Eucalyptus 4.4.4 Management Console Guide

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 8 (2018-07-09 19:10:59 UTC)

Install the Eucalyptus Management Console

This section covers how to install the Eucalyptus Management Console.

Install RHEL 7 Repositories for Console Support

To install additionally required RHEL 7 repositories, which are required for Management Console support, complete the steps in this topic.

Prerequisites

- These instructions assume you are installing Eucalyptus 4.4 on RHEL 7.
- Note that CentOS enables the 'extras' repo by default. See https://wiki.centos.org/AdditionalResources/Repositories for more information.

Additional RHEL 7 repos are required before installing the Eucalyptus 4.4 Management Console.

To install and enable the repositories for RHEL 7

1. (Optional) If you do not already have the yum-utils, install it with this command:

   ```
   yum install yum-utils
   ```

   This provides the yum-config-manager, which allows you to enable a repo.
2. Run the following commands:

   ```
   yum clean all
   ```

   ```
   yum install rhel-7-server-extras-rpms rhel-7-server-optional-rpms
   ```

   ```
   yum-config-manager --enable rhel-7-server-extras-rpms rhel-7-server-optional-rpms
   ```

The additional RHEL 7 repos are now installed and enabled.

You are now ready to Install on CentOS / RHEL 7.

Install on CentOS / RHEL 7

To install the Eucalyptus 4.4 Management Console, complete the steps in this topic.

Prerequisites

- The Eucalyptus Management Console package is installed with the Eucalyptus repositories. These instructions assume that you're installing the console on a host machine that's already running Eucalyptus.
- If you're installing the console on a stand-alone machine, see the Eucalyptus Installation Guide to set up the Eucalyptus repositories before following the instructions below.
- You must install and enable the RHEL 7 ‘rhel-7-server-extras-rpms’ repository before installing the console. See Install RHEL 7 Repositories for Console Support. (CentOS enables the 'extras' repo by default. See https://wiki.centos.org/AdditionalResources/Repositories for more information.)
- The version of the Management Console you're running must be the same as the version of Eucalyptus you're running. Running different versions is not supported.
- The Eucalyptus Management Console package installs only on 64-bit architectures.

Important: python-nss cannot be installed on any system running the Management Console. And in certain CentOS/RHEL default installs (not the "minimal" but others), python-nss is installed by default. If the python-nss package is installed, remove it with "`yum remove`" or "`rpm -e`". The console will not operate correctly with this package installed. If you run software which requires python-nss, install the console on another system.

Install the Eucalyptus Management Console on CentOS and RHEL

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.

Upgrade the Management Console

This topic describes how to upgrade the Management Console.

Prerequisites

- If you are upgrading when deploying the Management Console behind a load balancer (ELB), see Deploy the Management Console Behind an ELB.
- The following instructions assume you have already successfully configured the Eucalyptus Management Console for Nginx in a previous version of Eucalyptus.

To upgrade the Eucalyptus Management Console

1. Stop the eucaconsole service, if running:

   ```
   systemctl stop eucaconsole.service
   ```

2. Run the following command to install the new Eucalyptus Management Console repository:

   ```
   yum install http://downloads.eucalyptus.cloud/software/eucalyptus/4.4/
   rhel/7/x86_64/eucalyptus-release-4.4-2.8.as.el7.noarch.rpm
   ```

3. Upgrade eucaconsole:

   ```
   yum upgrade eucaconsole
   ```

4. 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
   ```

   Note: Self-signing certificates are automatically generated by default. To change this to use your own certificates, see Run the Management Console on nginx.

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) (Optional) Locate the `[server:main]` section. By default, the host is set securely to `127.0.0.1`, which means the console only communicates with Nginx on the same host. If you change the host setting to `0.0.0.0`, connections are accepted from anywhere.

   ```
   [server:main]
   ```

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

6. Start eucaconsole using the following command:

```
systemctl start eucaconsole.service
```

Note: This command starts Nginx automatically. There is no need to run Nginx manually.

Your upgrade is now complete.

7. You may now access your Management Console by pointing your web browser to the IP address for your console: `https://yourconsole_ip_address`

Management Console Scaling Overview

Cloud administrators can deploy the Eucalyptus Management Console in a cloud-compatible VM so that a console can scale to meet the demands of users and customers. Just as imaging, ELB, and workers are done currently, delivering the console inside an image provides the ability to eliminate work performed within the console itself.

Deploying the console this way allows only minor configuration of the console needed to launch an instance.

The following are limitations that exist today. Deploying the console behind an ELB makes possible the following, which are not possible otherwise:

- horizontal scalability
- isolated network environment with system-enforced network restrictions
- domain naming support for a fixed console endpoint (e.g., console.eucalyptus.subdomain.com)
- load balancing requests with ELB
- auto scaling based on console-controlled triggers

Deploy the Management Console Behind an ELB

This section describes the process for deploying the console behind a load balancer (ELB).

To run the console behind a load balancer:

1. If you don't have a RHEL / CentOS 7 image on your cloud, perform the following steps to install one:
   a) Download a RHEL / CentOS 7 image from the Eucalyptus Machine Image catalog.

   Note: Keep its ID handy as it will be required in the subsequent steps.
   b) Install the image onto your cloud. For more information, see Install an HVM Image
2. Establish a user account to install and run Euca2ools commands to set up your console. For more information, see Working with Euca2ools Configuration Files.
3. Once you have designated which user account to set up the console, complete the remaining procedure using Euca2ools. You can invoke Euca2ools commands anywhere.
4. Create or import an SSH key. For more information, see Create Key Pairs or euca-import-keypair.
5. Create the console stack using a pre-defined template from the eucaconsole github repository:
   a) First, download the template by running:

```
wget https://raw.githubusercontent.com/eucalyptus/eucaconsole/maint-4.2/
scripts/console-deploy.cfn
```

   b) Run the following command supplying your own values for each attribute, as outlined in the table below:

```
euform-create-stack -—template-file console-deploy.cfn
 <stack_name> -p KeyName=<your_ssh_key> -p ImageId=<emi_id> -p
 InstanceType=<instance_size> -p CloudIP=<fully_qualified_domain_name>
```

Attribute	Variable	Example
stack_name	<stack_name>	`eucaconsole-stack`

Attribute	Variable	Example
`keyName`	<your_ssh_key>	`dak-ssh-key`
`ImageId`	<emi_id>	`emi-2fb14ad7` **Note:** Obtained from step 1.a
`InstanceType`	<instance_size>	`m1.medium` **Note:** The InstanceType shown in the above example is generally sufficient in size. The image type (size) you choose should rarely be larger than m1.medium or c1.medium, unless you plan on accommodating more than 1000 users.
`CloudIP`	<fully_qualified_domain_name> (fqdn)	`a-09.autoqa.qa1.eucalyptus-systems.com`

6. Create an SSL certificate using the domain name for the ELB:
   a) run `euform-describe-stacks <stack_name>` to obtain the domain name from the resulting output URL.
   b) See Uploading SSL Certificates for Elastic Load Balancing to create an SSL certificate.
7. Upload the SSL certificate by running the following command, supplying your own values for each attribute outlined in the table below:

```
euare-servercertupload –s eucaconsole-cert -—private-key-file
 <your_private_key>.pem -—certificate-file <cert_name>.cert
```

Attribute	Variable	Example
`-—private-key-file`	<your_private_key>	`console-pk.pem`
`-—certificate-file`	<cert_name>	`console.crt`

8. Obtain the name of your load balancer by running the `eulb-describe-lbs` command in order to provide it later in step 9.b.
   The results display all the ELBs. There may be only one ELB if you haven't run others. Look for the ELB name that was prefixed with the <*stack_name*> you specified or "eucaconsole-stack" if you used the one supplied in step 5.b.
9. Add the HTTPS listener to your ELB:
   a) Obtain the SSL certificate ARN by running the command:

```
euare-servercertgetattributes –s <cert_name> | head –1
```

   b) Then add the listener by running the command:

```
eulb-create-lb-listeners <elb_name> --listener "protocol=HTTPS,lb-
port=443,instance-port=443,instance-protocol=HTTPS,cert-id=<cert_arn>"
```

   Now you should be able to reach the console via "https://<*cloudIP*>" (the cloudIP is the FQDN you provided when creating the stack in step 5.b).

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`.

Important:

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

Start the console using the following command:

```
systemctl start eucaconsole.service
```

Restart the console using the following command:

```
systemctl restart eucaconsole.service
```

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

Property	Description	Require	Default Value
ufshost	Formerly `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. For S3 downloads to work, `ufshost` may not be set to `localhost`, but specified with the IP or DNS name instead. When the console is used with a federated cloud, the `ufshost` must be set to the DNS name of the UFS. For more information, see Set the Cloud Front End IP Address.	yes	localhost
ufsport	Formerly `clcport`.The port of your cloud front end.	yes	8773
default.region	If the Eucalyptus cloud is configured for federation, set the default region.	no	--
oidc.hostname	See OpenID Connect (OIDC) properties table below.		
oidc.client.ini	See OpenID Connect (OIDC) properties table below.		

Property	Description	Require	Default Value
oidc.scope	See OpenID Connect (OIDC) properties table below.		
oidc.console.hostname	See OpenID Connect (OIDC) properties table below.		
oidc.login.button.label	See OpenID Connect (OIDC) properties table below.		
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 to use the Eucalyptus help system. For more information, see Set the Help Page URL.	yes	https://support.eucalyptus.com/hc/en-us
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. For example: `support.url=http://your-cloud-admin-portal/` `support.url=mailto:support@yourdomain.com` For more information, see Set the Administrator Support URL.	yes	--
log.useractions	To log user interaction in the std console log, set this to `true`.	yes	false
aws.enabled	When set to `true`, the AWS tab displays on the login screen. For more information, see Enable AWS Login.	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 **Note:** If you log into a multi-region cloud, the system automatically sets a default region based on which ufshost the console is configured to connect to. The console administrator can specify a different value for a user's default region in order to override the natural default, if needed.	yes	us-east-1
aws.govcloud.enabled	Set to `true` to enable the AWS `us-gov-west-1` region.	yes	false
static.cache.duration	Sets the cache control value for static assets in seconds; defaults to 12 hours.	no	43200
browser.password.save	Set to `true` to enable browser password saving.	yes	false
file.uploads.enabled	Defaults to `true` to enable file uploads for S3/Object Storage.	yes	true
connection.ssl.validation	Set to `true` to enable validation of the SSL certificate supplied by the ufshost (or other endpoint) to secure the connection to the service endpoint. Requires a properly-signed cert file.	yes	false
connection.ssl.certfile	If certificate validation is enabled, you can specify a different certificate file than the boto-supplied default.	no	cacerts.txt
cloudformation.samples.bucket	Set this to a public bucket that contains JSON templates.	no	sample-templates
cloudformation.url.whitelist	List wildcard patterns that represent acceptable URLs.	yes	http://*, https://*

Property	Description	Require	Default Value
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
connection.retries	Sets the number of retires used when issuing requests to service endpoints. Adjusting this higher may reduce UI responsiveness.	yes	2
pyramid.default_locale_name	The default locale if none is specified by the browser user agent. For more information, see Set the Locale.	no	en
session.key	The session cookie name, which defaults to 'eucaconsole_session'.	yes	eucaconsole_session
session.keyini	The location of a file that contains session encryption keys.	yes	/etc/eucaconsole/session-keys.ini
session.secure	Set to `true` to send session cookies over a secure connection (e.g., Nginx or a load balancer). Needs to be set to `false` if SSL is not configured.	yes	false
session.timeout	Sets the idle session timeout in seconds; defaults to 30 minutes. If null, never times out. For more information, see Configure Session Timeouts.	no	1800
session.cookie_expires	Sets the absolute session timeout in seconds; defaults to 12 hours. If null, never expires. See http://beaker.readthedocs.org/en/latest/configuration.html for more information about session options. For more information, see Configure Session Timeouts.	no	43200
cache.memory.url	Set the memory URL used for configuration of regions for dogpile.cache.	yes	/var/run/eucaconsole/memcached.sock
cache.short_term.expire	Minimum limit for cache expiry, in seconds.	yes	60
cache.default_term.expire	Default for cache expiry, in seconds.	yes	300
cache.long_term.expire	Longer term limit for cache expiry, in seconds.	yes	3600
cache.extra_long_term.expire	Maximum limit for cache expiry, in seconds.	yes	43200
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	--
cache.images.disable	If `true`, disable EC2 image cache on Eucalyptus. If `false`, EC2 image API fetches will be cached for cache.long_term.expire duration.	yes	true

The configurable options for the OpenID Connect (OIDC) properties in the `[app:main]` section of the console.ini file are:

Note: OpenID Connect (OIDC) is a Controlled Availability feature. For information about Controlled Availability features in Eucalyptus, see Special Status Release Features.

Property	Description	Require	Default Value
oidc.hostname	The OpenID Connect (OIDC) hostname for the ident host. OIDC login functionality is enabled when a value is assigned. Once enabled, all other OIDC properties are required. This property is commented out by default.	no	--
oidc.client.ini	The location of a file that contains the OIDC credentials. This file contains client id and secret that are generated by the ident provider.	yes	/etc/eucaconsole/oidc-credentials.ini
oidc.scope	The OIDC scope is specific to your ident provider and is used in a token API request.	yes	urn:globus:auth:scope openid email profile
oidc.console.hostname	The OIDC return URL hostname. Required to be the hostname that this console runs as, so callback from the ident provider can return control back to this application. If the console is installed on the UFS host, this value would be the same as ufshost above. It may be different based on where the console is running.	yes	localhost
oidc.login.button.label	The text that appears on the login button.	yes	Sign in with Globus Auth

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

Property	Description	Require	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	127.0.0.1
port	The port on which the console can be reached. For more information, see Configure the UI Port.	yes	8888
workers	The number of worker processes used to service requests. A rule of thumb is double the number of cores plus one. For more information, see Configure Workers.	yes	4
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. The 'eucaconsole' user must have write permission to the directory.	no	/var/tmp

Logging configuration options are at the end of the console.ini file. For more information on these settings, see http://docs.pylonsproject.org/projects/pyramid/en/latest/narr/logging.html.

Configure Memcached

Memcached is configured by default for the eucaconsole service on a single host. On multiple hosts (in a scaling group), it is required to run a central memcached, as outlined in the procedure below.

This procedure assumes that the Eucalyptus Management Console package is installed. For instructions on installing the packages, see Install the Eucalyptus Management Console.

Note: If there is just one Console server, the automatically configured memcached service is sufficient for use by the console.

1. Turn off the default memcached on all the consoles by editing `/etc/init.d/eucaconsole` and set `MEMCACHED_FLAGS="NO"`. This would normally be handled by your cloud-init or cfn-init script from your launch configuration.
2. Set up a central memcache to ensure your memcached instance is available and durable, we recommend running it within a scaling group of 1 and behind an ELB. The ELB requires a listener for port 11211 and its DNS address would be used in the cache.memory.url in the next step.
3. Configure the console.ini file to talk to the central memcached. This is typically defined in an init script, such as the cloud.init, shell script or cfn.init file. For example, the memcached socket in the cache memory URL should point to the port that memcached uses (11211) to listen:

   ```
   cache.memory.url = /var/run/eucaconsole/memcached.sock
   ```

   to

   ```
   cache.memory.url = [memcachedhost]:11211
   ```

   For example:

   ```
   cache.memory.url = 10.0.0.20:11211
   ```

Restarting the Console

If you add shared images with Euca2ools, you can make them available to users sooner by restarting the console, which clears the cache (memcached). To do that, restart the service:

```
servicectl restart eucaconsole
```

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

```
ufshost=127.0.0.1
```

Note: When the console is used with a federated cloud, the `ufshost` must be set to the DNS name of the UFS.

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
```

Run the Management Console on nginx

Nginx is a web server that manages SSL connections, and acts as a reverse proxy server, which redirects http protocol to https protocol.

