AWS Elemental Server

Configuration Guide

Version 2.16

AWS Elemental Server: Configuration Guide

Table of Contents

..... iv
About This Guide 1
Getting Ready 2
    Web Interface Access 2
Initial Configuration 3
    Enable SSL 3
    Verify the Licenses 4
    Set the Time Zone 4
    Configure Ethernet Devices 4
        Add Ethernet Devices 5
        Bond Ethernet Devices 5
    Configure DNS and NTP Servers 8
    Open Ports on the Firewall 8
    Add Mount Points 9
    Configure Database Backups 10
    Configure Notifications 10
        Email Notifications 11
        Web Callback Notification 15
        Simple Network Management Protocol (SNMP) Traps 17
        Simple Network Management Protocol (SNMP) Polling 17
    Enable User Authentication 19
    Add Users 20
Managing the Configuration 22
    Disable SSL 22
    Database Backups 22
        Restore a Backup 23
        Disable Automatic Database Backups 23
    Users 23
        View User Information 24
        Change and Delete Users 24
        Create New User Roles 24
        Manage Global Access Features 24
User Authentication Reference 25
    Supported Types of User Authentication 25
    Authentication User Types 25
Document History 27

This is version 2.16 of the AWS Elemental Server documentation. This is the latest version. For prior versions, see the *Previous Versions* section of AWS Elemental Conductor File and AWS Elemental Server Documentation.

About This Guide

This guide is intended for engineers who are performing the initial configuration on one or more AWS Elemental Server nodes that are each working in a stand-alone mode. The nodes aren't being controlled by AWS Elemental Conductor File.

Phase 2 of Installation

This guide provides detailed information on phase 2 of installation, including:

- Enable user authentication so that users must log in to use any product.
- Add users, if user authentication is enabled.
- Configure the time zone, DNS server, NTP servers, firewall, and alert notifications.
- Configure other Ethernet interfaces, as required.
- Configure routers and other input devices.

Prerequisite Knowledge

We assume that you know how to:

- Connect to the AWS Elemental Server web interface using your web browser.
- Log in to a remote terminal (Linux) session in order to work via the command line interface.

> **Note**
> To receive assistance with your AWS Elemental appliances and software products, see the forums and other helpful tools on the AWS Elemental User Community.

Getting Ready

Be aware of the following topics before starting phase 2 of the installation.

Web Interface Access

Most of the steps in the configuration procedure involve working in the web interface.

To access the web interface the first time

If you're accessing the web interface for the first time, or any time after if you haven't enabled user authentication, enter the IP address of the node in a browser. If you created a hostname through the install script, you can also use the hostname to access the node.

To access the web interface with user authentication

1. Enter the IP address or hostname of the node in a web browser.
2. At the login screen, enter your credentials for this node. If you haven't created additional users yet, use the REST API administrator credentials that you created when you enabled authentication.

   Important
   You cannot log in using the *elemental* user credentials!

Initial Configuration of the AWS Elemental Server Node

This section describes how to finish the setup of your AWS Elemental Server node. You might have completed some of this setup through the install script during the first phase of installation.

For information about changing settings once the node is already configured, see Managing the AWS Elemental Server Configuration (p. 22).

Topics

- Enable SSL (p. 3)
- Verify the Licenses for the Cluster (p. 4)
- Set the Time Zone (p. 4)
- Configure Ethernet Devices on AWS Elemental Server Nodes (p. 4)
- Configure DNS and NTP Servers (p. 8)
- Open Ports on the Firewall for AWS Elemental Server Nodes (p. 8)
- Add Mount Points to AWS Elemental ServerNodes (p. 9)
- Configure Database Backups for AWS Elemental Server (p. 10)
- Configure AWS Elemental Server Notifications (p. 10)
- Enable User Authentication (p. 19)
- Add Users (p. 20)

Enable SSL

The Secure Socket Layer (SSL) enables the secure version of HTTP (HTTPS) and encrypts communications between the client and server. Note the following about SSL:

- With SSL, all traffic over the communications layer must use a secure protocol. If SSL is disabled, all traffic must use the unsecured version. Traffic that uses the wrong protocol fails.
- When SSL is enabled, you must continue to use the `--https` flag with subsequent node reconfigurations through the command line interface. If you omit the flag, the installer disables SSL.

  Use `--https` with the following commands:
  - The run command, such as **sudo sh ./*product_installer_name_version*.run**
  - The configure command, such as **sudo ./configure**

To enable SSL

Follow these steps for all nodes that will have SSL enabled.

1. At your workstation, start a remote terminal session to the AWS Elemental Server node.
2. At the Linux prompt, log-in with the *elemental* user credentials.
3. Change to the directory where the configuration script is located, as shown here.

```
[elemental@hostname ~]$ cd /opt/elemental_se
```

4. Run the configuration script, as shown here.

```
[elemental@hostname elemental_se]$ sudo ./configure --https
```

   where `--https` enables SSL.

   Note
   If you run this command when SSL is already enabled, nothing changes in the configuration. SSL is still enabled.

5. At each configuration prompt, accept the suggestion. This way, you won't inadvertently change other aspects of the configuration.

Verify the Licenses for the Cluster

Make sure that you have the appropriate licenses installed.

To view installed licenses

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **Licenses**.
2. Verify that information for a standalone license (`eme.lic`) is displayed.
3. If you see a No license file detected message, follow the steps on the screen to upload a license. For additional assistance, see the AWS Elemental Server version 2.16 Installation Guide.

