What's New

This What's New is associated with the 2008-05-05 release of Amazon EC2. This guide was last updated on October 07, 2008.

The following table describes the important changes since the last release of the Amazon EC2 Developer Guide.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon EBS</td>
<td>Amazon EBS enables a single Amazon EC2 instance to attach to a highly available, highly reliable storage volume of up to 1 TB of data. Once attached, applications on a single Amazon EC2 instance can read or write from the Amazon EBS volume similar to a disk drive. With Amazon EBS, an Amazon EC2 instance can now be terminated without losing the data that resides on the Amazon EBS volume. One use case involves running a relational database within an Amazon EC2 instance, but maintaining the data within an Amazon EBS volume. For more information, see Amazon Elastic Block Store.</td>
<td>20 August 2008</td>
</tr>
<tr>
<td>Amazon EBS Volume Snapshots</td>
<td>Amazon EBS provides the ability to take point-in-time snapshots of your data, which are then stored in Amazon S3 for long term durability. Snapshots can also be used to create new Amazon EBS volumes from an existing data set or to restore a volume to an older version. Snapshots are point-in-time consistent and incremental to minimize Amazon S3 costs. This means that a snapshot will only contain the data in your volume that has changed since your last snapshot. Previous snapshots of your volume will continue to be available until they are deleted. For more information, see Amazon Elastic Block Store.</td>
<td>20 August 2008</td>
</tr>
<tr>
<td>Amazon EC2 Public AMI Unique SSH Host Keys</td>
<td>Amazon EC2 public AMIs generate unique SSH host keys each time you launch an instance. This enables you to get the host SSH keys from the console output and verify the host to which you are connecting. For more information, see Remove SSH Host Key Pairs and ec2-get-console-output.</td>
<td>1 July 2008</td>
</tr>
<tr>
<td>New fstab Bundling Behavior</td>
<td>The Amazon EC2 ec2-bundle-vol command option --fstab now bundles AMIs using /etc/fstab. The new option --generate-fstab bundles the AMI using an Amazon EC2-provided fstab. For more information, see ec2-bundle-vol.</td>
<td>1 July 2008</td>
</tr>
<tr>
<td>Minor Edits</td>
<td>Numerous minor edits were made based on forum and feedback comments.</td>
<td>1 July 2008</td>
</tr>
<tr>
<td>CPU Instance Types</td>
<td>Amazon EC2 now provides two new High-CPU instance types: c1.medium and c1.xlarge. These instance types have a higher CPU to memory ratio and are designed for processing-intensive applications. For more information, see Instance Types.</td>
<td>29 May 2008</td>
</tr>
<tr>
<td>Elastic IP Addresses</td>
<td>Elastic IP addresses are static IP addresses designed for dynamic cloud computing. Elastic IP addresses are associated with your account, not specific instances. Any elastic IP address that you associate with your account remains associated with your account until you explicitly release it. Unlike traditional static IP addresses, however, elastic IP addresses allow you to mask instance or availability zone failures by rapidly remapping your public IP addresses to any instance in your account. For more information, see <a href="#">Elastic IP Addresses</a>.</td>
<td>27 March 2008</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Availability Zones</td>
<td>Amazon EC2 now provides the ability to place instances in multiple locations. Amazon EC2 locations are composed of regions and availability zones. Regions are geographically dispersed and are in separate geographic areas or countries. Availability zones are separated from each other, but located in the same region. For more information, see <a href="#">Availability Zones</a>.</td>
<td>27 March 2008</td>
</tr>
<tr>
<td>User-Selectable Kernels</td>
<td>Amazon EC2 now enables you to select the kernel and RAM disk to bundle your AMI with or to specify a kernel and RAM disk at launch time. For more information, see <a href="#">Kernels, RAM Disks, and Block Device Mappings</a>.</td>
<td>27 March 2008</td>
</tr>
</tbody>
</table>
Welcome

Topics

- Audience
- How This Guide Is Organized
- Related Resources

This is the Amazon Elastic Compute Cloud Developer Guide. This section describes who should read this guide, how the guide is organized, and other resources related to Amazon Elastic Compute Cloud.

The Amazon Elastic Compute Cloud will occasionally be referred to within this guide as simply "Amazon EC2"; all copyrights and legal protections still apply.
Audience

This guide picks up where the Getting Started Guide ends and provides you with the information to create more sophisticated Amazon Machine Images (AMIs), using advanced service features.

Required Knowledge and Skills

Use of this guide assumes you are familiar with the following:

- XML (For an overview, go to the W3 Schools XML Tutorial)

- Basic understanding of web services (go to W3 Schools Web Services Tutorial)

You should also have worked through the Amazon EC2 Getting Started Guide, installed the command line and API tools, and have a general understanding of the service.
How This Guide Is Organized

This guide is organized into several major sections described in the following table.

<table>
<thead>
<tr>
<th>Information</th>
<th>Relevant Sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Describes how to create a customized software package (operating system</td>
<td>Creating and Preparing AMIs</td>
</tr>
<tr>
<td>and applications) that you can run on Amazon EC2</td>
<td></td>
</tr>
<tr>
<td>Describes Amazon EC2 instances and provides tips for using them effectively</td>
<td>Launching and Using Instances</td>
</tr>
<tr>
<td>Describes instance network addressing, explains the distributed firewall, and</td>
<td>Instance Addressing and Network Security</td>
</tr>
<tr>
<td>provides usage examples</td>
<td></td>
</tr>
<tr>
<td>Explains the basics of using the SOAP and Query APIs, including signing</td>
<td>Using the APIs</td>
</tr>
<tr>
<td>requests</td>
<td></td>
</tr>
<tr>
<td>Provides a comprehensive reference to the SOAP and Query APIs</td>
<td>API Reference</td>
</tr>
<tr>
<td>Provides a comprehensive reference to the Amazon EC2 command line tools</td>
<td>Command Line Tools Reference</td>
</tr>
<tr>
<td>Provides answers to commonly asked questions</td>
<td>Technical FAQ</td>
</tr>
<tr>
<td>Describes Amazon EC2 terms</td>
<td>Glossary</td>
</tr>
<tr>
<td>Typographic and symbol conventions</td>
<td>Document Conventions</td>
</tr>
</tbody>
</table>

Each section is written to stand on its own, so you should be able to look up the information you need and go back to work. However, you can also read through the major sections sequentially to get in-depth knowledge about Amazon EC2.
Related Resources

The following table lists related resources that you'll find useful as you work with this service.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amazon EC2 Getting Started Guide</strong></td>
<td>The Getting Started Guide provides a quick tutorial of the service based on a simple use case. Examples and instructions are included.</td>
</tr>
<tr>
<td><strong>Amazon EC2 Release Notes</strong></td>
<td>The Release Notes give a high-level overview of the current release. They specifically note any new features, corrections, and known issues.</td>
</tr>
<tr>
<td><strong>AWS Developer Resource Center</strong></td>
<td>A central starting point to find documentation, code samples, release notes, and other information to help you build innovative applications with AWS.</td>
</tr>
<tr>
<td><strong>Amazon EC2 product information</strong></td>
<td>The primary web page for information about Amazon EC2.</td>
</tr>
<tr>
<td><strong>AWS Support Center</strong></td>
<td>The home page for AWS Technical Support, including access to our Developer Forums, Technical FAQs, Service Status page, and (if you are subscribed to this program) AWS Premium Support.</td>
</tr>
<tr>
<td><strong>AWS Premium Support Information</strong></td>
<td>The primary web page for information about AWS Premium Support, a one-on-one, fast-response support channel to help you build and run applications on AWS Infrastructure Services.</td>
</tr>
<tr>
<td><strong>E-mail address for questions related to your AWS account: <a href="mailto:webservices@amazon.com">webservices@amazon.com</a></strong></td>
<td>This e-mail address is <em>only</em> for account questions. For technical questions, use the AWS Support Center.</td>
</tr>
<tr>
<td><strong>Conditions of Use</strong></td>
<td>Detailed information about the copyright and trademark usage at Amazon.com.</td>
</tr>
</tbody>
</table>
Introduction to Amazon Elastic Compute Cloud

Topics

- What is Amazon EC2?
- Features of Amazon EC2
- Popular Uses for Amazon EC2
- Components of Amazon EC2
- Paying for Amazon EC2
What is Amazon EC2?

Amazon EC2 is a web service that enables you to launch and manage server instances in Amazon's data centers using APIs or available tools and utilities. You can use Amazon EC2 server instances at any time, for as long as you need, and for any legal purpose. If you need 100 instances for a two-day research project, sure. If you need a fleet of instances that can be scaled up and down to meet the traffic fluctuations of your Facebook application, no problem.

Instances are available in different sizes and configurations. This allows us to provide different instance types that you can use to meet specific needs. For example, you might want to use an m1.small instance (one Amazon EC2 Compute Unit) as a web server, an m1.xlarge instance (eight Amazon EC2 Compute Units) as a database server, or an extra large High-CPU instance (twenty Amazon EC2 Compute Units) for processor intensive applications.

What makes Amazon EC2 different is that you use only the capacity that you need. This eliminates your need to make large and expensive hardware purchases, reduces the need to forecast traffic, and enables you to immediately deal with changes in requirements or spikes in popularity related to your application or service.
Features of Amazon EC2

Features

- **Elastic**—Amazon EC2 enables you to increase or decrease capacity within minutes, not hours or days. You can commission one, dozens, or hundreds of server instances simultaneously. Of course, because this is all controlled with web service APIs, your application can automatically scale itself up and down depending on its needs.

- **Completely Controlled**—You have complete control of your instances. You have root access to each one, and you can interact with them as you would any machine. Instances can be rebooted remotely using web service APIs. You also have access to console output of your instances.

- **Flexible**—You have the choice of several instance types, allowing you to select a configuration of memory, CPU, and instance storage that is optimal for your application.

- **Designed for use with other Amazon Web Services**—Amazon EC2 works in conjunction with Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB and Amazon Simple Queue Service (Amazon SQS) to provide a complete solution for computing, query processing and storage across a wide range of applications.

- **Reliable**—Amazon EC2 offers a highly reliable environment where replacement instances can be rapidly and reliably commissioned. The service runs within Amazon's proven network infrastructure and datacenters.

- **Features for Building Failure Resilient Applications**—Amazon EC2 provides powerful features to build failure resilient applications including:
  
  - **Multiple Locations**—Amazon EC2 provides the ability to place instances in multiple locations. Amazon EC2 locations are composed of regions and availability zones. Regions are geographically dispersed and will be in separate geographic areas or countries. Currently, Amazon EC2 exposes only a single region. Availability zones are
distinct locations that are engineered to be insulated from failures in other availability zones and provide inexpensive, low latency network connectivity to other availability zones in the same region. Regions consist of one or more availability zones. By launching instances in separate availability zones, you can protect your applications from failure of a single location.

- **Elastic IP Addresses**—Elastic IP addresses are static IP addresses designed for dynamic cloud computing. An Elastic IP address is associated with your account not a particular instance, and you control that address until you choose to explicitly release it. Unlike traditional static IP addresses, however, Elastic IP addresses allow you to mask instance or availability zone failures by programmatically remapping your public IP addresses to any instance in your account. Rather than waiting on a data technician to reconfigure or replace your host, or waiting for DNS to propagate to all of your customers, Amazon EC2 enables you to engineer around problems with your instance or software by quickly remapping your Elastic IP address to a replacement instance.

- **Secure**—Amazon EC2 provides web service interfaces to configure firewall settings that control network access to and between groups of instances.

- **Inexpensive**—Amazon EC2 passes on to you the financial benefits of Amazon's scale. You pay a very low rate for the compute capacity you actually consume. Compare this with the significant up-front expenditures traditionally required to purchase and maintain hardware, either in-house or hosted. This frees you from many of the complexities of capacity planning, transforms what are commonly large fixed costs into much smaller variable costs, and removes the need to over-buy "safety net" capacity to handle periodic traffic spikes.
Popular Uses for Amazon EC2

Although the applications for Amazon EC2 are only limited by your ingenuity, the following is a list of popular uses for Amazon EC2:

- **Scalable Applications**—You can build a scalable application that shrinks or expands to meet your current demands.

  This can help you use only the compute resources that you need and can help you respond to events where a mention on a popular news site can result in a dramatic spike in traffic.

- **Temporary Events**—You can use Amazon EC2 for temporary solutions and one-off events that would require you to maintain a fleet of compute resources that are normally idle.

  This includes hosting conferences in virtual worlds, live blogging, distribution of newly released media, and short-term promotional websites.

- **Batch Processing**—You can use Amazon EC2 for projects that require massive compute resources which would be expensive to build on your own.

  This includes video and image processing, financial data processing, and science and research applications.

- **Fault Resilient Applications**—You can build an application across multiple availability zones which will be protected against the loss of an entire physical location.
Components of Amazon EC2
AMIs

An Amazon Machine Image (AMI) is an encrypted machine image that contains all information necessary to boot instances of your software. For example, an AMI might contain Linux, Apache, and your web site or it might contain Linux, Hadoop, and a custom application.

AMIs are stored in Amazon S3.

Public AMIs are made available by Amazon and the Amazon EC2 community and can be downloaded from the Resource Center. You can use public AMIs as a base to create your own custom private AMIs.

Private AMIs are AMIs that you own and can only be accessed by you or those to whom you grant access.

Paid AMIs are AMIs that you purchase from developers or AMIs that come with service contracts from organization such as Red Hat.
**Instances**

After an AMI is launched, the resulting running system is called an instance. By default, you can run up to 20 instances. If you need more than 20 instances, please complete the [Amazon EC2 Instance Request Form](https://aws.amazon.com/ec2/request/) and your request will be considered.

Instances remain running unless they fail or are terminated. When this happens, the data on the instance is no longer available.
**Instance Store**

The instance store refers to the disk storage associated with an instance. In the event an instance fails or is terminated, all content on the instance store is deleted.
Paying for Amazon EC2

With Amazon EC2, you don’t have to pay upfront fees, you don’t have to commit to a fixed amount of bandwidth, and you don’t have to meet any minimum usage requirements. As with other AWS services, you only pay for what you use.

The following figure summarizes how you are charged for using Amazon EC2.
Using Amazon EC2

Topics

- Amazon EC2 Flow
- Creating and Preparing AMIs
- Launching and Using Instances
- Instance Addressing and Network Security
- Amazon Elastic Block Store
Amazon EC2 Flow

The following graphic and table explain the basic flow for using Amazon EC2.

**Launch Confirmation Process**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>You create an AMI from scratch or based on an existing AMI. This is optional, as you can launch instances of existing AMIs without modifying them. See <a href="#">Creating an AMI</a>.</td>
</tr>
<tr>
<td>2</td>
<td>You bundle the AMI and obtain an AMI ID so you can launch as many instances of the AMI as you want. See <a href="#">Bundling an AMI</a>.</td>
</tr>
<tr>
<td>3</td>
<td>You launch one or more instances of your AMI. See <a href="#">Launching and Using Instances</a>.</td>
</tr>
<tr>
<td>4</td>
<td>You administer and use your instances and you would with any servers.</td>
</tr>
</tbody>
</table>
Creating and Preparing AMIs

Topics

- Creating an AMI
- Bundling an AMI
- Sharing AMIs
- Creating Paid AMIs

This section describes how to build, store, and share Amazon Machine Images (AMIs).
Creating an AMI

Topics

- Starting with an Existing AMI
- Creating an AMI through a Loopback File

There are two common ways to create an AMI that offer a mix of ease of use and detailed customization levels.

The easiest method involves starting from an existing public AMI and modifying it according to your requirements, as described in Starting with an Existing AMI.

Another approach is to build a fresh installation either on a stand-alone machine or on an empty file system mounted by loopback. This essentially entails building an operating system installation from scratch and is described in Creating an AMI through a Loopback File.

After the installation package has been built to your satisfaction, you must bundle it and upload it to Amazon Simple Storage Service (Amazon S3) as described in Bundling an AMI.
Starting with an Existing AMI

To quickly and easily get a new working AMI, start with an existing public AMI or one of your own. You can then modify it and create a new AMI with the `ec2-bundle-vol` utility described in Bundling an AMI.

**Note**
Before selecting an AMI, determine whether the instance types you plan to launch are 32-bit or 64-bit. For more information, see Instance Types.

Make sure you are using GNU Tar 1.15 or later.

To use an existing AMI to create a new AMI, complete the following tasks:

**Using an Existing AMI**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select an AMI</td>
</tr>
<tr>
<td>2</td>
<td>Generate a Key Pair</td>
</tr>
<tr>
<td>3</td>
<td>Launch the Instance</td>
</tr>
<tr>
<td>4</td>
<td>Authorize Network Access</td>
</tr>
<tr>
<td>5</td>
<td>Connect to the Instance</td>
</tr>
<tr>
<td>6</td>
<td>Upload the Key and Certificate</td>
</tr>
</tbody>
</table>
Select an AMI

First, locate an AMI that contains the packages and services you require. This can be one of your own AMIs or a public AMIs provided by Amazon EC2.

To select an AMI

1. Get a list of available AMIs by entering the `ec2-describe-images` command:

   ```
PROMPT> ec2-describe-images -a
   
   The response includes the image ID, the location of the file in Amazon S3, and whether the file is available.
   ``

2. Choose an AMI from the list and write down its AMI ID.

Example

```
PROMPT> ec2-describe-images -o self -o amazon
IMAGE ami-60a54009 ec2-public-images/base-fc4-apache.manifest.xml 475219833042 available public
IMAGE ami-61a54028 <your-s3-bucket>/image.manifest.xml 495219933132 available private
IMAGE ami-2bb65342 ec2-public-images/getting-started.manifest.xml 475219833042 available public
IMAGE ami-6ea54007 ec2-public-images/base-fc3-mysql.manifest.xml 475219833042 available public
```
Generate a Key Pair

This step is only required if you selected one of the public AMIs provided by Amazon EC2. You must create a public/private key pair to ensure that only you have access to instances that you launch.

After you generate a key pair, the public key is stored in Amazon EC2 using the key pair name you selected. Whenever you launch an instance using the key pair name, the public key is copied to the instance metadata. This allows you to access the instance securely using your private key.

To create a public/private key pair

1. Enter the following command:

```
PROMPT> ec2-add-keypair <keypair-name>
```

The `<keypair-name>` is the name you select for the key pair.
The resulting private key is displayed.

2. Open a text editor.

3. Paste the entire private key, starting with the line "----- BEGIN RSA PRIVATE KEY-----" and ending with the line "----- END RSA PRIVATE KEY-----".

4. Save the file and exit.

**Note**
This file should only be readable by the file owner.

**Example**

