



Cluster Deployment Guide

Version 1.8.0

Contents

Copyright Notice	3
Document Revision History	4
OVA Download	5
OVA Deployment	6
Preparations	6
Network	7
Port Usage Outside of Cluster Group	7
Port Usage Inside of Cluster Group	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
Load Balancing	10
Round-Robin DNS	10
Hardware (Websocket Enabled)	10
SSL Certificates	10
OAuth Client	11
Node Setup	14
Network Setup (DHCP)	14
Network Setup (Static IP)	15
Initialize Cluster	23
Join Nodes to Cluster	29
Verify DNS and SSL	33
Disable Cloud-Init	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

February 11th, 2017

- Initial release of documentation.

May 31st, 2017

- Port 22 requirement for cluster administration.
- Node setup screenshots.

June 12th, 2017

- Network setup information.

June 20th, 2017

- Static IP network setup instructions.

July 11th, 2017

- OAuth client creation.

September 9th, 2017

- Specify supported VCC platform.

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.

<https://qumu-software.s3.amazonaws.com/beam-cluster.latest.ova>

OVA Deployment

Preparations

To set up Beam, you must have:

- Beam OVA
- Supported virtual infrastructure
- IP addresses of cluster nodes
- Nginx compatible SSL certificate and SSL certificate key

OVA Deployment

Network

Port Usage Outside of Cluster Group

Protocol	Port	Direction	Purpose
HTTPS	443	Inbound	Beam API
HTTPS	443	Outbound	VCC API
SSH	22	Inbound/Outbound	Cluster administration

Port Usage Inside of Cluster Group

Protocol	Port	Direction	Purpose
TCP	4369	Inbound/Outbound	Time series database (epmd)
TCP	8087	Inbound/Outbound	Time series database (client)
TCP	8099	Inbound/Outbound	Time series database (handoff)
TCP	6000-7999	Inbound/Outbound	Time series database (peer)
TCP	26379	Inbound/Outbound	Cluster messaging
HTTPS	443	Inbound/Outbound	Beam API
SSH	22	Inbound/Outbound	Cluster administration

OVA Deployment

System Requirements

Supported Platforms

- VMware ESXI 5.5 and later
- Qumu VCC 7.5 and later

Cluster Size

The recommended size of a Beam cluster is 5 nodes on 5 distinct physical hosts.

Virtual Machine Configuration

The minimum requirements for a Beam cluster node are:

CPU: 3 GHz dual core or 4 virtual processors

RAM: 8 GB

STORAGE: 80GB

The recommended requirements for a Beam cluster node are:

CPU: 3 GHz quad core or 8 virtual processors

RAM: 12 GB

STORAGE: 120GB, low-latency SATA or SSD drives

Browsers

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

Beam 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.

Load Balancing

Nodes do not require session affinity and utilize long-lived websocket connections.

The cluster can operate in two load balancing configurations:

Round-Robin DNS

All node IP addresses are assigned to a single DNS entry.

Hardware (Websocket Enabled)

Nodes can be used with hardware load balancers such as those available from Cisco or F5 for fault-tolerance. Hardware load balancers **must be configured for use with websockets**. Refer to your load balancer's documentation for instructions on enabling websockets.

SSL Certificates

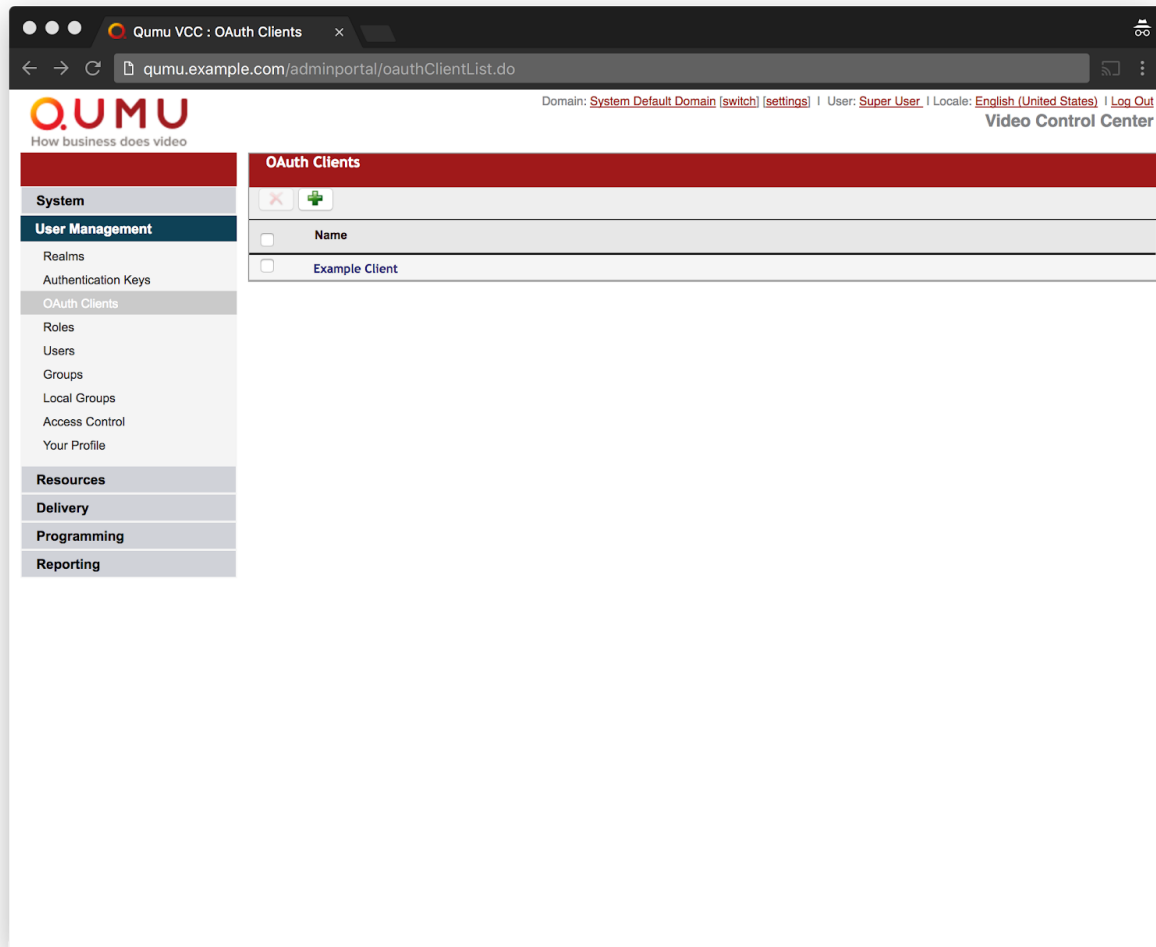
All cluster nodes share a single SSL certificate and certificate key to communicate with external services.

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

Optionally, a single PFX file containing a certificate and key may also be used.

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:** Beam
 - c. **Redirect URL Pattern:** `https://[BEAM_CLUSTER_NAME]/adminportal/beam/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 `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:** Beam *
- Redirect URL Pattern:** `https://qumu.example.com/adminportal/b` *
- Client Secret:** 0acba252-2cd4-427f-8be8-8b6aacfc1aa *
- Skip User Authorization:** ☒
- Access Token Expiry (seconds):** 86400 *
- Implicit Token Expiry (seconds):** 86400 *

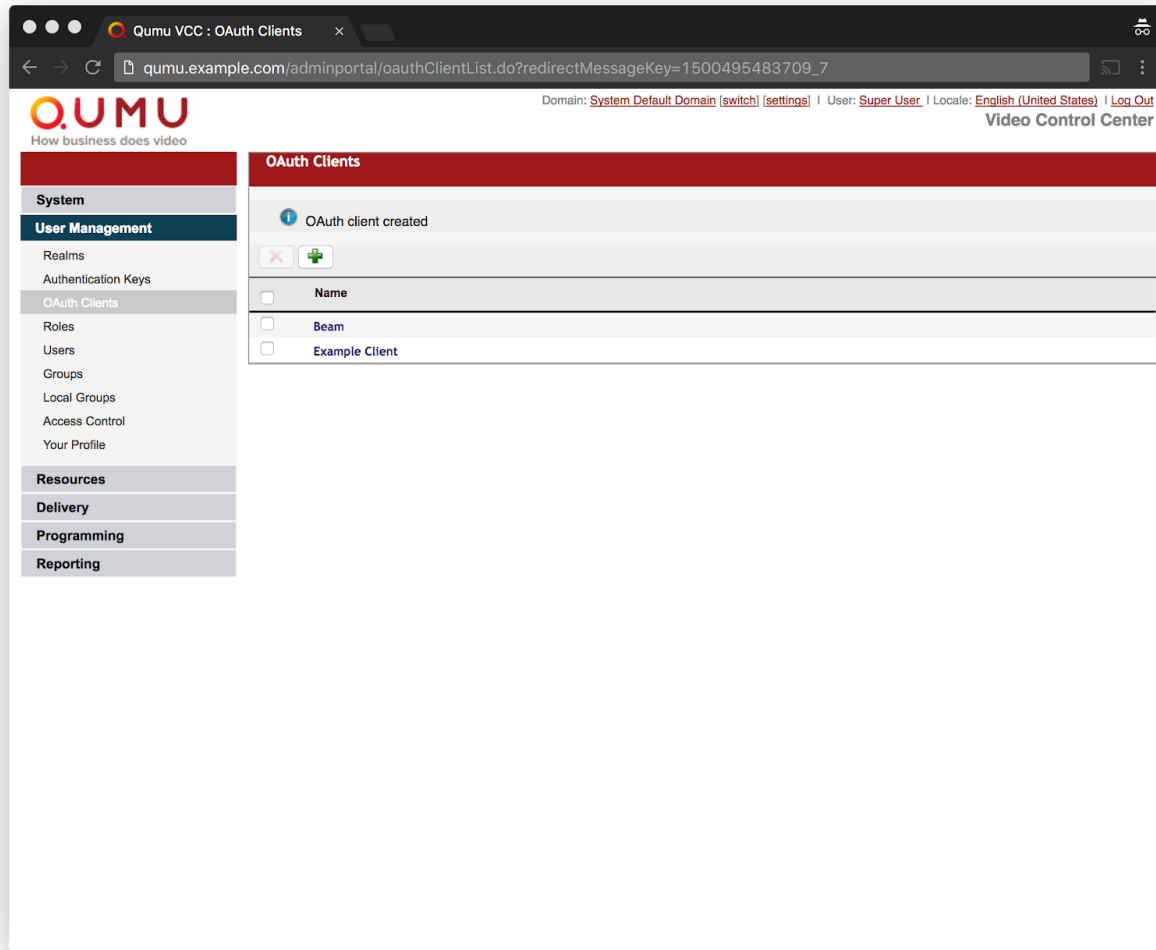
At the bottom of the form, there are two buttons: "Save" (with a green checkmark icon) and "Cancel".

