Configuration Guide

AWS Elemental Delta

Version 2.3

AWS Elemental Delta: Configuration Guide

Table of Contents

This is version 2.3 of the AWS Elemental Delta documentation. This is the latest version. For prior versions, see the *Previous Versions* section of AWS Elemental Delta Documentation.

About This Guide

This guide is intended for engineers who are performing the initial configuration on an AWS Elemental Delta cluster.

The full suite of configuration topics for AWS Elemental Delta is described in the following table.

Deployment	Description	Information
Single Delta node	One Delta node without a secondary Delta node. There is no redundancy for the single Delta node.	Configuring a Stand-alone Node – Quick Guide
Simple Delta cluster	One leader Delta node and one secondary Delta node. The secondary node provides redundancy for the cluster.	Configuring a Leader-Secondary Node Cluster
Delta Cluster with egress nodes	One leader Delta node, one secondary Delta node and one or more egress Delta nodes. The secondary node provides redundancy for the cluster. The egress nodes handle requests for output but do not handle input.	Configuring a Leader-Secondary-Egress Node Cluster

Phase 2 of Installation

This guide provides detailed information on phase 2 for setting up the AWS Elemental Delta cluster:

- Configure other Ethernet interfaces as required.
- Configure DNS server, NTP servers, and firewall.

- Add mount points to access remote servers.
- Create AWS credentials, if applicable.
- Configure backup of the database.
- Configure SNMP traps.
- Enable user authentication so that users must log in to use the Delta product.
- Configure the two Delta nodes into a redundant cluster.

Prerequisite Knowledge

We assume that you know how to:

- Connect to the AWS Elemental Delta 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 Support Center.

Cluster Deployment Options

You can set up your cluster with leader and secondary nodes or you can also add egress-only nodes.

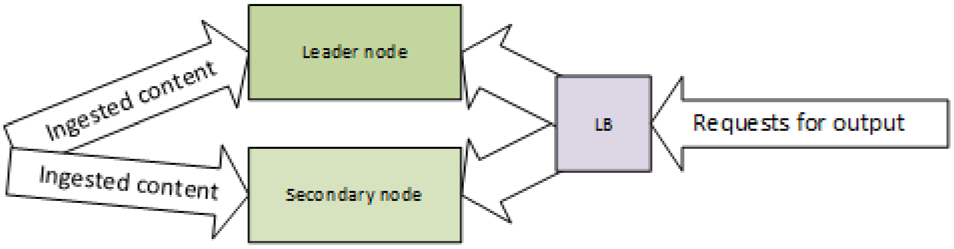
Important

It's assumed that you're using a load balancer with your AWS Elemental Delta cluster for outgoing traffic.

The load balancer is not controlled by AWS Elemental Delta and its setup is completely outside of Delta functionality. The load balancer can be set up in any suitable mode, for example, round robin mode.
The load balancer can use the Healthz feature of AWS Elemental Delta as described in Step G: Review the Cluster Management Configuration, to implement advanced balancing algorithms.

Leader and Secondary

Two nodes are set up, one as the leader and one as the secondary. You configure a load balancer on the outgoing side. This deployment is supported only in Delta 1.7 and later.



Ingest

Both the leader node and the secondary node ingest content, but only the leader node processes and stores content. If the leader node fails, the secondary node takes over content processing and storage.

Egress

Both the leader and the secondary handle requests for output. The cluster is set up with a load balancer on the request side. Incoming requests for output hit the load balancer and are redirected to either node: the leader or the secondary.

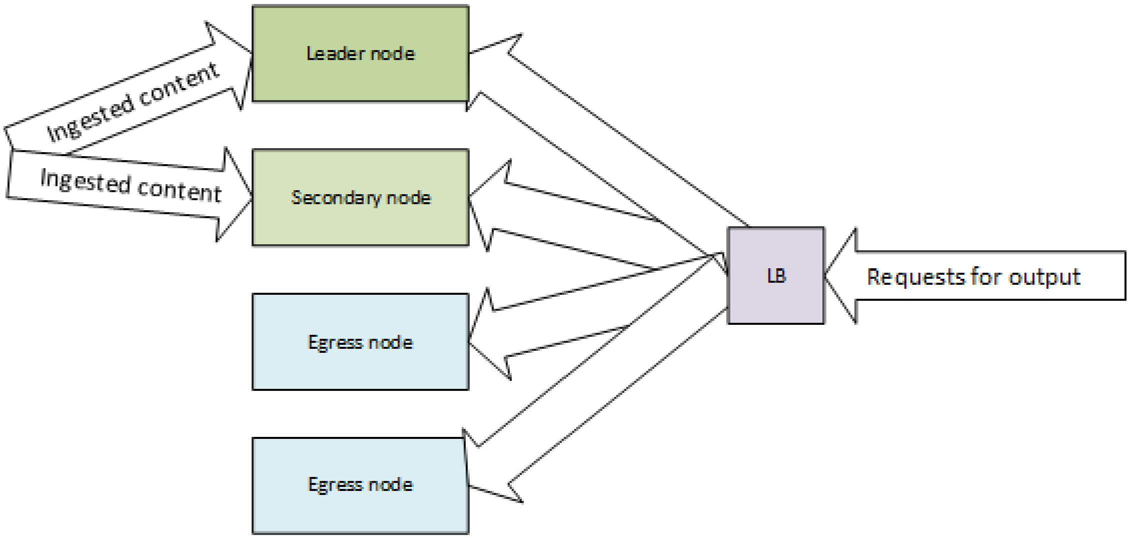
Fail Over

If it is detected that the leader has failed (the heartbeat from the leader is not detected by the secondary), then the secondary declares itself the leader and takes over ingest tasks. It also continues handling requests for output.

For more detailed information about what happens during fail over, see the article Delta Cluster Fail Over Procedure.

Leader, Secondary and Egress Nodes

Several nodes are set up, one leader, one secondary, and one or more egress nodes. You configure a load balancer on the outgoing side. This deployment is supported only in AWS Elemental Delta 1.7 and later.



Ingest

Both the leader node and the secondary node ingest content, but only the leader node processes and stores content. If the leader node fails, the secondary node takes over content processing and storage.

Egress

Every node handles requests for output.

The cluster is set up with a load balancer on the request side. Incoming requests for output hit the load balancer and are redirected to any of the egress nodes.

Fail over

If it is detected that the leader has failed (the heartbeat from the leader is not detected by the secondary), then the secondary declares itself the leader and takes over ingest tasks. It also continues handling requests for output. Egress nodes are never eligible to become leader.

If an egress node has failed, it simply becomes ineligible for handling requests for output. There is no fail over.

Creating a Cluster Configuration

A cluster of AWS Elemental Delta nodes is a grouping of nodes that work together to receive, package, and deliver content. The following sections describe how to create clusters.

Topics

- Configuring a Leader-Secondary Node Cluster
- Configuring a Leader-Secondary-Egress Node Cluster

Configuring a Leader-Secondary Node Cluster

This section describes how to create a cluster that has two nodes: a leader and a secondary node. For information about how this cluster works, see the section called “Leader and Secondary”.

Topics

- Step A: Gather Information
- Step B: Configure the Leader Node
- Step C: Configure VIPs Locally
- Step D: Configure Ports on the Firewall
- Step E: Add the Secondary Node
- Step F: Configure the Secondary Node
- Step G: Review the Cluster Management Configuration
- Step H: Test Fail Over
- Step I: Set-Up Users

Step A: Gather Information

Before you configure the leader-secondary node cluster, obtain the following information:

- The models and IP addresses (or hostnames) for all the nodes. The leader and secondary nodes must always be identical models.
- A list of Ethernet devices (for all nodes) and their IP addresses, including traffic rules such as:
    - Which IP addresses are intended to handle management and monitoring traffic.

  - Which IP addresses are intended to handle only incoming traffic (content ingest).
  - Which IP addresses are intended to handle only outgoing traffic (egress).
- A list of Ethernet devices (on the leader and secondary nodes) that are bonded, and the IP addresses for those bonds.
- A list of the Ethernet devices that were configured with IP addresses during installation of AWS Elemental Delta. The eth0 device is always configured during installation; other devices may or may not be. You need this information to determine which devices you need to figure in this configuration process and which you can assume are already configured.
- The addresses of any additional DNS servers and/or NTP servers the nodes access.
- The IP addresses of remote storage servers (CIFS, NFS or DAVFS) where ingested content is stored.
- The IP address of the remote server for AWS Elemental Delta database backups.
- The user credentials for Amazon (AWS) S3 storage, if applicable.
- A list of ports that you want to open beyond the ports that AWS Elemental Delta automatically opens.
- The IP addresses of VIPs on your network that are assigned to AWS Elemental Delta. These VIPs are associated with all of the *incoming* Ethernet devices on the leader and secondary nodes. (You have a load balancer so VIPs are not set up within Delta for the outgoing Ethernet devices.)
- The user credentials for users if you are setting up with user authentication.

