Eucalyptus 4.1.2 Management Console Guide

2016-01-26 Eucalyptus Systems

Contents

Management Console Overview

Welcome to the Eucalyptus Management Console Guide. The Eucalyptus Management Console is an easy to use web-based interface that allows you to manage your Eucalyptus cloud.

You can do many things with the Eucalyptus Management Console, including:

- Get a high-level overview of your cloud with the dashboard
- Create, manage, and delete instances
- Create volumes and snapshots
- Create and import key pairs
- Create and manage security groups
- Create and manage Auto Scaling groups
- Create and manage Elastic Load Balancers
- Manage your Amazon Web Services cloud
- Create and manage IAM users and groups
- Work with Elastic IP addresses

What's In This Guide

This guide contains information on how to install and configure the Eucalyptus Management Console, as well as a section on how to navigate and use the screens and dialogs contained in the management console:

Section	Description
Installing the Eucalyptus Management Console	Contains instructions on how to install the Eucalyptus Management Console.
Configuring the Eucalyptus Management Console	Describes how to locate and configure the console configuration file, as well as each setting in the configuration file.
Working with the Eucalyptus Management Console	Discusses how to get started using the Eucalyptus Management Console and how to navigate and use the screens and dialog boxes in the console.

Document version: Build 3029 (2016-01-26 12:00:31)

Install the Eucalyptus Management Console

This section covers how to install the Eucalyptus Management Console.

Install on Centos / RHEL 6.6

Note: The Eucalyptus Management Console package is installed with the Eucalyptus repositories. The following instruction assumes that you're installing the console on a server that's already running Eucalyptus. If you're installing the console on a stand-alone machine, please see the *Eucalyptus Installation Guide* to set up the Eucalyptus repositories before following the instructions below.

Note: The version of the management console you're running should be the same as the version of Eucalyptus you're running. Running a management console against a Eucalyptus installation with a different version is unsupported.

Note: The Eucalyptus Management Console package will only install on 64-bit architectures.

To install the Eucalyptus Console from packages on Centos and RHEL 6.6:

Run the following command to install the Eucalyptus Management Console:

```
yum install eucaconsole
```

Your installation is now complete.

You are now ready to *configure the Eucalyptus Management Console*.

Configure the Eucalyptus Management Console

This section covers how to configure the Eucalyptus Console.

Things You Need to Do to Get the Console Running

In order to get the console working for your cloud, you will need to do the following:

- Modify the configuration file, as detailed in this section. At minimum, you must specify the *front end address*, and the *UI port*. You should also be sure to specify the *administrative support URL* and the *support URL*.
- Configure Memcached. This is required for the eucaconsole service to use memcached on a single host.
- Create the user accounts using the Eucalyptus Administrative Console. For more information see the *Administration Guide*.
- Make sure that any images that you would like users to be able to launch instances from are installed in your cloud; users can't add images from the Eucalyptus Console.
- Communicate the URL for your Eucalyptus Console installation to the users, and instruct them to use their account name, user name, and password to log in.

Locate and Edit the Console Configuration File

The Eucalyptus Console configuration settings are stored in the `console.ini` file.

For Centos and RHEL installations from packages, this file is located in `/etc/eucaconsole/console.ini`.

The configurable options in the `[app:main]` section of the console.ini file are:

Note: The Default Values column denote the default value for a property that is not required, if applicable.

Property	Description	Required	Default Value
clchost	The IP address or DNS name of the machine running User-Facing Services (UFS), which can be different from the machine running the CLC. UFS can be running on several different hosts, and in that case, they must be specified with separate variables. For S3 downloads to work, you may set this to `localhost` only if `s3.host` is set to the IP or DNS name. Otherwise, the name for `clchost` needs to be resolvable by clients, so an IP or DNS name is preferred.	yes	--
clcport	The port of your cloud front end.	yes	8773

Property	Description	Required	Default Value
ec2.host	The IP address or DNS name of your ec2 service endpoint, if different than clchost.	no	--
ec2.port	The port of your ec2 service port, if different than clcport.	no	--
autoscale.host	The IP address or DNS name of your autoscale service endpoint, if different than clchost.	no	--
autoscale.port	The port of your autoscale service port, if different than clcport.	no	--
cloudwatch.host	The IP address or DNS name of your cloudwatch service endpoint, if different than clchost.	no	--
cloudwatch.port	The port of your cloudwatch service port, if different than clcport.	no	--
elb.host	The IP address or DNS name of your elb service endpoint, if different than clchost.	no	--
elb.port	The port of your elb service port, if different than clcport.	no	--
iam.host	The IP address or DNS name of your iam service endpoint, if different than clchost.	no	--
iam.port	The port of your IAM service port, if different than clcport.	no	--
sts.host	The IP address or DNS name of your STS service endpoint, if different than clchost.	no	--
sts.port	The port of your STS service port, if different than clcport.	no	--
s3.host	The IP address or DNS name of your S3 service endpoint, if different than clchost.	no	--
s3.port	The port of your S3 service port, if different than clcport.	no	--

Property	Description	Required	Default Value
help.url	A url that directs users who select 'help' on the account menu to a help page. You can customize for your installation if you do not want our help system.	yes	--
support.url	A URL given to users who have trouble logging in. It may be used to direct them to a cloud admin page or an e-mail address.	yes	--
aws.enabled	When set to `true`, the AWS tab displays on the login screen.	yes	true
aws.default.region	The name of the region to show by default when the user logs into AWS. Use any value from the **Region** column recognized by AWS: http://docs.aws.amazon.com/general/latest/gr/rande.html#ec2_region	yes	us-east-1
static.cache.duration	Sets the cache control value for static assets (in seconds).	no	43200 secs
browser.password.save	Set to `true` to enable browser password saving.	no	true
file.uploads.enabled	Defaults to `true` to enable file uploads for S3/Object Storage.	no	true
connection.ssl.validation	Set to `true` to enable validation of the SSL certificate supplied by the clchost (or other endpoint) to secure the connection to the service endpoint.	no	false
connection.ssl.certfile	If certificate validation is on, you may specify a different certificate file than the default.	no	--
connection.debug	Set to `true` to enable very detailed information about communication between the console server and service endpoints. Logs will become cluttered, so do not leave this on under normal operation.	yes	false

Property	Description	Required	Default Value
connection.retries	Sets the number of retires used when issuing requests to service endpoints. Adjusting this higher may reduce UI responsiveness.	no	2
pyramid.default_locale_name	The default locale if none is specified by browser.	no	en
session.keyini	The location of a file that contains session encryption keys.	yes	--
session.secure	Set to `true` to send session cookies over a secure connection only. Needs to be set to `false` if SSL not configured.	no	false
session.timeout	Sets the idle session timeout.	yes	--
session.cookie_expires	Sets the absolute session timeout.	yes	--
cache.username	Sets a username to be used when SASL authentication is enabled for memcached. If not set, the memcached connection is unauthenticated.	no	--
cache.password	Sets a password to be used when SASL authentication is enabled for memcached. If not set, the memcached connection is unauthenticated.	no	--

The configurable options in the `[server:main]` section of the console.ini file are:

Note: The Default Values column denote the default value for a property that is not required, if applicable.

Property	Description	Required	Default Value
host	Set to `0.0.0.0` to allow connections from any host. Set to `127.0.0.1` to allow connections from localhost only, which is preferred if running nginx.	yes	0.0.0.0
port	The port on which the console can be reached.	yes	8888

Property	Description	Required	Default Value
workers	The number of worker processes used to service requests. A rule of thumb is double the number of cores plus one.	yes	--
tmp_upload_dir	Specifies a different directory to be used for file uploads, if set. It should have plenty of space to handle large file uploads. Defaults to the system's temp directory.	no	--

Note:

You should always start (or restart) the console when you make changes to the console configuration.

You can start the console using the following command:

```
service eucaconsole start
```

You can restart the console using the following command:

```
service eucaconsole restart
```

Configure Memcached

Configuring memcached is required for the eucaconsole service to use memcached on a single host. The configuration provided instructs the memcached service to only accept connections from localhost. If you wish to run multiple eucaconsoles on separate hosts, you should set up a common memcached instance that accepts connections from those hosts.

Note: This procedure assumes that the Eucalyptus Management Console package is installed. For instructions on installing the packages, see the *Installing the Eucalyptus Management Console* section.

Note: If there is just one Console server, we recommend co-locating memcached on that server for optimum speed. Since memcached isn't critical to the functioning of the Console, a single memcached instance would suffice. If memcached were to go down, replacing it with another instance is adequate.

1. Run the following command to install memcached:

```
yum install -y memcached
```

2. Copy Eucalyptus' default configuration file with the following command:

```
cp /usr/share/doc/eucaconsole-4.1.0/memcached /etc
```

3. Configure the service to start automatically using the following command:

```
chkconfig memcached on
```

4. Launch the service to start immediately using the following command:

```
service memcached start
```

Flush Memcached in the Console

Changing the clchost could cause the image cache to not properly refresh in the Launch Instance and Create Launch Configuration wizards, which prevents the launching of instances and creating launch configurations. Clearing (flushing) memcached in the Console will refresh the cache to properly resume operations.

To flush memcache without restarting the server:

1. Telnet to the localhost on which the Console is running:

```
telnet localhost
```

2. Run the flush command:

```
flush_all
```

Note: Alternatively, if you change the console.ini file while installing the Console, you could restart memcached using the `service memcached restart` command instead.

Configure Account Credentials

Accounts that log in to the management console must have a password and access credentials assigned.

Note: You can find instructions to do this with the administrative console in the *Eucalyptus Administration Guide*.

To create a user account using the euare command line tools:

1. Create a user account using the `euare-accountcreate` command line tool. For example:

```
euare-accountcreate -a exampleaccount
```

2. Create a password for the newly created account by adding a login profile using the `euare-useraddloginprofile` command line tool. For example:

```
euare-useraddloginprofile --as-account exampleaccount -u admin -p
examplepassword
```

Set the Cloud Front End IP Address

To set the IP address or DNS name of your cloud front end:

Modify the `clchost` entry in the `[app:main]` section of the configuration file. For example:

```
clchost=127.0.0.1
```

Configure the UI Port

To set the port that the console will listen on:

Modify the `port` entry in the `[server:main]` section of the configuration file. For example:

```
port=8888
```

Configure the Management Console on nginx

Enable SSL for the Management Console

You can use secure HTTP for your console to allow secure connections from a web server to a browser.

To run your console over Secure HTTP:

1. Install nginx on your console server with the following command:

```
yum install nginx
```

2. Overwrite the default `nginx.conf` file with the template provided in `/usr/share/doc/eucaconsole-4.1.2/nginx.conf`.
3. Uncomment the 'listen' directive and uncomment/modify the SSL certificate paths in `/etc/nginx/nginx.conf` (search for "SSL configuration"). For example:

```
# SSL configuration
# SSL configuration
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
listen 443 ssl;
ssl_certificate <path to euca console cert file>;
#EXAMPLE:
#ssl_certificate /etc/eucaconsole/console.crt;
ssl_certificate_key <path to euca console key file>;
#EXAMPLE:
#ssl_certificate_key /etc/eucaconsole/console.key;

# end of SSL configuration
```

Tip: For more information on generating self-signed SSL certificates, go to *http://www.akadia.com/services/ssh_test_certificate.html*.

4. Restart nginx using the following command:

```
service nginx restart
```

5. Edit the `/etc/eucaconsole/console.ini` file:
   a) Locate the `session.secure =` parameter and change its value from `false` to `true`, per this example:

```
session.secure = true
```

Note: If HTTPS is used, meaning nginx is configured to use port 443, the `session.secure` setting must equal `true`.

   b) Locate the `[server:main]` section. If the host setting under `[server:main]` is set to `0.0.0.0`, connections are accepted from anywhere. If the UI proxy is used behind nginx on the same host, you can configure the proxy to listen on localhost only, by setting it to `127.0.0.1`, per this example:

```
[server:main]
use = egg:gunicorn#main
host = 127.0.0.1
port = 8888
```

Enable the Console to Run on Port 80

You can run the console on non-secure connections using HTTP. In order to configure the console without enabling secure connections, use port 80 instead. To accomplish this, nginx will have to be used as a proxy.

To run your console on port 80:

1. Install nginx on your console server with the following command:

```
yum install nginx
```

2. Locate the default configuration file from `conf/nginx.conf`.
3. Verify the `nginx.conf` file contains the following lines:

```
listen 80;
server_name  localhost;
```

4. If the file does not specify port 80 on the 'listen' directive, change it to reflect the above.
5. Restart nginx using the following command:

```
service nginx restart
```

6. Verify the `/etc/eucaconsole/console.ini` has the `session.secure =` parameter set to `false`, per this example:

```
session.secure = false
```

Note: If only port 80 is used (i.e. HTTPS isn't configured via port 443), the `session.secure` setting must equal `false`.

