



## Deployment Guide

Version 2.0.8

# Contents

<b>Copyright Notice</b>	<b>3</b>
<b>Document Revision History</b>	<b>4</b>
<b>OVA Download</b>	<b>5</b>
<b>OVA Deployment</b>	<b>6</b>
Preparations	6
Network	7
Port Usage	7
System Requirements	8
Supported Platforms	8
Cluster Size	8
Virtual Machine Configuration	8
Browsers	8
Deploying	9
<b>Cluster Setup</b>	<b>10</b>
Individual Node DNS Entries	10
SSL Certificates	10
OAuth Client	11
<b>Node Setup</b>	<b>14</b>
Network Setup (DHCP)	14
Network Setup (Static IP)	15
Initialize Cluster	24
Verify DNS and SSL	33
Disable Cloud-Init	34
<b>Content Gateway Setup</b>	<b>36</b>
Content Gateway Installer	36
SSL Certificates	36
SSL Certificates	36
<b>Content Gateway Setup</b>	<b>34</b>
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

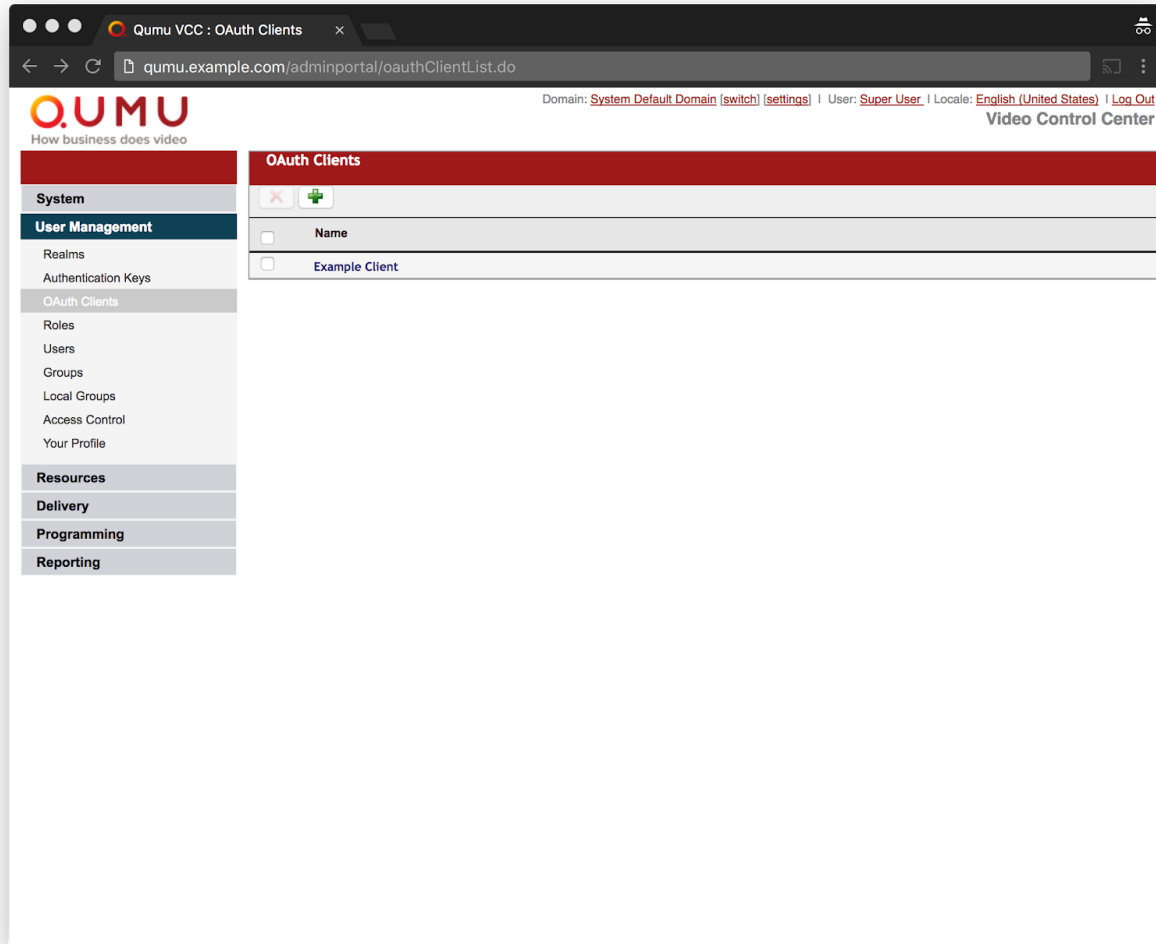
Individual nodes do not require distinct DNS entries but can be assigned one for administrative convenience.

## SSL Certificates

The SSL certificate and certificate key should be Nginx compatible. See - [http://nginx.org/en/docs/http/configuring\\_https\\_servers.html](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

The screenshot shows a web browser window with the address bar displaying `https://qumu.example.com/adminportal/oauthClientCreate.do`. The page title is "Qumu VCC : OAuth Clients". The main content area is titled "Add OAuth Client" and contains the following form fields:

- Client Id:** ExampleClientID \*
- Name:** Backpack \*
- Redirect URL Pattern:** `https://backpack.example.com/admin/log` \*
- Client Secret:** ExampleClientSecret \*
- Skip User Authorization:** ☒
- Access Token Expiry (seconds):** 86400 \*
- Implicit Token Expiry (seconds):** 86400 \*

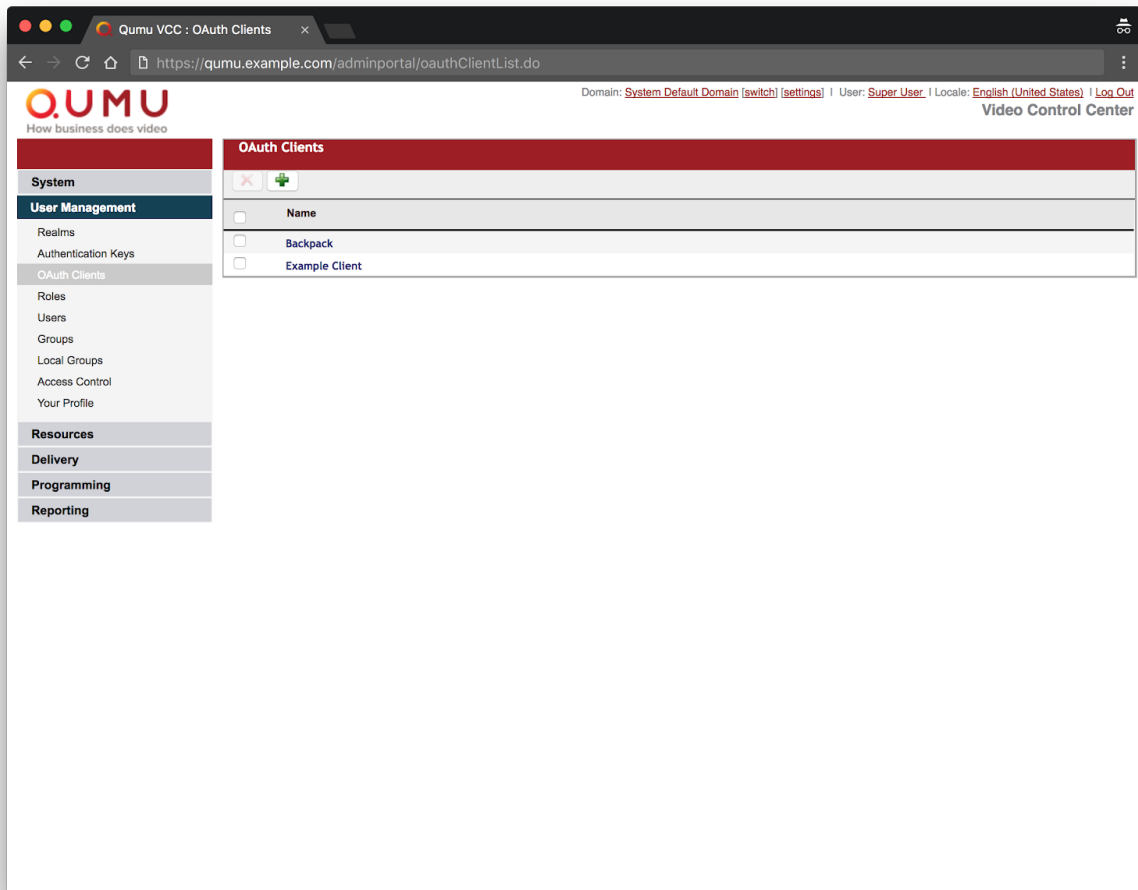
At the bottom of the form, there are two buttons: "Save" (with a green checkmark icon) and "Cancel".