Step B: Configure the Leader Node

Configure the storage and network settings on the leader node.

To configure the leader node

1. Access the web interface via the IP address of the node that is intended to be the leader.
2. On the main menu, choose **Settings**.
3. Perform the following required tasks:

   - Provide the node with access to mounted remote servers. For assistance, see Adding Mount Points.
   - Configure the node for database backups. For assistance, see Configuring for Database Backup.

4. As needed, perform these optional tasks:

   - Configure additional network devices (Ethernet devices) for the node. For assistance, see Configuring Ethernet Network Devices.
   - Set up additional DNS servers and NTP servers as needed. For assistance, see Setting up Additional DNS Servers and Setting up Additional Network Time Protocol (NTP) Servers.
   - Configure SNMP for the node. For assistance, see Setting up Alerts and Messages.
   - If you're using Amazon S3 for storage, add Amazon Web Services (AWS) credentials. For assistance, see Adding AWS Credentials.

Step C: Configure VIPs Locally

You can configure a virtual IP address (VIP) for access to manage the cluster. You use this IP address for REST API access and as a common access point for making changes to the cluster. This VIP is to be used for cluster management only. It is not intended for incoming or outgoing traffic!

To configure a VIP

1. On the main menu, choose **Nodes**.
2. Create a VIP for eth0 and any other Ethernet devices. For assistance, see Creating VIPs.

Step D: Configure Ports on the Firewall

You can leave the node firewall enabled or disabled. The installer configures each node's firewall for the ports that must be open for traffic to and from each node. If you plan to enable the firewall, you can open more ports for any reason.

For assistance opening ports or starting the firewall, see the section called “Opening Ports on the Firewall”.

⚠ **Important**

Whether the individual node firewalls are enabled or not, we recommend that the cluster always be installed behind a customer firewall on a private network.

Step E: Add the Secondary Node

Once you've set up the leader node, add the secondary node to the cluster.

To add the secondary node

1. On the web interface for the leader node, choose **Nodes** and click **Add Node** > **Ingest Capable**.
2. In the **Add New Ingest Capable Cluster Node** dialog, complete the fields: Enter the hostname or IP address of the secondary node, and the password for the *elemental* user.
3. Choose **Create**.

   The secondary node is added to the cluster. This operation may take several minutes. After a few minutes, the node is added to the cluster, shaded red on the web interface. When the addition is complete, the node is shaded green.

Step F: Configure the Secondary Node

Most of the information from the leader node is copied over to the secondary node. However, you must manually set up some features on the secondary node.

To configure the secondary node

1. Access the web interface via the VIP address for the management interface (eth0). You set up this VIP when you configured the leader node. See Creating VIPs.

   > **Note**
   >
   > Do not access the web interface from the IP address of the leader or secondary nodes.

2. Address these features if you enabled them on the leader node:

   Ethernet devices or bonds

   > Setup the secondary node with identical bonds. You can't assign the same IP address on both nodes, but you must create the same device names and bonds. For example, if the leader node is set up with eth0, eth2 and eth3 (bonded to bond0), and eth4 and eth5 (bonded to bond1), then on the secondary node, you must create eth2, eth3, eth4, eth5, bond0, and bond1.

If you don't set-up identically, then when a fail over occurs, some traffic might not failover.

For assistance, see Configuring Ethernet Network Devices.

Mount points

Set up the secondary with identical mount points as the leader node.

For assistance, see Adding Mount Points.

AWS credentials

Set up the secondary node with identical credentials as the leader node.

For assistance, see Adding AWS Credentials.

Firewall ports

Start the firewall and open the same ports on the secondary node that you opened on the leader node.

For assistance, see Opening Ports on the Firewall.

Step G: Review the Cluster Management Configuration

To ensure the leader and secondary node fail over is appropriate for your workflow, review the configuration of your cluster management settings.

To review the management configuration

1. Access the web interface via the VIP address for the management interface (eth0).
2. On the main menu, click **Nodes**.
3. Check the values of the fields across the top:

Field	Description
Heartbeat Interval	A heartbeat is sent between the leader and secondary nodes. The secondary node uses the presence or failure of this heartbeat to assume that the leader is (or is not) working.

Field	Description
Cluster-Mgr Interval	The interval (in seconds) for performing cluster management tasks such as checking for node timeouts.
Drop Node After	If it is detected that the leader node has failed (the heartbeat is not received by the secondary node), activity fails over to the secondary node after this many seconds.
Take Action Time	The number of seconds to wait after a fail over has occurred before allowing another fail over. This delay ensures that in a fail over, the new leader node has had time to completely gain control of the cluster. For example, if node A fails and node B becomes leader and this delay is too short, the system might detect that node B has failed. However, node B might not yet be completely responsive because it is still setting itself up as leader.
Healthz Replication Delay	Leave the default; this feature is not used because you do not have a load balancer.

4. To change any values, click **Settings** in the top-right corner and make your changes.

Step H: Test Fail Over

To ensure the leader and secondary node fail over works as expected, test the fail over setup.

To test fail over

1. Ideally, you should add at least one input so that AWS Elemental Delta is ingesting content. This setup provides a better test of the success of the failover.
2. Perform a forced failover to the secondary leader (node B):

    1. On the web interface for the leader node, choose **Nodes**.
    2. On the panel for the secondary node, click the fail over button (family tree icon).
3. Make sure the panels for both nodes show as green.
4. Make sure that node B shows **N/A (node is leader)** in the following fields:

    - Following Node ID
    - Replication Lag
    - Last Heartbeat
5. Display the Contents page and make sure that the content you created shows as **Live-Active**.
6. Make sure that node A shows the following:

    - **Following Node ID**: The node ID for node B.
    - **Replication Lag**: A number below 10 seconds.
    - **Last Heartbeat**: A number below 10 seconds.
7. Perform a forced fail over back to node A. Make sure that node A becomes the leader again and the content is still active.

Step I: Set-Up Users

Optionally configure the nodes for user authentication, and create users. With authentication enabled, users are required to provide valid credentials to access the AWS Elemental Delta nodes.

We recommend that you set up users as the last step in the configuration, after you have verified that node failover works.

User authentication with AWS Elemental Delta is intended to:

- Allow managers to track activity on the cluster on a per-user basis.
- To avoid accidental access to a node, create a unique username for each operator, and vary the usernames across the clusters. For example, varying usernames for each cluster ensures that a REST API operator with access to two clusters does not accidentally send a command to the wrong cluster.

Whether user authentication is enabled or not, we recommend that the cluster always be installed behind a customer firewall on a private network.

For help setting up authentication and users, see Configuring User Authentication.

Configuring a Leader-Secondary-Egress Node Cluster

This section describes how to create a cluster that has more than two nodes: a leader, a secondary, and one or more egress-only nodes. For information about how this cluster works, see the section called “Leader, Secondary and Egress Nodes”.

Topics

Step A: Gather Information

Before you configure the leader-secondary-egress node cluster, obtain the following information:

- The models and IP addresses (or hostnames) for all of the nodes. Note that:
  - The leader and secondary nodes must always be identical models.
  - The egress nodes can be different models from the leader and secondary nodes.
  - If you have more than one egress node, each node can be a different model.

  Make sure that you know which models are for which role!
- A list of Ethernet devices (for all nodes) and their IP addresses, including traffic rules such as:
  - Which IP addresses are intended to handle management and monitoring traffic.
  - Which IP addresses are intended to handle only incoming traffic (content ingest).

- Which IP addresses are intended to handle only outgoing traffic (egress).

  Keep in mind that the egress nodes handle only management traffic (typically on eth0) and outgoing traffic.

- A list of Ethernet devices (on all nodes) that are bonded, and the IP addresses for those bonds.
- A list of the Ethernet devices that were configured with IP addresses during installation of AWS Elemental Delta. The eth0 device is always configured during installation; other devices may or may not be. You need this information to determine which devices you need to figure in this configuration process and which you can assume are already configured.
- The addresses of any additional DNS servers and/or NTP servers the nodes access.
- The IP addresses of remote storage servers (CIFS, NFS or DAVFS) where ingested content is stored.
- The IP address of the remote server for AWS Elemental Delta database backups.
- The user credentials for Amazon (AWS) S3 storage, if applicable.
- A list of ports that you want to open beyond the ports that AWS Elemental Delta automatically opens.
- The IP addresses of VIPs on your network that are assigned to AWS Elemental Delta. These VIPs are associated with all of the Ethernet devices on all of the nodes.
- The user credentials for users if you are setting up with user authentication.