Set the Time Zone

Follow this procedure if you didn't set the time zone when you ran the install script (via the `-t` prompt), or if you want to change the time zone. You must perform these steps on each node in the cluster that needs the time zone updated.

To set the time zone (web interface)

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **General**.
2. In **Timezone**, choose your required time zone.
3. Choose **Update**.

The web interface shows all activity with a timestamp for the specified time zone.

This setting does not affect activity via SSH or via the REST API.

Configure Ethernet Devices on AWS Elemental Server Nodes

When you installed each AWS Elemental product in the cluster, you configured eth0. You can now set up eth1 and any additional Ethernet devices. Optionally, you can also bond two devices that you have set up.

Ethernet devices and the management interface

When you installed AWS Elemental Server, you configured eth0 as the management interface. Note that setting up a device as the management interface does *not* dedicate this device to management traffic. The device can still handle other traffic.

Topics

- Add Ethernet Devices (p. 5)
- Bond Ethernet Devices (p. 5)

> **Important**
> If you use the Linux CLI to configure network interfaces, DO NOT use the web interface to manage network settings. This will overwrite networking configurations that were made using the CLI.

Add Ethernet Devices

The eth0 device was automatically set up during installation. If you also set up eth1 at that time, no further configuration is required. If you didn't set up eth1 or want to set up more devices, use these instructions to do so.

To add Ethernet devices

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **Network**.
2. On the **Network** page, choose **Network Devices**.
3. On the **Network Devices** page, choose **Add Network Device**.
4. In the **Add a New Network Device** dialog, select **eth (ethN)**.
5. Complete the fields as follows:
   - **Device Name**: Select the eth device that you're setting up.
   - **Management**: Typically, leave this unchecked. This device won't be set up as a management interface. The node is usually installed with eth0 as the management interface and the node doesn't need more than one.
   - **Description**: Auto-populates when you choose a device name. You can modify the description as needed.
   - **Master Device**: Should display No devices with port bond settings available. This wording indicates that you haven't created a bond-type device, so bonding isn't available.
   - **Address Mode**: Select the type of IP addresses this device uses, either **dhcp**, **static**, or **none**. If you're bonding eth0 and eth1, use static IPs.
   - **IP Address**, **Netmask**, **Gateway**: Available when static IP addresses are used only. Complete with your networking information.
   - **Static Routes**: Select if you're using static routing.
   - **Network**, **Netmask**, **Gateway**: Available when static routes are used only. Complete with your networking information.
6. Choose **Save**. The new device appears in the Network Devices list.

Bond Ethernet Devices

You can bond Ethernet devices to suit your networking requirements. For example, you might set up two Ethernet devices as an active/redundant pair.

Bonding is a two-step process

- Step A: Create the Bond (p. 6)

- Step B: Assign the Devices (p. 8)

Important
We recommend that you set up both eth0 and eth1 with static IP addresses. Eth0, eth1 and bond0 should also all on the same subnet.

Prerequisites

Before you begin this process, make sure that you've done the following:

- Added to AWS Elemental Server the Ethernet devices (p. 5) that you're bonding.

Step A: Create the Bond

First, create the bond for the network devices. In the next step, you will add the devices to the bond.

To create the bond

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **Network**.
2. On the **Network** page, choose **Network Devices**.
3. On the **Network Devices** page, choose **Add Network Device**.
4. In the **Add a New Network Device** dialog, select **bond (bondN)**.
5. Complete the fields as follows:
   - **Bond ID**: Provide a number that is unique among your bonded interfaces.
   - **Management**: Select if the devices that you're bonding are management interfaces.
   - **Description**: Auto-populates when you choose a device name. You can modify the description as needed.
   - **Address Mode**: Select the type of IP addresses this device uses, either **dhcp**, **static**, or **none**. If you're bonding eth0 and eth1, use static IPs.
   - **IP Address**, **Netmask**, **Gateway**: Available when static IP addresses are used only. Complete with your networking information.
   - **Static Routes**: Select if you're using static routing.
   - **Network**, **Netmask**, **Gateway**: Available when static routes are used only. Complete with your networking information.
6. In **Mode**, select the bonding mode that you're using. The following table describes the modes that AWS Elemental Server supports:

Bonding mode	Description	
Round robin	Transmissions are received and sent sequentially on each bonded interface beginning with the first one available.	
Active backup	Transmissions are received and sent out via the first available bonded interface. The other interface is only used if the active interface fails.	
Balanced XOR	Using the exclusive-or (XOR) method, the interface matches up the incoming request's	

Bonding mode	Description	
	MAC address with the MAC address for one of the bonded interface NICs. Once this link is established, transmissions are sent out sequentially beginning with the first available interface.	
Broadcast	All transmissions are sent on all interfaces in the bond.	
IEEE 802.3ad dynamic link aggregation	Creates aggregation groups that share the same speed and duplex settings. Transmits and receives on all interfaces in the active aggregator. Requires a switch that is 802.3ad compliant.	
Adaptive transmit load balancing	Outgoing traffic is distributed according to current load on each interface in the bond. Incoming traffic is received by the currently active interface. If the receiving interface fails, another interface takes over the MAC address of the failed interface.	
Adaptive load balancing	Includes transmit and receive load balancing for IPV4 traffic. Receive load balancing is achieved through ARP negotiation.	

