ExpressCluster AWS Witness Server

How-to setup an ExpressCluster witness server using an AWS Lightsail instance.

Prerequisites

- Amazon AWS account
- An existing cluster running NEC ExpressCluster 4.1 or higher
- WinSCP
- Putty or other SSH client (optional)

Overview

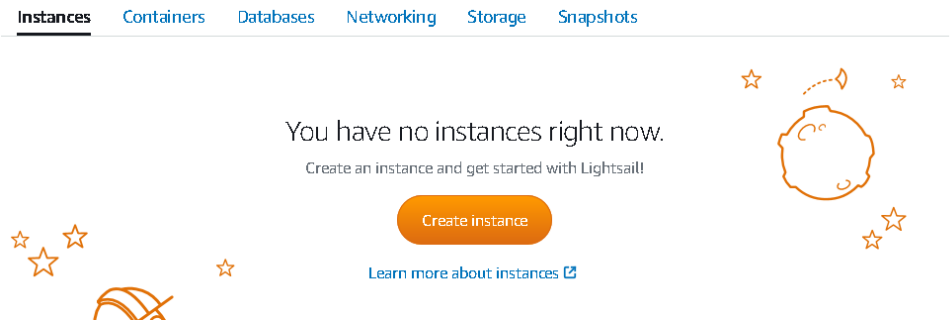
1. Create an AWS Lightsail instance
2. Create Static IP
3. Setup Firewall
4. Upload witness software
5. Install witness software
6. Configure witness software as a service
7. Add witness server to ExpressCluster

Step-by-step

Step 1 - Create an AWS Lightsail instance

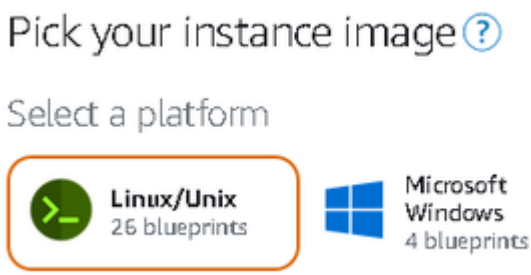
- Login to AWS Lightsail Homepage

- Click Create instance

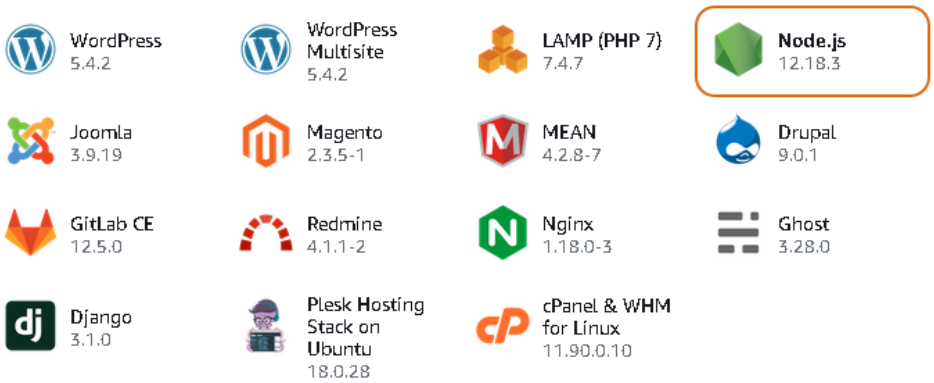


- Chose the region for the instance

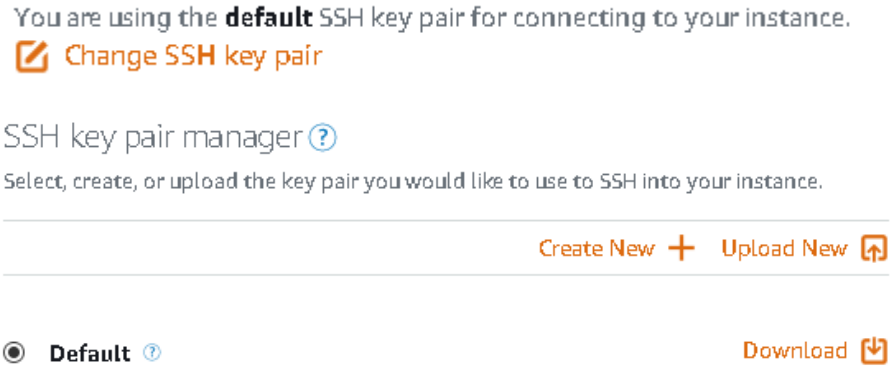
- Chose Linux/UNIX platform



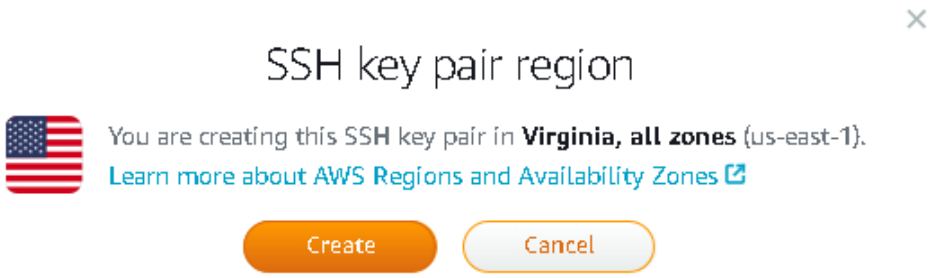
- Select the Node.js blueprint

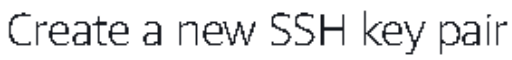


- Click the “Change SSH key pair” link

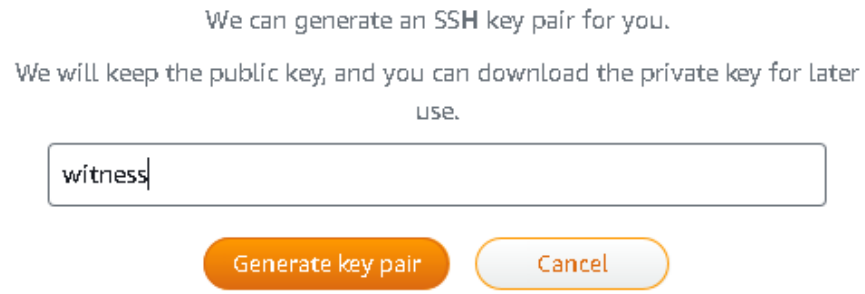


- Click “Create New”
- Click Create

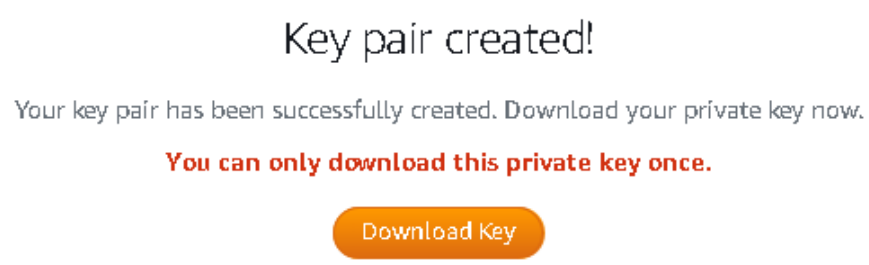




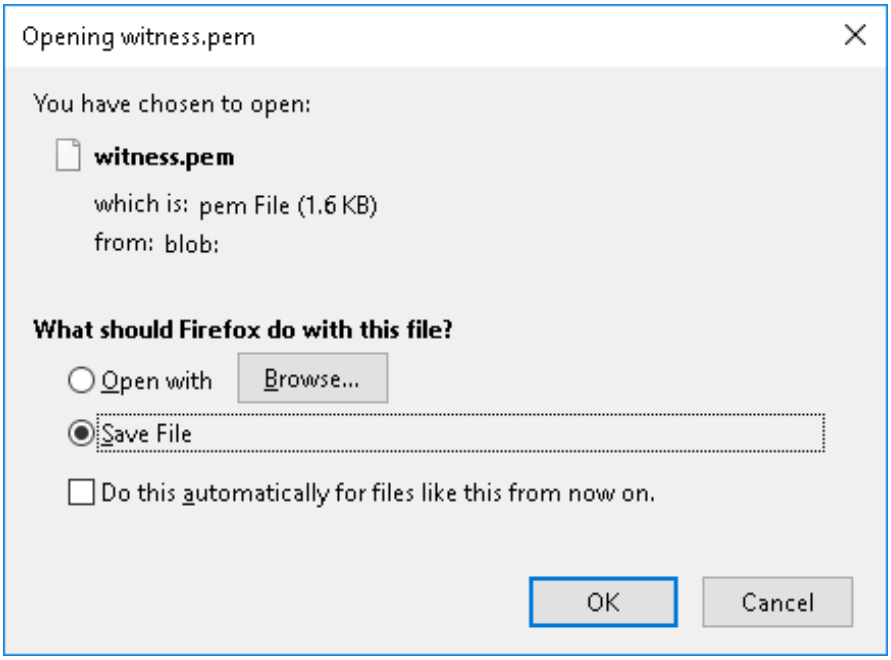
- Choose a name for the key pair and click Generate key pair.