```
PROMPT> ec2-add-keypair gsg-keypair
-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQBuLFg5ujHrtnjnutSo08Xe56Ltt+HM8Vv/xkaa39EstM3/aFxThgElqI:
HungXQ29VTC8rc1bW0ldk1d230H5eqkMhGhvEwqa0HWAUMmll4o3o/IX+0f2uPoKCOVUR+j:
5AU52E0fanIn3ZQ8fWF7Edp5a3q4dhjGLUKToHvb1c5E+g45zfB95WiywWZw6WUUF3lpO:
ebIUuqlqTBHkLbCC2r7RTn8vQPw47BVYGTsGSMpTRSP5hbuzzqj3itkiLHjU935sJCo7:
i8BygR4s3mhKBj8l+ePQxG1kGbF6R4yg6sECmXn17MRQX0DNHZbAgMBAECEgqEAY1tsiUsj:
91C3rYGuVfLyLflXenxfI50mDFMs/mUmTqlOHO7tr00riHDRS5k7wMCMY/Y5YkcXNo7mvU:
ZNUSj7rW9gZRTRf7Lylaj58kOcyajw8Tsc4e4LPbaHw5ld6k8xyh64066zgW4srsB61Cmr1:
wcfgt5ecIU4T7f00E9HJn+2eRlrsrjBdeori7KiUNPCaG23i6MdD0FEQRccS1gCj+4/mci:
SwS4dMrpb9FNSIfcadLxVM7/6KXg3JNfZc9XWu771g8x92Zd0fVh0ux5IZC+UvSKWB4c:
etE8C3p9bbU9VGYy5vLCaBb4qQKbQDLOi024GXrIkswF32YTBbMVgGSwU98h9H09mKAc2n:
JUE51pzRJTedc9I2q1IMUTwtngw42auSCzbUeYMURPdQy7p6Ajuj9p9EpmcSV0K9vXYL6:
xwMC0dtV61PknQ01zXRPKaFbwWADP1m68UAIVe/a5X5k5jwBQcKSpHi2EISh1uRkhx1:
idCIk6JBRsMvPbc0v58dKw5P5a0lOMd5R5Jv2vqZ5j5CyNpMay1/EDNTY50SIUJ+0KFMqBo:
rdLNLDA4+TcnT7c62/aH01ohYaf/VcBrHtL1BfqGoQc7+sAC8vMKesen7FfcCEKDFY/fdrx:
gCOIizzNAapayz1/JcTVtwEdi6j9qNxbC+z2YWm+IT0Fv/hwKx/ype0XniUcwoIt/YtC:
DQbsz7LcyY1HqxiHKYNYWvXgwWV+oiChjxvEkSdTTfnnK4VSCvU9XbDbQHjdINDBL60ar9z:
rBYvChjZF7LwUH4yVmPAoGAbZ2X7VxoeEO+u5Z58/BGK0IGHyHBDiXtzmHdJr15HTYjxK7:
gkK+8zP9lBvLDGMO3vft32XPEnuwv18tvC9F+AcsWlQADZKZsBSaOZ/h1FwhdMgCMcYeC:
JZKjTSU3i7vUxv6RzdSedXEMTZN4nQ1XJ3k5aHcukCgAY9T+zRvm1F0sEqPbLkn77EhX:
P8TTVW/6bdPi23ExzzzNhK0drcfLyRph1LHmAPoNV/x2xALIf91UB+v5ohtyloDoesL0gij1f:
2ERKkDwz0ZL9Sw6VdTdr/5S994C72f5y5WheERBdju1dHaK3M849JJuf8cSrVsb4g==
-----END RSA PRIVATE KEY-----
```
Launch the Instance

You are now ready to launch an instance of the AMI that you previously selected.

To launch an instance

1. Start the launch by entering the following command:

   ```bash
   PROMPT> ec2-run-instances <ami_id> -k <keypair-name>
   ```

   The `<ami_id>` is the AMI ID you selected earlier and `<keypair-name>` is the name of the key pair. The command will return the AMI instance ID, a unique identifier for each launched instance. You use the instance ID to manipulate the instance. This includes viewing the status of the instance, terminating the instance, and so on.

   Launching the instance will take a few minutes.

2. View the progress of the instance by entering the following command:

   ```bash
   PROMPT> ec2-describe-instances <instance_id>
   ```

   The `<instance_id>` is the ID of the instance.

   When the status field displays "running," the instance was created and is booting. However, the instance might not be immediately accessible over the network. Make sure to use the appropriate DNS name provided by the `ec2-describe-instances` command.

   **Important**

   Once you launch an instance, you will be billed for all usage, including hourly CPU time. Make sure to terminate any instances that you do not want to leave running. For information on Amazon EC2 pricing, go to the Amazon EC2 home page.

   **Example**

   The following example launches an instance of ami-2bb65342.

   ```bash
   PROMPT> ec2-run-instances ami-2bb65342 -k gsg-keypair
   RESERVATION r-302dc059 416161254515 default
   ```
The following shows the status of the launch:

<table>
<thead>
<tr>
<th>INSTANCE</th>
<th>i-eb977f82</th>
<th>ami-2bb65342</th>
<th>pending</th>
</tr>
</thead>
</table>

PROMPT> ec2-describe-instances i-eb977f82

<table>
<thead>
<tr>
<th>RESERVATION</th>
<th>r-302dc059</th>
<th>416161254515</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>i-eb977f82</td>
<td>ami-2bb65342</td>
<td>ec2-72-44-40-222.compute-1.amazonaws.com</td>
</tr>
</tbody>
</table>
Authorize Network Access

To reach a running instance from the Internet, you must enable access for the SSH service on port 22.

To enable SSH service on port 22

- Enter the following command:

```
PROMPT> ec2-authorize default -p 22
PERMISSION  default  ALLOWS  tcp  22  22  FROM  CIDR  0
```
Connect to the Instance

After starting an instance, you can log in and modify it according to your requirements.

To connect to an instance

- If you are launching an AMI that supports SSH login (e.g., public AMIs), use the following command to log in with your private key:

  ```
PROMPT> ssh -i <private-keyfile> root@<dns_location>
  ```

  The `<private-keyfile>` is the file that contains the private key and `dns_location` is the DNS location of the instance within Amazon EC2. Your instance displays a prompt that contains your username and the hostname of the instance.

You now have complete control over the instance. You can add, remove, modify, or upgrade packages and files to suit your needs.

⚠️ Important

We recommend exercising extreme care when changing some of the basic Amazon EC2 configuration settings, such as the network interface configuration and the `/etc/fstab` contents. Otherwise, the AMI might become unbootable or inaccessible from the network once running.

Example

The following example shows logging in to an AMI using SSH.

```
PROMPT> ssh -i id_rsa-gsg-keypair
root@ec2-67-202-51-223.compute-1.amazonaws.com
root@ec2-67-202-51-223 #
```
Upload the Key and Certificate

Your new AMI is encrypted and signed to ensure that only you and Amazon EC2 can access it. Therefore, you must upload your Amazon EC2 private key and X.509 certificate to the running instance, for use in the AMI bundling process.

Note
For information on obtaining your Amazon EC2 private key and X.509 certificate, refer to the Amazon Elastic Compute Cloud Getting Started Guide.

To upload your Amazon EC2 private key and X.509 certificate

1. Copy your Amazon EC2 private key and X.509 certificate to the /mnt directory.

2. Enter the following command:

```
PROMPT> scp <private_keyfile> <certificate_file> root@<dns_location>:/mnt
```

The `<private_keyfile>` is the file that contains the private key, `certificate_file` is the file that contains the certificate, and `dns_location` is the DNS location of the instance within Amazon EC2.

Amazon EC2 returns the name of the files and some performance statistics.

Note
It is important that the key and cert files are uploaded into /mnt to prevent them from being bundled with the new AMI.

You are ready to bundle the volume and uploading the resulting AMI to Amazon S3. For more information, see Bundling an AMI.

Example

```
PROMPT> scp pk-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CL0.pem
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CL0.pem
```
root@ec2-67-202-51-223.compute-1.amazonaws.com:/mnt
-i id_rsa-gsg-keypair
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CL0.pem 100% 717 0.7KB/s 00:00
cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CL0.pem 100% 685 0.7KB/s 00:00
Creating an AMI through a Loopback File

This method involves doing a full operating system installation on a clean root file system, but avoids having to create a new root disk partition and file system on a physical disk. Once you have installed your operating system, the resulting image can be bundled as an AMI with the `ec2-bundle-image` utility.

**Note**
Before selecting an AMI, determine whether the instance types you plan to launch are 32-bit or 64-bit. For more information, see Instance Types. Make sure you are using GNU Tar 1.15 or later. These examples use Fedora Core 4. Please make any adjustments for your distribution.

AMI Creation Process

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Create a File to Host the AMI.</strong></td>
</tr>
<tr>
<td>2</td>
<td><strong>Create a Root File System Inside the File.</strong></td>
</tr>
<tr>
<td>3</td>
<td><strong>Mount the File through Loopback.</strong></td>
</tr>
<tr>
<td>4</td>
<td><strong>Prepare for the Installation.</strong></td>
</tr>
<tr>
<td>5</td>
<td><strong>Install the Operating System.</strong></td>
</tr>
<tr>
<td>6</td>
<td><strong>Configure the Operating System.</strong></td>
</tr>
</tbody>
</table>
Create a File to Host the AMI

The dd utility can create files of arbitrary sizes. Make sure to create a file large enough to host the operating system, tools, and applications that you will install. For example, a baseline Linux installation requires about 700MB, so your file should be at least 1 GB.

To create a file to host the AMI

- Enter the following command:

```sh
# dd if=/dev/zero of=<image_name> bs=1M =<size>
```

The `<image_name>` is the name of the image file you are creating and `<size>` is the size of the file in megabytes.

Example

The following command creates a one gigabyte file (1024*1MB).

```sh
# dd if=/dev/zero of=my-image.fs bs=1M count=1024
1024+0 records in
1024+0 records out
```
Create a Root File System Inside the File

There are several variations on the `mkfs` utility that can create a file system inside the image file you are creating. Typical Linux installations default to ext2 or ext3 file systems.

To create an ext3 file system

- Enter the following command:

```
# mke2fs -F -j <image_name>
```

The `<image_name>` is the name of the image file.

Example

The following command creates an ext3 file system.

```
# mke2fs -F -j my-image.fs
mke2fs 1.38 (30-Jun-2005)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
131072 inodes, 262144 blocks
13107 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=268435456
8 block groups
32768 blocks per group, 32768 fragments per group
16384 inodes per group
Superblock backups stored on blocks:
 32768, 98304, 163840, 229376

Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 24 mounts or 180 days, whichever comes first. Use `tune2fs -c` or `-i` to override.
```
Mount the File through Loopback

The loopback module allows you to use a normal file as if it were a raw device, which gives you a file system within a file. Mounting a file system image file through loopback presents it as part of the normal file system. You can then modify it using your favorite file management tools and utilities.

To mount the file through loopback

1. Create a mount point in the file system where the image will be attached:

   ```
   # mkdir <image_mountpoint>
   ```

   The `<image_mountpoint>` is the location where the image will be mounted.

2. Mount the file system image:

   ```
   # mount -o loop <image_name> <image_mountpoint>
   ```

   The `<image_name>` is the name of the image file and `<image_mountpoint>` is the mount location.

Example

The following commands create and mount the my-image.fs image file.

```bash
# mkdir /mnt/ec2-fs
# mount -o loop my-image.fs /mnt/ec2-fs
```
Prepare for the Installation

Before the operating system installation can proceed, you must create and prepare the newly created root file system.

To prepare for the installation

1. Create a /dev directory and populate it with a minimal set of devices. You can ignore the errors in the output.

   ```
   # mkdir /mnt/ec2-fs/dev
   # /sbin/MAKEDEV -d <image_mountpoint>/dev -x console
   # /sbin/MAKEDEV -d <image_mountpoint>/dev -x null
   # /sbin/MAKEDEV -d <image_mountpoint>/dev -x zero
   
   The <image_mountpoint> is the mount location.
   ```

2. Create the fstab file within the /etc directory and add the following:

   ```
   /dev/sda1 / ext3 defaults 1 1
   none /dev/pts devpts gid=5,mode=620 0 0
   none /dev/shm tmpfs defaults 0 0
   none /proc proc defaults 0 0
   none /sys sysfs defaults 0 0
   
   The <image_mountpoint> is the mount location.
   ```

3. Create a temporary yum configuration file (e.g., yum-xen.conf) and add the following content.

   ```
   [main]
cachedir=/var/cache/yum
debugevel=2
logfile=/var/log/yum.log
exclude=*
exclude=debuginfo
gpgcheck=0
obsoletes=1
reposdir=/dev/null

   [base]
   name=Fedora Core 4 - $basearch - Base
   ```
mirrorlist=http://fedora.redhat.com/download/mirrors/fedora-core-$releasever
enabled=1

[updates-released]
name=Fedora Core 4 - $basearch - Released Updates
mirrorlist=http://fedora.redhat.com/download/mirrors/updates-released-fc$releasever
enabled=1

This ensures all the required basic packages and utilities are installed. This file can be located anywhere on your main file system (not on your loopback file system) and is only used during installation.

4. Enter the following:

```bash
# mkdir <image_mountpoint>/proc
# mount -t proc none <image_mountpoint>/proc
```

The `<image_mountpoint>` is the mount location. A groupadd utility bug in the shadow-utils package (versions prior to 4.0.7-7) requires you to mount the new proc file system manually with the preceding command.

**Example**

These commands create the /dev directory and populate it with a minimal set of devices:

```bash
# mkdir /mnt/ec2-fs/dev
#/sbin/MAKEDEV -d /mnt/ec2-fs/dev -x console
MAKEDEV: mkdir: File exists
MAKEDEV: mkdir: File exists
MAKEDEV: mkdir: File exists
#/sbin/MAKEDEV -d /mnt/ec2-fs/dev -x null
MAKEDEV: mkdir: File exists
MAKEDEV: mkdir: File exists
MAKEDEV: mkdir: File exists
#/sbin/MAKEDEV -d /mnt/ec2-fs/dev -x zero
MAKEDEV: mkdir: File exists
MAKEDEV: mkdir: File exists
MAKEDEV: mkdir: File exists
```

This example creates and mounts the /mnt/ec2-fs/proc directory.
# mkdir /mnt/ec2-fs/proc
# mount -t proc none /mnt/ec2-fs/proc
Install the Operating System

At this stage, the basic directories and files are created and you are ready to install the operating system. Depending on the speed of the host and network link to the repository, this process might take a while.

To install the operating system

- Enter the following command:

```
# yum -c <yum_configuration_file> --installroot=<image_mountpoint> -y groupinstall Base
```

The `<yum_configuration_file>` is the name of the yum configuration file and `<image_mountpoint>` is the mount location.

You now have a base installation, which you can configure for operation inside Amazon EC2 and customize for your use.

Example

This example installs the operating system at the `/mnt/ec2-fs` mount point using the `yum-xen.conf` yum configuration file.

```
# yum -c yum-xen.conf --installroot=/mnt/ec2-fs -y groupinstall Base

Setting up Group Process
Setting up repositories
base 100% |=================================================================| 1.1 kB 00:
updates-released 100% |=================================================================| 1.1 kB 00:
comps.xml 100% |=================================================================| 693 kB 00:
comps.xml 100% |=================================================================| 693 kB 00:
Setting up repositories
Reading repository metadata in from local files
primary.xml.gz 100% |=================================================================| 824 kB 00:
base : #2772/2772 Added 2772 new packages, deleted 0 old in 15.32 seconds
primary.xml.gz 100% |=================================================================| 824 kB 00:
updates-re: #2772/2772 Added 2772 new packages, deleted 0 old in 10.74 seconds
...
Complete!
```
Configure the Operating System

After successfully installing the base operating system, you must configure the networking and hard drives to work in the Amazon EC2 environment.

To configure the operating system

1. Edit (or create) /mnt/ec2-fs/etc/sysconfig/network-scripts/ifcfg-eth0 and make sure it contains at least the following information:

   ```
   DEVICE=eth0
   BOOTPROTO=dhcp
   ONBOOT=yes
   TYPE=Ethernet
   USERCTL=yes
   PEERDNS=yes
   IPV6INIT=no
   ```

   **Note**
   
   The Amazon EC2 DHCP server ignores hostname requests. If you set `DHCP_HOSTNAME`, the local hostname will be set on the instance but not externally. Additionally, the local hostname will be the same for all instances of the AMI, which might be confusing.

2. Ensure that networking starts by making sure the following line appears in the /mnt/ec2-fs/etc/sysconfig/network file:

   ```
   NETWORKING=yes
   ```

3. Ensure that local disk storage on /dev/sda2 and swap space on /dev/sda3 are mounted at system startup by adding the following lines to /mnt/ec2-fs/etc/fstab:

   ```
   /dev/sda2  /mnt  ext3  defaults  0 0
   /dev/sda3  swap  swap  defaults  0 0
   ```

   **Note**
The `/dev/sda2` and `/dev/sda3` storage locations only apply to small instances. For more information on instance storage, see [Instance Storage](#).

4. Make sure all of your required services start at system startup by allocating them appropriate system run levels. For example, to enable the service `my-service` on multi-user and networked run levels, enter the following commands:

```
# chroot /mnt/ec2-fs /bin/sh
# chkconfig --level 345 my-service on
# exit
```

Your new installation is successfully installed and configured to operate in the Amazon EC2 environment.

5. Umount the image by entering the following commands:

```
# umount <image_mountpoint>/proc
# umount -d <image_mountpoint>
```

The `<image_mountpoint>` is the mount location.

**Example**

The following example unmounts the installation from the `/mnt/ec2-fs` mount point.

```
# umount /mnt/ec2-fs/proc
# umount -d /mnt/ec2-fs
```
Bundling an AMI

To use a file system image with Amazon EC2, you must bundle it as an AMI. The bundling process does the following:

- Compresses the image to minimize bandwidth usage and storage requirements
- Encrypts and signs the compressed image to ensure confidentiality and authenticates the image against its creator
- Splits the encrypted image into manageable parts for upload
- Creates a manifest file that contains a list of the image parts with their checksums

This section describes the AMI tools that automate this process and provides examples of their use.

The AMI tools include three command-line utilities:

- `ec2-bundle-image` bundles an existing AMI
- `ec2-bundle-vol` creates an AMI from an existing machine or installed volume
- `ec2-upload-bundle` uploads a bundled AMI to Amazon S3 storage
Installing the AMI Tools

The AMI tools are packaged as an RPM suitable for running on Fedora Core with Ruby 1.8.2 (or greater) installed. You need root privileges to install the software.

The AMI tools RPM is available from our public Amazon S3 downloads bucket.

To install the AMI tools

1. Install Ruby using the yum package manager.

   ```
   # yum install ruby
   ```

2. Install the AMI tools RPM.

   ```
   # rpm -i ec2-ami-tools-x.x-xxxx.i386.rpm
   ```
Installation Issues

The AMI tools libraries install in /usr/lib/site_ruby.

If you receive a load error when running one of the AMI utilities, Ruby might not have found the path. To fix this, add /usr/lib/site_ruby to Ruby's library path, which is set in the RUBYLIB environment variable.
Viewing Documentation

To view the manual for each utility

- Append `--manual` to the command that invokes the utility.

```
# ec2-bundle-image --manual
```

To view help for each utility

- Append `--help` to the command that invokes the utility.

```
# ec2-bundle-image --help
```
Bundling an AMI Using the AMI Tools

After creating a machine image, it must be bundled as an AMI for use with Amazon EC2. How you bundle the image depends on how you created the image (for information about creating AMIs, see Creating an AMI).

To bundle the loopback file image

- Enter the following command:

```bash
# ec2-bundle-image -i <image_name>.img -k <private_keyfile> -c <certificate_file>
```

The `<image_name>` is the name of the image file, `<private_keyfile>` is the file that contains the private key, `<certificate_file>` is the file that contains the certificate, and `<user_id>` is the user ID associated with your account.

Note

The user ID is your AWS account ID without dashes. It is the same as your Amazon Access ID and consists of 12 digits.

To bundle a snapshot image (requires root privileges)

- Enter the following command:

```bash
# ec2-bundle-vol -k <private_keyfile> -C <certificate_file> -u <user_id>
```

The `<private_keyfile>` is the file that contains the private key, `<certificate_file>` is the file that contains the certificate, and `<user_id>` is the user ID associated with your account.

Note

Make sure to disable SELinux when running `ec2-bundle-vol`.

Note
The user ID is your AWS account ID without dashes. It is the same as your Amazon Access ID and consists of 12 digits.

**Example**

This command bundles an image created in a loopback file.

```
# ec2-bundle-image -i my-image.fs -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CL0.pem -C cert-HK2
image.part.00
image.part.01
...
image.part.NN
image.manifest.xml
```

This command bundles the local machine root file system.

```
# ec2-bundle-vol -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CL0.pem -C cert-HKZYKTAIG2ECMXYIBH3HX
image.part.00
image.part.01
...
image.part.NN
image.manifest.xml
```
Uploading a Bundled AMI

You must upload the bundled AMI to Amazon S3 before it can be accessed by Amazon EC2. Use `ec2-upload-bundle` to upload the bundled AMI that you created earlier. Amazon S3 stores data objects in buckets, which are similar to directories.

Buckets must have globally unique names. The `ec2-upload-bundle` utility uploads the bundled AMI to a specified bucket. If the specified bucket does not exist, it will be created. If the specified bucket exists and belongs to another user, the `ec2-upload-bundle` command will fail.

To upload the bundled AMI

- Enter the following command:

```
# ec2-upload-bundle -b <bucket> -m image.manifest.xml -a <access_key> -s <secret_key>
```

The `<bucket>` is the target bucket, `<access_key>` is your AWS Access Key, and `<secret_key>` is your AWS Secret Key.

The AMI manifest file and all image parts are uploaded to Amazon S3. The manifest file is encrypted with the Amazon EC2 public key before being uploaded.
Sharing AMIs

Topics

- Protecting a Shared AMI
  - Sharing AMIs
  - Making an AMI Public
  - Sharing an AMI with Specific Users
  - Publishing Shared AMIs

This section describes how to build and share AMIs.

Shared AMIs are AMIs that developers build and make available for other AWS developers to use. Building safe, secure, useable AMIs for public consumption is a fairly straightforward process, if you follow a few simple guidelines.

For information on building shared AMIs, see Protecting a Shared AMI. For information on sharing AMIs, see Sharing AMIs
Protecting a Shared AMI

These guidelines are not requirements and you are welcome to follow or ignore them. However, following these guidelines produces a better user experience, helps ensure your users' *instances* are secure, and can protect you.

To build a shared AMI, follow these guidelines:

**Shared AMI Guidelines**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Update the AMI Tools at Boot Time</td>
</tr>
<tr>
<td>2</td>
<td>Disable Password-Based Logins for Root</td>
</tr>
<tr>
<td>3</td>
<td>Install Public Key Credentials</td>
</tr>
<tr>
<td>4</td>
<td>Disable sshd DNS Checks (optional)</td>
</tr>
<tr>
<td>5</td>
<td>Identify Yourself</td>
</tr>
<tr>
<td>6</td>
<td>Protect Yourself</td>
</tr>
<tr>
<td>7</td>
<td>Protect Paid AMIs</td>
</tr>
</tbody>
</table>

*Note*

These guidelines are written for Fedora distributions, but the principles apply to any AMI. You might need to modify the provided examples for other distributions. For other distributions, review their documentation or search the AWS forums in case someone else has done it already.
Update the AMI Tools at Boot Time

We recommend that your AMIs download and upgrade the Amazon EC2 AMI creation tools during startup. This ensures that new AMIs based on your shared AMIs will have the latest AMI tools.

To update the AMI tools at startup on Fedora

- Add the following to rc.local:

```
# Update the Amazon EC2 AMI creation tools
echo " + Updating ec2-ami-tools"
wget http://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
rpm -Uvh ec2-ami-tools.noarch.rpm & & \
echo " + Updated ec2-ami-tools"
```

Use this method to automatically update other software on your image.

Note
When deciding which software to automatically update, consider the amount of WAN traffic that the update will generate (your users will be charged for it) and the risk of the update breaking other software on the AMI.

Note
The preceding procedure applies to Fedora distributions. For other distributions:
- On most Red Hat systems, add these steps to your /etc/rc.d/rc.local script.
- On Gentoo systems, add them to /etc/conf.d/local.local.
- On Ubuntu systems, add them to /etc/rc.local.
- On Debian, you might need to create a start up script in /etc/init.d and use update-rc.d <scriptname> defaults 99 (where <scriptname> is the name of the script you created) and add the steps to this script.
Disable Password-Based Logins for Root

Using a fixed root password for a public AMI is a security risk that can quickly become known. Even relying on users to change the password after the first login opens a small window of opportunity for potential abuse.

To solve this problem, disable password-based logins for the root user. Additionally, we recommend you randomize the root password at boot.

To disable password-based logins for root

1. Open the `/etc/ssh/sshd_config` file with a text editor and locate the following line:

   ```
   #PermitRootLogin yes
   ```

2. Change the line to:

   ```
   PermitRootLogin without-password
   ```

   The location of this configuration file might differ for your distribution, or if you are not running OpenSSH. If this is the case, consult the relevant documentation.

3. To randomize the root password, add the following to your boot process:

   ```
   if [ -f "/root/firstrun" ] ; then
     dd if=/dev/urandom count=50|md5sum|passwd --stdin root
     rm -f /root/firstrun
   else
     echo "* Firstrun *" && touch /root/firstrun
   fi
   ```

   **Note**
   This step assumes that a `/root/firstboot` file is bundled with the image. If file was not created, the root password will never be randomized and will be set to the default.

   **Note**
   If you are using a distribution other than Fedora, you might need to consult the documentation that accompanied the distribution.
Remove SSH Host Key Pairs

If you plan to share an AMI derived from a public AMI, remove the existing SSH host key pairs located in /etc/ssh. This forces SSH to generate new unique SSH key pairs when someone launches an instance using your AMI, improving security and reducing the likelihood of "man-in-the-middle" attacks.

The following list shows the SSH files to remove.

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
Install Public Key Credentials

After configuring the AMI to prevent logging in using a password, you must make sure users can log in using another mechanism.

Amazon EC2 allows users to specify a public-private key pair name when launching an instance. When a valid key pair name is provided to the `RunInstances` API call (or through the command line API tools), the public key (the portion of the key pair that Amazon EC2 retains on the server after a call to `CreateKeyPair`) is made available to the instance through an HTTP query against the instance metadata.

To login through SSH, your AMI must retrieve the key value at boot and append it to `/root/.ssh/authorized_keys` (or the equivalent for any other user account on the AMI). Users will be able to launch instances of your AMI with a key pair and log in without requiring a root password.

