



Cluster Deployment Guide

Version 1.5.0

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 the OVA	9
Cluster Setup	10
Individual Node DNS Entries	10
Load Balancing	10
Round-Robin DNS	10
Hardware (Websocket Enabled)	10
SSL Certificates	10
Node Setup	11
Network Setup (DHCP)	11
Network Setup (Static IP)	12
Initialize Cluster	19
Verify DNS and SSL	28
Client Administration	29

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, August 14th, 2017

- Initial release of documentation.

Wednesday, September 21st, 2017

- Admin portal added to verification.

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 Band, you must have:

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

OVA Deployment

Network

Port Usage Outside of Cluster Group

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

Port Usage Inside of Cluster Group

Protocol	Port	Direction	Purpose
TCP	7789	Inbound/Outbound	Cluster messaging
HTTPS	443	Inbound/Outbound	Band API
SSH	22	Inbound/Outbound	Cluster administration
TCP	1433*	Outbound	Database

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

OVA Deployment

System Requirements

Supported Platforms

VMware ESXI 5.5 and later are supported.

Cluster Size

The recommended size of a Band cluster is 2 nodes.

Virtual Machine Configuration

The requirements for a Band cluster node are:

CPU: 3 GHz dual core or 4 virtual processors

RAM: 8 GB

STORAGE: 80GB

Browsers

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

Band OVA 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.

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.

Node Setup

Network Setup (DHCP)

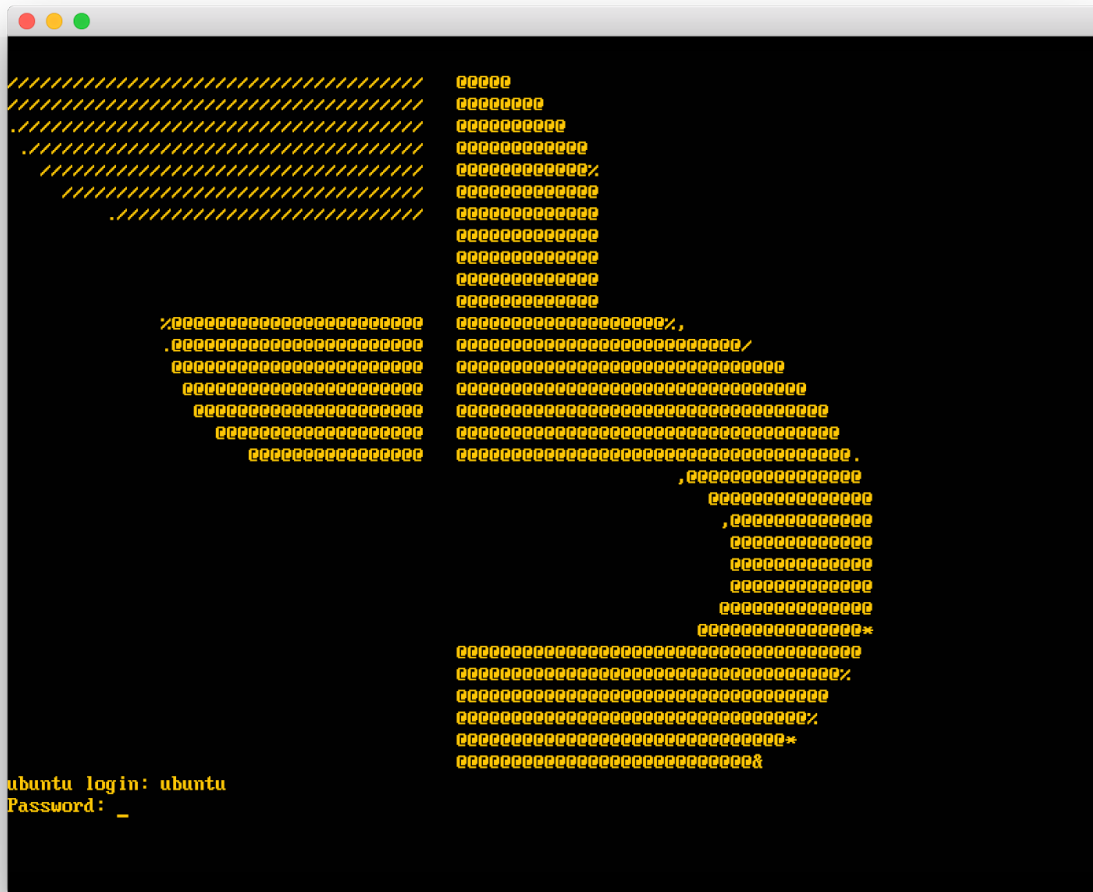
By default, nodes use dynamic host configuration protocol (DHCP) on network device eth0. No additional network setup is required on DHCP systems.

Network Setup (Static IP)

For systems with statically allocated IP addresses:

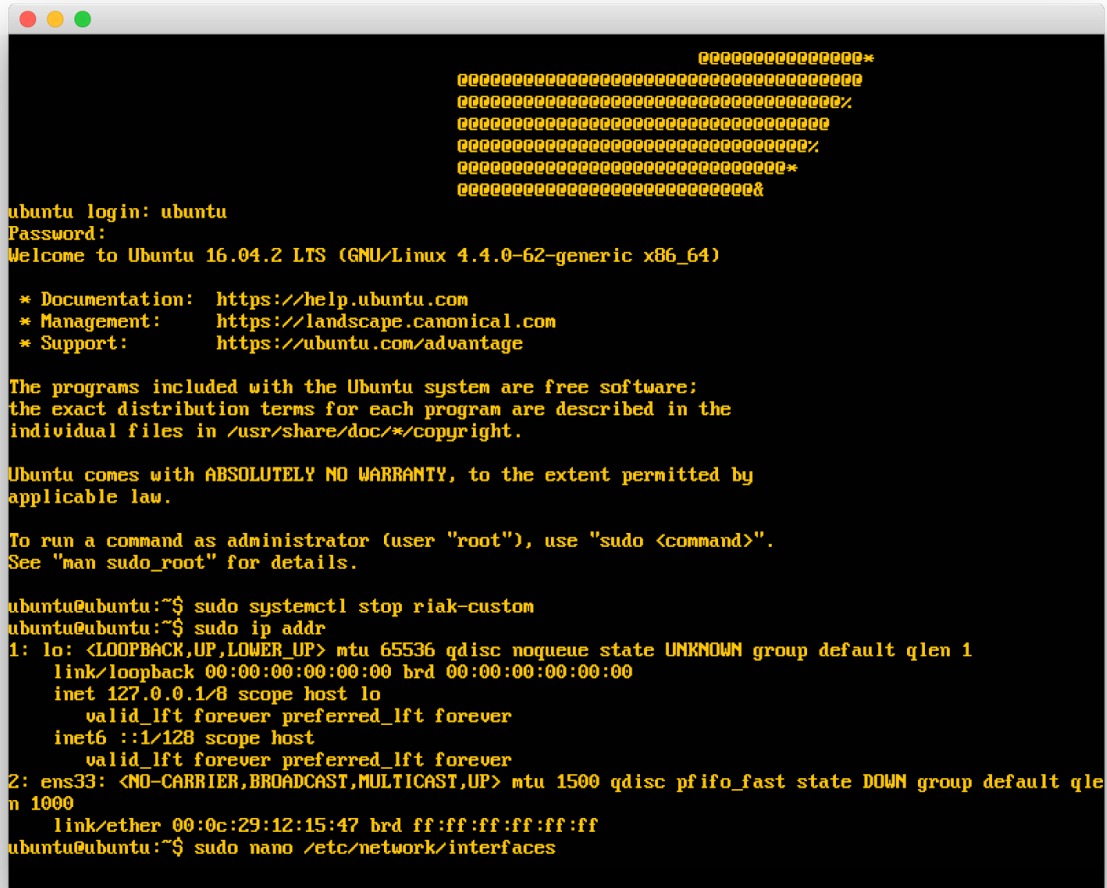
1. Access the virtual machine terminal.
2. At the login prompt, enter:

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



3. Open the network configuration file for editing:

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



```

                                *****
                                *****
                                *****%
                                *****%
                                *****%
                                *****
                                *****
ubuntu login: ubuntu
Password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

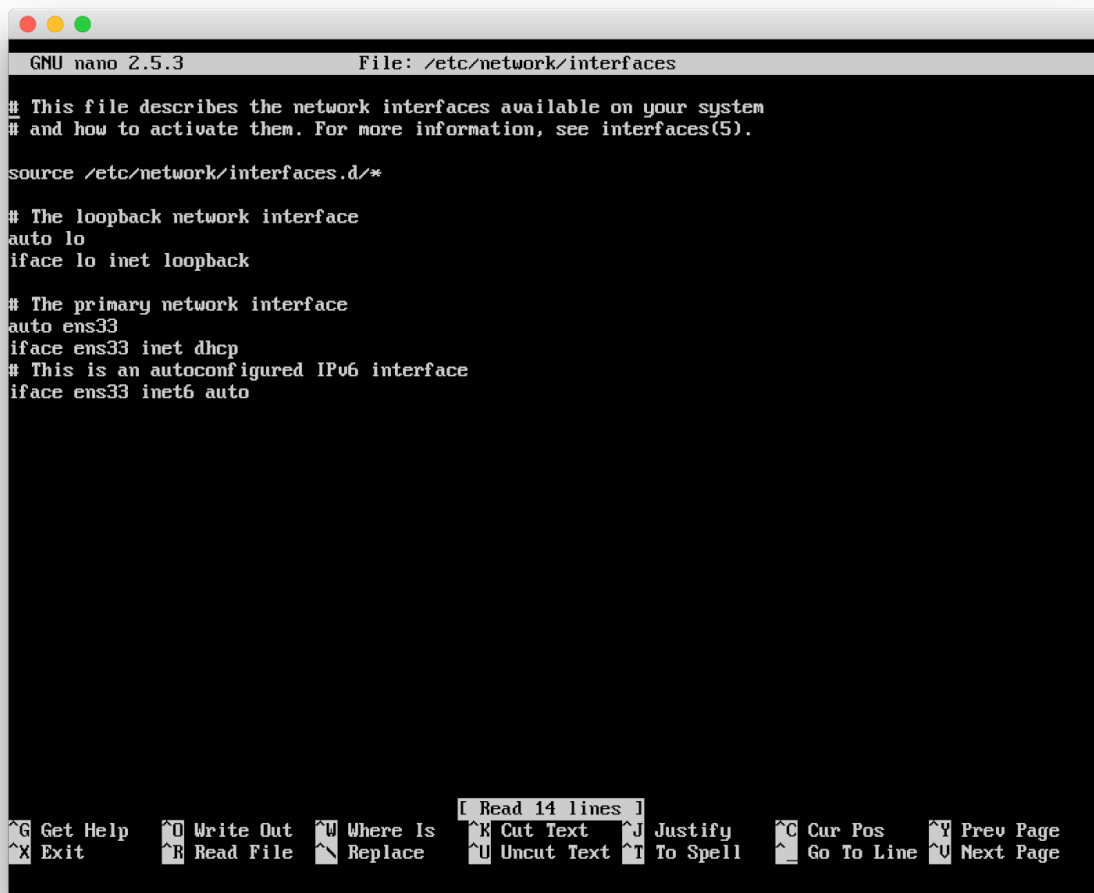
ubuntu@ubuntu:~$ sudo systemctl stop riak-custom
ubuntu@ubuntu:~$ sudo ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 00:0c:29:12:15:47 brd ff:ff:ff:ff:ff:ff
ubuntu@ubuntu:~$ sudo nano /etc/network/interfaces

```

4. 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
```

A screenshot of a terminal window running the nano text editor. The title bar shows 'GNU nano 2.5.3' and 'File: /etc/network/interfaces'. The editor displays the contents of the /etc/network/interfaces file, which includes comments and configuration for the loopback interface 'lo' and the primary interface 'ens33'. The configuration for 'ens33' is set to use DHCP and an autoconfigured IPv6 interface. The bottom status bar shows various keyboard shortcuts for nano, 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. A small status indicator '[Read 14 lines]' is also visible.

