



## Deployment Guide

Version 1.0.0

# 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 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 the OVA	9
Deploying ISO on Begin encoder	9
<b>Cluster Setup</b>	<b>10</b>
Individual Node DNS Entries	10
Load Balancing	10
Round-Robin DNS	10
Hardware (Websocket Enabled)	10
SSL Certificates	10
<b>Node Setup</b>	<b>11</b>
Network Setup (DHCP)	11
Network Setup (Static IP)	12
Initialize Cluster	19
Default Team information	25
Default User information	25
Verify DNS and SSL	28
Client Administration	29
Disable Cloud-Init	30
Set up Custom Timeserver (Optional)	31

## 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

## Monday, June 10th, 2019

- The initial release of documentation.

## 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 Begin, you must have:

- Begin OVA
- Supported infrastructure
- Time server address
- Nginx compatible SSL certificate and SSL certificate key

# OVA Deployment

## Network

### Port Usage Outside of Cluster Group

Protocol	Port	Direction	Purpose
HTTPS	443	Inbound	Begin API
HTTPS	4737	Inbound	IPFS Websockets
SSH	22	Inbound/Outbound	Cluster administration

### Port Usage Inside of Cluster Group

Protocol	Port	Direction	Purpose
TCP	13000-14000	Inbound/Outbound	Cluster messaging
HTTPS	443	Inbound/Outbound	Begin API
SSH	22	Inbound/Outbound	Cluster administration

\* Subject to change depending on customer's preferred storage implementation.

# OVA Deployment

## System Requirements

### Supported Platforms

- Begin Encoder
- VMware ESXi 5.5 and later are supported.

### Cluster Size

The recommended size of a Begin cluster is 2 nodes.

### Virtual Machine Configuration

The requirements for a Begin cluster node are:

**CPU:** 3 GHz dual-core or 4 virtual processors

**RAM:** 8 GB

**STORAGE:** 80GB

### Browsers

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



# Begin Deployment

## Deploying the OVA

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

## Deploying ISO on Begin encoder

Deploy ISO on Begin encoder by flashing the ISO onto to the Internal SD card on your begin encoder and booting through the SD card.

# 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 web sockets**. Refer to your load balancer's documentation for instructions on enabling web sockets.

## 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](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.

# Node Setup

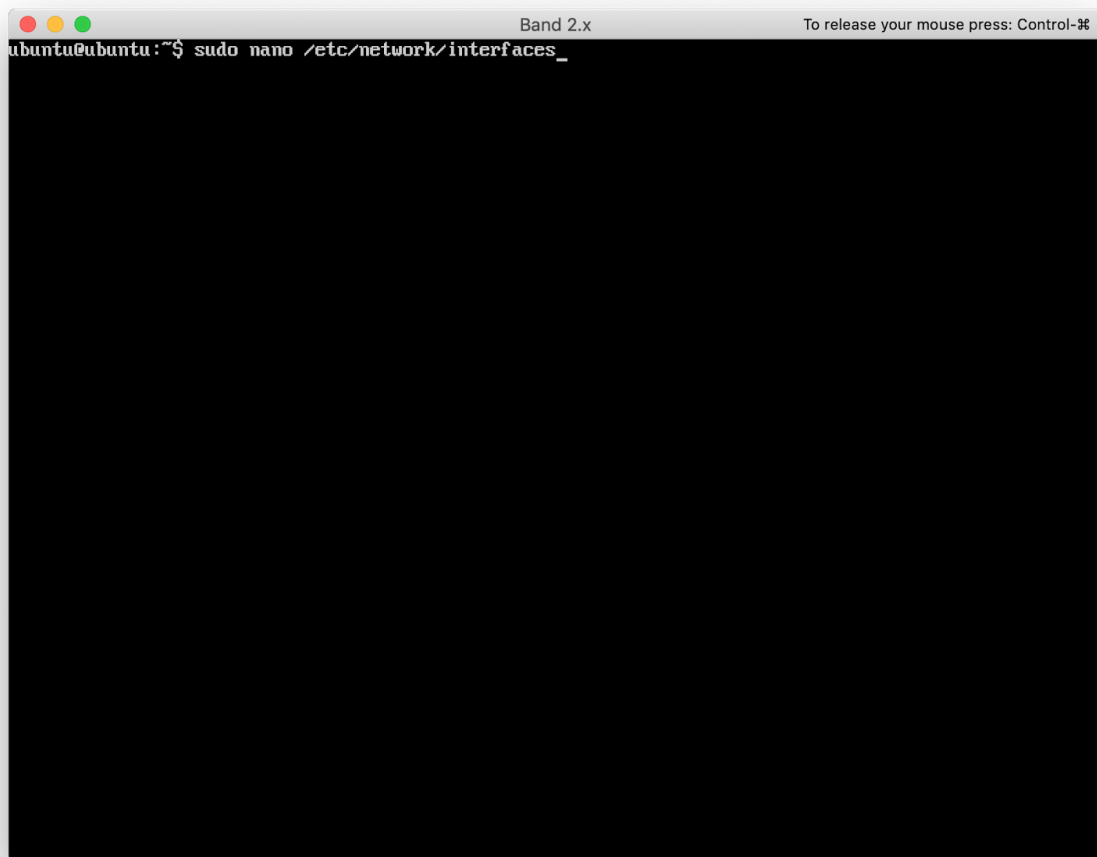
## Network Setup (DHCP)

By default, nodes use dynamic host configuration protocol (DHCP) on network device ens32. No additional network setup is required on DHCP systems.