```bash
if [ ! -d /root/.ssh ]; then
    mkdir -p /root/.ssh
    chmod 700 /root/.ssh
fi
#
# Fetch public key using HTTP

if [ $? -eq 0 ]; then
    cat /tmp/my-key >> /root/.ssh/authorized_keys
    chmod 600 /root/.ssh/authorized_keys
    rm /tmp/my-key
fi
```

This can be applied to any user account; you do not need to restrict it to root.

**Note**

Rebundling an instance based on this image includes the key with which it was launched. To prevent the key's inclusion, you must clear out (or delete) the `authorized_keys` file or exclude this file from rebundling.
Disable sshd DNS Checks (optional)

Disabling sshd DNS checks slightly weakens your sshd security. However, if DNS resolution fails, SSH logins will still work. If you do not disable sshd checks, DNS resolution failures prevent all logins.

To disable sshd DNS checks

1. Open the `/etc/ssh/sshd_config` file with a text editor and locate the following line:

```
#UseDNS yes
```

2. Change the line to:

```
UseDNS no
```

Note
The location of this configuration file can differ for your distribution or if you are not running OpenSSH. If this is the case, consult the relevant documentation.
Identify Yourself

Currently, there is no easy way to know who provided a shared AMI as each AMI is represented by a numeric user ID.

We recommend that you post a description of your AMI, and the AMI ID, in the Amazon EC2 developer forum. This provides a convenient central location for users who are interested in trying new shared AMIs.
Protect Yourself

The previous sections described how to make your shared AMIs safe, secure, and useable for the users who launch them. This section describes guidelines to protect yourself from the users of your AMI.

We recommend against storing sensitive data or software on any AMI that you share. Users who launch a shared AMI might be able to rebundle it and register it as their own. Follow these guidelines to help you to avoid some easily overlooked security risks:

- Always delete the shell history before bundling. If you attempt more than one bundle upload in the same image, the shell history contains your secret access key.

- Bundling a running instance requires your private key and X.509 certificate. Put these and other credentials in a location that is not bundled (such as the instance store).

- Exclude the ssh authorized keys when bundling the image. The Amazon public images store the public key used to launch an instance with its ssh authorized keys file.

**Note**

Unfortunately, it is not possible for this list of guidelines to be exhaustive. Build your shared AMIs carefully and take time to consider where you might expose sensitive data.
## Protect Paid AMIs

The simplest way to prevent users from rebundling Paid AMIs that you create is to not provide root access to the AMI and to pay attention to security announcements that involve privilege escalations. Amazon EC2 requires you to have root access any AMI that you rebundle.

If you must provide root access to an AMI, Amazon EC2 tools are designed to protect the product code. Although this is effective, it is not guaranteed and users might create AMIs using other tools.

To ensure users cannot rebundle your paid AMIs, we recommend that you configure your application to check the instance metadata to verify that the product code is intact.
Sharing AMIs

Amazon EC2 enables users to share their AMIs with other users. This section describes how to share AMIs using the Amazon EC2 command line tools.

**Note**
Before proceeding, make sure to read the security considerations of sharing AMIs in the [Protecting a Shared AMI](#) section.

AMIs have a `launchPermission` property that controls which users, besides the owner, are allowed to launch instances of that AMI. By modifying an AMI's `launchPermission` property, you can allow all users to launch the AMI (make the AMI public) or only allow a few specific users to launch the AMI.

The `launchPermission` attribute is a list of users and *launch groups*. *Launch permissions* can be granted by adding or removing items from the list. Explicit launch permissions for users are granted or revoked by adding or removing their AWS account IDs. The only launch group currently supported is the `all` group, which makes the AMI public. The rest of this section refers to launch groups simply as groups. Launch groups are not the same as security groups and the two should not be confused. An AMI can have both public and explicit launch permissions.

**Note**
You are not billed when your AMI is launched by other users. Users launching the AMI are billed.

Select from the following:

- [Making an AMI Public](#)
- [Sharing an AMI with Specific Users](#)
- [Publishing Shared AMIs](#)
Making an AMI Public

To make an AMI public

- Add the all group to the AMI's launchPermission attribute using the `ec2-modify-image-attribute` command, where `<ami_id>` is the ID of the AMI.

```prompt
ec2-modify-image-attribute <ami_id> --launch-permission -a all
```

To check the launch permissions of an AMI

- Enter the `ec2-describe-image-attribute` command, where `<ami_id>` is the ID of the AMI.

```prompt
ec2-describe-image-attribute <ami_id> -l
```

To make an AMI private again

- Remove the all group from its launch permissions, where `<ami_id>` is the ID of the AMI.

```prompt
ec2-modify-image-attribute <ami_id> -l -r all
```

This will not affect any explicit launch permissions for the AMI or any running instances of the AMI.

Example

This example makes the ami-2bb65342 AMI public.

```prompt
ec2-modify-image-attribute ami-2bb65342 --launch-permission -a all
```

This example displays the launch permissions of the ami-2bb65342 AMI.
This example removes the all group from the permissions of the ami-2bb65342 AMI, making it private.
Sharing an AMI with Specific Users

You can share an AMI with specific users without making the AMI public. All you need is the user's AWS user's account ID, which is available on the AWS Account Activity page.

To grant explicit launch permissions

- Enter the following command:

```
PROMPT> ec2-modify-image-attribute <ami_id> -l -a <user_id>
```

The `<ami_id>` is the ID of the AMI and `<user_id>` is the user's account ID, without hyphens.

To remove launch permissions for a user

- Enter the following command:

```
PROMPT> ec2-modify-image-attribute <ami_id> -l -r <user_id>
```

The `<ami_id>` is the ID of the AMI and `<user_id>` is the user's account ID, without hyphens.

To remove all launch permissions

- Enter the following command to remove all public and explicit launch permissions:

```
PROMPT> ec2-reset-image-attribute <ami_id> -l
```

The `<ami_id>` is the ID of the AMI.

⚠️ Note

The AMI owner always has rights to the AMI and will be unaffected by the `ec2-` command.
Example

The following example grants launch permissions to the 495219933132 user for the ami-2bb65342 AMI:

```
PROMPT> ec2-modify-image-attribute ami-2bb65342 -l -a 495219933132
launchPermission   ami-2bb65342   ADD   userId   495219933132
```

The following example removes launch permissions from the 495219933132 user for the ami-2bb65342 AMI:

```
PROMPT> ec2-modify-image-attribute ami-2bb65342 -l -r 495219933132
launchPermission   ami-2bb65342   REMOVE  userId   495219933132
```

The following example removes all public and explicit launch permissions from the ami-2bb65342 AMI:

```
PROMPT> ec2-reset-image-attribute ami-2bb65342 -l
launchPermission   ami-2bb65342   RESET
```
Publishing Shared AMIs

After creating a shared AMI, other developers can find it in the EC2 Resource Center.

To publish your AMI, post it in the Public AMIs Folder of the Amazon Web Services Resource Center.

You must include the following information when publishing AMIs:

- AMI ID
- AMI manifest

We recommend including the following information when publishing AMIs:

- Publisher
- Publisher URL
- OS / Distribution
- Key Features
- Description
- Daemons / Services
- Release Notes

You can cut and paste the following template into the document. You must be in HTML edit mode.

```
<strong>AMI ID: </strong>[ami-id]<br />
<strong>AMI Manifest: </strong>[bucket/image.manifest.xml]<br />
<h2>About this AMI;</h2>
<ul>
  <li>Published by [Publisher] (http://www.mysite.com)</li>
</ul>
```
<li>[Key Features] <br />
</li>
<li>[Description]</li>
<li>This image contains the following daemons / services:
<ul>
   <li>[Daemon 1]</li>
   <li>[Daemon 2]</li>
</ul>
</li>
<h2><strong>What's New?</strong></h2>The following changes were made on [Date].
<ul>
   <li>[Release Notes 1]</li>
</ul>
<span style="font-size: x-small; font-family: courier new,courier">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;- [Note 1]</span><br />
<span style="font-size: x-small; font-family: courier new,courier">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;- [Note 2]</span><br />
<span style="font-size: x-small; font-family: courier new,courier">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;- [Note 3]"
Creating Paid AMIs

Topics

- Amazon DevPay and Paid AMIs
  - Product Registration
  - Associating a Product Code with an AMI
  - Sharing Your Paid AMI with Select Users or the Public
  - Confirming an Instance Is Running an AMI Associated with a Product Code
  - Getting the Product Code from Within an Instance
  - Supported AMIs

This section gives an introduction to Amazon DevPay and paid AMIs, which are AMIs you sell to other Amazon EC2 users.
Amazon DevPay and Paid AMIs

A paid AMI is an AMI that you sell to other Amazon EC2 users. They pay you according to the price you set. To be able to create a paid AMI, you use Amazon DevPay. What is Amazon DevPay?

Amazon DevPay is a billing and account management service that enables you to get paid for an AMI you create and that other Amazon EC2 users use. Amazon DevPay creates and manages the order pipeline and billing system for you. Your customers sign up for your AMI, and Amazon DevPay automatically meters their usage of Amazon EC2, bills them based on the pricing you set, and collects their payments. DevPay offers the following:

- You can charge customers for your AMI; the charges can include recurring charges based on the customer's usage Amazon EC2, a fixed one-time charge, and a recurring monthly charge.
- Your customers can easily sign up and pay for your AMI with their trusted Amazon.com accounts.
- Your customers are authenticated, thus ensuring they have access only to what they should.
- If your customers don't pay their bills, DevPay turns off their access to your AMI for you.
- Amazon Payments handles payment processing.

Basic DevPay Flow

1. Your customer uses an Amazon.com account to sign up and pay for your AMI. The sign-up page
indicates that you have teamed up with Amazon Payments to make billing easy and secure.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Your customer pays the price you've defined to use your product.</td>
</tr>
<tr>
<td>3</td>
<td>DevPay subtracts the required DevPay fees and pays you the difference.</td>
</tr>
<tr>
<td>4</td>
<td>You pay the costs of Amazon EC2 that your AMI used.</td>
</tr>
</tbody>
</table>

For more information about Amazon DevPay, refer to the *Amazon DevPay Developer Guide*. 
Summary of How Paid AMIs Work

With a paid AMI, your customers:

- Must be signed up to use Amazon EC2 themselves
- Buy your paid AMI and then launch instances of it
- Always use *their own* AWS credentials when launching instances; you don't launch instances of your paid AMI for them with your credentials
- Pay the price you set for the paid AMI, and not the normal Amazon EC2 rates

The other way to use Amazon EC2 and Amazon DevPay together is with a *supported AMI*. For more information about supported AMIs, see [Supported AMIs](#).

The following figure and table summarize the basic flow for creating and using paid AMIs:

---

**Note**

Detailed information about most of the following steps is provided in the *Amazon DevPay Developer Guide*.

**Paid AMI Process**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>You create an AMI as described elsewhere in this guide.</td>
</tr>
<tr>
<td>2</td>
<td>You register a product with Amazon DevPay.</td>
</tr>
<tr>
<td></td>
<td>For more information, see <a href="#">Product Registration</a>. As part of this process, you provide a product</td>
</tr>
</tbody>
</table>
description, product pricing, etc. This registration process creates a product code for the product and a URL where customers can sign up to use the product (called the purchase URL).

3 You use an Amazon EC2 command or API call to associate the product code with your AMI. For more information, see Associating a Product Code with an AMI. This makes the AMI a paid AMI.

4 You use an Amazon EC2 command or API call to share the AMI with select customers or the public. For more information, see Sharing Your Paid AMI with Select Users or the Public.

Note

Even if you share a paid AMI and it has a product code, no one can use the AMI until they sign up for it (see the following steps).

5 You make your paid AMI available for sale. You can advertise your paid AMI in the Solutions Catalog on the AWS Developer Connection site and on the Amazon Machine Images (AMIs) page on the AWS Resource Center.

6 Customers use the purchase URL you provide to sign up for and purchase your product. If they're not already signed up for Amazon EC2, they'll be prompted to sign up. They purchase your product with their Amazon.com accounts. They must have the credentials needed to launch Amazon EC2 instances. At this point, they have the AMI ID (from step 5).

7 Customers then launch an Amazon EC2 instance specifying the AMI ID. Because you associated the shared AMI with the product code, the customers are charged at the rate you set. For more information, see Paying for AMIs.

Each customer's bill for the AMI is displayed on their Application Billing page, which shows the activity for DevPay products. Also, at any time, you can confirm the customer is still currently subscribed to your product. For more information, refer to the Amazon DevPay Developer Guide.
Association of the Product Code with the Customer's Instance

If you give the customer root access to your paid AMI, the customer can rebundle it. If your customer uses AWS tools to rebundle the AMI, the rebundled AMI inherits the product code. When launching instances of the rebundled AMI, the customer is still billed for usage based on your price. However, if the customer doesn't use the AWS tools when rebundling, the rebundled AMI won't inherit the product code, and the customer will pay normal Amazon EC2 prices and not your price. Also, a customer with root access could find some other way to remove the product code from the AMI.

When a customer contacts you for support for a paid AMI, you can confirm your product code is associated with the AMI and the customer's instance is currently running the AMI. For more information, see Confirming an Instance Is Running an AMI Associated with a Product Code.

If you have software installed on the AMI, the software can retrieve the instance metadata to determine if the product code is associated with the instance. For more information, see Getting the Product Code from Within an Instance.

Keep in mind that the preceding methods for confirming the association of the product code with the instance are not foolproof because a customer with root access to the instance could return false information indicating the product code is associated with the instance.
Product Registration

You must register a product with Amazon DevPay. The product can cover a single AMI that you want to sell or multiple AMIs (only if you want to sell them all at the same price). During registration, you provide product information such as pricing, and you receive information you need to sell your product.

Note
AWS must approve your product after you register it. The approval process takes several business days.

You provide the following information during registration:

- Company name
- Product name
- Product description (as you want your customers to see it)
- Redirect URL (the page you want customers to see after they have purchased the product)
- Any terms and conditions you want displayed (optional)
- Contact e-mail address and telephone number (to be used by AWS and not displayed to customers)
- Contact e-mail or URL (to be displayed to customers)
- Pricing for use of the product

The information you display at the redirect URL should give information about the AMI.

Registration provides you with the following information:

- Product code
- Product token
• Purchase URL

You need the product code and purchase URL to integrate your product with DevPay as described in [Summary of How Paid AMIs Work](#) and [Supported AMIs](#). You need the product token if you're going to set up your system to later verify whether a customer is still subscribed to your product. For more information, refer to the *Amazon DevPay Developer Guide*.

**Important**

The *Amazon DevPay Developer Guide* covers the procedure for registering your product with Amazon DevPay. Before you register your product, we recommend you read the information in that guide about how to set your AMI's price and how billing for Amazon DevPay products works.
Associating a Product Code with an AMI

You must be the owner of an AMI to associate a product code with it. Each AMI can have only a single product code associated with it, but you can associate a single product code with more than one AMI. You might do this if you have similar versions of an AMI (for example, a 32-bit version and a 64-bit version), you've assigned them all the same price, and you'd like to minimize the number of Amazon DevPay product codes you have (to make your bookkeeping easier).

To associate a product code with an AMI

- Enter the following command:

  ```shell
  PROMPT> ec2-modify-image-attribute <ami_id> --product-code <product_code>
  ```

  The `<ami_id>` is the AMI ID and `<product_code>` is the product code.

To verify the product code is associated with the AMI

- Enter the following command:

  ```shell
  PROMPT> ec2-describe-image-attribute <ami_id> --product-code
  ```

  You can't change or remove the `productCodes` attribute after you've set it. If you want to use the same image without the product code or associate a different product code with the image, you must reregister the image to obtain a new AMI ID. You can then use that AMI without a product code or associate the new product code with the AMI ID.

Example

The following example associates the ami-2bb65342 AMI with the 774F4FF8 product code.
This example verifies that the product code is associated with the AMI.
Sharing Your Paid AMI with Select Users or the Public

After you associate the product code with the AMI, you need to share the AMI with select customers or the public by using the `ec2-modify-image-attribute` command.

**To share the AMI**

- Enter the following command:

```
PROMPT> ec2-modify-image-attribute <ami_id> --launch-permission -a all
```

The `<ami_id>` is the AMI ID.

Even though you've shared the AMI, no one can use it until they sign up for your product by going to the purchase URL. Once customers sign up, any instances of the paid AMI they launch will be billed at the rate you specified during product registration.

**Example**

The following example shares the ami-2bb65342 AMI with the public.

```
PROMPT> ec2-modify-image-attribute ami-2bb65342 --launch-permission -a all
launchPermission      ami-2bb65342    ADD    group    all
```
Confirming an Instance Is Running an AMI Associated with a Product Code

If you have created a product for others to use with their AMIs (the supported AMI scenario), you might want to confirm that a particular AMI is associated with your product code and a particular instance is currently running that AMI.

**Note**
You must be the owner of the product code to successfully call `ec2-confirm-product-instance` with that product code. Because your customers don't own the product code, they should describe their instances to confirm their instances are running with your product code.

**To confirm an instance is running an AMI associated with your product code**

- Enter the following command:

```
PROMPT> ec2-confirm-product-instance <product_code> -i <instance>
```

The `<product_code>` is the product code and `<instance>` is the instance.

If the AMI is associated with the product code, `true` is returned with the AMI owner's account ID. Otherwise, `false` is returned.

**Example**

The following example confirms whether the i-10a64379 instance is running the 6883959E product code.