Enable nginx to Start with eucaconsole

When you install the Management Console, nginx is installed automatically. By default, the console is configured to use secure HTTP to allow secure connections from a web server to a browser.

- No procedure is required to enable nginx to start with eucaconsole, as it is part of the standard console installation and execution process.
- If you edit any of the parameters in the nginx.conf file, you must first stop the eucaconsole service and restart it for the changes to take effect:

```
systemctl stop eucaconsole.service
systemctl restart eucaconsole.service
```

Use Your Own Certificates

The Management Console generates self-signed certificates by default but can use your own certificates to run the console instead.

This procedure involves copying over your certificate files:

1. Stop eucaconsole and nginix, using the single command:

   ```
   systemctl stop eucaconsole.service
   ```
2. Edit the file `/etc/sysconfig/eucaconsole` to add:

   ```
   GENERATE_CERT=NO
   ```
3. Copy your certificates file from `cert/key` to `/etc/eucaconsole/console.key` and `/etc/eucaconsole/console.crt`.

   Note: The path shown above are the default locations for the certificate files. You may place them in another location if you prefer, but you must edit the `ssl_certificate` and the `ssl_certificate_key` in `/etc/nginx/nginx.conf` to point to the correct location.
4. Start the eucaconsole service:

   ```
   systemctl start eucaconsole.service
   ```

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 act as a proxy.

To run your console on port 80:

1. Locate the default configuration file from `conf/nginx.conf`.

2. Locate and remove the ***entire*** server section containing the `https rewrite` rule:

```
server {
    listen 80 default;
    server_name ~^(?<domain>.+)$;
    rewrite     ^ https://$domain$request_uri? permanent;
}
```

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 the eucaconsole service using the following command:

```
systemctl restart eucaconsole.service
```

Note: This command restarts nginx automatically. There is no need to run nginx manually.

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. The UI proxy is used behind nginx on the same host and therefore, the default host setting is configured to listen on localhost only. Verify the host setting under the `[server:main]` section is set to `127.0.0.1`, for localhost, per this example:

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

Note: If you prefer to accept connections from anywhere, you can configure the proxy by setting it to 0.0.0.0.

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 (IE 11 and Edge)

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.

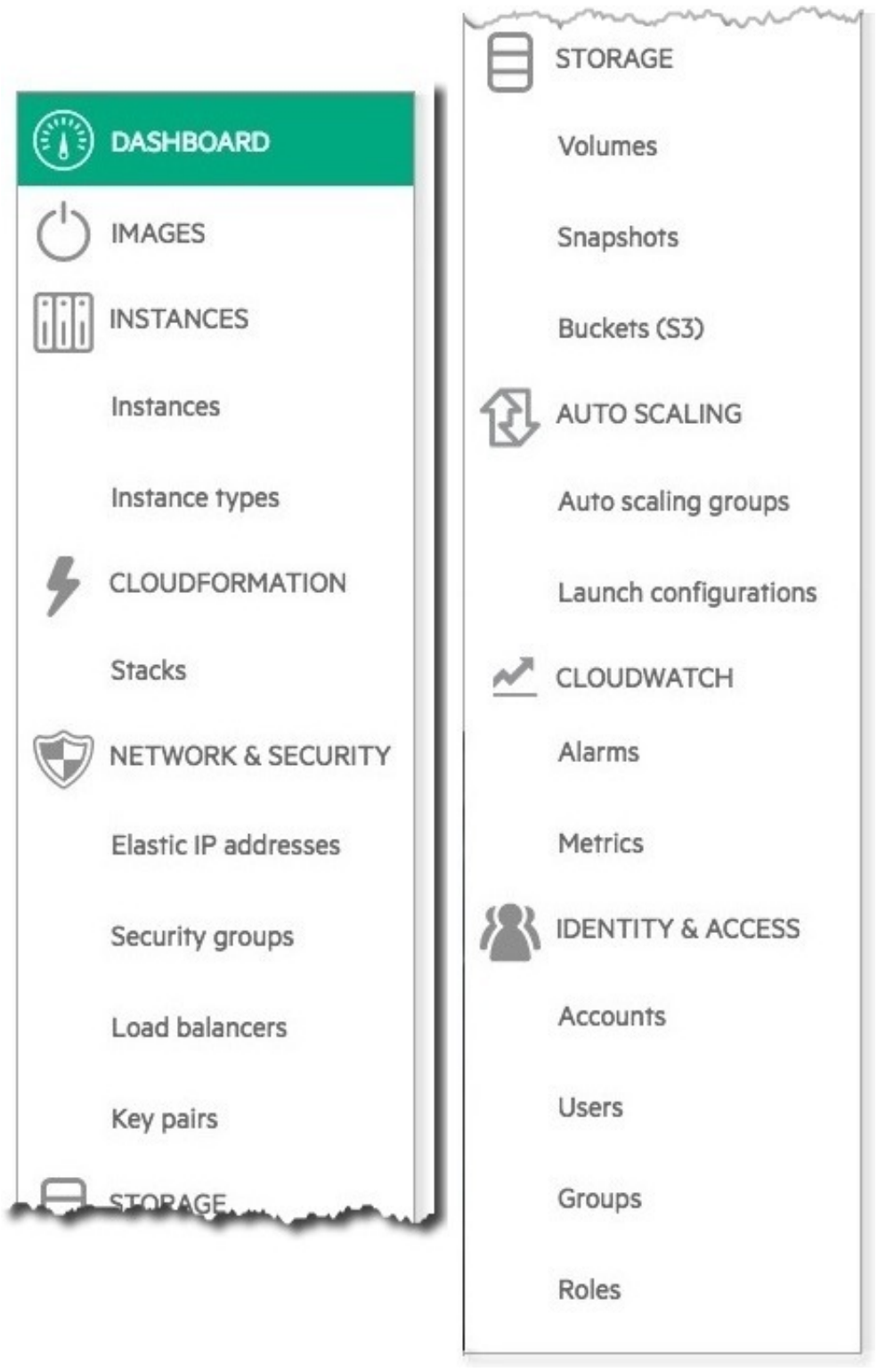
Navigate the Dashboard

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, load balancers, and IP addresses).

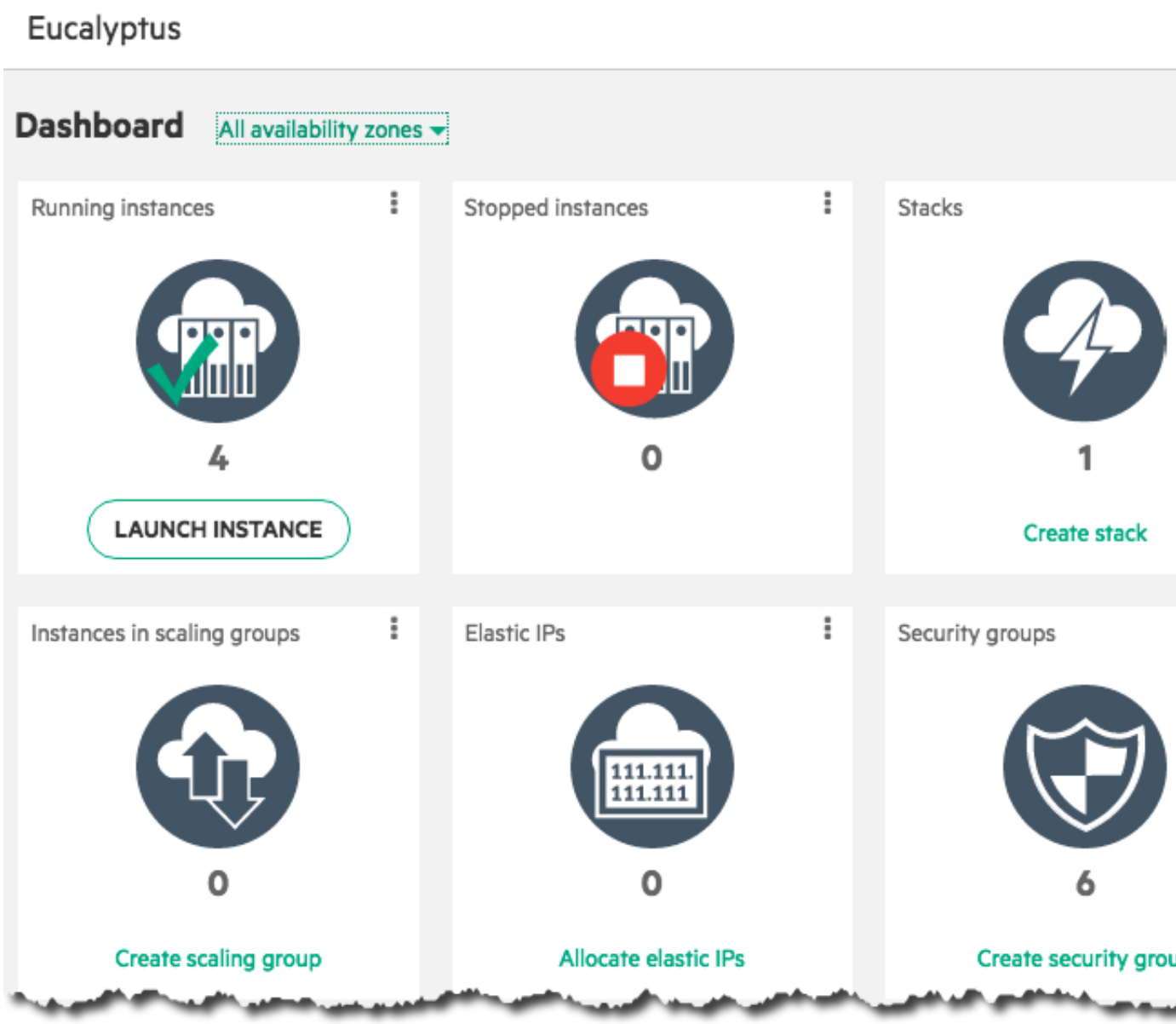
Basic Dashboard Navigation

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

1. You can click directly on a resource, listed under a category grouped by an icon at the left of the main console page to navigate directly to a resource management landing page or back to the main console screen (dashboard).



2. You can also navigate to a resource management landing page by clicking directly on a resource tile/icon or count in the main dashboard view.



3. You can also move resource tiles to any position on the dashboard to better accommodate the resources you use most often. To do this, hold and drag tiles to a different location on the screen.
4. You can also remove tiles if you do not wish to display them on the dashboard by clicking on the action icon (###) for the resource tile you want to remove and select **Remove**.
5. 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 list box at the top of the page.

Images

As one of the resources not available for access from the dashboard, you can access a list of images that are currently used by your cloud from a link on the left side navigation bar.

From the left side navigation bar, click the **Images** icon (power symbol) to display the **Images** landing page.

The **Images** landing page allows you to view details about each of the images currently used in your cloud configurations.

Instances

The dashboard allows you to see how many instances are running, stopped, and part of a scaling group; and allows you to navigate to the **Instances** landing page and the **Scaling Groups** landing page, respectively.

1. Click the **Running instances** icon (clouds with green check mark) or the **Stopped instances** icon (cloud with red stop symbol) from the dashboard to display the **Instances** landing page.
2. You can launch a new instance by clicking the **LAUNCH INSTANCE** button beneath the Running instances icon to display the **Launch new instance** wizard.
3. For additional information on completing that page, refer to the instructions provided in its Help content.
4. From the dashboard, you can view details about the instances that are part of a scaling group by clicking on the number in the Instances in scaling groups tile or clicking the **Scaling groups** icon (cloud with up and down arrows).

CloudFormation

The dashboard allows you to see how many CloudFormation stacks are active and to access the **Stacks** landing page.

1. Click the number in the Stacks tile or **Stacks** icon (cloud with lightning) from the dashboard to display the **Stacks** landing page.
2. You can create a new stack by clicking **Create stack** beneath the Stacks icon to launch the **Create stack** wizard.
3. For additional information on completing that page, refer to the instructions provided in its Help content.

Network and Security

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

1. To access the **Security groups** landing page, click the **Security groups** icon (shield symbol).

   You can create a new security group by clicking **Create security group** beneath the Security groups icon to launch the **Create security group** wizard.
2. To access the **Load balancers** landing page, click the **Load balancers** icon (spokes with arrows).

   You can create a new load balancer by clicking **Create load balancer** beneath the Load balancers icon to launch the **Create load balancer** wizard.
3. To access the **Key Pairs** landing page, click the **Key pairs** icon (key symbol).

   You can create a new key pair by clicking **Create key pair** beneath the Key pairs icon to launch the **Create key pair** wizard.
4. To access the **Elastic IPs** landing page, click the **Elastic IPs** icon (cloud with IP addresses).

   You can allocate elastic IP addresses from the cloud, then associate them with your instances by clicking **Allocate elastic IPs** beneath the Elastic IPs icon and follow the prompts to allocate elastic IP addresses.
5. For additional information on completing any of the creation steps, refer to the instructions provided in each of their respective Help content.

Storage

The dashboard allows you to see at a glance the number of volumes, snapshots, and buckets in your Eucalyptus cloud, and to navigate to landing pages for each type of storage object.

1. To access the **Volumes** landing page, click the **Volumes** icon (cloud with cylinder).

   You can create a new volume by clicking **Create volume** beneath the Volumes icon to launch the **Create new volume** wizard.
2. To access the **Snapshots** landing page, click the **Snapshots** icon (cloud with camera).

   You can create a new snapshot by clicking **Create snapshot** beneath the Snapshots icon to launch the **Create new snapshot** wizard.
3. To access the **Buckets** landing page, click the **Buckets (S3)** icon (bucket symbol).

   You can create a new bucket by clicking **Create bucket** beneath the Buckets icon to launch the **Create new bucket** wizard.

4. For additional information on completing any of the creation steps, refer to the instructions provided in each of their respective Help content.

Auto Scaling

The Auto Scaling category consists of scaling groups and launch configurations. The dashboard allows you to see how many scaling groups are configured and to navigate to the **Scaling groups** landing page.

1. From the dashboard, click on the number in the Instances in scaling groups tile or click the **Scaling groups** icon (cloud with up and down arrows) to display the **Scaling groups** landing page.
2. You can create a new scaling group by clicking **Create scaling group** beneath the Scaling groups icon to launch the **Create scaling group** wizard.

   For additional information on completing that page, refer to the instructions provided in its Help content.
3. As one of the resources not available for access from the dashboard, you can access a list of launch configurations by clicking on the **Launch configurations** link on the left side navigation bar under the Auto Scaling category.

CloudWatch

The CloudWatch category is used for monitoring purposes and consists of alarms and metrics. The dashboard allows you to see how many alarms are in alarm state and to navigate to the **Alarms** landing page.