The left sidebar contains a navigation menu with the following items:

- System
- User Management
- Realms
- Authentication Keys
- OAuth Clients
- Roles
- Users
- Groups
- Local Groups
- Access Control
- Your Profile
- Resources
- Delivery
- Programming
- Reporting

The top right of the page shows the user interface with the text: "Domain: System Default Domain [switch] [settings] | User: Super User | Locale: English (United States) | Log Out". Below this, it says "Video Control Center".

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)

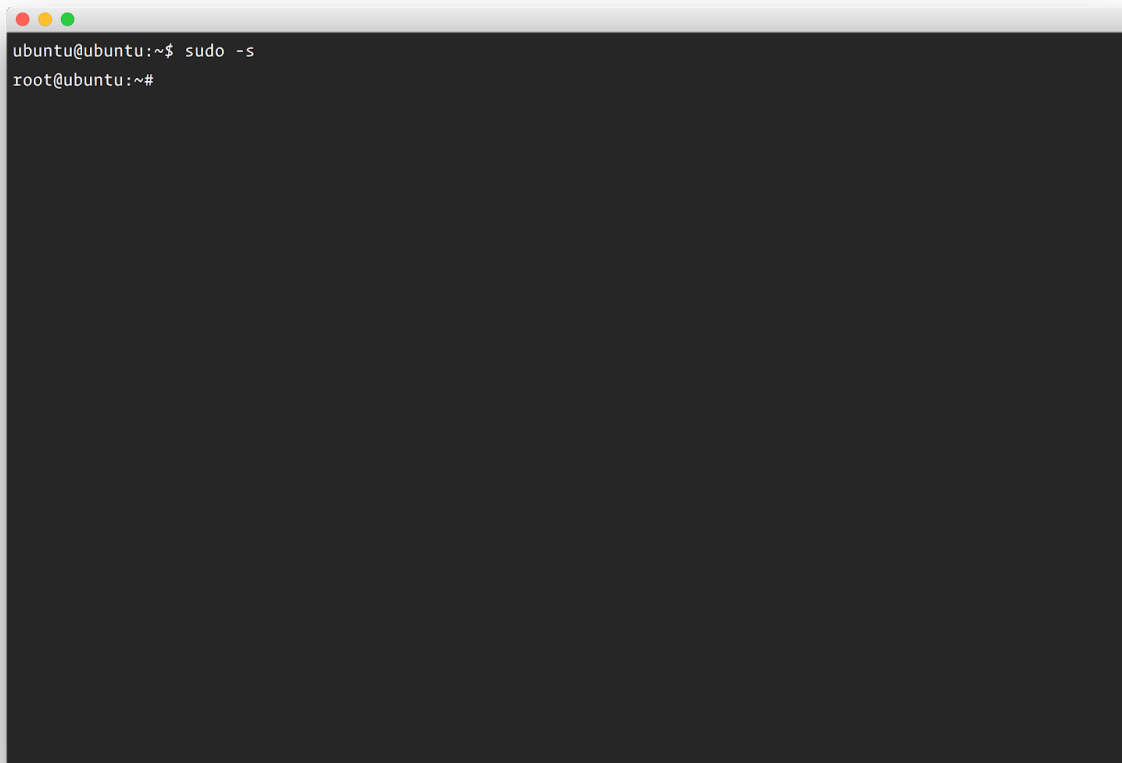
For systems with statically allocated IP addresses:

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

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

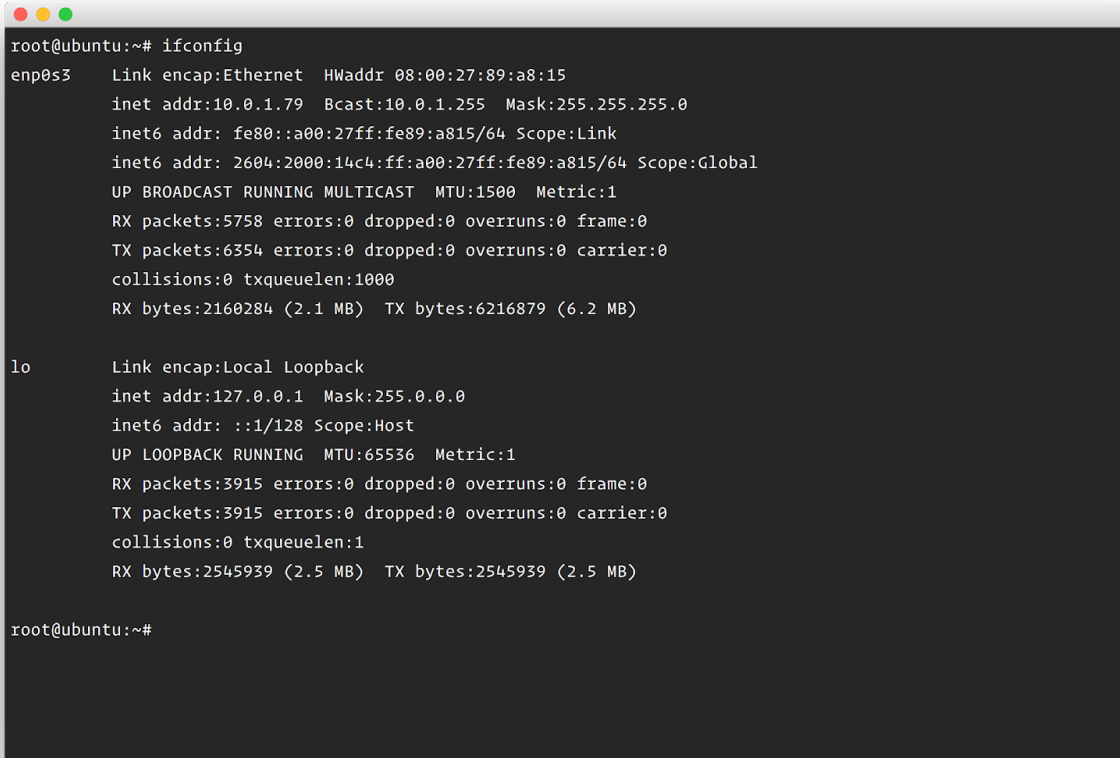
3. Run the following command to switch to 'root' user:

```
sudo -s
```