```
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/*

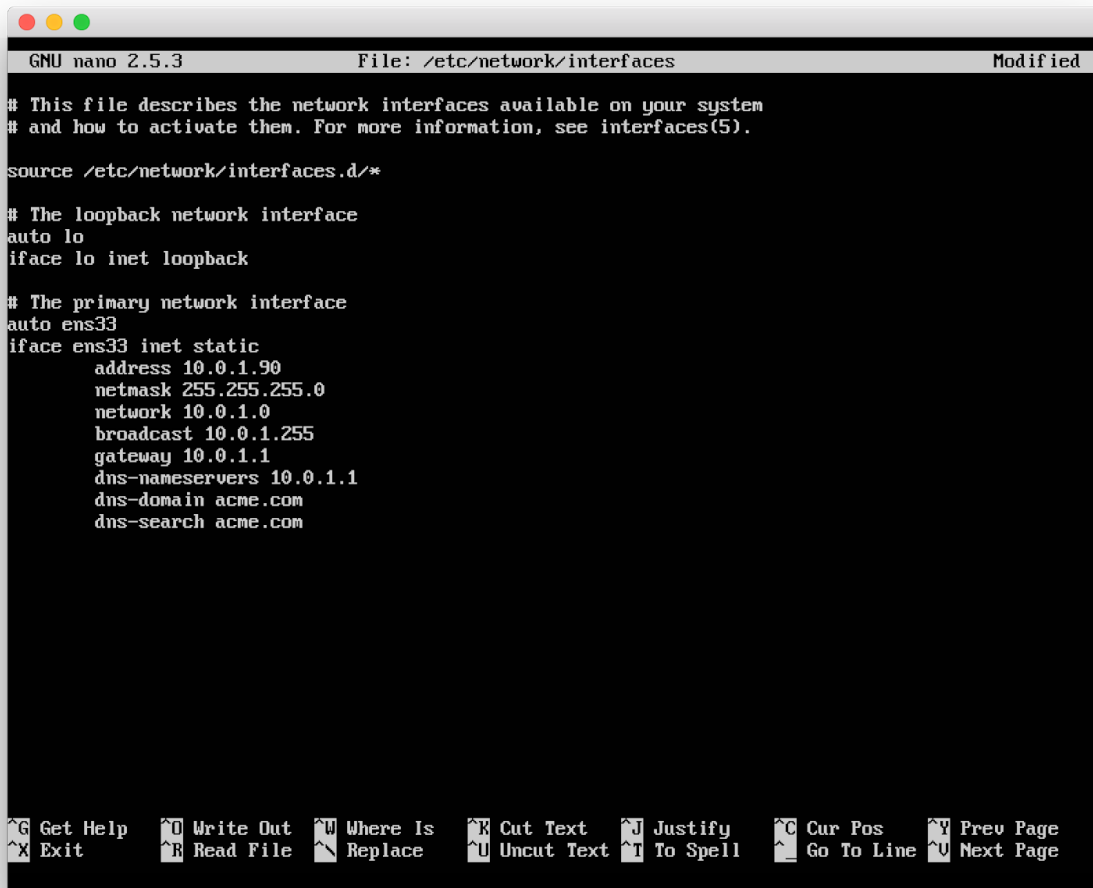
# The loopback network interface
auto lo
iface lo inet loopback

# 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 ^V 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 editor is editing the file /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).

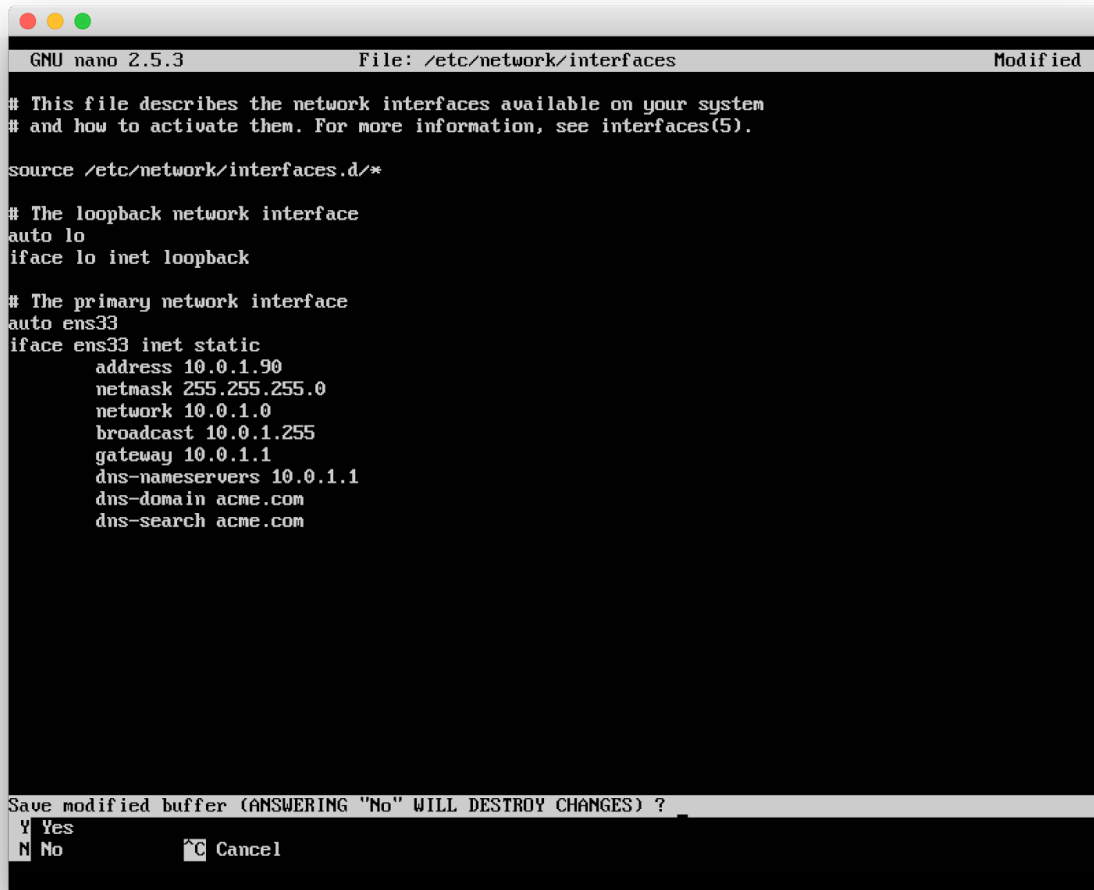
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto 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 editor's status bar at the bottom shows various keyboard shortcuts for navigation and editing, such as ^G Get Help, ^O Write Out, ^W Where Is, ^R 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.