Step B: Configure the Leader Node

Configure the storage and network settings on the leader node.

To configure the leader node

1. Access the web interface via the IP address of the node that is intended to be the leader.
2. On the main menu, choose **Settings**.
3. Perform the following required tasks:
   - Provide the node with access to mounted remote servers. For assistance, see Adding Mount Points.
   - Configure the node for database backups. For assistance, see Configuring for Database Backup.
4. As needed, perform these optional tasks:

- Configure additional network devices (Ethernet devices) for the node. For assistance, see Configuring Ethernet Network Devices.
- Set up additional DNS servers and NTP servers as needed. For assistance, see Setting up Additional DNS Servers and Setting up Additional Network Time Protocol (NTP) Servers.
- Configure SNMP for the node. For assistance, see Setting up Alerts and Messages.
- If you're using Amazon S3 for storage, add Amazon Web Services (AWS) credentials. For assistance, see Adding AWS Credentials.

Step C: Configure VIPs Locally

You can configure a VIP for access to manage the cluster. You use this IP address for REST API access and as a common access point for making changes to the cluster. Use this VIP for cluster management only. It is not intended for incoming or outgoing traffic!

You can configure a virtual IP address (VIP) for access to manage the cluster. You use this IP address for REST API access and as a common access point for making changes to the cluster. This VIP is to be used for cluster management only. It is not intended for incoming or outgoing traffic!

To configure a VIP

1. On the main menu, choose **Nodes**.
2. Create a VIP for eth0 and any other Ethernet devices. For assistance, see Creating VIPs.

Step D: Configure Ports on the Firewall

You can leave the node firewall enabled or disabled. The installer configures each node's firewall for the ports that must be open for traffic to and from each node. If you plan to enable the firewall, you can open more ports for any reason.

For assistance opening ports or starting the firewall, see the section called “Opening Ports on the Firewall”.

> ⚠ **Important**
>
> Whether the individual node firewalls are enabled or not, we recommend that the cluster always be installed behind a customer firewall on a private network.

Step E: Add the Secondary Node

Once you've set up the leader node, add the secondary node to the cluster.

To add the secondary node

1. On the web interface for the leader node, choose **Nodes** and click **Add Node** > **Ingest Capable**.
2. In the **Add New Ingest Capable Cluster Node** dialog, complete the fields: Enter the hostname or IP address of the secondary node, and the password for the *elemental* user.
3. Choose **Create**.

   The secondary node is added to the cluster. This operation may take several minutes. After a few minutes, the node is added to the cluster, shaded red on the web interface. When the addition is complete, the node is shaded green.

Step F: Configure the Secondary Node

Most of the information from the leader node is copied over to the secondary node. However, you must manually set up some features on the secondary node.

To configure the secondary node

1. Access the web interface via the VIP address for the management interface (eth0). You set up this VIP when you configured the leader node. See Creating VIPs.

   > **Note**
   >
   > Do not access the web interface from the IP address of the leader or secondary nodes.

2. Address these features if you enabled them on the leader node:

   Ethernet devices or bonds

      Setup the secondary node with identical bonds. You can't assign the same IP address on both nodes, but you must create the same device names and bonds. For example, if the leader node is set up with eth0, eth2 and eth3 (bonded to bond0), and eth4 and eth5 (bonded to bond1), then on the secondary node, you must create eth2, eth3, eth4, eth5, bond0, and bond1.

If you don't set-up identically, then when a fail over occurs, some traffic might not failover.

For assistance, see Configuring Ethernet Network Devices.

Mount points

Set up the secondary with identical mount points as the leader node.

For assistance, see Adding Mount Points.

AWS credentials

Set up the secondary node with identical credentials as the leader node.

For assistance, see Adding AWS Credentials.

Firewall ports

Start the firewall and open the same ports on the secondary node that you opened on the leader node.

For assistance, see Opening Ports on the Firewall.

Step G: Add the Egress Nodes

Once you've set up the leader and secondary nodes, add the egress nodes to the cluster.

To add egress nodes

1. On the web interface for the leader node, choose **Nodes** and click **Add Node** > **Egress Only**.
2. In the **Add New Egress Only Cluster Node** dialog, complete the fields: Enter the hostname or IP address of the first egress node, and the password for the *elemental* user.
3. Choose **Create**.

   The egress node is added to the cluster. This operation may take several minutes. After a few minutes, the node is added to the cluster, shaded red on the web interface. When the addition is complete, the node is shaded green.
4. Repeat these steps for each additional egress node.

Step H: Configure the Egress Nodes

Most of the information from the leader node is copied over to the egress nodes. However, you must manually set up some features on the egress nodes.

To configure the egress node

1. Access the web interface via the VIP address for the management interface (eth0). You set up this VIP when you configured the leader node. See Creating VIPs.

   > **Note**
   >
   > Do not access the web interface from the IP address of the leader or secondary nodes.

2. Set up the egress nodes with additional network devices or bonds as needed. For assistance, see Configuring Ethernet Network Devices.
3. Address these features if you enabled them on the leader node:

   Mount points

   Set up the egress nodes with identical mount points as the leader node.

   For assistance, see Adding Mount Points.

   AWS credentials

   Set up the secondary node with identical credentials as the leader node.

   For assistance, see Adding AWS Credentials.

   Firewall ports

   Start the firewall and open the same ports on the egress nodes that you opened on the leader node.

   For assistance, see Opening Ports on the Firewall.

Step I: Review the Cluster Management Configuration

To ensure the leader and secondary node fail over is appropriate for your workflow, review the configuration of your cluster management settings.

To review the management configuration

1. Access the web interface via the VIP address for the management interface (eth0).
2. On the main menu, click **Nodes**.
3. Check the values of the fields across the top:

Field	Description
Heartbeat Interval	A heartbeat is sent between the leader and secondary nodes. The secondary node uses the presence or failure of this heartbeat to assume that the leader is (or is not) working.
Cluster-Mgr Interval	The interval (in seconds) for performing cluster management tasks such as checking for node timeouts.
Drop Node After	If it is detected that the leader node has failed (the heartbeat is not received by the secondary node), activity fails over to the secondary node after this many seconds.
Take Action Time	The number of seconds to wait after a fail over has occurred before allowing another fail over. This delay ensures that in a fail over, the new leader node has had time to completely gain control of the cluster. For example, if node A fails and node B becomes leader and this delay is too short, the system might detect that node B has failed. However, node B might not yet be completely responsive because it is still setting itself up as leader.
Healthz Replication Delay	Leave the default; this feature is not used because you do not have a load balancer.

4. To change any values, click **Settings** in the top-right corner and make your changes.

Step J: Test Fail Over

To ensure the leader and secondary node fail over works as expected, test the fail over setup.

To test fail over

1. Ideally, you should add at least one input so that AWS Elemental Delta is ingesting content. This setup provides a better test of the success of the failover.
2. Perform a forced failover to the secondary leader (node B):
    1. On the web interface for the leader node, choose **Nodes**.
    2. On the panel for the secondary node, click the fail over button (family tree icon).
3. Make sure the panels for both nodes show as green.
4. Make sure that node B shows **N/A (node is leader)** in the following fields:
    - Following Node ID
    - Replication Lag
    - Last Heartbeat
5. Display the Contents page and make sure that the content you created shows as **Live-Active**.
6. Make sure that node A shows the following:
    - **Following Node ID**: The node ID for node B.
    - **Replication Lag**: A number below 10 seconds.
    - **Last Heartbeat**: A number below 10 seconds.
7. Perform a forced fail over back to node A. Make sure that node A becomes the leader again and the content is still active.

Step K: Set-Up Users

Optionally configure the nodes for user authentication, and create users. With authentication enabled, users are required to provide valid credentials to access the AWS Elemental Delta nodes.

We recommend that you set up users as the last step in the configuration, after you have verified that node failover works.

User authentication with AWS Elemental Delta is intended to:

- Allow managers to track activity on the cluster on a per-user basis.
- To avoid accidental access to a node, create a unique username for each operator, and vary the usernames across the clusters. For example, varying usernames for each cluster ensures that a REST API operator with access to two clusters does not accidentally send a command to the wrong cluster.