```
PROMPT> ec2-confirm-product-instance 6883959E -i i-10a64379
6883959E i-10a64379 true 495219933132
```
Getting the Product Code from Within an Instance

A running Amazon EC2 instance can determine if has an Amazon DevPay product code. The instance retrieves the product code similarly to how retrieves other metadata. For more information about retrieving metadata, see Instance Metadata.

To retrieve a product code, query a web server with this REST-like API call:

```
```

Amazon EC2 returns a response similar to the following:

```
774F4FF8
```
Supported AMIs

Supported AMIs are different from paid AMIs. With a supported AMI, you charge for software or a service you provide that customers use with their own AMIs. The following figure and table summarizes the flow for creating and using supported AMIs.

**Supported AMI Process**

1. You register a product with Amazon DevPay. For more information, see [Product Registration](#). As part of this process, you provide a product description, product pricing, etc. This registration process creates a product code for the product and a URL where customers can sign up to use the product (called the *purchase URL*).

2. You make your product available for sale.

3. Customers use the *purchase URL* to sign up for and purchase your product. If they're not already signed up for Amazon EC2, they'll be prompted to sign up. They purchase your product with their Amazon.com accounts. They must have the credentials needed to launch Amazon EC2 instances. At this point, they have the product code (from step 2).

4. Customers then use an Amazon EC2 command or API call to associate the product code with their AMIs. For more information, see [Associating a Product Code with an AMI](#).

5. Customers then launch one or more instances of the AMIs. Because the customers associated their AMIs with the product code, they are charged at the rate you set.

Each customer's bill for the AMI is displayed on their Application Billing page, which shows the activity for DevPay products. For more information, refer to the *Amazon DevPay Developer Guide*.

When a customer contacts you for support for an AMI, you can confirm your
product code is associated with the AMI and the customer's instance is currently running the AMI. For more information, see Confirming an Instance Is Running an AMI Associated with a Product Code.
Launching and Using Instances

Topics

- Instance Usage
- Instance Types
- Instance Metadata
- Instance Storage
- Availability Zones
- Using Shared AMIs
- Paying for AMIs
- Get Console Output and Reboot Instances

This section describes how to launch instances and retrieve instance-specific data from within the instance. It also covers launching shared AMIs and security risks associated with running shared AMIs.
Instance Usage

The instance is your basic computation building block. Amazon EC2 offers multiple instance types from which you can choose. You can run as many or as few instances as you need at any given time.

For information about available instance types, see Instance Types.

Once launched, an instance looks very much like a traditional host. You have complete control of your instances; you have root access to each one and you can interact with them as you would any machine.

Here are some suggestions for making the best use of Amazon EC2 instances:

- Do not rely on an instance's local storage for valuable, long-term data.
  
  When instances fail, the data on the local disk is lost. Use a replication strategy across multiple instances to keep your data safe or store your persistent data in Amazon S3

- Define images based on the type of work they perform.
  
  For "Internet applications," you might define one image for database instances and another for web servers. Image creation and storage are cheap and easy operations, so you can individualize and customize as necessary. Specialized images can result in smaller AMI sizes, which will boot considerably faster.

- Monitor the health of your instances.
  
  You can make your instances work for you by configuring them to monitor each other. For example, you could create an image that contains an open-source monitoring tool such as Nagios or OpenNMS. Then, your other instances could report their health to the monitoring instance.

- Keep your Amazon EC2 firewall permissions as restrictive as possible.
  
  Only open up permissions that you require. Use separate groups to deal with instances that have different security requirements. Consider using
additional security measures inside your instance (such as using your own firewall). If you need to log in interactively (ssh), consider creating a bastion security group that allows external login and keep the remainder of your instances in a group that does not allow external login.
Instance Types

Amazon EC2 instances are grouped into two families: standard and High-CPU. Standard instances have memory to CPU ratios suitable for most general purpose applications; High-CPU instances have proportionally more CPU resources than memory (RAM) and are well suited for compute-intensive applications. When selecting instance types, you might want to use less powerful instance types for your web server instances and more powerful instance types for your database instances. Additionally, you might want to run CPU instance types for CPU-intensive data processing tasks.

One of the advantages of EC2 is that you pay by the instance hour, which makes it convenient and inexpensive to test the performance of your application on different instance families and types. One good way to determine the most appropriate instance family and instance type is to launch test instances and benchmark your application.
Available Instance Types

The instance types described in the following table are available.

<table>
<thead>
<tr>
<th>Type</th>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
<th>Platform</th>
<th>I/O</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>1 EC2 Compute Unit (1 virtual core with 1 EC2 Compute Unit)</td>
<td>1.7 GB</td>
<td>160 GB instance storage (150 GB plus 10 GB root</td>
<td>32-bit</td>
<td>Moderate</td>
<td>m1.small</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>partition)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large</td>
<td>4 EC2 Compute Units (2 virtual cores with 2 EC2 Compute Units each)</td>
<td>7.5 GB</td>
<td>850 GB instance storage (2 x 420 GB plus 10 GB root</td>
<td>64-bit</td>
<td>High</td>
<td>m1.large</td>
</tr>
<tr>
<td>Extra</td>
<td>8 EC2 Compute Units (4 virtual cores with 2 EC2 Compute Units each)</td>
<td>15 GB</td>
<td>1690 GB instance storage (4 x 420 GB plus 10 GB root</td>
<td>64-bit</td>
<td>High</td>
<td>m1.xlarge</td>
</tr>
<tr>
<td>Large</td>
<td></td>
<td></td>
<td>partition)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High-CPU</td>
<td>5 EC2 Compute Units (2 virtual cores with 2.5 EC2 Compute Units each)</td>
<td>1.7 GB</td>
<td>350 GB instance storage (340 GB plus 10 GB root</td>
<td>32-bit</td>
<td>Moderate</td>
<td>c1.medium</td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td>partition)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High-CPU</td>
<td>20 EC2 Compute Units (8 virtual cores with 2.5 EC2 Compute Units each)</td>
<td>7 GB</td>
<td>1,690 GB instance storage (4 x 420 GB plus 10 GB root</td>
<td>64-bit</td>
<td>High</td>
<td>c1.xlarge</td>
</tr>
<tr>
<td>Extra</td>
<td></td>
<td></td>
<td>partition)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note

The small instance type is the original Amazon EC2 instance type available since the launch of Amazon EC2. It is the default instance type for all customers. To use other instance types, you must specify them through the RunInstances operation.

Important

We strongly recommend using the 2.6.18 Xen stock kernel with the c1.medium and c1.xlarge instances. Although the default Amazon EC2 kernels will work, the new kernels provide greater stability and performance for these instance types. For more information about kernels, see Kernels, RAM Disks, and Block Device Mappings.
Measuring Compute Resources

Transitioning to a utility computing model changes how developers are trained to think about CPU resources. Instead of purchasing or leasing a particular processor to use for several months or years, you are renting capacity by the hour. Because Amazon EC2 is built on commodity hardware, over time there might be several different types of physical processors underlying different virtual EC2 instances. Our goal is to provide a consistent amount of CPU capacity regardless of the actual underlying hardware.

Amazon EC2 uses a variety of measures to provide each instance with a consistent and predictable amount of CPU capacity. To make it easy for developers to compare CPU capacity between different instance types, we defined an Amazon EC2 Compute Unit.

Note

We use several internal benchmarks and tests to manage the consistency and predictability of the performance of an Amazon EC2 Compute Unit. For more information, go to the Instance page.

To find out which instance will work best for your application, we recommend launching an instance and using your own benchmark application. This will help you determine which instance type works best for your specific use case.
I/O Resources

Amazon EC2 provides virtualized server instances. While some resources like CPU, memory and instance storage are dedicated to a particular instance, other resources like the network and the disk subsystem are shared amongst instances. If each instance on a physical host tries to use as much of one of these shared resources as possible, each will receive an equal share of that resource. However, when a resource is under-utilized you will often be able to consume a higher share of that resource while it is available.

The different instance types will provide higher or lower minimum performance from the shared resources depending on their size. Each of the instance types has an I/O performance indicator (moderate or high). Instance types with high I/O performance have a larger allocation of shared resources. Allocating larger share of shared resources also reduces the variance of I/O performance. For most applications, moderate I/O performance is more than enough. However, for applications that require greater or more consistent I/O performance, consider instances with high I/O performance.
Instance Metadata

Amazon EC2 instances can access instance-specific metadata as well as data supplied when launching the instances. This data can be used to build more generic AMIs that can be modified by configuration files supplied at launch time.

If you run web servers for various small businesses, they can all use the same AMI and retrieve their content from the Amazon S3 bucket you specify at launch.

To add a new customer at any time, simply create a bucket for the customer, add their content, and launch your AMI.
# Categories of Available Data

The data available to instances is categorized into metadata and user-supplied data.

Metadata is specific to an instance and is described in the following table.

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
<th>Version Introduced</th>
</tr>
</thead>
<tbody>
<tr>
<td>ami-id</td>
<td>The AMI ID used to launch the instance.</td>
<td>1.0</td>
</tr>
<tr>
<td>ami-launch-index</td>
<td>The index of this instance in the reservation (per AMI).</td>
<td>1.0</td>
</tr>
<tr>
<td>ami-manifest-path</td>
<td>The manifest path of the AMI with which the instance was launched.</td>
<td>1.0</td>
</tr>
<tr>
<td>ancestor-ami-ids</td>
<td>The AMI IDs of any instances that were rebundled to create this AMI.</td>
<td>2007-10-10</td>
</tr>
<tr>
<td>block-device-mapping</td>
<td>Defines native device names to use when exposing virtual devices.</td>
<td>2007-10-10</td>
</tr>
<tr>
<td>instance-id</td>
<td>The ID of this instance.</td>
<td>1.0</td>
</tr>
<tr>
<td>instance-type</td>
<td>The type of instance to launch. For more information, see Instance Types.</td>
<td>2007-08-29</td>
</tr>
<tr>
<td>local-hostname</td>
<td>The local hostname of the instance.</td>
<td>2007-01-19</td>
</tr>
<tr>
<td>local-ipv4</td>
<td>Public IP address if launched with direct addressing; private IP address if launched with public addressing.</td>
<td>1.0</td>
</tr>
<tr>
<td>kernel-id</td>
<td>The ID of the kernel launched with this instance, if applicable.</td>
<td>2008-02-01</td>
</tr>
<tr>
<td>placement/availability-zone</td>
<td>The availability zone in which the instance launched.</td>
<td>2008-02-01</td>
</tr>
<tr>
<td>product-codes</td>
<td>Product codes associated with this instance.</td>
<td>2007-03-01</td>
</tr>
<tr>
<td>public-hostname</td>
<td>The public hostname of the instance.</td>
<td>2007-01-19</td>
</tr>
<tr>
<td>public-ipv4</td>
<td>NATted public IP Address</td>
<td>2007-01-19</td>
</tr>
<tr>
<td>public-keys/</td>
<td>Public keys. Only available if supplied at instance launch time</td>
<td>1.0</td>
</tr>
<tr>
<td>ramdisk-id</td>
<td>The ID of the RAM disk launched with this instance, if applicable.</td>
<td>2008-02-01</td>
</tr>
<tr>
<td>reservation-id</td>
<td>ID of the reservation.</td>
<td>1.0</td>
</tr>
<tr>
<td>security-groups</td>
<td>Names of the security groups the instance is launched in. Only</td>
<td>1.0</td>
</tr>
</tbody>
</table>
User-supplied data is treated as opaque data: what you give us is what you get back.

**Note**

- All instances launched together get the same user-supplied data. You can use the AMI launch index as an index into the data.
- User data is limited to 16K. This limit applies to the data in raw form, not base64 encoded form.
- The user data must be base64 encoded before being submitted to the API. The API command-line tools perform the base64 encoding for you. The data is in base64 and is decoded before presented to the instance.
Data Retrieval

An instance retrieves the data by querying a web server using a Query API. The base URI of all requests is http://169.254.169.254/2008-05-05/ where 2008-05-05 indicates the API version.

Note
Amazon EC2 Version 1.0 is part of a legacy versioning scheme. Newer versions follow a date based versioning scheme. For more information on the versioning scheme used by Amazon EC2, see API Versioning.

The latest version of the API is always available using the URI http://169.254.169.254/latest.

Security of Launch Data

Although only your specific instance can access launch data, the data is not protected by cryptographic methods. You should take suitable precautions to protect sensitive data (such as long lived encryption keys).

Note
You are not billed for HTTP requests used to retrieve metadata and user-supplied data.

Retrieving Metadata

Requests for a specific metadata resource returns the appropriate value or a 404 HTTP error code if the resource is not available. All metadata is returned as text (content type text/plain).

Requests for a general metadata resource (i.e. an URI ending with a /) return a list of available resources or a 404 HTTP error code if there is no such resource. The list items are on separate lines terminated by line feeds (ASCII 10).

Example

The following examples list HTTP GET requests and responses. You can use a
tool such as curl or wget to make these types of requests.

This example gets the available API versions.

```
GET http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2008-05-05
```

This example gets the top-level metadata items.

```
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
instance-id
instance-type
local-hostname
local-ipv4
placement/
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
```

This example gets the value of each metadata item from the preceding example.

```
```
This example gets the list of available public keys.

```
0=my-public-key
```

This example shows the formats in which public key 0 is available.

```
openssh-key
```

This example gets public key 0 (in openssh-key format).

```
ssh-rsa AAAA.....wZEf my-public-key
```

This example gets the product code.

```
774F4FF8
```

**Retrieving User Data**

Requests for the user data returns the data as-is (content type application/x-octetstream).

![Note](image)

All user-supplied data is treated as opaque data; what you give us is what you get back. It is the responsibility of the instance to interpret this data appropriately.

**Example**

This shows an example of returning comma-separated user-supplied data.

```
1234,fred,reboot,true | 4512,jimbo, | 173,,,
```
This shows an example of returning line-separated user-supplied data.

```
[general]
instances: 4

[instance-0]
s3-bucket: fred

[instance-1]
reboot-on-error: yes
```
Use Case: AMI Launch Index Value

In this example, Alice wants to launch four instances of her favorite database AMI with the first acting as master and the remainder acting as replicas.

The master database configuration specifies various database parameters (e.g., the size of store) while the replicas' configuration specifies different parameters, such as the replication strategy. Alice decides to provide this data as an ASCII string with a pipe symbol (| delimiting the data for the various instances:

```
store-size=123PB backup-every=5min | replicate-every=1min | replicate-every=2min | replicate-every=10min | replicate-every=20min
```

The store-size=123PB backup-every=5min defines the master database configuration, replicate-every=1min defines the first replicant's configuration, replicate-every=2min defines the second replicant's configuration, and so on.

Alice launches four instances.

```
$ ec2-run-instances ami-2bb65342 -n 4 -d "store-size=123PB backup-every=5min | replicate-every=1min | replicate-every=2min | replicate-every=10min | replicate-every=20min"
```

Once launched, all instances have a copy of the user data and the common metadata shown here:

- AMI id: ami-2bb65342
- AMI manifest path: ec2-public-images/getting-started.manifest.xml
- Reservation ID: r-fea54097
- Public keys: none
- Security group names: default
- Instance type: m1.small

However each instance has certain unique metadata.

**Instance 1**

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance-id</td>
<td>i-3ea74257</td>
</tr>
<tr>
<td>ami-launch-index</td>
<td>0</td>
</tr>
<tr>
<td>public-hostname</td>
<td>ec2-67-202-51-223.compute-1.amazonaws.com</td>
</tr>
<tr>
<td>public-ipv4</td>
<td>67.202.51.223</td>
</tr>
<tr>
<td>local-hostname</td>
<td>ip-10-251-50-35.ec2.internal</td>
</tr>
<tr>
<td>local-ipv4</td>
<td>10.251.50.35</td>
</tr>
</tbody>
</table>

**Instance 2**

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance-id</td>
<td>i-31a74258</td>
</tr>
<tr>
<td>ami-launch-index</td>
<td>1</td>
</tr>
<tr>
<td>public-hostname</td>
<td>ec2-67-202-51-224.compute-1.amazonaws.com</td>
</tr>
<tr>
<td>public-ipv4</td>
<td>67.202.51.224</td>
</tr>
<tr>
<td>local-hostname</td>
<td>ip-10-251-50-36.ec2.internal</td>
</tr>
<tr>
<td>local-ipv4</td>
<td>10.251.50.36</td>
</tr>
</tbody>
</table>

**Instance 3**

<table>
<thead>
<tr>
<th>Metadata</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance-id</td>
<td>i-31a74259</td>
</tr>
<tr>
<td>ami-launch-index</td>
<td>2</td>
</tr>
<tr>
<td>public-hostname</td>
<td>ec2-67-202-51-225.compute-1.amazonaws.com</td>
</tr>
<tr>
<td>public-ipv4</td>
<td>67.202.51.225</td>
</tr>
<tr>
<td>local-hostname</td>
<td>ip-10-251-50-37.ec2.internal</td>
</tr>
</tbody>
</table>
Therefore, an instance can determine its portion of the user-supplied data through the following process.

**Metadata Discovery Process**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 1 | Determine the instance in the launch group.  
| 2 | Retrieve the user data.  
store-size=123PB backup-every=5min | replicate-every=1min |
| 3 | Extract the appropriate part of the user data.  
user_data.split('|')[ami_launch_index] |
Instance Storage

Every instance includes a fixed amount of storage space on which you can store data. Within this document, it is referred to as the "instance store" as it is not designed to be a permanent storage solution.

If an instance reboots (intentionally or unintentionally), the data on the instance store will survive. If the underlying drive fails or the instance is terminated, the data will be lost.

We highly recommend backing up important data to Amazon S3.
## Storage Locations

Storage is exposed on the instance types as described in the following table.

<table>
<thead>
<tr>
<th>Location</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sda1</td>
<td>Formatted and mounted as root (/) on all instance types</td>
</tr>
<tr>
<td>/dev/sda2</td>
<td>Formatted and mounted as /mnt on m1.small and c1.medium instances</td>
</tr>
<tr>
<td>/dev/sda3</td>
<td>Formatted and mounted as /swap on m1.small and c1.medium instances</td>
</tr>
<tr>
<td>/dev/sdb</td>
<td>Formatted and mounted as /mnt on m1.large, m1.xlarge, and c1.xlarge instances</td>
</tr>
<tr>
<td>/dev/sdc</td>
<td>Available on m1.large, m1.xlarge, and c1.xlarge instances; not mounted</td>
</tr>
<tr>
<td>/dev/sdd</td>
<td>Available on m1.xlarge and c1.xlarge instances; not mounted</td>
</tr>
<tr>
<td>/dev/sde</td>
<td>Available on m1.xlarge and c1.xlarge instances; not mounted</td>
</tr>
</tbody>
</table>

**Note**

Depending on the instance type, some instance stores are not mounted or formatted. To mount and format an instance store, use the Unix `mount` and `mkfs` commands. For added security and safety, we recommend using an encrypted file system.
Disk Performance Optimization

Due to how Amazon EC2 virtualizes disks, the first write to any location on an instance’s drives will perform slower than subsequent writes. For most applications, amortizing this cost over the lifetime of the instance will be acceptable. However, if you require high disk performance, we recommend initializing drives by writing once to every drive location before production use.

To initialize the stores, use the following commands on the m1.large, m1.xlarge, and c1.xlarge instance types:

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M  (m1.xlarge only)
dd if=/dev/zero of=/dev/sde bs=1M  (m1.xlarge only)
```

To perform the initialization on all drives at the same time, use the following command:

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

*Note*
Make sure to unmount the drive before performing this command.

Initialization can take a long time (about 8 hours for an extra large instance).
RAID Configuration

Configuring drives for RAID initializes them by writing to every drive location. When configuring software-based RAID, make sure to change the minimum reconstruction speed:

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

**Note**

You cannot use iostat (part of the sar System Activity Reporting package) to watch performance. You also cannot watch `cat /proc/mdstat'.
Availability Zones

Amazon operates state-of-the-art, highly available data center facilities. However, failures can occur that affect the availability of instances that are in the same location. Although this is rare, if you host all your Amazon EC2 instances in a single location that is affected by such a failure, your instances will be unavailable.

Amazon EC2 provides the ability to place instances in multiple locations. Amazon EC2 locations are composed of availability zones and regions. Regions are geographically dispersed and located in separate geographic areas or countries. Currently, Amazon EC2 exposes only a single region with multiple availability zones. Availability zones are distinct locations that are engineered to be insulated from failures in other availability zones and provide inexpensive, low latency network connectivity to other availability zones in the same region. Regions consist of one or more availability zones. By launching instances in separate availability zones, you can protect your applications from the failure of a single location.

For example, if you have instances distributed across three availability zones and one of them fails, you can design your application so the instances in the remaining availability zones handle any requests.

**Note**

You can use availability zones in conjunction with elastic IP addresses to remap IP addresses across availability zones. For information on elastic IP addresses, see [Elastic IP Addresses](#).
Availability Zone Selection

When you launch an instance, you can optionally specify an availability zone. If you do not specify an availability zone, Amazon EC2 selects one for you. When launching your initial instances, we recommend accepting the default availability zone, which will allow Amazon EC2 to select the best the availability zone for you based on system health and available capacity. Even if you have other instances running, you might consider not specifying an availability zone if your new instances do not need to be close to, or separated from, your existing instances.

To view the availability zones available to you

- Enter the following command:

```
$ ec2-describe-availability-zones
AVAILABILITYZONE     us-east-1a     available
AVAILABILITYZONE     us-east-1b     available
AVAILABILITYZONE     us-east-1c     available
```

Note
Availability zones are not the same across accounts. The availability zone us-east-1a for account A is not necessarily the same as us-east-1a for account B. Zone assignments are mapped independently for each account.

After determining the availability zones that are available to you, you can launch instances in any of the zones.

Note
You will be charged a small bandwidth charge for data that crosses availability zones. For more information, go to the Amazon EC2 portal page.
Using Shared AMIs

This section describes how to find and safely use shared AMIs. One of the easiest ways to get started with Amazon EC2 is to use a shared AMI that has the components you need and add custom content.
Finding Shared AMIs

To find shared AMIs

- Enter the `ec2-describe-images` command (or the abbreviated `ec2dim` command) with a flag to filter the results.

Example

This command displays a list of all public AMIs.

```
PROMPT> ec2dim -x all
```

The `-x all` flag shows AMIs executable by all users. This includes AMIs you own.