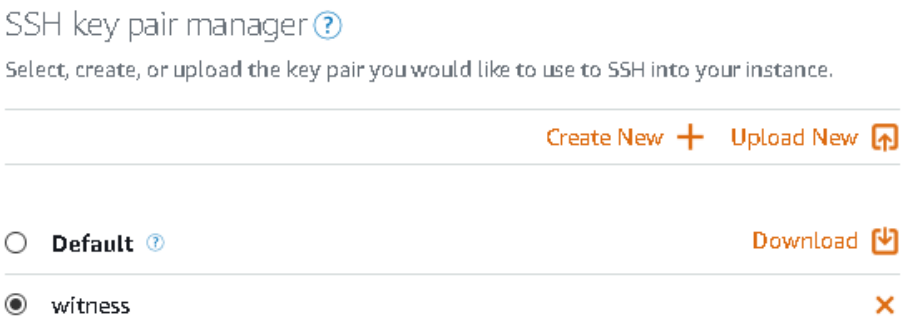
- Click download key



- Save the private key file to somewhere convenient.

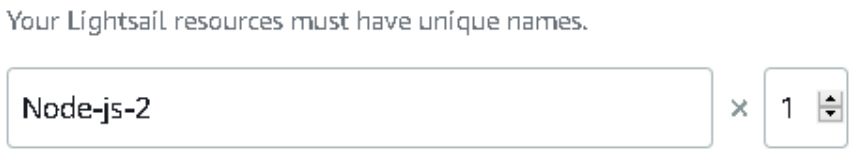


- Verify that the new key pair is selected instead of the Default.



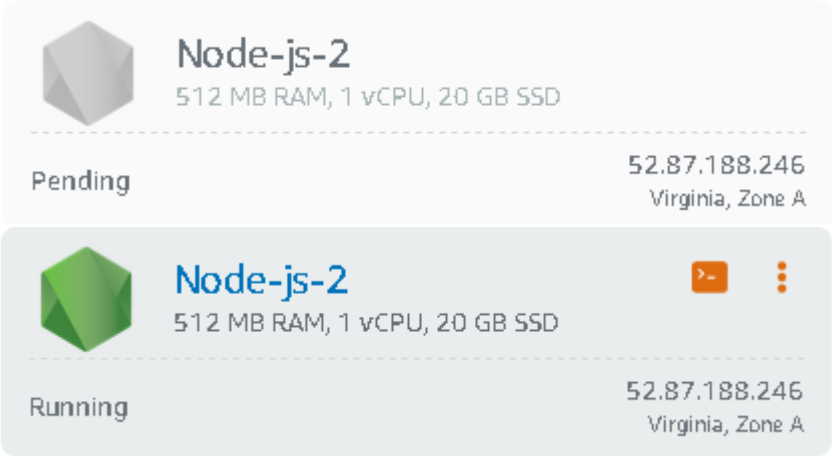
Identify your instance

- Chose a name for the instance.