1. From the dashboard, click on the number in the Alarms in alarm state tile or **Alarms** icon (bell symbol) to display the **Alarms** landing page.
2. A metric must be selected before you can create an alarm. This is achieved by creating an alarm from a Metrics page of the monitoring tab on any resource's detail page, or from the Metrics landing page.
3. As one of the resources not available for access from the dashboard, you can access a list of metrics by clicking on the **Metrics** link on the left side navigation bar under the CloudWatch category.

Identity and Access

If you are the administrator of your Eucalyptus cloud, the dashboard allows you to see at a glance the number of users, groups, and roles currently configured; and to navigate to the landing pages for each type of Identity and Access Management (IAM) object.

1. To access the **Users** landing page, click the **Users** icon (outline of a person).

   You can create a new user by clicking **Create users** beneath the Users icon to launch the **Create new users** wizard.
2. To access the **Groups** landing page, click the **Groups** icon (multiple persons symbol).

   You can create a new group by clicking **Create group** beneath the Groups icon to launch the **Create new group** wizard.
3. To access the **Roles** landing page, click the **Roles** icon (photo badge symbol).

   You can create a new role by clicking **Create role** beneath the Roles icon to launch the **Create new role** wizard.
4. For additional information on completing any of the creation steps, refer to the instructions provided in each of their respective Help content.

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 get help from the Eucalyptus support, manage your credentials, 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 or to generate a new set of access keys, select **Manage credentials** 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.

   Note: If generating new access keys, remember to save them as they are not stored anywhere on the cloud.

   Note: Please contact your cloud administrator to have them remove any old keys you are no longer using.

3. To show the software version running 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.

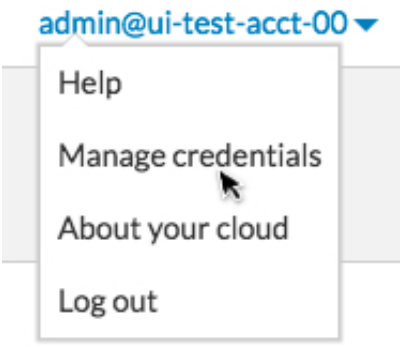
   Note: When logged into your AWS account, you can change your region by clicking on the drop-down menu next to the account menu in the upper right corner of the dashboard page. The Eucalyptus console will remember your last selected region.

Manage Credentials

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

Prerequisites

To access this page, you must be logged in as *administrator* and select the **Manage credentials** option from the account profile drop-down menu:



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

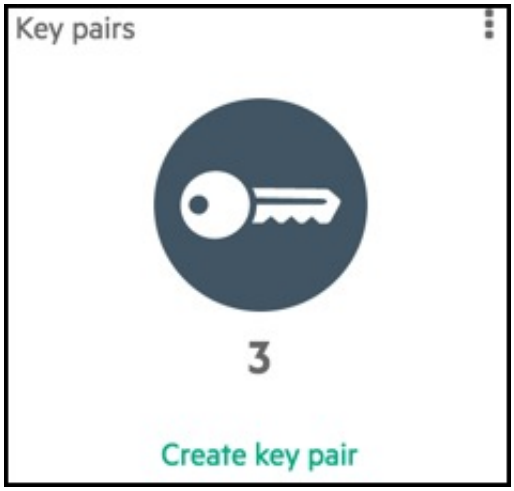
This section covers how to navigate and use the key pair screens and dialogs in the Eucalyptus Management Console.

Key Pairs Landing Page

The Key Pairs landing page allows you to view a list of your key pairs, create new key pairs, and delete key pairs. You can delete multiple key pairs at one time by checking the boxes next to the key pairs you want to delete. Use the scroll bar to view additional key pairs not in the browser's current view.

Prerequisites

To access this page from the dashboard, click **Key pairs** from the left navigation bar under **NETWORK & SECURITY** or click the key icon from the Key pairs tile:



Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Create a Key Pair

1. From the dashboard, locate the **Key pairs** tile and click **Create key pair**.

   OR

2. From the **Key pairs** landing page, click the **Create Key Pair** button near the top of the page.

The **Create new key pair** page opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

Import Key Pairs

1. Access the **Key Pairs** landing page from the dashboard.
2. From the **Key pairs** landing page, click the down arrow next to the **Create Key Pair** button near the top of the page.
3. Click **Import Public Key** to select it.

The **Import public key** page opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

View Details of a Key Pair

You can see details about a key pair, including its fingerprint information:

To see more details about a key pair:

1. Click the name of the key pair in the list of key pairs.

   OR

2. In the Actions column, click the action icon (###) for the key pair you want to view and select **View details**.

The details page for the selected key pair opens.

Actions

Two Action operations are available from the Keypair landing page:

- The **More Actions** button
- The action icon (###)

1. The **More Actions** button above the list of key pairs has a context menu that allow you to apply an action to a particular key pair or multiple key pairs.
   a) Select one key pair and both the **View details** and the **Delete key** options are available.
   b) Select multiple key pairs from the list and only the **Delete key** option is available.
2. Click the action icon (###) from the Actions column of a corresponding entry in the key pairs list, and the following action(s) can be performed:
   a) **View details**. Displays more information about the selected key pair.
   b) **Delete key**. Removes the selected key pair upon confirming the deletion.

Create a Key Pair

Eucalyptus uses cryptographic key pairs to verify access to instances. Key pairs are used if you want to connect to your instance using SSH. 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.
   The **Key Pairs** page opens.
2. Click the **Create Key Pair** button.
   The **Create new key pair** window opens.
3. Type a name for the new key pair into the **Name** text box.

   The name may contain up to 255 alphanumeric and special characters.
4. Click the **Create and Download** button. The private half of the key pair (.pem file) 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.

Security Groups Landing Page

The Security Groups landing page allows you to view, create, modify and delete security groups. Use the scroll bar to view additional security groups not in the browser's current view.

Prerequisites

To access this page from the dashboard, click **Security groups** from the left navigation bar under **NETWORK & SECURITY** or click the shield icon from the Security groups tile:

Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Create a Security Group

1. From the dashboard, locate the **Security groups** tile and click **Create security group**.

   OR

2. From the **Security groups** landing page, click the **CREATE NEW SECURITY GROUP** button near the top of the page.

The **Create new security group** page opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

View 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.

To see more details about a security group:

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

   OR

2. In the Actions column, click the action icon (###) for the security group you want to view and select **View details**.

The details page for the selected security group opens.

Actions

Two Action operations are available from the Security group landing page:

- The **More Actions** button
- The action icon (###)

1. The **More Actions** button above the list of security groups has a context menu that allow you to apply an action to a particular security group or multiple security groups.
   a) Select one security group and both the **View details** and the **Delete** options are available.
   b) Select multiple security groups from the list and only the **Delete** option is available. This operation allows you to delete multiple security groups at one time.
2. Click the action icon (###) from the Actions column of a corresponding entry in the security group list, and the following action(s) can be performed:
   a) **View details**. Displays more information about the selected security group.
   b) **Delete security group**. Removes the selected security group upon confirming the deletion.

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, 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.

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:

Add tags

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.
5. 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, 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.

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:

Add tags

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.
5. 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

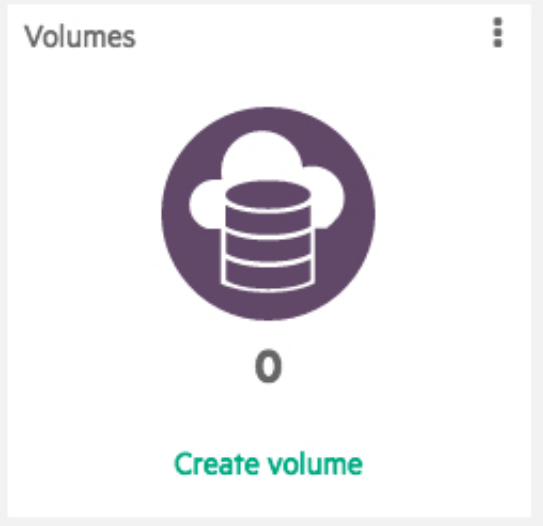
This section covers how to navigate and use the volume screens and dialogs in the Eucalyptus Management Console.

Volumes Landing Page

Eucalyptus offers persistent storage that you can attach to a running instance. These elastic 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. Use the scroll bar to view additional volumes not in the browser's current view.

Prerequisites

To access this page from the dashboard, click **Volumes** from the left navigation bar under **STORAGE** or click the **Volumes** icon (cloud with cylinder) from the Volumes tile:



Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Create a Volume

1. From the dashboard, locate the **Volumes** tile and click **Create volume**.

   OR

2. From the **Volumes** landing page, click the **CREATE NEW VOLUME** button near the top of the page.

The **Create new volume** page opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

View Details of a Volume

Several items in the volumes list allow you to click on them to see more detailed information, such as an object associated with it.

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

1. Click the name/ID in the list of volumes to display detailed information about the selected volume.

   OR

2. In the Actions column, click the action icon (###) for the volume you want to view and select **View details**. The details page for the selected volume opens.
3. To view the details of the instance associated with a particular volume, if applicable, click the instance ID that displays under the volume's Instance column.
4. To view the details of the snapshots associated with a particular volume, click the number that displays under the volume's Snapshots column.

Actions

Two Action operations are available from the Volumes landing page:

- The **More Actions** button
- The action icon (###)

1. The **More Actions** button above the list of volumes has a context menu that allow you to apply an action to a particular volume or multiple volumes.
   a) Select one volume and the **View details**, **Detach from instance** , **Manage snapshots**, and the **View monitoring** options are available.
   b) Select multiple volumes from the list and the **Attach from instance**, **Detach from instance**, and the **Delete** options are available.
2. Click the action icon (###) from the Actions column of a corresponding entry in the volumes list, and the following action(s) can be performed:
   a) **View details**. Displays more information about the selected volume.
   b) **Manage snapshots**. Brings up a page that allows you to view, add, and delete snapshots for a volume.
   c) **Monitor**. Opens the monitoring details that include information about CloudWatch alarms and metrics associated with that particular volume.
   d) **Attach to instance**. Allows you to attach the volume to a running instance.

      Note: This menu option will not appear if the volume is already attached to an instance.
   e) **Detach from instance**. Allows you to detach the volume from a running instance.

      Note: This menu option will not appear if the volume is not attached to an instance.
   f) **Delete volume**. Allows you to delete the selected volume.

      Note: This menu option will not appear if the volume is attached to an instance. You must first detach the volume from the instance before you are able to delete the volume.

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.

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:

Add tags

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.
5. 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.

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:

Add tags

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.
5. 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.

Volume Detail - Monitoring

This tab allows you to view and create alarms based on criteria you define, and provides a graphical view of various data points being monitored for your volume.

Alarms

This section displays a list of configured alarms and allows you to create a new alarm.

1. To view the details of currently configured CloudWatch alarms, expand it by clicking the plus symbol **(+)** next to the Cloudwatch alarms summary.
   The expanded view displays the state of each alarm, the alarm name, and their thresholds.
2. To create a new alarm, click the **Create Alarm** button.
   The Create Alarm page opens. Refer to the Help in the Create Alarm page for further instructions.

Context menu actions

A context menu, accessible by clicking the menu icon (row of three dots), contains actions associated with the monitoring of your instance.

The following context menu actions are available:

- **Turn monitoring on** displays monitoring data associated with your instance.
- **Turn monitoring off** disables monitoring data completely.
  When you select this option, no charts display. Instead, a reminder that monitoring is currently turned off, but you can turn it back on by clicking the **Enable Monitoring for this Instance** button.

CloudWatch metrics

This part of the page displays the CloudWatch data when you enabled monitoring for your instances.

1. The graphs displayed by default are:
   - **Read bandwidth**. Represents the total number of bytes transferred during a specified period of time to complete read operations over a 1024k I/O.
   - **Write bandwidth**.Represents the total number of bytes transferred during a specified period of time to complete write operations over a 1024k I/O.
   - **Read throughput (ops/sec)**. The total number of read I/O operations that has completed in a specified period of time.
   - **Write throughput (ops/sec)**. The total number of write I/O operations that has completed in a specified period of time.
   - **Average queue length**. The average read and write operation requests waiting to be completed in a specified period of time.
   - **Percent time spent idle**. The percentage of time over a specified period where no read or write operations are present.
   - **Average read size (KiB/op)**. The average size of each read I/O operation in a specified period of time.
   - **Average write size (KiB/op)**. The average size of each write I/O operation in a specified period of time.
   - **Average read latency (ms/op)**. The average number of seconds spent by read operations that completed in a specified period of time.
   - **Average write latency (ms/op)**. The average number of seconds spent by write operations that completed in a specified period of time
2. The various ways to view the data in the graphs are:
   - Click on a graph to expand it.
   - Hover inside the graph to display a read-out of data-points desired.
   - Use the drop-down list boxes for **Show data for** to focus in on a set of data within a specific period of time.

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

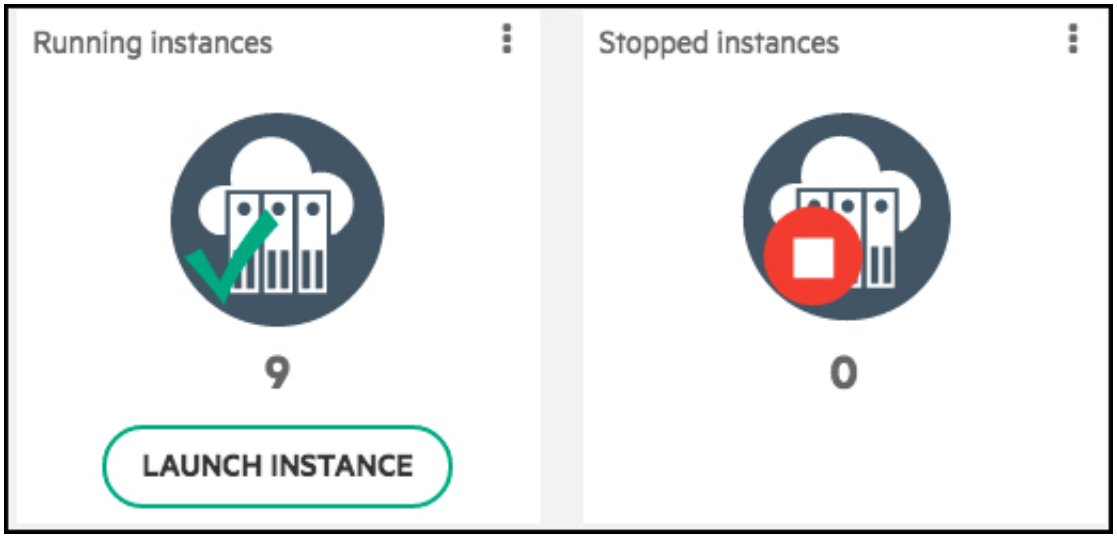
This section covers how to work with the instance dialogs and screens in the Eucalyptus Management Console.

Instances Landing Page

This page allows you to view a list of your instances, create new instances, and perform actions on your instances. Use the scroll bar to view additional instances not in the browser's current view.

Prerequisites

To access this page from the dashboard, click **Instances** from the left navigation bar under **INSTANCES** or click the **Running instances** icon (clouds with green check mark) or the **Stopped instances** icon (cloud with red stop symbol) to display the **Instances** landing page:



Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Launch an Instance

1. From the dashboard, click the **LAUNCH INSTANCE** button beneath the Running instances icon.

   OR

2. From the **Instances** landing page, click the **LAUNCH NEW INSTANCE** button near the top of the page.

The **Launch new instance** wizard opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

From the dashboard, you can view details about the instances that are part of a scaling group by clicking on the number in the Instances in scaling groups tile or clicking the **Scaling groups** icon (cloud with up and down arrows).