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

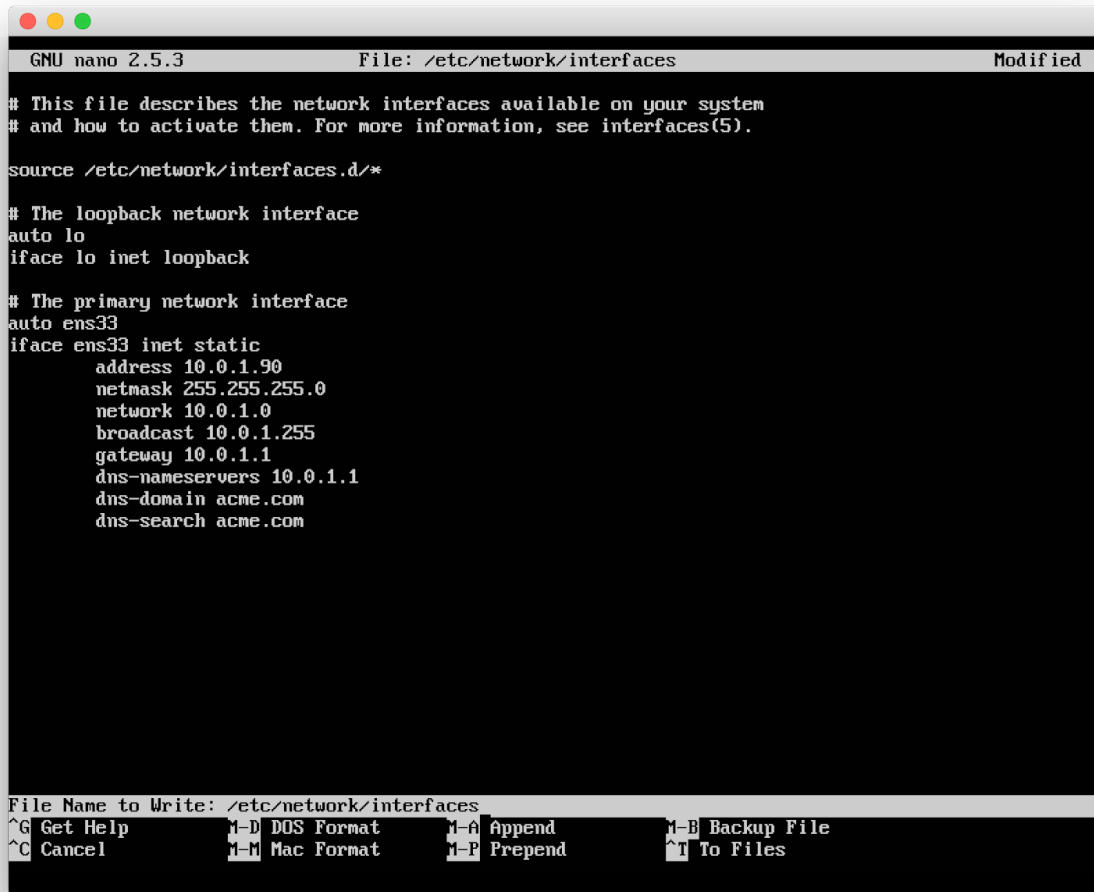
source /etc/network/interfaces.d/*

# 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
```


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 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

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 To Files
```

8. Restart the networking stack:

```
sudo systemctl restart networking
```

9. Reboot the virtual machine:

```
sudo reboot
```

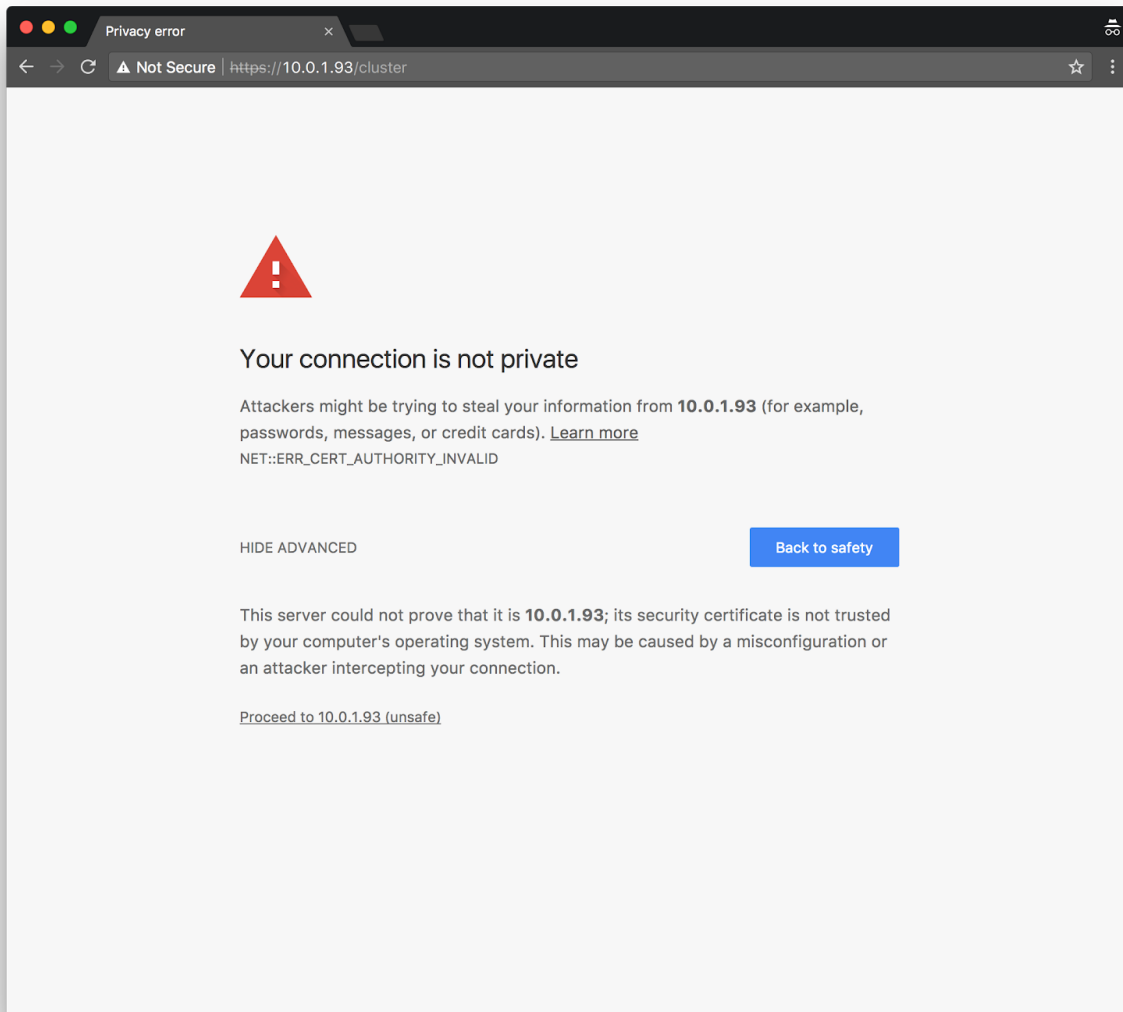
10. After the system restarts, confirm that it was configured successfully.