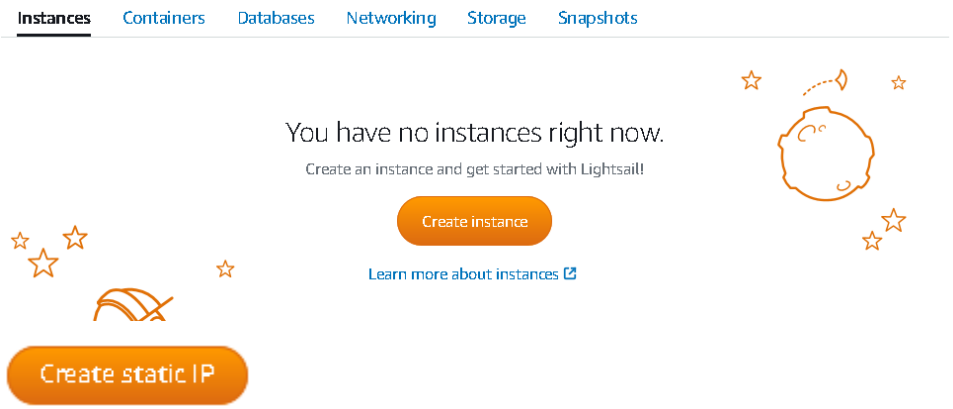
- Click Create Instance

- Wait for status to change from pending to running



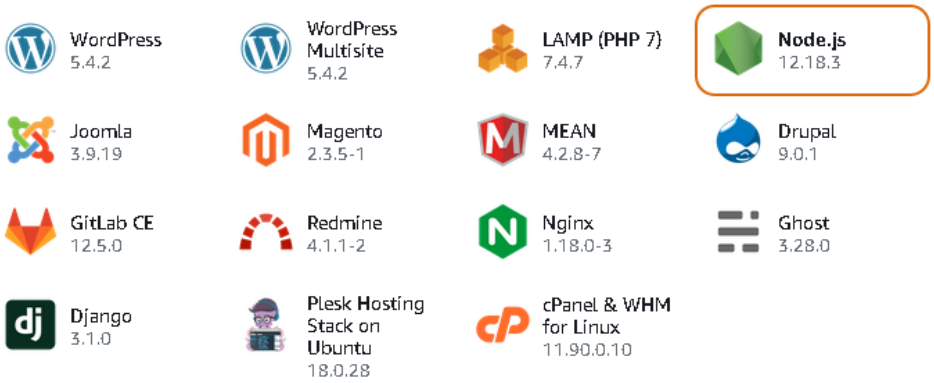
Step 2 - Create static IP

- Click Networking

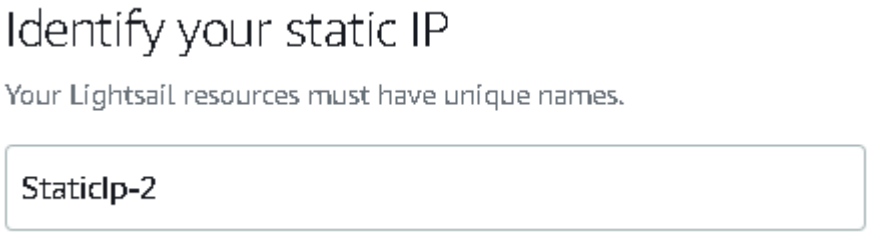


- Click Create static IP

- Select the instance to attach the IP to

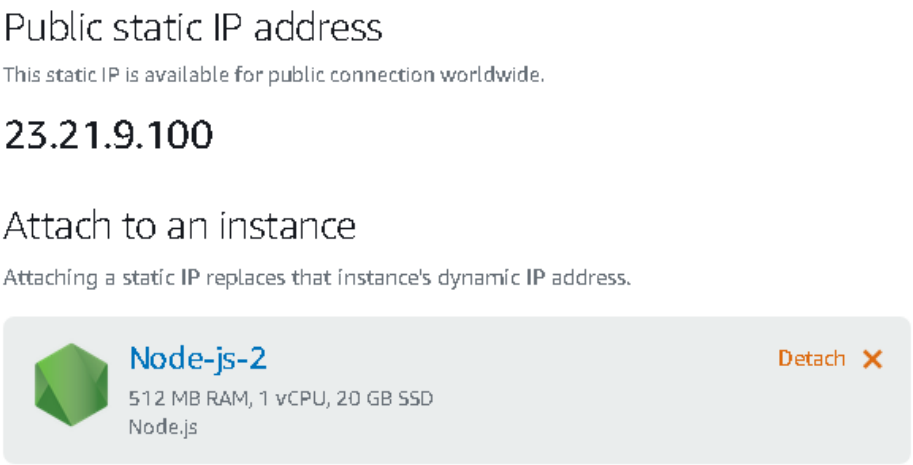


- Choose a name to identify the static IP



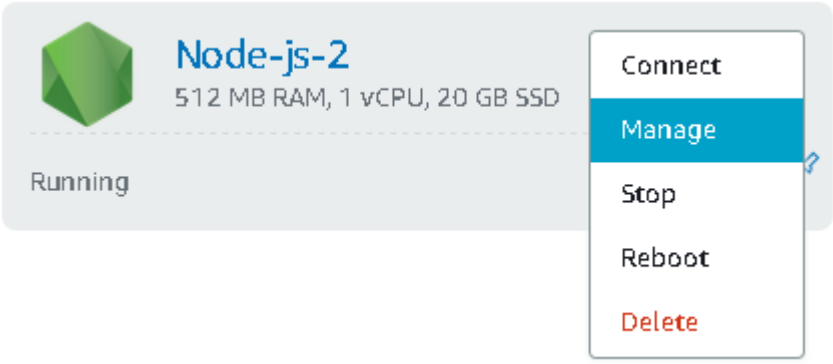
- Click create

- Verify and take note of static IP information

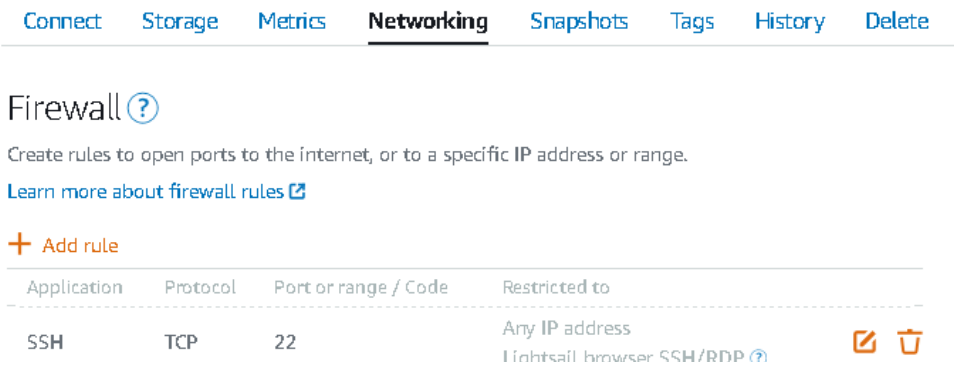


Step 3 - Setup Firewall

- From the AWS Lightsail home page, click on the toolbar radio on the right side of the instance and click manage



- Click Networking



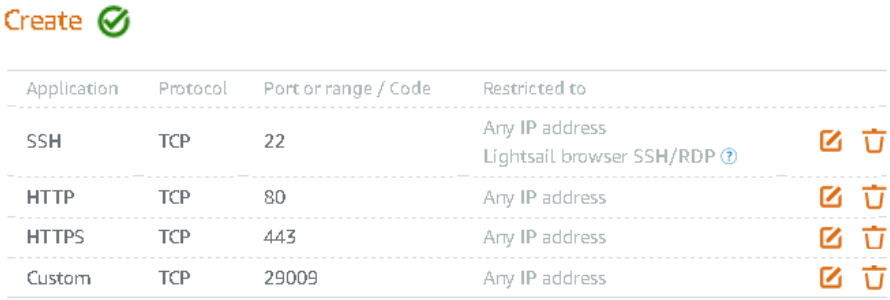
- Under Firewall click Add rule

HTTP	TCP	80	Any IP address
HTTPS	TCP	443	Any IP address

- Set the port to 29009

> NOTE: You can click the “Restrict to IP address” box to add the public IP(s) of the clustered servers to strictly limit connections on this port to the clustered servers.

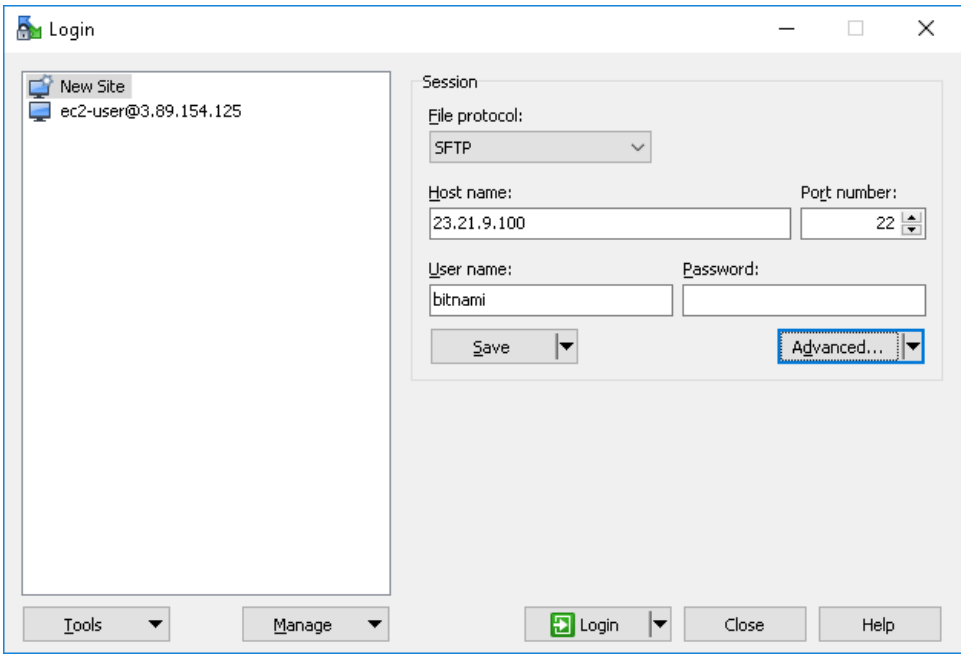
- Click create
- Verify the new rule is listed

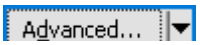


Step 4 - Upload witness software

- Launch WinSCP

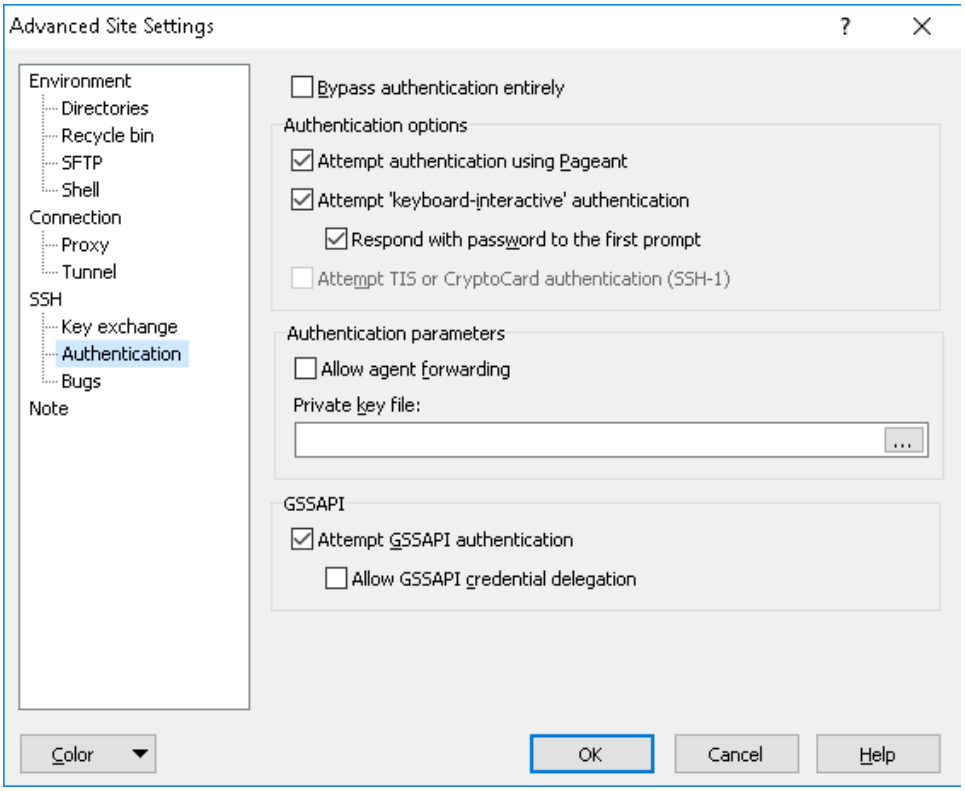
- Fill out the session settings as shown. NOTE: Be sure the username is set to “bitnami”





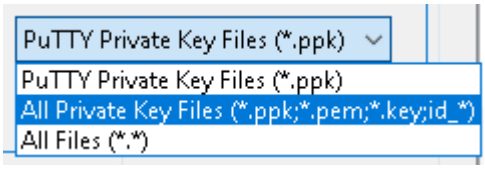
- Click the Advanced button

- Highlight Authentication on the left

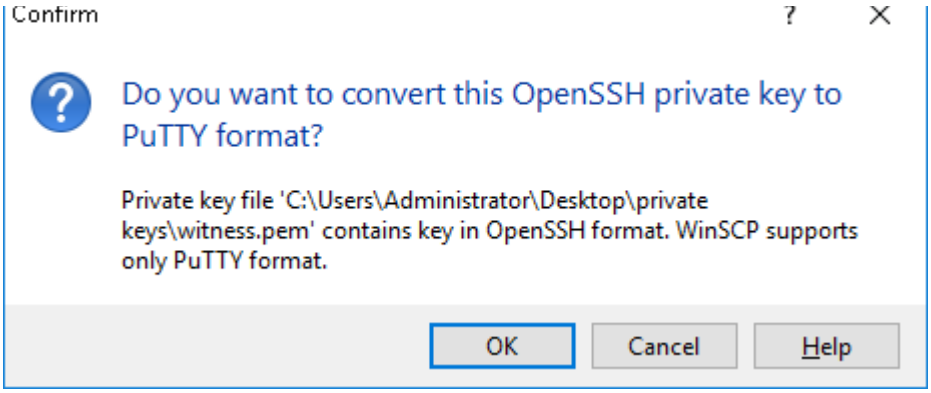


- Under Authentication parameters, click the "…" button to select a private key file