View Details of an Instance

Several items in the instances list allow you to click on them to see more detailed information, such as an image, security key, and security group associated with it.

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

1. Click the name/ID in the list of instances to display detailed information about the selected instance.

   OR

2. In the Actions column, click the action icon (###) for the instance you want to view and select **View details**. The details page for the selected instance opens.
3. Click an image ID to see detailed information about the image used to launch the selected instance.
4. Click a key name to see detailed information about the security key used to launch the instance.
5. 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 from 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**. Brings up the instance detail page.
- **Connect to instance**. Displays a dialog with instructions detailing how to connect to the selected instance.
- **Launch more like this**. Displays a dialog that allows you to create and customize one or more instances like the selected instance.
- **Create launch configuration**. Displays the Create new launch configuration wizard, which is used to define the parameters for new instances that are launched as part of your auto scaling group.

  Note: For more information on Auto Scaling, see *Using Auto Scaling* in the *Eucalyptus User Guide*.
- **View console output**. Displays a dialog box with the selected instance's console output.
- **Manage volumes**. Allows you to show the volume management page that will allow you to attach and detach volumes for the selected instance.
- **Associate IP address**. Associates an elastic IP address with the selected instance.
- **Stop**. Stops the selected EBS-backed instance.
- **Start**. Starts the selected EBS-backed instance.
- **Reboot**. Reboots the selected EBS-backed instance
- **Terminate**. Terminates the selected instance.

  Note: A terminated instance cannot 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 provides the details of an instance.

Instance

This section allows you to view details about the instance. The name is the only attribute about the instance that can be edited.

- To rename the instance, type the new name of the instance in the **Name** text field.

Actions 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 option displays a dialog with instructions detailing how to connect to the selected instance.
- **Launch more like this**. Selecting this option displays 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 option displays the **Create new launch configuration** wizard.

  Note: For more information on Auto Scaling, see Using Auto Scaling in the *Eucalyptus User Guide*.
- **Create image**. Selecting this option allows you to create a new image. Refer to the Help on that page to complete the fields.
- **View console output**. Selecting this option displays a dialog box showing the selected instance's console output.
- **Associate IP address**. Selecting this option opens the volume management page that will allow you to attach and detach volumes for the selected instance.
- **Stop**. This option displays for only EBS-backed instances that are active. Select this option to stop the selected EBS-backed instance.
- **Start**. This option displays for only EBS-backed instances that are stopped. Select this option to start the selected EBS-backed instance.
- **Reboot**. Select this option to reboot the selected instance.
- **Terminate**. Select this option to terminate the selected instance.

  Note: A terminated instance can't be restarted.

Image

This section provides information about the image used for this instance.

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:

Add tags

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.
5. 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.

Instance Detail - Volumes

This tab allows you to view and manage the volumes attached to the selected instance. Also, it allows you to attach volumes to your instance.

1. To attach a volume to your instance, click the **Attach a volume** icon to access the **Attach volume** page.
2. Refer to the Help on the Attach volume page for additional instructions.

Volumes context menu actions

Each tile in the volume list has a context menu. Clicking the action icon (a row of three dots) 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 option to detach the selected volume from the instance.

Instance Details - Monitoring

This tab allows you to view and create alarms based on criteria you define, and provides a graphical view of various data points being monitored for your instance.

Alarms

This section displays a list of configured alarms and allows you to create a new alarm.

1. To view the details of currently configured CloudWatch alarms, expand it by clicking the plus symbol **(+)** next to the Cloudwatch alarms summary.
   The expanded view displays the state of each alarm, the alarm name, and their thresholds.
2. To create a new alarm you must first select a metric, unless you are within the scaling policy creation workflow:
   a) Click **Create Alarm**.
   An instructional message opens.
   b) Either close the message and view a metric from the Monitoring tab of any resource's Details page or click the **Take Me to the Metrics Landing Page** button to be taken directly to the Metrics page.
   c) Select a metric to view and click **Create Alarm**.
   The Create alarm page opens. Refer to the Help in the Create alarm page for further instructions.

Context menu actions

A context menu, accessible by clicking the menu icon (row of three dots), contains actions associated with the monitoring of your instance.

The following context menu actions are available:

- **Turn monitoring on** displays monitoring data associated with your instance.
- **Turn monitoring off** disables monitoring data completely.
  When you select this option, no charts display. Instead, a reminder that monitoring is currently turned off, but you can turn it back on by clicking the **Enable Monitoring for this Instance** button.

CloudWatch metrics

This part of the page displays the CloudWatch data when you enabled monitoring for your instance.

1. The graphs displayed by default are:
   - **CPU utilization %**. Represents the percentage of processing power currently in use by the instance.
   - **Disk read bytes**. The amount of data that is being read from the instance's hard disk.
   - **Disk read operations**. The number of read operations that has completed on all ephemeral disks available to the instance.
   - **Disk write bytes**. The amount of data that is being written to the instance's hard disk.

- **Disk write operations**. The number of write operations that has completed on all ephemeral disks available to the instance.
- **Network in**. The amount of incoming network traffic to an application on this instance.
- **Network out**. The amount of outgoing network traffic to an application on this instance.

Each of the graphs default to the *average* statistic for the best output results.

2. The various ways to view the data in the graphs are:
   - Click on a graph to expand it.
   - Hover inside the graph to display a read-out of data-points desired.
   - Use the drop-down list boxes for **Statistic**, **Show data for**, and **Measurement period** to focus in on specific set of data points. For example, to view the combined number of healthy hosts within the last hour in 5-minute readings, select **Sum** from **Statistic**, **Last hour** from **Show data for**, and **5 minutes** from **Measurement period**.

Launch a New Instance

This Wizard allows you to create a new instance.

Select an Image

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

1. There are two ways to specify a base image:
   - Select an image from the list of images on the panel.

     Note: You can filter the list of images by typing some text into the search text box to narrow down the list.
   - Type an image name directly into the **Enter an image ID** text box.
2. Click the **Next** button to proceed to the **Details** panel.

Launch a New Instance - Details

Details

This tab allows you to specify details of your instance(s), such as the instance type, availability zone of your new instance(s), if applicable; tags, and user data.

1. Enter the number of new instances to create in the **Number of instances** text box.

   Note: You may not launch more than 10 instances in a single security group.
2. You can optionally enter one or more names for your new instance(s) in the **Name(s)** text box(es).
3. Select an instance type from the **Instance type** drop-down list box.
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. To specify custom user data:
   - manually enter the data by selecting the **Enter text** option and typing the data into the provided text box.
   - attach a file by selecting the **Upload file** option then clicking the **Choose File** button to browse for the file.

7. Click the **Next** button to proceed to the **Security** tab.

Launch a New Instance - Security

Security

This tab 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. You may keep the security group already specified in the **Security group** field, add another one, or specify a different one.
   - To specify a different security group, remove the one there by clicking on the **x** next to the security group's name and add a new one by clicking in the **Security Group** field and choose one from the list of previously-defined security groups.

     Note: You can narrow down the list of security groups by typing text directly into the text box.
   - 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.
6. You can also create a new security group by clicking the **Create security group** link. This opens the Create Security Group dialog box.

   Note: You may view the rules for the specified security group(s) by clicking the **+ Rules** control next to each security group to expand it.
7. 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.
8. You can optionally specify advanced options by clicking the **Select advanced options** link and refer to the next section for further details.
9. Otherwise, click the **Launch instance** button.

Launch a New Instance - Advanced

Specify Advanced Options

This tab allows you to specify advanced options for your new instance. You can override the kernel and RAM disk IDs, enable monitoring, and add additional storage, if applicable.

1. You can override the kernel ID in the selected image with the **Kernel ID** drop-down list box.
2. You can override the RAM disk ID in the selected image with the **RAM disk ID (RAMFS)** drop-down list box.
3. Click the **Enable monitoring** check box to specify that detailed CloudWatch metric gathering should be enabled for your new instance(s).
4. For instances, click the **Use private addressing only** check box to assign only private IP addresses from the range of IP addresses in your subnet to your new instance(s).

   For more information, see Amazon EC2 Instance IP Addressing.

   Note: This option is not applicable to launch configurations.
5. 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 **Snapshot** drop-down list box.
d) Type the size of the attached storage in gigabytes into the **Size (GB)** text box.
e) The **DELETE ON TERMINATE** indicator shows that the attached storage is to be automatically deleted by default when the instance is terminated. This option is non-editable.

Note: The **DELETE ON TERMINATE** indicator is not applicable for launch configurations.

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.

Confirm Entries

1. Make sure to double-check your entries.
2. Click the **Launch Instance** button to launch your new instance(s) or click **Cancel** to abandon your changes.

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 existing instance.

1. Specify the number of new instances to launch in the provided text box.
2. You can optionally type the name(s) of your new instances in the **Name(s)** text box.

   The read-only information associated with your new instances are pre-populated based on the instance from which you selected to launch more instances.
3. 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.
4. 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.

5. You can optionally specify advanced options by clicking the + control next to Advanced to expand it and refer to the next section for further details.
6. Otherwise, click the **Launch Instance** button to launch your new instances or click **Cancel** to abandon your changes.

Specify Advanced Options

This panel allows you to specify advanced options for your new instance(s). You can override the kernel and RAM disk IDs, enable monitoring, and add additional storage, if applicable.

1. You can override the kernel ID in the selected image with the **Kernel ID** drop-down list box.
2. You can override the RAM disk ID in the selected image with the **RAM disk ID (RAMFS)** drop-down list box.
3. Click the **Enable monitoring** check box to specify that detailed CloudWatch metric gathering should be enabled for your new instance(s).
4. 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.
5. Click the **Launch Instance** button to launch your new instance(s) or **Cancel** abandon your changes.

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

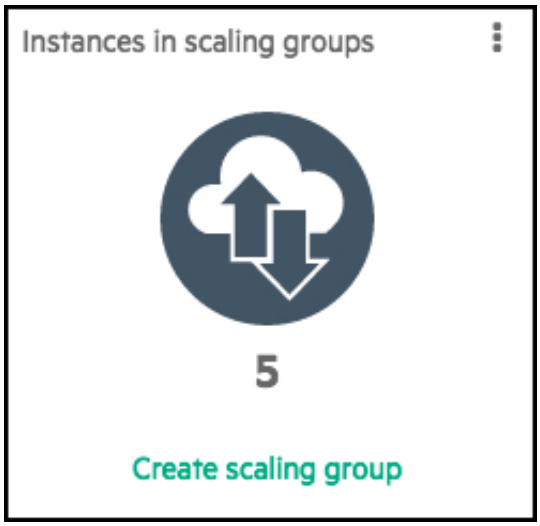
This section covers how to work with the auto scaling groups in the Eucalyptus Management Console.

Scaling Groups Landing Page

This page allows you to view a list of your scaling groups, create new scaling groups, and edit existing scaling groups. Use the scroll bar to view additional scaling groups not in the browser's current view.

Prerequisites

To access this page from the dashboard, click **Auto scaling groups** from the left navigation bar under **AUTO SCALING** or click the **Scaling groups** icon (cloud with up and down arrows) to display the **Scaling groups** landing page:



Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Create a New Scaling Group

1. From the dashboard, click **Create scaling group** beneath the Scaling groups icon.

   OR

2. From the **Scaling groups** landing page, click the **CREATE NEW SCALING GROUP** button near the top of the page.

The **Create new scaling group** wizard opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

From the dashboard, you can view details about the instances that are part of a scaling group by clicking on the number in the Instances in scaling groups tile.

View Details of a Scaling Group

Several items in the scaling groups list allow you to click on them to see more detailed information, such as name, launch configuration, and instances associated with it.

To see more details about a scaling group, or an object associated with it:

1. Click the name in the list of scaling groups to display detailed information about the selected scaling group, such as scaling capacity, scaling history, scaling policies, instances, and monitoring data.

   OR

2. In the Actions column, click the action icon (###) for the scaling group you want to view and select **View details**.

The details page for the selected scaling group opens.

3. Click a launch configuration to see to see detailed information about the launch configuration used for the selected scaling group.
4. Click the number under the Instances column to see detailed information about the instance(s) used in the scaling group.

Actions

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

The following context menu actions are available:

- **View details**. Brings up the scaling group detail page.
- **Monitor**. Opens the monitoring details that include information about CloudWatch alarms and metrics associated with that particular scaling group.
- **Manage instances**. Brings up a list of the instances in the auto scaling group that allows you to view details of each instance, mark them as unhealthy, or terminate them.
- **Manage policies**. Brings up a page that allows you to manage scaling policies for your auto scaling group, including the ability to delete them.
- **Delete scaling group**. Allows you to delete the selected scaling group.

Create a Scaling Group - General

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, 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 **name...** text box.

   Note: Tags cannot start with "`euca:`" or "`aws:`".
3. Type the value for your tag into the **value...** text box.
4. Click the **Add Tag** button.
5. If you wish to add additional tags, repeat the preceding steps.
6. To delete one or more tags, move your mouse over the tag you wish to delete, and click the **X** button.

Create a Scaling Group - Membership

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, see *Using Auto Scaling* in the *Eucalyptus User Guide*.

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 Zone(s)** field.
2. Select one or more load balancers for you new scaling group from the **Load balancer(s)** 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 (secs)** 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.

Advanced

This section allows you to specify whether to collect CloudWatch metrics for this scaling group.

Click the **Enable monitoring** check box to turn on the CloudWatch features for this scaling group and the instances it manages.

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, 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.

   Note: 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 launch configuration, VPC subnet(s), cooldown period, 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. To change the launch configuration, select a new one 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.
2. For VPC networks, the following options are available:
   a) You can add VPC subnets by selecting them from the **VPC subnet(s)** field.

      Note: 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.
   b) If a VPC network was associated with your scaling group, availability zones are view-only and are not editable. Otherwise, you can add availability zones by selecting them from the **Availability Zones** field.

      Note: You can remove a selected availability zone by clicking on the **x** next to the availability zone's name in the **Availability Zones** field.
3. The **Load balancer(s)** field lists all the load balancers associated with the scaling group.
4. You can change the amount of time after a scaling activity completes before any new scaling activity can start by editing the cooldown period, in seconds, in the **Default cooldown period (secs)** control.
5. 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.

   Note: The auto scaling health check uses EC2 instance status checks to determine the health state of each instance in your auto scaling group.

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 **name...** text box.

   Note: Tags cannot start with "`euca:`" or "`aws:`".
3. Type the value for your tag into the **value...** text box.
4. Click the **Add Tag** button.

5. If you wish to add additional tags, repeat the preceding steps.
6. 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 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.

Scaling Group Detail - Scaling History

This tab displays a running history of scaling activities occurring on the selected scaling group. All the information displayed is non-editable:

- Use the Magic search bar to filter the history data you want to view.

  Status is an criteria that can be specified, for example. Additionally, you can filter by typing in text similar to searching by keywords.

  You can also sort the table by most recent occurrences, or alphabetically by status or descriptor, by selecting an option from the **Sort by** drop-down menu.
- The **Status** column shows the state of the events associated with the selected scaling group.