Whether user authentication is enabled or not, we recommend that the cluster always be installed behind a customer firewall on a private network.

For help setting up authentication and users, see Configuring User Authentication.

Modifying the Configuration

The following section describes how to make changes to a cluster configuration.

Topics

- Adding an Egress Node to an Existing Deployment

Adding an Egress Node to an Existing Deployment

If you have a cluster with a leader and secondary node, you can also add any number of egress nodes.

This section describes how to add the egress nodes.

You can add each node while the cluster is in production, ingesting and outputting content.

Step A: Gather Information

Before you modify a cluster configuration, obtain the following information:

- The models and IP addresses (or hostnames) for all of the nodes. Note that:
  - The egress nodes can be different models from the leader and secondary nodes.
  - If you have more than one egress node, each node can be a different model.

  Make sure that you know which models are for which role!
- A list of Ethernet devices (for all egress nodes) and their IP addresses. Keep in mind that the egress nodes handle only management traffic (typically on eth0) and outgoing traffic.
- A list of Ethernet devices (on all egress nodes) that are bonded and the IP addresses for those bonds.
- A list of the Ethernet devices (on the egress nodes) that were configured with IP addresses during installation of AWS Elemental Delta. The eth0 device is always configured during installation; other devices may or may not be. You need this information to determine which devices you need to figure in this configuration process and which you can assume are already configured.
- The IP addresses of remote storage servers (CIFS, NFS or DAVFS) as already set up on the leader and secondary nodes.
- The user credentials for Amazon (AWS) S3 storage, if applicable.

- A list of ports that you want to open beyond the ports that AWS Elemental Delta automatically open.
- The user credentials for users if you are setting up with user authentication.

Step B: Add the Egress Nodes

When you have gathered all of the required information, add the egress nodes to the cluster.

To add egress nodes

1. On the web interface for the leader node, choose **Nodes** and click **Add Node** > **Egress Only**.
2. In the **Add New Egress Only Cluster Node** dialog, complete the fields: Enter the hostname or IP address of the first egress node, and the password for the *elemental* user.
3. Choose **Create**.

   The egress node is added to the cluster. This operation may take several minutes. After a few minutes, the node is added to the cluster, shaded red on the web interface. When the addition is complete, the node is shaded green.
4. Repeat these steps for each additional egress node.

Step C: Configure the Egress Nodes

Most of the information from the leader node is copied over to the egress nodes. However, you must manually set up some features on the egress nodes.

To configure the egress node

1. Access the web interface via the VIP address for the management interface (eth0). You set up this VIP when you configured the leader node. See Creating VIPs.

   > **Note**
   >
   > Do not access the web interface from the IP address of the leader or secondary nodes.
2. Set up the egress nodes with additional network devices or bonds as needed. For assistance, see Configuring Ethernet Network Devices.
3. Address these features if you enabled them on the leader node:

Mount points

Set up the egress nodes with identical mount points as the leader node.

For assistance, see Adding Mount Points.

AWS credentials

Set up the secondary node with identical credentials as the leader node.

For assistance, see Adding AWS Credentials.

Firewall ports

Start the firewall and open the same ports on the egress nodes that you opened on the leader node.

For assistance, see Opening Ports on the Firewall.

Tasks

The following sections provide steps to complete cluster and node configuration tasks.

Topics

Accessing and Navigating the Web Interface

At your workstation, open a web browser and enter the IP address and port (8080) of the node that is currently the leader or that is designated as the leader (for a cluster that has not yet been configured).

During configuration, the address you enter is the IP address of the individual node. (Later on, when AWS Elemental Delta is running, you typically access the web interface through the ingest virtual IP address that you set up during this configuration procedure.)

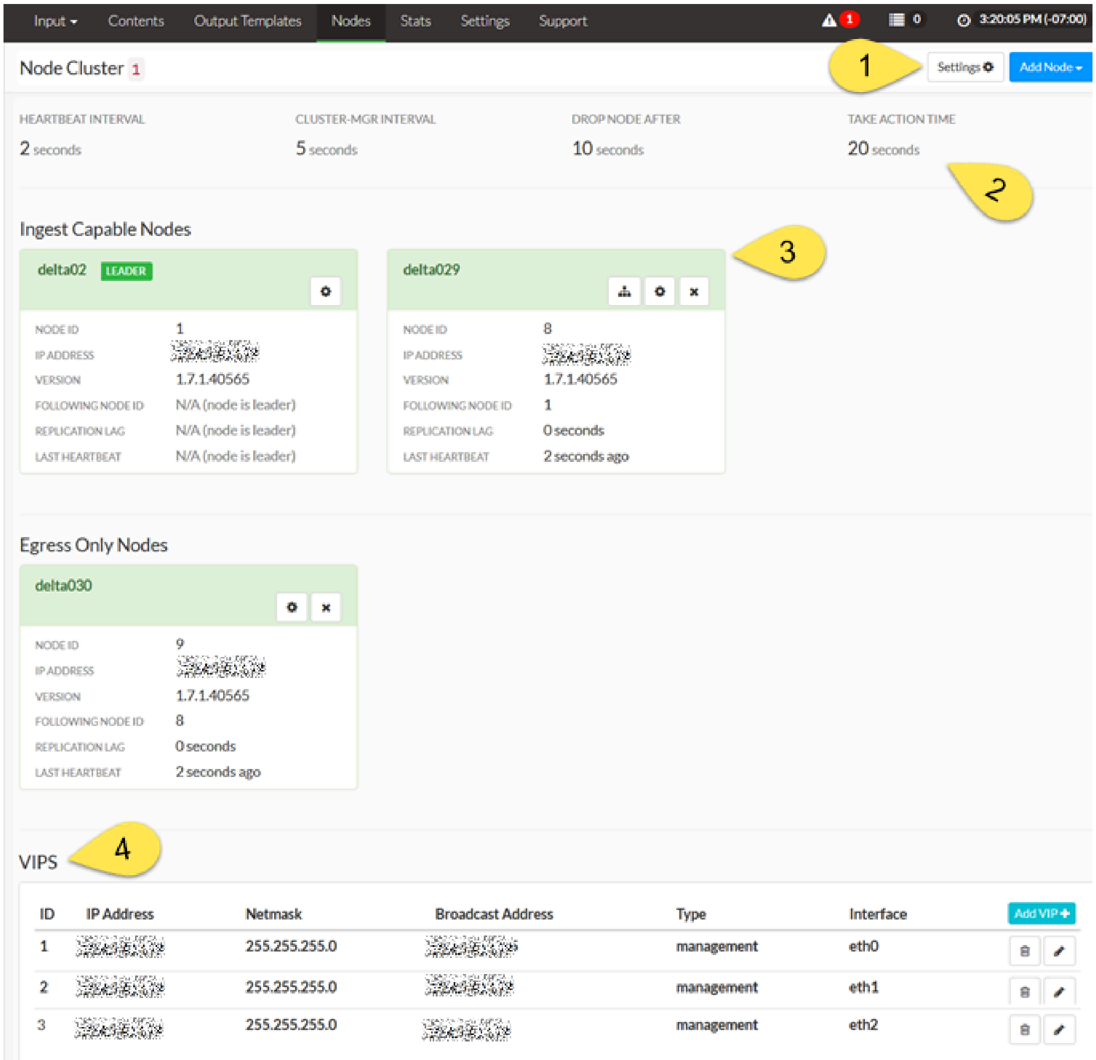
For example **`http://10.24.34.2:8080`**.

The web interface appears. The two screens used for configuration are the Node screen and the Settings screen.

Nodes Screen

The **Nodes** screen provides information about the cluster, such as what nodes make up the cluster.

The following graphic depicts an example **Nodes** screen. Important web elements are numbered and described in the table.



HEARTBEAT INTERVAL	CLUSTER-MGR INTERVAL	DROP NODE AFTER	TAKE ACTION TIME
2 seconds	5 seconds	10 seconds	20 seconds

Ingest Capable Nodes

delta02 LEADER

NODE ID	1
IP ADDRESS	[redacted]
VERSION	1.7.1.40565
FOLLOWING NODE ID	N/A (node is leader)
REPLICATION LAG	N/A (node is leader)
LAST HEARTBEAT	N/A (node is leader)

delta029

NODE ID	8
IP ADDRESS	[redacted]
VERSION	1.7.1.40565
FOLLOWING NODE ID	1
REPLICATION LAG	0 seconds
LAST HEARTBEAT	2 seconds ago

Egress Only Nodes

delta030

NODE ID	9
IP ADDRESS	[redacted]
VERSION	1.7.1.40565
FOLLOWING NODE ID	8
REPLICATION LAG	0 seconds
LAST HEARTBEAT	2 seconds ago

VIPS

ID	IP Address	Netmask	Broadcast Address	Type	Interface
1	[redacted]	255.255.255.0	[redacted]	management	eth0
2	[redacted]	255.255.255.0	[redacted]	management	eth1
3	[redacted]	255.255.255.0	[redacted]	management	eth2

The following table describes the web element for each number in the graphic.