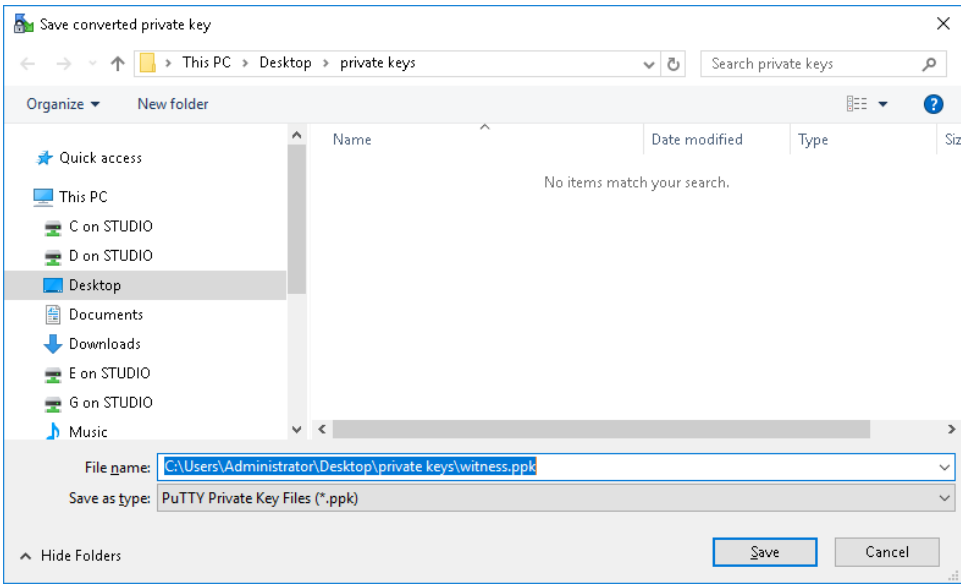
- Click the dropdown on the bottom right, select "All private key files", and open the private key that was downloaded previously from AWS



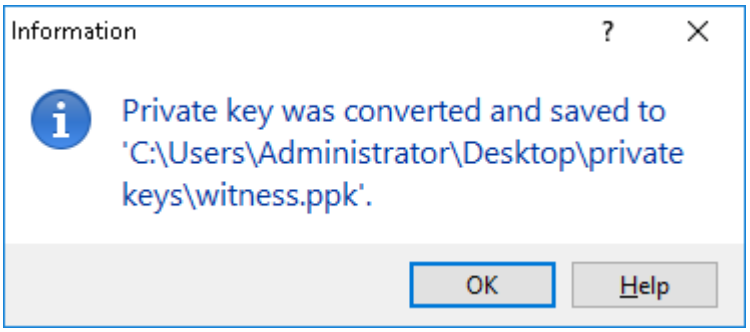
- When prompted to convert the key to putty format, click ok