7. Locate the `[server:main]` section. If the host setting under `[server:main]`is set to `0.0.0.0`, connections are accepted from anywhere. If the UI proxy is used behind nginx on the same host, you can configure the proxy to listen on localhost only, by setting it to `127.0.0.1`, per this example:

```
[server:main]
use = egg:gunicorn#main
host = 127.0.0.1
port = 8888
```

Set the Administrator Support URL

To set administrator URL or email address displayed in the console:

Modify the `support.url` entry in the `[app:main]` section of the configuration file. For example:

```
support.url=mailto:help@example.com
```

...or...

```
support.url=http://you-cloud.example.com/support
```

Set the Locale

To optionally set the default locale that you want the console to use for localization:

Modify the `pyramid.default_locale_name` entry in the `[app:main]` section of the configuration file with a Linux-compliant locale name. For example:

```
pyramid.default_locale_name = en
```

Set the Help Page URL

To configure the help page URL for the console:

Modify the `help.url` entry in the `[app:main]` section of the configuration file. For example:

```
help.url=https://example.com/help-me
```

This URL will open when the console user selects the **Help** menu item from the console dashboard.

Configure Session Timeouts

To set the session timeouts in the Management Console:

Modify the `session.timeout` and `session.cookie_expires`entries in the `[app:main]` section of the configuration file. The `session.timeout` value defines the number of seconds before an idle session is timed out. The `session.cookie_expires` is the maximum length that any session can be active before being timed out. All values are in seconds:

```
session.timeout=1800
```

```
session.cookie_expires=43200
```

Configure Workers

To set the number of worker processes used by the console:

In the `[server:main]` section of the configuration file, modify the `workers` setting. For example:

```
workers=9
```

Note: As a general rule, you should configure the number of workers to be twice the number of CPU cores, plus one. For more information, see the *Gunicorn documentation*.

Enable AWS Login

You can enable or disable Amazon Web Services (AWS) login with the Eucalyptus Management Console.

To enable or disable AWS login:

Modify the `aws.enabled` entry in the `[app:main]` section of the configuration file with `True` to enable AWS login or `False` to disable AWS login. For example:

```
aws.enabled=True
```

Work with the Eucalyptus Management Console

This section covers how to navigate and use the various screens and dialogs in the Eucalyptus Management Console.

Get Started with the Eucalyptus Management Console

This section covers how to connect to the console, login, and use the main navigation screen.

Browser Support

As of this writing, the Eucalyptus Management Console has been tested to support the latest stable releases of:

- Google Chrome
- Apple Safari
- Mozilla Firefox
- Microsoft Internet Explorer 10 or later

Other browsers that are not listed here may work; the list above only represents browsers that have been tested and confirmed to work with the Eucalyptus Management Console.

Console Login

This screen allows you to log in to the Eucalyptus Management Console with either your Eucalyptus or your Amazon Web Services account. If you've forgotten your password, don't have login credentials, or do not know the URL for the Eucalyptus Management Console for your Eucalyptus account, please contact your system administrator.

1. Navigate to the Eucalyptus Management Console by typing the URL of the Management Console into your browser's navigation bar. The URL of the Eucalyptus Management Console depends on how the console was installed in your cloud; see your system administrator for the specific URL for your installation.
2. Follow the appropriate instructions below for logging into either your Eucalyptus or your Amazon Web Services cloud.

Log in to your Eucalyptus cloud

This area of the login dialog allows you to log in to your Eucalyptus cloud.

1. Click the **Log in to Eucalyptus** tab.
2. Type your account name into the **Account name** text box.
3. Type your user name into the **User name** text box.
4. Type your password into the **Password** text box.
5. Click the **Log in to Eucalyptus** button.

Log in to your Amazon Web Services cloud

This area of the login dialog allows you to log in to your Amazon Web Services cloud.

1. Click the **Log in to AWS** tab.
2.  **Note:** To obtain your AWS security credentials, go to Amazon's *Your Security Credentials* page.

   Enter your AWS access key ID into the **Access key ID** text box.
3. Enter your AWS secret access key into the **Secret access key** text box.
4. Click the **Log in to AWS** button.

Navigate the Dashboard

The dashboard is your starting point for using the Eucalyptus console. From the Dashboard, you can access landing pages for instances, scaling groups, storage items (volumes, and snapshots), IAM users and groups, and networking and security objects (key pairs, security groups, and IP addresses).

Basic Dashboard Navigation

You can navigate to specific resource management dialogs in two ways: using the navigation icons at the top of the screen or clicking directly on a resource label or count in the Dashboard screen.

1. You can click directly on a resource name at the top of the main console page to navigate directly to a resource management screen or back to the main console screen.
2. You can also navigate to a resource management screen by clicking directly on a resource icon or count in the main dashboard window.
3. The dashboard shows resources in all availability zones by default. You can filter by availability zone by selecting an availability zone from the **Availability Zones** drop-down listbox at the top of the page.

Instances

The dashboard allows you to see how many instances are running and to access the **Instances** screen.

1. Click the **Running Instances** or **Stopped Instances** icon in the dashboard to display the **Manage Instances** screen.
2. You can launch a new instance by clicking the **Launch instance** button at the top of the page to display the **Launch new instance** wizard.

Scaling Groups

The **Instances in Scaling Groups** icon allows you to access the **Scaling groups** screen.

1. Click the **In Scaling Groups** icon to display the **Scaling Groups** screen.
2. You can create a new scaling group by clicking the **Create scaling group** link beneath the **In Scaling Groups** icon.

Storage

The **Volumes** and **Snapshots** icons allow you to see at a glance how many storage objects are running and directly access the storage object management screens.

1. To access the **Volumes** screen, click the **Volumes** icon.

   You can create a new volume by clicking the **Create volume** link beneath the **Volumes** icon.
2. To access the **Snapshots** screen, click the **Snapshots** icon.

   You can create a new snapshot by clicking the **Create snapshot** link beneath the **Snapshot** icon.

Network and Security

The dashboard allows you to see at a glance the number of security groups, key pairs, and elastic IP addresses in your Eucalyptus cloud, and to navigate to management screens for each type of object.

1. To access the **Security Groups** screen, click the **Security Groups** icon.

   You can create a new security group by clicking the **Create security group** link beneath the **Security Groups** icon.
2. To access the **Key Pairs** screen, click the **Key Pairs** icon.

   You can create a new key pair by clicking the **Create key pair** link beneath the **Key Pairs** icon.
3. To access the **Elastic IPs** screen, click the **Elastic IPs** icon.

   You can create a new elastic IP address by clicking the **Allocate elastic IPs** link beneath the **Elastic IPs** icon.

Miscellaneous Console Functions

Clicking on your account ID in the upper-right corner of the console window displays a drop-down menu showing options to change your password, get help from the Eucalyptus Engage web site, get information about your cloud, and log out of the console.

1. To get help from the Eucalyptus support web site, select **Help** from the drop-down menu.

2. To change your password, select **Change password** from the drop-down menu.

   Note: You can only change your Eucalyptus cloud password using the Eucalyptus console. To change your AWS password, use the *AWS Security Credentials page*.

3. To show a dialog box with information about your cloud, click **About your cloud** from the drop-down menu.
4. To log out of the Eucalyptus console, select **Log out** from the drop-down menu.
5. When logged into your AWS account, you can change your region by clicking on the drop-down menu next to the account menu in the upper right corner of the dashboard page. The Eucalyptus console will remember your last selected region.

Manage Credentials

This page allows you to change your user account password and generate a new set of access keys.

Change your password

1. Type your current password into the **Current password** text box.
2. Type your new password into the **New password** text box.
3. Type your new password into the **Confirm new password** text box to ensure that you have typed the new password correctly.
4. Click the **Change Password** button to save your changes.

Generate access keys

This option generates a new set of access keys for you and makes them active.

1. Click the **Create Access Keys** button.

   Important: As a security measure, contact your cloud administrator to remove any old keys you are no longer using or have exceeded the maximum of two access keys allowed.

   Once generated, the access key and the secret access key display below the Access keys heading.
2. You can copy and paste the keys to a file or click the **Download These Keys** button to download the file to your local drive.

   Important: Either method you choose to save your keys, be sure to keep them in a safe place, as they are not stored for you in the cloud.

Work with Key Pairs

This section covers how to navigate and use the key pair screens and dialogs in the Eucalyptus Management Console.

Manage Key Pairs

This screen allows you to view a list of your key pairs, create new key pairs, and delete key pairs. You can page through the list of key pairs by clicking the navigation buttons at the bottom of the screen.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Key Pairs List

Sort the key pairs list by selecting a sort order using the **Sort by** drop-down list box.

Searching and Filtering the Key Pairs List

To perform a simple search/filter, type some search text into the search text box at the top right of the page.

Creating a Key Pair

Click the **Create New Key Pair** button. The **Create new key pair** page will appear.

Importing Key Pairs

Click the **Import Public Key** button. The **Import key pair** page will appear.

Actions

Each entry in the key pairs list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected image.

The following context menu actions are available:

Delete key

This item will bring up the key pair delete confirmation dialog box.

Create a Key Pair

Eucalyptus uses cryptographic key pairs to verify access to instances. Before you can run an instance, you must create a key pair. Creating a key pair generates two keys: a public key (saved within Eucalyptus) and a corresponding private key (output to the user as a character string). To enable this private key you must save it to a file and set appropriate access permissions (using the chmod command), as shown in the example below.

Create Key Pairs with the Console

1. From the main dashboard screen, click the **Key Pairs** icon, or select the **Network and Security** menu at the top of the dashboard. The **Manage Keypairs** screen will appear.
2. On the **Key Pairs** screen, click the **Create New Key Pair** link. The **Create new key pair** page will appear.
3. Type a name for the new key pair into the **Name** text box.
4. Click the **Create and Download** button. The private half of the key pair is saved to the default download location for your browser.

   

   Note: Keep your private key file in a safe place. If you lose it, you will be unable to access instances created with the key pair.

5. Change file permissions to enable access to the private key file in the local directory. For example, on a Linux or Mac OS X system:

```
chmod 0600 <keypair_name>.private
```

Import a Public Key

This page allows you import an existing public key. Use this if you have an existing SSH key on your system you want to use with your Eucalyptus instances.

1. Enter a name for the key pair in the **Name** text box.
2. Paste the contents of your SSH key into the **SSH key contents** text box, or click on the **Browse...** link to read the contents of an existing SSH key file.
3. Click the **Import** button.

Delete Key Pair

This dialog box allows you to confirm or cancel a key pair delete operation.

Verify Key Pair Deletion

1. To verify that you wish to delete the selected key pair(s), click the **Yes, Delete** button.
2. To cancel the delete operation, click the **x** button in the upper right corner of the dialog box.

Work with Security Groups

This section covers how to navigate and use the security group screens and dialogs in the Eucalyptus Management Console.

Manage Security Groups

This screen allows you to view a list of your security groups and create, modify and delete security groups. You can page through the list of security groups by clicking the navigation buttons at the bottom of the screen.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Security Groups List

Sort the security groups list by selecting a sort order using the **Sort by** drop-down list box.

Searching and Filtering the Security Groups List

1. To perform a simple search/filter, type some search text into the search text box at the top right of the page.
2. For more precise filtering and searching, you can add one or more filters by clicking one of the available filters in the **Filter by** section on the right side of the page.

Creating a Security Group

Click the **Create New Security Group** button. The **Create Security Group** page will appear.

Viewing Details of a Security Group

You can expand a security group in the list to see details about the security group, including tags and rules associated with the security group.

Click the name of the security group in the list of security groups.

The details page for the selected security group will open.

Actions

Each entry in the security group list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected security group.

The following context menu actions are available:

View details

This item will bring up the security group detail page.

Delete security group

This item allows you to delete the security group.

Create a Security Group

Eucalyptus enables you to control access to your cloud using security groups. A security group contains a group of rules that control inbound and outbound traffic to instances in the group for the specified protocols and ports.

Security Group section

1. Enter a name for your security group in the **Name** text box.
2. Enter a description for your security group in the **Description** text box.
3. Select a Virtual Private Cloud (VPC) network from the drop-down menu.

Rules section

You can optionally create one or more rules for the security group. A *rule* grants a specified range of IP addresses access (inbound to or outbound from) your instances for a protocol or custom port range. Rules for many of the most popular protocols are pre-defined and available for selection in the drop-down list box, or you can define your own rule.

1. Select Inbound to set the rules for inbound access or select Outbound to set the rules for outbound access.

   Note: The Outbound option is not available if *No VPC* was selected for VPC network.

   Important: You should specify at least one rule for your security group.

2. Select a protocol for the rule from the **Protocol** drop-down list box, or select a custom protocol. If a custom protocol is selected:
   a) for TCP or UDP, enter a port range for the rule in the **Port range** text box.
   b) for ICMP, associate an ICMP type by selecting it from the drop-down list box.
   c) Identify the type of traffic to allow by selecting one of the following options:
      - To grant access to an IP address or range of IP addresses, select the **IP Address** radio button and enter a CIDR range in the text box.

        Note: For more information on CIDR notation, please see the *CIDR notation Wikipedia article*.

      - To grant access to all IP addresses, click **Open to all addresses**. This sets the value to 0.0.0.0/0
      - To grant access to only your computer, click **Use my IP address**.
      - To grant access to a security group, select the **Security group** radio button and select a group from the drop-down list box or enter the name of the security group in the text box.

        Note: To specify a security group in another account, use the format `accountid/groupname`.

   d) Click the **Add Rule** button when done.
      The newly added rule displays above the rule form.
3. Repeat as needed to add more rules.
   A list of added rules display above the rule form to indicate they have been successfully added.

