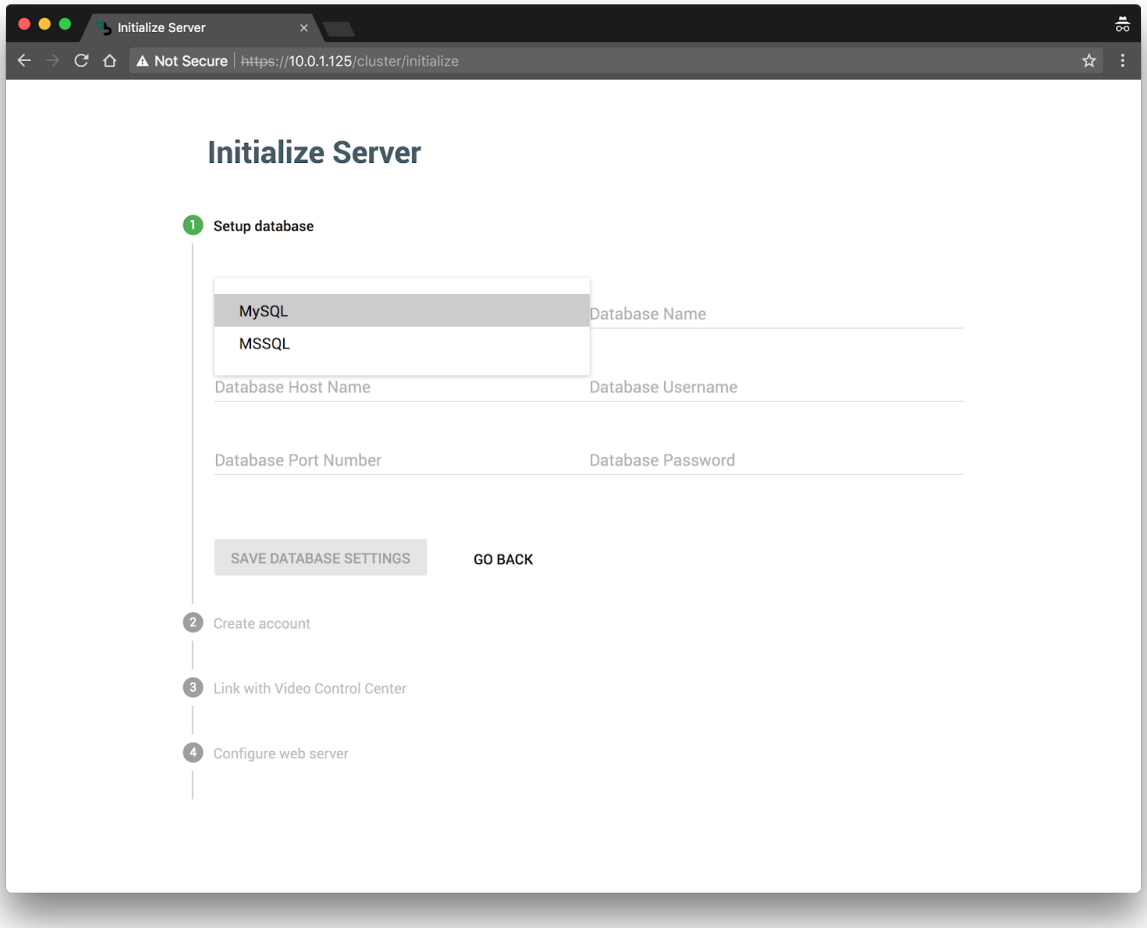


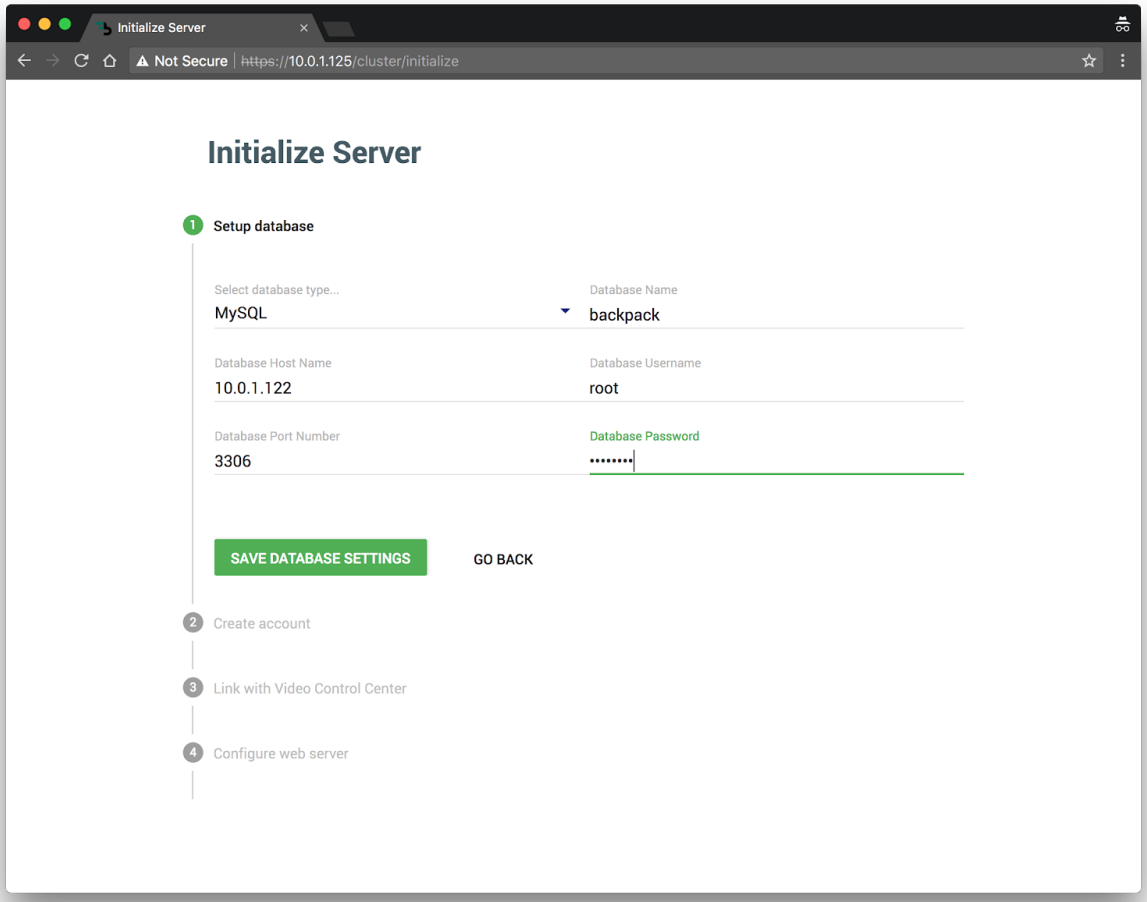
From the landing page, click on **Initialize Server**.