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

- System
- User Management (selected)
- 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 information: "Domain: System Default Domain [switch] [settings] | User: Super User | Locale: English (United States) | Log Out". The Qumu logo and tagline "How business does video" are visible in the top left.

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



Node Setup

Network Setup (DHCP)

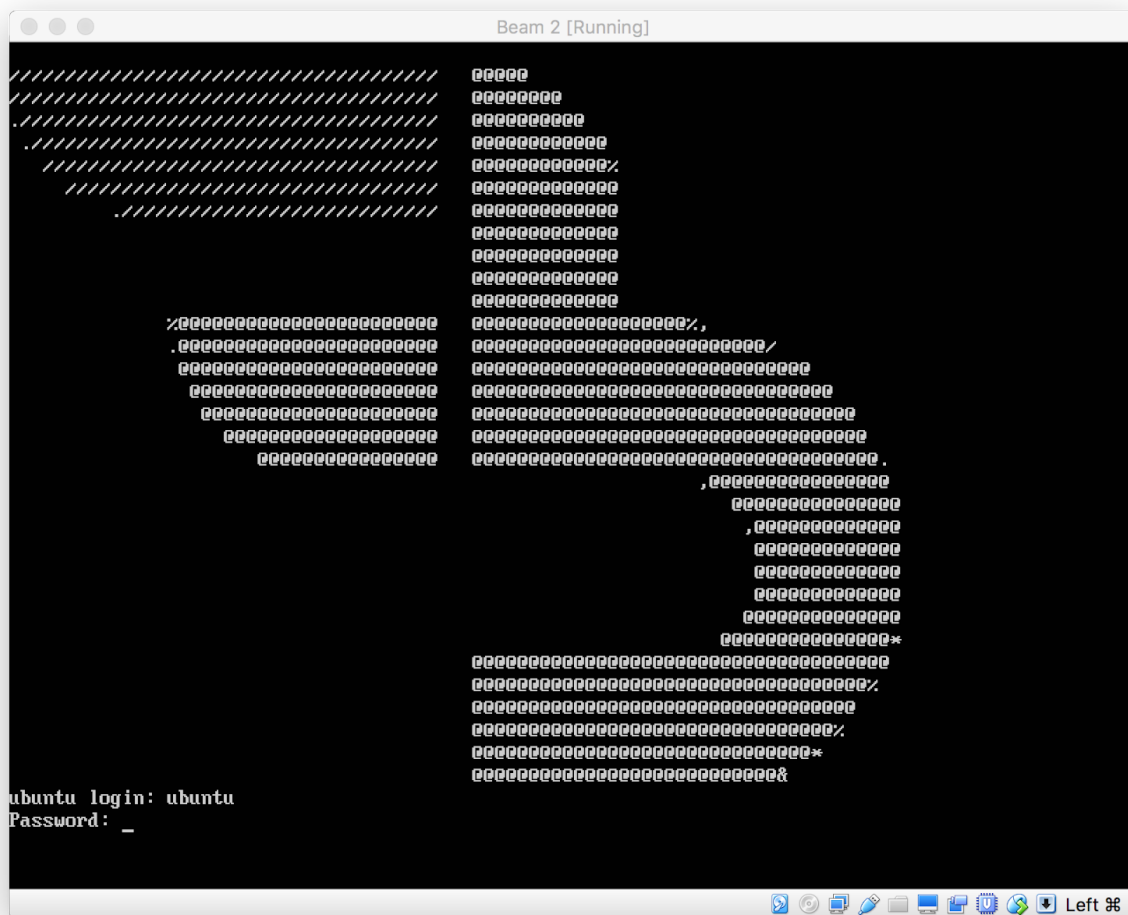
By default, nodes use dynamic host configuration protocol (DHCP) on network device eth0. No additional network setup is required on DHCP systems.

Network Setup (Static IP)

For systems with statically allocated IP addresses:

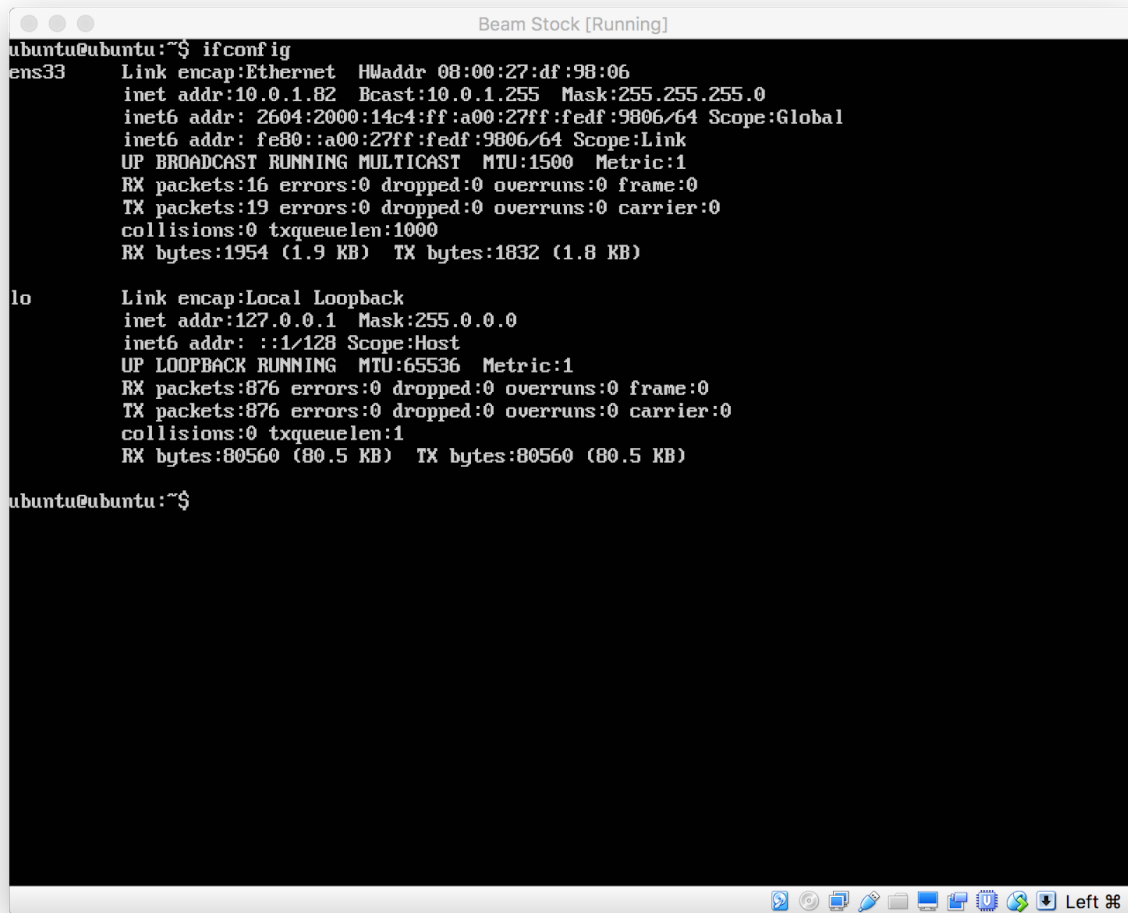
1. Access the virtual machine terminal.
2. At the login prompt, enter:

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



3. Verify the interface you plan to configure:

```
ifconfig
```



A terminal window titled "Beam Stock [Running]" showing the output of the `ifconfig` command. The output displays details for two network interfaces: `ens33` (Ethernet) and `lo` (Local Loopback). The `ens33` interface has an IP address of `10.0.1.82` and a MAC address of `08:00:27:df:98:06`. The `lo` interface has an IP address of `127.0.0.1`. The terminal window has a standard Ubuntu desktop environment background with a taskbar at the bottom.

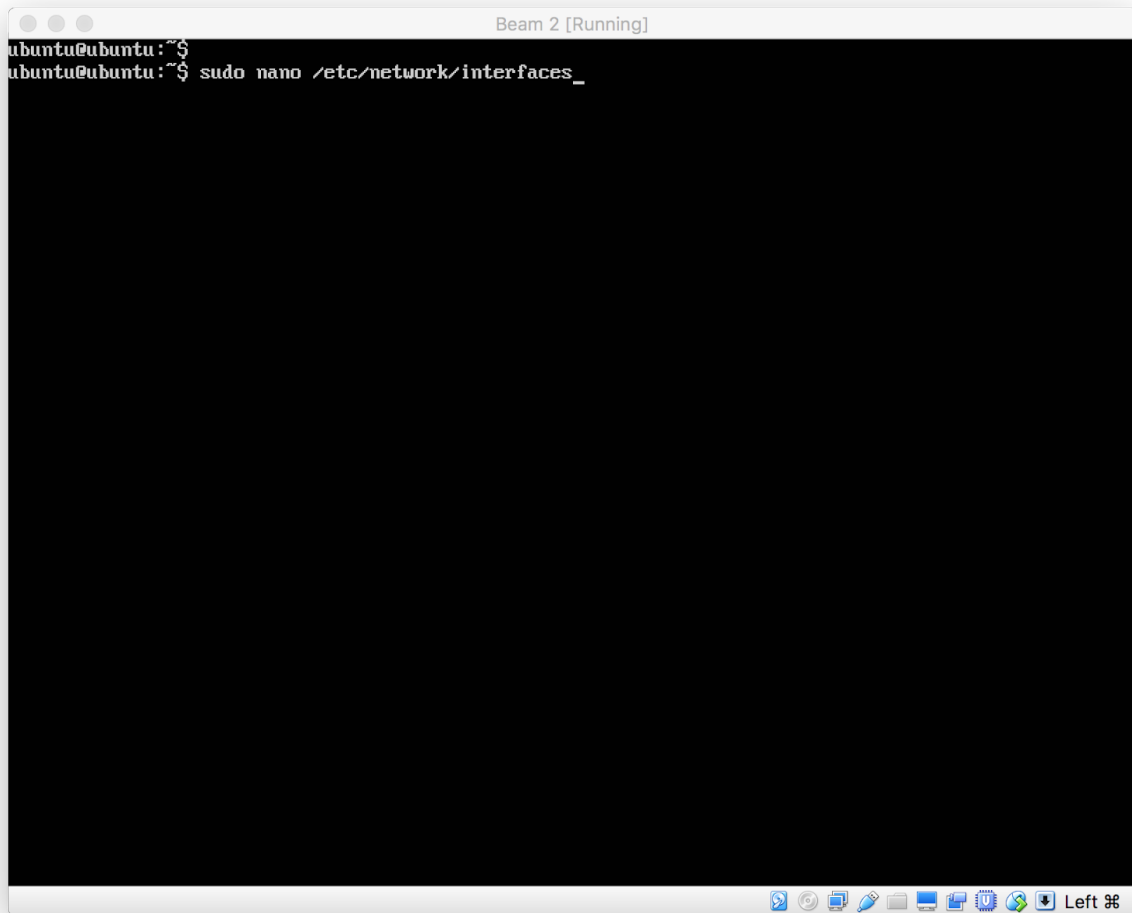
```
ubuntu@ubuntu:~$ ifconfig
ens33:  Link encap:Ethernet  HWaddr 08:00:27:df:98:06
        inet addr:10.0.1.82  Bcast:10.0.1.255  Mask:255.255.255.0
        inet6 addr: 2604:2000:14c4:ff:a00:27ff:fedf:9806/64 Scope:Global
        inet6 addr: fe80::a00:27ff:fedf:9806/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:16 errors:0 dropped:0 overruns:0 frame:0
        TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:1954 (1.9 KB)  TX bytes:1832 (1.8 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:876 errors:0 dropped:0 overruns:0 frame:0
        TX packets:876 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:80560 (80.5 KB)  TX bytes:80560 (80.5 KB)

ubuntu@ubuntu:~$
```