7. In **Link Mode**, select the linking mode that you're using for this bond and complete the relevant fields, as described here:

   - For media-independent interface (MII) mode, complete these fields:
     - **MII Monitoring Frequency**: Determines how often the link state of each bonded interface is inspected for link failure, in milliseconds. We recommend 100ms as a starting point.
     - **Use Carrier** (optional): When checked, MII uses MII or ETHTOOL ioctls instead of netif_carrier_ok. Relies on the device driver to maintain link state. Note that ETHTOOL ioctls is less efficient and uses deprecated kernel calling sequences.
     - **Down Delay** (optional): Specifies the time, in milliseconds, to wait before disabling an interface after a link failure is detected. This value should be a multiple of the MII monitoring frequency. Otherwise, it AWS Elemental Server rounds it to the nearest multiple of the monitoring frequency. The default is 0.
     - **LACP Rate** (optional): Used with IEEE 802.3ad dynamic link aggregation only. Determines the rate that control packets are sent to the interface. **Fast** is every one second, and **Slow** is every 30 seconds.
     - **Up Delay** (optional): Specifies the time, in milliseconds, to wait before enabling an interface after a link failure is detected. This value should be a multiple of the MII monitoring frequency. Otherwise, it AWS Elemental Server rounds it to the nearest multiple of the monitoring frequency. The default is 0.

- For address resolution protocol (ARP) mode, complete these fields:
  - **ARP Interval**: Determines how often the link state of each bonded interface is inspected, in milliseconds. Periodically checks devices for traffic and generates regular interval traffic via ARP probes for ARP IP target.
  - **ARP IP Target**: Specifies the IP address to use for ARP probes.
  - **Use Carrier** (optional): When checked, MII uses MII or ETHTOOL ioctls instead of netif_carrier_ok. Relies on the device driver to maintain link state. Note that ETHTOOL ioctls is less efficient and uses deprecated kernel calling sequences.
  - **LACP Rate** (optional): Used with IEEE 802.3ad dynamic link aggregation only. Determines the rate that control packets are sent to the interface. **Fast** is every one second, and **Slow** is every 30 seconds.

8. Choose **Save**. The new bond appears in the Network Devices list. Don't apply changes yet.

Step B: Assign the Devices

Next, add the Ethernet devices to the bond that you created in Step A: Create the Bond (p. 6).

To add devices to the bond

1. On the **Network Devices** page of the AWS Elemental Server web interface, locate the devices that you're adding to the bond.
2. For each device, choose **Edit Network Device** (pencil icon) and make the following changes:
   - Make sure that **Management** isn't selected. Whether the devices are management interfaces or not is defined in the bond and not in the individual devices.
   - In **Master Device**, select the bond that these devices are to be assigned to.
3. Choose **Save** and **Apply Changes**.

Configure DNS and NTP Servers

You can add Domain Name System (DNS) name servers and Network Time Protocol (NTP) servers for the node to use.

To configure servers

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **Network**.
2. On the **Network** page, choose **Hostname, DNS & NTP**.
3. As needed, add one server at a time to the **DNS Name Servers** and **NTP Servers** fields and choose **Save**.

Open Ports on the Firewall for AWS Elemental Server Nodes

You can enable or disable the firewall. We recommend that your nodes always be installed behind a customer firewall on a private network, regardless of if the individual firewall is enabled on each node. The node firewall is enabled by default.

When the node firewall is enabled, the installer configures the ports that must be open for incoming and outgoing traffic for each node. Use the following procedure to open more ports if you need them.

To open ports on the node firewall

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **Firewall**.

   You must turn on the node firewall before you can make any changes to the ports.
2. In the **Firewall Settings**, choose **Firewall On**.
3. (Optional) To enable a port, choose **Accept** for that port.
4. (Optional) To add a new port, complete the fields in the **Add Incoming Port** section.
5. When you're done, choose **Save**.

Add Mount Points to AWS Elemental ServerNodes

To make remote assets, such as scripts, image files, or video source files, available to your AWS Elemental Server nodes, create mount points as described in this section. When you mount a remote folder to a local folder on the node, all of the contents of the remote folder appear as if they are actually in the local mount folder. In this way, you can view the remote folder and verify that the backup files are created. You can also copy or delete a file from the remote folder by copying or deleting it from this mount folder.

The mount folder becomes a mount share. It's mounted to `/data/mnt/`*`folder`*.

To create a mount

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **Mount Points**.
2. On the **Mount Points** page, complete the mount point fields as described in the following table and choose **Save**:

Field	Description
Type	Choose the type of remote server: • **CIFS**: Choose this for a Windows CIF server or for a Windows, Linux, or Mac SMB server. • **NFS**: Choose this for a Linux server. • **DAVFS**: Choose this for a DavFS server.
Server Share	The address of the folder on the remote computer that you want to make available on this node.
Mount Folder	The folder on the node where the remote folder is mounted. As shown, this folder must be under `/data/mnt`. You can specify a sub-subfolder; if that folder does not already exist, AWS Elemental Server automatically creates it.
Username	If the remote server folder is protected with a username/password, enter the username here.
Password	If the remote server folder is protected with a username/password, enter the password here.

The newly mounted folder appears on the node after a few minutes.

Configure Database Backups for AWS Elemental Server

During a database backup, AWS Elemental Server copies the data that's related to your framework (channels, profiles, nodes, MPTS outputs, and redundancy groups) from the AWS Elemental Server node to another server. You can use this backup to restore the data to the node in case of a major hardware failure or if you have to re-install the software for any reason.