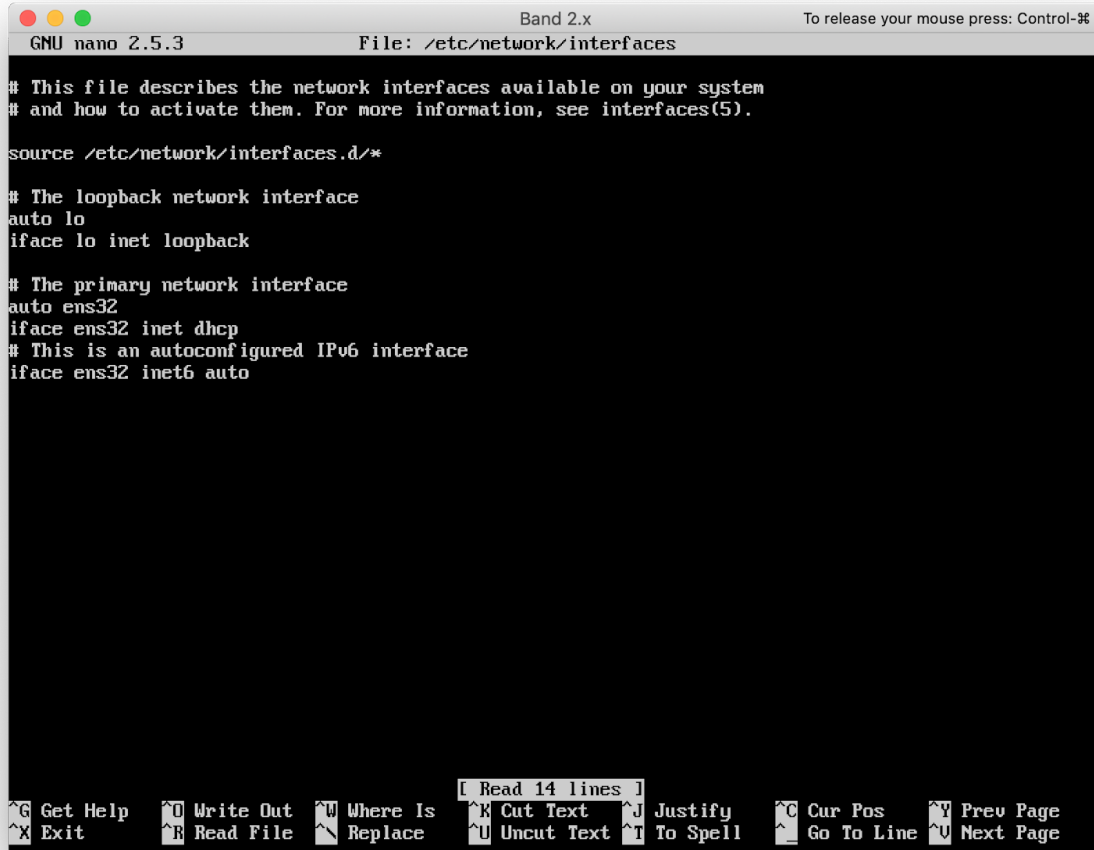


3. Open the network configuration file for editing:

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



4. Review and modify the settings as needed.



```
GNU nano 2.5.3      File: /etc/network/interfaces      To release your mouse press: Control-~

# 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 ens32
iface ens32 inet dhcp
# This is an autoconfigured IPv6 interface
iface ens32 inet6 auto

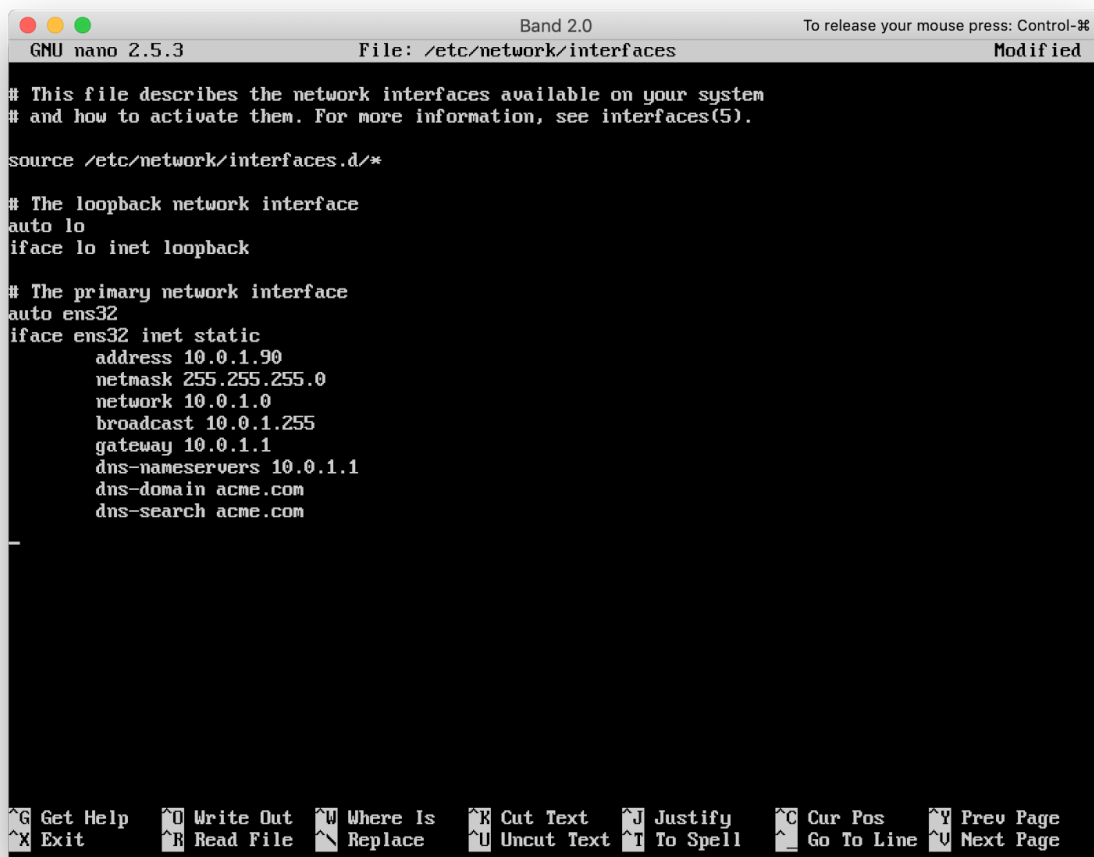
[ Read 14 lines ]
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify    ^C Cur Pos   ^Y Prev Page
^X Exit      ^R Read File  ^_ Replace   ^U Uncut Text ^T To Spell   ^_ Go To Line ^V Next Page
```