4. Open the network configuration file for editing:

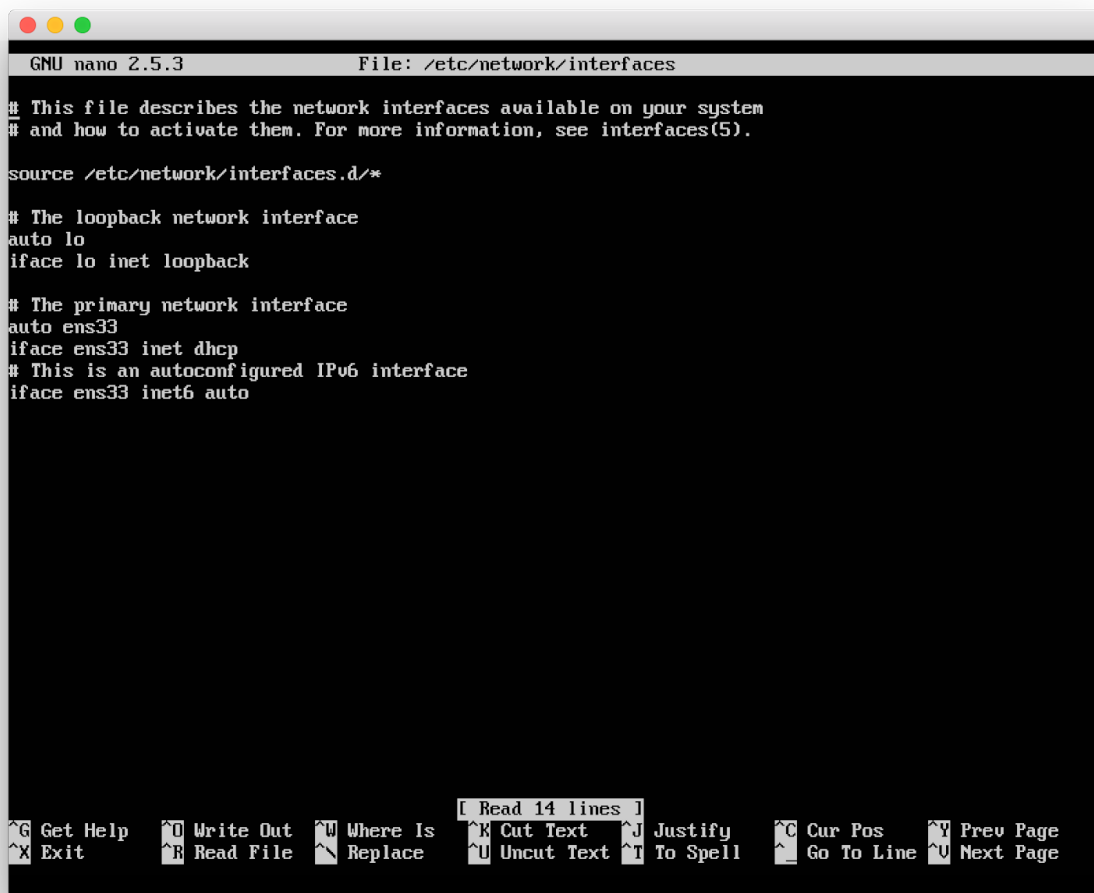
```
sudo nano /etc/network/interfaces
```



5. Review and modify the settings as needed.

- The file will look similar to:

```
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto ens33
iface ens33 inet dhcp
# This is an autoconfigured IPv6 interface
iface ens33 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/*

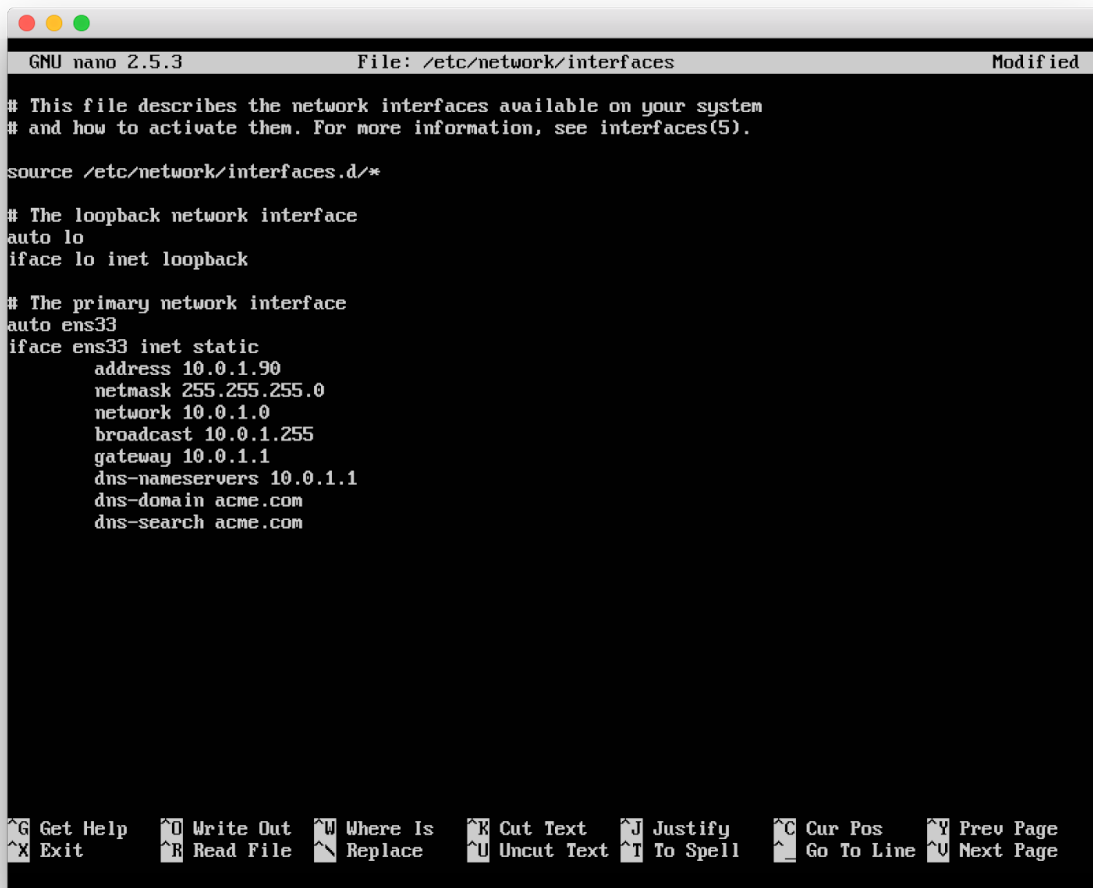
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens33
iface ens33 inet dhcp
# This is an autoconfigured IPv6 interface
iface ens33 inet6 auto

[ Read 14 lines ]
^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 ^U 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 ens33
iface ens33 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`. The editor displays the following content:

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

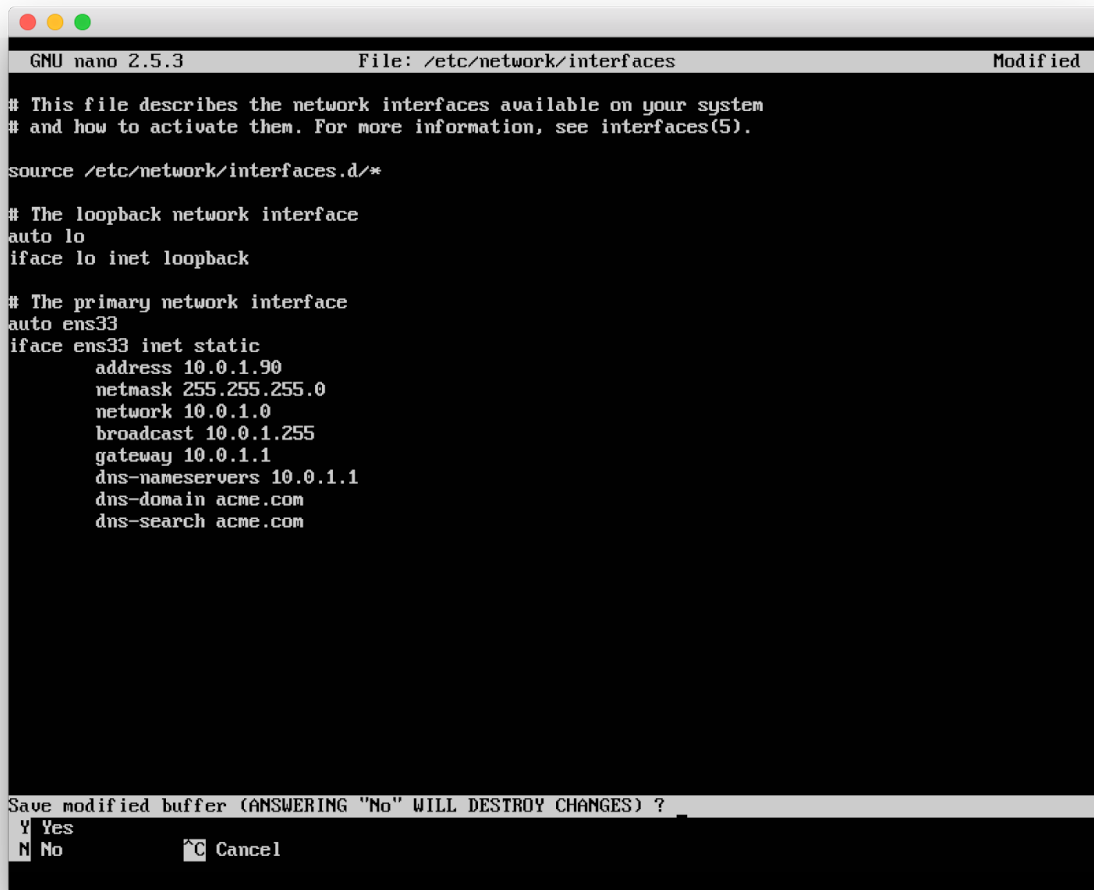
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens33
iface ens33 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 bottom of the window shows a status bar with various keyboard shortcuts for editing and navigation, such as `^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`, and `^U Next Page`.

6. When your modifications are completed press **CTRL-X** to exit.
7. 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).

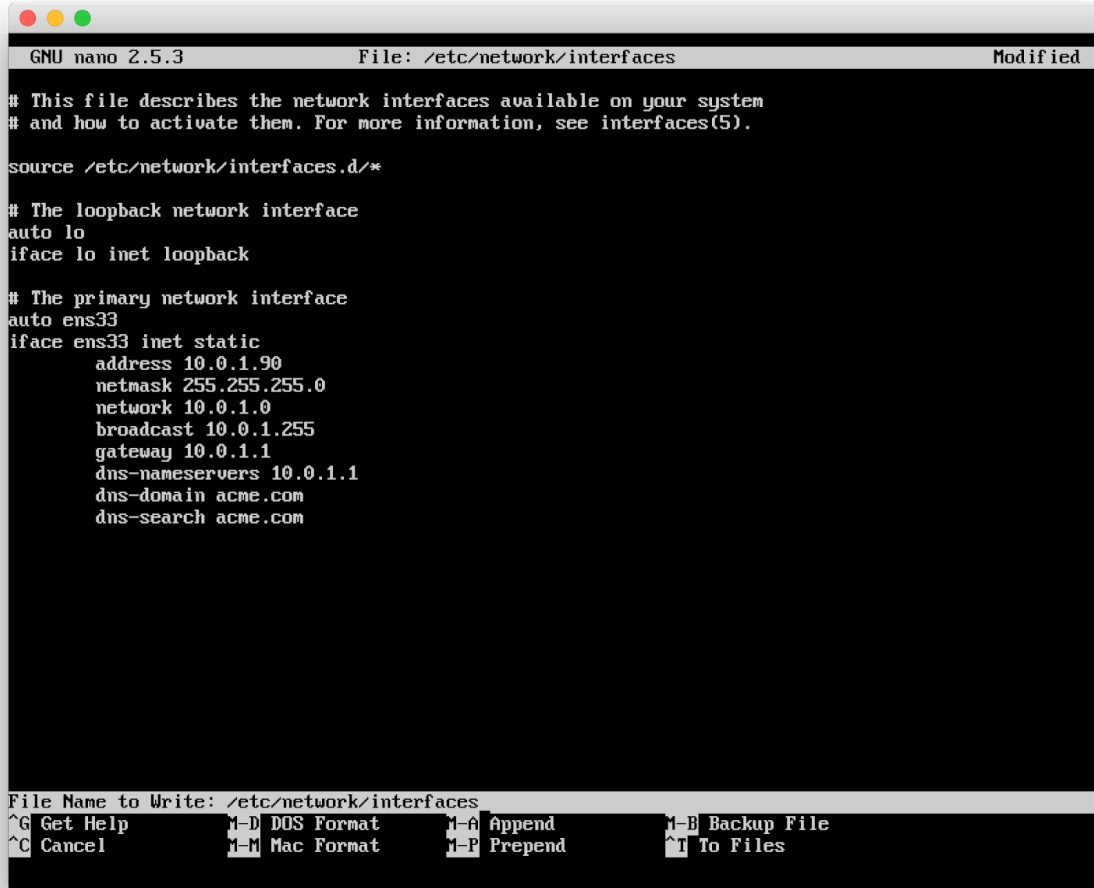
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens33
iface ens33 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
```