Backup files are named in this format: `elemental-db-backup_yyyy-mm- dd_hh-mm- ss.tar.bz2`

AWS Elemental Server is configured by default to create database backups and store them on a local disk. This section describes how to view the backup configuration and modify it for your needs.

For steps to restore a database backup, see Database Backups for AWS Elemental Server (p. 22)

To view and change the backup configuration

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **General**.
2. In the **Cluster Tasks** section, the following fields configure the database backups:
   - **Minutes between management database backups** indicates how often AWS Elemental Server creates backups.
   - **Management database backups to keep** indicates how many backups AWS Elemental Server keeps. When this number is reached, the oldest backup is removed so that the newest backup can be saved.
   - **Path to store management database backups** indicates where AWS Elemental Server stores backups.

     The folder to receive backups must be the local disk or on a remote server that is mounted to the node. For assistance, see Add Mount Points to AWS Elemental ServerNodes (p. 9).
3. Change any of these values as you need and choose **Save**.

Configure AWS Elemental Server Notifications

AWS Elemental Server provides status information through alerts and messages. You can configure notifications so you know when the node might need attention. The following table describes the differences between alerts and messages and how you can access each.

	Alerts	Messages
Access options	• Web interface • REST API calls • SNMP poll • SNMP trap • Email notification • Web callback notification	• Web interface • REST API calls • SNMP poll
Information conveyed	Alerts are feedback on a problem that must be fixed.	There are three types of messages: • **AuditMessage:** Informational messages that you do not

	Alerts	Messages
	The Job Error alert informs you that a job has moved to an Error state. This can be helpful when you are receiving automatic email notifications, letting you know to check for related messages on the web interface.	need to react to. Often, these messages are feedback to actions you performed. • **WarningMessage:** Messages that advise you that there is a risk that a future activity will fail unless you take action to prevent it. • **ErrorMessage:** Messages that indicate that a planned activity has failed or an unexpected system error has occurred.
Active or inactive status	Alerts are active until the underlying problem is resolved. When the cause of the alert is no longer present, the system clears the alert and it becomes inactive.	Messages are neither active nor inactive. They are defined as *recent* when they are less than 24 hours old.
Visibility (web interface only)	You can toggle the visibility of active alerts on the web interface. Suppressing an alert this way is similar to marking an email as read. Alerts are available through the other access options, regardless of their visibility in the web interface.	You can toggle the visibility of recent error messages on the web interface. This is similar to marking an email as read. Visibility does not affect the return on SNMP and REST requests.

The following sections describe how to setup notifications. For information about viewing alerts and messages on the web interface or through the API, see the AWS Elemental Server API and User Guide.

Topics

- Email Notifications (p. 11)
- Web Callback Notification (p. 15)
- Simple Network Management Protocol (SNMP) Traps (p. 17)
- Simple Network Management Protocol (SNMP) Polling (p. 17)

Email Notifications

You can configure AWS Elemental Server to email you notifications when alerts occur.

AWS Elemental Server uses open relay to send email notifications. Before subscribing to notifications, make sure that your network allows receipt of open relay email. If your network doesn't allow open relay messages, you must also configure a Sendmail relay server with another mail server.

> **Important**
> If you subscribe to email notifications in a network that doesn't allow open relay messages and you do not relay the messages, the generated messages will collect on the AWS Elemental Server system hard drive, eventually filling the partition and causing disk alert errors.

To set up email notifications

1. On the AWS Elemental Server web interface, subscribe to all or some alerts using the steps described here:

   Subscribe to all alerts

   1. On the AWS Elemental Server web interface, go to the **Settings** page and ensure that you're on the **General** tab.
   2. Complete the **Global Alert Notification** fields as described in the following table and choose **Update**.

Field	Instructions
Notification: Email	Enter the email address of the alert recipient. Required if you don't provide a URL in the **Web Callback URL** field.
Notification: Web Callback URL	If you want to receive web server notifications too, enter the URL of the appropriate `.php` file on your web server. For instructions on how to configure your web server for notifications, see Web Callback Notification (p. 15).
Notify	Select when you want to be notified, either when the alert is raised or when it's cleared. You can choose both options.
Notes	Add optional notes as needed.

   Subscribe to individual alerts

   1. On the AWS Elemental Server web interface, hover over **Stats** page and choose **Alerts**.
   2. On the **Alerts** page, choose **Configure Alerts**.
   3. In the list of alerts, locate the alert that you want to be notified on and choose it to expand it.
   4. Complete the fields as described in the following table and choose **Update**.

Field	Instructions
Notification: Email	Enter the email address of the alert recipient. Required if you don't provide a URL in the **Web Callback URL** field.
Notification: Web Callback URL	If you want to receive web server notifications too, enter the URL of the appropriate `.php` file on your web server. For instructions on how to configure your web server for notifications, see Web Callback Notification (p. 15).

Field	Instructions
Notify	Select when you want to be notified, either when the alert is raised or when it's cleared. You can choose both options.
Notes	Add optional notes as needed.

5. Locate, expand, and complete the fields for each alert that you want to be notified on.

2. If your network doesn't allow open relay messages, configure the sendmail server to relay the messages. For steps, see Configure Sendmail Relay Server (p. 13).

Configure Sendmail Relay Server

Use this procedure to set up a Sendmail relay server if your network doesn't accept open relay messages.