- Ping the configured IP address:

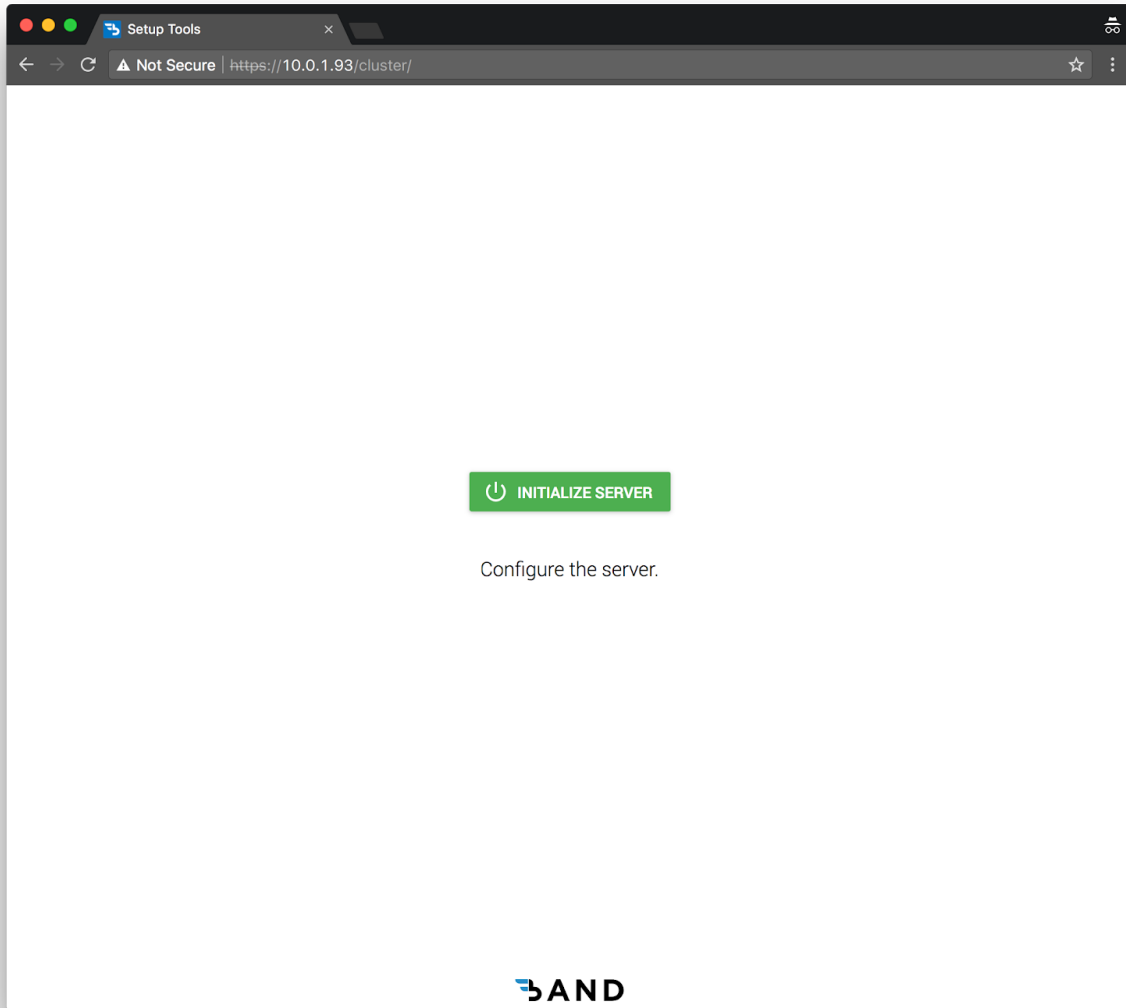
```
ping [configured IP address]
```
- Access **https://[configured IP address]/cluster** in a web browser and check for the cluster setup screen.

Initialize Cluster

Visit the HTTPS **/cluster** path of the first node. If the node IP were **10.0.1.93**, the address would be **https://10.0.1.93/cluster**. Proceed through the SSL certificate warnings.



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



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

The screenshot shows a web browser window titled 'Initialize Server' with the URL 'https://10.0.1.93/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: 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), 'Database Host Name' (a text input), 'Database Username' (a text input), 'Database Port Number' (a text input), and 'Database Password' (a text input). Below the form are two buttons: 'SAVE DATABASE SETTINGS' and 'GO BACK'.