Add tags

To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to resources in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. You can optionally add tags by performing the following steps:

To add new tags:

1. Type the key name for your tag into the **name...** text box.

   Note: Tags cannot start with "`euca:`" or "`aws:`".

2. Type the value for your tag into the **value...** text box.
3. Click the **Add Tag** button.
4. If you wish to add additional tags, repeat the preceding steps.

To delete one or more tags:

Move your mouse over the tag you wish to delete and click the **X** button.

Save Your Work

Click the **Create Security Group** button to save your work, or click the **Cancel** button to cancel the operation.

Security Group Details

This page allows you to view details, add/edit rules, or delete a security group.

Add Security Group Rules

You can optionally create one or more rules for the security group. A rule grants a specified range of IP addresses access to and from your instances for a protocol or custom port range. Rules for many of the most popular protocols are pre-defined and available for selection in the drop-down list box, or you can define your own rule.

1. Select Inbound to add the rules for inbound access or select Outbound to add the rules for outbound access.

   

   Note: The Outbound option is not available if *No VPC* was selected for VPC network.

   

   Important: You should specify at least one rule for your security group.

2. Select a protocol for the rule from the **Protocol** drop-down list box, or select a custom protocol. If a custom protocol is selected:
   a) for TCP or UDP, enter a port range for the rule in the **Port range** text box.
   b) for ICMP, associate an ICMP type by selecting it from the drop-down list box.
   c) Identify the type of traffic to allow by selecting one of the following options:

   - To grant access to an IP address or range of IP addresses, select the **IP Address** radio button and enter a CIDR range in the text box.

     

     Note: For more information on CIDR notation, please see the *CIDR notation Wikipedia article*.

   - To grant access to all IP addresses, click **Open to all addresses**. This sets the value to 0.0.0.0/0
   - To grant access to only your computer, click **Use my IP address**.
   - To grant access to a security group, select the **Security group** radio button and select a group from the drop-down list box or enter the name of the security group in the text box.

     

     Note: To specify a security group in another account, use the format `accountid/groupname`.

   d) Click the **Add Rule** button when done.
   The newly added rule displays above the rule form.

3. Repeat as needed to add more rules.
   A list of added rules display above the rule form to indicate they have been successfully added.

Delete Security Group Rules

Click the **X** on the existing rule you want to delete.

Add tags

To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to resources in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. You can optionally add tags by performing the following steps:

To add new tags:

1. Type the key name for your tag into the **name...** text box.

   

   Note: Tags cannot start with "`euca:`" or "`aws:`".

2. Type the value for your tag into the **value...** text box.
3. Click the **Add Tag** button.
4. If you wish to add additional tags, repeat the preceding steps.

To delete one or more tags:

Move your mouse over the tag you wish to delete and click the **X** button.

Saving Your Changes

Once you're satisfied with the edits to your security group, click the **Save changes** button.

Actions

Clicking the **Actions** button brings up a menu of actions that you can perform on the selected security group.

The following context menu actions are available:

Delete security group

Selecting this item will display the delete security group confirmation dialog box.

Delete Security Group

This dialog box allows you to confirm or cancel a security group delete operation.

Verify Security Group Deletion

1. To verify that you wish to delete the selected security group(s), click the **Yes, Delete** button.
2. To cancel the delete operation, click the **X** button in the upper right corner of the confirmation dialog box.

Work with Volumes

This section covers how to navigate and use the volume screens and dialogs in the Eucalyptus Management Console.

Manage Volumes

Eucalyptus offers persistent storage that you can attach to a running instance. These Eucalyptus block storage (EBS) volumes persist autonomously from the running life of an instance. After you attach a block volume to an instance, you can use it like any other physical hard drive. This screen allows you to view a list of your volumes, create new volumes, attach and detach volumes to a running instance, and delete volumes. You can page through the list of volumes by clicking the navigation buttons at the bottom of the screen.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Volumes List

Sort the volumes list by selecting a sort order using the **Sort by** drop-down list box.

Searching and Filtering the Volumes List

1. To perform a simple search/filter, type some search text into the search text box at the top right of the page.
2. For more precise filtering and searching, you can add one or more filters by clicking one of the available filters in the **Filter by** section on the right side of the page.

Creating a Volume

Click the **Create New Volume** button. The **Create new volume** page will appear.

Viewing Details of a Volume

Several items in the volume list allow you to click on them to see more detailed information.

To see more details about a volume, or an object associated with an image:

1. Click the name/ID in the list of volumes to display detailed information about the selected volume.
2. Click an instance ID to see to see detailed information about the instance associated with the selected volume.

3. Click the number of snapshots to see a detailed list of all of the snapshots associated with the selected volume.

Actions

Each entry in the image list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected image.

The following context menu actions are available:

View details

This item will bring up the volume detail page.

Manage snapshots

This item brings up a page that allows you to view, add, and delete snapshots for a volume.

Attach to instance

This item allows you to attach the volume to a running instance.

Note: This menu item will not appear if the volume is already attached to an instance.

Detach a Volume from a Running Instance

This item allows you to detach the volume from a running instance.

Note: This menu item will not appear if the volume is not attached to an instance.

Deleting Volumes

This item allows you to delete a volume.

Note: This menu item will not appear if the volume is attached to an instance.

Create a Volume

Eucalyptus offers persistent storage that you can attach to a running instance. These Eucalyptus block storage (EBS) volumes persist autonomously from the running life of an instance. After you attach a block volume to an instance, you can use it like any other physical hard drive.

Enter volume information

Add the details of your new volume:

1. Type the name of your volume in the **Name** text box.
2. If you would like to create a volume from an existing snapshot, select the snapshot from the **Create from snapshot?** drop-down listbox.
3. Enter the size of the volume in gigabytes in the **Volume size (GB)** text box.

Note: If you're creating a volume from a snapshot, you can't enter a volume size that's smaller than the original snapshot you've selected.

4. Select an availability zone from the **Availability zone** drop-down list box.

Note: You can only attach a volume to an instance in the same availability zone.

Add tags

To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to resources in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. You can optionally add tags by performing the following steps:

To add new tags:

1. Type the key name for your tag into the **name...** text box.

   

   Note: Tags cannot start with "`euca:`" or "`aws:`".

2. Type the value for your tag into the **value...** text box.
3. Click the **Add Tag** button.
4. If you wish to add additional tags, repeat the preceding steps.

To delete one or more tags:

Move your mouse over the tag you wish to delete and click the **X** button.

Save Your Work

Click the **Create volume** button to save your work, or click the **Cancel** button to cancel the operation.

Volume Detail - General

This page shows you the details for a volume.

General

This section allows you to view general details about the volume, rename the volume, and add tags.

Rename the volume

Type the new name of the volume in the **Name** text field.

Add tags

To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to resources in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. You can optionally add tags by performing the following steps:

To add new tags:

1. Type the key name for your tag into the **name...** text box.

   

   Note: Tags cannot start with "`euca:`" or "`aws:`".

2. Type the value for your tag into the **value...** text box.
3. Click the **Add Tag** button.
4. If you wish to add additional tags, repeat the preceding steps.

To delete one or more tags:

Move your mouse over the tag you wish to delete and click the **X** button.

Saving Your Changes

Once you're satisfied with the edits to your volume, click the **Save changes** button.

Action menu

Clicking the **Actions** button brings up a menu of actions that you can perform on the selected volume.

The following context menu actions are available:

Attach to instance

This item allows you to attach the volume to a running instance.

Note: This menu item will not appear if the volume is already attached to an instance.

Detach from instance

This item allows you to detach the volume from a running instance.

Note: This menu item will not appear if the volume is not attached to an instance.

Deleting Volumes

This item allows you to delete a volume.

Note: This menu item will not appear if the volume is attached to an instance.

Volume Detail - Snapshots

This page shows you the details for a volume's snapshots.

Snapshots

This section allows you to view and manage snapshots associated with the volume.

Create a new snapshot

Click the **Create a snapshot** icon to display the **Create snapshot from volume** dialog.

Context menu actions

Each tile in the snapshots list has a context menu. Clicking the action icon in the upper right corner of a volume tile brings up a menu of actions that you can perform on the selected snapshot.

The following context menu actions are available:

View details

This item will bring up the snapshot detail page.

Register as image

This item allows you to register the selected snapshot as an image in your cloud, if it was created from a volume containing a root file system. The image can then be used to launch EBS-backed instances.

Delete snapshot

This item allows you to delete a snapshot.

Delete Volume

This dialog box allows you to confirm or cancel a volume delete operation.

Verify Volume Deletion

1. To verify that you wish to delete the selected volume(s), click the **Yes, Delete** button.
2. To cancel the delete operation, click the **X** button in the upper right corner.

Attach a Volume

This dialog box lets you attach an EBS volume to an instance running in the same availability zone.

1. Start typing the identifier of the volume to attach into the **Volume** text box (the volume is already in the text box if you navigated to this dialog from the **Manage Volumes** screen). A list of matching volumes will appear; select the volume from the list.
2. Start typing the instance identifier into the **Instance** text box (this instance is pre-selected for you if you navigated to this dialog from the **Manage Instances** screen). A list of matching instances will appear; select the instance from the list.
3. To optionally specify a device name to use for the attached volume, type the device name into the **Attach as device** text box.

4. Click the **Attach Volume** button.

Detach Volumes

This dialog box lets you verify that you wish to detach one or more volumes from running instance(s).

1. Verify that you want to detach the listed volume(s).
2. Click the **Yes, Detach Volume** button.

Work with Instances

This section covers how to work with the instance dialogs and screens in the Eucalyptus Management Console.

Manage Instances

This page allows you to view a list of your instances, create new instances, and perform actions on your instances. You can page through the list of instances by clicking the navigation buttons at the bottom of the screen.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Instances List

Sort the instance list by selecting a sort order using the **Sort by** drop-down list box.

Searching and Filtering the Instance List

1. To perform a simple search/filter, type some search text into the search text box at the top right of the page.
2. For more precise filtering and searching, you can add one or more filters by clicking one of the available filters in the **Filter by** section on the right side of the page.

Launch an Instance

Click the **Launch new instance** button. The **Launch Instance** wizard will appear.

Viewing Details of an Instance

Several items in the instance list allow you to click on them to see more detailed information.

To see more details about an instance, or an object associated with an instance:

1. Click the name/ID in the list of instances to display detailed information about the selected instance.
2. Click an image ID to see to see detailed information about the image used to launch the selected instance.
3. Click a key name to see detailed information about the security key used to launch the instance.
4. Click a security group name to see detailed information about the security group used to launch the instance.

Actions

Each entry in the instance list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected instance.

The following context menu actions are available:

View details

This item will bring up the instance detail page.

Connect to instance

Selecting this menu will display a dialog with instructions detailing how to connect to the selected instance.

Launch more like this

Selecting this menu will display a dialog that allows you to create and customize one or more instances like the selected instance.

Create launch configuration

A launch configuration is used to define the parameters for new instances that are launched as part of your auto scaling group. Selecting this menu displays the **Create new launch configuration** wizard.

Note: For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

View console output

Selecting this menu will display a dialog box showing the selected instance's console output.

Manage volumes

This menu item allows you to show the volume management page that will allow you to attach and detach volumes for the selected instance.

Associate IP address

Select **Associate IP address** from the **Actions** menu to associate an elastic IP address with the selected instance.

Stop

Select this item to stop the selected EBS-backed instance.

Start

Select this item to start the selected EBS-backed instance.

Reboot

Select this item to reboot the selected EBS-backed instance.

Terminate

Select this to terminate the selected instance.

Note: A terminated instance can't be restarted.

Configure Instance Types

You can customize the available instance types that are listed for your cloud. To do this:

1. Specify the number of CPUs by selecting a value from the **CPU** drop-down list box.
2. Specify the size of the memory by selecting a value from the **Memory (GB)** drop-down list box.
3. Specify the amount of disk space by selecting a value from the **Disk (GB)** drop-down list box.

Note: If the value you want is not on the list of options, you can enter any value as long as it is a positive whole number by typing it directly in the appropriate text field(s).

Instance Detail - General

This page shows you the details for an instance.

General

This tab allows you to view general details about the instance, rename the instance, and add tags.

Rename the instance

Type the new name of the volume in the **Name** text field.

Add tags

To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to resources in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. You can optionally add tags by performing the following steps:

To add new tags:

1. Type the key name for your tag into the **name...** text box.

   

   Note: Tags cannot start with "`euca:`" or "`aws:`".

2. Type the value for your tag into the **value...** text box.
3. Click the **Add Tag** button.
4. If you wish to add additional tags, repeat the preceding steps.

To delete one or more tags:

Move your mouse over the tag you wish to delete and click the **X** button.

Saving Your Changes

Once you're satisfied with the edits to your instance, click the **Save changes** button.

Action menu

Clicking the **Actions** button brings up a menu of actions that you can perform on the selected instance.

The following context menu actions are available:

Connect to instance

Selecting this menu will display a dialog with instructions detailing how to connect to the selected instance.

Launch more like this

Selecting this menu will display a dialog that allows you to create and customize one or more instances like the selected instance.

Create launch configuration

A launch configuration is used to define the parameters for new instances that are launched as part of your auto scaling group. Selecting this menu displays the **Create new launch configuration** wizard.