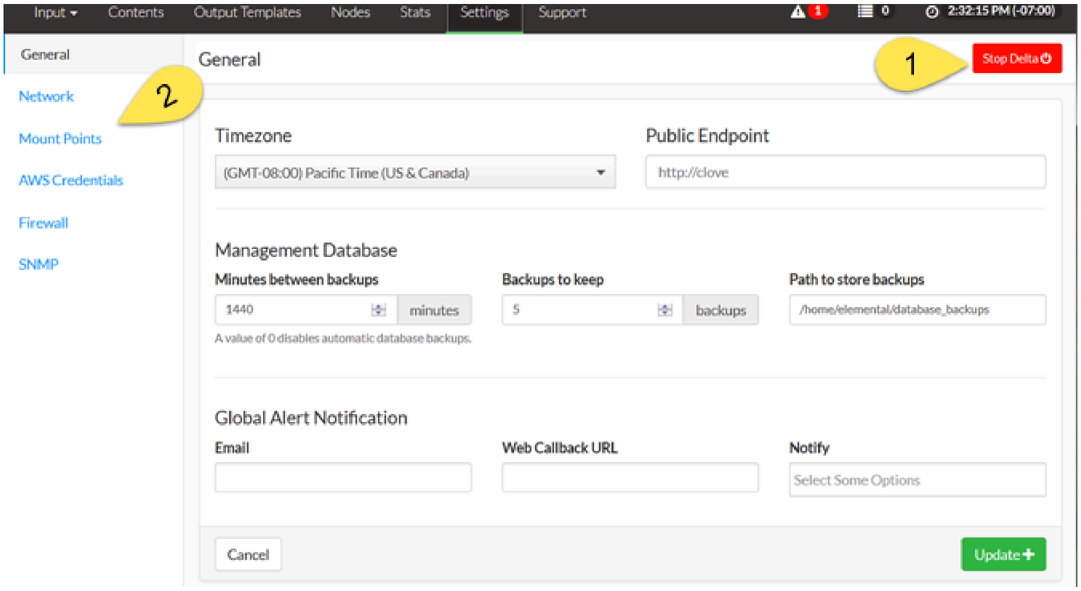
Number in Graphic	Web Element	Instructions
1	**Settings** and **Add Node** buttons	Choose **Settings** to access the cluster settings. Choose **Add Node** to add a secondary or egress node to the cluster.

Number in Graphic	Web Element	Instructions
2	**Heartbeat Interval**, **Cluster-Mgr Interval**, **Drop Node After**, **Take Action Time** fields	Settings for the cluster. For definitions of the fields, see Step I: Review the Cluster Management Configuration.
3	Node information boxes	Information about each of the nodes in the cluster. You set these when you configure the cluster management. You can also use the buttons to stop a node or force failover to the secondary node.
4	VIPS section	An element which provides information about the VIPs that you set up on the cluster. For information,Creating VIPs.

Settings Screen

The Settings screen provides information about general settings for the cluster.

The following graphic depicts an example **Settings** screen. Important web elements are numbered and described in the table.



General

Timezone: (GMT-08:00) Pacific Time (US & Canada)

Public Endpoint: http://clove

Management Database

Minutes between backups: 1440 minutes

A value of 0 disables automatic database backups.

Backups to keep: 5 backups

Path to store backups: /home/elemental/database_backups

Global Alert Notification

Email:

Web Callback URL:

Notify: Select Some Options

The following table describes the web element for each number in the graphic.

Number in Graphic	Web Interface Element	Instructions
1	**Stop Delta** button	Click to stop the elemental_se service on this node only.
2	List of settings pages	Click to modify settings. For more information, see these sections: • General settings • Configuring the Time Zone • Configuring for Database Backup • Designating VOD Catalog Metadata Storage • Setting up for Email or Web Server Alert Notification • Network settings

Number in Graphic	Web Interface Element	Instructions
		- Configuring Ethernet Network Devices - Setting up Additional DNS Servers - Setting up Additional Network Time Protocol (NTP) Servers • Mount Points settings - Adding Mount Points • AWS Credentials settings - Adding AWS Credentials • Firewall settings - Opening Ports on the Firewall • SNMP settings - Setting Up SNMP Traps

Configuring the Time Zone

Follow this procedure if you did not set the time zone when installing (via the `-t` prompt) or if you want to change the time zone.

To configure the time zone

1. From the web interface for the node, go to the **Settings** > **General** screen and set the time zone.
2. Choose **Update**.

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

This setting does not affect the following:

- Time reporting on the individual AWS Elemental Delta nodes: you should have set the time zone for each node when you installed Delta.
- Activity via SSH or via the REST API.

Configuring for Database Backup

The node is automatically configured to back up its database to `/home/elemental/database_backups` on the local disk.

> ⚠ **Important**
>
> We strongly advise that you mount a remote folder as the location for backups. In that way, if the hardware unit fails, you can restore the database from that remote folder.

Perform the following procedure on each node.

To configure database backups

1. Choose a remote server in your organization and designate a folder for backups. Mount that folder to the node as described in the section called “Adding Mount Points”.
2. On the web interface for the node, choose **Settings** > **General**.
3. In **Path to Store Backups,** enter the path to the mount folder. The path always starts with /data/mnt/. For example, **`/data/mnt/delta01-backups`**

   > ⓘ **Note**
   >
   > Make sure you back up each node’s database to its own folder; do not back up the two nodes to the same folder.

4. Change other fields as desired.

   Note that, when you reach the indicated number of backups to keep, AWS Elemental Delta deletes the oldest file before saving the next backup.
5. If you changed the **Minutes between backups**, you must restart the node for the change to take effect. Run this command from the node:

```
[elemental@hostname ~]$ sudo reboot
```

Backup files are named in this format: <yyyy-mm-dd_hh-mm-ss.tar.bz2>

To restore a database to a node

1. At your workstation, start a remote terminal session to the hardware unit that is running AWS Elemental Delta. Log in with the user name *elemental*.
2. Run the install script with the restore option:

   ```
   [elemental@hostname ~]$ sudo sh product --restore-db-backup pathbackup-file
   ```

   where:

   - *product* is the product installer. For example, elemental_production_delta.2.3.0.123456.run.
   - *path* is the path to the backup file. This path could simply be the remote folder where backups were originally stored.
   - *backup-file* is the file you want to restore. AWS Elemental Delta unzips the file and copies it to the appropriate folder. Do not unzip the file manually before restoring it!

Designating VOD Catalog Metadata Storage

If any assets that AWS Elemental Delta ingests are converted to VOD Catalog contents, you must specify the location for metadata storage in the settings for Delta.

To configure VOD Catalog metadata storage

1. From the web interface for the node, go to the **Settings** > **General** screen.
2. In the **VOD Catalog Metadata Storage** section, complete **Location** and **AWS Credentials** (if the storage location is an Amazon S3 bucket).
3. Click **Update** to save the information.

For more information about VOD Catalog, see the Working with VOD Catalog Assets in AWS Elemental Delta feature guide.

Configuring Ethernet Network Devices

When you installed AWS Elemental Delta on each node, eth0 was automatically set up. You may also have chosen to set up other Ethernet devices via installation. If you did not do so, you can set them up on the **Settings** > **Network** screen.

In addition, you can optionally set up bonding for any Ethernet devices that have been set up.

Adding Ethernet Devices

You can add Ethernet devices after the initial installation is complete.

To add Ethernet devices

1. On the web interface, go to the **Settings** > **Network** screen.
2. Click **Add Device** and choose **Ethernet**.
3. In the **Add New Network Device** dialog, complete the following fields.

Field	Description
Device Name	Choose a name for the device. The list is populated with Ethernet ports that have been detected on the node.
Description	Optional
Master	Specify **No devices with port bond settings available**. This wording indicates that you have not created a bond-type device, so bonding is not available.
Management	Leave this unchecked because eth0 typically has usually been set up as the management interface.
DHCP / Static Routing / Port Bonding	Check **DHCP** or **Static Routing**.
If you choose Static Routing, extra fields appear for you to configure the device.	**IP Address**, **Netmask**, **Gateway** and (optionally) **Static Routes**.