- The file will look similar to:

```
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto ens32
iface ens32 inet dhcp
# This is an autoconfigured IPv6 interface
iface ens32 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 ens32
iface ens32 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 nano 2.5.3 text editor. The title bar indicates the file being edited is `/etc/network/interfaces`. The editor's status bar at the top shows "GNU nano 2.5.3", "File: /etc/network/interfaces", and "Modified". The main text area contains the following configuration:

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

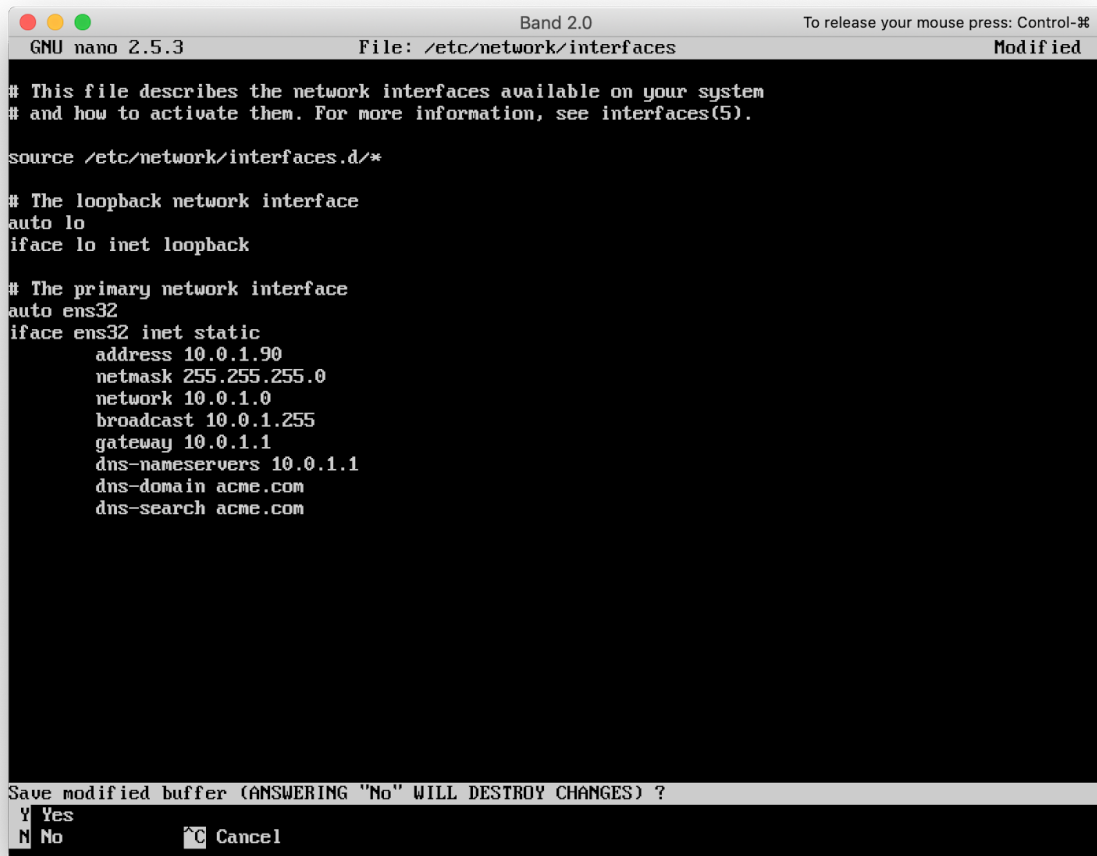
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens32
iface ens32 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 status bar of the nano editor displays various keyboard shortcuts for navigation and editing, 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 `^V Next Page`.

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



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:

```
# 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

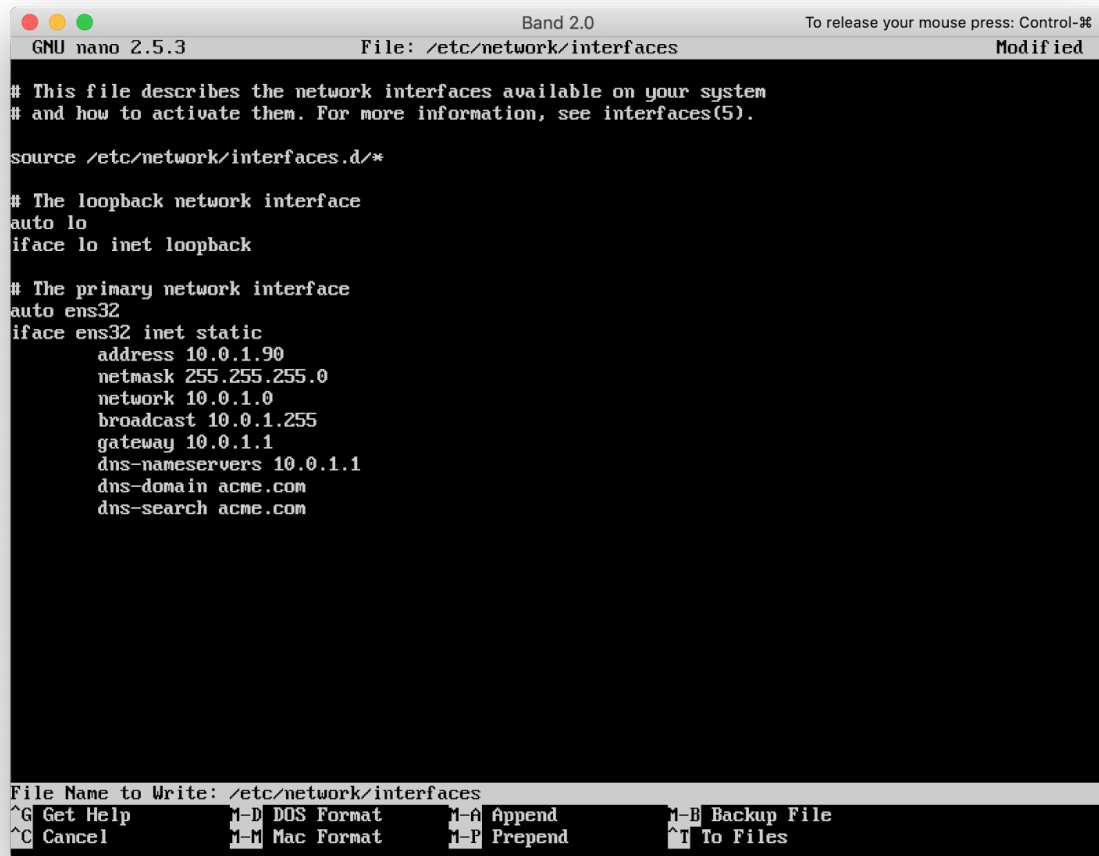
# The primary network interface
auto ens32
iface ens32 inet static
    address 10.0.1.90
    netmask 255.255.255.0
    network 10.0.1.0
    broadcast 10.0.1.255
    gateway 10.0.1.1
    dns-nameservers 10.0.1.1
    dns-domain acme.com
    dns-search acme.com
```

At the bottom of the window, a prompt asks: "Save modified buffer (ANSWERING 'No' WILL DESTROY CHANGES) ?". The options shown are:

```
Y Yes
N No      ^C Cancel
```



7. 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 ens32
iface ens32 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     ^M-T To Files
```

8. Restart the networking stack:

```
sudo systemctl restart networking
```

9. Reboot the virtual machine:

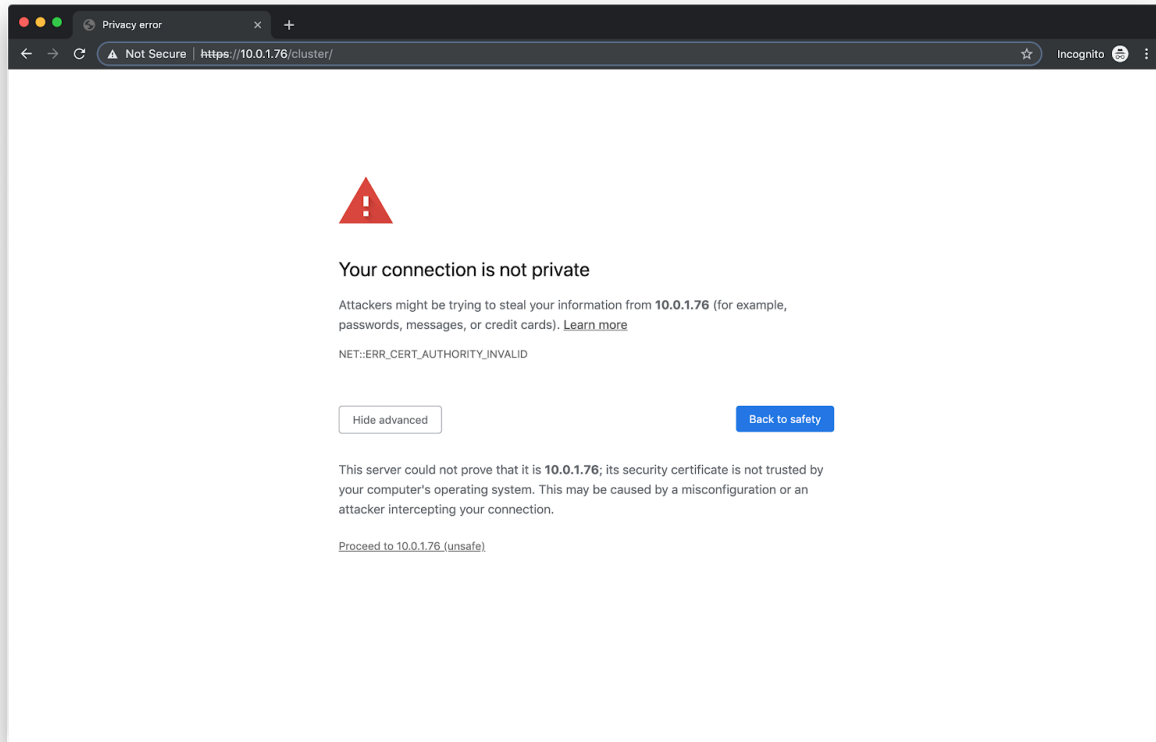
```
sudo reboot
```

10. After the system restarts, confirm that it was configured successfully.

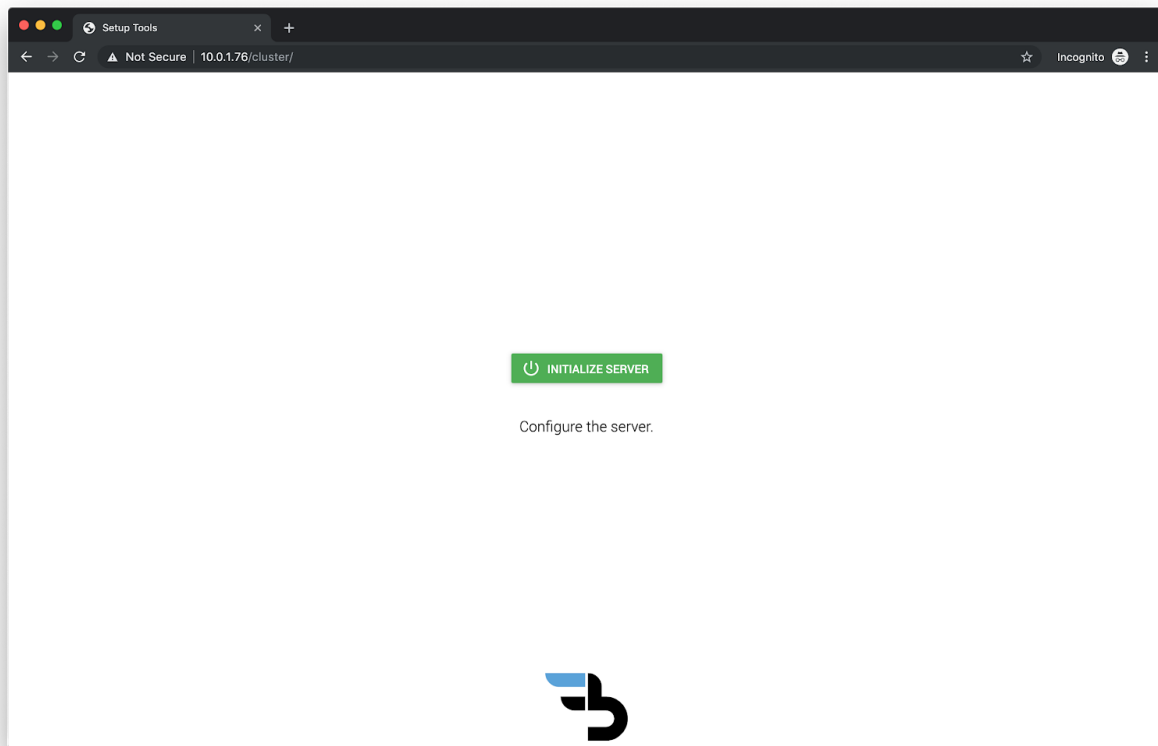
- Ping the configured IP address:  
ping [configured IP address]
- Access **https://[configured IP address]/cluster** in a web browser and check for the cluster setup screen.

## Initialize Cluster

Visit the HTTPS **/cluster** path of the first node. If the node IP were **10.0.1.76**, the address would be **https://10.0.1.76/cluster**. Proceed through the SSL certificate warnings.



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



**Initialize Server: Setup database** is pre-populated, skip that step and click on **Create account**.

From **Initialize Server: Create account**, enter a username and enter the same password under both **New Password** and **Confirm Password** fields and click on **Create Account** in order to create cluster administrative account. Make a note of these credentials since they are required to access the cluster administration page.

**NOTE** Credentials entered in this step cannot be recovered automatically.

From **Initialize Server: Configure Timeserver**, enter the address of the organization's NTP timeserver if available and Click on **Set Timeserver URL**. For example, if the organization uses **time.windows.com** as the default NTP server then the Timeserver URL would be **time.windows.com**.

If the Timeserver is not available, Click on **Skip** to skip configuring the timeserver.

The screenshot shows a web browser window titled 'Initialize Server' with the address bar displaying '10.0.1.78/cluster/initialize'. The page has a dark header bar with navigation icons. The main content area is white and features a vertical progress bar on the left with five steps: 'Setup database' (checked), 'Create account' (checked), 'Configure Timeserver' (active, highlighted with a green circle), 'Configure web server' (disabled, greyed out), and 'Create Default Application' (disabled, greyed out). The 'Configure Timeserver' step includes a label 'Timeserver URL' and a text input field containing 'time.windows.com'. Below the input field are three buttons: 'SET TIMESERVER URL' (green), 'GO BACK' (grey), and 'SKIP' (grey).