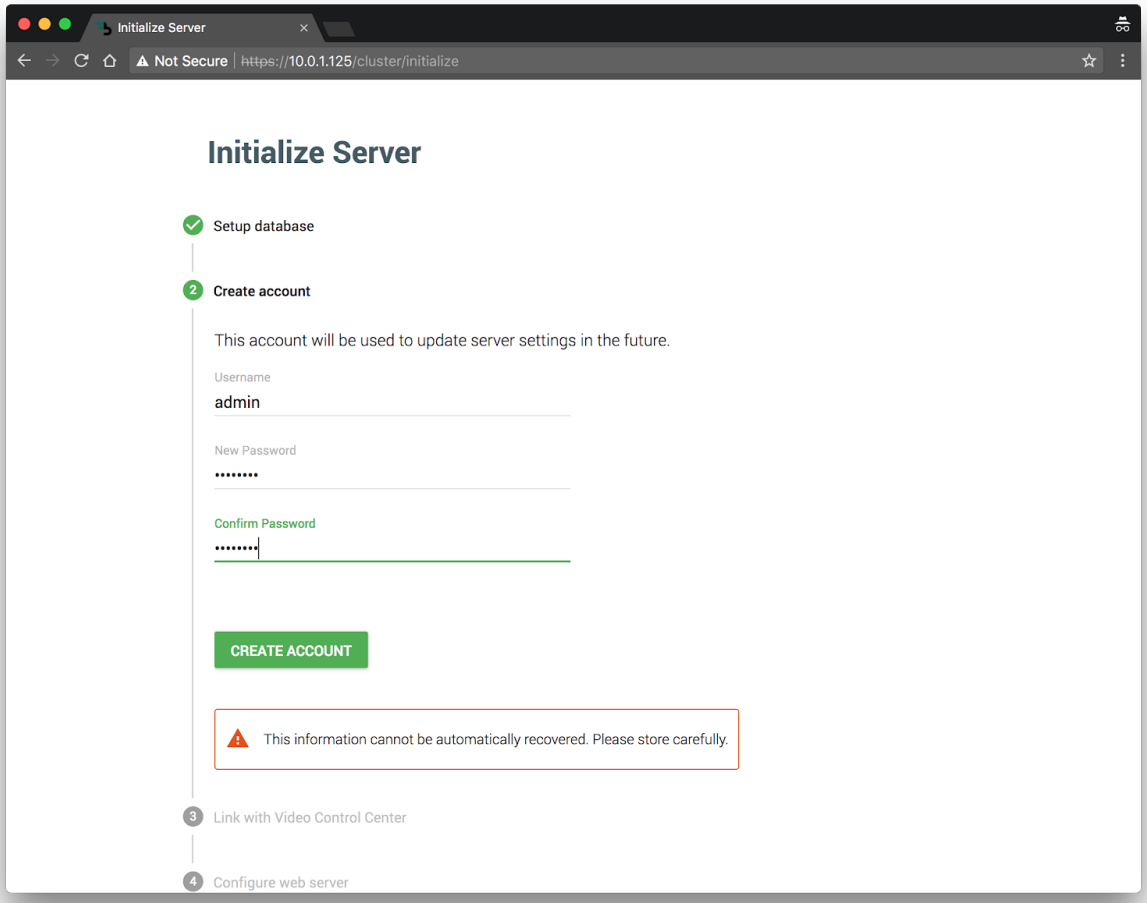
From **Initialize Server: Setup database**, enter the credentials of a previously set up MySQL or MSSQL database.