Note: For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

View console output

Selecting this menu will display a dialog box showing the selected instance's console output.

Create image

Selecting this option allows you to create a new image. Refer to the Help on that page to complete the fields.

Associate IP address

Select **Associate IP address** from the **Actions** menu to show the volume management page that will allow you to attach and detach volumes for the selected instance.

Stop

Select this item to stop the selected EBS-backed instance.

Start

Select this item to start the selected EBS-backed instance.

Reboot

Select this item to reboot the selected instance.

Terminate

Select this to terminate the selected instance.

Note: A terminated instance can't be restarted.

Instance Detail - Volumes

This page shows you the details for a volume.

Volumes

This tab allows you to view and manage the volumes attached to the selected instance.

Attach a volume

Click the **Attach a volume** icon to display the **Attach volume** dialog.

Context menu actions

Each tile in the volume list has a context menu. Clicking the action icon in the upper right corner of a volume tile brings up a menu of actions that you can perform on the selected volume.

The following context menu actions are available:

Detach volume

Select this item to detach the selected volume from the instance.

Launch a New Instance

This screen allows you create a new instance.

Select an Image

This panel allows you to select a base image to use for creating your instance.

1. There are two ways to specify a base image:
   - Type an image name directly into the **Enter an image ID** text box
   - Select an image from the list of images on the panel.

     

     Note: You can filter the list of images by typing some filter text into the search textbox, or by selected one or more filters in the **Filter by** section to the left of the image list.

2. Click the **Next** button to proceed to the **Details** panel.

Details

This panel allows you to specify the names, tags, instance size, number of instances, and the availability zone of your new instance(s).

1. Enter the number of new instances to create in the **Number of instances** text box.
2. You can optionally enter one or more names for your new instance(s) in the **Instance name(s)** text box(es).
3. Select an instance size from the **Instance size** drop-down list box.

   

   Note: Information about the instance size is displayed when you click the instance size link.

4. If you want to specify an availability zone other than the default, select an availability zone using the **Availability zone** drop-down list box.

Note: The availability zone does not apply if you choose a VPC network for your security settings in the proceeding panel.

5. To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to each resource in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. To add tags to this resource:
   a) Type the key name for your tag into the **name...** text box.
   b) Type the value for your tag into the **value...** text box.
   c) To add this tag, click the **Add Tag** button.
   d) If you wish to delete a tag that you've already entered, click the **x** button to the right of the tag.
6. Click the **Next** button to proceed to the **Security** panel.

Security

This panel allows you to specify a Virtual Private Cloud (VPC) network, key pair and security group that will be used by your new instance(s). NOTE: if you create a key pair or security group in this section, they will automatically be selected for use in your new instance.

1. Select a VPC network from the drop-down list box.
   If a VPC network is selected, the **VPC subnet** and the **Auto-assign public IP** drop-down list boxes display.
2. Select a CIDR range from the **VPC subnet** drop-down list box.
3. Select whether to enable or disable public IP auto assignment from the **Auto-assign public IP** drop-down list box.
4. Select a key pair using the **Key name** drop-down list box.

Note: You can also create a new key pair by clicking the **Create a key pair** link.

5. Select a security group using the **Security group** drop-down list box.

Note: If you select the default security group, make sure that you've added rules to the default security group so that you can access your instances.

Note: You can also create a new security group by clicking the **Create a security group** link. This opens the Create Security Group dialog box.

   If one of the existing security groups is chosen, the rules associated with the security group display.
6. You can optionally specify an IAM role using the **Role** drop-down list box.

Note: If you select a role, make sure that the correct permissions are defined for that role so that the appropriate level of access is applied to your instance.

7. You can optionally specify advanced options by clicking the **Select advanced options** link and refer to the next section for further details.
8. Click the **Launch instance(s)** button.

Specify Advanced Options

This panel allows you to specify advanced options for your new instance(s). You can add user data, override the kernel and RAM disk IDs, specify private networking, and add additional storage.

1. Specify custom user data by typing it into the **User data** text box or by attaching a file by selecting Upload file then clicking the **Choose File...** button to browse for the file.
2. You can override the kernel ID in the selected image with the **Kernel ID** drop-down list box.
3. You can override the RAM disk ID in the selected image with the **RAM disk ID (RAMFS)** drop-down list box.
4. Click the **Enable monitoring** check box to specify that detailed CloudWatch metric gathering should be enabled for your new instance(s).

5. Click the **Use private addressing only** check box to specify that your new instance should use private addressing only. Private addresses cannot connect directly to the Internet and must go through a NAT (Network Address Translation) device or an elastic IP address mapped to the instance.
6. The Storage section will only display if you have an EBS-backed image. If this is the case, you can configure additional storage for your instance:
   a) Select a volume type using the **Volume** drop-down list box.
   b) Type the desired mapping for the storage into the **Mapping** text box (for example: `/dev/sdb`).
   c) If you want to create the storage from an existing snapshot, specify it in the **Create from snapshot** drop-down list box.
   d) Type the size of the attached storage in gigabytes into the **Size (GB)** text box.
   e) Select the **Delete on termination** check box if you would like the attached storage to be deleted when the instance is terminated.
   f) Click the **Add device** button to add this storage.
   g) You can delete storage you've already added by clicking the minus button on the right side of the storage list item.
7. Click the **Launch Instance** button to launch your new instance(s).

Stop Instance

This dialog box allows you to confirm or cancel a stop instance operation.

Verify Stop Instance

1. To verify that you wish to stop the selected instance(s), click the **Yes, Stop Instance** button.
2. To cancel the stop operation, click the **x** button in the upper right corner of the dialog box.

Reboot Instance

This dialog box allows you to confirm or cancel a reboot instance operation.

Verify Reboot Instance

1. To verify that you wish to reboot the selected instance(s), click the **Yes, Reboot** button.
2. To cancel the reboot operation, click the **x** button in the upper right corner of the dialog box.

Get Console Output

This dialog box displays the console output of the selected instance.

Click the **x** button in the upper right corner of the dialog box to dismiss the console output dialog box.

Launch More Instances Like This

This page allows you create one or more new instances that have the same characteristics as an instance already created.

Specify the Number of Instances

This panel allows you to specify the number of new instances to launch.

1. Enter the number of instances to launch into the provided text box.
2. You can optionally type the name(s) of your new instances in the **Names** text box.
3. You can optionally specify advanced options by clicking the **Select advanced options** link.
4. Click the **Launch Instance** button to launch your new instances.

Specify Advanced Options

This panel allows you to specify advanced options for your new instance(s). You can add user data, override the kernel and RAM disk IDs, specify private networking, and add additional storage.

1. To specify custom user data using a manual entry:

a) Select **Enter text** from the **User data** options.
b) Enter the user data into the provided text box.

2. To specify user data with a file:
   a) Select **Upload file** to attach a user data file.
   b) Click the **Choose File** button.
   A window opens prompting you to select a file from your local file system.
   c) Navigate to the location of the file you want to upload.
   d) Select the file to upload and click **Open** from the file chooser window.
   The name of the selected file displays next to the **Choose File** button.
3. You can override the kernel ID in the selected image with the **Kernel ID** drop-down list box.
4. You can override the RAM disk ID in the selected image with the **RAM disk ID (RAMFS)** drop-down list box.
5. Click the **Enable monitoring** check box to specify that detailed CloudWatch metric gathering should be enabled for your new instance(s).
6. Click the **Use private addressing only** check box to specify that your new instance should use private addressing only. Private addresses cannot connect directly to the Internet and must go through a NAT (Network Address Translation) device or an elastic IP address mapped to the instance.
7. For EBS-backed instances, you can configure the root volume or additional storage for your instance in the Storage section:
   a) Change the size of the root volume by entering the size of the attached storage in gigabytes into the **Size (GB)** text box.
   b) Select the **Delete on terminate** check box if you want the attached storage deleted when the instance is terminated.
   c) You can configure additional storage for your instance by selecting a volume type from the **Volume** drop-down list box.
   d) Type the desired mapping for the storage into the **Mapping** text box (for example: `/dev/sdb`).
   e) If you want to create the storage from an existing snapshot, specify it in the **Create from snapshot** drop-down list box.
   f) Type the size of the attached storage in gigabytes into the **Size (GB)** text box.
   g) Select the **Delete on terminate** check box if you would like the attached storage to be deleted when the instance is terminated.
   h) Click the **Add Device** button to add this storage.
   Added storage displays as a row in the table under the Storage area.
   i) You can delete existing storage by clicking the minus button on the right side of the storage list item.
8. Click the **Launch Instance** button to launch your new instance(s).

Terminate Instance

This dialog box allows you to confirm or cancel a terminate instance operation.

Verify Instance Termination

1. Verify that you wish to terminate the selected instance(s).
2. If you are being prompted to terminate more than one instance and want to remove an instance from the list, you may click the **x** button on the instance ID to remove the instance from the list of instances to be deleted.
3. To terminate the instance(s), click the **Yes, Terminate** button.
4. To cancel the terminate operation, click the **x** button in the upper right corner of the dialog box.

Work with Auto Scaling Groups

This section covers how to work with the auto scaling groups in the Eucalyptus Management Console.

Manage Scaling Groups

This page allows you to view a list of your scaling groups, create new scaling groups, and edit existing scaling groups. You can page through the list of scaling groups by clicking the navigation buttons at the bottom of the screen.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Scaling Groups List

Sort the scaling groups list by selecting a sort order using the **Sort by** drop-down list box.

Searching and Filtering the Scaling Groups List

1. To perform a simple search/filter, type some search text into the search text box at the top right of the page.
2. For more precise filtering and searching, you can add one or more filters by clicking one of the available filters in the **Filter by** section on the right side of the page.

Create a New Scaling Group

Click the **Create New Scaling Group** button. The **Create New Scaling Group** wizard will appear.

Actions

Each entry in the image list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected image.

The following context menu actions are available:

View details

This item will bring up the scaling group detail page.

Manage instances

This will bring up a list of the instances in the auto scaling group.

Manage policies

This item brings up a page that allows manage scaling policies for your auto scaling group.

Deleting scaling group

This item allows you to delete a scaling group.

Create a Scaling Group

This page allows you to create a scaling group. An Auto Scaling group defines the parameters for the Eucalyptus instances that are used for scaling, as well as the minimum, maximum, and the desired number of instances to use for Auto Scaling your application. In order to create a scaling group, you must first have a launch configuration created. For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

General

This section is where you specify the basic configuration of your new auto scaling group.

1. Type the name of your new auto scaling group in the **Name** textbox.
2. Select a launch configuration from the **Launch Configuration** drop-down list box. A launch configuration defines the properties of the instances that are launched as part of your auto scaling group.
3. From the **VPC network** drop-down list box, select No VPC or specify which of your VPCs you want to launch instances in this scaling group.
   If a VPC network is selected, the **VPC subnet(s)** drop-down list box displays.
4. Select a CIDR range from the **VPC subnet(s)** drop-down list box.

Capacity

Use the capacity values to manually scale your scaling groups.

1. Specify the minimum number of instances you want running in your autoscaling group using the **Min** control.
2. Specify the desired number of instances you want running using the **Desired** control.
3. Specify the maximum number of instances you want running using the **Max** control.
4. A termination policy defines how instances that are no longer needed in the scaling group are terminated. A default termination policy is already pre-selected but you can change the policy to a different one, or add more termination policies from the **Termination policies** text box. Termination policies are executed in the order they are listed.

   For information on termination policies, see *Configure Instance Termination Policy for Your Auto Scaling Group*
5. To apply tags, proceed to the next section. Otherwise, click **Next** to proceed to the Membership tab.

Tags

A tag is a key/value pair containing data that you can attach to resources in your cloud. This section of the **Create Scaling Group** wizard allows you to define tags for your scaling group and for instances that run in your scaling group.

1. If you want to apply the new tag to instances running in the scaling group, select the **Propagate** check box.
2. Type the key name for your tag into the **Key** text box.
3. Type the value for your tag into the **Value** text box.
4. To add this tag, click the **Add Tag** button.
5. If you wish to delete a tag that you've already entered, click the **x** on the tag icon.
6. Click **Next** to proceed to the Membership tab.

Membership

In this tab, you can specify availability zones and health checks for the instances that run in your auto scaling group.

1. If present, select one or more availability zones for your new scaling group from the **Availability zones** drop-down list box.

   

   Note: Availability zones are not applicable if a VPC network is selected.

   You can remove a selected availability zone by clicking on the **x** next to the availability zone's name in the **Availability Zones** field.
2. Select one or more load balancers for you new scaling group from the **Load balancers** drop-down list box.

   You can add another load balancer to the new auto scaling group by clicking the **+** button next to the drop-down list box.

   The auto scaling health check uses EC2 instance status checks to determine the health state of each instance in your auto scaling group. If your auto scaling group is using a load balancer, auto scaling will use both EC2 instance status checks and load balancing instance health checks.
3. Type the amount of grace period, in seconds, into the **Health check grace period** text box or use the scroll bars to incrementally adjust the values. This is the amount of time after a new instance is launched in your auto scaling group before health checks start for the instance.

Saving the Scaling Group

1. Once you are satisfied with the properties you defined for your scaling group, click the **Create Scaling Group** button to create your scaling group.
   The Next Step dialog box opens prompting you to add scaling policies for this scaling group.
2. You may choose not to show this message again by checking the **Do not show me this again** checkbox.
3. Click **add scaling policies** to continue. Refer to the help page of the Create scaling policy window to complete the required information.