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

```
ifconfig
```



```
root@ubuntu:~# ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:89:a8:15
        inet addr:10.0.1.79  Bcast:10.0.1.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe89:a815/64 Scope:Link
        inet6 addr: 2604:2000:14c4:ff:a00:27ff:fe89:a815/64 Scope:Global
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:5758 errors:0 dropped:0 overruns:0 frame:0
        TX packets:6354 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:2160284 (2.1 MB)  TX bytes:6216879 (6.2 MB)

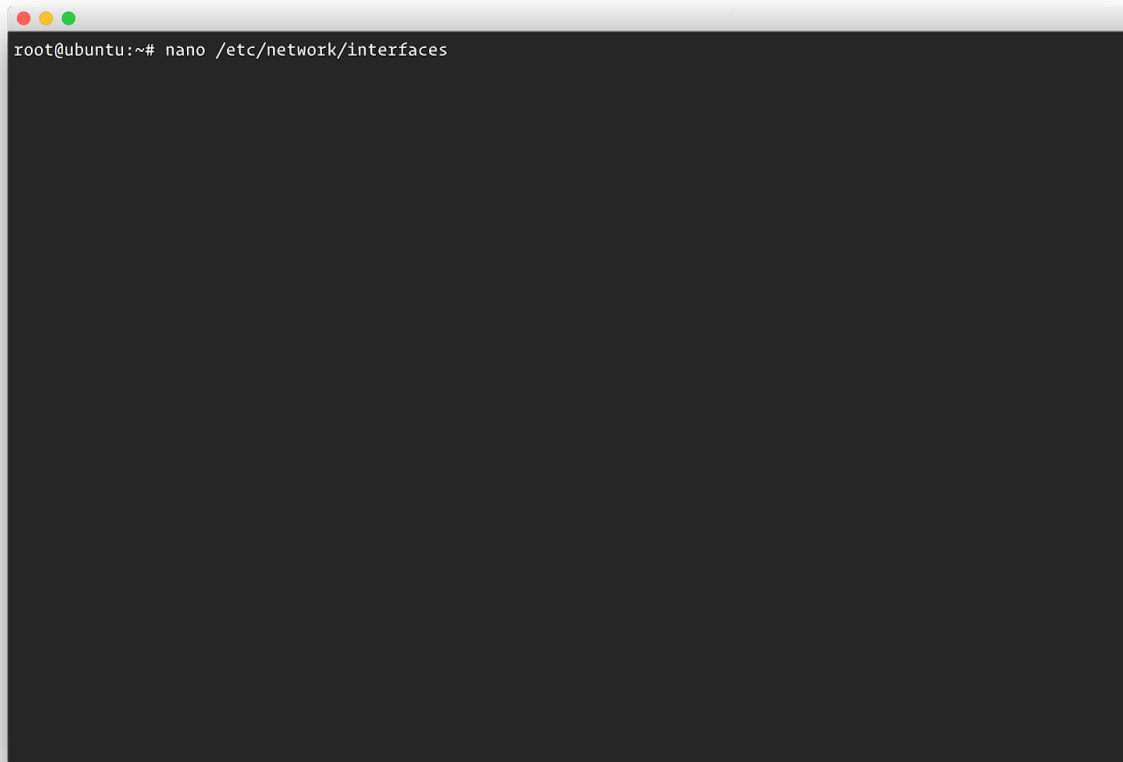
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:3915 errors:0 dropped:0 overruns:0 frame:0
        TX packets:3915 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:2545939 (2.5 MB)  TX bytes:2545939 (2.5 MB)

root@ubuntu:~#
```



5. Open the network configuration file for editing:

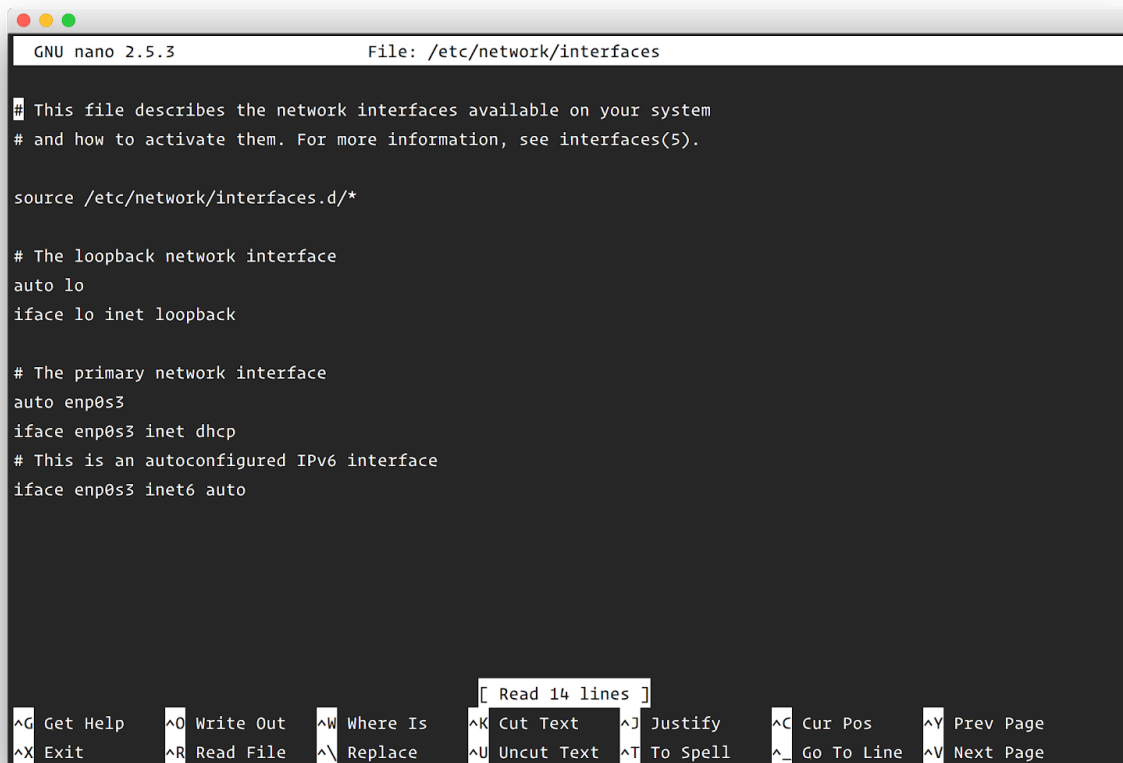
```
nano /etc/network/interfaces
```



## 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
```



```
GNU nano 2.5.3      File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# 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
```

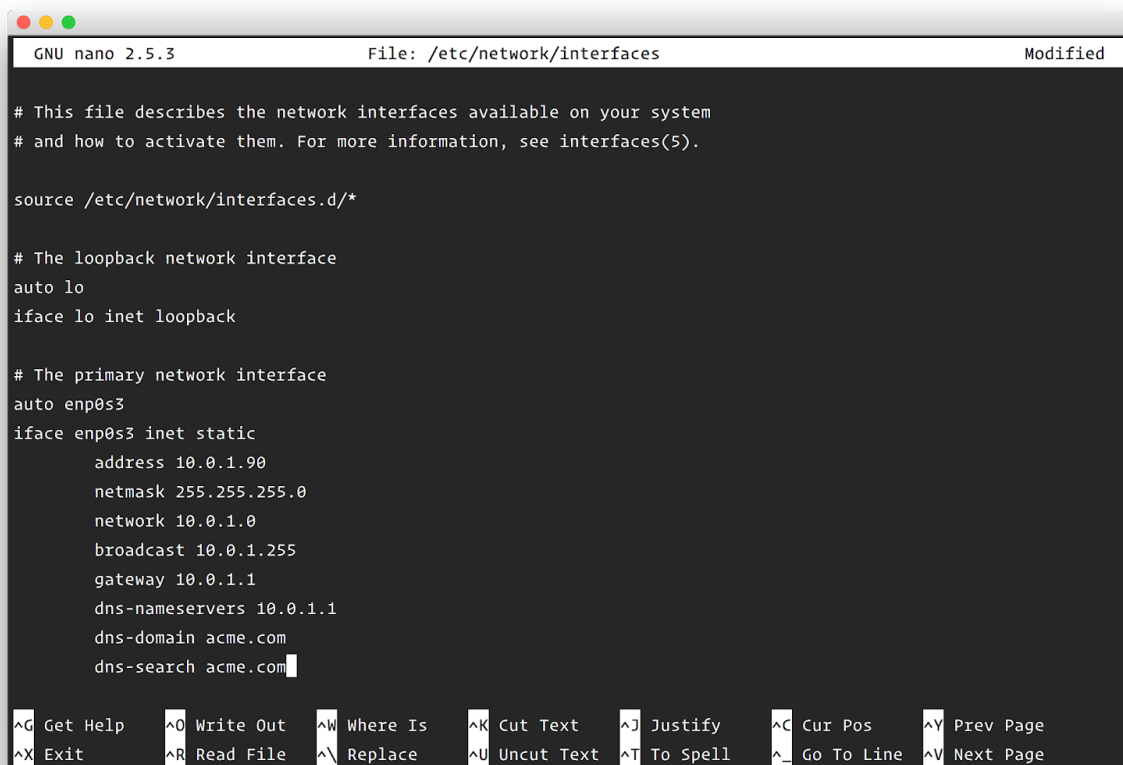
[ Read 14 lines ]

<b>^G</b> Get Help	<b>^O</b> Write Out	<b>^W</b> Where Is	<b>^K</b> Cut Text	<b>^J</b> Justify	<b>^C</b> Cur Pos	<b>^Y</b> Prev Page
<b>^X</b> Exit	<b>^R</b> Read File	<b>^_</b> Replace	<b>^U</b> Uncut Text	<b>^T</b> To Spell	<b>^_</b> Go To Line	<b>^V</b> Next Page

- 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
```