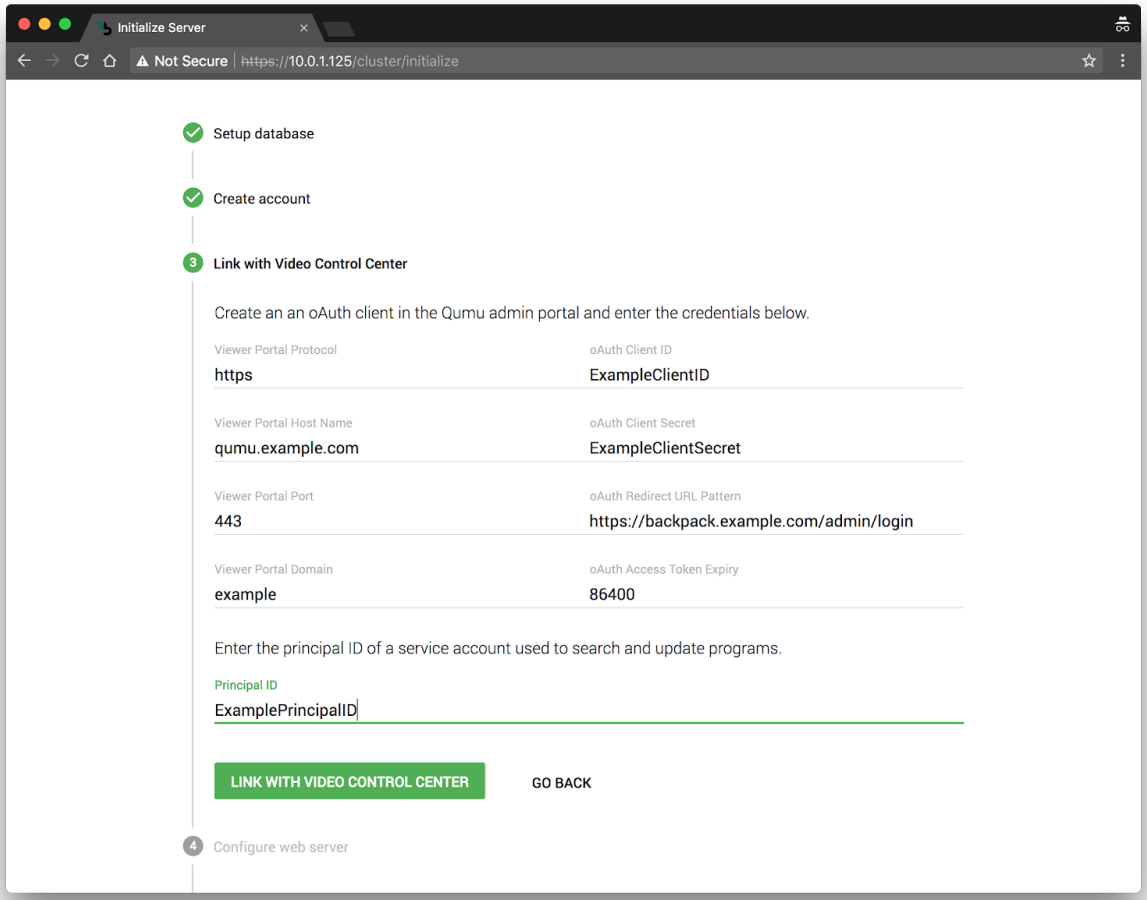

Initialize Server
Not Secure | https://10.0.1.125/cluster/initialize
Initialize Server
1 Setup database
MySQL
MSSQL
Database Name
Database Host Name
Database Username
Database Port Number
Database Password
SAVE DATABASE SETTINGS
GO BACK
2 Create account
3 Link with Video Control Center
4 Configure web server


Initialize Server
Not Secure
https://10.0.1.125/cluster/initialize
Initialize Server
1
Setup database
Select database type...
MySQL
Database Name
backpack
Database Host Name
10.0.1.122
Database Username
root
Database Port Number
3306
Database Password
SAVE DATABASE SETTINGS
GO BACK
2
Create account
3
Link with Video Control Center
4
Configure web server

From **Initialize Server: Create account**, enter a username and password to create an account for cluster administration. Please note this information cannot be automatically recovered.



From **Initialize Server: Link with Video Control Center**, enter the Qumu Viewer Portal network and domain information. Enter the credentials of an oAuth client previously set up in the Qumu Admin Portal, and a principal ID with administrative access.