This command displays a list of AMIs for which you have explicit launch permissions.

```
PROMPT> ec2dim -x self
```

AMIs that you own are excluded from the list.

This command displays a list of AMIs owned by Amazon.

```
PROMPT> ec2dim -o amazon
```

This command displays a list of AMIs owned by a particular user.

```
PROMPT> ec2dim -o <target_uid>
```

The `<target_uid>` is the account ID of the user who owns the AMIs for which you are looking.
Safe Use of Shared AMIs

AMIs are launched at the user's own risk. Amazon cannot vouch for the integrity or security of AMIs shared by other users. Therefore, you should treat shared AMIs as you would any foreign code that you might consider deploying in your own data center and perform the appropriate due diligence.

Ideally, you should get the AMI ID from a trusted source (a website, another user, etc). If you do not know the source of an AMI, we recommended that you search the forums for comments on the AMI before launching it. Conversely, if you have questions or observations about a shared AMI, feel free to use the AWS forums to ask or comment.

Amazon's public images have an aliased owner and display amazon in the userId field. This allows you to find Amazon's public images easily.

**Note**

Users cannot alias an AMI's owner.

If you plan to use a shared AMI, review the following table to confirm the AMI is not doing anything malicious.

### Launch Confirmation Process

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Check the ssh authorized keys file. The only key in the file should be the key you used to launch the AMI.</td>
</tr>
<tr>
<td>2</td>
<td>Check open ports and running services.</td>
</tr>
<tr>
<td>3</td>
<td>Change the root password if is not randomized on startup. For more information on randomizing the root password on startup, see <a href="#">Disable Password-Based Logins for Root</a>.</td>
</tr>
<tr>
<td>4</td>
<td>Check if ssh allows root password logins. See <a href="#">Disable Password-Based Logins for Root</a> for more information on disabling root based password logins.</td>
</tr>
<tr>
<td>5</td>
<td>Check whether there are any other user accounts that might allow backdoor entry to your instance. Accounts with super user privileges are particularly dangerous.</td>
</tr>
<tr>
<td>6</td>
<td>Verify that all cron jobs are legitimate.</td>
</tr>
</tbody>
</table>
Paying for AMIs

- Finding Paid AMIs
- Purchasing a Paid AMI
- Launching Paid AMIs
- Paying for Support
- Bills for Paid and Supported AMIs

Amazon EC2 integrates with Amazon DevPay, allowing developers to charge users for the use of their AMIs or to provide support for instances. To learn more about Amazon DevPay refer to the *Amazon DevPay Developer Guide*. For more information about charging for your use of your AMIs, or providing support, see *Creating Paid AMIs*

This section describes how to discover paid AMIs, launch paid AMIs, and launch instances with a support product code. Paid AMIs are AMIs you can purchase from other developers.
Finding Paid AMIs

There are several ways you can determine what paid AMIs are available for you to purchase. You can look for information about them on the Amazon EC2 resource center and forums. Alternatively, a developer might give you information about a paid AMI directly.

You can also tell if an AMI is a paid AMI by describing the image with the `ec2-describe-images` command. This command lists the product code associated with an AMI (see the following example). If the AMI is a paid AMI, it has a product code. Otherwise, it does not. You can then go to the Amazon EC2 resource center and forums, which might have more information about the paid Amazon EC2 and where you can sign up to use it.

Note
You must sign up for a paid AMI before you can launch it.

To check if an AMI is paid

- Enter the following command:

  ```bash
  $ ec2-describe-images <ami_id>
  ```

  The `<ami_id>` is the AMI ID.

  The command returns the following:

  ```
  IMAGE <ami_id> <manifest> <user_id>, <status> {private | public} <product_code>
  ```

  The `<ami_id>` is the AMI ID, `<manifest>` is the manifest location, `<user_id>` is the ID of the user that owns the AMI, `<status>` indicates whether the AMI is available, and `<product_code>` is the product code associated with the AMI. If a product code is present, the AMI is a paid AMI.
Example

This example shows an `ec2-describe-images` call describing a paid AMI. The product code is 774F4FF8.

```
$ ec2-describe-images ami-2bb65342
IMAGE ami-2bb65342 awesome-ami/webserver.manifest.xml 495219933132 available private 774F4
```
Purchasing a Paid AMI

You must sign up for (purchase) the paid AMI before you can launch it.

Typically a seller of a paid AMI presents you with information about the AMI, its price, and a link where you can buy it. When you click the link, you're first asked to log in with an Amazon.com login, and then you are taken to a page where you see the paid AMI's price and you confirm you want to purchase the AMI.
Launching Paid AMIs

This section describes how to launch paid AMIs and launch instances with a support product code.

After you purchase a paid AMI, you can launch instances of it. Launching a paid AMI is the same as launching any other AMI. No additional parameters are required. The instance will be charged according to the rates set by the owner of the AMI (which will be more than the base Amazon EC2 rate).

To launch a paid AMI

- Enter the following command:

  ```
  $ ec2-run-instances <ami_id>
  ```

  The `<ami_id>` is the AMI ID.

  **Note**

  The owner of a paid AMI will be able to confirm if a particular instance was launched using their paid AMI.

Example

This example shows the command used to launch the ami-2bb65342 AMI.

```
Paying for Support

The paid AMI feature also allows developers to offer support for software (or derived AMIs). Developers can create support products that you can sign up to use. With this model, the developer provides you with a product. During sign-up for the product, the developer gives you a product code for that product, which you must then associate with your own AMI. This allows the developer to confirm that your instance is eligible for support. It also ensures that when you run instances of the product, you are charged according to the developer's terms for the product.

To associate the product code with your AMI

- Enter the `ec2-modify-image-attribute` command:

  ```text
  PROMPT> ec2-modify-image-attribute <ami_id> --product-code <product_code>
  ```

  The `<ami_id>` is the AMI ID and `<product_code>` is the product code.

  **Important**
  Once set, the product code attribute cannot be changed or removed.

  To launch a paid AMI, no additional parameters are required for the `run-instances`. The instance is charged according to the rates set by the AMI owner.

**Example**

The following command associates the `ami-2bb65342` AMI with the `774F4FF8` product code.

  ```text
  PROMPT> ec2-modify-image-attribute ami-2bb65342 --product-code 774F4FF8
  productCodes ami-2bb65342 productCode 774F4FF8
  ```

  The following command launches the `ami-2bb65342` paid AMI.
$ ec2-run-instances ami-2bb65342
RESERVATION r-a034c7c9 924417782495 default
INSTANCE i-400df629 ami-2bb65342 pending 0 m1.small 2008-03-21T18:49:33+0000 us-east-1c
Bills for Paid and Supported AMIs

At the end of each month, you receive an e-mail with the amount your credit card has been charged for using the paid or supported AMIs during the month. This bill is separate from your regular Amazon EC2 bill.

At any time, you can view the usage information for your paid and supported AMIs (go to http://www.amazon.com/dp-applications).
Get Console Output and Reboot Instances

Console output is a valuable tool for problem diagnosis. It is especially useful for troubleshooting kernel problems and service configuration issues that could cause an instance to terminate or become unreachable before its SSH daemon can be started.

Similarly, the ability to reboot instances that are otherwise unreachable is valuable for both troubleshooting and general instance management.

Amazon EC2 instances do not have a physical monitor through which you can view their console output. They also lack physical controls that allow you to power up, reboot, or shut them down. To allow these actions, we provide them through the Amazon EC2 SOAP API, Query API, and command-line tools.
Get Console Output

The Amazon EC2 instance console output displays the exact console output that would normally be displayed on a physical monitor attached to a machine. This output is buffered because the instance produces it and then posts it to a store where the instances owner can retrieve it.

The posted output is not continuously updated; only when it is likely to be of the most value. This includes shortly after instance boot, after reboot, and when the instance terminates.

**Note**

Only the most recent 64 KB of posted output is stored, which is available for at least 1 hour after the last posting.

You can retrieve the console output for an instance through the SOAP API call described in GetConsoleOutput, the Query API call described in GetConsoleOutput, and the command line tool described in ec2-get-console-output.

**Note**

Only the instance owner can access the console output.
Reboot Instances

Just as you can reset a machine by pressing the reset button, you can reset Amazon EC2 instances through the SOAP API described in RebootInstances, the Query API described in RebootInstances, and the command line tool described in ec2-reboot-instances.
Instance Addressing and Network Security

Topics

- Instance Addressing
- Network Security

This section provides information on the IP addresses that are assigned to instances and how to configure the firewall provided by Amazon EC2.
Instance Addressing

All Amazon EC2 instances are assigned two IP addresses at launch: a private address (RFC 1918), and a public address. The public IP address is directly mapped to the private address through Network Address Translation (NAT). Private addresses are only reachable from within the Amazon EC2 network. Public addresses are reachable from the Internet.

Amazon EC2 also provides an internal DNS name and a public DNS name which map to the private and public IP addresses respectively. The internal DNS name can only be resolved within Amazon EC2. The public DNS name resolves to the public IP address outside the Amazon EC2 network and the private IP address within the Amazon EC2 network.

Note

If you require persistent Internet routable IP addresses that can be assigned to and removed from instances as necessary, use elastic IP addresses. For more information, see Elastic IP Addresses.
Private (RFC 1918) Addresses

All Amazon EC2 instances are allocated a private address by DHCP. These ranges are defined in RFC 1918, are only routable within Amazon EC2, and are used for communication between instances. For more information, go to RFC 1918.

This private address is associated exclusively with the instance for its lifetime and is only returned to Amazon EC2 when the instance terminates.

Always use the internal address when you are communicating between Amazon EC2 instances. This ensures that your network traffic follows the highest bandwidth, lowest cost, and lowest latency path through our network.

To determine your IP address

1. Connect to the instance.

2. Enter one of the following commands:

   ○ PROMPT> **ifconfig eth0**
   

The second option refers to the instance data. For more information, see Instance Metadata.
Internal DNS Name

Each instance is provided an internal DNS name in the form ip-10-251-157-188.ec2.internal. It will resolve to the private IP address of the instance from within Amazon EC2; it will not resolve outside of Amazon EC2.
Public Addresses

At launch, a public address is also associated with each Amazon EC2 instance using Network Address Translation (NAT). For more information about NAT, go to "RFC 1631: The IP Network Address Translator (NAT)".

This public address is associated exclusively with the instance until it is terminated or replaced with an elastic IP address.

⚠️ Important
Amazon EC2 instances that access other instances through their public NAT IP address are charged for regional data transfer.

The following example shows how you can determine your public IP address from your instance by referring to the instance data.

Public DNS

Each instance is provided an external DNS name in the form `ec2-72-44-45-204.compute-1.amazonaws.com`. This DNS name resolves to the public IP address of the instance outside the Amazon EC2 network and the private IP address from within Amazon EC2 network.
Elastic IP Addresses

By default, all Amazon EC2 instances are assigned two IP addresses at launch: a private (RFC 1918) address and a public address that is mapped to the private IP address through Network Address Translation (NAT).

If you use dynamic DNS to map an existing DNS name to a new instance's public IP address, it might take up to 24 hours for the IP address to propagate through the Internet. As a result, new instances might not receive traffic while terminated instances continue to receive requests.

To solve this problem, Amazon EC2 provides elastic IP addresses. Elastic IP addresses are static IP addresses designed for dynamic cloud computing. Elastic IP addresses are associated with your account, not specific instances. Any elastic IP addresses that you associate with your account remain associated with your account until you explicitly release them. Unlike traditional static IP addresses, however, elastic IP addresses allow you to mask instance or availability zone failures by rapidly remapping your public IP addresses to any instance in your account.

Note
You can only associate one elastic IP address with one instance at a time.

In the following example, web servers are connected to the Internet through elastic IP addresses and to database servers through their private IP addresses.
The administrator decides to replace a web server with a larger instance type. To do this, the administrator starts a new instance using a larger instance type (1), disassociates an elastic IP address from a running instance (2), associates the elastic IP address with the new instance (3), and terminates the old instance (4).

The following code snippet demonstrates how to set up these tasks.

```
$ ec2-run-instances ami-6ba54002 -n 1 --availability-zone us-east-1a
RESERVATION r-a034c7c9 9214417782495 default
INSTANCE i-3ea74257 ami-6ba54002 pending 0 m1.large 2007-07-11T16:40:44+0000 us-east-1a

$ ec2-disassociate-address 67.202.55.255
ADDRESS 67.202.55.255

$ ec2-associate-address -i i-3ea74257 67.202.55.255
ADDRESS 67.202.55.255 i-43a4412a

$ ec2-terminate-instances i-4bc32334
INSTANCE i-4bc32334 running shutting-down
```

**Note**
To ensure our customers are efficiently using elastic IP addresses, we impose a
small hourly charge when these IP addresses are not mapped to an instance. When these IP addresses are mapped to an instance, they are free of charge.

When you associate an elastic IP address with an instance, its current public IP address is released to the Amazon EC2 public IP address pool. If you disassociate an elastic IP address from the instance, the instance is automatically assigned a new public IP address within five to ten minutes.
Network Security

Topics

- Concepts
- Examples

The Amazon EC2 service allows you to dynamically add and remove instances. However, this flexibility can complicate firewall configuration and maintenance which traditionally relies on IP addresses, subnet ranges or DNS host names as the basis for the firewall rules.

The Amazon EC2 firewall allows you to assign your instances to user-defined groups and define firewall rules for these groups. As instances are added or removed, the appropriate rules are enforced. Similarly, if you change a rule for a group, the changes are automatically applied to all members of the group.
Concepts
Security Groups

A security group is a named collection of access rules. These access rules specify which ingress (i.e., incoming) network traffic should be delivered to your instance. All other ingress traffic will be discarded.

You can modify rules for a group at any time. The new rules are automatically enforced for all running instances and instances launched in the future.

Note
You can create up to 100 security groups.
Group Membership

When you launch an AMI instance, you can assign it to as many groups as you like.

If no groups are specified, the instance is assigned to the default group. By default, this group allows all network traffic from other members of this group and discards traffic from other IP addresses and groups. If this does not meet your needs, you can modify the rule settings of the default group.
**Group Access Rights**

The access rules define source based access either for named security groups or for IP addresses (i.e., CIDR-based rules). For CIDR-based rules, you can also specify the protocol and port range (or ICMP type/code).
Examples

This section provides two examples of how to use the Amazon EC2 firewall.

📖 **Note**
These examples use the Command Line Tools Reference. You can also achieve these results using the SOAP API. For more information, see Using the SOAP API.
Default Group

This example shows Albert modifying the default group to meet his security needs.

Albert Modifies the Default Group

1. Albert launches a copy of his favorite *public AMI*.

```bash
$ ec2-run-instances ami-eca54085
  RESERVATION r-a034c7c9 924417782495 default
  INSTANCE i-cfd732a6 ami-eca54085 pending 0 m1.small 2007-07-11T16:40:44
```

2. After a little wait for image launch to complete. Albert, who is a cautious type, checks the access rules:

```bash
$ ec2-describe-group default
  GROUP 598916040194 default default group
  PERMISSION default ALLOWS all FROM USER 598916040194 GRPNAME default
```

Albert notices that it only accepts ingress network connections from other members of the default group.

3. Albert, being paranoid as well as cautious, port scans his instance:

```bash
$ nmap -P0 -p1-100 ec2-67-202-51-105.compute-1.amazonaws.com
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-08-07 15:42
All 100 scanned ports on ec2-67-202-51-105.compute-1.amazonaws.com (67.202.51.105) are:	filtered
Nmap finished: 1 IP address (1 host up) scanned in 31.008 seconds
```

4. Albert decides he should be able to SSH into his instance, but only from his own machine.

```bash
$ ec2-authorize default -P tcp -p 22 -s 192.168.1.130/32
  GROUP default
  PERMISSION default ALLOWS tcp 22 22 FROM CIDR 192.168.1.130/32
```

5. Albert repeats the port scan.

```bash
$ nmap -P0 -p1-100 ec2-67-202-51-105.compute-1.amazonaws.com
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-08-07 15:43
PORT STATE SERVICE
22/tcp open ssh
| Nmap finished: 1 IP address (1 host up) scanned in 32.705 seconds |
Albert is happy (or at least less paranoid).
Three-Tier Web Service

Mary wants to deploy her public, failure resilient, three-tier web service in Amazon EC2. Her grand plan is to have her web tier start off executing in seven instances of ami-fba54092, her application tier executing in twenty instances of ami-e3a5408a, and her multi-master database in two instances of ami-f1a54098. She's concerned about the security of her subscriber database, so she wants to restrict network access to her middle and back tier machines. When the traffic to her site increases over the holiday shopping period, she adds additional instances to her web and application tiers to handle the extra load.

Launch Process

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
</tr>
</thead>
</table>
| 1    | First, Mary creates a group for her Apache web server instances and allows HTTP access to the world.  

```
$ ec2-add-group apache -d "Mary's Apache group"
GROUP  apache  Mary's Apache group

$ ec2-describe-group apache
GROUP  598916040194  apache  Mary's Apache group

$ ec2-authorize apache -P tcp -p 80 -s 0.0.0.0/0
GROUP  apache
PERMISSION  apache  ALLOWS  tcp  80  80  FROM  CIDR  0.0.

$ ec2-describe-group apache
GROUP  598916040194  apache  Mary's Apache group
PERMISSION  598916040194  apache  ALLOWS  tcp  80  80  FROM |

```

|     | 2    | Mary launches seven instances of her web server AMI as members of the apache group.  

```
$ ec2run ami-fba54092 -n 7 -g apache
RESERVATION  r-0592776c  598916040194  default
INSTANCE  i-cfd732a6  ami-fba54092  pending  0  m1.small  2007-07-11T16:4
INSTANCE  i-cfd732a7  ami-fba54092  pending  0  m1.small  2007-07-11T16:4
INSTANCE  i-cfd732a8  ami-fba54092  pending  0  m1.small  2007-07-11T16:4
INSTANCE  i-cfd732a9  ami-fba54092  pending  0  m1.small  2007-07-11T16:4
INSTANCE  i-cfd732aa  ami-fba54092  pending  0  m1.small  2007-07-11T16:4
INSTANCE  i-cfd732ab  ami-fba54092  pending  0  m1.small  2007-07-11T16:4
INSTANCE  i-cfd732ac  ami-fba54092  pending  0  m1.small  2007-07-11T16:4

$ ec2din i-cfd732a6
```
3 Being as paranoid as Albert, Mary does a port scan to confirm the permissions she just configured.

```
$ nmap -P0 -p1-100 ec2-67-202-51-245.compute-1.amazonaws.com
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-08-07
(The 99 ports scanned but not shown are in state: filtered)
PORT      STATE     SERVICE
80/tcp    open       http
```

Nmap finished: 1 IP address (1 host up) scanned in 33.409 seconds

4 Mary verifies her web server can be reached.

```
$ telnet ec2-67-202-51-245.compute-1.amazonaws.com 80
Trying 67.202.51.245...
Escape character is '^]'.
```

Mary can reach her web server.

5 Mary creates a separate group for her application server.

```
$ ec2-add-group appserver -d "Mary's app server"
GROUP     appserver       Mary's app server
```

6 Mary starts twenty instances as members of appserver group.

```
$ ec2run ami-e3a5408a -n 20 -g appserver
```

7 Mary grants network access between her web server group and the application server group.

```
$ ec2-authorize appserver -o apache -u 495219933132
GROUP     appserver
PERMISSION appserver ALLOWS all FROM USER 495219933132
```

8 Mary verifies access to her app server is restricted by port scanning one of the application servers.

```
$ nmap -P0 -p1-100 ec2-67-202-51-162.compute-1.amazonaws.com
Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-08-07
All 100 scanned ports on ec2-67-202-51-162.compute-1.amazonaws.com
```

```
Nmap finished: 1 IP address (1 host up) scanned in 31.008 seconds

9 Mary confirms that her web servers have access to her application servers.
   A. She (temporarily) grants SSH access from her workstation to the web server group:

```
$ ec2-authorize apache -P tcp -p 22 -s 192.168.1.130/32
```

B. She logs in to one of her web servers and connects to an application server on TCP port 8080.

```
$ telnet ec2-67-202-51-162.compute-1.amazonaws.com 8080
Trying 67.202.51.162...
Connected to ec2-67-202-51-162.compute-1.amazonaws.com
Escape character is '^]'
```

C. Satisfied with the setup, she revokes SSH access to the web server group.