4. Click **Create**. The new device now appears in the **Network Devices** section.

Bonding Ethernet Devices

You can create as many separate bonds as you want. You can include as many Ethernet devices as you want in each bond (you can bond any number of devices together). You must have already set up the Ethernet devices that are to be bonded, as described in Adding Ethernet Devices.

Step A: Create the Bond

Create the bond to which you will add Ethernet devices in a later step.

To create the bond

1. Click **Add Device** and choose **Bonded**.
2. In the **Add New Network Device** dialog, complete the following fields.

Field	Description
Device Name	Must be named **bond** plus a number, typically starting at 0.
Description	Optional.
Management Enabled	Checked if the bond interface will be used for management. Check this field only if you are bonding eth0 and another Ethernet device.
Port Bonding Mode	Choose the desired mode. See the following *Bonding Modes* table.
Link Mode	Choose the appropriate mode. See the following *MII Link Modes* table.
Carrier	Check if appropriate.
Static Routes	Complete fields or leave blank.

3. Click **Create**. The bond appears in the **Network Devices** section.

Bonding Modes

The following table describes the bonding modes that are available.

Mode ID	Mode	Description
0	Round Robin	Sets a round robin policy for fault tolerance and load balancing among the Ethernet ports.Receives and sends out transmissions sequentially on each bonded slave interface, beginning with the first one available.
1	Active Backup	Sets an active backup policy for fault tolerance. Receives and sends out transmissions via the first available bonded slave interface. The other bonded slave interface is only used if the active bonded slave interface fails.
2	Balanced XOR	Sets an XOR (exclusive-or) policy for fault tolerance and load balancing (among the Ethernet ports). Using this method, the interface matches up the incoming request's MAC address with the MAC address for one of the slave NICs. Once this link is established, sends out transmissions sequentia lly, beginning with the first available interface.

Mode ID	Mode	Description
3	Broadcast	Sets a broadcast policy for fault tolerance. Sends out all transmissions on all slave interfaces.
4	IEEE 803.ad Dynamic Link Aggregation	Sets an IEEE 802.3ad dynamic link aggregation policy. Creates aggregation groups that share the same speed and duplex settings. Transmits and receives transmissions on all slaves in the active aggregator. Requires a switch that is 802.3ad-compliant.
5	Adaptive Transmit Load Balancing	Sets a Transmit Load Balancing (TLB) policy for fault tolerance and load balancing (among the Ethernet ports). Distributes the outgoing traffic according to the current load on each slave interface. The current slave receives incoming traffic. If the receiving slave fails, another slave takes over the MAC address of the failed slave.

Mode ID	Mode	Description
6	Adaptive Load Balancing	Sets an Active Load Balancing (ALB) policy for fault tolerance and load balancing . This includes transmit and receive load balancing for IPV4 traffic. Achieves receive load balancing through address resolution protocol (ARP) negotiation.

MII Link Mode Fields

The following table describes the fields for MII Link bonding mode.

Field	Description
MII Monitoring Frequency	Specifies the MII link-monitoring frequency in milliseconds. The frequency determines how often the link state of each slave is inspected for link failures. 100ms is a good starting point.
Down Delay	Specifies the time in milliseconds to wait before disabling a slave after a link failure has been detected. Only applies to the MII Link Mode; should be a multiple of the MII Monitoring Frequency (rounded to nearest multiple). Defaults to 0.
Up Delay	Specifies the time, in milliseconds, to wait before enabling a slave after a link recovery has been detected. Only applies to the MII Link Mode; should be a multiple of the MII Monitoring Frequency (rounded to the nearest multiple). Defaults to 0.

Field	Description
Carrier	Used in conjunction with the MII Link Mode. If checked, then MII uses MII or ETHTOOL `ioctls` (less efficient and uses deprecated kernel calling sequences) instead of netif_car rier_ok. This setting relies on the device driver to maintain link state.

ARP Mode Fields

The following table describes the fields for ARP bonding mode.

Field	Description
ARP Interval	Specifies the ARP link-monitoring frequency in milliseconds. It periodically checks slave devices for traffic; generates regular interval traffic via ARP probes for ARP IP Target.
ARP IP Target	Specifies the IP address to use for ARP probes in ARP Link Mode.

Step B: Assign the Bond

After you create the bond, assign devices to it.

To assign the bond

1. Click **Edit** at the far right of the first Ethernet device to assign to the bond.
2. On the **Manage Network Device** dialog, in **Master**, choose the bond.
3. Click **Create**.

   This device now shows with **Master** unchecked to indicate that it is bonded.
4. Repeat for each device to include in the given bond.
5. Repeat to add other devices to other bonds, if applicable.

Setting up Additional DNS Servers

The DNS server for the node is usually set up initially during the node installation. After the install is complete, you can use the web interface to add more DNS servers, as required.

To set up DNS servers

1. On the web interface for the node, choose **Settings** > **Network** screen.
2. In the **Domain Name Servers** section, click **Add DNS**.
3. Add the IP address and click **Add**.

Setting up Additional Network Time Protocol (NTP) Servers

The Network Time Protocol (NTP) server for the node is usually set up initially during node installation. After the install is complete, you can use the web interface to add more NTP servers, as required.

To set up NTP servers

1. On the web interface for the node, choose **Settings** > **Network** screen.
2. In the **Network Time Protocol Servers** section, click **Add NTP**.
3. Add the IP address and click **Add**.

Adding Mount Points

A mount point provides AWS Elemental Delta access to a remote server. The following are some examples for why Delta might need to access a remote server:

- For storage: In input filters, you must specify a storage location for the content associated with the input filter. If this location is a remote folder, it must be mounted to the Delta node.

  Both the leader and secondary node should mount the same remote storage folders to ensure that the storage stays the same regardless of which node is the leader.
- For database backup: We strongly recommend that you back up the database to a remote server. This server must be mounted to the Delta node.

Each node in the cluster should mount a different database backup storage folder: the nodes should not be storing to the same remote server location.

Remote servers are always mounted to this location on the AWS Elemental Delta node: `/data/mnt/<folder>`.

When you mount a remote folder to a local mount folder, all of the contents of the remote folder appear in this mount folder, as if the contents were actually in this folder on the local hardware unit. In this way, you can view the folder, and, for example, verify that backup files have been created.

To add mount points

1. On the web interface for the node, choose **Settings** > **Mount Points**.
2. Click **Add Mount Point**.
3. In the **Add New Mount Point** dialog, complete the dialog. The following table describes the settings.

Field	Description
Type	Choose the type of remote server: • **cifs**: Choose this for a Windows CIF server or for a Windows or Mac SMB server. • **nfs**: Choose this for a Linux server. • **webdav**: Choose this for a DavFS server. ⚠ **Important** For live workflow storage, we recommend that you use NFS or CIFS file servers. AWS Elemental Delta provides DavFS as a mounting option for a limited number of use cases, such as moving ancillary files (like DRM

Field	Description
	policy files) at a low rate. DavFS is often too slow to be used as storage for live inputs.
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, it is automatically created.
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.

4. Click **Create** and wait a few minutes. The newly mounted folder appears on the screen.

Adding AWS Credentials

If you use an Amazon S3 remote server to store ingested assets, you must set up Amazon Web Services (AWS) credentials. Then, when you create an input filter on the AWS Elemental Delta web interface, these credentials automatically appear in the **AWS Credentials** field.

This procedure assumes that you have already set up an account on AWS and have user credentials.

To add AWS credentials

1. On the web interface for the node, choose **Settings** > **AWS Credentials**.
2. Click **Add Credentials**.

3. In the **Add New AWS Credentials** dialog, complete the fields and click **Create**.

The credentials are added to the list on the **AWS Credentials** screen.

> **Note**
>
> You can't modify AWS credentials. If you need to make a change, delete the existing credential and add another.

Opening Ports on the Firewall

This section describes how to enable or disable the firewall around individual nodes. The installer configures the ports on your firewall that must be open for incoming and outgoing traffic to and from each node. You can open more ports if required for any reason.

> **Note**
>
> Whether the individual firewalls are enabled or not, we recommend that the cluster always be installed behind a customer firewall on a private network.

Perform this procedure on each node.