Scaling Group Detail - General

An Auto Scaling group defines the parameters for the Eucalyptus instances that are used for scaling, as well as the minimum, maximum, and desired number of instances to use for Auto Scaling your application. This page allows you to view and edit a scaling group. For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

Capacity

Use the capacity values to manually scale your scaling groups.

1. Use the **Min** control to change the minimum number of instances you want running in your auto scaling group.
2. Use the **Desired** control to change the desired number of instances you want running.
3. Use the **Max** control to change the maximum number of instances you want running.
4. A termination policy defines how instances that are no longer needed in the scaling group are terminated. A default termination policy is already pre-selected and you can add termination policies by selecting them from the **Termination policies** field. The termination policies are executed in the order they are listed.
5. You can remove a selected termination policy by clicking on the **X** next to the policy name in the **Termination policies** field.

Scaling group

You can change the scaling group's VPC network(s), availability zones, load balancers, and health check grace period here.

If a VPC network was selected for the scaling group, the VPC network and its subnets display. If no VPC network was selected, the VPC components are not shown and the availability zone(s) are editable.

1. You can add VPC subnets by selecting them from the **VPC subnet(s)** field.
2. You can remove a selected VPC subnet by clicking on the **X** next to the IP address associated with each subnet in the **VPC subnet(s)** field.
3. If a VPC network was associated with your scaling group, availability zones are view-only and are not editable. You can add availability zones by selecting them from the **Availability Zones** field.
4. You can remove a selected availability zone by clicking on the **x** next to the availability zone's name in the **Availability Zones** field.
5. You can add load balancers by selecting them from the **Load balancer(s)** field.
6. You can remove a selected load balancer by clicking on the **X** next to each load balancer in the **Load balancer(s)** field.
7. You can change the amount of time after a new instance is launched in your auto scaling group before health checks start for the instance by editing the grace period, in seconds, in the **Health check grace period (secs)** control.

Tags

A tag is a key/value pair containing data that you can attach to resources in your cloud. This section allows you to view, add or delete tags for your scaling group and for instances that run in your scaling group.

1. If you want to apply a new tag to instances running in the scaling group, select the **Propagate** check box.
2. Type the key name for your tag into the **Key** text box.
3. Type the value for your tag into the **Value** text box.
4. If you wish to add additional tags, click the **Add Tag** button.
5. If you wish to delete a tag that you have already entered, click the **X** on the tag icon.

Saving Your Changes

Once you are satisfied with the edits you made to your scaling group, click the **Save Changes** button, or click the **X** button in the upper right corner to cancel the updates.

For more information on Auto Scaling, see *Eucalyptus User Guide.*

Scaling Group Detail - Policies

An Auto Scaling group defines the parameters for the Eucalyptus instances that are used for scaling, as well as the minimum, maximum, and desired number of instances to use for Auto Scaling your application. This page allows you to view and edit a scaling group. For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

Policies

This tab allows you to view and manage scaling policies associated with the auto scaling group.

Add a policy

Click the **Add a policy** icon to display the **Create scaling policy** dialog.

Context menu actions

Each tile in the policies list has a context menu, accessible by clicking on the gear icon, with actions that you can perform on the selected policy.

The following context menu actions are available:

Delete policy

This item allows you to delete a policy.

Scaling Group Detail - Instances

An Auto Scaling group defines the parameters for the Eucalyptus instances that are used for scaling, as well as the minimum, maximum, and desired number of instances to use for Auto Scaling your application. This page allows you to view and edit a scaling group. For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

Instances

This tab allows you to view and manage instances in the auto scaling group.

Context menu actions

Each entry in the policies list has a context menu, accessible by clicking on the gear icon, with actions that you can perform on the selected policy.

The following context menu actions are available:

View details

This item allows you to view the details page for the selected instance.

Mark unhealthy

This item allows you to mark an instance as unhealthy. This will cause auto scaling to terminate the instance and launch a new instance to replace it.

Terminate

This action terminates the selected instance.

Create Scaling Policy

An Auto Scaling policy defines how to perform scaling actions in response to CloudWatch alarms. Auto scaling policies can either scale-in, which terminates instances in your Auto Scaling group, or scale-out, which will launch new instances in your Auto Scaling group. For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

1. Type a name for the scaling policy in the **Name** text box.
2. Select an action type using the **Action** control. The action specifies what to do when a scaling condition is met.
3. Type the numerical unit for the scaling action in the **Amount** text box. This value is used in conjunction with the value entered in the **Measure** control to determine how many instances to scale for this policy.
4. Select the measure for the scaling action using the **Measure** control. This can be either a number of instances (for example: 'scale up by 2 instances') or a percentage value (for example: 'scale down by 10 percent').

5. The cooldown period is the amount of time after the previous alarm-related scaling activity ends before new alarm-related scaling activities can start. Use the **Cooldown period (seconds)** widget to specify a cooldown period.
6. **Note:** A CloudWatch alarm cannot be associated with more than 5 scaling policies.

   Select a CloudWatch alarm from the **Alarm** control. You can click the **Create Alarm** link to display the **Create Alarm** dialog. Auto Scaling uses CloudWatch alarms to determine when to take scaling actions.

Saving the Scaling Group

Once you're satisfied with the properties you've defined for your scaling policy, click the **Add Policy** button to save your work, or click the **Cancel** button to cancel.

For more information on Auto Scaling, see Eucalyptus User Guide.

Delete Scaling Group

This dialog box allows you to confirm or cancel a scaling group delete operation.

Verify Scaling Group Deletion

1. To verify that you wish to delete the selected scaling group, click the **Yes, delete** button.
2. To cancel the delete operation, click the **x** button in the upper right corner of the dialog box.

Create CloudWatch Alarm

Auto Scaling uses CloudWatch alarms to trigger scaling actions. An alarm watches a single metric (for example: CPU utilization) over a time period you set, and performs one or more actions based on the value of the metric relative to a given threshold. CloudWatch alarms will not invoke actions just because they are in a particular state. For more information, please see the Eucalyptus CloudWatch documentation in the *Eucalyptus User Guide.*

To create a CloudWatch alarm

1. Enter the name for your alarm in the **Name** text box.
2. Type a description for your alarm in the **Description** text box.
3. Select a statistic from the first drop-down list box. A statistic is computed aggregation of metric data over a specified period of time; valid values are minimum, maximum, average, sum, and sample count.
4. Select a metric from the next drop-down list box. A metric is a time-ordered set of data points - for example, CPU utilization or volume write ops. You can get metric data from Eucalyptus cloud resources (like instances or volumes), or you can publish your own set of custom metric data points to CloudWatch. You then retrieve statistics about those data points as an ordered set of time-series data.
5. Select trigger dimensions. A dimension is a name-value pair that uniquely identifies a metric; for example: "`Scaling group`" = "`myscalinggroup`".
6. Select a comparison operator for the statistic value.
7. Select a trigger threshold value. This is value is used in combination with the comparison operator and the measurement period and time length to determine whether the alarm should be triggered.
8. Select the number of measurement periods and the period lengths using the controls in the **Evaluation** section of the dialog box. Periods define the time period over which the metric value is compared to the trigger threshold, as well as how many consecutive periods the trigger threshold must be breached before the alarm is triggered.
9. To save your new alarm, click the **Create Alarm** button.

For more information on Auto Scaling and CloudWatch, see the Eucalyptus User Guide.

Work with Launch Configurations

This section covers how to work with Auto Scaling launch configurations in the Eucalyptus Management Console.

Manage Launch Configurations

This screen allows you to view a list of your launch configurations, create new launch configurations, create new scaling groups based on a launch configuration, and delete existing launch configurations.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Launch Configurations List

Sort the launch configurations list with the **Sort by** drop-down list box.

Creating a New Launch Configuration

Click the **Create New Launch Configuration** button. The **Create new launch configuration** wizard will appear.

Viewing Details of a Launch Configuration

Several items in the launch configurations list allow you to click on them to see more detailed information.

To see more details about a launch configuration, or an object associated with an image:

1. Click the name iof the launch configuration to display detailed information about the selected launch configuration.
2. Click an image ID to see to see detailed information about the image associated with the selected launch configuration.
3. Click the name of a key pair to see to see detailed information about the key pair associated with the selected launch configuration.
4. Click the name of a security group to see to see detailed information about the security group associated with the selected launch configuration.

Actions

Each entry in the launch configurations list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected snapshot.

The following context menu actions are available:

View details

This item will bring up the launch configuration detail page.

Use to create scaling group

Selecting this item will cause the **Create scaling group** dialog box to appear with the launch configuration selection pre-populated with the selected launch configuration.

Delete launch configuration

Select this item to delete the selected launch configuration.

Create Launch Configuration

This screen allows you create a new launch configuration. The launch configuration is used to define the parameters for new instances that are launched as part of your auto scaling group. For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

Select an Image

This panel allows you to select a base image to use for creating instances in your auto scaling group.

1. Refine and filter your results by typing search criteria into the **Search** text box or using the **Filter by** section on the left side of the page.
2. Type an image ID into the **Enter an Image ID** text box, or select an image by clicking on the image in the list.
3. Click the **Next** button to proceed to the **Details** panel.

Details

This panel allows you to specify the instance size for new instance in your auto scaling group.

1. Type the name of your launch configuration in the **Name** text box.
2. Select an instance size/type from the **Instance type** drop-down list.

   

   Note: Information about the instance size is displayed when you click the instance size link.

3. Click the **Next** button to proceed to the **Security** panel.

Specify Security

This panel allows you to specify the VPC network settings, key pair and a security group that will be used by the new instances in your auto scaling group. NOTE: if you create a key pair or security group in this section, they will automatically be selected for use in your new instances.

1. If the launch configuration is used with a scaling group using a VPC network, select how the VPC IP assignment is to be applied by selecting an option from the drop-down list box.
2. Select a key pair using the **Key name** drop-down list box.

   

   Note: You can also create a new key pair by clicking the **Create key pair** link. This opens the Create Key Pair dialog box.

3. Select a security group using the **Security group** drop-down list box.

   

   Note: If you select the default security group, make sure that you've added rules to the default security group so that you can access your instances.

   

   Note: You can also create a new security group by clicking the **Create a security group** link. This opens the Create Security Group dialog box.

   If one of the existing security groups is chosen, the rules associated with the security group display, along information about the VPC network in which it resides, if any.
4. You can optionally specify an IAM role using the **Role** drop-down list box.

   

   Note: If you select a role, make sure that the correct permissions are defined for that role so that the appropriate level of access is applied to your instance.

5. The **Create scaling group using this launch configuration** checkbox is checked by default, allowing you to create a new auto scaling group based on this launch configuration. When this is selected, the **New Scaling Group** dialog will display after you've clicked the **Create Launch Configuration** button, with the Launch configuration field pre-populated with the name of your new launch configuration.
6. You can optionally specify advanced options by clicking the **Select advanced options** link and refer to the next section for further details.

Specify Advanced Options

This panel allows you to specify advanced options for the new instance in your auto scaling group. You can add user data, override the kernel and RAM disk IDs, specify private networking, and add additional storage.

1. Specify custom user data by typing it into the **User data** text box or by attaching a file by clicking the **Choose file** button.
2. You can override the kernel ID in the selected image with the **Kernel ID** drop-down list box.
3. You can override the RAM disk ID in the selected image with the **RAM disk ID** drop-down list box.
4. You can configure additional storage for your instance in the Storage section:
   a) Select a volume type using the **Volume** drop-down list box.
   b) Type the desired mapping for the storage into the **Mapping** text box (for example: `/dev/sdb`).

c) If you want to create the storage from an existing snapshot, specify it in the **Create from snapshot** drop-down list box.
d) Type the size of the attached storage in gigabytes into the **Size (GB)** text box.

   The attached storage will be deleted when the instance is terminated, as indicated next to the **Delete on termination** field.

e) Click the **Add device** button to add this storage.
f) You can delete storage you've already added by clicking the minus button on the right side of the storage list item.

5. Click the **Create launch configuration** button.

For more information on Auto Scaling, see the *Eucalyptus User Guide*.

View Launch Configuration Details

This page displays details for a launch configuration.

Actions

Each entry in the snapshots list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected launch configuration.

The following context menu actions are available:

Use to create scaling group

Selecting this item will cause the **Create scaling group** dialog box to appear with the launch configuration selection pre-populated with the selected launch configuration.

Delete launch configuration

Select this item to delete the selected launch configuration.

Delete Launch Configuration

This dialog box allows you to confirm or cancel a launch configuration delete operation.

Verify Launch Configuration Deletion

1. To verify that you wish to delete the selected launch configuration, click the **Yes, delete** button.
2. To cancel the delete operation, click the **Cancel** button.

Work with Snapshots

This section covers how to work with the snapshot dialogs and screens in the Eucalyptus Management Console.

Manage Snapshots

This screen allows you to view a list of your snapshots, create new snapshots, and delete snapshots.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Snapshots List

Sort the snapshots list by selecting a sort order using the **Sort by** drop-down list box.