The screenshot shows a terminal window with the GNU nano 2.5.3 text editor. The title bar indicates the file being edited is `/etc/network/interfaces` and it has been modified. The editor's content matches the configuration shown in the previous block, including comments about the loopback and primary network interfaces, and their respective settings. The bottom of the window displays a row of keyboard shortcuts for various editing actions.

```
GNU nano 2.5.3      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

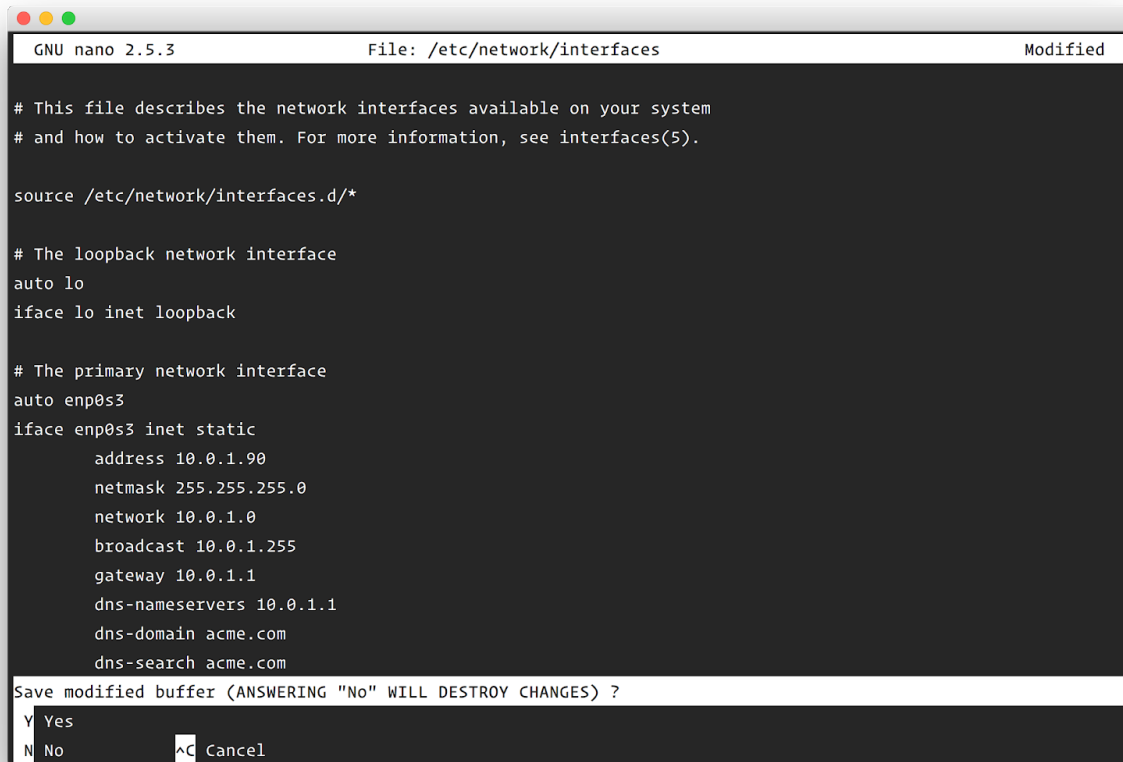
source /etc/network/interfaces.d/*

# 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

^G Get Help      ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      ^Y Prev Page
^X Exit          ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line    ^V Next Page
```

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



```
GNU nano 2.5.3      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

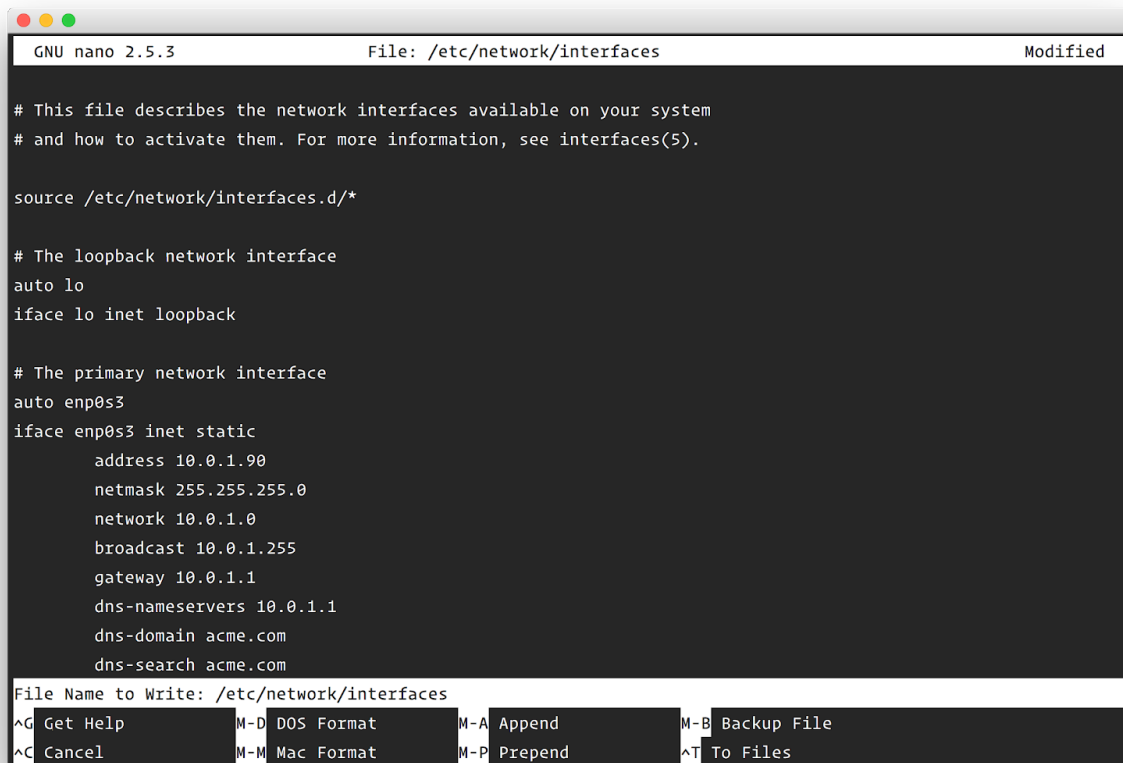
source /etc/network/interfaces.d/*

# 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

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Y Yes
N No      ^C Cancel
```