Initialize Server

1 Setup database

Select database type... Database Name

Database Host Name Database Username

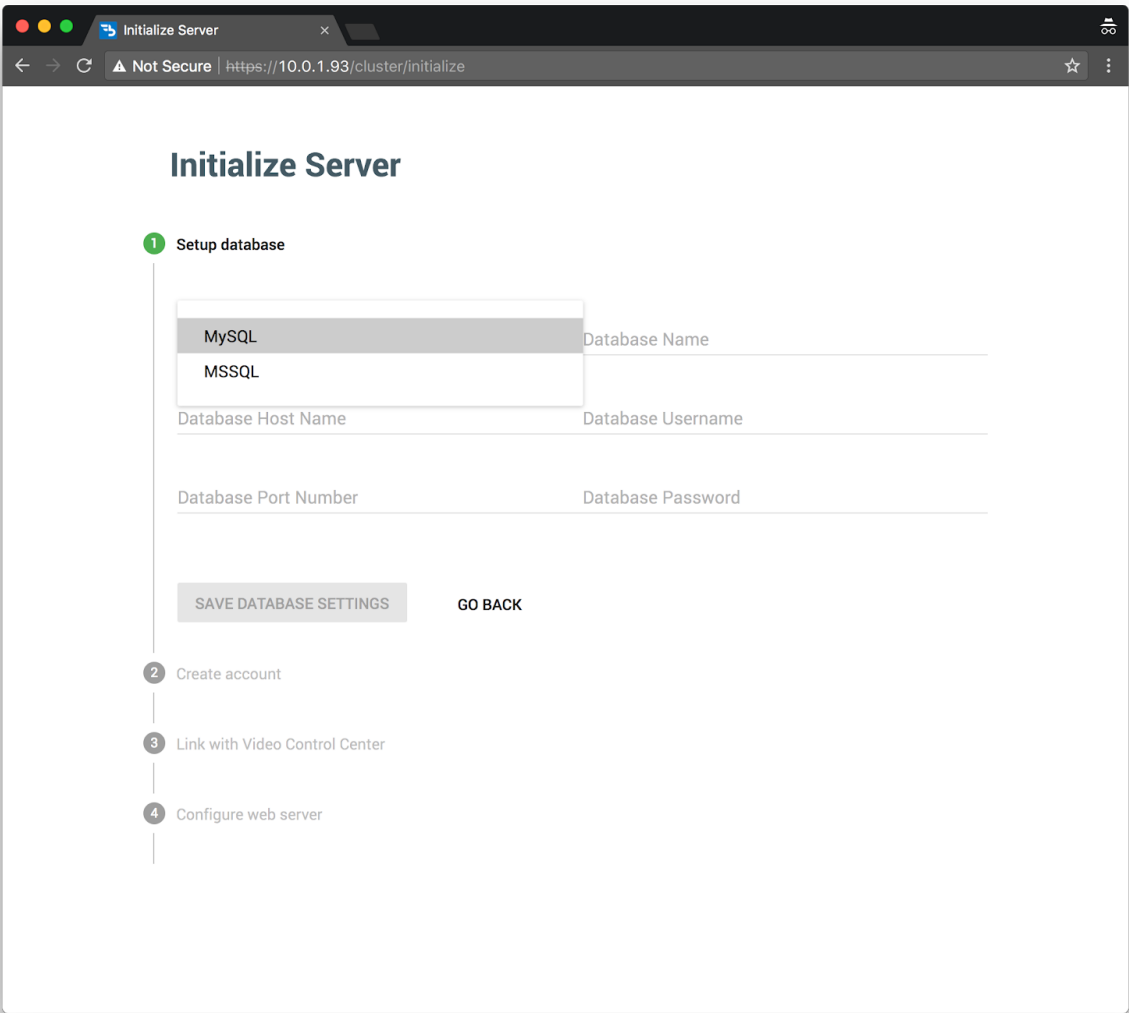
Database Port Number Database Password

SAVE DATABASE SETTINGS GO BACK

2 Create account

3 Link with Video Control Center

4 Configure web server



Initialize Server

Not Secure | https://10.0.1.93/cluster/initialize

Initialize Server

1 Setup database

Select database type...
MySQL

Database Name
band

Database Host Name
band.example.com

Database Username
root

Database Port Number
3306

Database Password
password

SAVE DATABASE SETTINGS

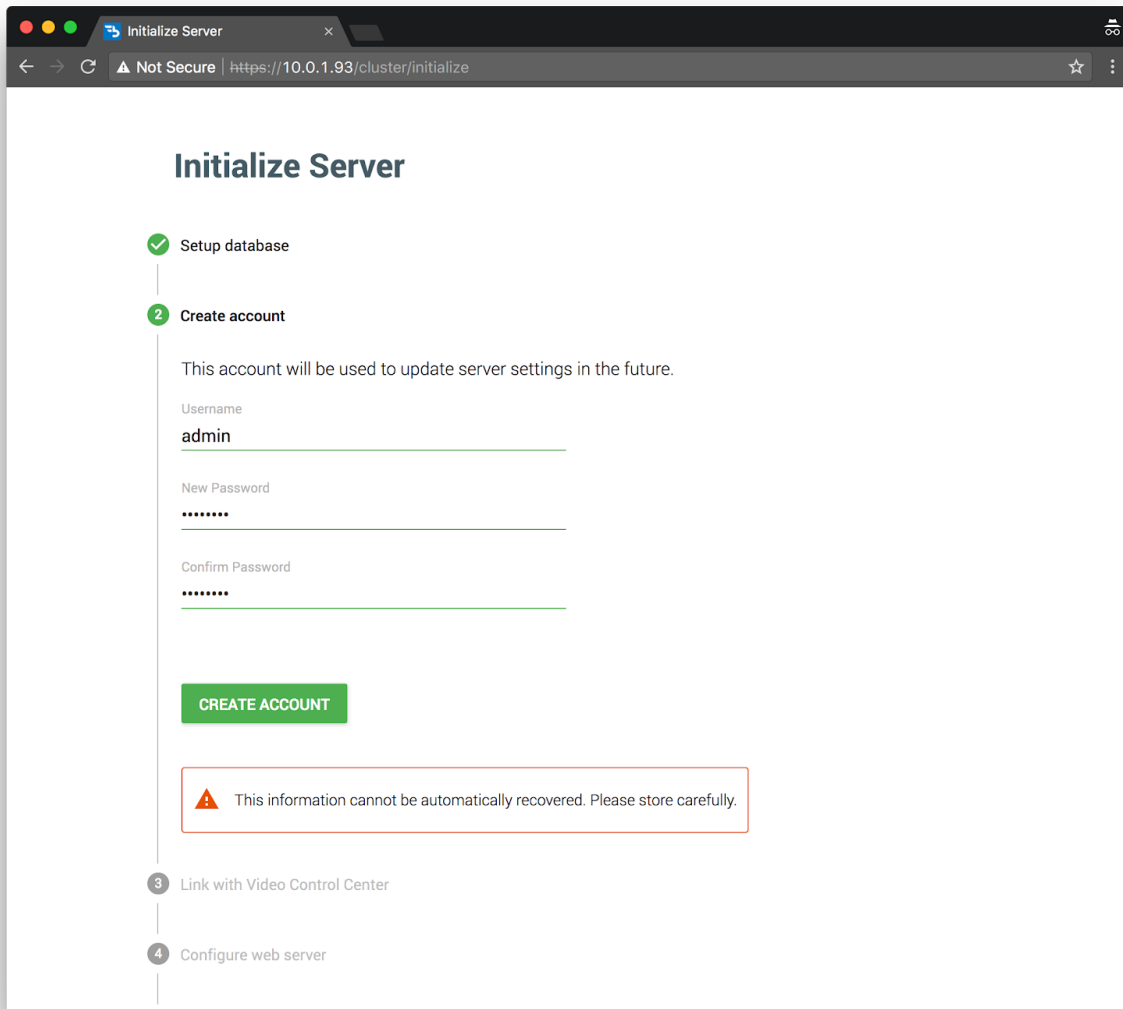
GO BACK

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.



The screenshot shows a web browser window titled "Initialize Server" with the URL `https://10.0.1.93/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. At the top, the title "Initialize Server" is displayed in a large, bold, dark blue font. A vertical progress bar on the left side of the page indicates the current step in the initialization process. The steps are: 1. Setup database (completed, marked with a green checkmark), 2. Create account (current step, marked with a green circle and the number 2), 3. Link with Video Control Center (not started, marked with a grey circle and the number 3), and 4. Configure web server (not started, marked with a grey circle and the number 4). The "Create account" section contains the following elements: a text input field for "Username" with the value "admin", a text input field for "New Password" with masked characters "*****", and a text input field for "Confirm Password" with masked characters "*****". Below these fields is a green button labeled "CREATE ACCOUNT". A red-bordered warning box with a red triangle icon contains the text: "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.