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



The screenshot shows a terminal window with the nano 2.5.3 text editor. The file being edited is /etc/network/interfaces. The content of the file is as follows:

```
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

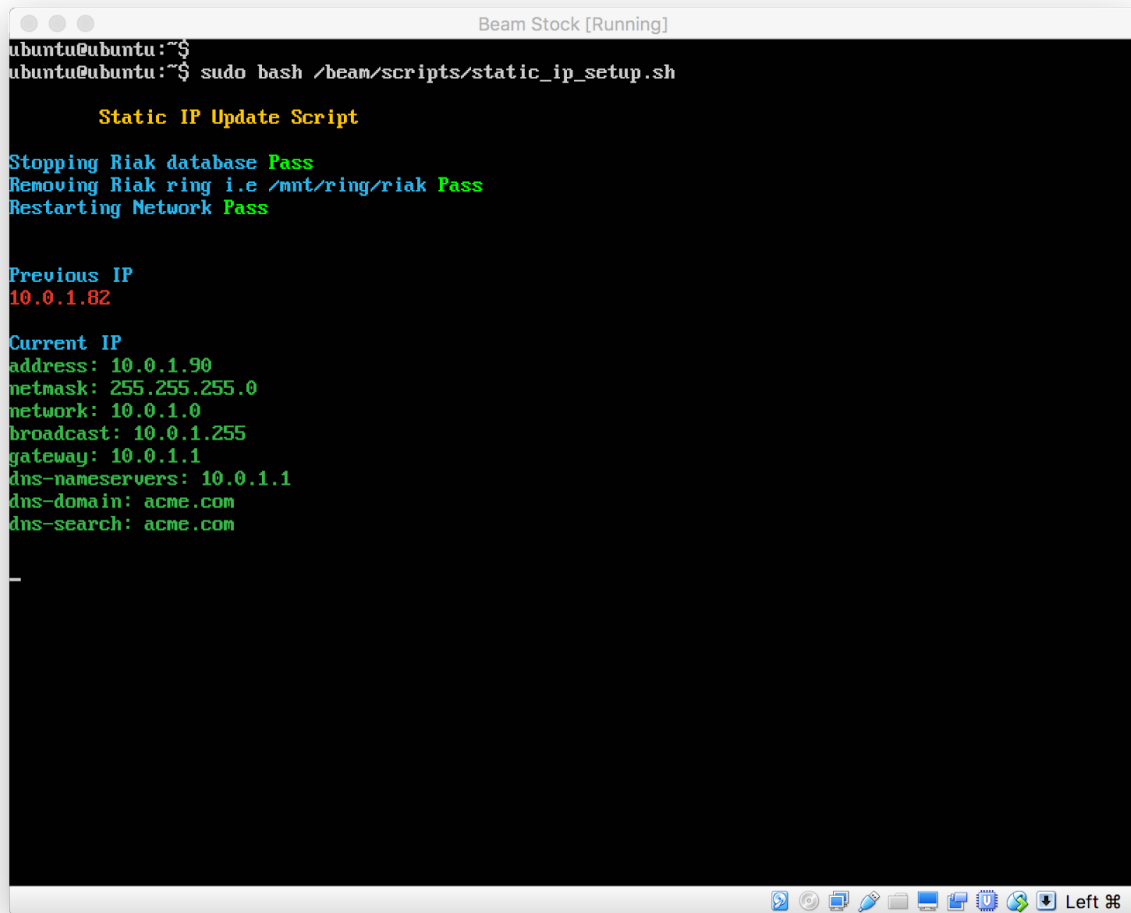
# The primary network interface
auto ens33
iface ens33 inet static
    address 10.0.1.90
    netmask 255.255.255.0
    network 10.0.1.0
    broadcast 10.0.1.255
    gateway 10.0.1.1
    dns-nameservers 10.0.1.1
    dns-domain acme.com
    dns-search acme.com
```

At the bottom of the window, the file name to write is shown as /etc/network/interfaces. Below this, there is a menu bar with the following options:

- ^G Get Help
- ^C Cancel
- ^M-D DOS Format
- ^M-M Mac Format
- ^M-A Append
- ^M-P Prepend
- ^M-B Backup File
- ^M To Files

9. Run **static_ip_setup.sh** script with sudo:

```
sudo bash /beam/scripts/static_ip_setup.sh
```

A terminal window titled "Beam Stock [Running]" showing the execution of the script. The prompt is "ubuntu@ubuntu:~\$". The user enters "sudo bash /beam/scripts/static_ip_setup.sh". The script output is as follows:

```
Static IP Update Script

Stopping Riak database Pass
Removing Riak ring i.e /mnt/ring/riak Pass
Restarting Network Pass

Previous IP
10.0.1.82

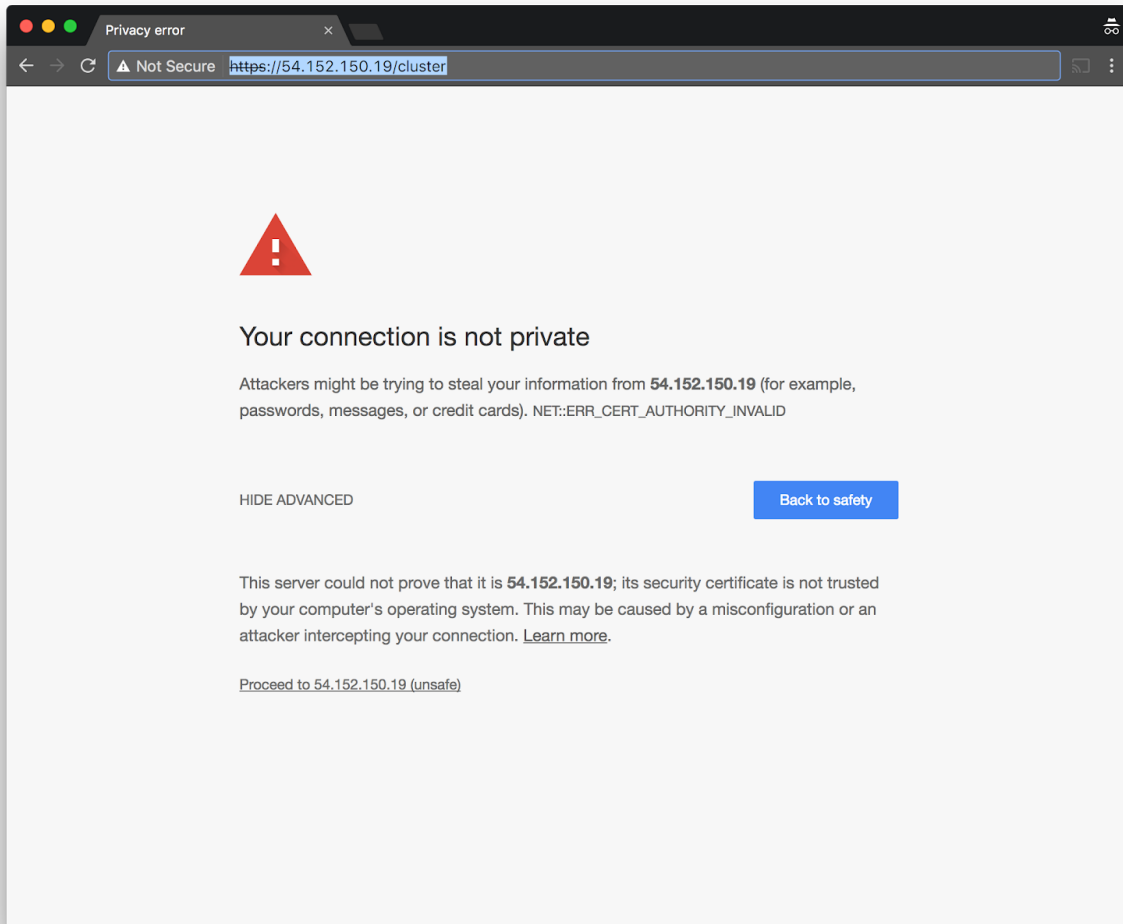
Current IP
address: 10.0.1.90
netmask: 255.255.255.0
network: 10.0.1.0
broadcast: 10.0.1.255
gateway: 10.0.1.1
dns-nameservers: 10.0.1.1
dns-domain: acme.com
dns-search: acme.com
```