Searching and Filtering the Volumes List

1. To perform a simple search/filter, type some search text into the search text box at the top right of the page.
2. For more precise filtering and searching, you can add one or more filters by clicking one of the available filters in the **Filter by** section on the right side of the page.

Creating a Snapshot

Click the **Create New Snapshot** button. The **Create new snapshot** page will appear.

Viewing Details of a Snapshot

Several items in the snapshot list allow you to click on them to see more detailed information.

To see more details about a snapshot, or an object associated with an image:

1. Click the name in the list of snapshots to display detailed information about the selected snapshot.
2. Click a volume ID to see to see detailed information about the volume associated with the selected snapshot.

Actions

Each entry in the snapshots list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected snapshot.

The following context menu actions are available:

View details

This item will bring up the snapshot detail page.

Create volume from snapshot

This item brings up a page that allows you to create a volume from the selected snapshot.

Register as image

This item allows you to register the selected snapshot as an image in your cloud, if it was created from a volume containing a root file system. The image can then be used to launch EBS-backed instances.

Deleting snapshot

This item allows you to delete a snapshot.

Create a Snapshot

A snapshot is a backup of a volume. You can use snapshots to create new volumes to be used with your instances.

Snapshot

Add the details of your snapshot:

1. Enter a name for the snapshot in the **Name** text box.
2. Select the volume that you would like to use to create the snapshot from the **Create from volume** drop-down listbox.
3. Enter a description for the snapshot in the **Description** text box.
4. Click the **Create** button to create your new snapshot, or click the **Cancel** button to cancel the operation.

Add tags

To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to resources in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. You can optionally add tags by performing the following steps:

To add new tags:

1. Type the key name for your tag into the **name...** text box.

   

   Note: Tags cannot start with "`euca:`" or "`aws:`".

2. Type the value for your tag into the **value...** text box.
3. Click the **Add Tag** button.
4. If you wish to add additional tags, repeat the preceding steps.

To delete one or more tags:

Move your mouse over the tag you wish to delete and click the **X** button.

Save Your Work

Click the **Save Changes** button to save your work, or click the **Cancel** button to cancel the operation.

Snapshot Details

This page allows you to view details and perform actions on the selected snapshot .

Rename the snapshot

Type the new name for the snapshot into the **Name** text box.

Add tags

To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to resources in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. You can optionally add tags by performing the following steps:

To add new tags:

1. Type the key name for your tag into the **name...** text box.

   

   Note: Tags cannot start with "`euca:`" or "`aws:`".

2. Type the value for your tag into the **value...** text box.
3. Click the **Add Tag** button.
4. If you wish to add additional tags, repeat the preceding steps.

To delete one or more tags:

Move your mouse over the tag you wish to delete and click the **X** button.

Save Your Work

Click the **Create snapshot** button to save your work, or click the **Cancel** button to cancel the operation.

Context menu actions

Clicking the **Action** button brings up a menu of actions that you can perform on the selected snapshot.

The following actions are available:

View details

This item will bring up the snapshot detail page.

Create volume from snapshot

This item brings up a page that allows you to create a volume from the selected snapshot.

Register as image

This item allows you to register the selected snapshot as an image in your cloud, if it was created from a volume containing a root file system. The image can then be used to launch EBS-backed instances.

Delete snapshot

This item allows you to delete a snapshot.

Register a Snapshot as an Image

A snapshot is a block level storage volume that is created by copying an existing volume and is backed by persistent storage. You can register a snapshot as an image if it the snapshot was created from a volume containing a root file system. Once registered, this image can then be used to launch EBS-backed instances.

1. Enter a name for the image in the **Name** text box.
2. Enter a description for the image in the **Description** text box.

3. Click the **Register** button.
4. Select the **Delete on terminate** checkbox if you want the image to delete on termination.
5. Select the **Register as a Windows OS image** checkbox if you're registering a Windows image.
6. Click the **Register as Image** button.

Delete Snapshot

This dialog box allows you to confirm or cancel a snapshot delete operation.

Verify Snapshot Deletion

1. To verify that you wish to delete the selected snapshot(s), click the **Yes, delete** button.
2. To cancel the delete operation, click the **Cancel** button.

Work with Buckets

This section covers how to work with the bucket screens and dialogs in the Eucalyptus Management Console.

Create a Bucket

A bucket is an object storage similar to a file system that allows you to store data on the Internet. You can upload any number of objects to a bucket.

For more information about buckets, go to *Working with Amazon S3 Buckets*.

Create new bucket

Add the details of your bucket:

1. Enter a name for the bucket in the **Name** text box.
2. Click the **Create Bucket** button to create your new bucket, or click the **Cancel** button to cancel the operation.
   A default sharing setting of Private Full Control is applied to all newly-created buckets, meaning the bucket owner is the only one who has full access to it.

Bucket Details

This page allows you to view details about the bucket and edit the sharing properties of a bucket.

Bucket summary

The Bucket section provides a summary of the bucket, including the number of objects it contains.

Actions menu

Clicking the **Actions** menu displays various options you can perform on the current bucket.

View bucket contents

The **View contents** option allows you to see the objects (files and folders) in each bucket. You can also upload new files, create new folders, or delete existing objects.

Create folder

The **Create folder** option allows you to create a folder within the current bucket directly, without requiring you view the contents of the bucket first.

Upload file(s)

The **Upload file(s)** option allows you to upload files directly into the current bucket, without requiring you view the contents of the bucket first.

Enable versioning

The **Enable versioning** option allows you to turn versioning on for the current bucket if it is disabled or suspended.

Suspend versioning

The **Suspend versioning** option allows you to suspend versioning for the current bucket if it is enabled.

Delete a bucket

The **Delete** option allows you to delete the bucket if it is empty.

Edit the sharing settings

The sharing settings dictate whether your account or another account can access your bucket and its contents.

1. To edit the sharing settings:
   a) Click the **Propagate grantee permissions...** checkbox to apply the same sharing settings to all objects in this bucket.

      This checkbox is unchecked by default.

   b) Select the type of user from the **Grantee** drop-down text list to grant access to your bucket.

      Newly-created buckets have a default sharing setting of owner full control.

      

      Note: You can remove an existing account and permission pair by clicking on the **x** next to the pair listed under the **Propagate grantee permissions...** checkbox.

   c) Select the level of access from the **Permission** drop-down list box to apply to the specified users you granted access to your bucket.

      If you enter a user's email address, sharing will be extended to all users in their account.

   d) Click the **Add Grantee** button to add the grantee-permission pair.

      If a user is already granted, the header shows "Add another grantee".

2. When done, click the **Save Changes** button to save your work, or click **Cancel** to abandon your changes.

Object Details

This page allows you to perform a variety of operations associated with objects within buckets.

Object summary

The Object section provides a summary of the object, including its identifiers and a link to view it. The object **Name** is the only editable field but its extension cannot be changed.

Actions menu

Clicking the **Actions** menu displays the options to download, copy, or delete the object.

Download object

The **Download** option allows you to download the object to a specified location on your local file system. A copy of the file remains on S3 until it is deleted from S3 itself.

Copy object

The **Copy** option allows you to copy an object along with all of its attributes from one bucket to another.

Copying an object to the same bucket is not allowed.

Make object public

The **Make public** option allows anyone who has the URL to access and download the object, even if they are not authenticated users.

Delete an object

The **Delete** option allows you to delete the object.

Edit object metadata

Each object has a set of attributes. These attributes identify the object by its key and contain metadata about its size, creation and modified dates, encoding type, encryption, and other pieces of information that allow S3 to process it. Metadata can be system-defined or user-defined.

For more information about object metadata, go to *Object Key and Metadata*.

To edit object metadata, you can delete existing metadata or add a metadata pair:

1. To add a metadata pair:
   a) Select a key from the **Key** drop-down list box or define your own key by typing it in the **Key** search field and click **Add metadata** from the list box.
   b) Select a value for the selected key from the **Value** drop-down list box.
   c) Click **Add Metadata Pair** to acknowledge the message and continue.
2. To remove an existing metadata pair, click the **x** next to the pair listed under the Metadata heading.

Edit the sharing settings

The sharing settings grant specific account(s) certain levels of access to your object.

1. To edit the sharing settings, select from the following:
   a) Select the type of user from the **Grantee** drop-down text list to grant access to your object.
      Newly-created objects have a default sharing setting of owner full control.
   b) Select the level of access from the **Permission** drop-down list box to apply to the specified users you granted access to your object.
      If you enter a user's email address, sharing will be extended to all users in their account.
   c) Click the **Add Grantee** button to add the grantee-permission pair.
      If a user is already granted, the header shows "Add another grantee".
2. When done, click the **Save Changes** button to save your work, or click **Cancel** to abandon your changes.

Create a Folder

A folder acts like a file system folder that allows you to store objects and files. You can create any number of folders in a bucket or in a folder; and organize any number of files in a folder. Any sharing attributes apply to files rather than folders.

Create new folder

Add the details of your folder:

1. Enter a name for the folder in the **Name** text box.
2. Click the **Create Folder** button to create your new folder, or click the **X** in the corner of the window to cancel the operation.
   After the folder is created, the bucket view or parent folder (if present) of the folder created displays.

Upload file

This page allows you to upload a file from your local file system to a folder in one of your buckets and specify sharing attributes and metadata for it.

Select file(s)

1. Click the **Choose Files** button.
   A window opens prompting you to select a file from your local file system.
2. Navigate to the location of the file you want to upload.
3. Select the file to upload or to select multiple files, hold down the **[Ctrl]** key while selecting files.
   The file size limit is 5 TB.
4. Click **Open** from the file chooser window.
   The selected file(s) display under the **Choose Files** button. To remove selected file(s) or add more, start over by repeating all the above steps.
5. You can optionally specify advanced options by clicking the **Advanced** link and refer to the next section for further details.

Specify Advanced Options

You can optionally specify sharing parameters or apply metadata to the object.

Edit the sharing settings

The sharing options for the selected object(s) have been automatically set to match their bucket. Adjust these options if necessary.

1. To edit the sharing settings, select from the following:
   a) Select **Public** to allow everyone access to your object.

   Important: Making an object (or file) public means anyone who has the URL can access the object, even if they are not authenticated users.

   b) Select **Private** to allow only those specified to access your object.
   The Share with others section displays only if **Private** was chosen as the Sharing option for this object.
2. Specify access control parameters by performing the following:
   a) Select **Use canned ACL** to use a pre-defined Access Control List established by your organization.

   Note: For more information about ACL, go to *Access Control List (ACL) Overview.*

   b) To change to another pre-defined ACL, select an ACL from the **Use canned ACL** drop-down list box.
   c) Select **Manually define sharing** to grant only specific accounts certain levels of access to your object.

   Note: In order to manually define sharing with other accounts, specify that account with an account ID or an email address associated with a user in the account. To obtain an account ID, coordinate with the owners or administrators of those accounts. Otherwise, specifying an email address of a user in the account will effectively grant access to everyone in that account.

   Note: You can remove an existing account and permission pair by clicking on the **x** next to the pair listed under the **Manually define sharing** option.

   d) Enter the 12-digit account ID or email address of a user in the account in the **Account** field.
   e) Select the appropriate level of access for the account by selecting it from the **Permissions** drop-down list box.
   f) Click the **Add Account** or **Add another account** button (if one or more accounts were already present) to add it to the list of accounts with which your object is shared.

Edit object metadata

Each object has a set of attributes. These attributes identify the object by its key and contain metadata about its size, creation and modified dates, encoding type, encryption, and other pieces of information that allow S3 to process it. Metadata can be system-defined or user-defined.

For more information about object metadata, go to *Object Key and Metadata*.

To edit object metadata, you can delete existing metadata or add a metadata pair:

1. To add a metadata pair:
   a) Select a key from the **Key** drop-down list box or define your own key by typing it in the **Key** search field and click **Add metadata** from the list box.
   b) Select a value for the selected key from the **Value** drop-down list box.
   c) Click **Add Metadata Pair** to acknowledge the message and continue.
2. To remove an existing metadata pair, click the **x** next to the pair listed under the Metadata heading.

Begin the Upload

1. When done, click the **Upload File(s)** button to upload the select file(s), or click **Cancel** to abandon the operation.
   A confirmation dialog box opens if you proceed to upload.
2. Click **OK, Let's Do This Now!** to confirm and begin uploading the file(s).

A new window opens, displaying the status of the upload with a progress indicator.

3. Stay on the page to complete the upload process.
4. Otherwise, click **Cancel Upload** or navigate away from this page to cancel the uploading process.
   Any files that do not upload completely during the cancel operation are cleaned up automatically. Those that have already uploaded remain in the bucket.

Work with Images

This section covers how to work with the image screens and dialogs in the Eucalyptus Management Console.

Manage Images

This screen allows you to view a list of your images and launch images from an image. You can page through the list of images by clicking the navigation buttons at the bottom of the screen.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Instances List

Sort the images list by selecting a sort order using the **Sort by** drop-down list box.

Searching and Filtering the Images List

1. To perform a simple search/filter, type some search text into the search text box at the top right of the page.
2. For more precise filtering and searching, you can add one or more filters by clicking one of the available filters in the **Filter by** section on the right side of the page.

Viewing Details of an Image

Several items in the image list allow you to click on them to see more detailed information.

To see more details about an image, or an object associated with an instance:

Click the name/ID in the list of images to display detailed information about the selected image.