  Possible states can be: Successful, In progress, Not yet in service, Failed, Canceled, Waiting for launch, and Waiting for terminate.
- The **Description** column describes the event associated with the selected scaling group. For example, the action associated with launching an instance within the scaling group is identified as its own event.
- The **Start Time** column shows the start time and date for which the event associated with the status occurred.
- The **End Time** column shows the time and date for which the event associated with the status completed.

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

Scaling Group Detail - Scaling Policies

This tab allows you to view and manage the policies applied to the selected scaling group. Also, it allows you to add scaling policies to your scaling group.

1. To apply a scaling policy to your scaling group, click the **+ ADD A SCALING POLICY** button to access the **Create scaling policy** page.
2. Refer to the Help on the Create scaling policy page for additional instructions.

Policies context menu actions

Each tile in the policy list has a context menu. Clicking the action icon (a row of three dots) in the upper right corner of a policy tile brings up a menu of actions that you can perform on the selected scaling policy.

The following context menu actions are available:

- **Delete policy**. Select this option to delete the selected policy from the scaling group.

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 tab allows you to view and manage the instances associated with the selected scaling group.

1. To manage instances (launch configurations) currently associated with your scaling group, click the link to the launch configuration inside the instance's tile to access its details page.
2. Refer to the Help on the Details for launch configuration page for additional instructions.

Instances context menu actions

Each tile in the instances list has a context menu. Clicking the action icon (a row of three dots) in the upper right corner of a policy tile brings up a menu of actions that you can perform on the selected instance.

The following context menu actions are available:

- **View details**. Select this option to view the details page for the selected instance.
- **Mark unhealthy**. Select this option to mark an instance as unhealthy. This will cause auto scaling to terminate the instance and launch a new instance to replace it.
- **Terminate**. Select this option to terminate the selected instance.

Scaling Group Details - Monitoring

This tab provides a graphical view of various data points being monitored for your scaling group.

Alarms

This section displays a list of configured alarms and allows you to create a new alarm.

1. To view the details of currently configured CloudWatch alarms, expand it by clicking the plus symbol **(+)** next to the Cloudwatch alarms summary.
   The expanded view displays the state of each alarm, the alarm name, and their thresholds.
2. To create a new alarm you must first select a metric, unless you are within the scaling policy creation workflow:
   a) Click **Create Alarm**.
   An instructional message opens.
   b) Either close the message and view a metric from the Monitoring tab of any resource's Details page or click the **Take Me to the Metrics Landing Page** button to be taken directly to the Metrics page.
   c) Select a metric to view and click **Create Alarm**.
   The Create alarm page opens. Refer to the Help in the Create alarm page for further instructions.

CloudWatch instance metrics

This part of the page displays the CloudWatch data when you enabled monitoring for your launch configuration(s).

If a launch configuration does not have monitoring enabled, no charts display. Instead, a reminder that monitoring is currently turned off for that particular launch configuration. To view CloudWatch metrics for this scaling group, change the scaling group's launch configuration from the General tab to enable instance monitoring.

1. To adjust the range of data to display, select a desired range from the **Show data for** drop-down list box. Any changes in the time range applies to both instance and scaling group metrics.
2. The graphs displayed by default are:

   - **CPU utilization %**. Represents the percentage of processing power currently in use by the instance.
   - **Disk read bytes**. The amount of data that is being read from the instance's hard disk.
   - **Disk read operations**. The number of read operations that has completed on all ephemeral disks available to the instance.
   - **Disk write bytes**. The amount of data that is being written to the instance's hard disk.
   - **Disk write operations**. The number of write operations that has completed on all ephemeral disks available to the instance.
   - **Network in**. The amount of incoming network traffic to an application on this instance.
   - **Network out**. The amount of outgoing network traffic to an application on this instance.

   Each of the graphs default to the *average* statistic for the best output results.
3. The various ways to view the data in the graphs are:

   - Click on a graph to expand it.
   - Hover inside the graph to display a read-out of data-points desired.
   - Use the drop-down list boxes for **Statistic**, **Show data for**, and **Measurement period** to focus in on specific set of data points. For example, to view the combined number of healthy hosts within the last hour in 5-minute readings, select **Sum** from **Statistic**, **Last hour** from **Show data for**, and **5 minutes** from **Measurement period**.

CloudWatch scaling group metrics

This part of the page displays the CloudWatch data when you enabled monitoring for your scaling group.

Context menu actions

A context menu, accessible by clicking the menu icon (row of three dots), contains actions associated with the monitoring of your scaling group.

The following context menu actions are available:

- **Turn monitoring on** displays monitoring data associated with your scaling group.
- **Turn monitoring off** disables monitoring data completely.
  When you select this option, no charts display. Instead, a reminder that monitoring is currently turned off, but you can turn it back on by clicking the **Turn Monitoring On For This Scaling Group** button.

Specify data range

You can specify a range in time to display the monitoring data shown in the graphs.

1. To adjust the range of data to display, select a desired range from the **Show data for** drop-down list box. Any changes in the time range applies to both instance and scaling group metrics.
2. The graphs displayed by default are:

   - **Total instances**. Represents the total number of instances currently in the scaling group, regardless of state.
   - **In service instances**. The number of instances currently in the scaling group that are in service (running and active).
   - **Group min size**. The smallest size of the scaling group.
   - **Group max size**. The largest size of the scaling group.
   - **Group desired capacity**. The number of instances the scaling group attempts to maintain.
   - **Pending instances**. The number of instances currently in the scaling group that are in pending state and not yet in service.
   - **Terminating instances**. The number of instances currently in the scaling group that are in the process of terminating.

   Each of the graphs default to the *Maximum* statistic within the last hour for the best output results.
3. The various ways to view the data in the graphs are:

   - Click on a graph to expand it.
   - Hover inside the graph to display a read-out of data-points desired.
   - Use the drop-down list boxes for **Statistic**, **Show data for**, and **Measurement period** to focus in on specific set of data points. For example, to view the combined number of healthy hosts within the last hour in 5-minute readings, select **Sum** from **Statistic**, **Last hour** from **Show data for**, and **5 minutes** from **Measurement period**.

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, 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 **Create Scaling 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, 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 trigger dimensions, if not already pre-populated with the selected resource such as an image or scaling group. A dimension is a name-value pair that uniquely identifies a metric; for example: "`Scaling group`" = "`myscalinggroup`".
4. When **Create Alarm** is launched from a resources' detail page, pre-defined metrics specific to those resources display. Select a metric from the 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 a statistic from the **Trigger alarm when the** drop-down list box. A statistic is computed aggregation of metric data over a specified period of time; valid values are average, minimum, maximum, sum, and data samples.
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 **for at least** and **consecutive period(s) of** areas 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.
   As you specify the values in this section, the chart that follows display the graphical representation of that statistic data.
9. In the **Actions** section of the Create alarm window, specify the action to be taken when an alarm is triggered.

   Note: This section does not display if creating alarms is launched from the create scaling policy workflow.

   a) The **Action type** is pre-populated with the resource activity associated with the alarm.
   b) Select the state you want the alarm to take action from the **When alarm state is** drop-down list box.
   c) If launched from a scaling group, the name of that scaling group displays as the default selection in the **For scaling group** drop-down list box. Select a different scaling group, if needed.

When a scaling group is selected, the **Execute scaling policy** drop-down list box displays with only the policies associated with the selected scaling group.

d) Choose a policy to execute from the **Execute scaling policy** drop-down list box.

Note: If there is already an action associated with this alarm, the policy selection is not applicable.

Note: If all scaling policies are already associated with actions, or there are none defined, the policy selection displays, "No policies available."

10. To save your new alarm, click the **Create Alarm** button.

For more details about CloudWatch alarm properties, see AWS Resource Types Reference for Alarms.

Work with Launch Configurations

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

Launch configurations Landing Page

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. Use the scroll bar to view additional launch configurations not in the browser's current view.

Prerequisites

As one of the resources not available as a tile on the dashboard, you can access a list of launch configurations by clicking **Launch configurations** from the left navigation bar under **AUTO SCALING**.

Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Create a New Launch Configuration

1. As one of the resources not available for access from the dashboard, access the Launch configurations landing page by clicking the **Launch configurations** link on the left side navigation bar under the AUTO SCALING category.
2. From the **Launch configurations** landing page, click the **CREATE NEW LAUNCH CONFIGURATION** button near the top of the page.

The **Create new launch configuration** wizard opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

View Details of a Launch Configuration

Several items in the launch configurations list allow you to click on them to see more detailed information, such as, name, image, key pair, and security group associated with each launch configuration.

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

1. Click the name of the launch configuration to display detailed information about the selected launch configuration.

   OR

2. In the Actions column, click the action icon (###) for the launch configuration you want to view and select **View details**.
   The details page for the selected launch configuration opens.
3. Click an image ID to see to see detailed information about the image associated with the selected launch configuration.
4. Click the name of a key pair to see to see detailed information about the key pair associated with the selected launch configuration.
5. 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 from 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:

- **View details**. Brings up the detail page for selected launch configuration.
- **Create launch configuration like this**. Opens the Create launch configuration page that is pre-populated with many of the same attributes as the selected launch configuration.
- **Use to create scaling group**. Opens the **Create new scaling group** wizard with the selected launch configuration pre-populated.
- **Delete launch configuration**. Allows you 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, see *Using Auto Scaling* in the *Eucalyptus User Guide*.

Select an Image

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

1. There are two ways to specify a base image:
   - Select an image from the list of images on the panel.

     Note: You can filter the list of images by typing some text into the search text box to narrow down the list.
   - Type an image name directly into the **Enter an image ID** text box.
2. Click the **Next** button to proceed to the **Details** panel.

Create Launch Configuration - Details

Details

This tab allows you to specify the name, instance size, and user data associated with the launch configuration.

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.
3. To specify custom user data:
   - manually enter the data by selecting the **Enter text** option and typing the data into the provided text box.
   - attach a file by selecting the **Upload file** option then clicking the **Choose File** button to browse for the file.
4. Click the **Next** button to proceed to the **Security** tab.

Create Launch Configuration - Security

Specify Security

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

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 launch configurations.

   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, You may view the rules for the specified security group by clicking the **+ Rules** control to expand it.
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 launch configurations.
5. The **Create scaling group using this launch configuration** check box 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.

Create Launch Configuration - Advanced

Specify Advanced Options

This tab allows you to specify advanced options for your new instance. You can override the kernel and RAM disk IDs, enable monitoring, and add additional storage, if applicable.

1. You can override the kernel ID in the selected image with the **Kernel ID** drop-down list box.
2. You can override the RAM disk ID in the selected image with the **RAM disk ID (RAMFS)** drop-down list box.
3. Click the **Enable monitoring** check box to specify that detailed CloudWatch metric gathering should be enabled for your new instance(s).
4. For instances, click the **Use private addressing only** check box to assign only private IP addresses from the range of IP addresses in your subnet to your new instance(s).

   For more information, see Amazon EC2 Instance IP Addressing.

   Note: This option is not applicable to launch configurations.
5. 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 **Snapshot** drop-down list box.
   d) Type the size of the attached storage in gigabytes into the **Size (GB)** text box.
   e) The **DELETE ON TERMINATE** indicator shows that the attached storage is to be automatically deleted by default when the instance is terminated. This option is non-editable.

      Note: The **DELETE ON TERMINATE** indicator is not applicable for launch configurations.

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.

Confirm Entries

1. The **Create scaling group using this launch configuration** check box 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.
2. Make sure to double-check your entries.
3. Click the **Create Launch Configuration** button to confirm or click **Cancel** to abandon your changes.

Create Launch Configuration from Instance

This page is accessed via the **Actions (...)** menu on the **Manage Instances** or **Instance Detail** page, and is pre-populated with values based on the selected instance that are not editable. A launch configuration is used to define the parameters for the new instances that are launched as part of your auto scaling group.

Name Your Launch Configuration

This panel allows you to enter a name for your new launch configuration. It also displays the platform, type, and keypair/security group for your launch instance; these values are derived from the instance you had selected in the **Manage instances** landing page and cannot be changed.

1. Type the name of your new launch configuration into the **Name** text box.
2. Specify custom user data by typing it into the **User data** text box or by attaching a file by clicking the **Choose file** button.
3. Click **Next** to proceed to the security options.

Specify Security Options

This panel allows you to specify network and security options for your new launch configuration.

1. If using this launch configuration 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. The security group is automatically chosen based on the instance from which you created this launch configuration. You may view the rules for the specified security group by clicking the **+ Rules** control to expand it.
3. 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 launch configuration.
4. 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.
5. You can optionally specify advanced options by clicking the **Select advanced options** link and refer to the next section for further details. Otherwise, click **Create Launch Configuration** to begin creating the launch configuration.

Specify Advanced Options

This panel allows you to optionally specify advanced options for the new launch configuration. You can override the kernel and RAM disk IDs, enable monitoring, and adding additional storage, if applicable.

1. You can override the kernel ID in the selected image with the **Kernel ID** drop-down list box.
2. You can override the RAM disk ID in the selected image with the **RAM disk ID (RAMFS)** drop-down list box.
3. Click the **Enable monitoring** check box to specify that detailed CloudWatch metric gathering should be enabled for your new launch configuration(s).

4. 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.
5. Click the **Create Launch Configuration** button or click **Cancel** to abandon your changes.

Create Launch Configuration Like This

This page allows you create another instance that has the same characteristics as an existing instance.

1. Enter the name of the new launch configuration into the **Name** text box.
2. Select the size and type for the instance from the **Instance type** drop-down list box.
3. If using this launch configuration 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.
4. Select a key pair from the **Key name** drop-down list box.
5. You may keep the security group already specified in the **Security group** field, add another one, or specify a different one.
   - To specify a different security group, remove the one there by clicking on the **x** next to the security group's name and add a new one by clicking in the **Security Group** field and choose one from the list of previously-defined security groups.

     Note: You can narrow down the list of security groups by typing text directly into the text box.
   - 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 launch configurations.
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 launch configurations.
7. 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.
8. 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.
9. You can optionally specify advanced options by expanding the **+** control next to Advanced and refer to the next section for further details.

10. Otherwise, click the **Create Launch Configuration** button to launch your new launch configurations.

Specify Advanced Options

This panel allows you to specify advanced options for your new launch configuration(s), such as overriding the kernel and RAM disk IDs, enable monitoring, and adding additional storage, if applicable.

1. You can override the kernel ID in the selected image with the **Kernel ID** drop-down list box.
2. You can override the RAM disk ID in the selected image with the **RAM disk ID (RAMFS)** drop-down list box.
3. Click the **Enable monitoring** check box to specify that detailed CloudWatch metric gathering should be enabled for your new launch configuration(s).
4. 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.
5. Click the **Create Launch Configuration** button to launch your new launch configuration(s).

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

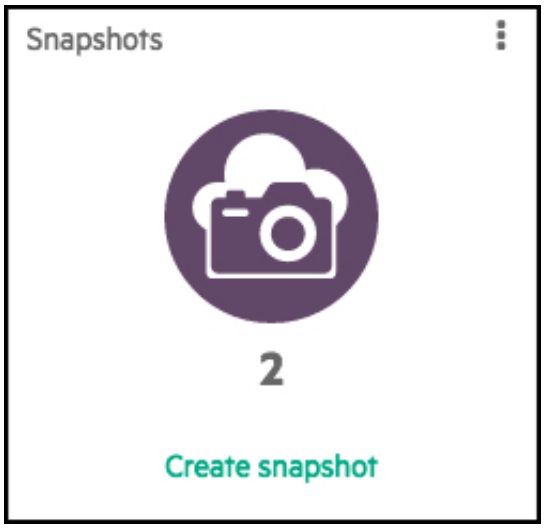
This section covers how to work with the snapshot dialogs and screens in the Eucalyptus Management Console.