```
$ ec2-revoke apache -P tcp -p 22 -s 192.168.1.130/32
```

10 Mary repeats these steps to create the database server group and to grant access between the application server and database server.

Note

In addition to the distributed firewall, you can maintain your own firewall on any of your instances. This can be useful if you have specific requirements not met by the Amazon EC2 distributed firewall.
Amazon Elastic Block Store

Topics

- Overview
- Amazon EBS Concepts
- Amazon EBS Use Cases
- Amazon EBS API Overview
- Creating Amazon EBS Volumes and Snapshots

This section provides a high level overview of Amazon Elastic Block Store (Amazon EBS).
Overview

Amazon Elastic Block Store (Amazon EBS) is a new type of storage designed specifically for Amazon EC2 instances. Amazon EBS allows you to create volumes that can be mounted as devices by Amazon EC2 instances. Amazon EBS volumes behave like raw unformatted external block devices. They have user supplied device names and provide a block device interface. You can load a file system on top of Amazon EBS volumes, or use them just as you would use a block device.

You can create up to twenty Amazon EBS volumes of any size (from one GiB up to one TiB). Each Amazon EBS volume can be attached to any Amazon EC2 instance in the same availability zone or can be left unattached.

Amazon EBS provides the ability to create snapshots of your Amazon EBS volumes to Amazon S3. You can use these snapshots as the starting point for new Amazon EBS volumes and can protect your data for long term durability.
Amazon EBS Concepts

Amazon EBS volumes provide the following:

- Off-instance storage
- Persistence beyond the lifetime of instances
- High availability and reliability
- Ability to attach to and detach from a running instance
- Exposure as a device within an instance

Amazon EBS snapshots provide the following:

- Ability to capture the current state of a volume
- Data backup
- A method for instantiating new volumes that contain the exact contents of a snapshot
Amazon EBS Use Cases

This section describes common Amazon EBS use cases.
Data Survival of Instance Failure

Amazon EBS is designed to allow you to attach any instance to a storage volume. In the event you experience an instance failure, your Amazon EBS volume automatically detaches with your data intact. You can then reattach the volume to a new instance and quickly recover.

1. You are running an Amazon EC2 instance that is attached to an Amazon EBS volume, when your Amazon EC2 instance fails or is experiencing problems.
2. To recover, you detach the Amazon EBS volume from your instance (if it has not already automatically detached), launch a new Amazon EC2 instance, and attach the Amazon EBS volume to the new instance.
3. In the unlikely event the Amazon EBS volume fails, you can create a new Amazon EBS volume based on the most recent snapshot of your failed volume.
Volume Instantiation Using Snapshots

Amazon EBS snapshots allow you to quickly launch new volumes, using a previous snapshot as a starting point for those new volumes.

1. You are running a web service with a large data set.
2. When the data is ready, you can store a snapshot of your volume to Amazon S3 for long term durability.
3. When traffic and resource usage increases, you can launch a new volume from the snapshot, launch a new instance, and then attach the new volume to the new instance.
4. If traffic decreases, you can shut down one or more Amazon EC2 instances and delete their Amazon EBS volumes.
Data Persistence After Shutting Down Instances

Amazon EBS volumes exist separately from the actual instances and persist until you delete them. This allows you to store your data without leaving an Amazon EC2 instance running.

1. You run an instance periodically to perform a batch processing job on a large and growing data set.
2. At the end of your job, you shut down the Amazon EC2 instance, but leave your Amazon EBS volume running.
3. The next time you process the data set, you launch a new EC2 instance and reattach it to your existing Amazon EBS volume.

Using this model, you can process and store your data set indefinitely, only using the processing and storage resources that you require.
Large Datasets

Amazon EBS supports larger volumes than provided by Amazon EC2 instances. You can create up to one TiB Amazon EBS volumes.
Amazon EBS API Overview

To configure and use Amazon EBS, we provide eight new API functions. This section provides a brief overview of each function.

API List

- **CreateVolume**—Creates a new Amazon EBS volume using the specified size or creates a new volume based on a previously created snapshot.

- **DeleteVolume**—Deletes the specified volume. This function does not delete any snapshots that were created from this volume.

- **DescribeVolumes**—Describes all volumes, including size, source snapshot, availability zone, creation time, and status (available, in-use).

- **AttachVolume**—Attaches the specified volume to a specified instance, exposing the volume using the specified device name.

  A volume can only be attached to a single instance at any time. The volume and instance must be in the same availability zone.

- **DetachVolume**—Detaches the specified volume from the instance to which it is attached.

  This operation does not delete the volume. The volume can be attached to another instance and will have the same data as when it was detached.

- **CreateSnapshot**—Creates a snapshot of the volume you specify.
Once created, you can use the snapshot to create volumes that contain exactly the same data as the original volume.

- **DeleteSnapshot**—Deletes the specified snapshot.

  This function does not affect currently running Amazon EBS volumes, regardless of whether they were used to create the snapshot or were derived from the snapshot.

- **DescribeSnapshots**—Describes all snapshots, including their source volume, snapshot initiation time, progress (percentage complete), and status (pending, completed).
Creating Amazon EBS Volumes and Snapshots

Topics

- Creating an Amazon EBS Volume
- Attaching the Volume to an Instance
- Describing Volumes and Instances
- Using an Amazon EBS Volume within an Instance
- Creating an Amazon EBS Snapshot
- Describing Snapshots
- Detaching an Amazon EBS Volume from an Instance
- Deleting an Amazon EBS Snapshot
- Deleting an Amazon EBS Volume

This section provides examples of how to create and use Amazon EBS volumes.
Creating an Amazon EBS Volume

To use Amazon EBS, you first create a volume that can be attached to any Amazon EC2 instance within the same availability zone. This example creates an 800 GiB Amazon EBS volume.

To create an Amazon EBS volume

1. Enter the following command.

```
PROMPT> ec2-create-volume --size 800 --zone us-east-1a
```

Amazon EBS returns information about the volume similar to the following example.

```
VOLUME vol-4d826724 800 us-east-1a available 2008-02-14T00:00:00+0000
```

2. To check whether the volume is ready, use the following command.

```
PROMPT> ec2-describe-volumes vol-4d826724
```

Amazon EBS returns information about the volume similar to the following example.

```
VOLUME vol-4d826724 800 us-east-1a available 2008-07-29T08:49:25+0000
```
Attaching the Volume to an Instance

This example attaches volume vol-4d826724 to instance i-6058a509 and exposes it as device /dev/sdh.

To attach an Amazon EBS volume

- Enter the following command.

```
PROMPT> ec2-attach-volume vol-4d826724 -i i-6058a509 -d /dev/sdh
```

Amazon EBS returns information similar to the following example.

```
ATTACHMENT vol-4d826724 i-6058a509 /dev/sdh attaching 2008-02-14T00:15:00+0000
```
Describing Volumes and Instances

After creating Amazon EBS volumes and attaching them to instances, you can list them using the DescribeVolumes and the DescribeInstances operations.

DescribeVolumes returns the volume ID, capacity, status (in-use or available) and creation time of each volume. If the volume is attached, an attachment line shows the volume ID, the instance ID to which the volume is attached, the device name exposed to the instance, its status (attaching, attached, detaching, detached), and when it attached.

DescribeInstances lists volumes that are attached to running instances.

To describe volumes

- Enter the following command.

```
PROMPT> ec2-describe-volumes
```

Amazon EBS returns information about all volumes that you own.

```
VOLUME vol-4d926724 us-east-1a 800 in-use 2008-02-14T00:00:00+0000
ATTACHMENT vol-4d926724 i-6058a569 /dev/sdh attached 2008-02-14T00:17+0000
VOLUME vol-50057039 13 us-east-1a available 2008-02-09T00:00+0000
VOLUME vol-6682670f 1 us-east-1a in-use 2008-02-11T00:00+0000
ATTACHMENT vol-6682670f i-69a54000 /dev/sdh attached 2008-02-11T00:56+0000
```

To describe instances

- Enter the following command.

```
PROMPT> ec2-describe-instances
```

Amazon EBS returns information about all running instances and volumes attached to those instances.

```
RESERVATION r-e112fc88 416161254515 default
INSTANCE i-3b887c52 ami-3fd13456 ec2-67-202-27-216.compute-1.amazonaws.com dom running gsg-keypair 0 m1.small 2007-11-26T13:20:35+0000 vol-4d926724
```
<table>
<thead>
<tr>
<th>RESERVATION</th>
<th>r-e612fc8f</th>
<th>416161254515</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTANCE</td>
<td>i-21b63c22</td>
<td>ami-3fd13456</td>
<td>ec2-67-202-18-227.compute-1.amazonaws.com domU</td>
</tr>
<tr>
<td>running</td>
<td>gsg-keypair</td>
<td>0</td>
<td>m1.small</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>vol-6682670f, vol-50957039</td>
</tr>
</tbody>
</table>
Using an Amazon EBS Volume within an Instance

Inside the instance, the Amazon EBS volume is exposed as a normal block device and can be formatted as any file system and mounted. This example creates an ext3 file system on the Amazon EBS volume and mounts it as /mnt/data-store.

To use an Amazon EBS volume

1. Enter the following command.

```
PROMPT> yes | mkfs -t ext3 /dev/sdh
```

2. Enter the following command.

```
PROMPT> mkdir /mnt/data-store
```

3. Enter the following command.

```
PROMPT> mount /dev/sdh /mnt/data-store
```

Any data written to this file system is written to the Amazon EBS volume and is transparent to applications using the device.
Creating an Amazon EBS Snapshot

After writing data to an Amazon EBS volume, you can periodically create a snapshot of the volume to use as a baseline for new volumes or for data backup.

This example creates a snapshot of the vol-4d826724 Amazon EBS volume using the CreateSnapshot function.

To create a snapshot

- Enter the following command.

  ```
PROMPT> ec2-create-snapshot vol-4d826724
  ```

  Amazon EBS returns information similar to the following example.

  ```
SNAPSHOT snap-78a54011 vol-4d826724 pending 2008-02-15T09:38:58+0000
  ```

  The snapshot occurs asynchronously and the volume's status indicates "pending" until it completes.

  **Note**
  For information on creating an Amazon EBS volume from a snapshot, refer to the *Amazon Elastic Compute Cloud Developer Guide*. 
Describing Snapshots

This example describes snapshots using the `CreateSnapshot` function.

To describe snapshots

- Enter the following command.

```
PROMPT> ec2-describe-snapshots snap-78a54011
```

Amazon EBS returns information about all snapshots that you own.

```
SNAPSHOT snap-78a54011 vol-4d826724 pending 2008-02-15T09:03:58+0000 60%
```

When the snapshot is complete, its status will change to `completed` and the percentage will change to 100%.
Detaching an Amazon EBS Volume from an Instance

An Amazon EBS volume can be detached from an instance by either explicitly detaching the volume or terminating the instance. This example unmounts the volume and explicitly detaches it from the instance.

**Caution**
A volume must be unmounted inside the instance before being detached. Failure to do so will result in damage to the file system or the data it contains.

**To detach an Amazon EBS volume**

- Enter the following command.

  PROMPT> `ec2-detach-volume vol-4d826724`

  Amazon EBS returns information similar to the following example.

  ATTACHMENT  vol-4d826724  i-6058a509  /dev/sdh  detaching  2008-02-14T00:00:17+0000

**To detach an Amazon EBS volume by terminating the instance**

- Enter the following command.

  PROMPT> `ec2-terminate-instances i-6058a509`

  Amazon EBS returns information similar to the following example.

  INSTANCE  i-6058a509  running  shutting-down

To verify the volume is no longer attached to the instance, use the `DescribeVolumes`.
Deleting an Amazon EBS Snapshot

After a snapshot is no longer needed, it can be deleted. This example deletes a snapshot.

To delete a snapshot

- Enter the following command.

```
PROMPT> ec2-delete-snapshot snap-78a54011
```

Amazon EBS returns information similar to the following example.

```
SNAPSHOT snap-78a54011
```
Deleting an Amazon EBS Volume

After a volume is no longer needed, it can be deleted. Once deleted, its data is deleted and it cannot be attached to any instance. However, you can store a snapshot of the volume that you can use to recreate it later.

This example deletes a volume.

To delete a volume

- Enter the following command.

```
PROMPT> ec2-delete-volume vol-4282672b
```

Amazon EBS returns information similar to the following example.

```
VOLUME vol-4282672b
```
Using the APIs

Topics

- Using the SOAP API
- Using the Query API

This section provides an overview of the SOAP and Query APIs.
Using the SOAP API

Topics

- WSDL and Schema Definitions
- Programming Language Support in Amazon EC2
- Request Authentication
- The Response Structure
- Web Services References
WSDL and Schema Definitions

The Amazon EC2 web service can be accessed using the SOAP web services messaging protocol. This interface is described by a Web Services Description Language (WSDL) document which defines the operations and security model for the service. The WSDL references an XML Schema document which strictly defines the data types that might appear in SOAP requests and responses. For more information on WSDL and SOAP, see Web Services References.

All schemas have a version number (the latest is 2008-05-05). The version number appears in the URL of a schema file, and in a schema's target namespace. This makes upgrading easy by differentiating requests based on the version number.

Note

In addition to the latest version, the service will support the older versions for some time, allowing customers plenty of time to upgrade.

The Amazon EC2 services API WSDL is available from the web at 'http://ec2.amazonaws.com/doc/<version>/ec2.wsdl' where version is the version of the API. At the time this document was released, the current API version was 2008-05-05, which is available at http://ec2.amazonaws.com/doc/2008-05-05/AmazonEC2.wsdl
Programming Language Support in Amazon EC2

Since the SOAP requests and responses in the Amazon EC2 Web Service follow current standards, any programming language with the appropriate library support can be used. Languages known to have this support include C++, C#, Java, Perl, Python and Ruby.
Request Authentication

The Amazon EC2 web service complies with the current WS-Security standard, requiring SOAP request messages to be hashed and signed for integrity and non-repudiation. WS-Security defines profiles which are used to implement various levels of security. Amazon EC2 secure SOAP messages use the BinarySecurityToken profile, consisting of an X.509 certificate with an RSA public key.

The following is the content of an insecure RunInstances operation:

```xml
<RunInstances xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <instancesSet>
    <item>
      <imageId>ami-60a54009</imageId>
      <minCount>1</minCount>
      <maxCount>3</maxCount>
    </item>
  </instancesSet>
  <groupSet/>
</RunInstances>
```

To secure the request, we add the BinarySecurityToken element. The Java libraries we supply rely on the Apache Axis project for XML security, canonicalization, and SOAP support. The Sun Java Web Service Developer's Pack supplies libraries of equivalent functionality.

The secure version of the request begins with the following:

```xml
  <SOAP-ENV:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <wsse:BinarySecurityToken
        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
        EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
        ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
        wsu:Id="CertId-1064304">....many, many lines of base64 encoded X.509 certificate...</wsse:BinarySecurityToken>
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"></ds:CanonicalizationMethod>
          ...</ds:SignedInfo>
    </wsse:Security>
  </SOAP-ENV:Header>
  ...
</SOAP-ENV:Envelope>
```
If you are matching this against requests generated by Amazon EC2 supplied libraries, or those of another vendor, the following are the most important elements:

**Elements**

- **BinarySecurityToken**—Contains the X.509 certificate in base64 encoded PEM format

- **Signature**—Contains an XML digital signature created using the canonicalization, signature algorithm, and digest method
• **Timestamp**—Requests to Amazon EC2 are valid within 5 minutes of this value to help prevent replay attacks
The Response Structure

In response to a request, the Amazon EC2 web service returns an XML data structure that conforms to an XML schema defined as part of the Amazon EC2 WSDL. The structure of a XML response is specific to the associated request. In general, the response data types are named according to the operation performed and whether the data type is a container (can have children). Examples of containers include groupSet for security groups and instancesSet for instances. Item elements are children of containers and their contents vary according to the container's role.

The following is an example response:

```xml
<RunInstancesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <reservationId>r-47a5402e</reservationId>
  <ownerId>UYY3TLBUXIEON5NQVUUX60MPWBZI0NFM</ownerId>
  <groupSet>
    <item>
      <groupId>default</groupId>
    </item>
  </groupSet>
  <instancesSet>
    <item>
      <instanceId>i-2ba64342</instanceId>
      <imageId>ami-60a54009</imageId>
      <instanceState>
        <code>0</code>
        <name>pending</name>
      </instanceState>
      <dnsName></dnsName>
    </item>
    <item>
      <instanceId>i-2bc64242</instanceId>
      <imageId>ami-60a54009</imageId>
      <instanceState>
        <code>0</code>
        <name>pending</name>
      </instanceState>
      <dnsName>ec2-67-202-51-176.compute-1.amazonaws.com</dnsName>
    </item>
    <item>
      <instanceId>i-2be64332</instanceId>
      <imageId>ami-60a54009</imageId>
      <instanceState>
```
<code>0</code>
<name>pending</name>
</instanceState>
<dnsName>ec2-67-202-51-122.compute-1.amazonaws.com</dnsName>
<keyName>example-key-name</keyName>
<instanceType>m1.small</instanceType>
<launchTime>2007-08-07T11:54:42.000Z</launchTime>
</item>
</instancesSet>
</RunInstancesResponse>
Web Services References

- Web Service Description Language (WSDL)
- WS-Security BinarySecurityToken Profile
Using the Query API

Topics

•

Query Parameters
• Query API Authentication
• Example Request

HTTP Query-based requests are HTTP requests that use the HTTP verb GET or POST and a Query parameter named Action or Operation. Action is used throughout this documentation, although Operation is supported for backward compatibility with other AWS Query APIs.
Query Parameters

Each Query request must include some common parameters to handle authentication and selection of an action. For more information, see Common Query Parameters.

Some operations take lists of parameters. These lists are specified using the $param.n$ notation. Values of $n$ are integers starting from 1.
Query API Authentication

Every request to Amazon EC2 must contain a request signature. A request signature is calculated by constructing a string and then calculating an RFC 2104-compliant HMAC-SHA1 hash, using the Secret AWS Access Key as the key. For more information, go to http://www.faqs.org/rfcs/rfc2104.html.

The following are the basic steps used to authenticate requests to AWS. This assumes the developer is registered with AWS and has an Access Key ID and Secret Access Key.

Query Authentication Process

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The sender constructs a request to AWS.</td>
</tr>
<tr>
<td>2</td>
<td>The sender calculates the request signature, a Keyed-Hashing for Message Authentication Code (HMAC) with a SHA-1 hash function, as defined in the next section of this topic.</td>
</tr>
<tr>
<td>3</td>
<td>The sender of the request sends the request data, the signature, and Access Key ID (the key-identifier of the Secret Access Key used) to AWS.</td>
</tr>
<tr>
<td>4</td>
<td>AWS uses the Access Key ID to look up the Secret Access Key.</td>
</tr>
<tr>
<td>5</td>
<td>AWS generates a signature from the request data and the Secret Access Key using the same algorithm used to calculate the signature in the request.</td>
</tr>
<tr>
<td>6</td>
<td>If the signatures match, the request is considered to be authentic. If the comparison fails, the request is discarded, and AWS returns an error response.</td>
</tr>
</tbody>
</table>

Note

If a request contains a Timestamp parameter, the signature calculated for the request expires 15 minutes its value. If a request contains an Expires parameter, the signature expires at the time specified by the Expires parameter.

Calculating the request signature

1. Based on the API (Query/SOAP/REST) you are using, construct a string.
   a. Sort the query parameters (not URL-encoded) without using case-sensitively.
   b. Concatenate the parameter names and values without the initial ? or the separating & and = characters.
2. Compute an RFC 2104 compliant HMAC using the Secret AWS Access
Key as the "key".
3. Convert the value to base64.
4. Include the value as the value of the signature parameter in the request.

For example, the following is a Query string (linebreaks added for clarity).

```plaintext
?Action=DescribeImages
&AWSAccessKeyId=10QMXFEV71ZS32XQFTR2
&SignatureVersion=1
&Timestamp=2006-12-08T07%3A48%3A03Z
&Version=2007-01-03
```

For the preceding Query string, you would calculate the HMAC signature over the following string.

```plaintext
ActionDescribeImagesAWSAccessKeyId10QMXFEV71ZS32XQFTR2SignatureVersion1
```

Using the preceding string and the secret key
DMADSSfPfdJdjbK+RRuhs/aDrjsiZadgAUM8gRU2 the base64 encoded signature is as follows:

```plaintext
GjH3941IBe6qsgQu+k7FpCJjpcn=
```

The following is a Java code sample to compute the signature from the string and the private key.

```java
import java.security.SignatureException;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;

public class HmacExample
{

    private static final String HMAC_SHA1_ALGORITHM = "HmacSHA1";

    /**
     * Computes RFC 2104-compliant HMAC signature.
     *
     * @param data
     * @param The data to be signed.
     */
```
public static String calculateRFC2104HMAC(String data, String key) throws java.security.SignatureException {
    String result;
    try {
        // get an hmac_sha1 key from the raw key bytes
        SecretKeySpec signingKey = new SecretKeySpec(key.getBytes(), HMAC_SHA1_ALGORITHM);

        // get an hmac_sha1 Mac instance and initialize with the signing key
        Mac mac = Mac.getInstance(HMAC_SHA1_ALGORITHM);
        mac.init(signingKey);

        // compute the hmac on input data bytes
        byte[] rawHmac = mac.doFinal(data.getBytes());

        // base64-encode the hmac
        result = Base64.encodeBytes(rawHmac);
    } catch (Exception e) {
        throw new SignatureException("Failed to generate HMAC : " + e.getMessage());
    }
    return result;
}

Note
You must import a base 64 encoder to perform the last step in the preceding example.
Example Request

The following is a complete example request, including all required parameters.