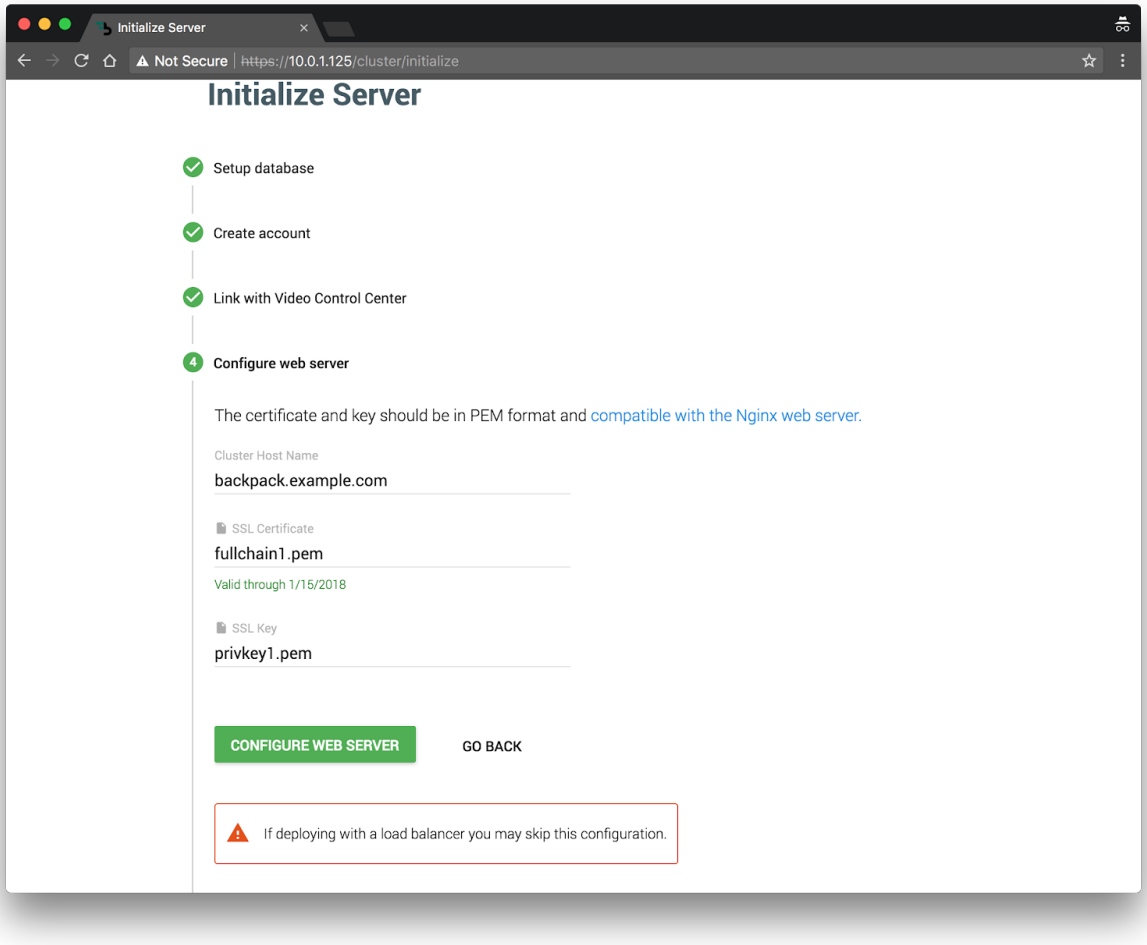


How to retrieve the principal ID from the Video Control Center:

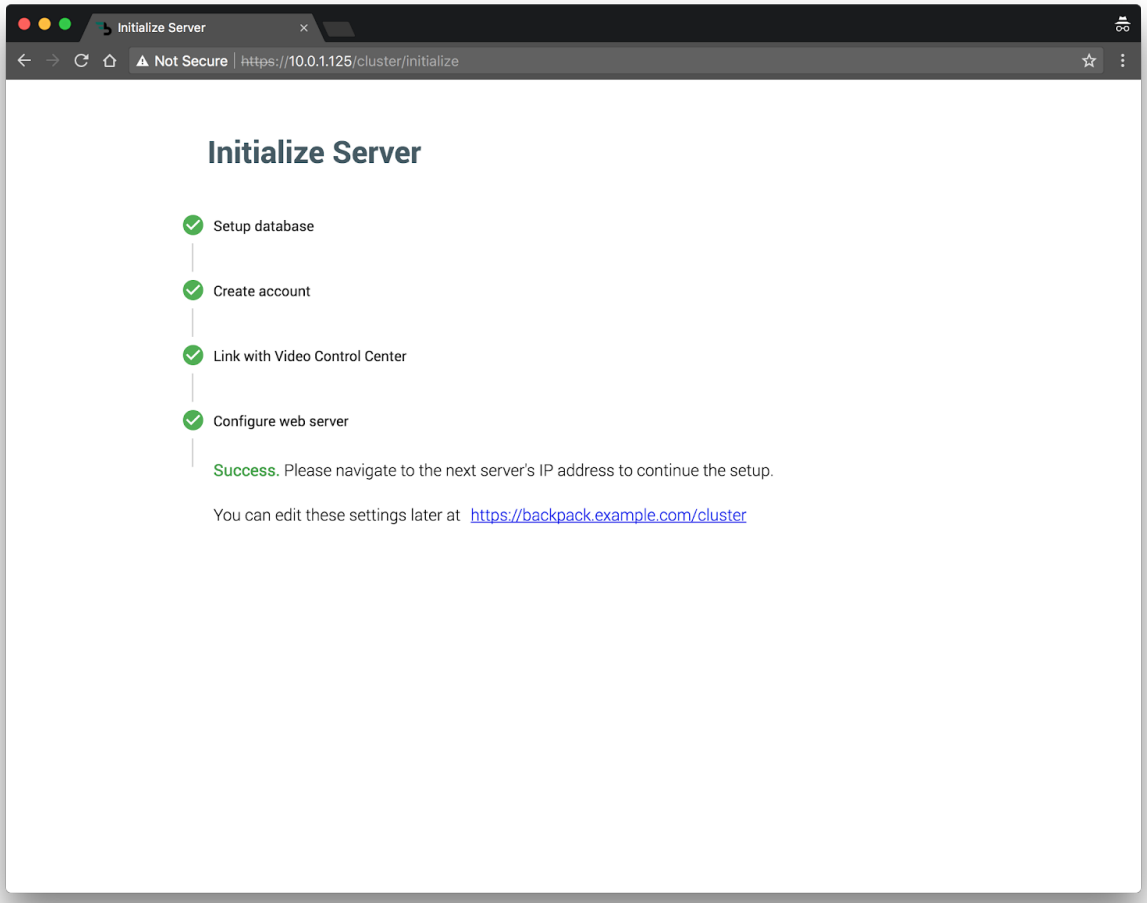
1) If the HTTPS path was **vcc.example.com** and the domain was **qumu**, the address would be:
https://vcc.example.com/viewerportal/services/rest/qumu/users/currentUser