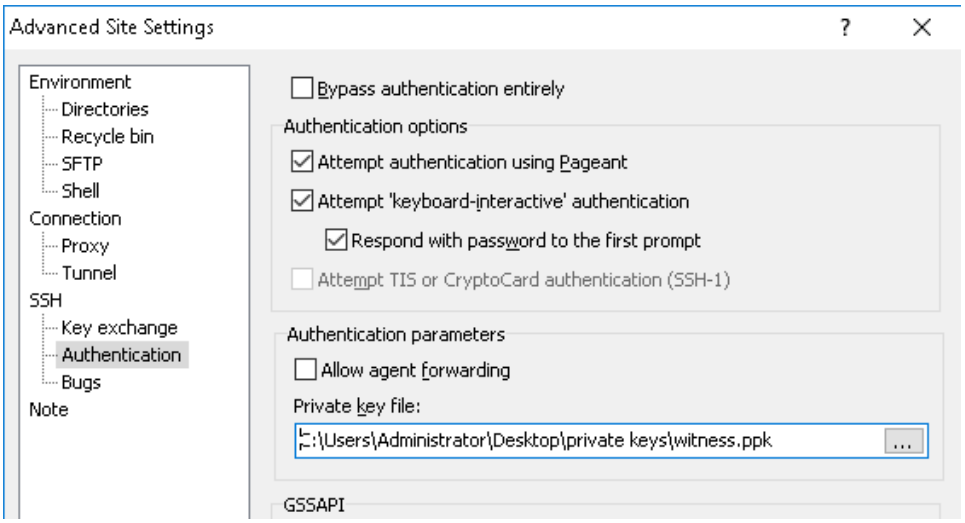
- Save the newly converted key

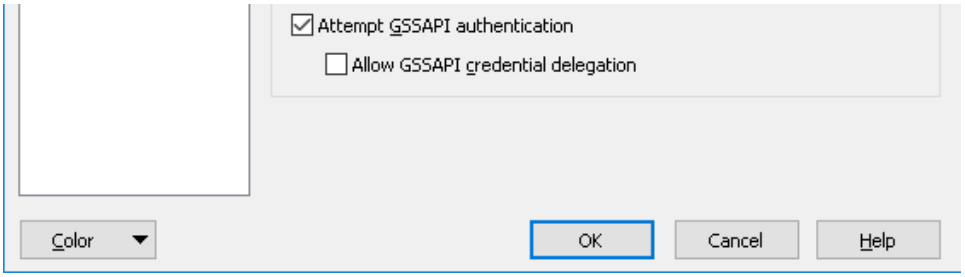


- Click ok



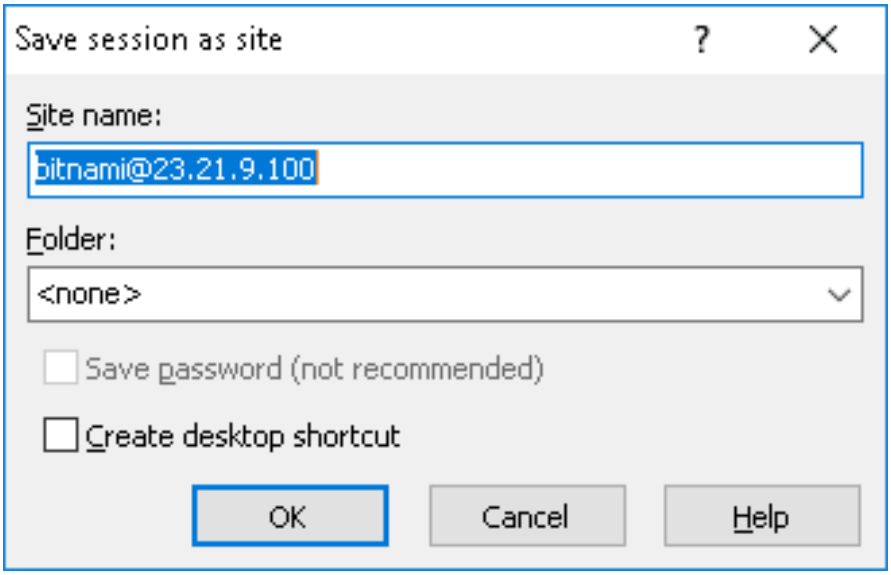
- Click ok again





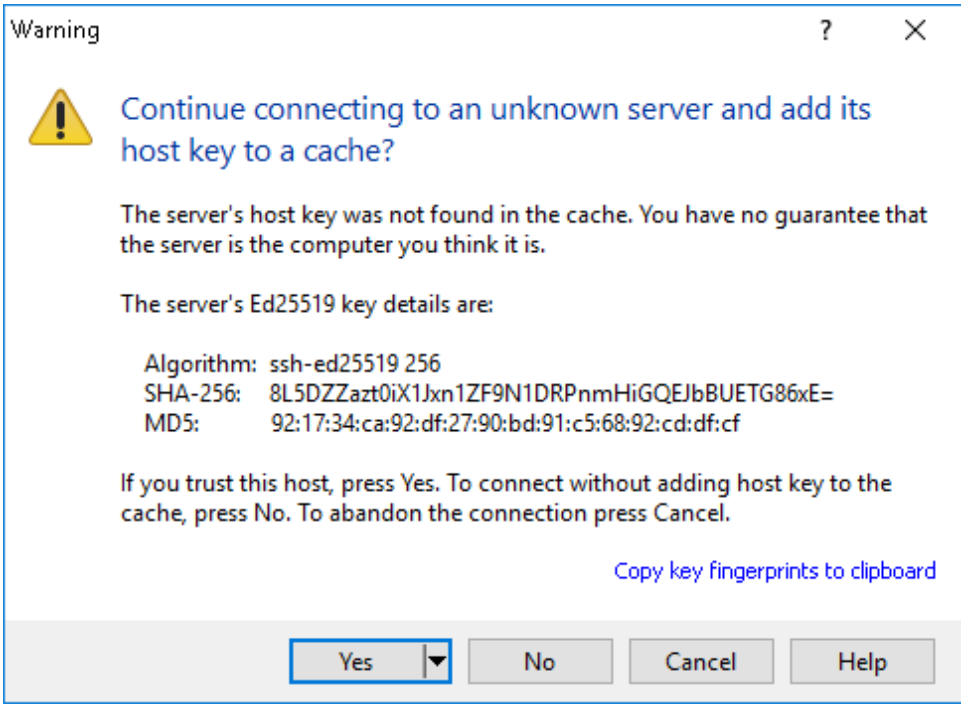
- Click Save

- Choose a session name and click ok

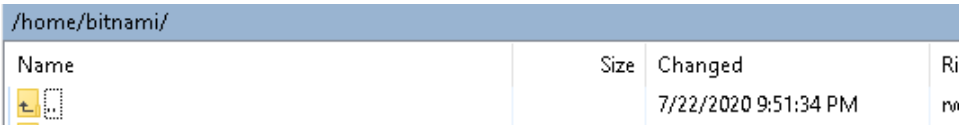


- Click Login

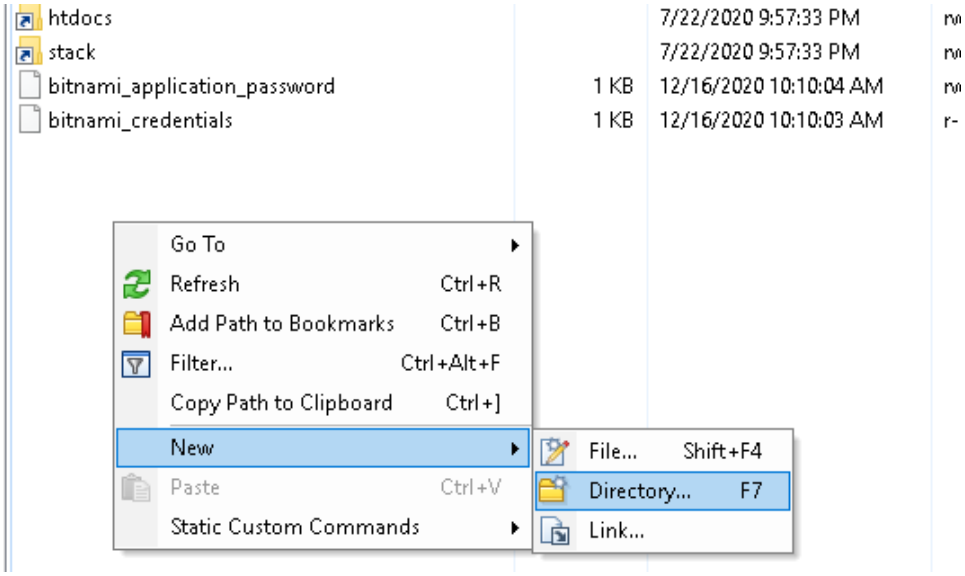
- Click yes to trust the host



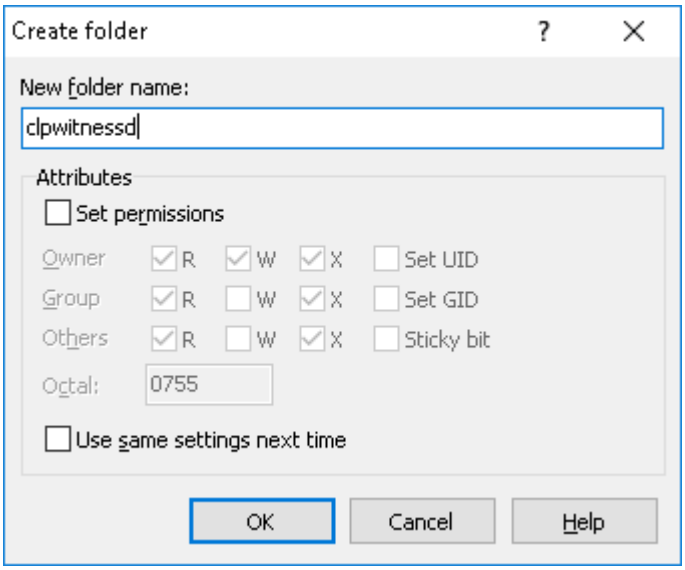
- On the host side file browser right



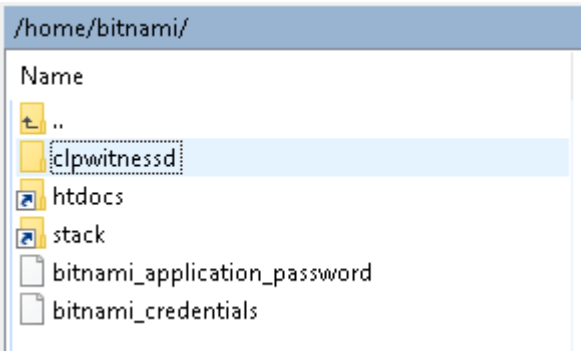
click and select New->Directory



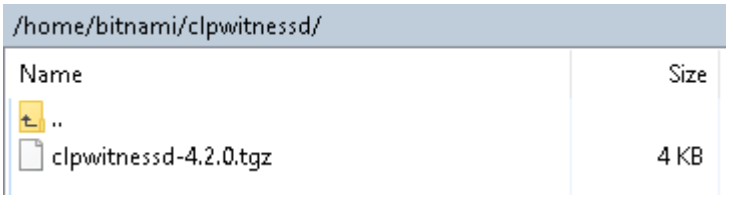
- Name the directly “clpwitnessd” and click ok



- Double click the clpwitnessd folder to change directory

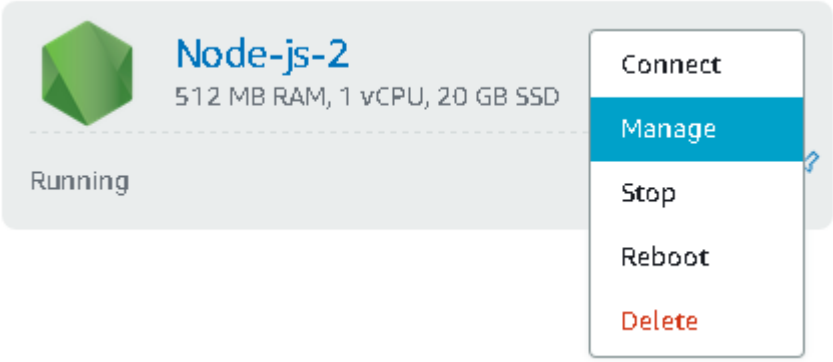


- Upload clpwitnessd-<version>.tgz to the “/home/bitnami /clpwitnessd” folder

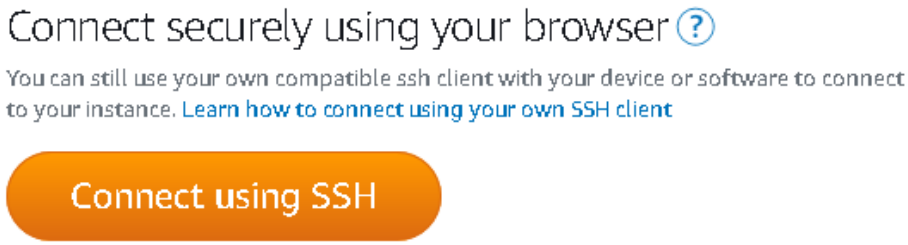


Step 5 - Install witness software

- From the AWS Lightsail home page, click on the toolbar radio on the right side of the instance and click manage



- Click Connect using SSH

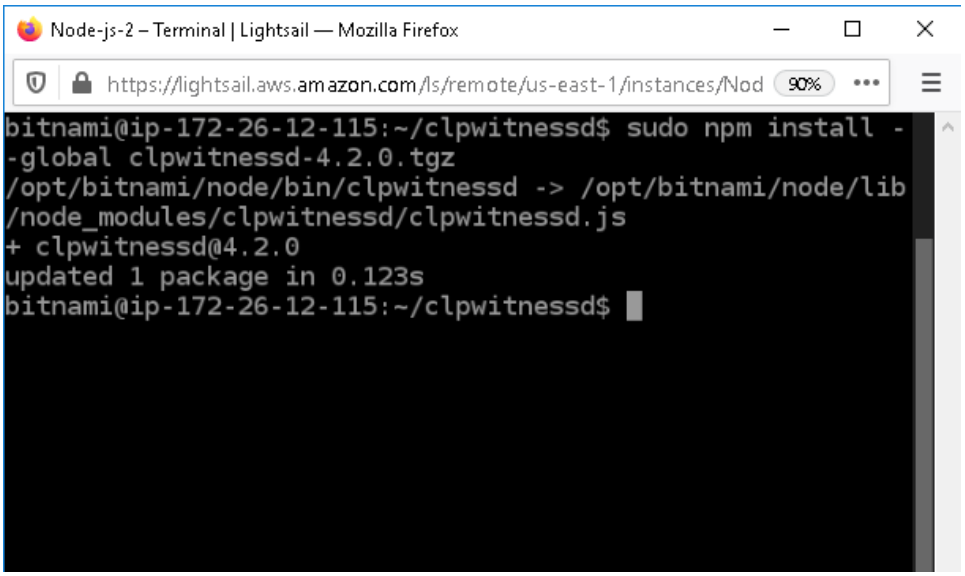


> Note: Alternatively, you can configure putty or any other ssh client to connect, using the private key created in previous steps.