Snapshots Landing Page

This screen allows you to view a list of your snapshots, create new snapshots, and delete snapshots. Use the scroll bar to view additional snapshots not in the browser's current view.

Prerequisites

To access this page from the dashboard, click **Snapshots** from the left navigation bar under **STORAGE** or click the **Snapshots** icon (cloud with camera) to display the **Snapshots** landing page:



Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Create a New Snapshot

1. From the dashboard, click **Create snapshot** beneath the Snapshots icon.

   OR

2. From the **Snapshots** landing page, click the **CREATE NEW SNAPSHOT** button near the top of the page.

The **Create new snapshot** page opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

View Details of a Snapshot

You can see details about a snapshot, such as its status, size, and the volume from which it was created.

To see more details about a snapshot:

1. Click the name in the list of snapshots to display detailed information about the selected snapshot.

   OR

2. In the Actions column, click the action icon (###) for the snapshot you want to view and select **View details**. The details page for the selected snapshot opens.

Actions

Each entry in the snapshots list has a context menu, accessible from 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**. Brings up the detail page for selected snapshot.
- **Create volume from snapshot**. Allows you to create a volume from the selected snapshot.
- **Register as image**. 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**. Allows you to delete the selected 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.

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:

Add tags

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.
5. 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.

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.

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:

Add tags

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.
5. 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.

Buckets Landing Page

This screen allows you to view a list of your buckets, create new buckets, and delete buckets. Use the scroll bar to view additional buckets not in the browser's current view.

Prerequisites

To access this page from the dashboard, click **Buckets** from the left navigation bar under **STORAGE** or click the **Buckets** icon (bucket symbol) to display the **Buckets** landing page:

Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Create a New Bucket

1. From the dashboard, click **Create bucket** beneath the Buckets icon.

   OR
2. From the **Buckets** landing page, click the **CREATE BUCKET** button near the top of the page.

The **Create new bucket** page opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

Shared Bucket

Shared buckets are in other accounts that you may or may not have access. If you do not have permissions to open a shared bucket, you may still have permissions to download objects from it or upload files to it.

1. To open a shared bucket:
   a) From the **Buckets** landing page, click the **OPEN SHARED BUCKET** button near the top of the page.
   The **Open shared bucket** dialog box opens.
   b) Enter the name of the bucket you want to access in the field provided.
   c) You may optionally choose to save this bucket to your own list of buckets to bookmark it for later, click the check box.
   d) Click **OPEN BUCKET** to open the bucket.

   Note: If you see a message that you don't have permissions to open the bucket or the bucket you entered does not exist. Check the name again, or contact the owner or administrator of the bucket to grant you permissions to the bucket.

   Note: If you chose to save the bucket to your list, the name of the bucket you entered displays on the list, whether or not you were successful gaining access to it. A shared bucket appearing on the list is denoted by a smaller bucket icon with a line under it.

   If access is allowed, the page for the shared bucket opens with a list of its objects.
2. To download an object from a shared bucket, you must know the object's full path:
   a) From the **Buckets** landing page, click the down arrow next to the **OPEN SHARED BUCKET** button near the top of the page.
   b) Select **Download Object**.
   The **Download object** dialog box opens.
   c) Enter the full path of the object, including the name of the bucket you want to access in the field provided.
   d) Click **DOWNLOAD OBJECT** to download the object.

   Note: If you get an error message that the object cannot be retrieved, check the names again, or contact the owner or administrator of the bucket to grant you the proper permissions.

   If access is allowed, the object downloads to your designated folder.
3. To upload an object to a shared bucket, you must specify a folder in the shared bucket:
   a) From the **Buckets** landing page, click the down arrow next to the **OPEN SHARED BUCKET** button near the top of the page.
   b) Select **Upload Object(s)**.
   The **Upload object(s)** dialog box opens. For additional information on completing that page, refer to the instructions provided in its Help content.
4. To delete a shared bucket from your Buckets list:
   a) From the **Buckets** landing page, locate a shared bucket by its smaller bucket icon with a line under it.
   b) In the Actions column, click the action icon (###) for the shared bucket you no longer want to display and select **Remove from view**.

View Details of a Bucket

The most important detail about a bucket is the objects it contains.

To view the objects in a bucket from the Buckets landing page:

1. Click a bucket from the Name column or click a number from the Objects column of the bucket you want to view.
   OR
2. In the Actions column, click the action icon (###) for the bucket you want to view and select **View contents**.
3. To view details of the bucket itself:
   a) From the Buckets landing page, click a name in the list of buckets.
   b) In the selected bucket's page, click **View details** near the top of the page, next to the bucket's name.
   OR

c) From the Buckets landing page, click the action icon (###) from the Actions column of the bucket you want to view and select **View details**.

Actions

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

The following context menu actions are available:

- **View contents**. Brings up a list of objects associated with selected bucket.
- **View details**. Brings up the detail page for selected bucket.
- **Delete**. Allows you to delete the selected bucket.

  Note: You cannot delete a bucket unless it is empty. To delete a bucket, you must first delete all the folders and files the bucket contains.

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. Use DNS-compliant bucket names regardless of the region in which you create the bucket. For more information on bucket naming conventions, go to AWS Bucket Restrictions and Limitations.
2. Click the **Create Bucket** button to create your new bucket, or click the **Cancel** button to cancel the operation. The Bucket Details page for your newly created bucket opens. 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 and a link to its contents.

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.

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 associated with bucket Access Control Lists (ACLs):

   Note: For more information about ACLs, see Manage Walrus Resources in the *Eucalyptus Administration Guide*.

   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. To edit the settings associated with Cross-Origin Resource Sharing (CORS):

   a) If a CORS has already been configured, you can:

      - view or edit, by clicking on the pencil icon, or
      - delete it by clicking the remove icon (#) next to the configuration

   b) Otherwise, if a CORS has not been configured, click the **Add CORS Configuration** button.
   A dialog box opens with an XML template of a basic CORS configuration that you can edit.

   c) Edit the values of the existing configuration, or create a new one.

      Note: For more information about CORS, see Working with CORS in the *Eucalyptus Console Guide*.

   d) To add the configuration, click the **Save CORS Configuration** button.
   Upon successful creation, the configuration displays below the CORS Configuration settings.

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

Working with CORS

Cross-Origin Resource Sharing (CORS) allows client web applications that reside in one domain to interact with resources in a different domain, within the same bucket.

Eucalyptus supports creating (enabling), getting, and deleting a CORS configuration on a bucket. An authenticated user who owns a bucket, can do the following:

- Use the `PUT` command to enable CORS, with a valid CORS configuration, to allow sharing across other domains.
- Use the `GET` command to obtain a CORS configuration, if one exists.
- Use the `DELETE` command to disable CORS to forbid sharing across other domains.

In the above scenarios, the equivalent operations in the Eucalyptus Management Console can be found in the sharing settings of a bucket:

- **Add CORS Configuration** to enable CORS within that bucket.
- **View/Edit** to obtain a CORS configuration and modify it.
- **Delete CORS Configuration** to disable CORS within that bucket.

For more information about CORS in AWS, such as creating different rules, go to AWS Cross-Origin Resource Sharing (CORS).

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 GB.
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 Objects

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

Objects List Page

The objects list page allows you to view a list of all the objects in a bucket or folder, upload and download objects, copy and delete objects or folders, create folders, manage permissions, view details, and make public on selected objects. Use the scroll bar to view additional objects not in the browser's current view.

Prerequisites

To access this page, you must first access a bucket or folder. In order to access a folder, you must first access a bucket. Each bucket or folder displays a list of objects, such as files or folders it contains. The objects list page is identified by the name of the bucket or folder that the objects reside.

Note: To access a bucket, see bucket access prerequisites.

Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Manage Object(s)

Objects can be uploaded, downloaded and deleted from a bucket or folder.

1. To upload an object to a bucket or folder:
   a) From the list of objects page or from a folder, click the **UPLOAD OBJECT(S)** button near the top of the page.
   The **Upload object(s)** dialog box opens. For additional information on completing that page, refer to the instructions provided in its Help content.
2. To download an object from a bucket or folder:
   a) From the list of objects page or from a folder, locate the object or file you want to download.
   b) In the Actions column, click the action icon (###) for the object you want to download and select **Download**.

      Note: If you get an error message that the object cannot be retrieved, check the names again, or contact the owner or administrator of the bucket or folder to grant you the proper permissions.

      If access is allowed, the object downloads to your designated folder.
3. To delete an object from a bucket or folder:
   a) From the list of objects page or from a folder, locate the object or file you want to delete.
   b) In the Actions column, click the action icon (###) for the object you want to delete and select **Delete**.
   The **Delete object** confirmation dialog box opens.
   c) Click **Yes, delete object** to confirm the deletion of the object from the bucket or folder.

      Alternatively, you can delete all objects and files in a bucket or folder at once. To do so, click the **DELETE ALL OBJECTS/FOLDERS** button near the top of the page. A confirmation dialog box opens to confirm the deletion.

For more information on folders, see the subsequent sections on how to create a folder, paste an object, and folder options.

Manage Folders

You can create folders to organize objects and files. You can upload files and objects to folders, or place copied files into a folder. You can create folders within buckets or within other folders.

Create a Folder

To create a folder:

1. From the list of objects page, click the down arrow next to the **UPLOAD OBJECT(S)** button near the top of the page.
2. Select **Create Folder**.
   The **Create new folder** dialog box opens.
3. Enter the name of the new folder in the field provided.
4. Click the **CREATE FOLDER** button.
   If access is allowed, the newly created folder displays as a folder icon in the list of objects of the selected bucket or folder.

Paste an Object/File

You can place a copy of any object, such as a folder or a file into a folder.

To paste an object/file to a folder:

1. From the list of objects page, locate the object/file you want to copy.
2. In the Actions column, click the action icon (###) for the object/file you want to copy and select **Copy**.
3. Navigate to a folder you want to paste the copied object/file and select the folder.
4. Click the paste icon button near the top of the page:

   The folder shows the pasted object/file in the list.

Folder Options

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

The following context menu actions are available:

- **View contents**. Brings up a list of objects associated with selected folder.
- **Copy folder**. Allows you to make a copy of the selected folder and paste the object into another bucket or folder.
- **Paste object**. Allows you to paste a copied object directly in the selected folder without opening it.
- **Delete**. Allows you to delete the selected folder and all its contents.

View Details of an Object

You can see details about an object, such as its last modification time and date, the link to the file, and any metadata or permissions assigned to it.

To view the details of an object:

1. From the list of objects page, locate the object or file you want to view.
2. In the Actions column, click the action icon (###) for the object you want to view and select **View details**. The Details page for the selected object opens. For additional information on viewing or editing the information on that page, refer to its Help content.

Actions

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

The following context menu actions are available:

- **View details**. Brings up the detail page for selected object.
- **Manage permissions**. Allows you to view and edit the permissions of the selected object.
- **Download**. Allows you to download the selected object to a designated folder.
- **Make public**. Allows any user to view and download the selected object, as long as they have the object's URL. These users are not required to be authenticated with the cloud.
- **Copy object**. Allows you to make a copy of the selected object and paste the object into another folder.
- **Delete**. Allows you to delete the selected object.

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.

Work with Images

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

Images Landing Page

This screen allows you to view a list of your images and launch a configuration from an image. Use the scroll bar to view additional images not in the browser's current view.

Prerequisites

As one of the resources not available as a tile on the dashboard, you can access a list of images by clicking the **IMAGES** menu selection icon (power symbol) from the left navigation bar:

Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.

- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

View Image Details

You can see details about an image, such as its status, EMI name, and the platform it runs on.

To see more details about an image:

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

   OR

2. In the Actions column, click the action icon (###) for the snapshot you want to view and select **View details**. The details page for the selected image opens.

Actions

Two Action operations are available from the Images landing page:

- The **More Actions** button
- The action icon (###)

1. The **More Actions** button above the list of images has a context menu that allow you to apply an action to a particular image or multiple images.
   a) Select one image and the **View details**, **Launch instance**, and the **Create launch configuration** options are available.
   b) Select multiple images from the list and depending on the circumstances of all the selected images, some options may be available and not others:
      - The **Remove from cloud** option is only available if the logged-in account/user is the owner of the image(s).
      - If all the selected images are in the process of being created, the **Cancel image creation** option is available
      - If the selected images are in different states, no options may be available.
2. Each entry in the images list has a context menu, accessible from the **Actions** column. Clicking the action icon brings up a menu of actions that you can perform on the selected image:
   a) **View details**. Brings up the detail page for selected image. This option is available whether the image is available or in the process of being created.
   b) **Launch instance**. This option is only available if the image is available. Opens the **Launch new instance** wizard that allows you to launch an instance using the selected image.
   c) **Create launch configuration**. A launch configuration is used to define the parameters for new images that are launched as part of an auto scaling group. This option is only available if the image is available. Selecting this option opens the **Create new launch configuration** wizard.

      Note: For more information on Auto Scaling, see *Using Auto Scaling* in the *Eucalyptus User Guide*.
   d) **Cancel image creation**. Cancels any images that are in the process of being created (status "pending").
   e) **Remove from cloud**. This option is used to clean up images that are no longer needed. Once removed, an image becomes de-registered but can be re-registered if its snapshot has not been deleted. This option is only available if the image is available. Selecting this option displays the **Remove image from cloud** confirmation dialog box.

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, 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.

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:

Add tags

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.
5. 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.

   Note: The admin user will be created automatically for each account as part of the account creation, and therefore, adding it manually is not allowed.
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.

   Note: The admin user cannot be deleted.
4. Select one or both options to apply to all the users you want to create, including the admin user:
   - **Create and download random password**.
   - **Create and download access keys**.

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, you can specify a path for the new user in the **Path** text box field.

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, go to 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 the **Add Policy** button to bring up the **Add Access Policy** page.

Delete a policy

To delete a policy:

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

View/edit a policy

To view or edit a policy:

Click 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 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 - 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. **Note:** The admin user will be created automatically for each account as part of the account creation, and therefore, adding it manually is not allowed.

   You can optionally create additional users for this account by entering them in the Add a user text field, then click **Add User**.
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.

   Note: The admin user cannot be deleted.
4. Select one or both options to apply to all the users you want to create, including the admin user:
   - **Create and download random password**.
   - **Create and download access keys**.
5. 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.

Work with Stacks

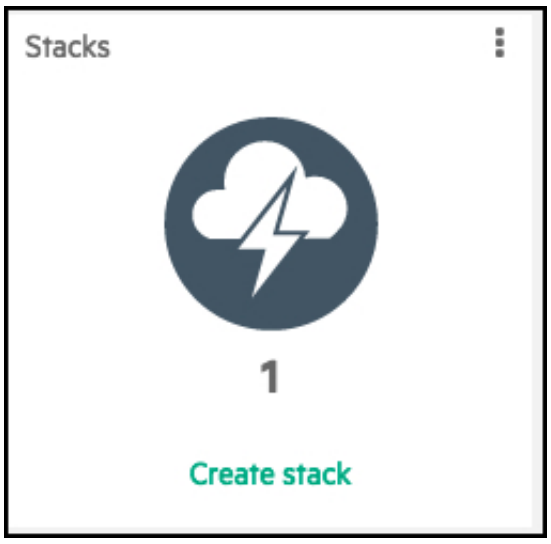
This section covers how to work with stacks (CloudFormation) in the Eucalyptus Management Console.