10. After the system restarts, confirm that it was configured successfully.
 - Ping the configured IP address:

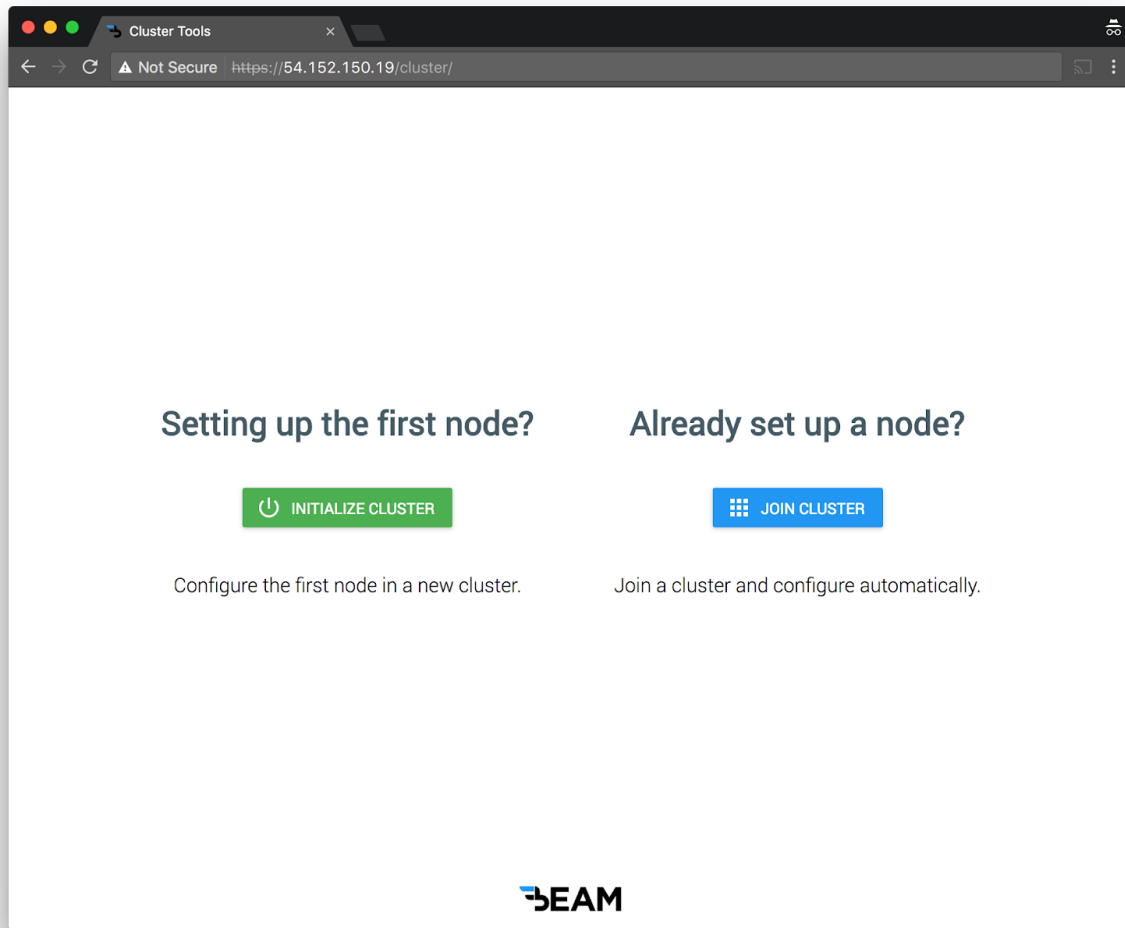
```
ping [configured IP address]
```
 - Access **[https://\[configured IP address\]/cluster](https://[configured IP address]/cluster)** in a web browser and check for the cluster setup screen.

Initialize Cluster

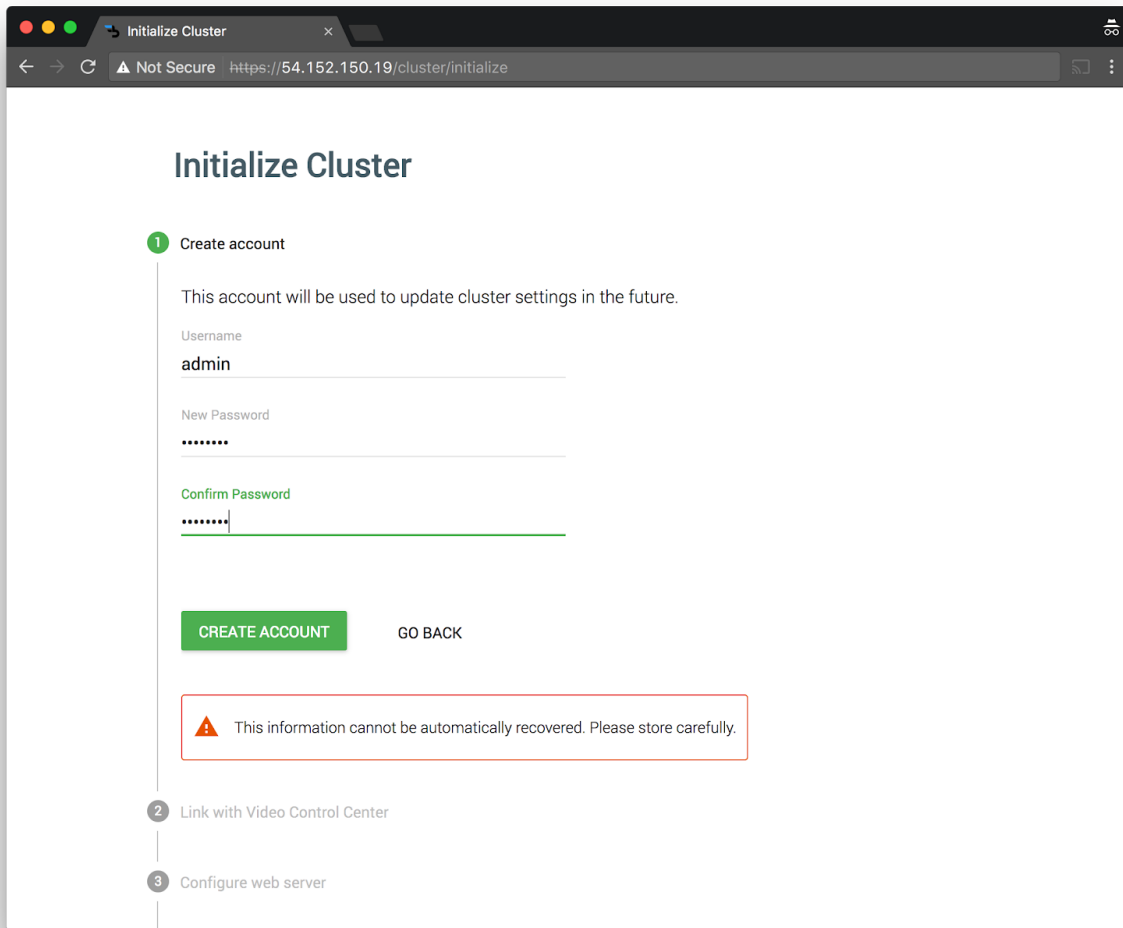
Visit the HTTPS **/cluster** path of the first node. If the node IP were **54.152.150.19**, the address would be **https://54.152.150.19/cluster**. Proceed through the SSL certificate warnings.



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



From **Initialize Cluster: Step 1**, 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 Cluster" with the URL `https://54.152.150.19/cluster/initialize`. The page has a header "Initialize Cluster" and a progress indicator with three steps: "1 Create account", "2 Link with Video Control Center", and "3 Configure web server".

Under "1 Create account", there is a message: "This account will be used to update cluster 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 "*****".

At the bottom of the form are two buttons: "CREATE ACCOUNT" (green) and "GO BACK" (grey).

A red-bordered warning box contains a warning icon and the text: "This information cannot be automatically recovered. Please store carefully."

From **Initialize Cluster: Step 2**, enter the Qumu Viewer Portal network and domain information, and the credentials of an oAuth client previously set up in the Qumu Admin Portal.

The screenshot shows a web browser window with the title 'Initialize Cluster' and the URL 'https://54.152.150.19/cluster/initialize'. The page has a dark header bar with window controls and a 'Not Secure' warning. The main content area is white and titled 'Initialize Cluster'. A vertical progress bar on the left shows three steps: '1 Create account' (completed with a green checkmark), '2 Link with Video Control Center' (active with a green circle), and '3 Configure web server' (disabled with a grey circle). Step 2 includes the instruction: 'Create an an oAuth client in the Qumu admin portal and enter the credentials below.' Below this are two columns of input fields. The left column contains: 'Viewer Portal Protocol' (https), 'Viewer Portal Host Name' (qumu.example.com), 'Viewer Portal Port' (443), and 'Viewer Portal Domain' (example). The right column contains: 'oAuth Client ID' (ExampleClientID), 'oAuth Client Secret' (ExampleClientSecret), 'oAuth Redirect URL Pattern' (https://qumu.example.com/adminportal/beam/), and 'oAuth Access Token Expiry' (86400). At the bottom of the form are two buttons: a green 'LINK WITH VIDEO CONTROL CENTER' button and a grey 'GO BACK' button.