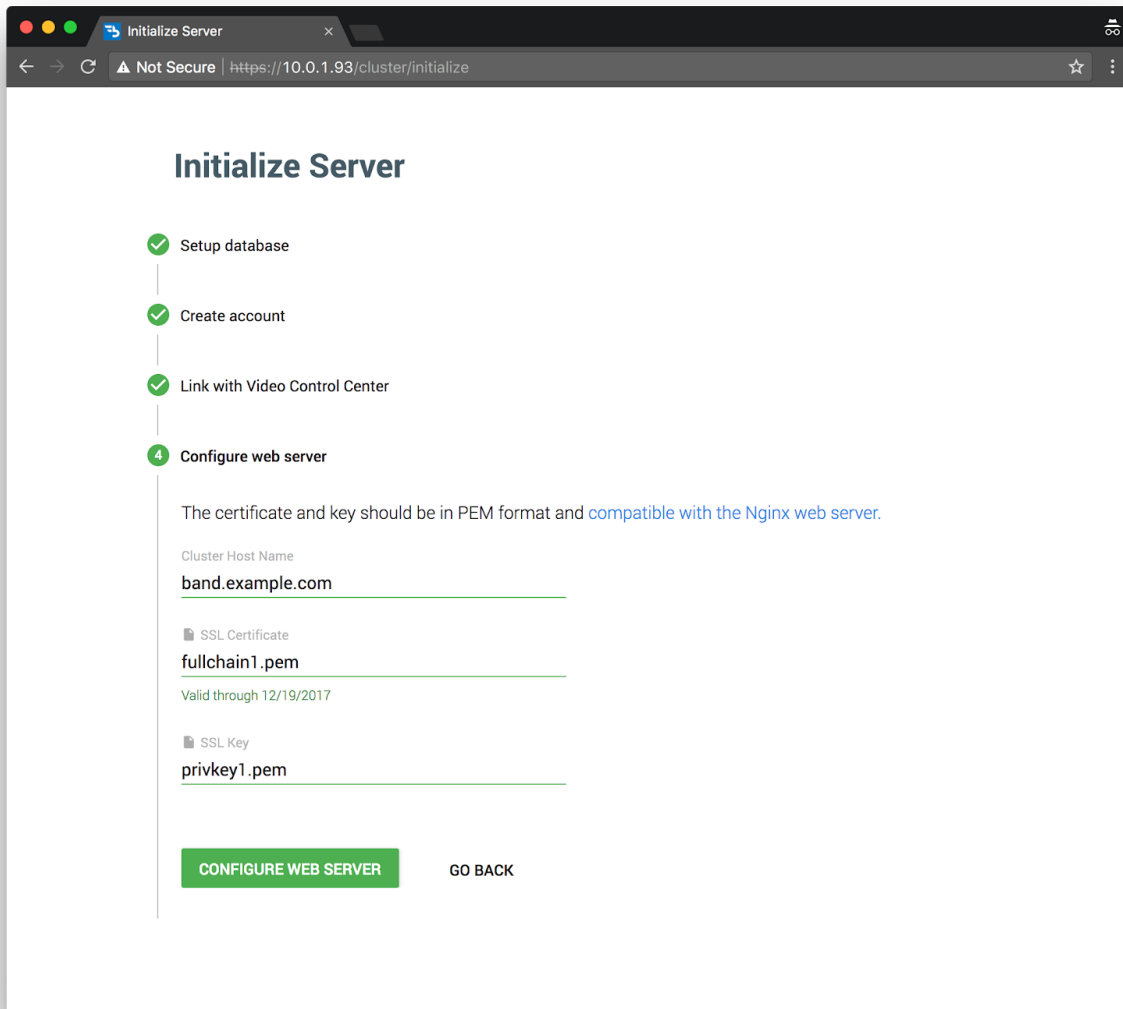
From **Initialize Server: Link with Video Control Center**, enter the Qumu Viewer Portal network and domain information. Enter the credentials of an oAuth client previously set up in the Qumu Admin Portal, and a principal ID with administrative access.

The screenshot shows a web browser window titled 'Initialize Server' with the URL `https://10.0.1.93/cluster/initialize`. The page has a progress bar on the left with four steps: 'Setup database' (checked), 'Create account' (checked), 'Link with Video Control Center' (active), and 'Configure web server' (next). The main content area for the active step includes instructions: 'Create an oAuth client in the Qumu admin portal and enter the credentials below.' It contains several input fields with labels and values: 'Viewer Portal Protocol' (https), 'oAuth Client ID' (ExampleClientID), 'Viewer Portal Host Name' (qumu.example.com), 'oAuth Client Secret' (ExampleClientSecret), 'Viewer Portal Port' (443), 'oAuth Redirect URL Pattern' (https://band.example.com/admin/login), 'Viewer Portal Domain' (example), and 'oAuth Access Token Expiry' (86400). Below these fields 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 an input field containing 'ExamplePrincipalID'. At the bottom of the form are two buttons: 'LINK WITH VIDEO CONTROL CENTER' (green) and 'GO BACK' (grey).

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 with the title 'Initialize Server' and the URL 'https://10.0.1.93/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. At the top, the title 'Initialize Server' is displayed in a large, bold, dark blue font. Below the title, there is a vertical progress bar with four steps, each marked with a green checkmark in a circle. The steps are: 'Setup database', 'Create account', 'Link with Video Control Center', and '4 Configure web server'. The fourth step is currently selected. Below the progress bar, there is a text block that reads: 'The certificate and key should be in PEM format and [compatible with the Nginx web server](#).' Below this text, there are three input fields. The first is labeled 'Cluster Host Name' and contains the text 'band.example.com'. The second is labeled 'SSL Certificate' and contains the text 'fullchain1.pem'. Below the second input field, there is a text label 'Valid through 12/19/2017'. The third input field is labeled 'SSL Key' and contains the text 'privkey1.pem'. At the bottom of the form, there are two buttons: a green button labeled 'CONFIGURE WEB SERVER' and a gray button labeled 'GO BACK'.

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](#).