- Install the witness software by executing the following command

```
$ cd ~/clpwitnessd
$ sudo install --global clpwitnessd-<version>.
tgz
```

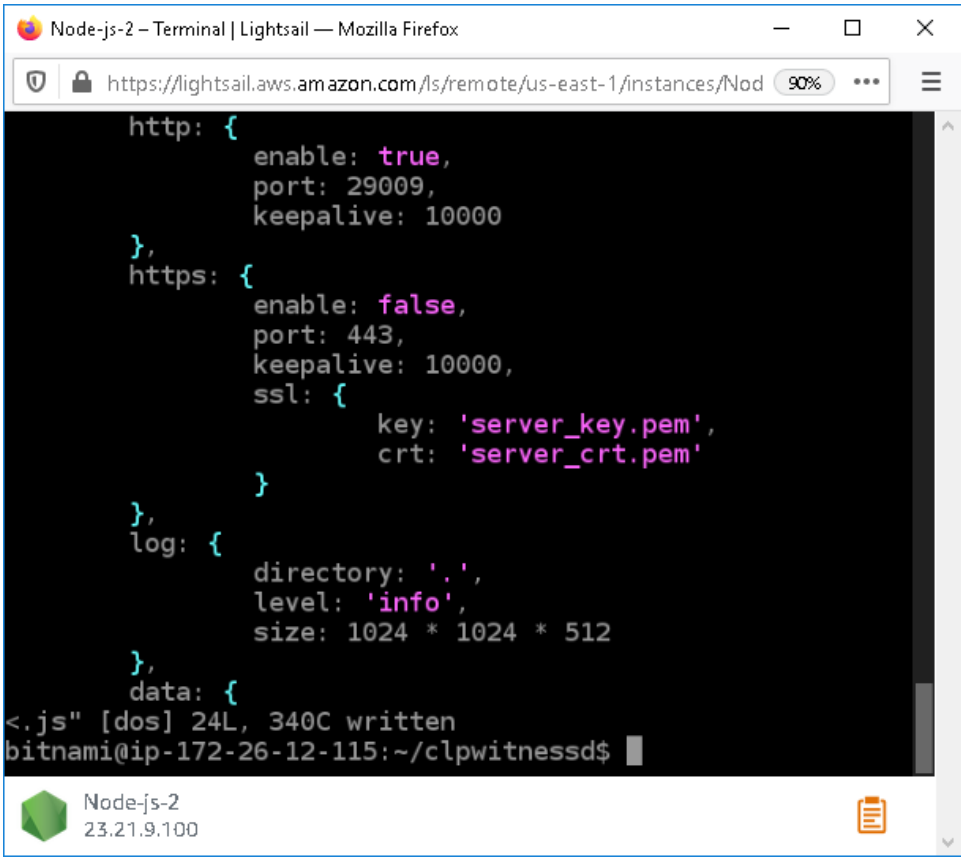
- If successful, the following should be displayed



- Edit the witness config file

```
$ sudo vi /opt/bitnami/node/lib/node_modules
/clpwitnessd/clpwitnessd.conf.js$ sudo vi /opt
/bitnami/node/lib/node_modules/clpwitnessd
/clpwitnessd.conf.js
```

- Under the http section of the file, change the port from 80 to 29009 and save



Step 6 - Configure witness software as a service

- Create and edit the clpwitnessd.service file

```
$ sudo vi /etc/systemd/system/clpwitnessd.
service
```

- Copy or paste the following text into the clpwitnessd. service file and save

```
[Unit]
Description=ECX AWS Witness
After=syslog.target network.target
[Service]
Type=simple
ExecStart=/opt/bitnami/node/bin/clpwitnessd
WorkingDirectory=/opt/bitnami/node/lib
/node_modules/clpwitnessd
KillMode=process
Restart=always
[Install]
WantedBy=multi-user.target
```

- Edit clpwitnessd script.

```
$ sudo vi /opt/bitnami/node/bin/clpwitnessd
```

- Edit the shebang in the script to reflect the proper location of the “node” executable.

Find the line that shows..

```
#!/usr/bin/env  node
```

and change to the following…

```
#!/usr/bin/env /opt/bitnami/node/bin/node
```

- Enable the clpwitnessd service

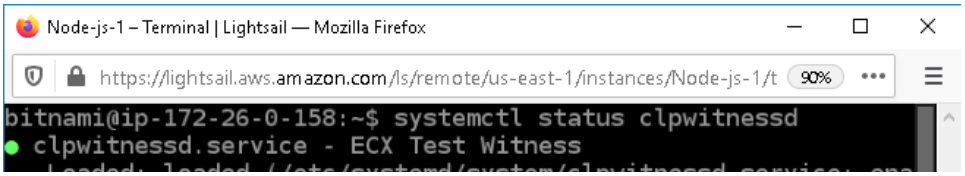
```
$ sudo systemctl enable clpwitnessd
```

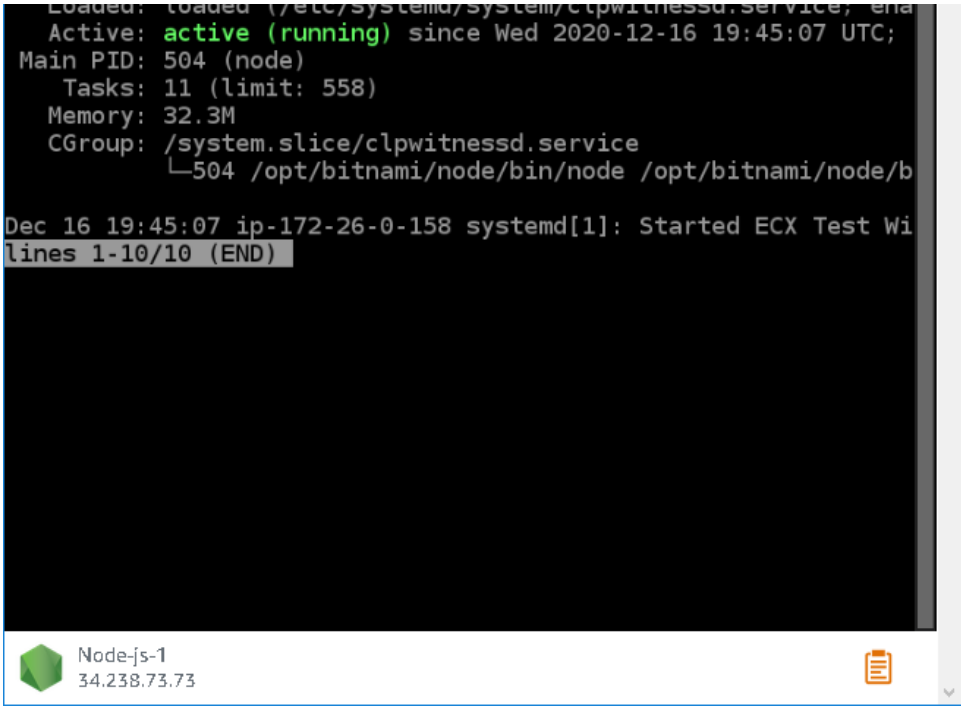
- Start the clpwitnessd service

```
$ sudo systemctl start clpwitnessd
```

- Verify the clpwitnessd service is running properly.