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



```
GNU nano 2.5.3      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

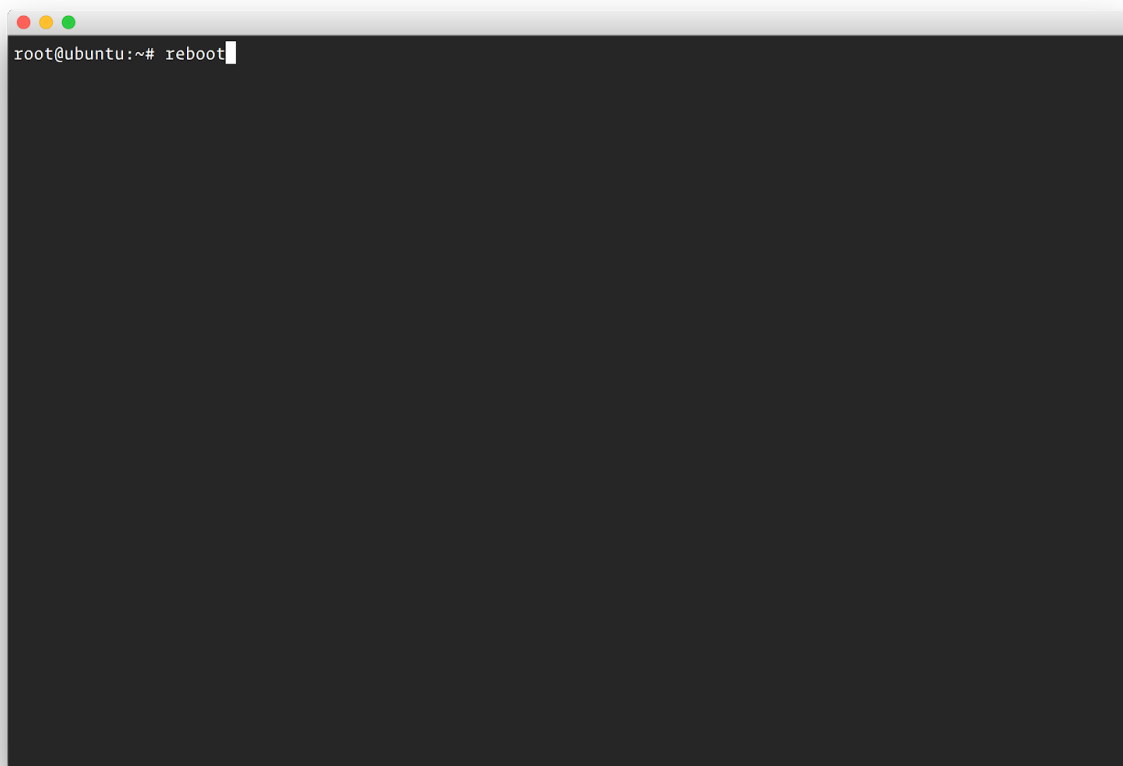
# The loopback network interface
auto lo
iface lo inet loopback

# 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

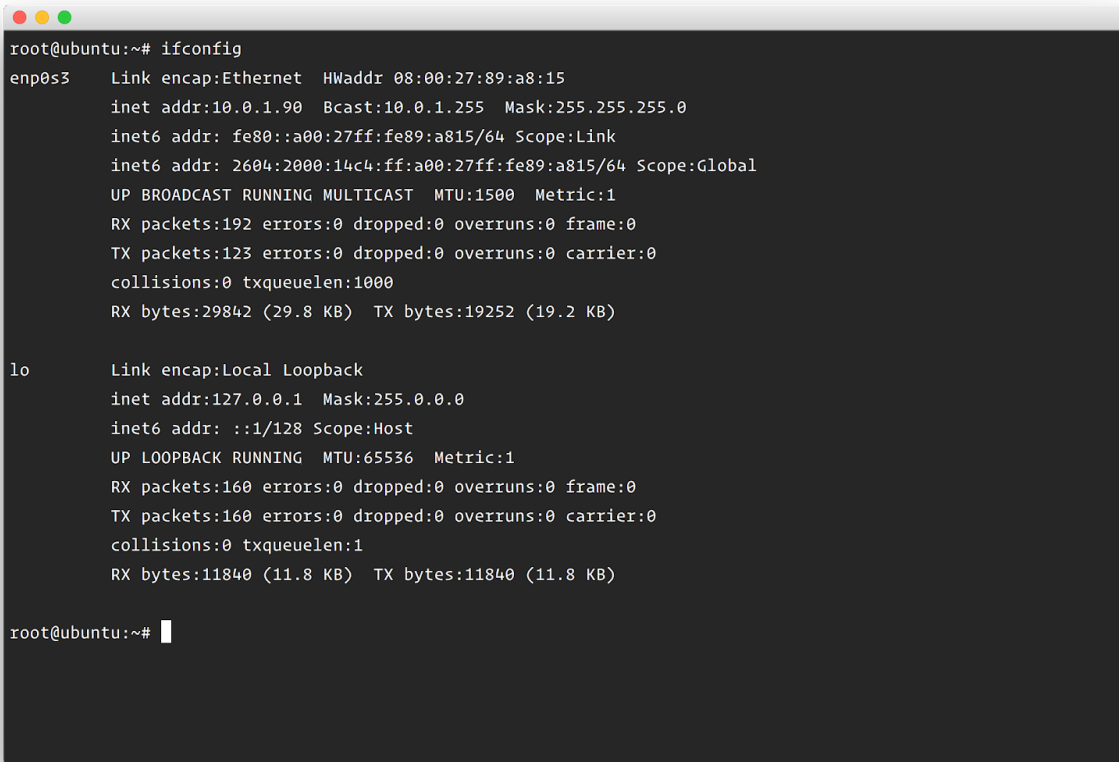
File Name to Write: /etc/network/interfaces
^G Get Help      M-D DOS Format  M-A Append      M-B Backup File
^C Cancel        M-M Mac Format  M-P Prepend     ^T To Files
```

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](https://[configured IP address]/cluster) in a web browser and check for the cluster setup screen.



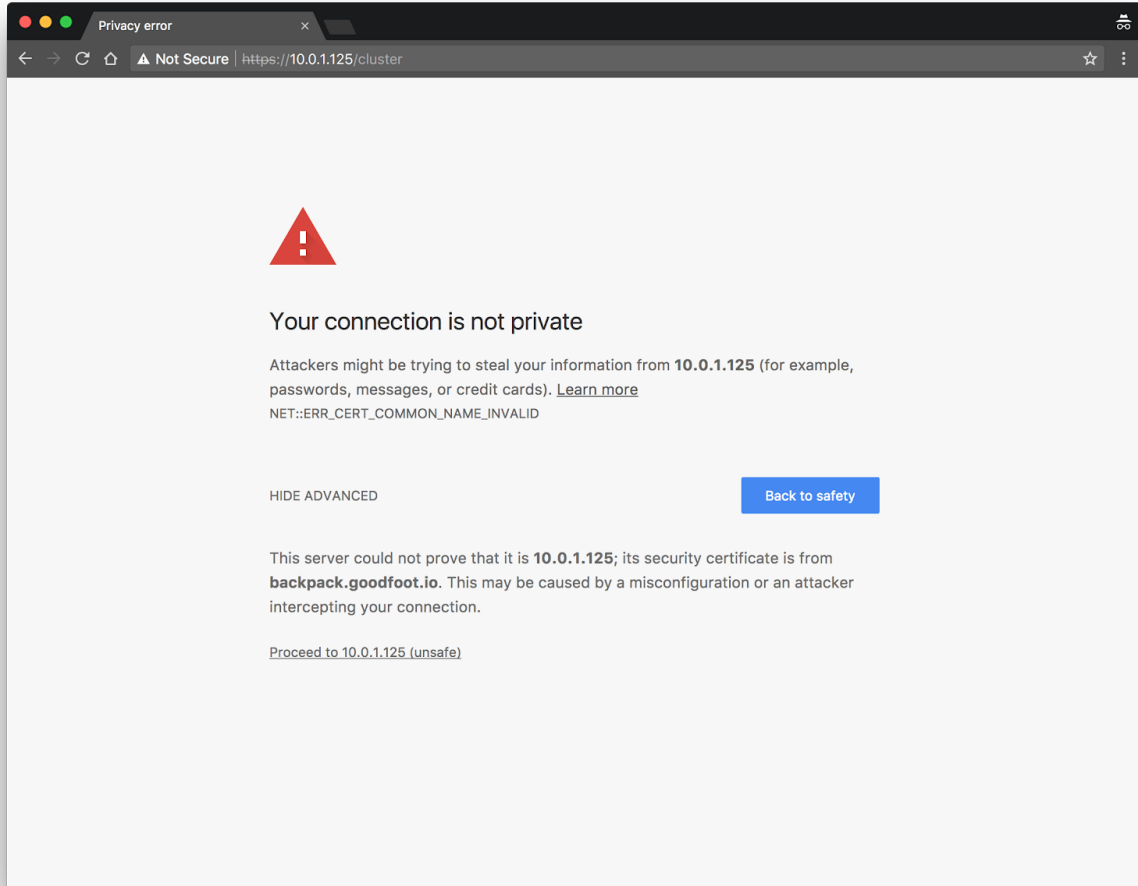
```
root@ubuntu:~# ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:89:a8:15
        inet addr:10.0.1.90  Bcast:10.0.1.255  Mask:255.255.255.0
        inet6 addr: fe80::a00:27ff:fe89:a815/64 Scope:Link
        inet6 addr: 2604:2000:14c4:ff:a00:27ff:fe89:a815/64 Scope:Global
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:192 errors:0 dropped:0 overruns:0 frame:0
        TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:29842 (29.8 KB)  TX bytes:19252 (19.2 KB)

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:65536  Metric:1
        RX packets:160 errors:0 dropped:0 overruns:0 frame:0
        TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:11840 (11.8 KB)  TX bytes:11840 (11.8 KB)

root@ubuntu:~#
```