Actions

If an image is available and not in the process of being created (status "pending"), each entry in the image list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected image.

The following context menu actions are available:

View details

This option is available whether the image is available or in the process of being created.

This item will bring up the image detail page.

Launch instance

This option is only available if the image is available.

Selecting this menu will display a dialog that allows you to launch an instance using the selected image.

Create launch configuration

This option is only available if the image is available.

A launch configuration is used to define the parameters for new images that are launched as part of your auto scaling group. Selecting this menu displays the **Create new launch configuration** wizard.

Note: For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

Remove from cloud

The Remove from cloud option is used to clean up images that are no longer needed. Once removed, it will become de-registered but can be re-registered if its snapshot has not been deleted. This option is only available if the image is available.

1. Selecting this menu displays the **Remove image from cloud** confirmation window.
2. To confirm, click **Yes, Remove Image from the Cloud**.

Image Detail

This screen shows you the details for an image. From this page, you can add tags to an image, launch an instance based on this image, or create a launch configuration based on this image.

Actions

Clicking the **Actions** button brings up a menu of actions that you can perform on the selected image.

The following menu actions are available:

Launch instance

Selecting this menu will display a dialog that allows you to launch an instance using the selected image.

Create launch configuration

A launch configuration is used to define the parameters for new images that are launched as part of your auto scaling group. Selecting this menu displays the **Create new launch configuration** wizard.

Note: For more information on Auto Scaling, please see *Using Auto Scaling* in the *Eucalyptus User Guide*.

Cancel image creation

This option is only available if the image is in a pending, waiting for shutdown, bundling, or storing state.

Remove from cloud

The Remove from cloud option is used to clean up images that are no longer needed. Once removed, it will become de-registered but can be re-registered if its snapshot has not been deleted. This option is only available if the image is available.

1. Selecting this menu displays the **Remove image from cloud** confirmation window.
2. To confirm, click **Yes, Remove Image from the Cloud**.

Sharing

The sharing settings dictate whether your account or another account can access your image.

1. To edit the sharing settings, select from the following:
   a) Select **Public** to allow everyone access to your image.

Important: Making an image public means anyone who has the URL can access that image, even if they are not authenticated users.

   b) Select **Private** to allow only those specified to access your image.
   The Share with others section displays only if **Private** was chosen as the Sharing option for this image.
   c) In order to manually define sharing with other accounts, specify that account with an account ID or an email address associated with a user in the account in the provided text field.

Note: To obtain an account ID, coordinate with the owners or administrators of those accounts. Otherwise, specifying an email address of a user in the account will effectively grant access to everyone in that account.

Note: You can remove an existing account by clicking on the **x** next to the account listed under the Share with specific accounts heading.

d) Click the **Add Account** or **Add another account** button (if one or more accounts were already present) to add it to the list of accounts with which your image is shared.

2. When done, click the **Save Changes** button to save your work, or click **Cancel** to abandon your changes.

Storage

This section is present for EBS-backed instances only. Information about each volume, including the root volume, is listed in rows beneath the Storage heading, along with any additional storage configured for this image:

- VOLUME lists the volume type(s).
- MAPPING defines the instance to which the specified image is attached for this device.
- SNAPSHOT shows the snapshot from which the storage was created.
- SIZE (GB) describes the size of the attached storage in gigabytes.
- DELETE ON TERMINATE specifies whether the attached storage is deleted when the instance is terminated.

Add tags

To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to resources in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. You can optionally add tags by performing the following steps:

To add new tags:

1. Type the key name for your tag into the **name...** text box.

Note: Tags cannot start with "`euca:`" or "`aws:`".

2. Type the value for your tag into the **value...** text box.
3. Click the **Add Tag** button.
4. If you wish to add additional tags, repeat the preceding steps.

To delete one or more tags:

Move your mouse over the tag you wish to delete and click the **X** button.

Work with IP Addresses

This section covers how to work with the IP address screens and dialogs in the Eucalyptus Management Console.

Manage Elastic IP Addresses

Your Eucalyptus cloud can offer elastic IP addresses that you can associate with your running instances. This page allows you to view a list of your available elastic IP addresses, allocate new elastic IP addresses, associate and disassociate elastic IP addresses with running instances, and release elastic IP addresses.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Elastic IPs List

Sort the list of elastic IPs by selecting a sort order using the **Sort by** drop-down list box.

Searching and Filtering the Elastic IP List

1. To perform a simple search/filter, type some search text into the search text box at the top right of the page.
2. For more precise filtering and searching, you can add one or more filters by clicking one of the available filters in the **Filter by** section on the right side of the page.

Allocate an Elastic IP Address

Click the **Allocate Elastic IP Addresses** button to allocate one or more elastic IP addresses.

Viewing Details of a IP Address

Several items in the snapshot list allow you to click on them to see more detailed information.

To see more details about an IP address or associated object:

1. Click the IP address to display detailed information.
2. If there's an instance associated with an IP address, you can click on the instance ID to display detailed information about the instance.

Actions

Each entry in the eips list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected IP address.

The following context menu actions are available:

Associate with instance

This selection allows you to associate the selected IP address with a running instance.

Disassociate from instance

This selection allows you to disassociate the IP address from an instance.

Release to cloud

This item releases the selected IP address back to the cloud.

Elastic IP Address Detail

This screen shows you the details for an elastic IP address. From this page, you can associate an IP address with an instance, disassociate an IP address from an instance, or release an IP address back to the cloud.

Actions

Clicking the **Actions** button brings up a menu of actions that you can perform on the selected elastic IP address.

The following context menu actions are available:

Associate with instance

This selection allows you to associate the selected IP address with a running instance.

Disassociate from instance

This selection allows you to disassociate the IP address from an instance.

Release to cloud

This item releases the selected IP address back to the cloud.

Allocate IP Addresses

This dialog box lets you allocate IP addresses for your cloud.

1. Type the number of IP addresses you want to allocate into the text box.

   

   Note: This operation may not allocated all the requested addresses if the number of addresses you entered exceeds the number of addresses you're allowed by administrative policy. For more information, refer to your system administrator.

2. Click the **Associate addresses from cloud** button.

Release IP Addresses

This dialog box allows you to confirm or cancel an IP address release operation.

1. To verify that you wish to release the selected IP address(es), click the **Yes, release** button.
2. To cancel the delete operation, click the **x** button.

Associate an Elastic IP Address with an Instance

This dialog box lets you associate an elastic IP address with a running instance.

1. Start typing the ID of an instance and then select the instance from the drop-down list box.
2. Click the **Associate Address** button.

Disassociate an Elastic IP Address from an Instance

This dialog box lets you verify that you wish to disassociate one or more elastic IP addresses from running instance(s).

1. Verify that you want to disassociate the listed IP addresses.
2. Click the **Yes, disassociate** button.

Work with Tags

This section covers how to work with resource tags in the Eucalyptus Management Console.

Add tags

To help you manage your cloud's instances, images, and other Eucalyptus resources, you can optionally assign your own metadata to resources in the form of tags. You can use tags to create user-friendly names, make resource searching easier, and improve coordination between multiple users. You can optionally add tags by performing the following steps:

To add new tags:

1. Type the key name for your tag into the **name...** text box.

   

   Note: Tags cannot start with "`euca:`" or "`aws:`".

2. Type the value for your tag into the **value...** text box.
3. Click the **Add Tag** button.
4. If you wish to add additional tags, repeat the preceding steps.

To delete one or more tags:

Move your mouse over the tag you wish to delete and click the **X** button.

Work with IAM

This section covers how to work with IAM resources in the Eucalyptus Management Console.

Create IAM Users

Eucalyptus allows you to manage user permissions using IAM users and groups. This page allows you to add IAM users to your cloud.

Create new users

Add the details of your new user:

1. Type the name of your new user.
2. Click **Add User** to add the user to the list of users to create.
3. If you want to remove a user from the list of users to create, click the minus icon next to the user in the list.
4. Select from the following options:

Note: These options apply to all the users you want to create. Only apply policies if you do not intend to manage user access with IAM groups.

- **Create and download random password**.
- **Create and download access keys**.
- **Allow read/write access to all resources except users and groups**.

Quotas

In this section, you can define limits on what resources your users can create.

Expand the section for each service that you want to specify limits for, and type in the maximum number of that resource that the user is allowed to create in the text field. Leaving a text field blank means no limit is assigned to that resource.

Advanced

In this section...

The **Advanced** section allows you to specify a path for the new user. For more information, see *IAM Identifiers*.

Save Your Work

Click the **Create Users** button to save your work, or click the **Cancel** button to cancel the operation.

Manage IAM Users

Eucalyptus allows you to manage user permissions using IAM users and groups. This page allows you to manage IAM users.

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the User List

Sort the user list by selecting a sort order using the **Sort by** drop-down list box.

Searching and Filtering the User List

To perform a search/filter, type some search text into the search text box at the top right of the page.

Creating a User

Click the **Create New Users** button. The **Create new users** page will appear.

Viewing Details of a User

Several items in the user list allow you to click on them to see more detailed information.

To see more details about a user or associated object:

Click the name/ID in the list of the user to display detailed information about the selected user.

Actions

Each entry in the image list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected user.

The following context menu actions are available:

View details

This item will bring up the user detail page.

Disable

This item deletes a user's password and creates an IAM access "deny all actions" policy that prevents them from executing any actions against the cloud. The user's other information, including active access keys, is maintained until you either make the user active again or delete them.

Enable

This action enables a previously disable user and removes the IAM "deny all actions" policy. You will need to create a new password to allow the user to login.

Delete

This item allows you to delete a user.

Note: This menu item deletes a user and all keys, passwords and permissions associated with that user.

IAM User Detail - General

This page allows you to view and edit the details for an IAM user.

General tab

This tab lets you rename a user, add a user to groups, and add a policy for the user.

Rename a user

To rename a user:

1. Type the name into the **Name** text field.
2. Click the **Save Changes** button to save your work, or click the **Cancel** button to abandon your changes.

Change the path

1. Use the **Path** text field to change the path for the user. For more information, see *IAM Identifiers*.
2. Click the **Save Changes** button to save your work, or click the **Cancel** button to abandon your changes.

Add a user to a group

To add a user to a group:

1. Select the group from the **Select a group...** drop-down list box.
2. Click the **Add User to Group** button.

Remove the user from a group

To remove the user from a group:

1. Click on the gear icon in the group tile. A context menu will appear.
2. Select **Remove user** from the context menu.

Add user policies

An IAM access policy allows you to explicitly define permissions over what your users and groups can access.

To add a policy:

Note: As a best practice, you should use group policies instead of creating individual policies for each user.

Click on the **Add Policy** button to bring up the **Add Access Policy** page.

Delete a policy

An IAM access policy allows you to explicitly define permissions over what your users and groups can access.

To delete a policy:

Click on the **Remove policy** icon (a minus sign in a circle) next to a policy to delete that policy.

View/edit a policy

An IAM access policy allows you to explicitly define permissions over what your users and groups can access.

To view or edit a policy:

Click on the **View/edit** icon (a pencil) next to a policy to view or edit the text of that policy.

Actions menu

Clicking the **Actions** button brings up a menu of actions that you can perform on the selected image.

The following context menu actions are available:

Disable

This item deletes a user's password and creates an IAM access "deny all actions" policy that prevents them from executing any actions against the cloud. The user's other information, including active access keys, is maintained until you either make the user active again or delete them.

Delete

This item allows you to delete a user.

Note: This menu item deletes a user and all keys, passwords and permissions associated with that user.

IAM User Detail - Security

This page allows you to view and edit the details for am IAM user.

Security credentials tab

This tab lets you create or modify a password and generate access keys for a user.

Generate a random password

To generate a random password for the user:

1. Click the **Generate Random Password** button. The system will set a random password for the selected user, and a dialog box will appear, prompting you to save the generated password, which is delivered in a comma-separated values (CSV) file.
2. Save the CSV file in a secure place.

Manually enter a password

To manually create a password:

1. Type a password in the **New password** text box. Note that an indicator will appear under the text box as you type, indicating how strong the password is.
2. Verify the password by typing it again into the **Confirm new password** text box.
3. Click the **Save Password** button.
4. A **Change Password** dialog box will appear, prompting you to enter your password to continue.
5. Type your password into the Your password text box.
6. Click the **OK** button. A dialog box will appear, prompting you to save the new password, which is delivered in a comma-separated values (CSV) file. Save the file in a secure place.

Delete a password

If a password is set for the user, the word "Yes" will appear next to the Password set? label. You can delete this password.

To delete a password:

Note: Deleting the password will disable console access for the user.

1. Click the **Delete password** link on the screen. A dialog box asking you to verify the password deletion appears.
2. Click the **Yes, Delete Password** button to delete the password, or dismiss the dialog box by clicking the **x** in the upper right corner to cancel the delete operation.

Generate access keys

To access to the cloud through Euca2ools or other third party tools, the user will need a set of access keys.

To generate access keys:

1. Click the **Generate Access Keys** button. A dialog box will appear, prompting you to save the comma-separated value file containing the access keys.
2. Save the generated key file in a secure place.

The generated access key will appear in the list of access keys.

Manage access keys

Each access key associated with the selected user is shown in a list in the **Access keys** section of the page. The list shows the access key ID, and a status of either `Active` or `Inactive`. Each entry in the list of access keys has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected instance.