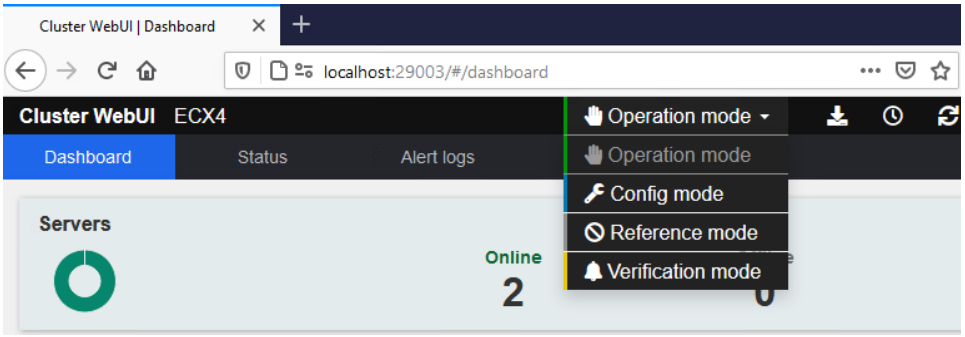
```
$ sudo systemctl status clpwitnessd
```



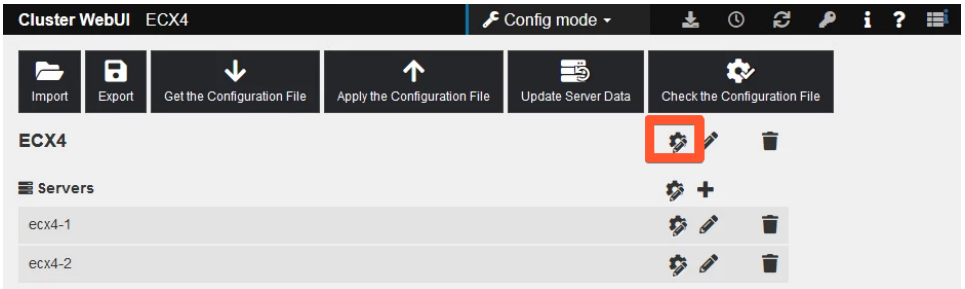


Step 7 - Add witness server to ExpressCluster

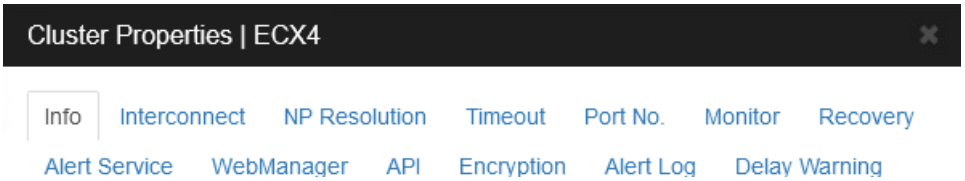
- Launch the ExpressCluster web manager
- Switch to config mode