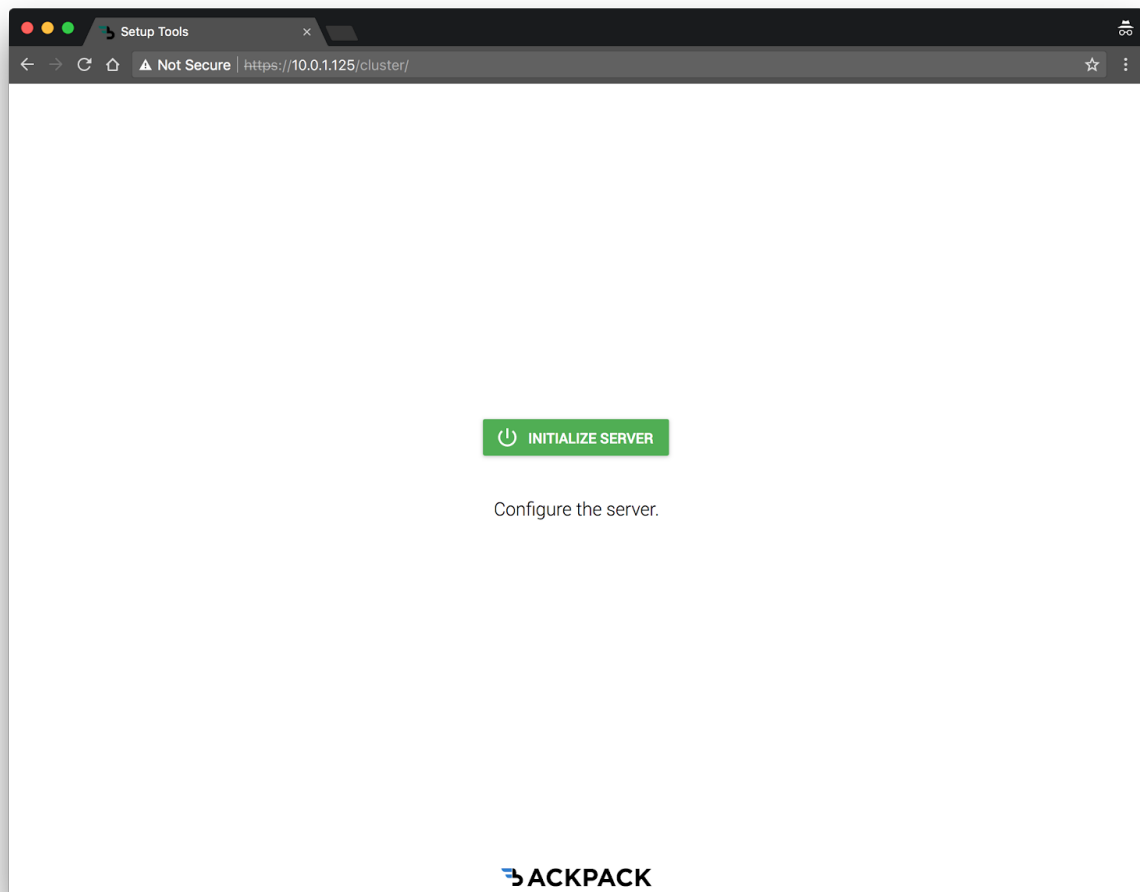
## Initialize Cluster

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.

The screenshot shows a web browser window titled "Initialize Server" with the URL `https://10.0.1.125/cluster/initialize`. The page has a dark header bar with the title and a close button. Below the header, the main content area is titled "Initialize Server". A vertical progress bar on the left side of the page indicates four steps: 1. Setup database (highlighted with a green circle), 2. Create account, 3. Link with Video Control Center, and 4. Configure web server. The "Setup database" step contains a form with the following fields: "Select database type..." (a dropdown menu), "Database Name" (a text input field), "Database Host Name" (a text input field), "Database Username" (a text input field), "Database Port Number" (a text input field), and "Database Password" (a text input field). Below the form, there are two buttons: "SAVE DATABASE SETTINGS" and "GO BACK".

**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

The screenshot shows a web browser window titled "Initialize Server" with the URL `https://10.0.1.125/cluster/initialize`. The page has a dark header bar with the title and a close button. Below the header, the main content area is white and features the title "Initialize Server" in a large, bold, dark font. A vertical progress indicator on the left side of the form shows four steps: "1 Setup database" (highlighted with a green circle), "2 Create account", "3 Link with Video Control Center", and "4 Configure web server". The "Setup database" section contains several input fields: "Select database type..." with a dropdown menu showing "MySQL"; "Database Name" with a dropdown menu showing "backpack"; "Database Host Name" with a text input field containing "10.0.1.122"; "Database Username" with a text input field containing "root"; "Database Port Number" with a text input field containing "3306"; and "Database Password" with a text input field containing "\*\*\*\*\*". Below these fields are two buttons: a green "SAVE DATABASE SETTINGS" button and a grey "GO BACK" button.

## Initialize Server

- 1 Setup database**
- 2 Create account
- 3 Link with Video Control Center
- 4 Configure web server

Select database type...  
MySQL

Database Name  
backpack

Database Host Name  
10.0.1.122

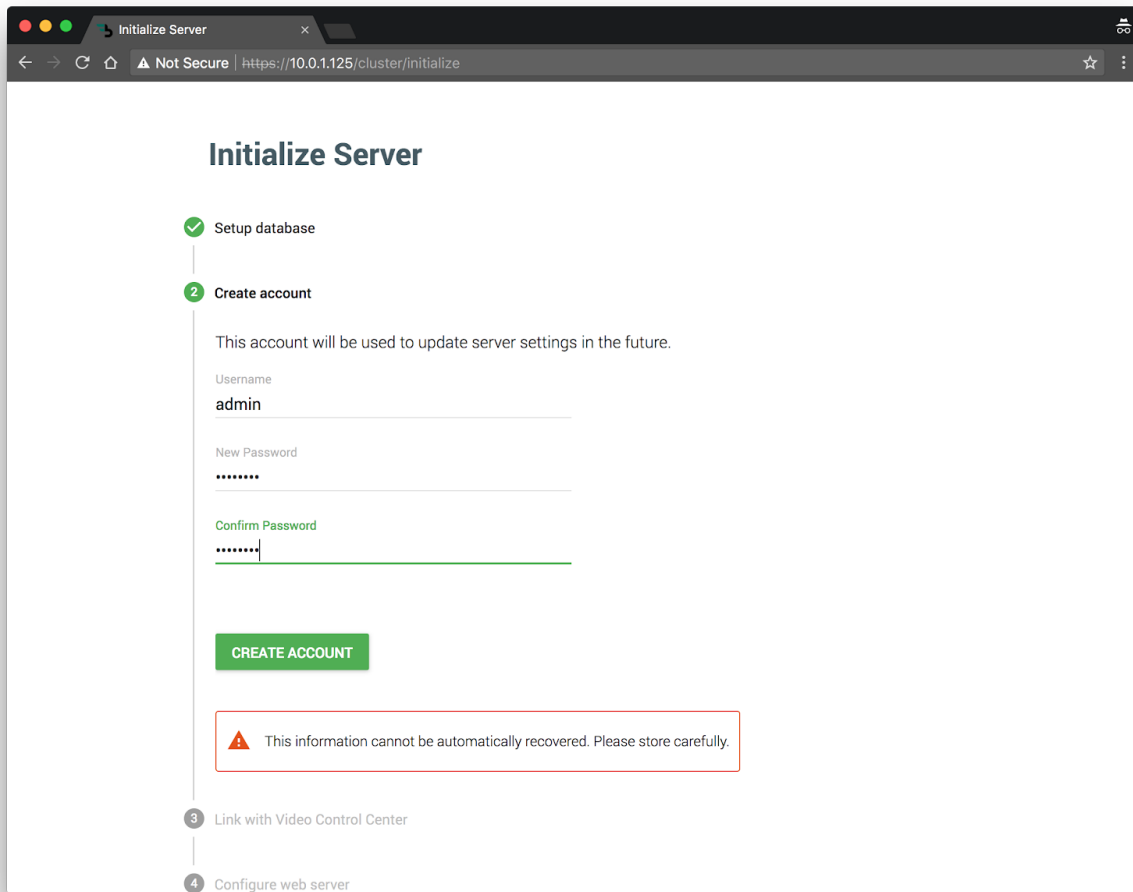
Database Username  
root

Database Port Number  
3306

Database Password  
\*\*\*\*\*

**SAVE DATABASE SETTINGS** GO BACK

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.