Initialize Cluster

1 ☒ Create account

2 ☒ Link with Video Control Center

Create an an oAuth client in the Qumu admin portal and enter the credentials below.

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://qumu.example.com/adminportal/beam/
Viewer Portal Domain	oAuth Access Token Expiry
example	86400

[LINK WITH VIDEO CONTROL CENTER](#) [GO BACK](#)

3 ☐ Configure web server

From **Initialize Cluster: Step 3**, enter the cluster hostname and associated SSL certificate and keys. These files should be [compatible with the Nginx web server](#).

Option 1: Upload certificate file and key file separately

The screenshot shows a web browser window with the title 'Initialize Cluster' and the URL 'https://54.152.150.19/cluster/initialize'. The page displays a progress bar with three steps: 'Link with Video Control Center' (completed), 'Configure web server' (current step, marked with a green circle and the number 3), and a third step (partially visible). Under 'Configure web server', there is a label 'Enter the Cluster Host Name' and a text input field containing 'beam.example.com'. Below this, there is a section for 'Option 1: Upload certificate and key separately' with a note that the certificate and key should be in PEM format and compatible with the Nginx web server. This section includes two file upload fields: 'SSL Certificate' with the filename 'fullchain3.pem' and a validity date of 'Valid through 4/24/2018', and 'SSL Key' with the filename 'privkey3.pem'. Below these, there is a section for 'Option 2: Upload PFX File' with a note to upload a single PFX file containing both the certificate and private key. This section includes a file upload field for 'SSL PFX File' and a text input field for 'PFX Passphrase'. At the bottom of the form, there are two buttons: a green 'CONFIGURE WEB SERVER' button and a 'GO BACK' link.

Initialize Cluster

https://54.152.150.19/cluster/initialize

Link with Video Control Center

3 Configure web server

Enter the Cluster Host Name

Cluster Host Name

beam.example.com

Option 1: Upload certificate and key separately

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

SSL Certificate

fullchain3.pem

Valid through 4/24/2018

SSL Key

privkey3.pem

Option 2: Upload PFX File

Upload a single PFX file that contains both the certificate and private key

SSL PFX File

PFX Passphrase

CONFIGURE WEB SERVER GO BACK

Option 2: Upload a PFX file containing both the certificate and private key. Enter a passphrase is the PFX file requires one.

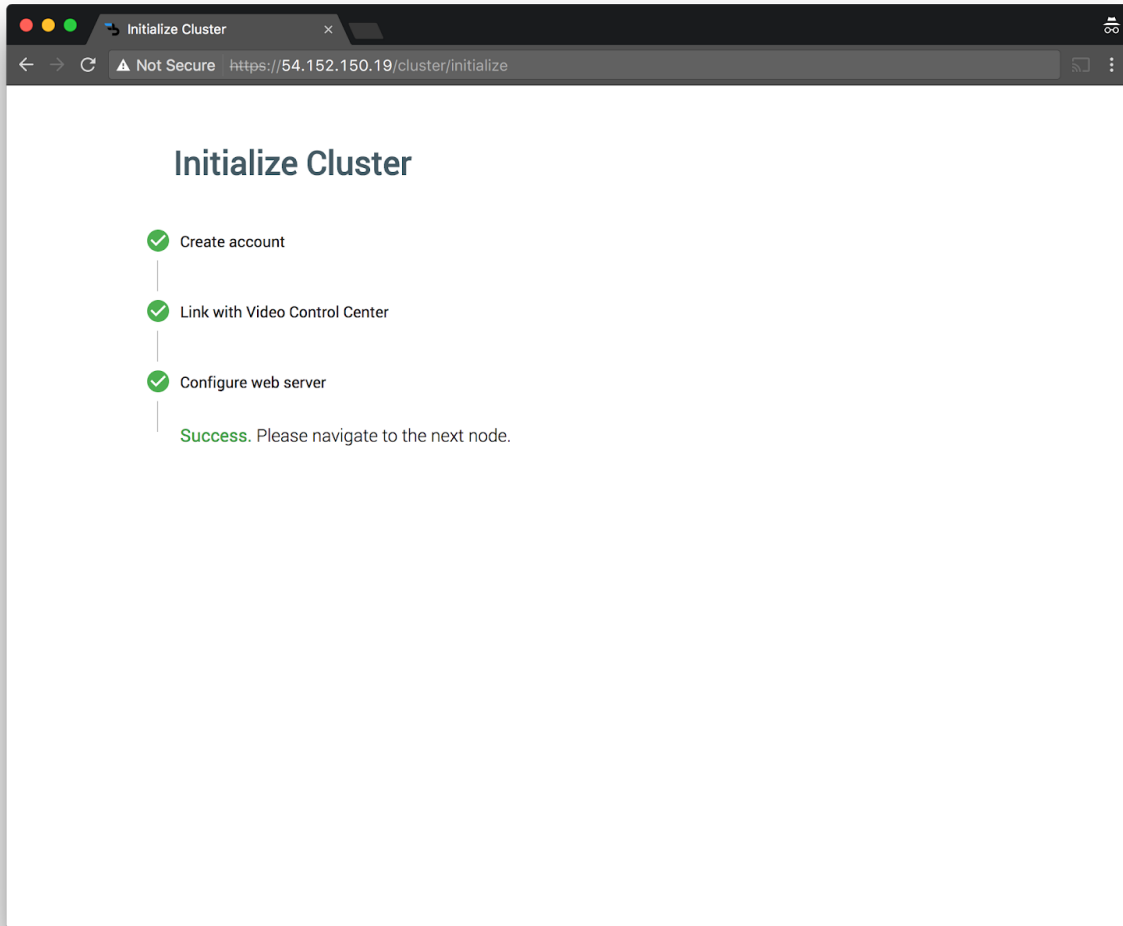
The screenshot shows a web browser window with the title 'Initialize Cluster' and the URL 'https://54.152.150.19/cluster/initialize'. The page has a progress bar on the left with two steps: 'Link with Video Control Center' (completed) and '3 Configure web server' (current step). The main content area is titled 'Configure web server' and contains the following fields and options:

- Enter the Cluster Host Name**
Cluster Host Name
- Option 1: Upload certificate and key separately**
The certificate and key should be in PEM format and [compatible with the Nginx web server](#).
- Option 2: Upload PFX File**
Upload a single PFX file that contains both the certificate and private key

Valid through 4/2/2019
PFX Passphrase

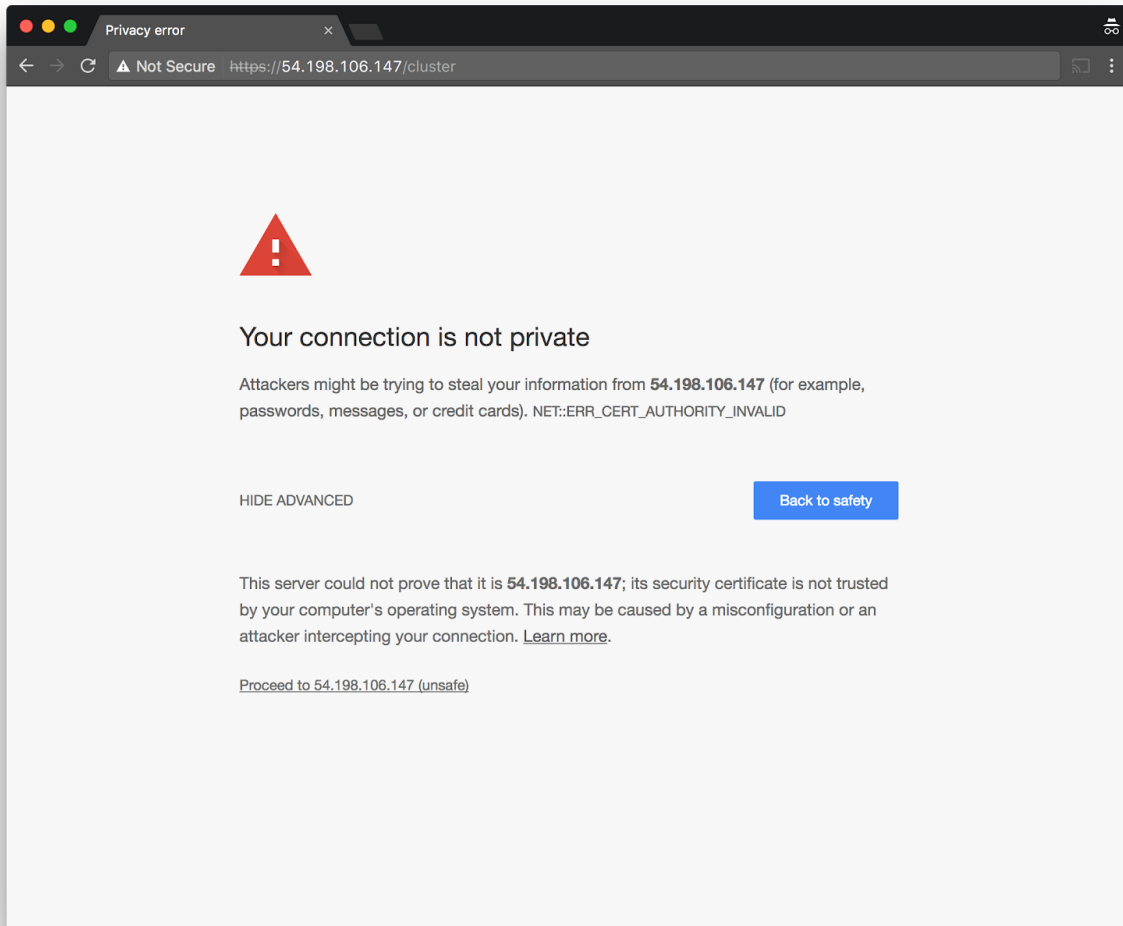
At the bottom, there are two buttons: 'CONFIGURE WEB SERVER' (green) and 'GO BACK'.

After completion, navigate to the next node in the cluster.