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](#).

**Option 1:** Upload certificate file and key file separately

The screenshot shows a web browser window titled 'Initialize Server' with the URL '10.0.1.78/cluster/initialize'. The page has a dark header bar with navigation icons. The main content area is white and displays a progress indicator on the left with two steps: 'Configure Timeserver' (completed) and 'Configure web server' (active). The 'Configure web server' section contains the following fields and options:

- Enter the Cluster Host Name**: A text input field with the value 'begin.example.com'. Below it, a red error message states: 'Hostname provided does not match SSL Certificate'.
- Option 1: Upload certificate and key separately**: A section header followed by the instruction: 'The certificate and key should be in PEM format and [compatible with the Nginx web server](#).'
- SSL Certificate**: A text input field with the value 'cert.pem'. Below it, a green message states: 'Valid through 7/1/2019'.
- SSL Key**: A text input field with the value 'key.pem'.
- Option 2: Upload PFX File**: A section header followed by the instruction: 'Upload a single PFX file that contains both the certificate and private key'.
- SSL PFX File**: A text input field.
- PFX Passphrase**: A text input field.

At the bottom of the form, there is a green button labeled 'CONFIGURE WEB SERVER' and a link labeled '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 titled 'Initialize Server' with the URL `https://10.0.1.76/cluster/initialize`. The page displays a progress bar with two steps: 'Configure Timeserver' (completed) and '4 Configure web server' (current step). Under 'Configure web server', there is a section 'Enter the Cluster Host Name' with a text input field containing 'begin.example.com'. Below this, there are two options for SSL configuration. 'Option 1: Upload certificate and key separately' includes fields for 'SSL Certificate' and 'SSL Key'. 'Option 2: Upload PFX File' includes a description 'Upload a single PFX file that contains both the certificate and private key', a file upload field labeled 'SSL PFX File' with the filename 'Cert.pfx', and a 'PFX Passphrase' field with masked characters. At the bottom, there are two buttons: 'CONFIGURE WEB SERVER' (highlighted in green) and 'GO BACK'.



From **Initialize Server: Create Default Application**, click on **Create Default Team** to create a team with the team name as **default** and a single user within the team with the following credentials.