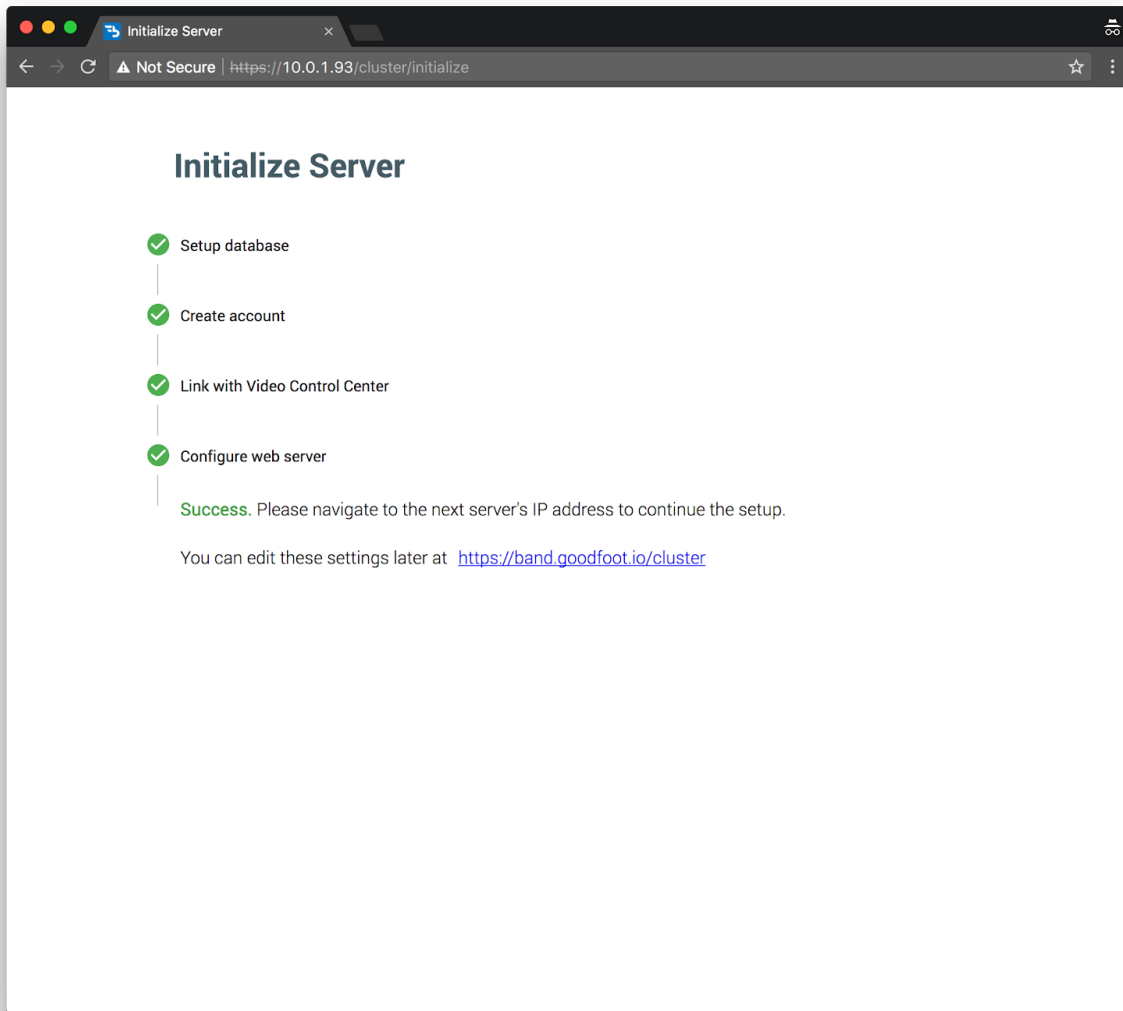
Cluster Host Name
band.example.com

SSL Certificate
fullchain1.pem
Valid through 12/19/2017

SSL Key
privkey1.pem

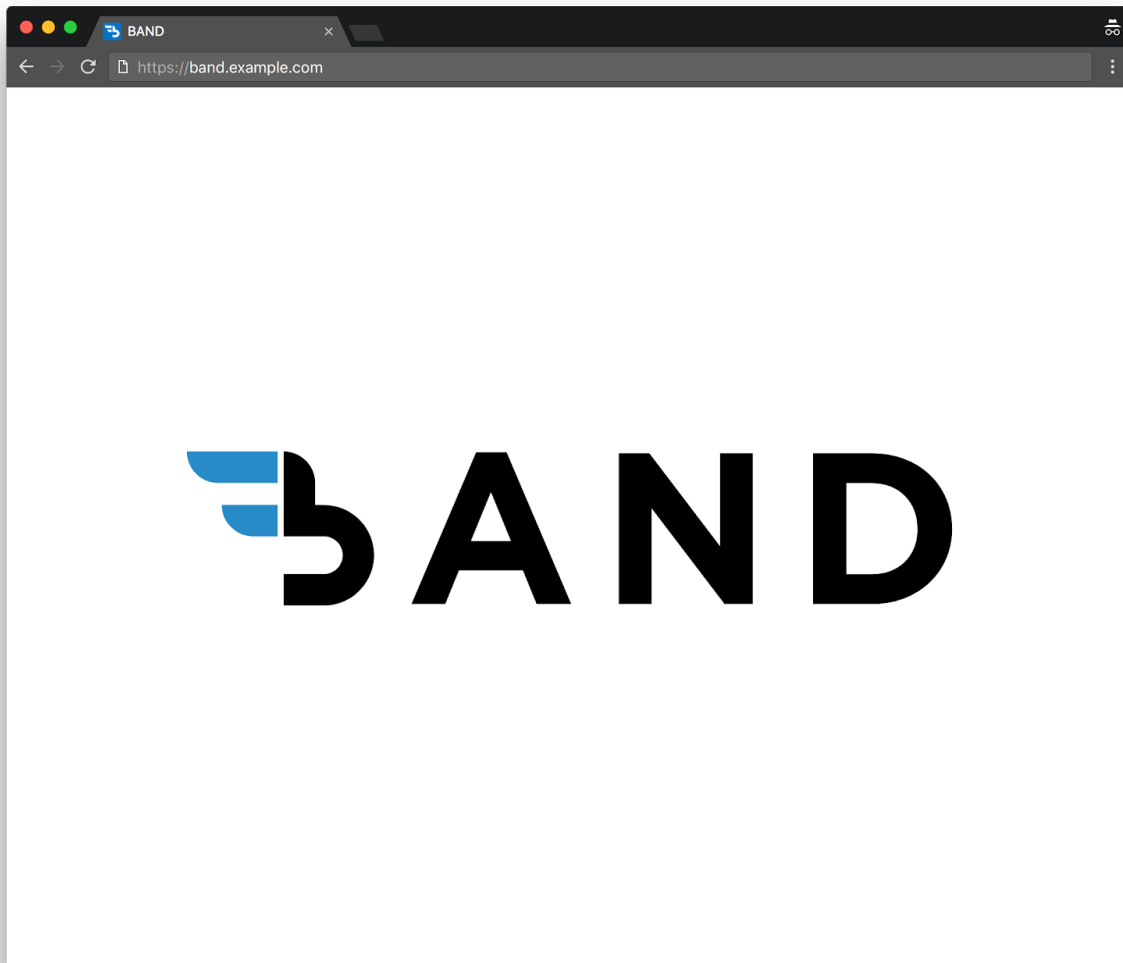
CONFIGURE WEB SERVER **GO BACK**

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 **band.example.com**, the address would be **https://band.example.com**.



Client Administration

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

Please note, the user that will be initializing Band needs to have a **Super User** role.