```
?AWSAccessKeyId=10QMXFEV71ZS32XQFTR2&Action=DescribeImages&SignatureVersion=1&Timestamp=2006-12-08T07%3A48%3A03Z&Version=2007-01-03&Signature=69DSJs1z%2B0wWJmdB77%2BLm0N0Trs%3D
```
API Reference

Topics

- API Conventions
- API Versioning
- API Error Codes
- Data Types
- Amazon EC2 SOAP API
- Amazon EC2 Query API

Amazon EC2 provides two APIs: Using the SOAP API and Using the Query API, which allow you to launch and control instances from your own applications.

This section discusses the operations available in the Amazon EC2 APIs, their semantics, and their required parameters. Examples of requests and responses are also provided.

Note
The same XML body is returned in both the Query API and SOAP API.

Before using the API, we recommend that you familiarize yourself with their API Conventions.
API Conventions
Overview

This section describes Amazon EC2 API conventions.
Actions

Actions encapsulate the possible interactions with Amazon EC2. These can be viewed as remote procedure calls and consist of a request and response message pair. Requests must be signed, allowing Amazon EC2 to Request Authentication. For clarity, the sample requests and responses illustrating each of the operations described in this reference are not signed.
Data Types and the Amazon EC2 WSDL

The current version of the Amazon EC2 WSDL is available at: [http://ec2.amazonaws.com/doc/2008-05-05/AmazonEC2.wsdl](http://ec2.amazonaws.com/doc/2008-05-05/AmazonEC2.wsdl). Some libraries can generate code directly from the WSDL. Other libraries require a little more work on your part.

Values provided as parameters to the various operations must be of the indicated type. Standard XSD types (like `string`, `boolean`, `int`) are prefixed with `xsd:`. Complex types defined by the Amazon EC2 WSDL are prefixed with `ec2:`.

Parameters that consist of lists of information are defined within our WSDL to require `<info>` tags around each member. Throughout the API, type references for parameters that accept such a list of values are specified using the notation `type[]` The type referred to in these instances is the type `nested within the <info>` tag (for Amazon EC2 types this is defined in the WSDL).

For example, the `<imagesSet>` element in the following XML snippet is of type `xsd:string[]`.

```xml
<imagesSet>
  <item>
    <imageId>ami-61a54008</imageId>
  </item>
  <item>
    <imageId>ami-61b54608</imageId>
  </item>
</imagesSet>
```

The `<instancesSet>` element in the following XML snippet is of type `xsd:string[]`.

```xml
<instancesSet>
  <item>
    <imageId>ami-60a54009</imageId>
    <minCount>10</minCount>
    <maxCount>30</maxCount>
  </item>
  <item>
    <imageId>ami-60b54209</imageId>
  </item>
</instancesSet>
```
<minCount>5</minCount>
<maxCount>20</maxCount>
</item>
</instancesSet>
API Versioning

Because features and changes can introduce incompatible API changes, all Amazon EC2 API updates are versioned. By including a version in the request, clients receive responses they can process.

Each API revision is assigned a version in date form (the current API version is 2008-05-05). This version is included in the request as part of the document namespace when using our SOAP API and as a Version parameter when using our Query API. The response that Amazon EC2 returns honors the version included in the request.

SOAP clients that retrieve the Amazon EC2 WSDL at runtime and generate their requests dynamically using that WSDL should reference the WSDL for the version of the API that the client was developed against. This ensures that the client software continues to work even if backwards incompatible API changes are introduced. The WSDL for each supported API version is available from the following URI:

http://ec2.amazonaws.com/doc/<api-version>/AmazonEC2.wsdl

The WSDL for latest version of our API is available from the following URI:

http://ec2.amazonaws.com/doc/2008-05-05/AmazonEC2.wsdl

Note

The WSDL should be treated as a moving target as it will always map to the latest release of the Amazon EC2 SOAP API. If your software depends on retrieving the WSDL at runtime, we strongly recommend you reference the specific version of the WSDL you are developing against.
API Error Codes
Overview

There are two types of error codes: client and server.

Client error codes suggest that the error was caused by something the client did, such as an authentication failure or an invalid AMI identifier. In the SOAP API, these error codes are prefixed with Client. For example: Client.AuthFailure. In the Query API, these errors are accompanied by a 400-series HTTP response code.

Server error codes suggest a server-side issue caused the error and should be reported. In the SOAP API, these error codes are prefixed with Server. For example: Server.Unavailable. In the Query API, these errors are accompanied by a 500-series HTTP response code.
# Summary of Client Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddressLimitExceeded</td>
<td>User has the maximum number of allowed IP addresses.</td>
<td>Each user has an IP address limit. For new users, this limit is 5. If you need more than 5 Elastic IP addresses, please complete the Amazon EC2 Elastic IP Address Request Form.</td>
</tr>
<tr>
<td>AttachmentLimitExceeded</td>
<td>The limit on the number of Amazon EBS volumes attached to one instance has been exceeded.</td>
<td>CHOICE FOR AN ERROR MESSAGE EXAMPLE: AttachmentLimitExceeded The limit on the number of Amazon EBS volumes attached to one instance has been exceeded. If you need more than 5 EBS volumes, please complete the Amazon EBS Volume Request Form.</td>
</tr>
<tr>
<td>AuthFailure</td>
<td>User not authorized.</td>
<td>You might be trying to run an AMI for which you do not have permission.</td>
</tr>
<tr>
<td>IncorrectState</td>
<td>Volume is in incorrect state To attach to an instance, it must be in the 'available' state.</td>
<td>IncorrectState Volume is in incorrect state To attach to an instance, it must be in the 'available' state.</td>
</tr>
<tr>
<td>InstanceLimitExceeded</td>
<td>User has max allowed concurrent running instances. Each user has a concurrent running instance limit. For new users, this limit is 20. If you need more than 20 instances, please complete the Amazon EC2 Instance Request Form and your request will be considered.</td>
<td>CHOICE FOR AN ERROR MESSAGE EXAMPLE: InstanceLimitExceeded User has max allowed concurrent running instances. For new users, this limit is 20. If you need more than 20 instances, please complete the Amazon EC2 Instance Request Form and your request will be considered.</td>
</tr>
<tr>
<td>InvalidAMIAttributeItemValue</td>
<td>The value of an item added to, or removed from, an image attribute is invalid. If you are specifying a userId, check that it is in the form of an AWS account ID.</td>
<td>InvalidAMIAttributeItemValue The value of an item added to, or removed from, an image attribute is invalid. If you are specifying a userId, check that it is in the form of an AWS account ID.</td>
</tr>
<tr>
<td>InvalidAMIID.Malformed</td>
<td>Specified AMI ID is not valid.</td>
<td>InvalidAMIID.Malformed Specified AMI ID is not valid.</td>
</tr>
<tr>
<td>InvalidAMIID.NotFound</td>
<td>Specified AMI ID does not exist.</td>
<td>InvalidAMIID.NotFound Specified AMI ID does not exist.</td>
</tr>
<tr>
<td>InvalidAMIID.Unavailable</td>
<td>Specified AMI ID has been deregistered and is no longer available.</td>
<td>InvalidAMIID.Unavailable Specified AMI ID has been deregistered and is no longer available.</td>
</tr>
<tr>
<td>InvalidAttachment.NotFound</td>
<td>The instance cannot detach from a volume to which it is not attached.</td>
<td>InvalidAttachment.NotFound The instance cannot detach from a volume to which it is not attached.</td>
</tr>
<tr>
<td>InvalidDevice.InUse</td>
<td>The device to which you are trying to attach (i.e. /dev/sdh) is already in use on the instance.</td>
<td>InvalidDevice.InUse The device to which you are trying to attach (i.e. /dev/sdh) is already in use on the instance.</td>
</tr>
<tr>
<td>InvalidInstanceId.Malformed</td>
<td>Specified instance ID is not valid.</td>
<td>InvalidInstanceId.Malformed Specified instance ID is not valid.</td>
</tr>
<tr>
<td>InvalidInstanceId.NotFound</td>
<td>Specified instance ID does not exist.</td>
<td>InvalidInstanceId.NotFound Specified instance ID does not exist.</td>
</tr>
<tr>
<td>InvalidKeyPair.Duplicate</td>
<td>Attempt to create a duplicate key pair.</td>
<td>InvalidKeyPair.Duplicate Attempt to create a duplicate key pair.</td>
</tr>
<tr>
<td>InvalidGroup.Duplicate</td>
<td>Attempt to create a duplicate group.</td>
<td>InvalidGroup.Duplicate Attempt to create a duplicate group.</td>
</tr>
<tr>
<td>InvalidGroup.InUse</td>
<td>Specified group cannot be deleted because it is in use.</td>
<td>InvalidGroup.InUse Specified group cannot be deleted because it is in use.</td>
</tr>
<tr>
<td>InvalidGroup.Reserved</td>
<td>Specified group name is a reserved name.</td>
<td>InvalidGroup.Reserved Specified group name is a reserved name.</td>
</tr>
<tr>
<td>InvalidManifest</td>
<td>Specified AMI has an unparsable Manifest.</td>
<td>InvalidManifest Specified AMI has an unparsable Manifest.</td>
</tr>
<tr>
<td>InvalidParameterValue</td>
<td>The value supplied for a parameter was invalid.</td>
<td>InvalidParameterValue The value supplied for a parameter was invalid. Requests that could cause this error include (for example) supplying an invalid image attribute to the DescribeImageAttribute request or an invalid version of the Amazon EC2 Elastic IP Address Request Form.</td>
</tr>
</tbody>
</table>
encoding value for the userData in a RunInstances request. 
InvalidPermission.Duplicate Attempt to authorize a permission that has already been authorized. InvalidPermission.Malformed Specified permission is invalid. InvalidReservationID.Malformed Specified reservation ID is invalid. InvalidReservationID.NotFound Specified reservation ID does not exist. InvalidParameterCombination RunInstances was called with minCount and maxCount set to 0 or minCount > maxCount. InvalidSnapshotID.Malformed The snapshot ID that was passed as an argument was malformed. InvalidSnapshotID.NotFound The specified snapshot does not exist. InvalidUserID.Malformed The user ID is neither in the form of an AWS account ID or one of the special values accepted by the owner or executableBy flags in the DescribeImages call. InvalidVolumeID.Malformed The volume ID that was passed as an argument was malformed. InvalidVolumeID.NotFound The volume specified does not exist. InvalidVolumeID.Duplicate The volume already exists in the system. InvalidVolumeID.ZoneMismatch The specified volume ID and instance ID are in different availability zones. InvalidZone.NotFound The specified zone does not exist. NonEBSInstance The instance specified does not support EBS. Please restart the instance and try again. This will ensure that the code is run on an instance with updated code. PendingSnapshotLimitExceeded The limit on the number of Amazon EBS snapshots in the pending state has been exceeded. SnapshotLimitExceeded The limit on the number of Amazon EBS snapshots has been exceeded. UnknownParameter An unknown or unrecognized parameter was supplied. Requests that could cause this error include supplying a misspelled parameter or a parameter that is not supported for the specified API version. VolumeLimitExceeded The limit on the number of Amazon EBS volumes has been exceeded.
# Summary of Server Error Codes

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>InternalError</td>
<td>Internal Error.</td>
<td>This error should not occur. If it does, please try to reproduce it and let us know by posting a message on the <a href="https://aws.amazon.com/forums">AWS forums</a>.</td>
</tr>
<tr>
<td>InsufficientAddressCapacity</td>
<td>Not enough available addresses to satisfy your minimum request.</td>
<td>Reduce the number of addresses you are requesting or wait for additional capacity to become available.</td>
</tr>
<tr>
<td>InsufficientInstanceCapacity</td>
<td>Not enough available instances to satisfy your minimum request.</td>
<td>Reduce the number of instances in your request or wait for additional capacity to become available.</td>
</tr>
<tr>
<td>Unavailable</td>
<td>The server is overloaded and cannot handle the request.</td>
<td></td>
</tr>
</tbody>
</table>
Data Types
Common Data Types

The Amazon EC2 API contains several data types that various operations use. This section describes each data type in detail.

Since both the Query and SOAP APIs return the same XML body, the data types described in the WSDL are used in both.

- AvailabilityZoneItemType
- BlockDeviceMappingItemType
- DescribeImagesResponseItemType
- DescribeKeyPairsResponseItemType
- EmptyElementType
- GroupSetType
- InstanceStateType
- IpPermissionType
- LaunchPermissionItemType
- LaunchPermissionOperationType
- PlacementRequestType
- PlacementResponseType
- ProductCodeItemType
- ProductInstanceResponseItemType
- ReservationInfoType
- RunningInstancesItemType
- SecurityGroupItemType
- TerminateInstancesResponseInfoType
- UserDataType
- UserIdGroupPairType
AvailabilityZoneItemType

The AvailabilityZoneItemType data type.
Relevant Operations

- [DescribeAvailabilityZones](#)
The following table describes the elements contained in AvailabilityZoneItemType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>zoneName</td>
<td>Name of the availability zone. Type: xsd:string</td>
</tr>
<tr>
<td>zoneState</td>
<td>State of the availability zone. Type: xsd:string</td>
</tr>
</tbody>
</table>
BlockDeviceMappingItemType

The BlockDeviceMappingItemType data type.
Relevant Operations

- DescribeImageAttribute
- RunInstances
The following table describes the elements contained in `BlockDeviceMappingItemType`.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtualName</td>
<td>Virtual name assigned to the device. Type: xsd:string</td>
</tr>
<tr>
<td>deviceName</td>
<td>Name of the device within Amazon EC2. Type: xsd:string</td>
</tr>
</tbody>
</table>
DescribeImagesResponseItemType

The DescribeImagesResponseItemType data type.
Relevant Operations

- DescribeImages
The following table describes the elements contained in DescribeImagesResponseItemType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>imageId</code></td>
<td>Unique ID of the AMI described. Type: xsd:string</td>
</tr>
<tr>
<td><code>imageState</code></td>
<td>Current state of the AMI. If the operation returns available, the image is successfully registered and available for launching. If the operation returns deregistered, the image is deregistered and no longer available for launching. For more information, see <a href="#">DeregisterImage</a>. Type: xsd:string</td>
</tr>
<tr>
<td><code>imageOwnerId</code></td>
<td>AWS Access Key ID of the image owner. Type: xsd:string</td>
</tr>
<tr>
<td><code>isPublic</code></td>
<td>Returns true if this image has public launch permissions. Returns false if it only has implicit and explicit launch permissions. Type: xsd:boolean</td>
</tr>
<tr>
<td><code>productCodes</code></td>
<td>Product codes associated with this image. Type: [ProductCodeItemType][1]</td>
</tr>
<tr>
<td><code>architecture</code></td>
<td>The architecture of the image (i386 or x86_64). Type: xsd:string</td>
</tr>
<tr>
<td><code>imageType</code></td>
<td>The type of image (machine, kernel, or ramdisk). Type: xsd:string</td>
</tr>
<tr>
<td><code>kernelId</code></td>
<td>The kernel associated with the image, if any. Only applicable for machine images. Type: xsd:string</td>
</tr>
<tr>
<td><code>ramdiskId</code></td>
<td>The ramdisk associated with the image, if any. Only applicable for machine images. Type: xsd:string</td>
</tr>
</tbody>
</table>
DescribeKeyPairsResponseItemType

The DescribeKeyPairsResponseItemType data type.
Relevant Operations

- DeleteKeyPair
- DescribeKeyPairs
# Contents

The following table describes the elements contained in `DescribeKeyPairsResponseItemType`.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyName</td>
<td>The user supplied name for this key pair. Type: <code>xsd:string</code></td>
</tr>
<tr>
<td>keyFingerprint</td>
<td>A fingerprint for the private key of this key pair. This is computed as the SHA-1 digest of the DER encoded form of the private key. Type: <code>xsd:string</code></td>
</tr>
</tbody>
</table>
EmptyElementType

The EmptyElementType data type.
Relevant Operations

- ResetImageAttribute
- DescribeImageAttribute
Contents

The empty element has no contents.
GroupSetType

The GroupSetType data type.
Relevant Operations

- RunInstances
Contents

The following table describes the elements contained in GroupSetType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupId</td>
<td>Name of a security group.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
</tbody>
</table>
InstanceStateType

The InstanceStateTypedata type.
Relevant Operations

- RunInstances
- DescribeInstances
- TerminateInstances
The following table describes the elements contained in InstanceStateType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| code | A 16-bit unsigned integer. The high byte is an opaque internal value and should be ignored. The low byte is set based on the state represented:  
  - 0: pending  
  - 16: running  
  - 32: shutting-down  
  - 48: terminated  
  Type: xsd:int |
| state | The current state of the instance.  
  - pending: the instance is in the process of being launched  
  - running: the instance launched (although the boot process might not be completed)  
  - shutting-down: the instance started shutting down  
  - terminated: the instance terminated  
  Type: xsd:string |
IpPermissionType

The IpPermissionType data type.
Relevant Operations

- AuthorizeSecurityGroupIngress
- DescribeSecurityGroups
- RevokeSecurityGroupIngress
Contents

The following table describes the elements contained in IpPermissionType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipProtocol</td>
<td>IP protocol. Type: xsd:string</td>
</tr>
<tr>
<td>fromPort</td>
<td>Start of port range for the TCP and UDP protocols, or an ICMP type number. An ICMP type number of -1 indicates a wildcard (i.e., any ICMP type number). Type: xsd:int</td>
</tr>
<tr>
<td>toPort</td>
<td>End of port range for the TCP and UDP protocols, or an ICMP code. An ICMP code of -1 indicates a wildcard (i.e., any ICMP code). Type: xsd:int</td>
</tr>
<tr>
<td>groups</td>
<td>List of security group and user ID pairs. Type: UserIdGroupPairType[]</td>
</tr>
<tr>
<td>ipRanges</td>
<td>List of CIDR IP range specifications. Type: xsd:string</td>
</tr>
</tbody>
</table>
LaunchPermissionItemType

The LaunchPermissionItemType data type.
Relevant Operations

- ModifyImageAttribute
- DescribeImageAttribute
Contents

The following table describes the elements contained in LaunchPermissionItemType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>A launch permission for a group. Currently only all is supported, which gives public launch permissions. Type: xsd:string</td>
<td>Choice between group and userId</td>
</tr>
<tr>
<td>userId</td>
<td>A launch permission for a user. userId is an AWS account ID. Type: xsd:string</td>
<td>Choice between group and userId</td>
</tr>
</tbody>
</table>
LaunchPermissionOperationType

The LaunchPermissionOperationType data type.
Relevant Operations

- ModifyImageAttribute
## Contents

The following table describes the elements contained in LaunchPermissionOperationType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds launch permissions. Type: <code>LaunchPermissionItemType[]</code></td>
<td>Choice between add and remove</td>
</tr>
<tr>
<td>remove</td>
<td>Removes launch permissions. Type: <code>LaunchPermissionItemType[]</code></td>
<td>Choice between add and remove</td>
</tr>
</tbody>
</table>
PlacementRequestType

The PlacementRequestType data type.
Relevant Operations

- RunInstances
Contents

The following table describes the elements contained in PlacementRequestType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>availabilityZone</td>
<td>The availability zone in which to launch the instance(s).</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
</tbody>
</table>
PlacementResponseType

The PlacementResponseType data type.
Relevant Operations

- DescribeInstances
## Contents

The following table describes the elements contained in PlacementResponseType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>availabilityZone</td>
<td>The availability zone in which to launch the instance(s). Type: xsd:string</td>
</tr>
</tbody>
</table>
ProductCodeItemType

The ProductCodeItemType data type.
Relevant Operations

- ModifyImageAttribute
- DescribeImageAttribute
The following table describes the elements contained in ProductCodeItemType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>productCode</td>
<td>A product code. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
ProductInstanceResponseItemType

The ProductInstanceResponseItemType data type.
Relevant Operations

- ConfirmProductInstance
## Contents

The following table describes the elements contained in `ProductInstanceResponseItemType`.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>productCode</code></td>
<td>The product code attached to the instance that matches one of the product codes in the <code>ConfirmProductInstance</code> request. Type: xsd:string</td>
</tr>
<tr>
<td><code>instanceId</code></td>
<td>Unique ID of the instance. Type: xsd:string</td>
</tr>
<tr>
<td><code>ownerId</code></td>
<td>The account ID of the owner of the instance. Type: xsd:string</td>
</tr>
</tbody>
</table>
ReservationInfoType

The ReservationInfoType data type.
Relevant Operations

- RunInstances
- DescribeInstances
The following table describes the elements contained in ReservationInfoType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reservationId</td>
<td>Unique ID of the reservation described. Type: xsd:string</td>
</tr>
<tr>
<td>ownerId</td>
<td>AWS Access Key ID of the user who owns the reservation. Type: xsd:string</td>
</tr>
<tr>
<td>groupSet</td>
<td>Set of security groups these instances were launched in. Type: GroupSetType[]</td>
</tr>
<tr>
<td>instancesSet</td>
<td>Information about instances started. Type: RunningInstancesItemType[]</td>
</tr>
</tbody>
</table>
RunningInstancesItemType

The RunningInstancesItemType data type.
Relevant Operations

- RunInstances
- DescribeInstances
Contents

The following table describes the elements contained in RunningInstancesItemType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>amiLaunchIndex</td>
<td>Optional. The AMI launch index, which can be used to find this instance within the launch group. For more information, see Instance Metadata.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>dnsName</td>
<td>The public DNS name assigned to the instance. This DNS name is contactable from outside the Amazon EC2 network. This element remains empty until the instance enters a running state. For more information, see Instance Addressing and Network Security.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>imageId</td>
<td>Image ID of the AMI used to launch the instance.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>instanceId</td>
<td>Unique ID of the instance launched.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>instanceState</td>
<td>The current state of the instance.</td>
</tr>
<tr>
<td></td>
<td>- pending: the instance is in the process of launching</td>
</tr>
<tr>
<td></td>
<td>- running: the instance launched (although it the boot process might not be complete)</td>
</tr>
<tr>
<td></td>
<td>- shutting-down: the instance is shutting down</td>
</tr>
<tr>
<td></td>
<td>- terminated: the instance terminated</td>
</tr>
<tr>
<td></td>
<td>Type: InstanceStateType</td>
</tr>
<tr>
<td>instanceType</td>
<td>The instance type. For more information on instance types, see Instance Types.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>keyName</td>
<td>Optional. If this instance was launched with an associated key pair, this displays the key pair name.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>kernelId</td>
<td>Optional. Kernel associated with this instance.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>launchTime</td>
<td>The time the instance launched.</td>
</tr>
<tr>
<td></td>
<td>Type: xs:dateTime</td>
</tr>
<tr>
<td>placement</td>
<td>The location where the instance launched.</td>
</tr>
<tr>
<td></td>
<td>Type: PlacementResponseType</td>
</tr>
<tr>
<td>privateDnsName</td>
<td>The private DNS name assigned to the instance. This DNS name can only be used inside the Amazon EC2 network. This element remains empty until the instance enters a running state. For more information, see Instance Addressing and Network Security.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>productCodes</td>
<td>Optional. Product codes attached to this instance.</td>
</tr>
<tr>
<td>ramdiskId</td>
<td>Optional. RAM disk associated with this instance.</td>
</tr>
<tr>
<td>reason</td>
<td>Optional. Reason for the most recent state transition. This might be an empty string.</td>
</tr>
</tbody>
</table>
SecurityGroupItemType

The SecurityGroupItemType data type.
Relevant Operations

- DescribeSecurityGroups
Contents

The following table describes the elements contained in SecurityGroupItemType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ownerId</td>
<td>AWS Access Key ID of the owner of the security group. Type: xsd:string</td>
</tr>
<tr>
<td>groupName</td>
<td>Name of the security group. Type: xsd:string</td>
</tr>
<tr>
<td>groupDescription</td>
<td>Description of the security group. Type: xsd:string</td>
</tr>
<tr>
<td>ipPermissions</td>
<td>Set of IP permissions associated with the security group. Type: IpPermissionType[]</td>
</tr>
</tbody>
</table>
TerminateInstancesResponseInfoType

The TerminateInstancesResponseInfoType data type.
Relevant Operations

- TerminateInstances
The following table describes the elements contained in TerminateInstancesResponseInfoType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instanceId</td>
<td>Instance ID returned from previous call to RunInstances Type: xsd:string</td>
</tr>
</tbody>
</table>
UserDataType

The UserDataType data type.
Relevant Operations

- RunInstances
Contents

The following table describes the elements contained in UserDataType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data</td>
<td>The user data.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
</tbody>
</table>

Notes

- The version and encoding attributes are required.

- The user data is base64-encoded as described in [RFC3548](https://tools.ietf.org/html/rfc3548) with the following additional restrictions:

  - Implementations MUST NOT add line feeds to encoded data.
  - Implementations MUST pad the end of the encoded data with '=' if required.
  - Implementations MUST ignore characters in the encoded stream that are not in the encoding alphabet. This differs from RFC3548, but provides more leeway for clients.
  - Implementation MUST use the encoding alphabet in table 1 of [RFC3548](https://tools.ietf.org/html/rfc3548) (i.e. A-Za-z0-9+/).
  - Implementation MUST follow the user data size limit before base64 encoding.
UserIdGroupPairType

The UserIdGroupPairType data type.
Relevant Operations

- AuthorizeSecurityGroupIngress
- DescribeSecurityGroups
- RevokeSecurityGroupIngress
## Contents

The following table describes the elements contained in UserIdGroupPairType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>userId</td>
<td>AWS Access Key ID of a user. Type: xsd:string</td>
</tr>
<tr>
<td>groupName</td>
<td>Name of a security group. Type: xsd:string</td>
</tr>
</tbody>
</table>
Amazon EBS Data Types

- AttachVolumeResponseType
- AttachVolumeType
- CreateSnapshotResponseType
- CreateSnapshotType
- CreateVolumeResponseType
- CreateVolumeType
- DeleteSnapshotResponseType
- DeleteSnapshotType
- DeleteVolumeResponseType
- DeleteVolumeType
- DescribeSnapshotsResponseType
- DescribeSnapshotsType
- DescribeVolumesResponseType
- DescribeVolumesType
- DetachVolumeResponseType
- DetachVolumeType
AttachVolumeResponseType

The AttachVolumeResponseType data type.
Relevant Operations

- AttachVolume
The following table describes the elements contained in AttachVolumeResponseType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>device</td>
<td>The device as it is exposed to the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Attachment state (e.g., attaching, attached, detached, busy)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>attachTime</td>
<td>Time stamp when the attachment was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
</tbody>
</table>
AttachVolumeType

The AttachVolumeType data type.
Relevant Operations

- AttachVolume
## Contents

The following table describes the elements contained in AttachVolumeType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| volumeId | The ID of the Amazon EBS volume  
Type: xsd:string  
Default: none  
Valid Values: ID of a volume that you own  
Constraints: The volume and instance must be within the same availability zone |
| instanceId | The ID of the instance that attaches to the volume  
Type: xsd:string  
Default: none  
Valid Values: ID of an instance that you own  
Constraints: The volume and instance must be within the same availability zone |
| device | Specifies how the device is exposed inside the instance (e.g., Linux: /dev/sdh). For information on standard storage locations, see [Storage Locations](#).  
Type: xsd:string  
Default: none  
Valid Values: Valid device ID  
Constraints: The specified device ID cannot be in use by another device or an instance store |
CreateSnapshotResponseType

The CreateSnapshotResponseType data type.
Relevant Operations

- CreateSnapshot
## Contents

The following table describes the elements contained in CreateSnapshotResponseType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshotId</td>
<td>The ID of the snapshot</td>
</tr>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td>status</td>
<td>Snapshot state (e.g., pending, completed)</td>
</tr>
<tr>
<td>startTime</td>
<td>Time stamp when the snapshot was initiated</td>
</tr>
<tr>
<td>progress</td>
<td>The progress of the snapshot, in percentage</td>
</tr>
</tbody>
</table>
CreateSnapshotType

The CreateSnapshotType data type.
Relevant Operations

- CreateSnapshot
Contents

The following table describes the elements contained in CreateSnapshotType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the Amazon EBS volume to snapshot</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a volume that you own</td>
</tr>
<tr>
<td></td>
<td>Constraints: ID of a volume that you own</td>
</tr>
</tbody>
</table>
CreateVolumeResponseType

The CreateVolumeResponseType data type.
Relevant Operations

- CreateVolume
The following table describes the elements contained in CreateVolumeResponseType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>size</td>
<td>The size of the volume, in GiB</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., creating, available, in-use, deleting)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>createTime</td>
<td>Time stamp when volume creation was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td>zone</td>
<td>Availability zone in which the volume is running</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>snapshotId</td>
<td>Snapshot from which the volume was created, if applicable</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
</tbody>
</table>
CreateVolumeType

The CreateVolumeType data type.
Relevant Operations

- CreateVolume
The following table describes the elements contained in `CreateVolumeType`.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>size</td>
<td>The size of the volume, in GiB&lt;br&gt;Type: xsd:string&lt;br&gt;Default: none&lt;br&gt;Valid Values: 1 to 1024&lt;br&gt;Constraints: none</td>
</tr>
<tr>
<td>snapshotId</td>
<td>The snapshot on which to base the new volume.&lt;br&gt;Type: xsd:string&lt;br&gt;Default: none&lt;br&gt;Valid Values: ID of a snapshot that you own&lt;br&gt;Constraints: none</td>
</tr>
<tr>
<td>zone</td>
<td>Availability zone in which to create the volume.&lt;br&gt;Type: xsd:string&lt;br&gt;Default: none&lt;br&gt;Valid Values: A valid availability zone&lt;br&gt;Constraints: none</td>
</tr>
</tbody>
</table>
DeleteSnapshotResponseType

The DeleteSnapshotResponseType data type.
Relevant Operations

- DeleteSnapshot
The following table describes the elements contained in DeleteSnapshotResponseType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>True if deletion succeeded. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
DeleteSnapshotType

The DeleteSnapshotType data type.
Relevant Operations

- DeleteSnapshot
Contents

The following table describes the elements contained in DeleteSnapshotType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshotId</td>
<td>The ID of the Amazon EBS snapshot to delete</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a snapshot that you own</td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
</tr>
</tbody>
</table>
DeleteVolumeResponseType

The DeleteVolumeResponseType data type.
Relevant Operations

- DeleteVolume
The following table describes the elements contained in DeleteVolumeResponseType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if deletion succeeded. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
DeleteVolumeType

The DeleteVolumeType data type.
Relevant Operations

- DeleteVolume
## Contents

The following table describes the elements contained in `DeleteVolumeType`.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume to delete</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a volume that you own</td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
</tr>
</tbody>
</table>
DescribeSnapshotsResponseType

The DescribeSnapshotsResponseType data type.
Relevant Operations

- DescribeSnapshots
Contents

The following table describes the elements contained in DescribeSnapshotsResponseType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshotId</td>
<td>The ID of the snapshot&lt;br&gt;Type: xsd:string&lt;br&gt;Default: Describes all snapshots that you own&lt;br&gt;Valid Values: ID of a snapshot that you own&lt;br&gt;Constraints: none</td>
</tr>
<tr>
<td>volumeId</td>
<td>The ID of the volume&lt;br&gt;Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Snapshot state (e.g., pending, completed)&lt;br&gt;Type: xsd:string</td>
</tr>
<tr>
<td>startTime</td>
<td>Time stamp when the snapshot was initiated&lt;br&gt;Type: xsd:dateTime</td>
</tr>
<tr>
<td>progress</td>
<td>The progress of the snapshot, in percentage&lt;br&gt;Type: xsd:string</td>
</tr>
</tbody>
</table>
DescribeSnapshotsType

The DescribeSnapshotsType data type.
Relevant Operations

- DescribeSnapshots
## Contents

The following table describes the elements contained in DescribeSnapshotsType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshotId</td>
<td>The ID of the Amazon EBS snapshot</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Default: Describes all snapshots that you own</td>
</tr>
<tr>
<td></td>
<td>Valid Values: IDs of one or more snapshots that you own</td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
</tr>
</tbody>
</table>
DescribeVolumesResponseType

The DescribeVolumesResponseType data type.
Relevant Operations

- DescribeVolumes
## Contents

The following table describes the elements contained in DescribeVolumesResponseType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>size</td>
<td>The size of the volume, in GiBs</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., creating, available, in-use, deleting)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>createTime</td>
<td>Time stamp when volume creation was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td>zone</td>
<td>Availability zone in which the instance launched</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>snapshotId</td>
<td>Snapshot from which the volume is based, if applicable</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>attachmentSet</td>
<td>Specifies an attachment of a volume to an instance</td>
</tr>
<tr>
<td></td>
<td>Type: AttachmentSet</td>
</tr>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Ancestor: attachmentSet</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Ancestor: attachmentSet</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., creating, available)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Ancestor: attachmentSet</td>
</tr>
<tr>
<td>attachTime</td>
<td>Time stamp when the attachment was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td></td>
<td>Ancestor: attachmentSet</td>
</tr>
</tbody>
</table>
DescribeVolumesType

The DescribeVolumesType data type.
Relevant Operations

- DescribeVolumes
Contents

The following table describes the elements contained in DescribeVolumesType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| volumeId | The ID of the volume to list  
Type: xsd:string  
Default: Describes all volumes that you own  
Valid Values: IDs of one or more volumes that you own  
Constraints: none |
DetachVolumeResponseType

The DetachVolumeResponseType data type.
Relevant Operations

- DetachVolume
## Contents

The following table describes the elements contained in `DetachVolumeResponse`.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>device</td>
<td>The device as it is exposed to the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Attachment state (e.g., attaching, detached, detaching, busy)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>attachTime</td>
<td>Time stamp when detaching was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
</tbody>
</table>
DetachVolumeType

The DetachVolumeType data type.
Relevant Operations

- DetachVolume
Contents

The following table describes the elements contained in DetachVolumeType.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the Amazon EBS volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a volume that you own</td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance from which the volume will detach</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of the instance attached to the volume</td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
</tr>
<tr>
<td>device</td>
<td>The device name</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
<tr>
<td></td>
<td>Valid Values: Valid device ID</td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
</tr>
<tr>
<td>force</td>
<td>Forces detachment if the previous detachment attempt did not occur cleanly</td>
</tr>
<tr>
<td></td>
<td>(logging into an instance, unmounting the volume, and detaching normally).</td>
</tr>
<tr>
<td></td>
<td>This option can lead to data loss or a corrupted file system. Use this</td>
</tr>
<tr>
<td></td>
<td>option only as a last resort to detach an instance from a failed instance.</td>
</tr>
<tr>
<td></td>
<td>The instance will not have an opportunity to flush file system caches nor</td>
</tr>
<tr>
<td></td>
<td>file system meta data.</td>
</tr>
<tr>
<td></td>
<td>If you use this option, you must perform file system check and repair</td>
</tr>
<tr>
<td></td>
<td>procedures.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:boolean</td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
</tr>
<tr>
<td></td>
<td>Valid Values: none</td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
</tr>
</tbody>
</table>
Amazon EC2 SOAP API

The Amazon EC2 API consists of web service operations for every task the service can perform. This section describes each operation in detail.

- AllocateAddress
- AssociateAddress
- AttachVolume
- AuthorizeSecurityGroupIngress
- ConfirmProductInstance
- CreateKeyPair
- CreateSecurityGroup
- CreateSnapshot
- CreateVolume
- DeleteKeyPair
- DeleteSecurityGroup
- DeleteSnapshot
- DeleteVolume
- DeregisterImage
- DescribeAddresses
- DescribeAvailabilityZones
- DescribeImageAttribute
- DescribeImages
- DescribeInstances
- DescribeKeyPairs
- DescribeSecurityGroups
- DescribeSnapshots
- DescribeVolumes
- DetachVolume
- DisassociateAddress
- GetConsoleOutput
- ModifyImageAttribute
- RebootInstances
- RegisterImage
- ReleaseAddress
- ResetImageAttribute
- RevokeSecurityGroupIngress
- RunInstances
- TerminateInstances
List of Operations by Function

Images
- RegisterImage
- DescribeImages
- DeregisterImage

Instances
- RunInstances
- DescribeInstances
- TerminateInstances
- ConfirmProductInstance

Key Pairs
- CreateKeyPair
- DescribeKeyPairs
- DeleteKeyPair

Image Attributes
- ModifyImageAttribute
- DescribeImageAttribute
- ResetImageAttribute

Security Groups
- CreateSecurityGroup
- DescribeSecurityGroups
- DeleteSecurityGroup
- AuthorizeSecurityGroupIngress
- RevokeSecurityGroupIngress

**Elastic IP Addresses**
- AllocateAddress
- DescribeAddresses
- ReleaseAddress
- AssociateAddress
- DisassociateAddress

**Availability Zones**
- DescribeAvailabilityZones

**Amazon EBS**
- CreateVolume
- DescribeVolumes
- DeleteVolume
- AttachVolume
- DetachVolume
- CreateSnapshot
- DescribeSnapshots
- DeleteSnapshot
AllocateAddress

The AllocateAddress operation acquires an elastic IP address for use with your account.
Request Parameters

The AllocateAddress operation does not have any request parameters.
Response Elements

The following table describes the default response tags included in AllocateAddress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>publicIp</td>
<td>Returned IP address. Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

<AllocateAddress/>
Sample Response

<AllocateAddressResponse xmlns="http://ec2.amazonaws.com/doc/2008-02-01/"
</AllocateAddressResponse>
Related Operations

- DescribeAddresses
- ReleaseAddress
- AssociateAddress
- DisassociateAddress
AssociateAddress

The AssociateAddress operation associates an elastic IP address with an instance. If the IP address is currently assigned to another instance, the IP address is assigned to the new instance. This is an idempotent operation. If you enter it more than once, Amazon EC2 does not return an error.
# Request Parameters

The following table describes the request parameters for `AssociateAddress`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>instanceId</code></td>
<td>The instance to which the IP address is assigned. Type: xsd:string</td>
<td>Yes</td>
</tr>
<tr>
<td><code>publicIp</code></td>
<td>IP address that you are assigning to the instance. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Response Elements

The following table describes the default response tags included in `AssociateAddress` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the IP address is associated with the instance. Otherwise, false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