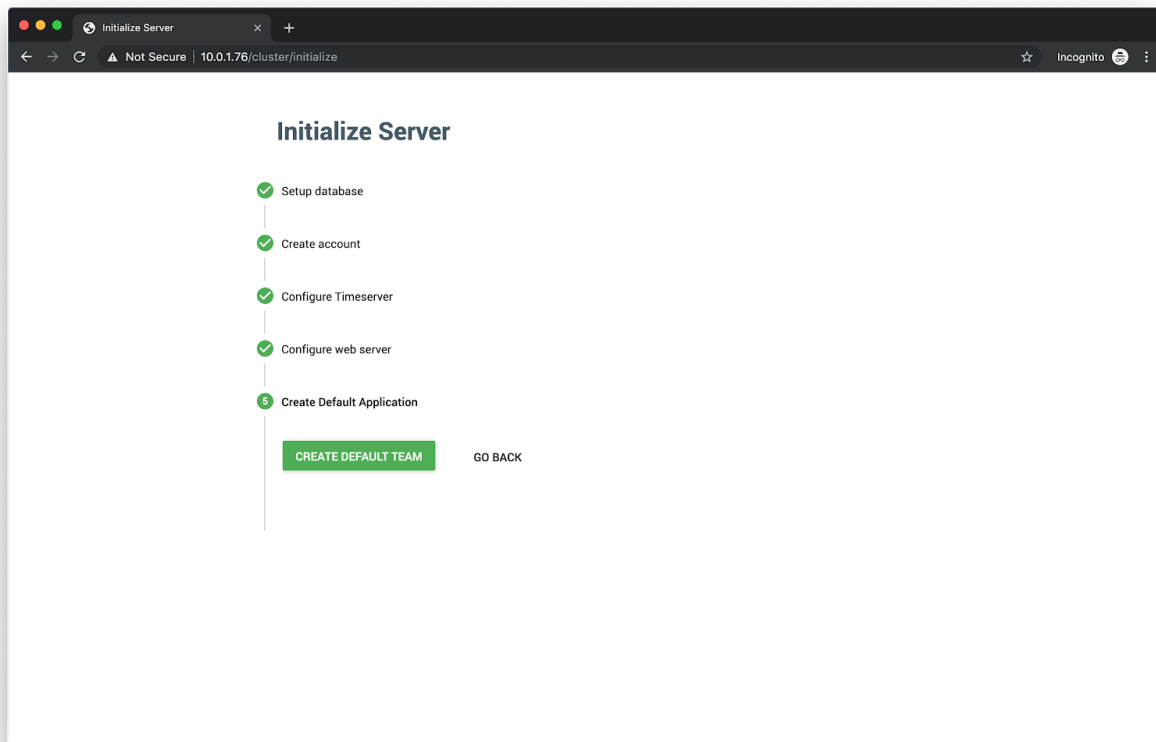
Default Team information

**Team name:** default

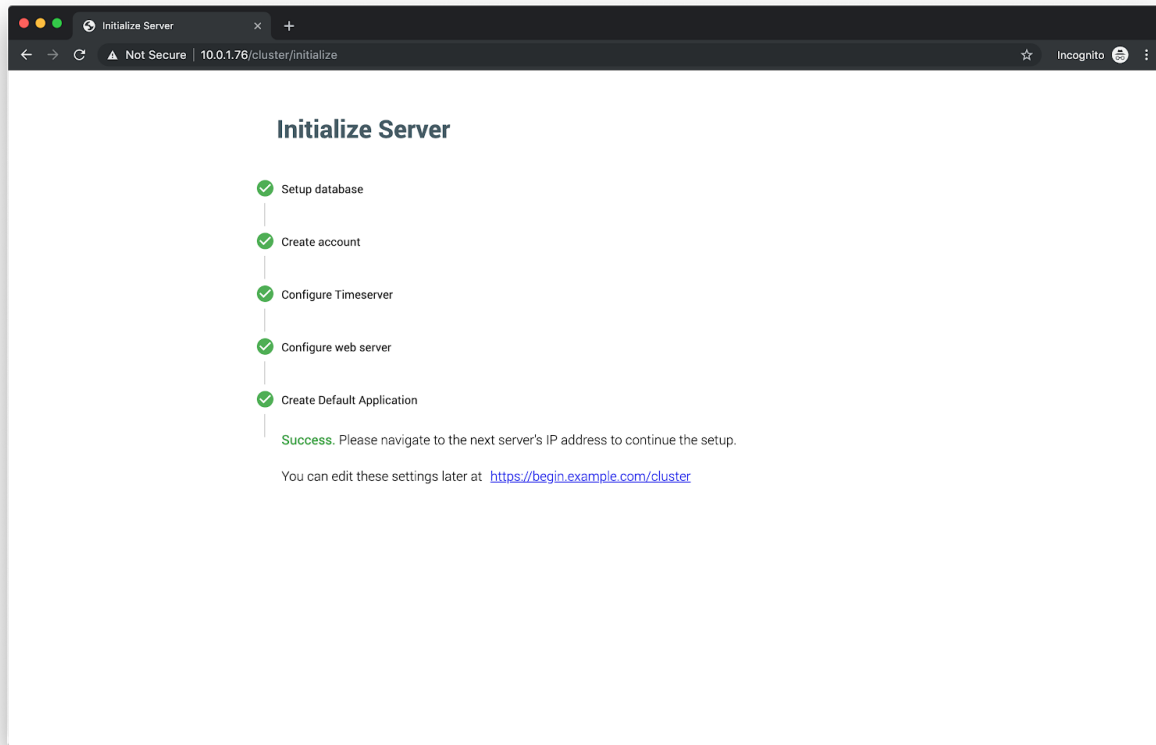
Default User information

**Username:** admin

**Password:** admin

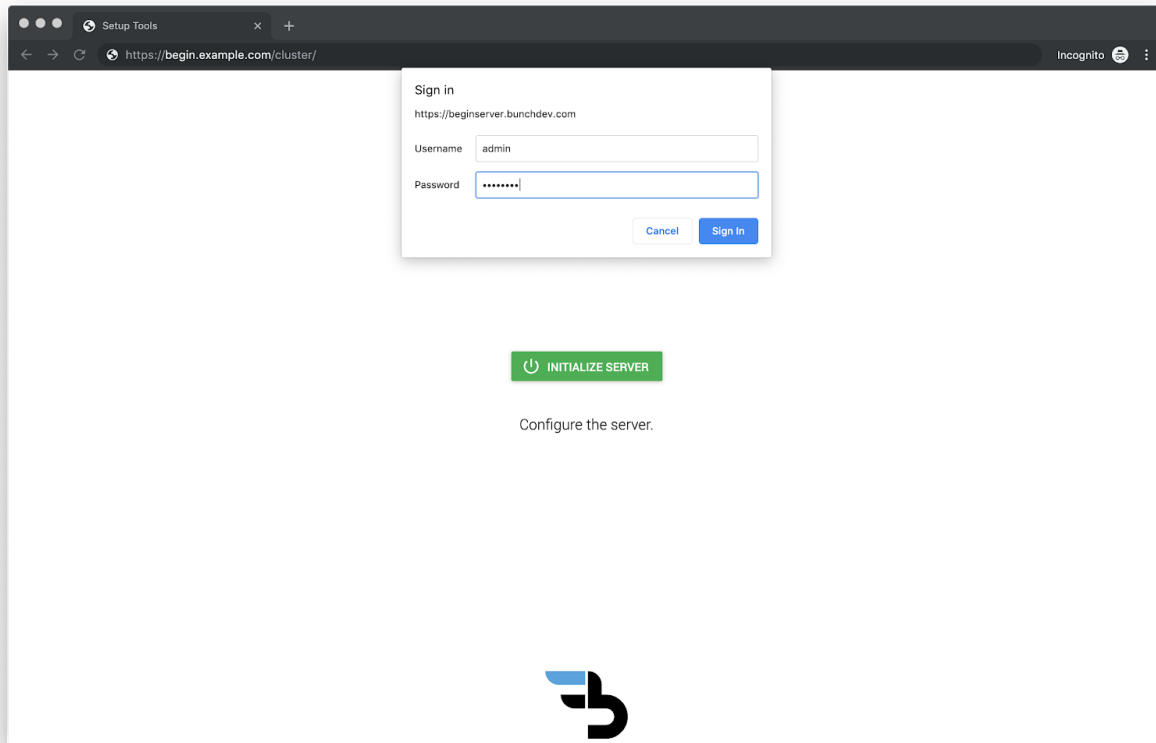


After creating default team navigate to the admin page by entering /admin after the domain name. For example, If the configured domain name is **begin.example.com** then the admin page is located at **begin.example.com/admin**.