The screenshot shows a web browser window titled "Initialize Server" with the URL "https://10.0.1.125/cluster/initialize". The page has a dark header bar with the title and a "Not Secure" warning. The main content area is white and features a progress indicator on the left with four steps: "Setup database" (completed), "Create account" (active), "Link with Video Control Center", and "Configure web server". The "Create account" step includes a sub-header "Create account" and a note: "This account will be used to update server settings in the future." Below this are three input fields: "Username" with the value "admin", "New Password" with masked characters, and "Confirm Password" with masked characters. A green "CREATE ACCOUNT" button is positioned below the password fields. A red-bordered warning box at the bottom of the form states: "⚠ This information cannot be automatically recovered. Please store carefully."

## Initialize Server

- ✓ Setup database
- 2 Create account
- 3 Link with Video Control Center
- 4 Configure web server

This account will be used to update server settings in the future.

Username  
**admin**

New Password  
.....

Confirm Password  
.....

**CREATE ACCOUNT**

⚠ This information cannot be automatically recovered. Please store carefully.

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.

The screenshot shows a web browser window titled 'Initialize Server' with the URL 'https://10.0.1.125/cluster/initialize'. The page displays a progress bar with four steps: 'Setup database' (checked), 'Create account' (checked), 'Link with Video Control Center' (active), and 'Configure web server' (next). The active step contains the following form fields:

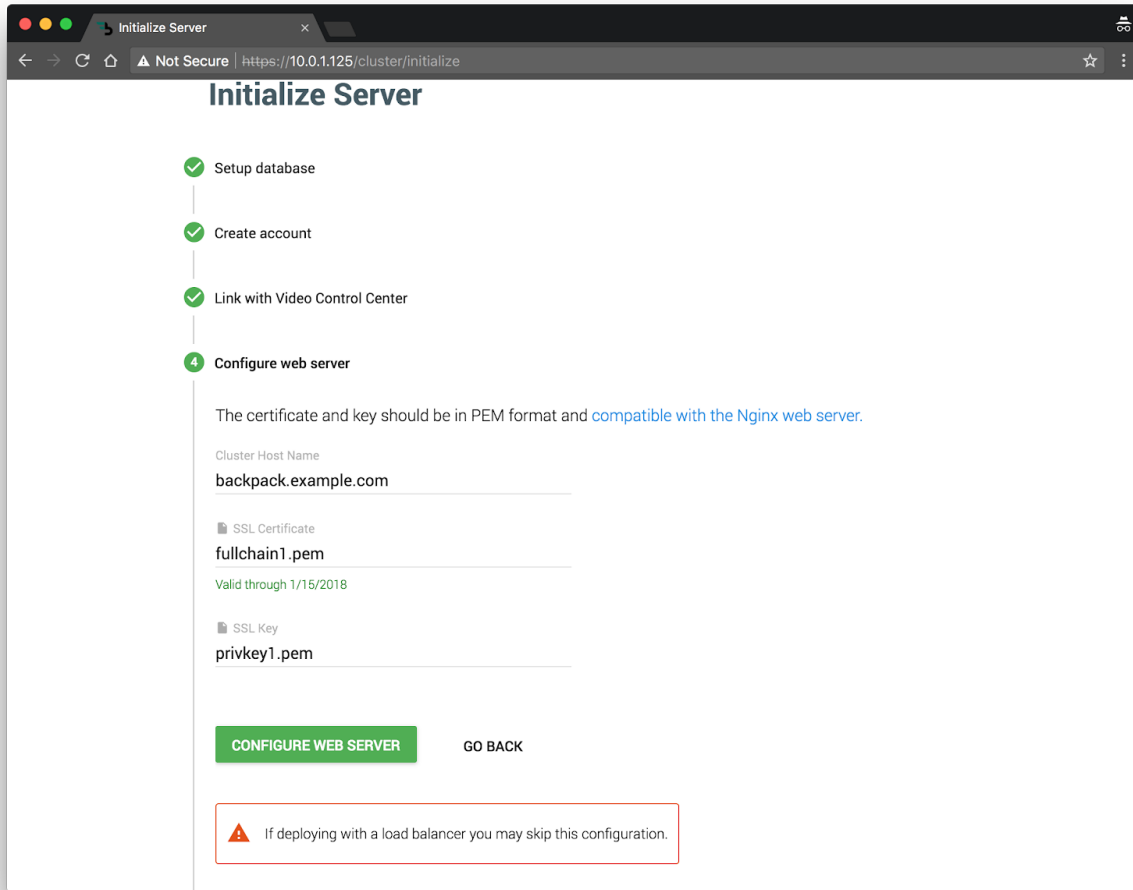
Viewer Portal Protocol	oAuth Client ID
https	ExampleClientID
Viewer Portal Host Name	oAuth Client Secret
qumu.example.com	ExampleClientSecret
Viewer Portal Port	oAuth Redirect URL Pattern
443	https://backpack.example.com/admin/login
Viewer Portal Domain	oAuth Access Token Expiry
example	86400

Below the form, there is a text prompt: 'Enter the principal ID of a service account used to search and update programs.' followed by a 'Principal ID' label and a text input field containing 'ExamplePrincipalID'. At the bottom of the form, there are two buttons: 'LINK WITH VIDEO CONTROL CENTER' (green) and 'GO BACK'.

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](#).



The screenshot shows a web browser window titled "Initialize Server" with the URL "https://10.0.1.125/cluster/initialize". The page has a dark header bar with the title and a "Not Secure" warning. The main content area is white and features a vertical progress bar on the left with four steps: "Setup database", "Create account", "Link with Video Control Center", and "4 Configure web server". The "Configure web server" step is active and highlighted. Below the progress bar, there is a text instruction: "The certificate and key should be in PEM format and [compatible with the Nginx web server](#)." Below this, there are three input fields: "Cluster Host Name" with the value "backpack.example.com", "SSL Certificate" with the value "fullchain1.pem" and a note "Valid through 1/15/2018", and "SSL Key" with the value "privkey1.pem". At the bottom of the form, there are two buttons: a green "CONFIGURE WEB SERVER" button and a grey "GO BACK" button. A red-bordered warning box at the bottom contains a warning icon and the text: "If deploying with a load balancer you may skip this configuration."

**Initialize Server**

- ✓ Setup database
- ✓ Create account
- ✓ Link with Video Control Center
- 4 Configure web server**

The certificate and key should be in PEM format and [compatible with the Nginx web server](#).

Cluster Host Name  
backpack.example.com

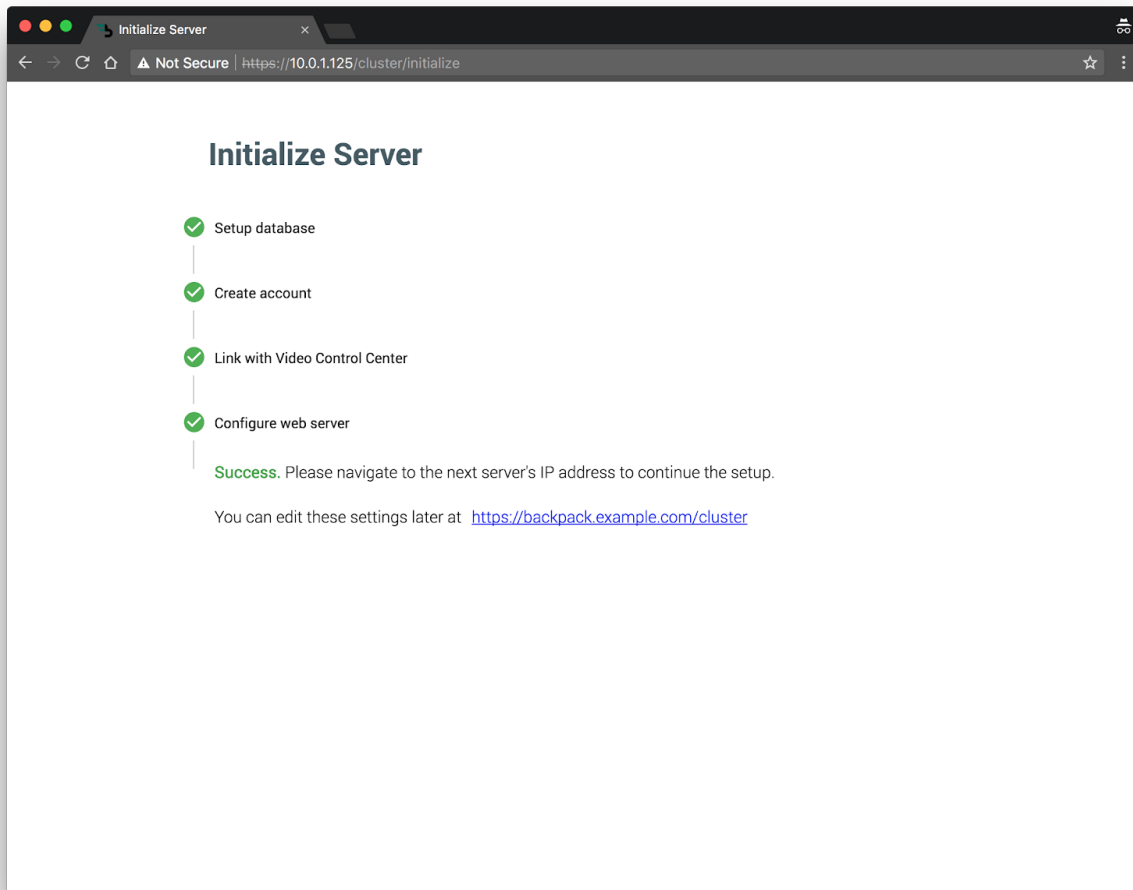
SSL Certificate  
fullchain1.pem  
Valid through 1/15/2018