2) The page should be displaying JSON data containing a field labeled **id**. Please enter the **id** into the **Principal ID** field in the setup screen.

From **Initialize Server: Configure web server**, enter the cluster hostname and associated SSL certificate and keys. These files should be compatible with the Nginx web server.

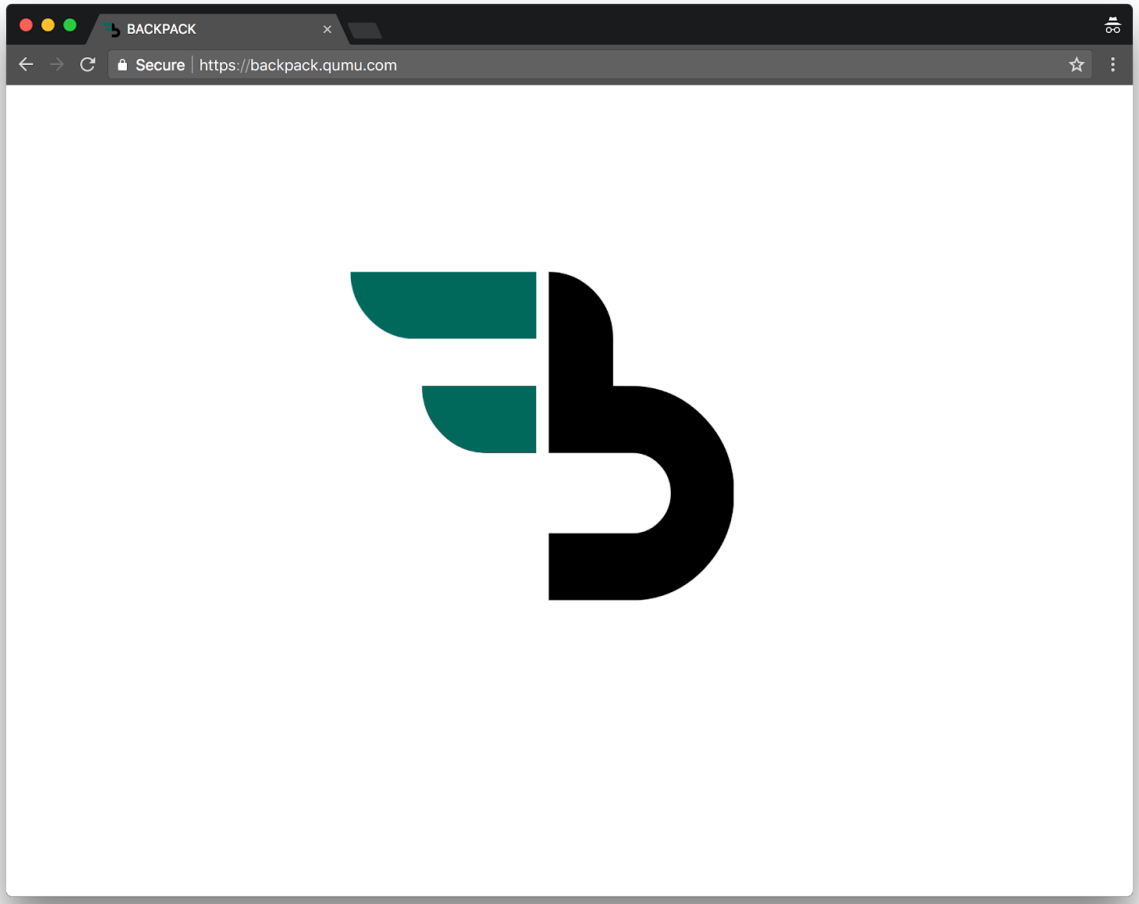