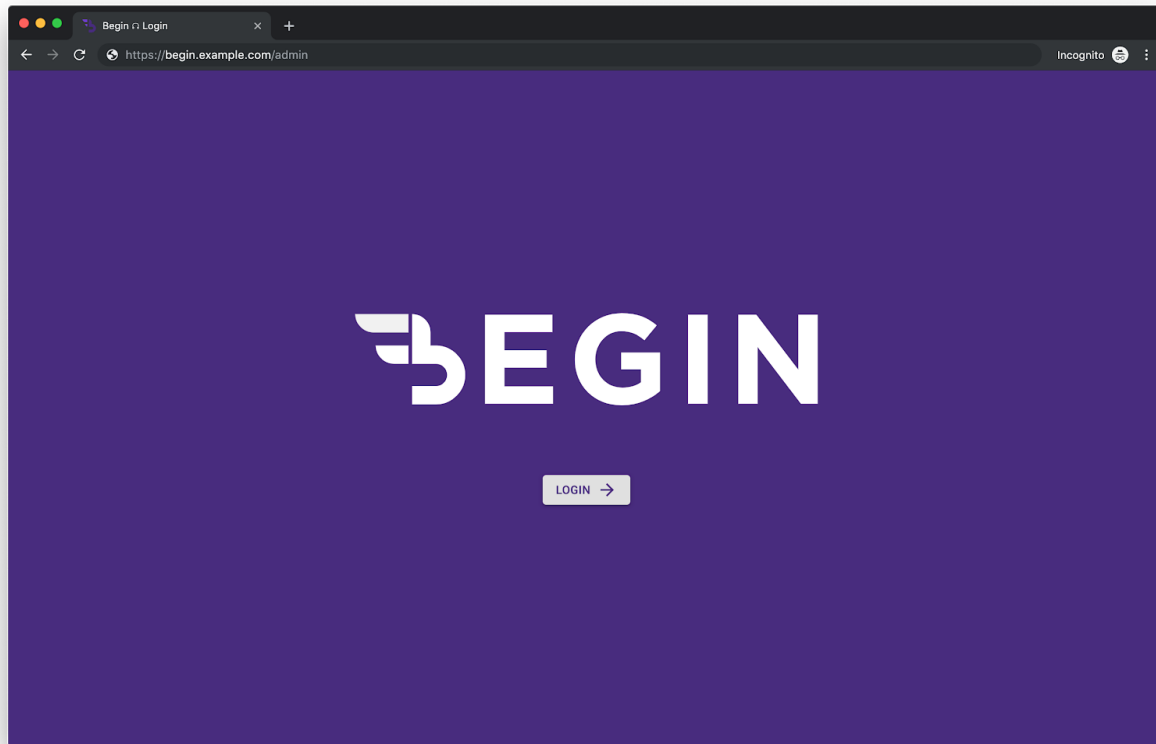
If the settings need to be updated in the future, go to the cluster page and enter the credentials used in **Initialize Server: Create account** step.

For example, If the **username** and **password** used in Create account step are **admin**, **password** respectively then enter those credentials in the popup dialog and click **Sign In** to log in to the cluster page.