SSL Key  
privkey1.pem

**CONFIGURE WEB SERVER** GO BACK

⚠ If deploying with a load balancer you may skip this configuration.

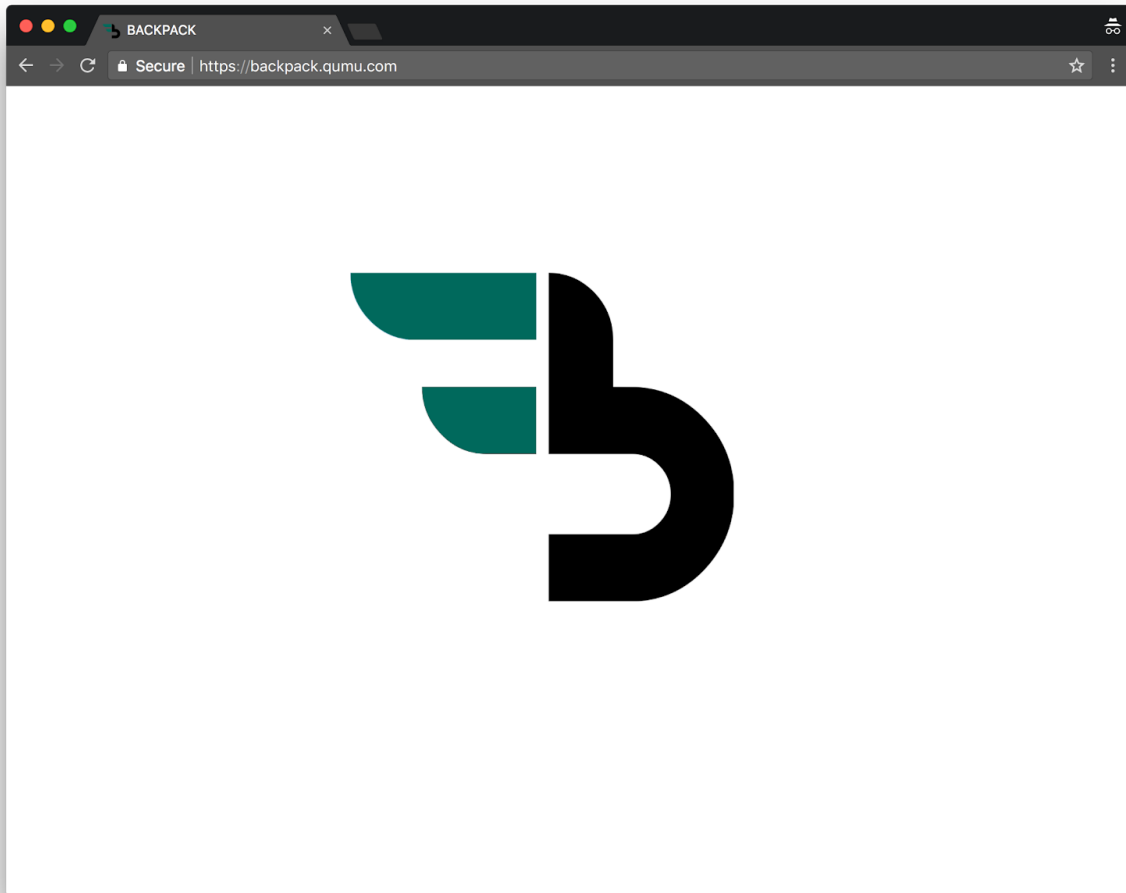
After completion, navigate to the next server's IP address to continue the setup. You can also click the link to navigate to server settings.





## Verify DNS and SSL

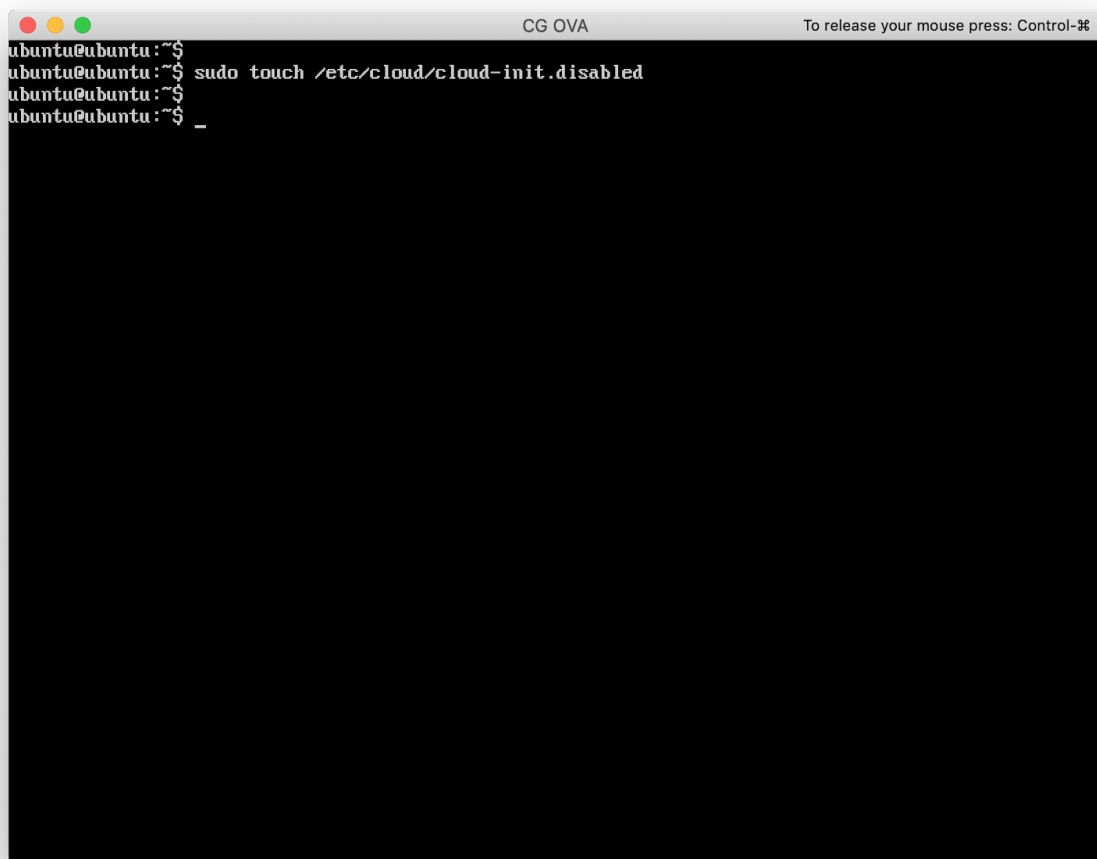
Navigate to the HTTPS designated cluster hostname to verify setup. If the cluster hostname were **backpack.example.com**, the address would be **https://backpack.example.com**



## 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
```

A terminal window titled "CG OVA" with a subtitle "To release your mouse press: Control-⌘". The terminal shows the following commands and output:

```
ubuntu@ubuntu:~$  
ubuntu@ubuntu:~$ sudo touch /etc/cloud/cloud-init.disabled  
ubuntu@ubuntu:~$  
ubuntu@ubuntu:~$ _
```



# 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