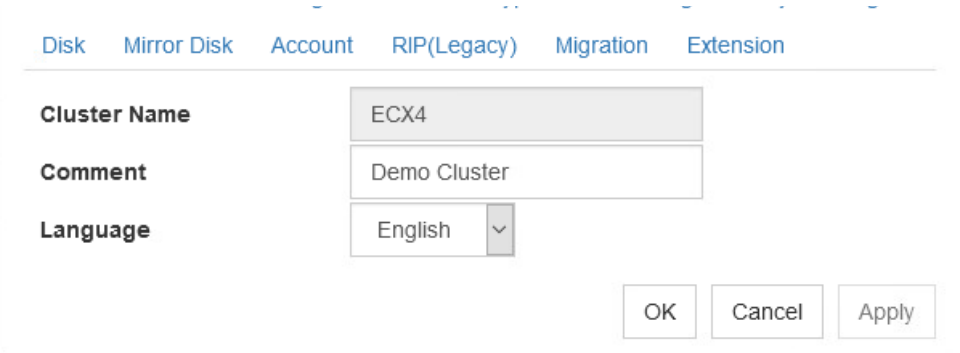


- Click the cluster properties button

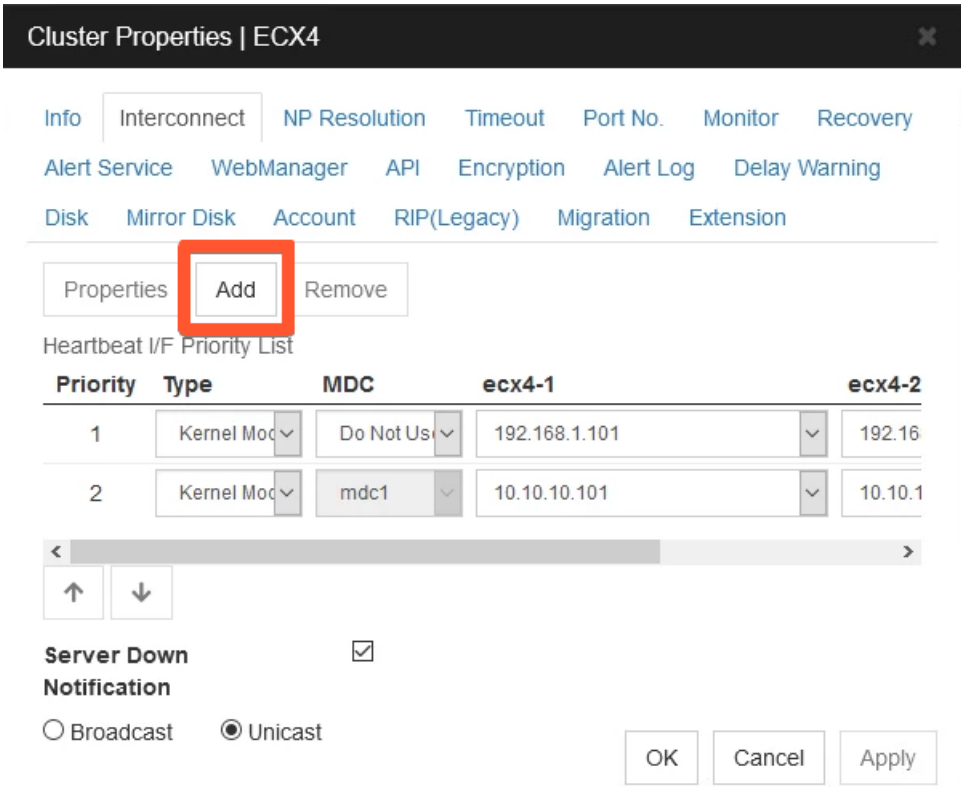


- Click the Interconnect tab

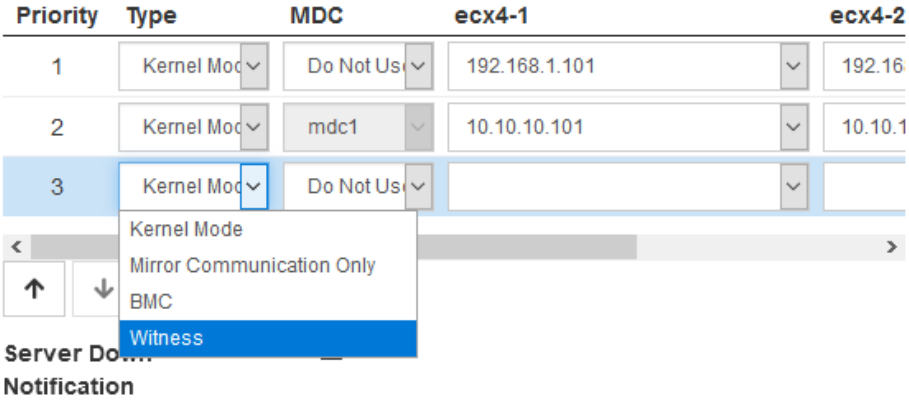




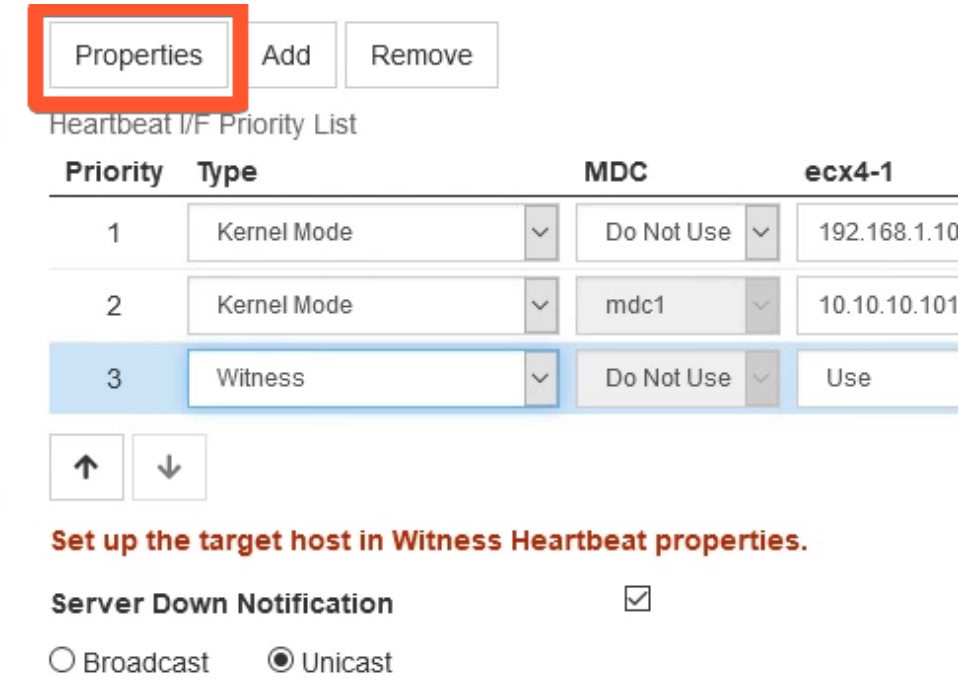
- Click the Add button



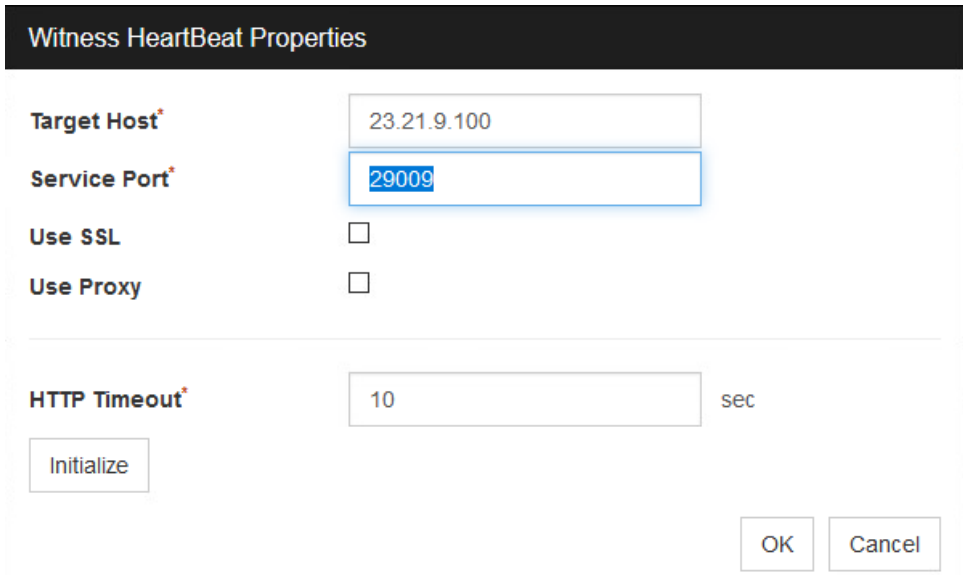
- Under the Type dropdown for the newly added I/F, select Witness



- Make sure the new I/F is selected and click the Properties button

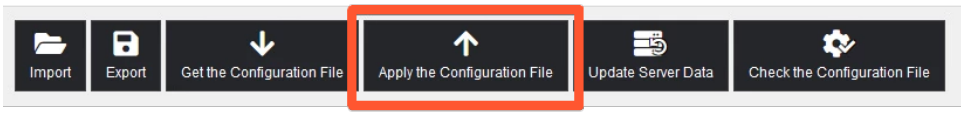


- Change the Target Host to the static IP associated with the AWS instance, set the Service Port to 29009 and click OK

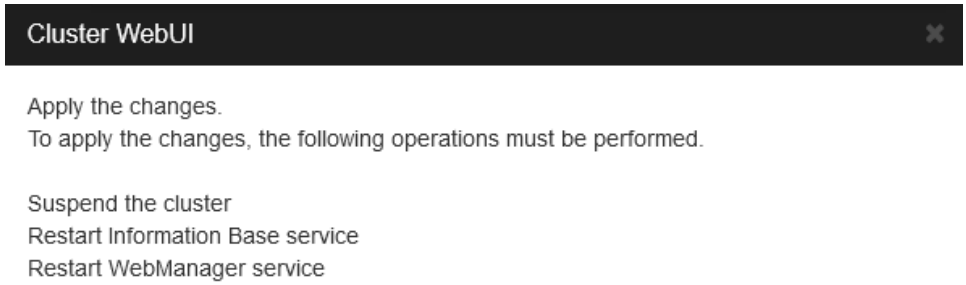


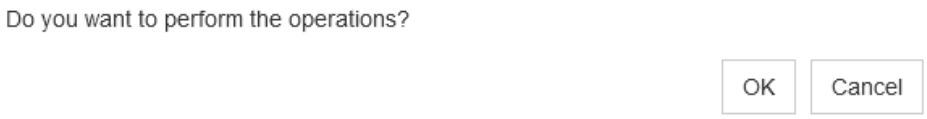
- Click OK again

- Click Apply the Configuration File

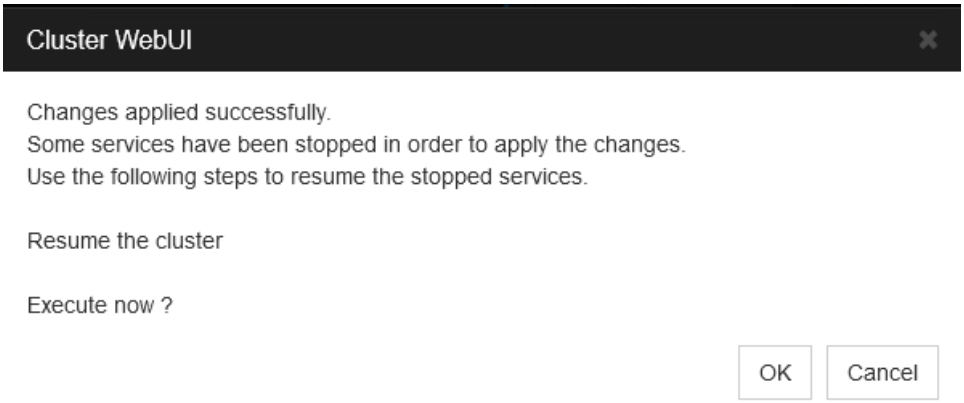


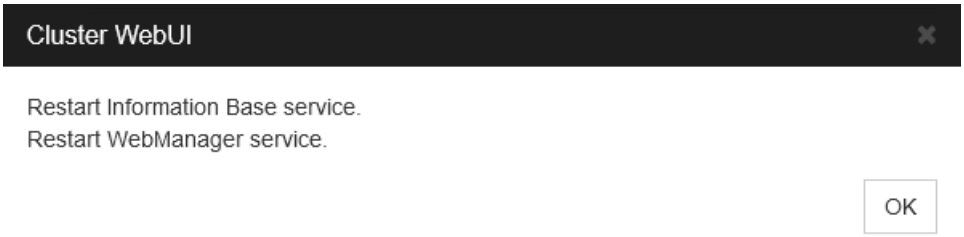
- Click OK



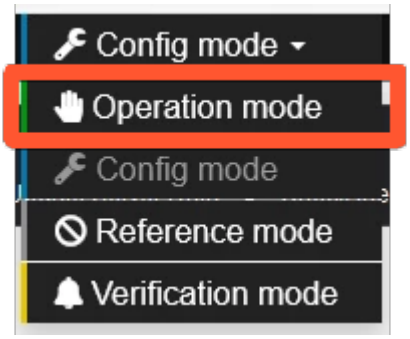


- If you see the following messages, click OK

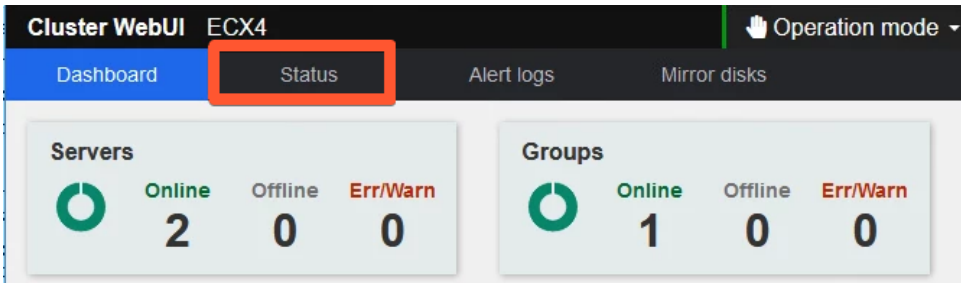




- Switch back to Operation Mode

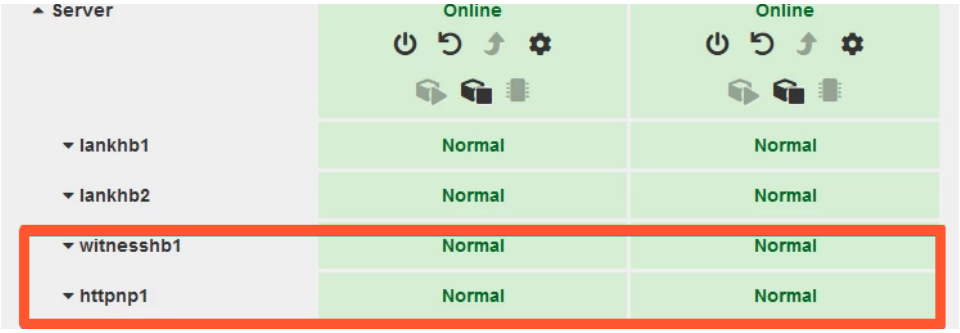


- Click on Status



- Click the Server down-arrow to expand view

- Verify witnesshb1 and httpnp1 are Normal status for both servers



NOTE: The HTTPnp resource is added automatically when the witness heartbeat is added to the cluster config. This can be removed later if desired without affecting the witness heartbeat.

Related articles