Step A: Gather the mail server information

To configure AWS Elemental Server to relay the notification emails through a mail server, you need the following information:

- The hostname of the mail server
- If your network doesn't have DNS configured, the IP address of the mail server

Step B: Install the Sendmail configuration tool

To install the configuration tool

1. Install the `sendmail.cf` configuration tool by typing the following at the command line.

```
sudo yum install sendmail-cf
```

2. When you receive a caution message asking you to confirm that you want to run the command, enter **`yes`**.
3. When you receive the following prompt, enter **`y`**.

```
Is this ok [y/N]:
```

4. When you receive the following message, move on to the next step.

```
Complete!
```

Step C: Edit the `sendmail.mc` file

To edit the file

1. With a text editor, open the `sendmail.mc` file. If you use Nano, which comes installed on all AWS Elemental systems, type the following at the command line to open the file in Nano.

```
sudo nano /etc/mail/sendmail.mc
```

2. Locate the line that defines `SMART_HOST`. It's generally just past halfway down the page and should look like this.

```
dnl define(`SMART_HOST', `smtp.your.provider')dnl
```

3. Uncomment this line by deleting the `dnl` at the beginning and end of the line.
4. Change the following text to the hostname of the mail server that is performing the relay.

```
smtp.your.provider
```

5. Save and exit the file. For Nano, press **Ctrl**+**O** to save and **Ctrl**+**X** to exit.

Step D: Check the `hosts` file

If your network isn't configured with DNS, add a static entry to the `hosts` file on AWS Elemental Server.

To add an entry to the `hosts` file

1. With a text editor, open the `/etc/hosts` file. If you use nano, type the following at the command line.

```
sudo nano /etc/mail/hosts
```

2. Add a line to the end of the file that has the IP address of the relay server, a space, and the hostname of the relay server. The following shows an example.

```
10.24.34.2 ExampleMailHostname
```

3. Save and exit the file. For nano, press **Ctrl**+**O** to save and **Ctrl**+**X** to exit.

Step E: Apply the changes

1. To apply changes, enter the following command.

```
sudo make -C /etc/mail
```

The system responds as follows.

```
make: Entering directory `/etc/mail'
make: Leaving directory `/etc/mail'
```

2. Restart Sendmail by typing the following.

```
sudo service sendmail restart
```

Step F: Test the new configuration

Test the relay by having the system email you an alert notification.

To test the configuration

1. If you haven't already, subscribe to global alert notifications as described in Email Notifications (p. 11). Provide an email address that you have easy access to.
2. Generate a fake alert. A simple way to do so is to create and start a channel with a simple UDP input and output with a fake input address, such as **`udp://1.1.1.1:1111`**.

3. Check your email for the notifications message.
4. If necessary, return the global alert notifications to your desired settings.

Web Callback Notification

You can configure AWS Elemental Server to send you web callback notifications when alerts occur.

To receive web callback notifications, you must have a web server that supports a service-side script such as nodeJS or PHP. Use the following steps to configure this server with PHP install to receive alert notifications from AWS Elemental Server.

To set up web callback notifications

1. Use a text editor such as Notepad on a Windows system or Nano on Linux to create a `.php` file containing the following text.

```
<?php
    function get_raw_post(){
        $data = @file_get_contents('php://input');
        if ($data){
            return $data;
        }
            return "nothing passed";
        }

    $file = "../webcallback/notify";
    $fh = fopen($file, "a");
    $data = get_raw_post();
    fwrite($fh, $data);
    fclose($fh);
?>
```

2. Save the file in a directory on your web server.
3. Subscribe to all or some alerts using the steps described here:

   Subscribe to all alerts

   1. On the AWS Elemental Server web interface, go to the **Settings** page and ensure that you're on the **General** tab.
   2. Complete the **Global Alert Notification** fields as described in the following table and choose **Update**.

Field	Instructions
Notification: Email	If you want to receive email notifications too, enter the email address of the alert recipient. If your network doesn't allow open relay messages, see Configure Sendmail Relay Server (p. 13) to configure a sendmail server to relay messages.
Notification: Web Callback URL	Enter the URL of the appropriate `.php` file on your web server. Required if you don't provide an address in the **Email** field.

Field	Instructions
Notify	Select when you want to be notified, either when the alert is raised, or when it's cleared. You can choose both options.
Notes	Add optional notes as needed.

Subscribe to individual alerts

1. On the AWS Elemental Server web interface, hover over **Stats** page and choose **Alerts**.
2. On the **Alerts** page, choose **Configure Alerts**.
3. In the list of alerts, locate the alert that you want to be notified on and choose it to expand it.
4. Complete the fields as described in the following table and choose **Update**.

Field	Instructions
Notification: Email	If you want to receive email notifications too, enter the email address of the alert recipient. If your network doesn't allow open relay messages, see Configure Sendmail Relay Server (p. 13) to configure a sendmail server to relay messages.
Notification: Web Callback URL	Enter the URL of the appropriate `.php` file on your web server. Required if you don't provide an address in the **Email** field.
Notify	Select when you want to be notified, either when the alert is raised or when it's cleared. You can choose both options.
Notes	Add optional notes as needed.