To open ports on the firewall

1. On the web interface, choose **Settings** > **Firewall**.
2. Click **Start Firewall.**
3. In the list of ports, add or delete ports as desired.

Setting up Alerts and Messages

AWS Elemental systems provide information about the status of the systems and the channels via alerts and messages. Alerts can be sent to you on the status of the system. You can view the content of the alert in a variety of ways. The following table describes how you can access alerts and messages, and what information each provides.

	Alerts	Messages
Access Options	Web UI SNMP poll REST calls Automatic email notification Web callback notification SNMP trap	Web UI SNMP poll REST calls
Information Conveyed	Alerts are feedback on a problem that must be fixed. This can be helpful when you are receiving automatic email notifications, letting you know to check for related messages on the web interface.	There are three types of messages: **AuditMessage:** Informational messages to which you do not need to react. 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/Inactive	Alerts are active until the underlying problem is resolved. When the cause of the alert is no longer present,	Messages are neither active nor inactive. They are defined as *recent* when they are fewer than 24 hours old.

	Alerts	Messages
	the system clears the alert and it becomes inactive.	
Visibility (Web UI 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. Visibility does not affect the return of SNMP and REST requests. Visibility does not affect email notifications, web callback notifications, or the emission of SNMP traps.	You can toggle the visibilit y 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.

See the AWS Elemental Delta 2.3 User Guide for details on viewing alerts and messages via the web interface.

See the AWS Elemental Delta 2.3 API Guide for information about using the REST interface to get alerts and messages.

Setting up for Email or Web Server Alert Notification

You can set up AWS Elemental Delta to notify you when alerts occur. The notification can be an email or an HTTP POST to a web server.

AWS Elemental use open relay to send email notifications. Before subscribing to notifications, make sure that your network allows receipt of open relay email. To receive messages from an AWS Elemental system in a network that does not allow receipt of open relay email, configure a sendmail relay with another mail server, as described in Configuring Sendmail Relay Server.

⚠ **Warning**

If you subscribe to email notifications in a network that does not allow open relay and you do not relay the messages, the generated messages collect on the system hard drive, eventually fill the partition, and cause disk alert errors.

To subscribe to all alerts generated by the cluster

1. Go to **Settings**, which defaults to the **General** tab.
2. Complete the dialog by selecting settings from the table that follows.

Field	Instructions
Settings	Click to go to the **Settings** > **General** tab.
Email	Enter the email address of the alert recipient. This is required if you do not enter a URL in the Web Callback field.
Web Callback URL	Enter the URL of the appropriate .php file on your web server in the Web Callback URL field. This is required if you do not enter an email address. For instructions on how to configure your web server to receive notifications, see Configuring a Web Server for Notifications.
Notify	Select one or more of the options in the **Notify** drop-down box. The selections represent the type of change to the alert; for example, "On Started" means *when the alert first appears*. You can select several options. Some options only apply to some alerts.

Field	Instructions
Update	Click to finish subscribing to alerts.

To subscribe to only specific alerts

1. Go to the **Stats** > **Alerts** page and click **All** to bring up a list of all alerts.
2. In the row for the alert you want to subscribe to, click the edit (pencil) icon to bring up the **Notification** dialog.
3. Complete the dialog by selecting settings from the following table.

Field	Instructions
Notify	Select one or more of the options in the Notify drop-down box. The selections represent the type of change to the alert; for example, "On Started" means “when the alert first appears”. You can select several options. Some options only apply to some alerts.
Email	Enter the email address of the alert recipient. This is required if you do not enter a URL in the Web Callback field.
Web Callback URL	Enter the URL of the appropriate .php file on your web server in the Web Callback URL field. This is required if you do not enter an email address. For instructions on how to configure your web server to receive notifications, see Configuring a Web Server for Notifications.
Update	Click to finish subscribing to alerts.

4. Repeat these steps for each individual alert to which you're subscribing.

Configuring a Web Server for Notifications

To receive web callback notifications, you must have a web server that supports Hypertext Preprocessor (PHP) scripting. You can configure this server to receive alert notifications from AWS Elemental systems as follows.

To configure a web server

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. In this example, the file is called `notification.`php and is saved in the directory `/webcallback.`

3. Subscribe to global or individual alerts as described Setting up for Email or Web Server Alert Notification. In the **Web Callback URL** field, enter the URL to your web server, e.g.**`http://yourdomain.com/webcallback/notification.php`**

4. Test your setup by typing the following (in a single line) at the command line of your AWS Elemental Delta system:

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

5. Open your `notification.`php file 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=value1&param2=value2
```

6. Enter your web callback URL (e.g. http://yourdomain.com/webcallback/notify) into a web browser to see the HTTP POST.

Configuring Sendmail Relay Server

Use this procedure to set up a Sendmail relay server if your network does not accept open relay messages.

This procedure involves editing a file using a text editor at the Linux command line. These instructions are for using Nano, which is already installed on all AWS Elemental systems.

Topics

- Step A: Gather the Mail Server Information
- Step B: Install the Sendmail Configuration Tool
- Step C: Edit the Sendmail.mc File
- Step D: Check the Hosts File
- Step E: Apply the Changes
- Step F: Test the New Configuration

Step A: Gather the Mail Server Information

To configure your AWS Elemental Delta node to relay the notification emails through a mail server, you need the following information about the mail server.

- hostname
- IP address; this is only required if DNS is not configured on the network.

Step B: Install the Sendmail Configuration Tool

Install the sendmail-cf configuration tool to make required changes.

To install the Sendmail configuration tool

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

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

   You see a caution message asking you to confirm that you want to run the command.

   ```
   ##############################################################
   ##############################################################

   CAUTION: Updating system configurations can interfere with
   the proper operation of Elemental software.

   ##############################################################
   ##############################################################
   ```

2. Type **yes**.

   The system will work for a while, then prompt you:

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

3. Type **y**.

   The system will work for a while, then return the message `Complete!`.

Step C: Edit the Sendmail.mc File

Edit the `sendmail.mc` file to update the mail server host name.

To edit the sendmail.mc file

1. Open the `sendmail.mc` file:

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

   This opens the file in Nano. You see the cursor at the top of the screen.

2. Use the down arrow key to go to the line that defines SMART_HOST. It is just past halfway down the page.

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

3. Uncomment this line by using the Delete key and the arrow keys to delete the `dnl` at the beginning and end of the line.
4. Change the text “`smtp.your.provider`” to the host name of the mail server that is performing the relay.
5. Use the keys Ctrl+o to save the file, then Ctrl+x to exit Nano.

Step D: Check the Hosts File

If your network is not configured with DNS, you also need to add a static entry to the hosts file on your AWS Elemental Delta node. To do so:

To check the hosts file

1. Open the file `/etc/hosts` in Nano as shown here:

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

   You see something similar to this:

   ```
   132.0.0.1 SYS-1 localhost localhost.localdomain localhost4 localhost4.localdomain4
   ::1 SYS-1 localhost localhost.localdomain localhost6 localhost6.localdomain6
   ```

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 as shown below.

   ```
   192.0.2.0 ExampleMailHostname
   ```

3. Use the keys Ctrl+o to save the file, then Ctrl+x to exit Nano.

Step E: Apply the Changes

Save and apply the changes that you made.

To apply the changes

1. Type the following command to apply the changes:

   ```
   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:

   ```
   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. Subscribe to global alert notifications on the AWS Elemental Delta web interface, on the **Settings** page. Provide an email address that to which you have easy access.
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 but provide a bogus input address, such as udp://1.1.1.1:1111.
3. Check your email for the notifications message.

4. If you changed the alert recipient in step 1, return to Settings and re-subscribe the original recipient.

Setting Up SNMP Traps

Nodes can be configured to generate SNMPv2 traps for all active alerts generated by the leader AWS Elemental Delta node.

SNMP traps are generated for the following event:

Notification	Event	Contents
ELEMENTAL-MIB::alert	Any alert generated by the nodes within the cluster.	• ELEMENTAL-MIB::alertSet: 1 if the alert is being set, 0 if the alert is being cleared. • ELEMENTAL-MIB::ale rtMessage: Message describing the alert that was set or cleared.

The SNMP MIB for AWS Elemental Delta is at `http://<Delta IP>:8080/mib/ ELEMENTAL_MIB.txt`.

Perform this procedure on each node.

To set up SNMP traps

1. On the web interface for the node, choose **Settings** > **SNMP Interface**.
2. On the SNMP screen, complete the fields.

Field	Description
Allow external SNMP access	Answer **`Yes`** to open the SNMP port on the firewall. The port must be open in order to submit an SNMP walk.
Generate SNMP traps for alerts	Answer **`True`** to generate traps.

Field	Description
SNMP Management Host	List the IP address of the trap destination.
SNMP Management Trap Port	Enter **162**
SNMP Management Community	Enter **`Public`**

3. Click **Update**.

Setting Up SNMP Polling

Rather than passively receiving traps sent to you by the systems, you can actively poll the SNMP interface. Polling the AWS Elemental Delta node with an `snmpwalk` command provides you with information about all systems in the cluster.

You can interact with the AWS Elemental Delta node 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 you are logged into the system directly or over SSH. Examples in this document show the use of `net-snmp` commands.

In order to access the SNMP interface externally, either disable the firewall or enable access to just the SNMP interface. Default settings allow external access to the SNMP interface. For instructions on enabling and disabling the firewall, see Opening Ports on the Firewall. The setting for enabling access to the SNMP interface through the firewall is on the **Settings** > **SNMP** tab.

Management Information Bases (MIBs)

AWS Elemental provides the following Management Information Bases (MIBs) for use with AWS Elemental Delta clusters:

`ELEMENTAL_MIB.txt`- Base MIB for all AWS Elemental systems

Details on the MIB are provided in the subsections below. This MIB is installed on the system by default and is located in `/opt/elemental_se/web/public/mib/`.

You can use the MIBs with the `net-snmp` tools to query individual variables as shown.

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

returns

```
ELEMENTAL-MIB::serviceStatus.0 = INTEGER: 1
```

All Elemental: ELEMENTAL_MIB

All AWS Elemental systems ship with the base MIB, which can provide information on the system itself. The following table describes the variables that are available via this MIB.

Variable	Values
serviceStatus	0 if the elemental_se service is not running, 1 if the service is running.
firewallStatus	0 if the system's firewall is off, 1 if on.
networkSettings	Always returns 1. This is required for some network management systems.
mountPoints	Number of user-mounted file systems in /mnt.
version	Product version.
httpdStatus	0 if the HTTPD service is not running, 1 if the service is running.
databaseBackup	1 if writes (starting backups) are allowed, 0 if writes are not allowed.

Polling the Entire SNMP Interface

You can gather information on their events by sending an `snmpwalk` command to the AWS Elemental Delta node. This provides information on all channels running in the cluster.

The entire AWS Elemental Delta interface can be queried via `snmpwalk` as follows.

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

Creating VIPs

You can create a VIP for a common IP address for the web interface and REST API connections. When you connect via the VIP for management purposes, you go to the current leader node.

⚠ **Important**

This VIP is not used for traffic ingest or output!

Important points:

- Create VIPs for only the Ethernet devices on the ingest side. The Ethernet devices on the outgoing traffic side are configured on the load balancer, not in AWS Elemental Delta.
- You can set up the VIP for either the device itself or for the bond.

To create a VIP

1. On the web interface of the node that's intended to be the leader, choose **Nodes**.
2. On the **Nodes** screen, click **Add VIP**.
3. In the **Add New Cluster VIP** dialog, complete the fields from this table to create a VIP for eth0.

Field	Description
Ethernet Interface	eth0
IP Address	A valid IPv4 address. This address must be an address on your network that is never allocated to any other host.
Broadcast Address	This broadcast address typically matches the broadcast address on the interface to which the VIP is assigned.
Netmask	This Netmask typically matches the Netmask on the interface to which the VIP is assigned.

4. Click **Create**.

Configuring User Authentication

User authentication with AWS Elemental Delta is intended to:

- Allow managers to track activity on the cluster on a per-user basis.
- To avoid accidental access to a node, create a unique username for each operator, and vary the usernames across the clusters. For example, varying usernames for each cluster ensures that a REST API operator with access to two clusters does not accidentally send a command to the wrong cluster.

Whether user authentication is enabled or not, we recommend that the cluster always be installed behind a customer firewall on a private network.

Scope of User Authentication

When user authentication is enabled, each user of AWS Elemental Delta must be set up with credentials in order to access the following.

- The web interface: When the user goes to the web interface, a login page appears.
- The REST API: Users of the REST API must include their individual API keys when entering REST commands. Use of the key is described in the introductory sections of the AWS Elemental Delta 2.3 API Guide.

User Roles

Assign a role to each user to indicate the level of permissions assigned. The following table describes what roles are needed for each action.

Action	Roles			
	Admin	**Manager**	**Operator**	**Viewer**
View	Yes	Yes	Yes	Yes
Manage Input Filters	Yes	Yes v	Yes	No

Action	Roles			
Manage Output Filters	Yes	No	Yes	No
Manage Input Users	Yes	Yes	Yes	No
Manage Content	Yes	Yes	Yes	No
Manage Output Templates	Yes	Yes	Yes	No
Manage Alerts	Yes	Yes	Yes	No
Manage Messages	Yes	Yes	Yes	No
Manage Logs	Yes	Yes	Yes	No
Manage System Settings	Yes	Yes	Yes	No
Manage User Profile	Yes	Yes	Yes	No
Manage Nodes	Yes	Yes	Yes	No
Manage Users	Yes	No	No	No

Enabling User Authentication

Follow these steps to enable user authentication.

To enable user authentication

1. On the leader node, run the configuration script to enable user authentication.
2. If the secondary node is already running, restart the node to enable user authentication.
3. Log in to the web interface of the leader node using the administrator credentials that you created in Step 1.

4. On the leader node only, create credentials for all the users.

See the following sections for more information about these steps.

Topics

- Step A: Run the Configuration Script
- Step B: Restart the Secondary Node
- Step C: Log in to the Web Interface
- Step D: Add Users

Step A: Run the Configuration Script

Run the configuration script to enable user authentication if users are required to provide credentials to access the nodes. You must perform this procedure at the Linux command line for the leader node.

To run the configuration script

1. At your workstation, start a remote terminal session to the AWS Elemental Delta node.
2. At the Linux prompt, log in with the *elemental* user credentials.
3. Change to the folder where the configuration script is located with this command:

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

4. Run the configuration script with this command:

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

   where **-a** specifies to show only the user authentication prompts.
5. Enter **Yes** to this prompt: `Do you wish to enable authentication?`
6. The system prompts you to enter a username, email address and password for an "admin" user. Use these credentials when you log into the web interface in the next step.

Once the configuration is complete, the elemental service starts.

```
Installation and configuration complete!
```

```
. . .
Enjoy!
```

Step B: Restart the Secondary Node

If the secondary node is already running, restart it to enable authentication.

> **Important**
>
> Do *not* run the configure script on the secondary node.

To restart the node

1. Enter this command:

   ```
   [elemental@hostname ~]$ sudo reboot
   ```

2. When the reboot completes, the elemental _se service automatically starts. Look for this message on the command line:

   ```
   Starting elemental_se: [ OK ]
   ```

   If the system does not prompt you to reboot, it prompts you to start elemental_se.

   ```
   Would you like to start the Elemental service now? [Y] y
   ```

   Enter **y**.

   The service restarts.

Step C: Log in to the Web Interface

Now that you have enabled user authentication, you must log in to the web interface.

To log in to the web interface

1. On the leader AWS Elemental Delta node, display the web interface in the usual way.The login screen appears.

2. Log into the web interface using the “admin” credentials you created via the configure script.

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

Step D: Add Users

To add users, perform this procedure on the leader AWS Elemental Delta node.

To add users

1. Make sure you are logged into the web interface as the *admin* user you created via the configuration script.
2. In the menu bar, click the *admin* name and choose **Manage Users**.
3. On the **Manage Users** screen, click **Add User**.
4. In the **Add New User** dialog, complete all fields and click **Save**.
5. Notify users of the following:

   - That they must provide a username and password.
   - That they can manage their profiles; see User Self-Management .

Disabling User Authentication

If you no longer require users to provide credentials to access the cluster, you can disable user authentication.

To disable user authentication

1. To disable user authentication on the entire cluster, run the configuration script again, as described in Enabling User Authentication.
2. This prompt appears: `Do you wish to enable authentication?`

   Enter **Yes**.

User Self-Management

Users you have set up can view their capabilities and obtain their API key.

Instruct users to log into the web interface and click their name in the menu bar, then click **Profile** on the drop- down menu. In their profile, they can reset the password and update the contact email address.

Document History for Configuration Guide

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

- **API version:** 2.3
- **Release notes:** AWS Elemental Delta Release Notes

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

Change	Description	Date
Guide format conversion	This guide has been converted for HTML delivery.	January 2, 2020