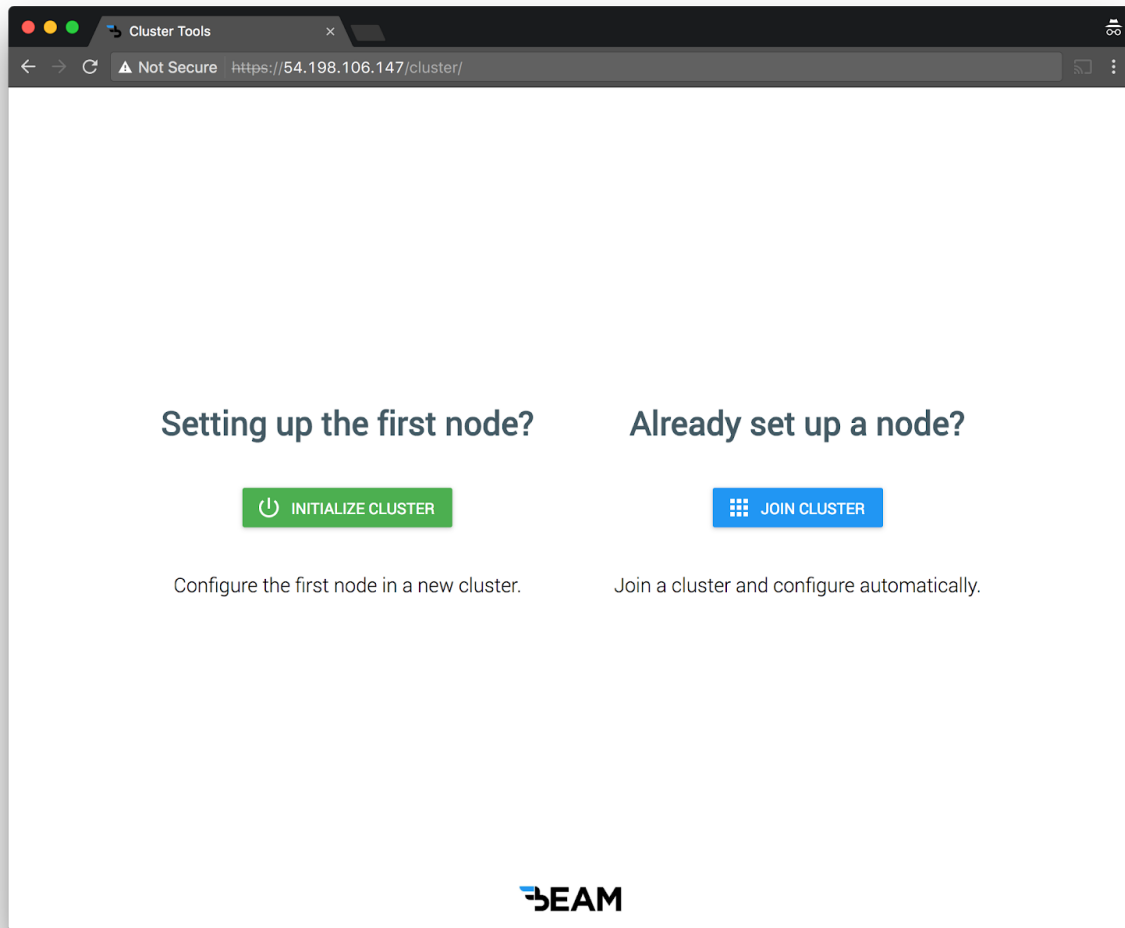


Join Nodes to Cluster

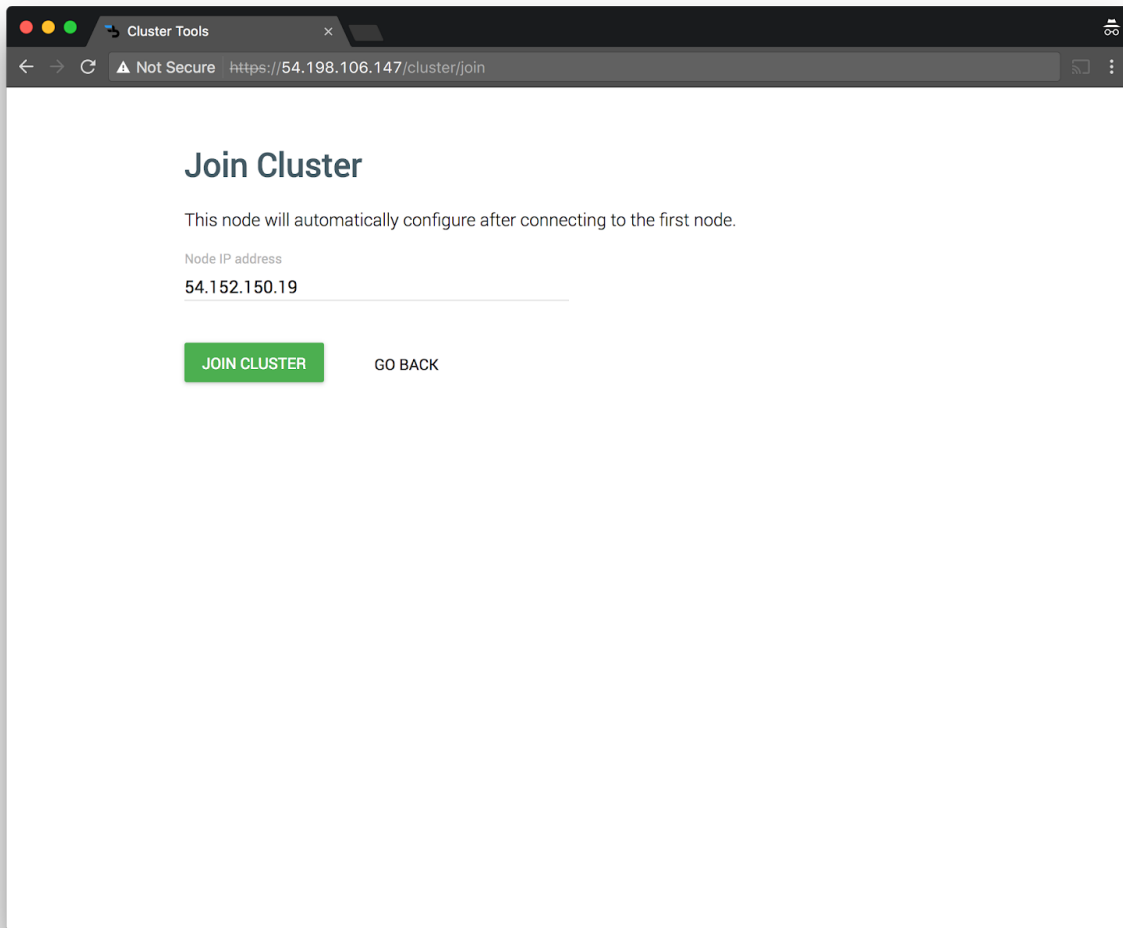
Visit the HTTPS **/cluster** path of the next node. If the node IP were **54.192.106.147**, the address would be **https://54.192.106.147/cluster**. Proceed through the SSL certificate warnings.



From the landing page, click **Join Cluster**.



From **Join Cluster**, enter the IP address of the first configured node that was used to initialize the cluster.



The screenshot shows a web browser window titled "Cluster Tools" with a single tab. The address bar displays "https://54.198.106.147/cluster/join" with a "Not Secure" warning. The main content area has the heading "Join Cluster" and a subtext: "This node will automatically configure after connecting to the first node." Below this, there is a label "Node IP address" followed by a text input field containing "54.152.150.19". At the bottom, there are two buttons: a green "JOIN CLUSTER" button and a "GO BACK" link.

Join Cluster

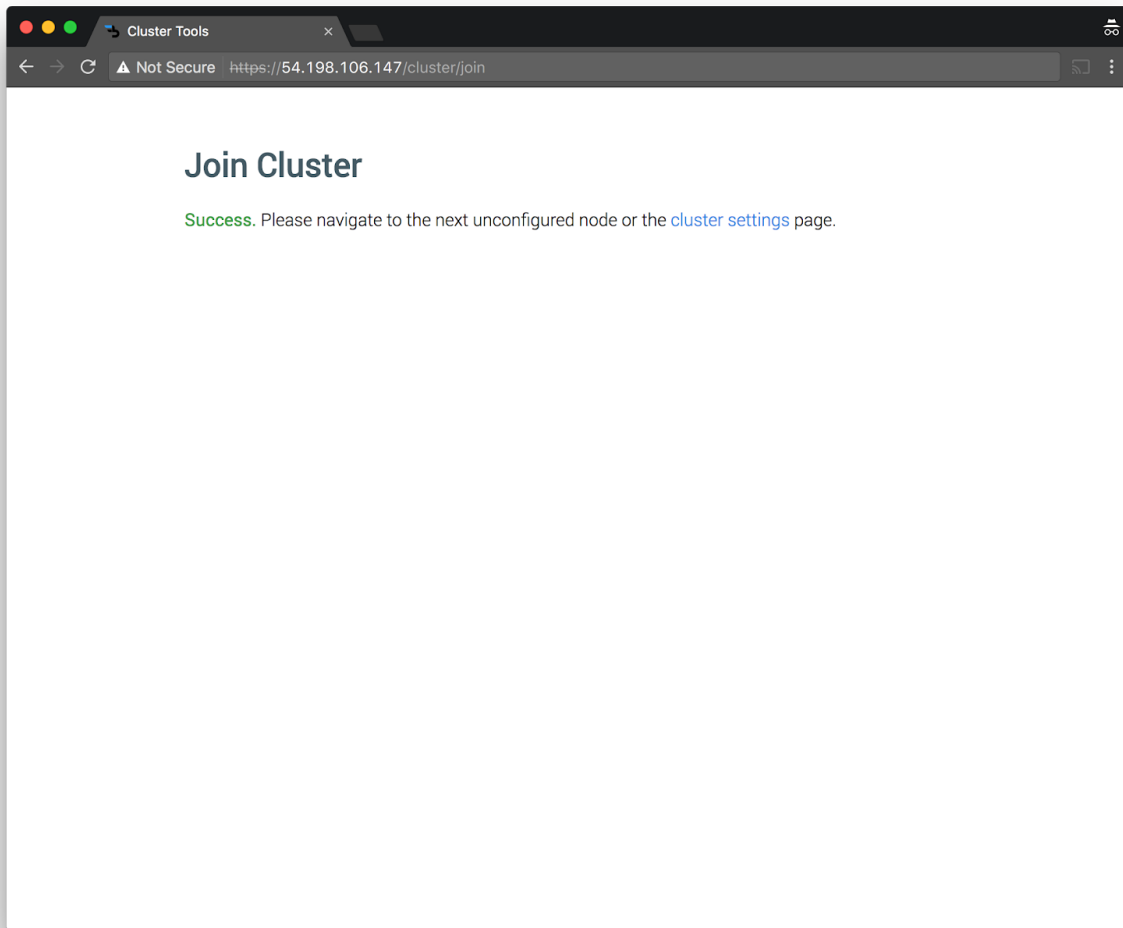
This node will automatically configure after connecting to the first node.