After completion, navigate to the next server's IP address to continue the setup. You can also click the link to navigate to server settings.



Verify DNS and SSL

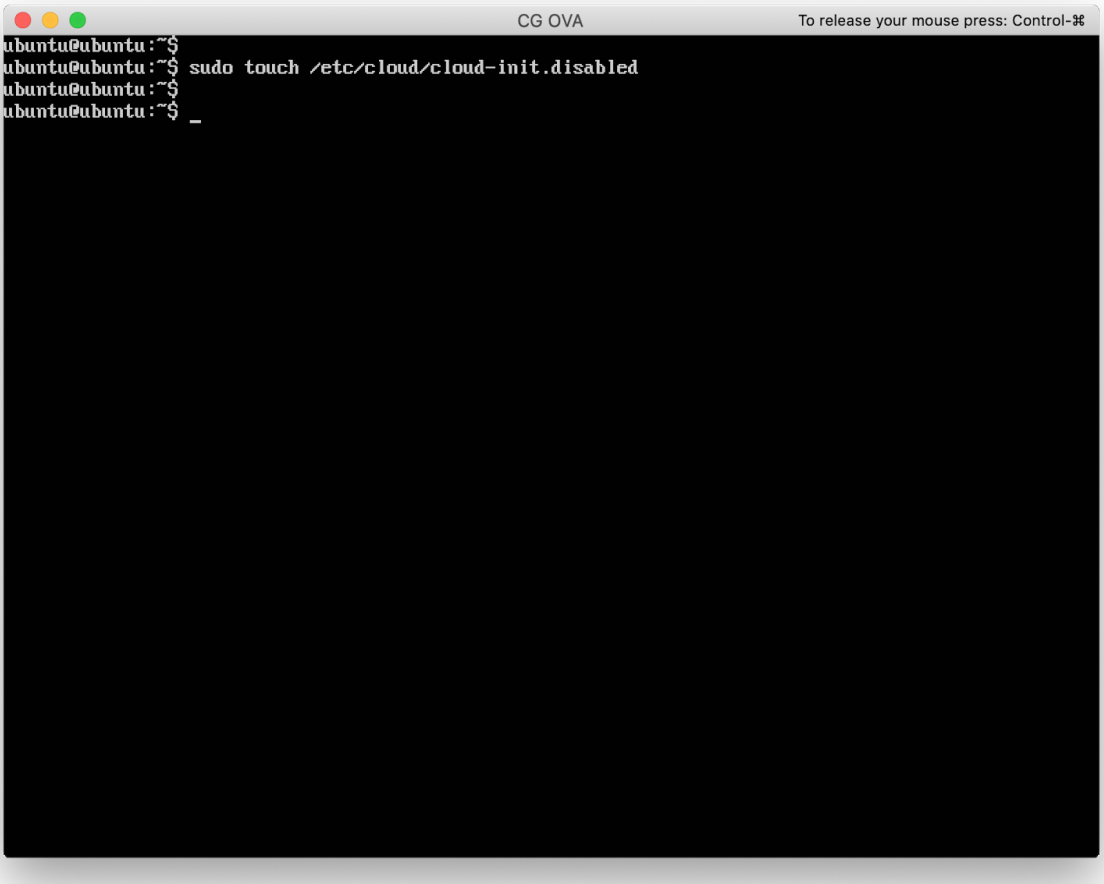
Navigate to the HTTPS designated cluster hostname to verify setup. If the cluster hostname were **backpack.example.com,** the address would be **https://backpack.example.com**