5. Locate, expand, and complete the fields for each alert that you want to be notified on.

4. Test your setup by typing the following at the command line of the AWS Elemental Server node:

```
curl -X POST -d "param1=value1&param2=value2" http://yourdomain.com/webcallback/
notification.php
```

5. Open your `notify.php` to check that it was updated. The text of your file should contain something like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<job href="/jobs/3401">
  <node>earhart</node>
  <user_data></user_data>
  <submitted>2014-11-14 01:27:05 -0800</submitted>
  <priority>50</priority>
  <status>preprocessing</status>
  <pct_complete>0</pct_complete>
  <average_fps>0.0</average_fps>
  <elapsed>0</elapsed>
  <start_time>2014-11-14 01:27:06 -0800</start_time>
  <elapsed_time_in_words>00:00:00</elapsed_time_in_words>
```

```
</job>
param1=value&param2=value2
```

6. Enter your web callback URL into a web browser to see the HTTP post.

Simple Network Management Protocol (SNMP) Traps

You can configure AWS Elemental Server to generate Simple Network Management Protocol (SNMPv2) traps for activity on the node. For information about the management information bases (MIBs) in AWS Elemental Server, go to the **Settings** page in the AWS Elemental Server web interface and choose **SNMP Interface**.

AWS Elemental Server generates traps for the events described in the following table.

Notification	Event	Contents
ELEMENTAL-MIB::alert	Any alert that worker nodes in the cluster generate.	• ELEMENTAL-MIB::alertSet: `1` if the alert is being set, `0` if the alert is being cleared. • ELEMENTAL-MIB::alertMessage: describes the alert that was set or cleared.

To set up SNMP traps

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **SNMP**.
2. On the **SNMP** page, complete the fields, using the instructions in the following table as a guide. Choose **Save**:

Field	Instructions
Allow external SNMP access	Choose **Yes** to open the SNMP port on the firewall. The port must be open if you will send an **snmpwalk** command.
Generate SNMP Traps for Alerts	Choose **Yes** to generate traps.
SNMP Management Host	Enter the IP address of the trap destination.
SNMP Management Trap Port	Enter **`162`**.
SNMP Management Community	Enter **`Public`**.

Simple Network Management Protocol (SNMP) Polling

Rather than passively receiving SNMP traps from AWS Elemental Server, you can actively poll the SNMP interface.

You can interact with AWS Elemental Server using a variety of network management systems. AWS Elemental products ship with the Net-SNMP (http://www.net-snmp.org/) command line tools to access the SNMP interface while logged into the system directly or over SSH. Examples in this document are given using net-snmp commands.

To set up SNMP polling

1. Either disable the node firewall, or enable external access to SNMP interface.
   - For help disabling the firewall, see Open Ports on the Firewall for AWS Elemental Server Nodes (p. 8).
   - External access to the SNMP interface is enabled by default. To check the setting, access the **Settings** page on the AWS Elemental Server web interface and choose **SNMP**.
2. Query either individual variables, or the entire SNMP interface.

   To query individual variables

   Use the Net-SNMP tools to query variables as follows.

   ```
   snmpget -c elemental_snmp -v2c -m <MIB>
           localhost MIBvariable
   ```

   Example

   ```
   snmpget -c elemental_snmp -v2c -m ELEMENTAL-MIB
             localhost serviceStatus
   ```

   For a list of MIBs and their variables, see Management Information Bases (MIBs) in AWS Elemental Server (p. 18).

   To query the entire SNMP interface

   Use the Net-SNMP tools to do an snmpwalk to gather information about all of the running channels.

   ```
   snmpwalk -c elemental_snmp -v2c -m ELEMENTAL-MIB:ELEMENTAL-LIVE-MIB localhost
       elemental
   ```

Management Information Bases (MIBs) in AWS Elemental Server

AWS Elemental provides the following management information bases (MIBs) for use with AWS Elemental Server:

ELEMENTAL-MIB

This is the base MIB for all AWS Elemental products.

Variable	Values
`serviceStatus`	• 0 if the AWS Elemental Server isn't running. • 1 if it is running.
`firewallSettings`	• 0 if the node firewall is off. • 1 if it is on.
`networkSettings`	Always 1.

Variable	Values
	Required for some network management systems.
`mountPoints`	Number of user-mounted filesystems in `/mnt`.
`version`	The version of the AWS Elemental Server node.
`httpdStatus`	• 0 if the `httpd` service isn't running. • 1 if it is running.
`databaseBackup`	• 0 if writes (starting backups) is allowed. • 1 if they aren't allowed.

ELEMENTAL-SERVER-MIB

This MIB describes objects that are specific to AWS Elemental Server.

Variable	Values
`jobId`	The numerical ID of the job. This is the index to the jobTable.
`jobPending`	• 0 if the job isn't a pending state. • 1 if it is a pending state.
`jobRunning`	• 0 if the job isn't running. • 1 if it is running.
`jobError`	• 0 if the job isn't in an error state. • 1 if it is in an error state.
`jobComplete`	• 0 if the job isn't running complete. • 1 if it is in a complete state.
`nodeId`	The numerical ID of the node that the job is running on.

Both the ELEMENTAL-MIB and ELEMENTAL-LIVE-MIB come installed on AWS Elemental Server. They are located in `/opt/elemental_se/web/public/mib/`.

For more information, access the AWS Elemental Server web interface, go to the **Support** page and choose **SNMP Interface**.

Enable User Authentication

You can require users to provide valid credentials when they access AWS Elemental Server from both the web interface and REST API.

- For the web interface, users must complete the fields on the login screen.
- For the REST API, users must include these additional HTTP headers in commands that they send:
  - `X-Auth-User`

- `X-Auth-Expires`
- `X-Auth-Key`

For more information about using the API with authentication enabled, see the AWS Elemental Server REST API documentation.

To enable user authentication

1. At your workstation, start a remote terminal session to the AWS Elemental Server node.
2. At the Linux prompt, log in with the *elemental* user credentials.
3. Change to the directory where the configuration script is located, as shown here.