Node IP address

54.152.150.19

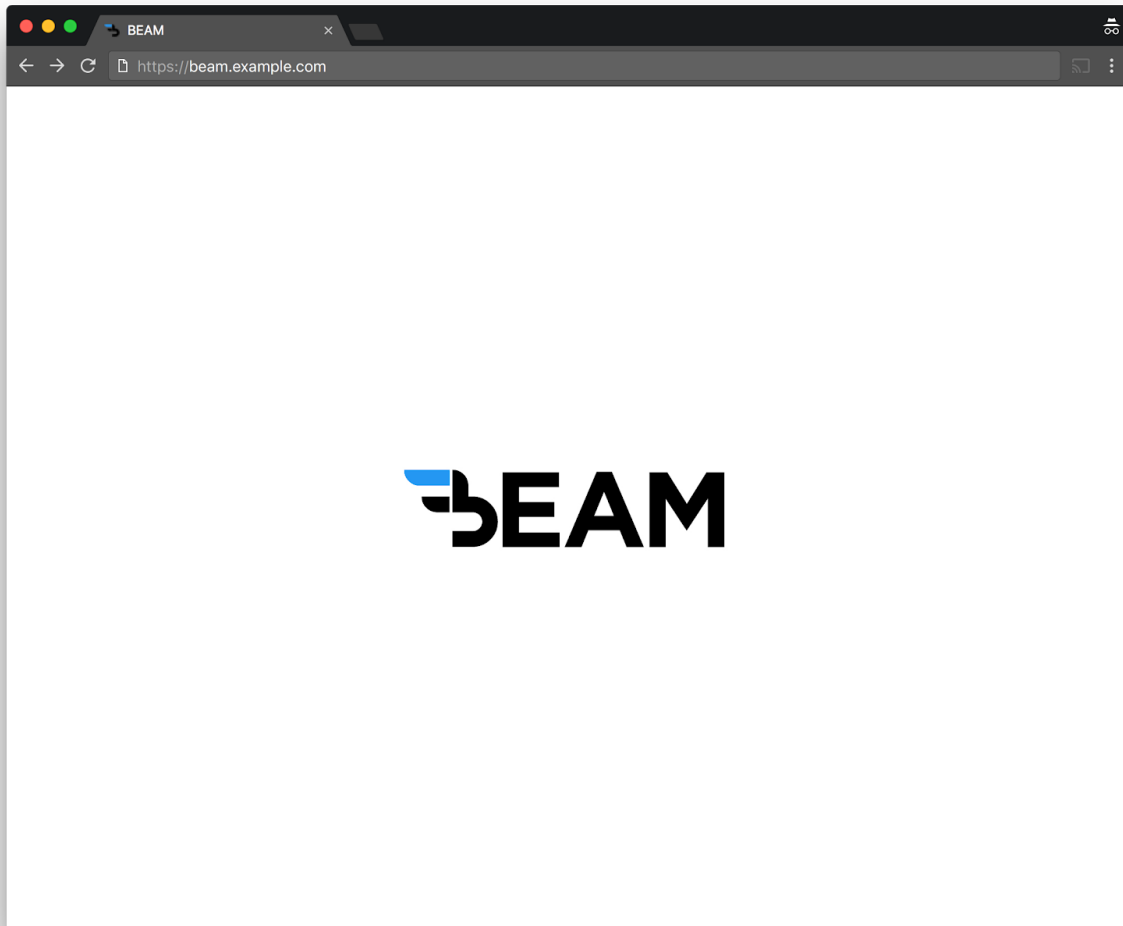
[JOIN CLUSTER](#) [GO BACK](#)

After completion, join the next node to the cluster [using the same steps](#) until all the provisioned nodes have been added.



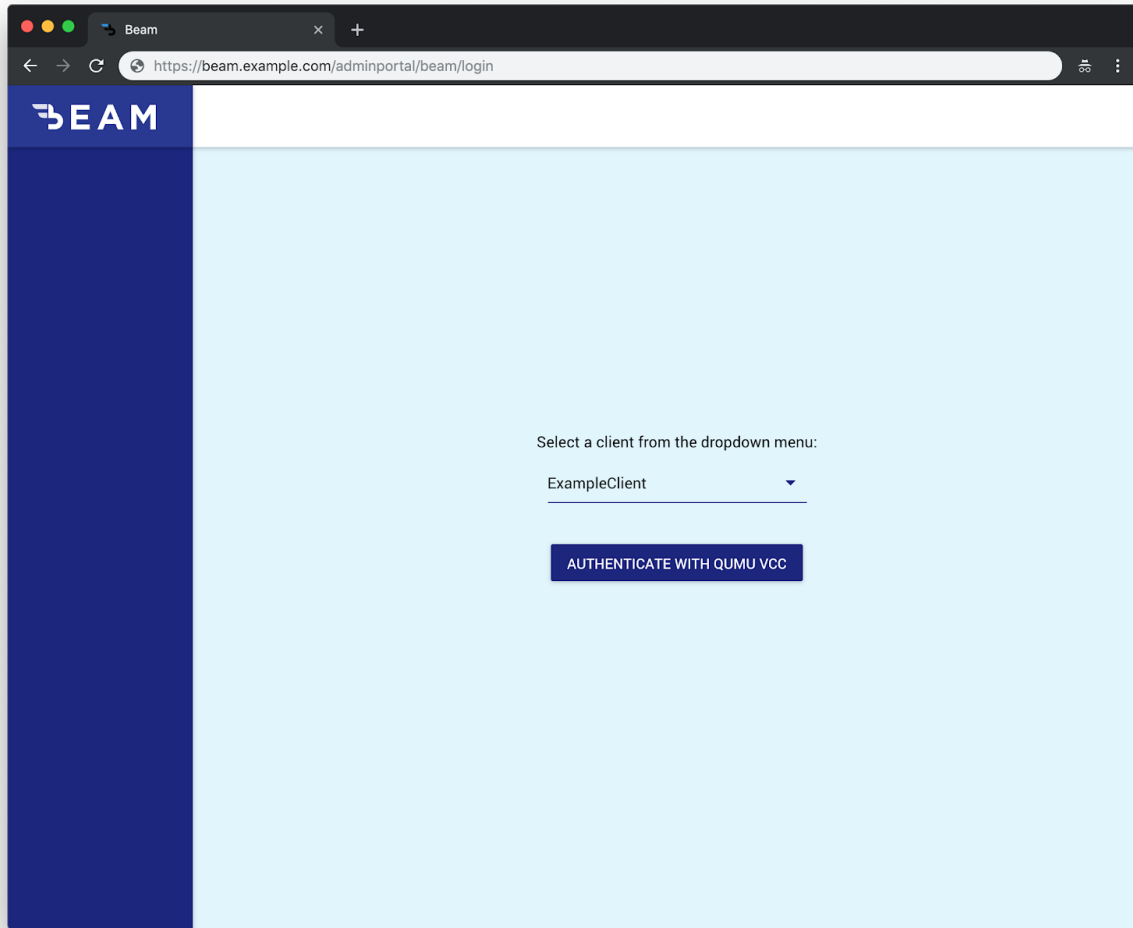
Verify DNS and SSL

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



Verify Web Interface

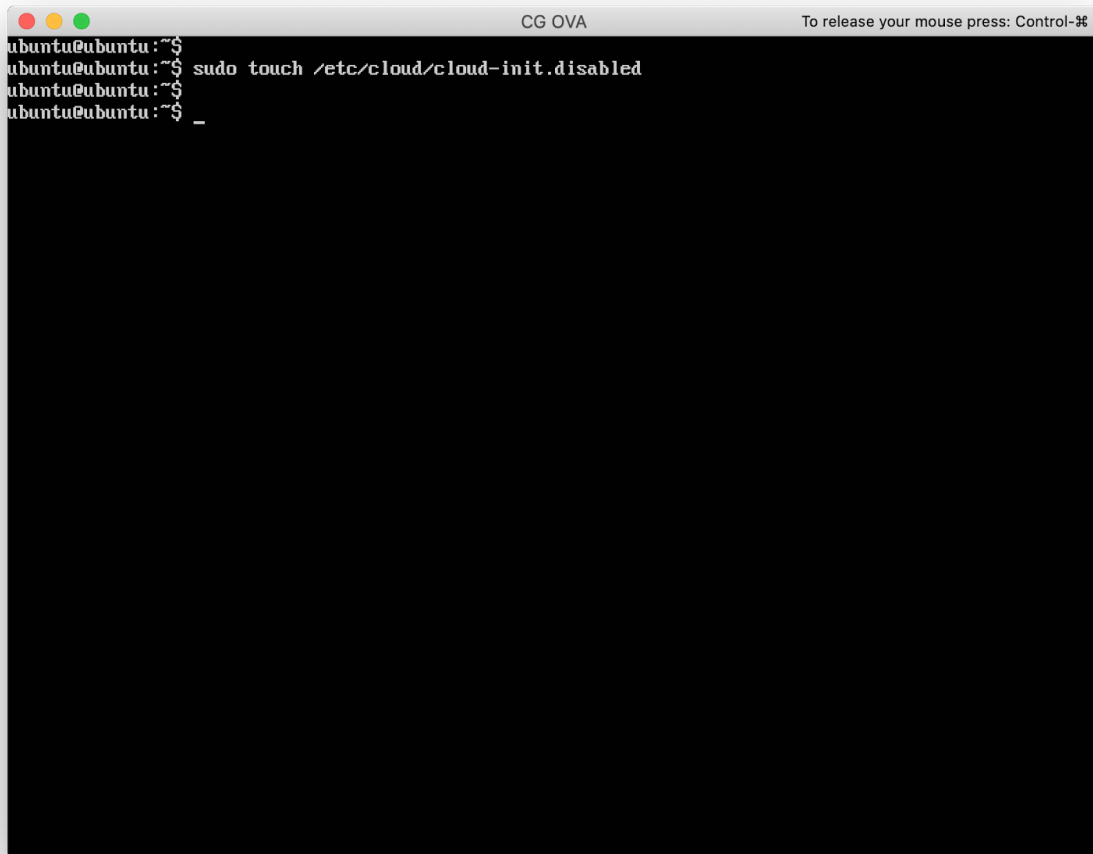
Navigate to the HTTPS designated cluster hostname to verify the web interface was installed. If the cluster hostname were **beam.example.com**, the address would be **https://beam.example.com/adminportal/beam**.



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 a series of prompts and commands: "ubuntu@ubuntu:~\$", "ubuntu@ubuntu:~\$ sudo touch /etc/cloud/cloud-init.disabled", "ubuntu@ubuntu:~\$", and "ubuntu@ubuntu:~\$ _". The terminal background is black, and the text is white.

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