Stacks Landing Page

This screen allows you to view a list of your CloudFormation stacks, create new stacks, update existing stacks, and delete stacks. Use the scroll bar to view additional stacks not in the browser's current view.

Prerequisites

To access this page from the dashboard, click **Stacks** from the left navigation bar under **CLOUDFORMATION** or click the **Stacks** icon (cloud with lightning bolt) to display the **Stacks** landing page:



Change the Information Displayed

A variety of ways to display information is available from this page.

You can use the search feature to display only information important to you; and use the sort and views to manipulate how the information is displayed:

- **Change 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.
- **Sort the list**. In the table view, sort the list by name using the arrow icon next to the **NAME** column to toggle between ascending and descending sort order.
- **Search and filter**. To perform a simple search/filter, type some search text into the search text box above the list.

Create a New Stack

1. From the dashboard, click **Create stack** beneath the Stacks icon.

   OR

2. From the **Stacks** landing page, click the **CREATE STACK** button near the top of the page.

The **Create new stack** page opens.

For additional information on completing that page, refer to the instructions provided in its Help content.

View Details of a Stack

You can see details about a stack, such as its status, the resources associated with it, templates used, and events associated with it.

To see more details about a stack:

1. Click the name in the list of stacks to display detailed information about the selected stack.

   OR

2. In the Actions column, click the action icon (###) for the stack you want to view and select **View details**.
   The details page for the selected stack opens. For further information about the details page, refer to its Help content.

Actions

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

The following context menu actions are available:

- **View details**. Brings up the detail page for selected stack.

- **Update stack**. Allows you to update the selected stack.
- **Delete stack**. Allows you to delete the selected stack.

Create a Stack - General

This page allows you to create a CloudFormation stack. Combining resources into a stack allows you to create and delete them as a single unit.

General

Specify basic information about your stack in this section.

Type the name of your new stack in the **Name** text box.

Names are unique per account and region, but may be reused once a stack is deleted.

Note: If the name you enter is not valid, refer to the rules for naming that appears below the text box.

Template

Specify a template to apply to your stack.

1. Choose among the available options for applying a template:
   - Select **Use sample template** to choose from a list of pre-made templates.
   - Select **Upload template** to browse and apply a template from your local hard drive.

     Note: Acceptable file formats are JSON files (max size: 460,800 bytes). For more information, go to Template Anatomy in the *AWS CloudFormation User Guide*.
   - Select **Use template from URL** to choose a template from a web address.

     Note: The URL must point to a template (max size: 460,800 bytes) anywhere publically available that you have read permissions to, located in the same region as the stack. The maximum length of the URL itself is 1024 characters long.

   A Warning dialog opens if you are trying to use a template that was not originally designed for this cloud (for example, using an AWS template on a Eucalyptus cloud). Based on the information provided on the Warning dialog, you can either:

   - Expand **Details** to convert unsupported parameters
   - Click the **I Understand, Use This Template** button and all the unsupported parameters will convert automatically
   - Click **Go back, I want to select a different template** to discard the current template selection and repeat the above steps to choose another template
2. If you are trying to use an AWS template that contains services and resources that Eucalyptus does not yet support, a Warning dialog box opens.
   a) Click to expand **Details** to view the unsupported items.
   Any remaining unsupported items will be automatically removed.
   b) Once the chosen template is free of incompatible items, click **I Understand, Use This Template** to proceed.
3. To apply tags, proceed to the next section. Otherwise, click **Next** to proceed to the Parameters tab.

Add tags

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.
5. To delete one or more tags, move your mouse over the tag you wish to delete, and click the **X** button.

Create a Stack - Parameters

This section allows you to specify values for the parameters defined in the template you chose in the previous tab. With parameters, you can create templates that are customized each time you create a stack.

1. For each parameter listed, if not already populated with default values, you must provide a valid value to define the characteristic(s) you want the stack to have.

   Note: Hover over the **(?)** for more information about each parameter.

   Note: Some parameters require a value that is pulled from another resource. If not available, create the resource it needs to proceed.

   Note: Some parameters allow you to enter values in the provided text box while other parameters, you must select a valid value from the provided drop-down list box.

   Note: If there is a single resource available in the drop-down list box for a parameter, that value will be pre-selected.

   The entries for each parameter populate in the **Summary** panel on the right side of the screen.
2. To save your entries and proceed with creating the stack, click the **Create Stack** button.
   The stack is successfully created when the Stack Detail window opens, displaying a banner across the top of the new window stating, `Successfully sent create stack request. It may take a moment to create the stack` and the status of the newly-created stack shows `Create in progress`. When the stack is fully created, the status changes to `Create complete`.
3. Refer to the Help in the Stack Detail page for instructions associated with that page.

Update a Stack - Template

This page allows you to update the template and parameters of a CloudFormation stack.

Template

This page allows you to edit the currently applied template, upload a new one, or choose another one from a URL.

1. Choose among the available options for editing a template:

   - Select **Use current template** and click the pencil icon to edit the currently applied template. Another window opens to allow you to edit the contents of the template. When you are done editing, click the **SAVE TEMPLATE** button.
   - Select **Upload template** to browse and apply a different template from your local hard drive.

     Note: Acceptable file formats are JSON files (max size: 16 KB). For more information, go to Template Anatomy in the *AWS CloudFormation User Guide*.
   - Select **Use template from URL** to choose a different template from a web address.

     Note: The URL must point to a template (max size: 460,800 bytes) anywhere publically available that you have read permissions to, located in the same region as the stack. The maximum length of the URL itself is 1024 characters long.

   A Warning dialog opens if you are trying to use a template that was not originally designed for this cloud (for example, using an AWS template on a Eucalyptus cloud). Based on the information provided on the Warning dialog, you can either:

   - Expand **Details** to convert unsupported parameters
   - Click the **I Understand, Use This Template** button and all the unsupported parameters will convert automatically
   - Click **Go back, I want to select a different template** to discard the current template selection and repeat the above steps to choose another template
2. If you are trying to use an AWS template that contains services and resources that Eucalyptus does not yet support, a Warning dialog box opens.
   a) Click to expand **Details** to view the unsupported items.
   Any remaining unsupported items will be automatically removed.

b) Once the chosen template is free of incompatible items, click **I Understand, Use This Template** to proceed.

3. If you edit a template and it passes validation, the next tab automatically opens. Otherwise, click the **Next** button to advance to the Parameters tab.

Update a Stack - Parameters

This section allows you to edit the values for the parameters previously defined in the template used in your stack.

1. You can edit any of the parameters listed. Each parameter shows the currently selected value. You can change any of these values, as needed.

   Note: Hover over the **(?)** for more information about each parameter.

   Any changes you make update in the **Summary** panel on the right side of the screen accordingly.

2. To proceed with the changes, click the **Update Stack** button.
   The stack is successfully updated when the Stack Detail window opens, displaying a banner across the top stating, `Successfully sent update stack request. It may take a moment to update the stack.` and the status shows, `Update in progress`, followed by `Update complete cleanup in progress`. When the stack is fully updated, the status changes to `Update complete`.
3. Refer to the Help in the Stack Detail page for more information about that page.

Stack Detail - General

This page allows you to view details and delete the stack.

General tab

The General tab displays a variety of information about the stack. All the information in this window is non-editable.

- The **Stack** section shows the name of the stack, the ID associated with the stack, when it was created, its current status, and a reason why it is in its current state.
- The **Tags** section shows up to 10 user-defined tags to associate with this stack, represented by key/value pairs. Tags defined for the stack are propagated to EC2 resources that are created as part of the stack.
- The **Outputs** section displays the resulting values, or outputs from the template.
- The **Resources** section lists the various resources used in the stack, such as auto scaling groups, security groups, load balancers, launch configurations, and so on. Each resource is identified by its logical and physical ID, its current status and how it got there.

Actions menu

Clicking the down arrow from the **Actions** menu allows you to delete the stack.

Delete a stack

To delete a stack:

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

Stack Detail - Template

Template tab

The Template tab displays information about the template used to create the stack.

- The **Template** section provides a description of the template used to create the stack.
- The **Parameters** section displays the set of values provided when creating the stack that match the parameters defined in the template.

Stack Detail - Events

Events tab

The Events tab lists each event that took place in creation of a stack.

- Use the Magic search bar to filter the events you want to view.

  Status is an event criteria that can be specified. Additionally, you can filter by typing in text similar to searching by keywords.
- The **Timestamp** column shows the date and time in which the event associated with the status occurred.
- The **Status** column shows the current state of a particular resource applied to the stack. For example, the action associated with establishing a load balancer for the stack is identified as its own event.
- The **Status Reason** column shows any reason for an exception of an event to occur on a particular action made on the stack.
- The **Type (Logical ID)** column shows the type of resource created that triggered the event.
- The **Physical ID** column provides an active link (if available) to the resource created that triggered the event.

Work with Load Balancers

This section covers how to work with Load Balancers in the Eucalyptus Management Console.

Create Load Balancer - General

This wizard allows you to create a new load balancer. A load balancer allows you to automatically balance incoming traffic among a predefined group of instances, ensuring that requests are sent to an instance that has the capacity to serve them. For more information on load balancers, see *Using Elastic Load Balancing* in the *Eucalyptus User Guide*.

General

This section is where you specify the basic configuration of your new load balancer.

1. Type the name of your load balancer in the **Name** text box.
2. Define listener(s) for your load balancer.
   A listener checks the connection requests from the client to the load balancer (client-side) and ports that the load balancer uses to monitor and route incoming traffic to the load balancer's registered instances (instance-side). A default listener is pre-defined with an HTTP protocol port 80 on the client and the instance side. You may delete a listener but you must define at least one listener to properly configure a load balancer.

   To delete a listener, click the **Remove listener** icon (a minus sign in a circle) next to the one you want to remove.

   a) To add a listener, scroll past the table (if a listener is already defined) and select an option from the **Protocol** drop-down list box for the CLIENT SIDE.
      The client-side port may be populated with a common default port for a chosen protocol but you can change the port, if neccessary.
   b) If not already populated, or you want to change the client-side port, enter the port number in the **Port** text box.

      Ports assigned for the client-side must be either 25, 80, 443, 465, 587 or from 1024 to 65535 and may not already be in use.
   c) On the INSTANCE SIDE, select the protocol from the **Protocol** drop-down list box.
   d) If not already auto-populated, enter the number of the instance-side port into the **Port** text box.

Security Policy

The ability to apply a security policy is only available if HTTPS or SSL is specified as the protocol.

1. The latest existing security policy is displayed by default next to Policy in the Security area but you may change it by clicking **Change**.
   The Select security policy window opens.
2. Select from the available security options:

   - **Choose a predefined security policy** and select a policy from the **Policy name** drop-down list box.

   Note: For more information on pre-defined security policies, go to AWS Predefined SSL Security Policies for Elastic Load Balancing

OR

- **Create a custom security policy**. Choosing this option opens the **SSL PROTOCOLS** and the **SSL CIPHERS** drop-down list box with values pre-populated.

a) To delete any of the pre-populated values, click the **x** next to the value(s) you do not want.
b) To add or select another protocol, click in the **SSL PROTOCOLS** field and select one from the drop-down list box.
c) To add or select another encryption algorithm, click in the **SSL CIPHERS** field and select one from the drop-down list box.

Note: You must specify at least one protocol and one encryption algorithm.

d) In the SSL OPTIONS, click to select **Server order preference** if you want it for SSL negotiation.
e) Click the **Use This Policy** button to select the defined security policy.
The Select security policy window closes and the specified policy is displayed next to the Policy field.

Certificate

The ability to apply a security certificate is only available if HTTPS or SSL is specified as the protocol.

1. **Note:** Skip this step if you want to continue using a certificate that is already installed on your load balancer.

   To select a certificate, if available, click **Select** next to Certificates.
2. If a certificate is already assigned and you want to change it, click **Change** instead.
   Choosing this option opens the Select certificate(s) window.

   Note: Tabs display for SSL and Backend only if the instance side uses HTTPS or SSL protocol.
3. Select from the available options for assigning a certificate to your load balancer:

   - **Choose an existing SSL certificate** from the **Certificate Name** drop down list, if available.

     Note: If one is not available, upload a new certificate.
   - **Upload a new SSL certificate**. Choosing this option opens a form to upload a new certificate:

   a) Type the name of the new certificate in the **Certificate name** text field.
   b) Paste the contents of your public key certificate file in the **Public key certificate** text field. Refer to the bubble help **(?)** for additional details.
   c) Paste the contents of your private key certificate file in the **Private key** text field. Refer to the bubble help **(?)** for additional details.
   d) Enter the contents of your certificate chain file in the **Certificate chain** text field.
   e) To specify certificates for the backend, click the **Back end** tab. Otherwise, click the **Use This Certificate** button.
   Choosing to specify the backend certificate(s) opens another form that may already be populated with pre-loaded certificates.

   Note: Backend certificates are used to ensure added security measures between your load balancers and its communication with your server. Backend certificates are optional, but you may add multiple certificates on this form.

   f) To delete any of the pre-populated certificates, click the **x** next to the cetificate(s) you do not want.
   g) To add or select another certificate, click **Add a certificate** or **Add another certificate**, respectively.
   h) Type the name of the new certificate in the **Certificate name** text field.
   i) Paste the contents of your certificate file in the **Body (pem encoded)** text field.
   j) Click the **Add Certificate** button to add it.
   k) Click the **Use These Certificates** button to apply the certificates to your load balancer.
   The Select certificate(s) window closes and the specified certificate(s) is displayed next to the Certificates field.
   l) After listeners have been declared, click the **Add Listener** button to continue.
   The entries for your new load balancer is recorded in the Summary panel located on the right side of the screen.

m) To add more listeners, repeat the above steps.

4. To apply tags, proceed to the next section. Otherwise, click **Next** to proceed to the Network & Security tab.

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:

Add tags

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.
5. To delete one or more tags, move your mouse over the tag you wish to delete, and click the **X** button.

Create Load Balancer - Network and Security

This tab is present for all AWS clouds and Euca VPC-enabled clouds only. This step allows you to define a VPC network and assign a security group to your load balancer.

1. Select the name of the VPC from the **VPC network** drop-down list.

   For a non-VPC AWS cloud, select **No VPC**.

   The Security groups option displays if a VPC network is selected.
2. Select a security group to assign to the network from the **Security groups** drop-down list.
3. Click **Next** to proceed to the Instances tab.

Create Load Balancer - Instances

This step allows you to associate availability zones (or VPC subnets, if cloud is VPC) and add instances to your new load balancer. Adding availability zones allows the load balancer to route traffic to instances in the selected zone(s). Similarly, if on a VPC network, adding a VPC subnet allows traffic to instances in the selected VPC subnet(s).

1. Click the **Add availability zones** or **Add VPC subnets** text field to search and select a zone or subnet from the drop-down list. Repeat to add more availability zones or subnets.
2. The ability to select **Enable cross-zone load balancing** is only present for a load balancer not on a VPC network. This option evenly distributes traffic across all instances in all availability zones.
3. Select from the list of instances to specify between which instances to balance traffic.