```
[elemental@hostname ~]$ cd /opt/elemental_se
```

4. Run the configuration script, as shown here.

```
[elemental@hostname elemental_se]$ sudo ./configure --config-auth
```

Important
If you have SSL enabled, you must also include the `--https` flag in the command. Otherwise, the script will disable SSL.

5. For the prompt `Do you wish to enable authentication?`, type **`Y`**.
6. If you didn't use the `--https` flag in the configure command, the following prompt appears.

```
If you wish to enable authentication, please re-run with the '--https' option.
If SSL isn't enabled, any usernames/passwords entered here including LDAP passwords
 would be transmitted in plain text without encryption. This poses a significant
 security risk.
Accept the risk and continue without SSL?
```

If you intended to enable authentication without SSL enabled, enter **`Y`** to proceed. Otherwise, enter **`N`** to re-enter the configuration script with `--https`.

7. For the prompt `Do you wish to enable PAM?`, type **`N`**. If you're using PAM authentication, type **`Y`**.

   For information about the different authentication options, see User Authentication Reference (p. 25)
8. At the prompts, create an admin API user name, email address, and password.

   Note that the only time you log in with this information is upon initial access to each node's web interface after authentication is enabled. For more information about the administrator API user, see Authentication User Types (p. 25)
9. For the prompt `Httpd must be restarted, which may interrupt REST commands. Restart now?`, type **`Y`**.
10. Create users through the node's web interface. For instructions, see Add Users (p. 20).

Add Users

When you enable local authentication on the node, users must enter valid credentials to access the node. This section describes how to create users. For information about user authentication, see User Authentication Reference (p. 25).

Note
If you enabled PAM authentication, your users are maintained in the LDAP server. You can manage the roles through the node, as described in Create New User Roles (p. 24), but you don't add the users to the node.

To add users

1. Log in to the AWS Elemental Server web interface using the REST API administrator credentials that you created when you enabled authentication.
2. Hover over **Settings** and choose **Users**.
3. On the **Users** screen, choose **New User**.
4. Complete all fields and choose **Create**. Some notes:

   - **Expires**: If selected, the user name automatically expires after the specified period of time.
   - **Force Password Reset**: If checked, the users must reset their passwords the first time they log in.
   - **Role**: Select a role. The available options are Admin, Manager, User, Viewer. For information about the actions allowed with each role, see the following section *User roles*.
5. If your organization uses the REST API, make sure to tell each user to choose **Settings** > **User Profile** to make note of their personal API key. Users have a different key for each node that they can access.

   This API key is randomly generated when the user is created. You can't manually set the API key.

User roles

Node access is defined by the role assigned to the user. This section describes the actions that each user role can perform.

- **Viewer**
  - Read-only access to AWS Elemental Server
- **Operator**
  - Same access as Viewer
  - Control the state of a job (cancel, archive, etc)
- **Manager**
  - Same access as Viewer
  - Same access as Operator
  - Create and edit jobs
  - Create and edit presets
  - Create and edit profiles
  - Create and edit watch folders
- **Administrator**
  - Access to the entire AWS Elemental Server system, including all of the access provided by the other roles

Managing the AWS Elemental Server Configuration

This section describes how to manage settings after you've completed the initial configuration of the node.

Topics

- Disable SSL (p. 22)
- Database Backups for AWS Elemental Server (p. 22)
- Users in AWS Elemental Server (p. 23)

Disable SSL

This section describes how to disable HTTPs (SSL) access to the node. For assistance enabling, see Enable SSL (p. 3).

To disable SSL, run the **Configure** command without the `--https` flag.

1. At your workstation, start a remote terminal session to the AWS Elemental Server node.
2. At the Linux prompt, log-in with the *elemental* user credentials.
3. Change to the directory where the configuration script is located, as shown here.

```
[elemental@hostname ~]$ cd /opt/elemental_se
```

4. Run the configuration script, as shown here.

```
[elemental@hostname elemental_se]$ sudo ./configure
```

   Note
   If you run this command when SSL is already disabled, nothing changes in the configuration. SSL is still disabled.

5. At each configuration prompt, accept the suggestion. This way, you won't inadvertently change other aspects of the configuration.

Database Backups for AWS Elemental Server

This section describes how to restore a database backup, and how to disable backups entirely. For assistance changing backup settings, such as minutes between backups, see Configure Database Backups for AWS Elemental Server (p. 10).

Topics

- Restore a Backup (p. 23)
- Disable Automatic Database Backups (p. 23)

Restore a Backup

Follow this procedure if you ever need to restore a backed-up version of the database.

To restore the database

1. At your workstation, start a remote terminal session to the AWS Elemental Server hardware unit. Log in with the elemental user credentials.
2. Type the following command to identify the version of AWS Elemental Server that is currently installed.

   ```
   [elemental@hostname ~]$ cat /opt/elemental_se/versions.txt
   ```

   Several lines of information appear, including the version number. For example: `AWS Elemental Server (2.16.1.12345)`.
3. Run the install script with the restore option.

   ```
   [elemental@hostname ~]$ sudo sh product