Disable Cloud-Init

Cloud-init is the service that initializes cloud images on EC2. However, it is not required when running the server on-premise. Disable cloud-init by running the following command,

```
sudo touch /etc/cloud/cloud-init.disabled
```

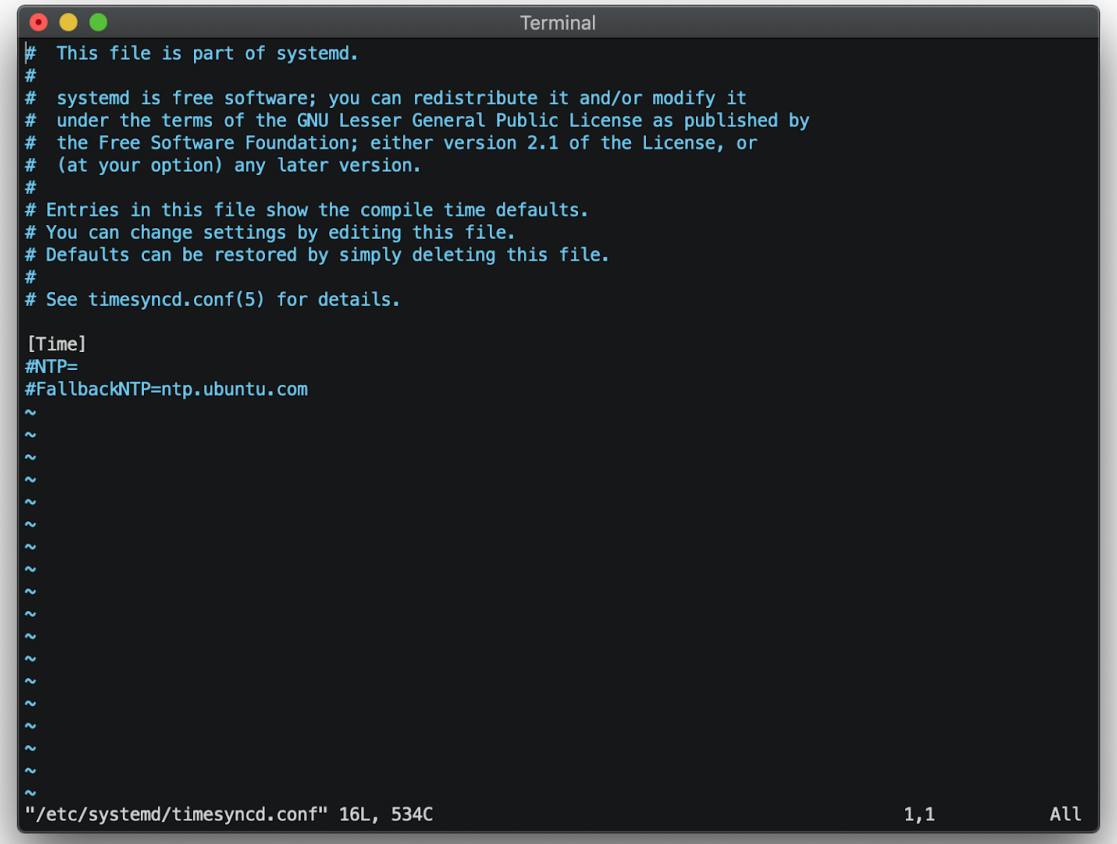


Set up Custom Timeserver (Optional)

Ubuntu 16.04 by default uses the time server at **ntp.ubuntu.com.**

To change the default server, paste the following command in the terminal to edit the configuration file in the VIM editor:

```
sudo vim /etc/systemd/timesyncd.conf
```



Uncomment the NTP line by removing the hash and enter the desired time server address. For example, if the NTP time server was **time.google.com**, the entry would be **NTP=time.google.com**

Quit the editor by hitting **ESC**, and type **:wq** to save and exit. Hit **Enter**. Restart the time server by running the following command in the terminal:

```
systemctl restart systemd-timesyncd
```

To check the status of the timeserver, run the following command in the terminal:

```
systemctl status systemd-timesyncd
```

Content Gateway Setup

Content Gateway Installer

Run through steps with screenshots

SSL Certificates

Convert .pem to .pfx
Run through steps in IIS with screenshots

SSL Certificates