   You may use the Magic Search bar to narrow down the list of instances by specifying the availability zone (or VPC subnet), security group, or status.

   Selecting an instance automatically adds that instance to the availability zone or VPC subnet field above and the number of instances selected is reflected in the **Summary** pane on the right side of the screen.
4. Click **Next** to proceed to the Health Check & Advanced tab.

Create Load Balancer - Health Check & Advanced

This wizard allows you to specify the various health checks you want your load balancer to monitor. Any instances that fail the health check will be automatically removed from the load balancer.

1. Specify the settings for pinging your instances:
   a) Select a protocol from the **Protocol** drop-down list.
   b) Enter the port in the **Port** text field.

The port may be populated with a common default port for a chosen protocol but you can change the port, if neccessary.

c) For http or https protocols, you may enter the path of the ping in the **Path** text field.

TCP and SSL protocols do not display this field.

2. Optionally, you can click **Advanced** to expand the health check timing options.
3. Enter the time in seconds in the **Response timeout (secs)** text field to specify how long to wait for a ping response before it times out.
4. Select the desired ping interval from the **Time between pings** drop-down list.
5. Specify the thresholds for declaring the health of instances:
   a) Select the number of failed attempts from the **Failures until unhealthy** drop-down list before declaring an instance unhealthy.
   b) Select the number of successful attempts from the **Passes until healthy** drop-down list before declaring an instance healthy.
6. Specify information about the logs generated from the health check activities:
   a) Click to select **Enable logging** to turn on the logging feature.

   If left unchecked, the logging feature is disabled and you do not have the ability to specify any information about your log outputs.

   Checking the box opens a logging permissions window and displays additional fields below. The Enable Bucket Access for Logging window prompts for user confirmation to proceed.

   b) Click **I Understand, Enable Access Logging** to continue.
   c) Specify a bucket to store your logs by selecting one from the **Bucket name** drop-down list or click **Create bucket** to create a new bucket for storing the logs.
   If creating a new bucket, the Create bucket window opens and prompts for a name.

   Note: Upon clicking **Create Bucket**, the system validates the name of the new bucket to ensure it is unique and not already in use. It is very important that each bucket has a unique name across the cloud.

   d) Using all lowercase characters, you may optionally enter the path in the **Prefix** text field to specify the path within the bucket to store your log files.

   If the path is not specified, the location defaults to the bucket's root level.

   The recommended default interval for capturing logs is pre-populated but you may change it, if necessary.

   e) To change the interval, select another one from the **Collection interval** drop-down list.

   If health check criteria were specified and logging is enabled, they are reflected in the **Summary** pane on the right side of the screen.
7. Click **Create new load balancer**.
   The message, `Successfully created elastic load balancer` *`[name]`* indicates a successful creation of the load balancer.

Load Balancer Details - General

This tab allows you to view details about the load balancer and edit or add listeners, if necessary.

Actions menu

Clicking the down arrow from the **Actions** menu allows you to delete the load balancer.

Delete a load balancer

To delete a load balancer:

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

Load balancer

This section shows the name, the creation time and the source security group associated with the load balancer. A special source security group is used to ensure back-end instances only receive traffic from your load balancer and is

a non-editable entity. The only value you may change is the amount of time a connection to an instance can be idle before timing out. To change the idle timeout, type a new value in the **Idle timeout (secs)** control or use the up and down arrows to adjust the values incrementally.

Listeners

This section shows what listeners are currently assigned to the load balancer, but you may add more or edit one by deleting it and adding a new listener. A listener checks the connection requests from the client to the load balancer (client-side) and ports that the load balancer uses to monitor and route incoming traffic to the load balancer's registered instances (instance-side). A default listener is pre-defined with an HTTP protocol port 80 on the client and the instance side. You cannot edit the protocol or port associated with the listener. However, you may delete a listener and re-add a new one with a different protocol or port.

1. To delete a listener, click the **Remove listener** icon (a minus sign in a circle) next to the one you want to remove.

   Note: You may delete a listener but you must define at least one listener to properly configure a load balancer.
2. To add a listener, scroll past the table (if a listener is already defined) and select an option from the **Protocol** drop-down list box for the CLIENT SIDE.
   The client-side port may be populated with a common default port for a chosen protocol but you can change the port, if neccessary.

   Note: Ports assigned for the client-side must be either 25, 80, 443, 465, 587 or from 1024 to 65535 and may not already be in use.
3. On the INSTANCE SIDE, select the protocol from the **Protocol** drop-down list box.
4. If not already auto-populated, or to change it, enter the number of the instance-side port into the **Port** text box.

Security Policy

The ability to apply a security policy is only available if HTTPS or SSL is specified as the protocol.

1. The latest existing security policy is displayed by default next to Policy in the Security area but you may change it by clicking **Change**.
   The Select security policy window opens.
2. Select from the available security options:

   - **Choose a predefined security policy** and select a policy from the **Policy name** drop-down list box.

   Note: For more information on pre-defined security policies, go to AWS Predefined SSL Security Policies for Elastic Load Balancing

   OR

   - **Create a custom security policy**. Choosing this option opens the **SSL PROTOCOLS** and the **SSL CIPHERS** drop-down list box with values pre-populated.

   a) To delete any of the pre-populated values, click the **x** next to the value(s) you do not want.
   b) To add or select another protocol, click in the **SSL PROTOCOLS** field and select one from the drop-down list box.
   c) To add or select another encryption algorithm, click in the **SSL CIPHERS** field and select one from the drop-down list box.

      Note: You must specify at least one protocol and one encryption algorithm.
   d) In the SSL OPTIONS, click to select **Server order preference** if you want it for SSL negotiation.
   e) Click the **Use This Policy** button to select the defined security policy.
      The Select security policy window closes and the specified policy is displayed next to the Policy field.

Certificate

The ability to apply an SSL certificate is only available if HTTPS or SSL is specified as the protocol.

1. **Note:** Skip this step if you want to continue using a certificate that is already installed on your load balancer.

   To select a certificate, if available, click **Select** next to Certificates.
2. If a certificate is already assigned and you want to change it, click **Change** instead.

Choosing this option opens the Select certificate(s) window.

Note: Tabs display for SSL and Backend only if the instance side uses HTTPS or SSL protocol.

3. Select from the available options for assigning a certificate to your load balancer:

   - **Choose an existing SSL certificate** from the **Certificate Name** drop down list, if available.

     Note: If one is not available, upload a new certificate.
   - **Upload a new SSL certificate**. Choosing this option opens a form to upload a new certificate:

   a) Type the name of the new certificate in the **Certificate name** text field.
   b) Paste the contents of your public key certificate file in the **Public key certificate** text field. Refer to the bubble help **(?)** for additional details.
   c) Paste the contents of your private key certificate file in the **Private key** text field. Refer to the bubble help **(?)** for additional details.
   d) Enter the contents of your certificate chain file in the **Certificate chain** text field.
   e) To specify certificates for the backend, click the **Back end** tab. Otherwise, click the **Use This Certificate** button.

      Note: Back-end certificates are optional, and you may add multiple certificates on this form. Back-end certificates are an advanced means to ensure added security measures between your load balancer(s) and its communication with your server. Back-end certificates can only be applied if a secure protocol is assigned to the instance side of the listener.

      Choosing to specify the backend certificate(s) opens another form that may already be populated with pre-loaded certificates.
   f) To delete any of the pre-populated certificates, click the **x** next to the cetificate(s) you do not want.
   g) To add or select another certificate, click **Add a certificate** or **Add another certificate**, respectively.
   h) Type the name of the new certificate in the **Certificate name** text field.
   i) Paste the contents of your certificate file in the **Body (pem encoded)** text field.
   j) Click the **Add Certificate** button to add it.
   k) Click the **Use These Certificates** button to apply the certificates to your load balancer.
   The Select certificate(s) window closes and the specified certificate(s) is displayed next to the Certificates field.
   l) After listeners have been declared, click the **Add Listener** button to continue.
   m) To add more listeners, repeat the above steps.

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:

Add tags

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.
5. To delete one or more tags, move your mouse over the tag you wish to delete, and click the **X** button.

Access logs

This section allows you to enable and disable logs, view or change the location for where the logs are stored, and other collection information defined in the Access Logs section of the Create Load Balancer Wizard.

1. Click to select **Enable logging** to turn on the logging feature.

If left unchecked, the logging feature is disabled and you do not have the ability to specify any information about your log outputs.

Checking the box opens a logging permissions window and displays additional fields below. The Enable Bucket Access for Logging window prompts for user confirmation to proceed.

2. Click **I Understand, Enable Access Logging** to continue.
3. Specify or change the bucket to store your logs by selecting one from the **Bucket name** drop-down list or click **Create bucket** to create a new bucket for storing the logs.
   If creating a new bucket, the Create bucket window opens and prompts for a name.

   Note: Upon clicking **Create Bucket**, the system validates the name of the new bucket to ensure it is unique and not already in use. It is very important that each bucket has a unique name across the cloud.
4. Using all lowercase characters, you may optionally enter or change the path in the **Prefix** text field to specify the path within the bucket to store your log files.

   If the path is not specified, the location defaults to the bucket's root level.

   The recommended default interval for capturing logs is pre-populated but you may change it, if necessary.
5. To change the interval, select another one from the **Collection interval** drop-down list.
6. Click **View latest log** to open a separate window that contains the logs associated with your load balancer.
7. Click **View my bucket** to open an S3 bucket to view its contents.

Network & security

This section is only visible for load balancers in a VPC environment. The VPC network name and ID associated with the load balancer is not editable you may edit the security groups, if necessary.

1. To delete any of the security groups, click the **x** next to the one(s) you do not want.
2. To add a security group, type the first letters of the secuirty group name and choose the security group you want to add.

Save your changes

Click **Save Changes** to save your changes or **Cancel** to abandon your changes.
The message, `Successfully updated load balancer [name]` indicates changes saved successfully.

Load Balancer Details - Monitoring

This tab provides a graphical view of various data points being monitored for your load balancer. This tab opens as the default view when launched from the load balancers landing page.

1. Filter the data by the range of time you want to view by selecting it from the **Show data for** drop down list box.

   If the graphs do not refresh, click the **#** (circular arrow) icon.
2. The graphs displayed by default are:

   - **Sum request count**. The total number of completed requests that were received and routed to the registered instances. Defaults to the *sum* statistic for the best output results.
   - **Avg latency (MS)**. The average elapsed time (in milliseconds) between a request from the load balancer and when a response is received. Defaults to the *average* statistic for the best output results.
   - **Unhealthy hosts**. The number of unhealthy instances in each Availability Zone as it exceeds the unhealthy threshold defined for the health checks. If load balancing is enabled across zones, the number of unhealthy instances is based on the health criteria across all Availability Zones. Use the *average* statistic for the best output results.
   - **Healthy hosts**. The number of healthy instances in each Availability Zone as defined by the healthy threshold. If load balancing is enabled across zones, the number of healthy instances is based on the health criteria across all Availability Zones. Use the *average* statistic for the best output results.
   - **Sum ELB 4xxs**. When the listener is configured to use HTTP or HTTPS protocols, this metric represents the number of HTTP 4XX *client* error codes generated by the load balancer when a request is malformed or incomplete. Defaults to the *sum* statistic for the best output results.

- **Sum ELB 5xxs**. When the listener is configured to use HTTP or HTTPS protocols, this metric represents the number of HTTP 5XX *server* error codes generated by the load balancer if there are no healthy instances registered, or if the request rate exceeds the capacity of the instances or the load balancer. Defaults to the *sum* statistic for the best output results.
- **Sum HTTP 2xxs**. The number of HTTP response codes generated by registered instances but not by the load balancer. Defaults to the *sum* statistic for the best output results.
- **Sum HTTP 3xxs**. The number of HTTP response codes generated by registered instances but not by the load balancer. Defaults to the *sum* statistic for the best output results.
- **Sum HTTP 4xxs**. The number of HTTP response codes generated by registered instances but not by the load balancer. Defaults to the *sum* statistic for the best output results.
- **Sum HTTP 5xxs**. The number of HTTP response codes generated by registered instances but not by the load balancer. Defaults to the *sum* statistic for the best output results.

3. The various ways to view the data in the graphs are:
   - Click on a graph to expand it.
   - Hover inside the graph to display a read-out of data-points desired.
   - Use the drop-down list boxes for **Statistic**, **Show data for**, and **Measurement period** to focus in on specific set of data points. For example, to view the combined number of healthy hosts within the last hour in 5-minute readings, select **Sum** from **Statistic**, **Last hour** from **Show data for**, and **5 minutes** from **Measurement period**.

Load Balancer Details - Instances

This tab displays instances tied to your load balancer.

Actions menu

Clicking the down arrow from the **Actions** menu allows you to delete the load balancer.

Delete a load balancer

To delete a load balancer:

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

Availability zones

This section allows you to view or disable the availability zones (or VPC subnets, if cloud is VPC) and add or remove instances from a load balancer. You can add instances to a load balancer without enabling the zone, but they will not receive traffic until the zone is enabled.

1. The ability to select **Enable cross-zone load balancing** is only present for a load balancer not on a VPC network. This option evenly distributes traffic across all instances in all availability zones.
2. You can disable an availability zone (or a VPC subnet, if the cloud is VPC) from the **(...)** icon in the upper-right corner of the box that represents it.
3. Select from the list of instances to specify between which instances to balance traffic.

   You may use the Magic Search bar to narrow down the list of instances by specifying the availability zone (or VPC subnet), security group, or status.

   Hover over the instances with *out of service* status for additonal details about those instances.

   If present, hover over the warning icons (#) in the availability zones or subnets for additonal details about those instances.

   Selecting an instance automatically adds that instance to the availability zone or VPC subnet field above and the number of instances selected is also reflected.
4. Click **Save Changes** to save your changes or **Cancel** to abandon your changes.
   The message, `Successfully updated load balancer [name]` indicates changes saved successfully.

Load Balancer Details - Health check

This page allows you to view and edit various health checks associated with monitoring a load balancer. Any instances that fail the health check will be automatically removed from the load balancer.

Actions menu

Clicking the down arrow from the **Actions** menu allows you to delete the load balancer.

Delete a load balancer

To delete a load balancer:

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

Ping settings

1. Change the settings for pinging your instances:
   a) Select a protocol from the **Protocol** drop-down list.
   b) Enter the port in the **Port** text field.

      The port may be populated with a common default port for a chosen protocol but you can change the port, if neccessary.
   c) For http or https protocols, you may enter the path of the ping in the **Path** text field.

      TCP and SSL protocols do not display this field.
2. Optionally, you can click **Advanced** to expand the health check timing options.
3. Enter the time in seconds in the **Response timeout (secs)** text field to specify how long to wait for a ping response before it times out.
4. Select the desired ping interval from the **Time between pings** drop-down list.
5. Specify the thresholds for declaring the health of instances:
   a) Select the number of failed attempts from the **Failures until unhealthy** drop-down list before declaring an instance unhealthy.
   b) Select the number of successful attempts from the **Passes until healthy** drop-down list before declaring an instance healthy.
6. Click **Save Changes** to save your changes or **Cancel** to abandon your changes.
   The message, `Successfully updated health checks for [name]` indicates changes saved successfully.

Console Guide History

This section contains information about changes to the Management Console documentation in this release.

Section / Topic	Description of Change	Date Changed
Management Console	Cross-origin resource sharing (CORS) configuration for S3 buckets support.	March 2017