   --restore-db-backup path backup-file --https
   ```

   where:

   1. `product` is the product installer, including the version number that you obtained in the previous step: `elemental_production_server_2.16.1.12345.run`.
   2. `path` is the path to the backup file. This path could simply be the remote folder where backups were originally stored.
   3. `backup-file` is the file that you want to restore. The file is unzipped and copied to the appropriate folder. Do not unzip the file manually before restoring it!
   4. `--https` keeps SSL enabled. If you omit this flag, SSL is disabled when you run the install script. If you don't have or don't want SSL, omit this flag.

Disable Automatic Database Backups

Follow these steps to disable automatic backups.

1. On the AWS Elemental Server web interface, go to the **Settings** page and choose **General**.
2. In the **Cluster Tasks** section, change the value in **Minutes between management database backups** to **0**.
3. Choose **Save**.

Users in AWS Elemental Server

This section describes how to manage users that you've already added to the AWS Elemental Server node. For assistance adding users, see Add Users (p. 20).

Topics

- View User Information (p. 24)
- Change and Delete Users (p. 24)
- Create New User Roles (p. 24)
- Manage Global Access Features (p. 24)

View User Information

Each user can log in to the web interface and view their own profile. Go to **Settings** > **User Profile**. The following information is displayed:

- The features and controls of AWS Elemental Server that the user is allowed to use.
- The user's API key.

Change and Delete Users

To change or delete a user

1. Log in to the AWS Elemental Server web interface using administrator credentials.
2. Hover over **Settings** and choose **Users**.
3. On the **Users** screen, perform the following actions as needed:
   - To change the existing information for a user, choose **Edit** (pencil icon).
   - To reset a forgotten password, edit the user and enter a new password.
   - To force a user to reset their password the next time they log in, edit the user, and select **Force Password Reset**.
   - To reactivate a deactivated user, edit the user by extending the length of time that user password is in effect. In **Password Expires**, change **Expired** to another option.
   - To reset the API key for a user, choose **Reset API Key** (key icon). A new key is created. The user can view this key in the User Profile screen (**Settings** > **User Profile**).
   - To deactivate a user, choose **Deactivate** (banned icon).
   - To delete a user, choose **Delete** (X icon).

Create New User Roles

The policies determine what actions a user can perform on the node. AWS Elemental Server comes with administrator, manager, operator, and viewer default policies. You can't edit these default policies, but you can create new ones if the defaults don't meet your requirements.

To create new user roles

1. Log in to the AWS Elemental Server web interface using administrator credentials.
2. Hover over **Settings** and choose **Roles**.
3. On the **Roles** screen, assign a name to the new user role, select the actions to include, and choose **Create**. The new role appears in the list.

Manage Global Access Features

You can set some access features that apply globally to all users on the node.

To manage access

1. Log in to the AWS Elemental Server web interface using administrator credentials.
2. Go to the **Settings** page and choose **Authentication**.
3. Review the current values for the fields. Make any changes and choose **Save**.

User Authentication Reference

Enabling user authentication provides you more control over your AWS Elemental systems. Authentication helps secure your nodes while also allowing you to do the following:

- Track node activity on a per-user basis.
- Limit accidental access to a node by allowing distinct login credentials for each node. This way, an operator with access to multiple nodes must enter the credentials for a specific node prior to sending any commands.

Whether or not you enable authentication, we recommend that all of your nodes are installed behind a customer firewall or on a private network.

The following sections provide more information about user authentication.

Topics

- Supported Types of User Authentication (p. 25)
- Authentication User Types (p. 25)

Supported Types of User Authentication

AWS Elemental Server supports the following types of user authentication:

Local authentication

An administrator creates and manages user credentials from the AWS Elemental Server node.

Users logging in to nodes with local authentication enabled must enter valid credentials for access. They must also supply credentials when using the REST API.

The credentials that users enter are validated against credentials that are housed locally on the node that they're accessing.

Privileged Access Management (PAM) authentication

An administrator creates and manages user credentials from a Lightweight Directory Access Protocol (LDAP) server that's external from the AWS Elemental systems.

Users logging in to nodes with PAM authentication enabled must enter valid credentials for access. They must also supply credentials when using the REST API.

The credentials that users enter are validated against credentials that are housed on an external LDAP server.

Authentication User Types

This table describes the types of users available with authentication.

User type	How created	Log-in username	Log-in password	Use
Default, remote terminal user	Built-in	**`Customer-created at install.`**	Default, or as changed by an administrator.	Users manually enter this

User type	How created	Log-in username	Log-in password	Use
				information at these times: • When logging in to a remote terminal session for the node. • When PAM is enabled and it's the first time that any users access the node after authentication is enabled.
Admin REST API user	An administrator enables local authentication on the node when they create the administrator user in the command line.	Customer-created. The username must not be the name of a real person.	Customer-created.	The administrator API user is used at these times: • The person configuring authentication uses the admin API user information the first time that they access a node's web interface after local authentication is enabled. Typically, this is the only time that a user manually uses this user information.
People and third-party clients	An administrator user creates these users either through the node's web interface (for local authentication) or through an LDAP server (for PAM authentication).	Customer-created.	Customer-created.	Users manually enter their log-in credentials when accessing the node through the web interface or REST API. With local authentication. If a person has access to multiple nodes, you must create a user for them in each node.

Document History for Configuration Guide

The following table describes the documentation for this release of AWS Elemental Server.

- **API version:** 2.16
- **Release notes:** AWS Elemental Server Release Notes

The following table describes the documentation for this release of AWS Elemental Server. For notification about updates to this documentation, you can subscribe to an RSS feed.

update-history-change	update-history-description	update-history-date
Version 2.16 release (p. 1)	Changes to support the 2.16 software release.	June 16, 2020