The following context menu actions are available:

Activate

Activates the selected access key.

Deactivate

Deactivates the selected access key.

Delete

Deletes the selected access key.

Actions menu

Clicking the **Actions** button brings up a menu of actions that you can perform on the selected user.

The following context menu actions are available:

Disable

This item deletes a user's password and creates an IAM access "deny all actions" policy that prevents them from executing any actions against the cloud. The user's other information, including active access keys, is maintained until you either make the user active again or delete them.

Delete

This item allows you to delete a user.

Note: This menu item deletes a user and all keys, passwords and permissions associated with that user.

IAM User Detail - Quotas

This page allows you to view and edit the details for an IAM user.

Quotas tab

This tab lets you define limits on resources that this user is allowed to create. The quotas you define will be saved as a policy that will appear in the user's policy list.

Quotas

In this section, you can define limits on what resources your users can create.

1. Expand the section for each service that you want to specify limits for, and type in the maximum number of that resource in the text field. Leaving a text field blank means no limit is assigned to that resource.
2. When you are finished setting quotas, click the **Save Quotas** button to save your work, or click the **Cancel** button to cancel.

Actions menu

Clicking the **Actions** button brings up a menu of actions that you can perform on the selected user.

The following context menu actions are available:

Disable

This item deletes the selected user's password and creates an IAM access "deny all actions" policy that prevents them from executing any actions against the cloud. The user's other information, including active access keys, is maintained until you either make the user active again or delete them.

Delete

This item allows you to delete the specified user.

Note: This menu item deletes the selected user and all keys, passwords and permissions associated with that user.

Create Accounts

Accounts are the highest entity for managing your users, groups and roles. Each account owns and controls all the resources created under it and its set of assigned permissions.

Create an account

Add the details of your new account:

1. Type the name of your new account.
2. In the Add a user text field, type the name of each user to include in this account and click **Add User**.

Note: The admin user will be created for each account as part of the account creation, in addition to any other defined users. Because the admin user is created automatically, you do not have to do add it manually.

3. Repeat for each user to include in the account.

Account Detail - Quotas

Quotas lets you define limits on resources that users for this account is allowed to create. The quotas you define will be saved as a policy that will appear in the account's policy list.

Expand the section for each service that you want to specify limits for, and type in the maximum number of that resource in the text field. Leaving a text field blank means no limit is assigned to that resource.

Save Your Work

Click the **Create Account** button to save your work, or click the **Cancel** button to cancel the operation.
Creating the account assigns it an ID, then generates and downloads a .csv file containing user information along with passwords and access keys associated with each user.

Account Detail - General

This page allows you to view, delete the IAM account, as well as creating and applying access policies and permissions associated with that account.

General Tab

The General tab displays the name of the account, the ID assigned to the account, users and groups in the account, and roles defined for the account, if any.

Actions menu

Clicking the gear icon from the **Actions** menu allows you to delete the account.

Delete an account

To delete an account:

1. Click the **Actions** menu and select **Delete account**.
2. When the confirmation dialog box displays, click the **Yes, Delete Account** button to confirm the deletion. Otherwise, close the confirmation dialog box to cancel.

Denial policies

On accounts, you can only apply "Deny" policies that disallow users of the particular account from performing certain functions.

1. Click the **Add Access Policy** button to open a policy editor window in order to edit each policy defined. For more information, go to *IAM Identifiers*. Refer to the Help in the Access Policy window for additional instructions.
2. If policies are defined and listed, click the **View/edit** icon (a pencil) next to the policy to view or edit that policy.

Delete an account policy

To delete a denial policy from an account:

1. Click on the **Remove policy** icon (a minus sign in a circle) next to a policy to delete that policy.
2. When the confirmation dialog box displays, click the **Yes, Delete** button to confirm the deletion. Otherwise, close the confirmation dialog box to cancel.

Account Detail - Quotas

Quotas let you define limits on resources that users for this account is allowed to create. The quotas you define will be saved as a policy that will appear in the account's policy list.

1. Expand the section for each service that you want to specify limits for, and type in the maximum number of that resource in the text field. Leaving a text field blank means no limit is assigned to that resource.
2. When you are finished setting quotas, click the **Save Quotas** button to save your work, or click the **Cancel** button to cancel.
   Specified quotas are displayed in a list under the **Add Access Policy** button of the General tab.

Manage IAM Groups

Changing the View

You can toggle between the table view and the grid view by clicking the appropriate icon next to the **View** label at the top right of the screen.

Sorting the Groups List

Change the sort order of the groups list by with the **Sort by** drop-down list box.

Searching and Filtering the Groups List

To perform a search/filter, type some search text into the search text box at the top right of the page.

Creating a New IAM Group

Click the **Create Group** button. The **Create new group** dialog box will appear.

Viewing Details of a Snapshot

Several items in the snapshot list allow you to click on them to see more detailed information.

To see more details about a group, or objects associated with the group:

Click the name in the list of groups to display detailed information about the selected group.

Context menu actions

Each entry in the group list has a context menu, accessible in the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected snapshot.

The following context menu actions are available:

View details

This item will bring up the group detail/edit page.

Delete

This item allows you to delete a group.

Create an IAM Group

Eucalyptus allows you to manage user permissions using IAM users and groups. This page allows you to create an IAM group.

Create a new IAM group:

Add the details of your new group:

1. Type the name of your group in the **Name** text field.
2. Click the **Advanced** link to expand the advanced options panel.
   a) The **Advanced** section allows you to specify a path for the new group. For more information, see *IAM Identifiers*.

Save Your Work

Click the **Create group** button to save your work, or click the **Cancel** button to cancel the operation.

IAM Group Details

Eucalyptus allows you to manage user permissions using IAM users and groups. This page allows you to view and edit an IAM group.

Rename the group

To rename the group:

Type the group name into the **Name** text field.

Add users to the group

To add a user to a group:

1. Click the **Users** drop-down list box and select a user from the list. An icon with the user's name will appear on the page.
2. Click the **Save Changes** button.

Remove the user from a group

To remove the user from a group:

Click on the **X** icon to the right of the user icon.

Add a policy

An IAM access policy allows you to explicitly define permissions over what your users and groups can access.

To add a policy:

Click on the **Add Policy** button to bring up the **Add Access Policy** page.

Delete a policy

An IAM access policy allows you to explicitly define permissions over what your users and groups can access.

To delete a policy:

Click on the **Remove policy** icon (a minus sign in a circle) next to a policy to delete that policy.

View/edit a policy

An IAM access policy allows you to explicitly define permissions over what your users and groups can access.

To view or edit a policy:

Click on the **View/edit** icon (a pencil) next to a policy to view or edit the text of a policy.

Actions menu

Clicking the **Actions** button brings up a menu of actions that you can perform on the selected image.

The following context menu actions are available:

Delete

This item allows you to delete the group.

Note: This action deletes a group an all permissions associated with the group. Selecting this item will display a confirmation dialog.

Save Your Work

Click the **Save Changes** button to save your work, or click the **Cancel** button to cancel the operation.

Add Access Policy

An IAM access policy allows you to explicitly define permissions over what your users and groups can access. The **Add Access Policy** page enables you to select and apply an existing access policy template, or define your own access policies by either using the policy generator or writing a policy directly using the built-in editor.

Note: For information on IAM access policies, see *Overview of AWS IAM Policies*

Create a custom policy using the policy generator

The policy generator is an easy-to-use graphical tool that allows you to create a new access policy without having to know IAM's access policy language.

Allow actions

You can allow all actions for a specific service

To allow all actions for a service:

Select the check mark icon next to the service name in the Allow/Deny list.

Deny all actions

You can deny all actions for a specific service

To deny all actions for a service:

Select the x mark icon next to the service name in the Allow/Deny list.

Allow specific actions

You can allow specific actions for a service.

To allow specific actions for a service:

1. Click the + icon to the left of the service to expand the list of available actions for that service.
2. Select the check mark icon next to the action in the Allow/Deny list.

Deny specific actions

You can deny specific actions for a service.

To allow specific actions for a service:

1. Click the + icon to the left of a service to expand the list of available actions for that service.
2. Select the x mark icon next to the action in the Allow/Deny list.

Allow or deny actions for a specific resource

You can allow or deny actions for a specific resource.

To allow or deny actions for a specific resource:

1. Click the + icon to the left of a service to expand the list of available actions for that service.
2. Click the **Advanced** button next to the action in the Allow/Deny list. The list entry for the action will expand to show drop-down lists for setting up resources and conditionals.

3. From the **Set a specific resource** drop-down list on the left, select a resource. The drop-down list to the right will automatically populate with valid values for the selected resource.
4. From the drop-down list on the right, select the appropriate value for the resource you've selected.
5. Select the check box next to the action entry to allow access to the specified resource, or select the x mark to deny access.
6. Click the **Add Resource** button. Note that the ARN of the resource you've selected will appear in the list, and the results of your selections will appear in the **View/Edit Policy** text box on the right side of the page.

Note: To remove a resource you've added, click the **-** icon next to the ARN in the resource list.

Conditional permissions

You can allow or deny permissions based on specific conditions, such as user name or image ID.

To add a condition:

1. Click the + icon to the left of a service to expand the list of available actions for that service.
2. Click the **Advanced** button next to the action in the Allow/Deny list. The list entry for the action will expand to show drop-down lists for setting up resources and conditionals.
3. In the **Conditions (optional)** section, from the **Add a condition** drop-down list on the left, select a comparison element. The drop-down list to the right will automatically populate with valid conditional comparisons for the selected element.
4. From the drop-down list on the right, select the appropriate comparison operator for the element you've selected.
5. If appropriate, enter the comparison value in the text field that appears under the drop-down lists.
6. Click the **Add Resource** button. Note that the conditional you've just added will appear in the list, and the results of your selections will appear in the **View/Edit Policy** text box on the right side of the page.

Note: To remove a condition that you've added, click the **-** icon next to the conditional in the list.

Upload or write a policy

You can use this section to upload an existing policy file or write an access policy directly into the text editor.

1. You can paste or type policy language directly into the View/Edit policy text box on the right side of the screen.
2. To upload an existing policy file: expand the + icon next to the **Upload or write a file (advanced)** label and click the **Browse...** button.

Select a template

This section allows you to apply a pre-defined access policy template.

Click on **Select** button next to the appropriate template in the list.

Save Your Work

Click the **Create Policy** button to save your work, or click the **Cancel** button to cancel the operation.

Create IAM Roles

Roles are used to temporarily allow users or services to access resources without sharing long-term security credentials. Permissions are applied to roles so they not attached to any IAM user or group, allowing applications or services (like Euca2ools) to assume a role that allows them to make programmatic requests to Eucalyptus.

Create a role

Add the details of your new role:

1. Type the name of your new role.
2. Select the role type from the following options:

Note: These options apply to all the users associated with this role.

- **EC2 service** allows EC2 instances to call other services on your behalf.
- **Cross-account access** grants IAM users from another account to access this account. Hover over the (?) icon for more details about choosing this option.

Advanced

You can also optionally give the role a path that you define to identify which part of the organization it belongs to.

The **Advanced** section allows you to associate a path for the new role. Organize your roles in a way that makes sense to you, but ultimately, a path is not used to define how the role is applied. For more information, go to *IAM Identifiers*.

Save Your Work

Click the **Create Role** button to save your work, or click the **Cancel** button to cancel the operation.
A subsequent screen appears, allowing you to add access policies for your newly created role. Refer to its context help for details on completing that operation.

IAM Role Detail

This page allows you to view, delete, and edit the details of an IAM role, such as defining who can assume the role and when, and set permissions on the role.

Actions menu

Clicking the gear icon from the **Actions** menu allows you to delete the role.

Delete a role

To delete role:

1. Click the **Actions** menu and select **Delete role**.
2. When the confirmation dialog box displays, click the **Yes, Delete Role** button to confirm the deletion. Otherwise, close the confirmation dialog box to cancel.

Edit the trust relationships

Trust relationships define what type of role it is, who can use it (for service or cross-account access). To edit a policy associated with a trust relationship:

1. Click the **Edit Trust Policy** button to open a free-form text editor window in order to edit each policy defined. For more information, go to *IAM Identifiers*.
2. Click the **Save Changes** button to save your work, or close the text editor window to cancel.

Add role policies

An IAM access policy allows you to explicitly define permissions for what each role can access.

To add a policy to a role:

Click on the **Add Policy** button to bring up the **Add access policy** for your role page.
The Add access policy page allows you to add new or edit existing access policies for your role. Refer to its context help for details on completing that operation.

Delete a role policy

An IAM access policy allows you to explicitly define permissions for what each role can access.

To delete a policy from a role:

1. Click on the **Remove policy** icon (a minus sign in a circle) next to a policy to delete that policy.
2. When the confirmation dialog box displays, click the **Yes, Delete** button to confirm the deletion. Otherwise, close the confirmation dialog box to cancel.

View/edit a policy

An IAM access policy allows you to explicitly define permissions for what each role can access.

To view or edit a role policy:

1. Click on the **View/Edit policy** icon (a pencil) next to a policy to view or edit the text of that policy.
2. When done, click the **Save Changes** button to save your work, or close the text editor window to cancel.