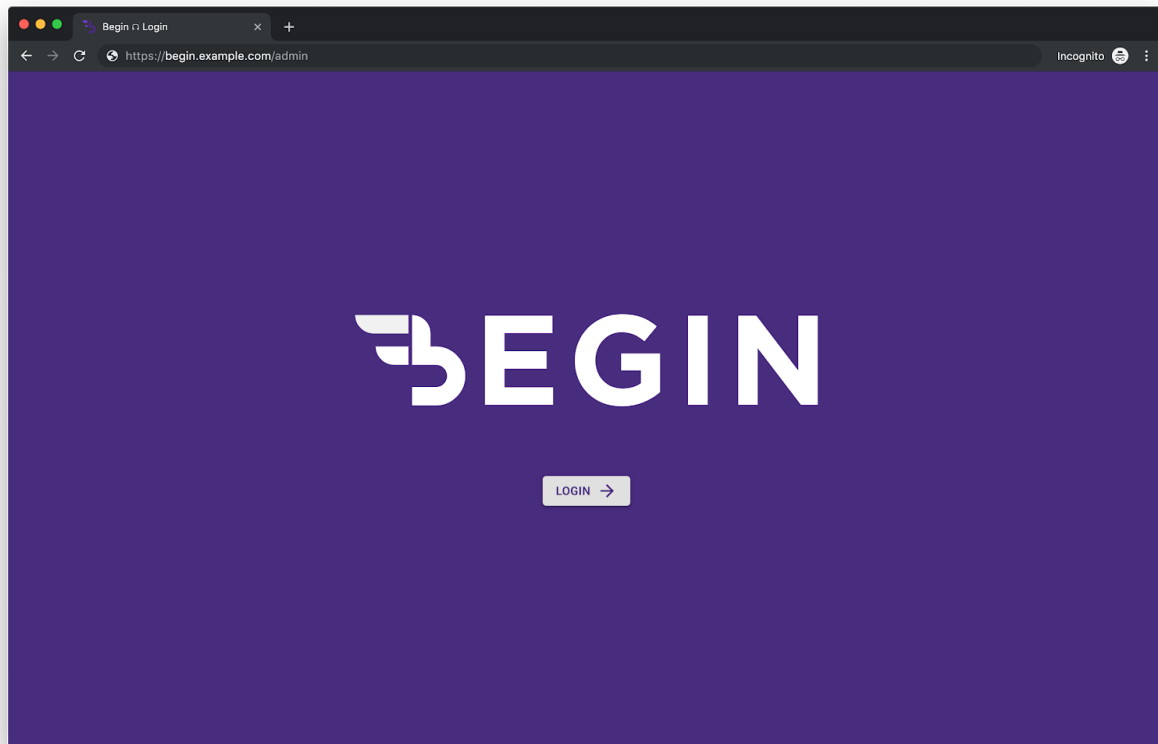
## Verify DNS and SSL

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



## Client Administration

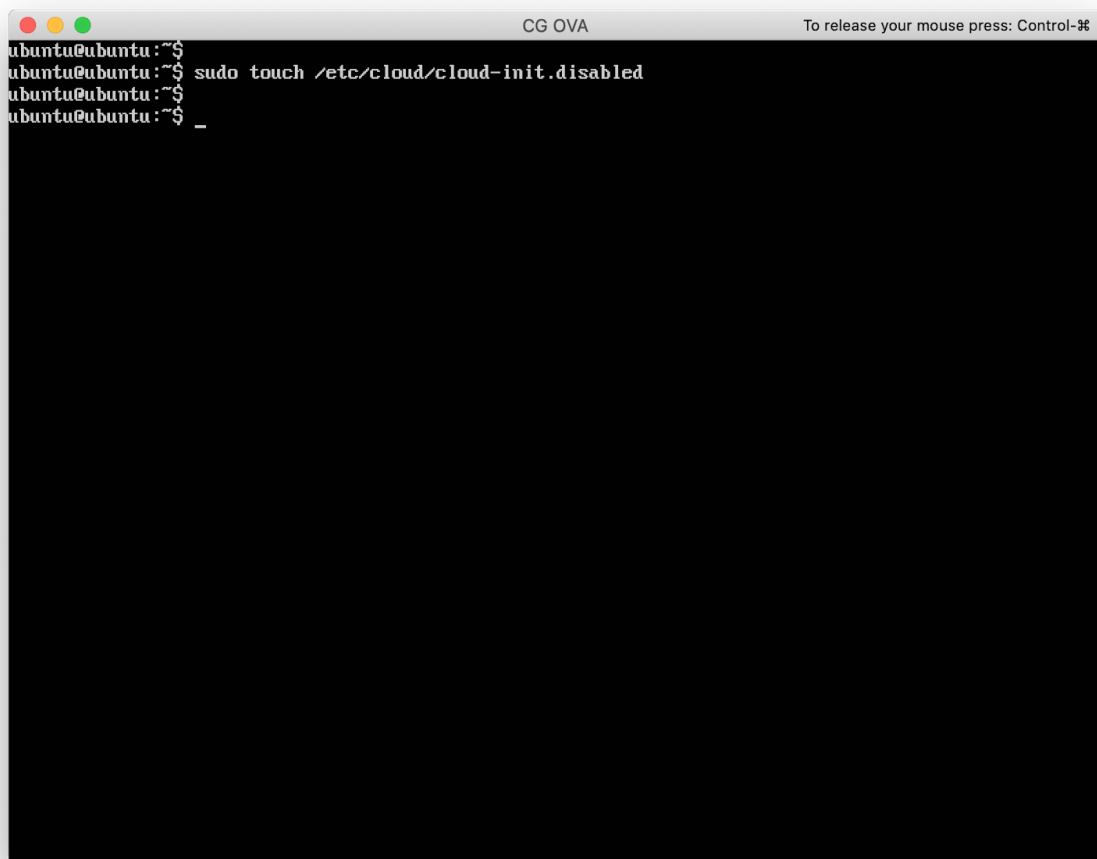
To access the client site, navigate to the **/admin** route. If the cluster hostname were **begin.example.com**, the address would be **https://begin.example.com/admin**.



## 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:~$ _
```