```xml
<AssociateAddress xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <instanceId>i-28a64341</instanceId>
</AssociateAddress>
```
Sample Response

<?xml version="1.0" encoding="UTF-8"?>
<AssociateAddressResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
  <return>true</return>
</AssociateAddressResponse>
Related Operations

- AllocateAddress
- DescribeAddresses
- ReleaseAddress
- DisassociateAddress
AttachVolume

The AttachVolume operation attaches an Amazon EBS volume to an instance. For more information about Amazon EBS, see Amazon Elastic Block Store.
## Request Parameters

The following table describes the request parameters for AttachVolume. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the Amazon EBS volume</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a volume that you own</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: The volume and instance must be within the same availability zone</td>
<td></td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance to which the volume attaches</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of an instance that you own</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: The volume and instance must be within the same availability zone</td>
<td></td>
</tr>
<tr>
<td>device</td>
<td>Specifies how the device is exposed to the instance (e.g., /dev/sdh)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: Valid device ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: The specified device ID cannot be in use by another device or an instance store</td>
<td></td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in AttachVolume responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>device</td>
<td>The device as it is exposed to the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., attaching, attached)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>attachTime</td>
<td>Time stamp when the attachment was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
</tbody>
</table>
Sample Request

|   | <volumeId>vol-4d826724</volumeId>
|   | <instanceId>i-6058a509</instanceId>
|   | <device>/dev/sdh</device>
| </AttachVolume> |
Sample Response

  <volumeId>vol-4d826724</volumeId>
  <instanceId>i-6058a509</instanceId>
  <device>/dev/sdh</device>
  <status>attaching</status>
  <attachTime>2008-05-07T11:51:50.000Z</attachTime>
</AttachVolumeResponse>
Related Operations

- CreateVolume
- DeleteVolume
- DescribeVolumes
- DetachVolume
AuthorizeSecurityGroupIngress

The AuthorizeSecurityGroupIngress operation adds permissions to a security group.

Permissions are specified by the IP protocol (TCP, UDP or ICMP), the source of the request (by IP range or an Amazon EC2 user-group pair), the source and destination port ranges (for TCP and UDP), and the ICMP codes and types (for ICMP).

Permission changes are propagated to instances within the security group as quickly as possible. However, depending on the number of instances, a small delay might occur.
Request Parameters

The following table describes the request parameters for 
AuthorizeSecurityGroupIngress. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>userId</td>
<td>AWS Access Key ID. Type: xsd:string</td>
<td>Yes</td>
</tr>
<tr>
<td>groupName</td>
<td>Name of the group to modify. Type: xsd:string</td>
<td>Yes</td>
</tr>
<tr>
<td>ipPermissions</td>
<td>Set of permissions to add to the group. Type: IpPermissionType[]</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in AuthorizeSecurityGroupIngress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if permissions successfully added. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

```xml
  <groupId/>
  <groupName>WebServers</groupName>
  <ipPermissions>
    <item>
      <ipProtocol>tcp</ipProtocol>
      <fromPort>80</fromPort>
      <toPort>80</toPort>
      <groups/>
      <ipRanges>
        <item>
          <cidrIp>0.0.0.0/0</cidrIp>
        </item>
      </ipRanges>
    </item>
  </ipPermissions>
</AuthorizeSecurityGroupIngress>
```
Sample Response

```
  <return>true</return>
</AuthorizeSecurityGroupIngressResponse>
```
Related Operations

- [CreateSecurityGroup](#)
- [DescribeSecurityGroups](#)
- [RevokeSecurityGroupIngress](#)
- [DeleteSecurityGroup](#)
ConfirmProductInstance

The ConfirmProductInstance operation returns true if the specified product code is attached to the specified instance. The operation returns false if the product code is not attached to the instance.

The ConfirmProductInstance operation can only be executed by the owner of the AMI. This feature is useful when an AMI owner is providing support and wants to verify whether a user's instance is eligible.
## Request Parameters

The following table describes the request parameters for ConfirmProductInstance. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| `productCode` | The product code to confirm.  
Type: xsd:string                                                                    | Yes      |
| `instanceId` | The instance for which to confirm the product code.  
Type: xsd:string                                                                  | Yes      |
## Response Elements

The following table describes the default response tags included in ConfirmProductInstance responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>True if the product code is attached to the instance, false if it is not.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:boolean</td>
</tr>
<tr>
<td>ownerId</td>
<td>The instance owner's account ID. Only present if the product code is attached to the instance.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>Sample Request</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td></td>
</tr>
</tbody>
</table>
  <productCode>774F4FF8</productCode>  
  <instanceId>i-10a64379</instanceId>  
</ConfirmProductInstance>` |
Sample Response

<ConfirmProductInstanceResponse
xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <return>true</return>
  <ownerId>254933287430</ownerId>
</ConfirmProductInstanceResponse>
Related Operations

- DescribeInstances
- RunInstances
CreateKeyPair

The CreateKeyPair operation creates a new 2048 bit RSA key pair and returns a unique ID that can be used to reference this key pair when launching new instances. For more information, see RunInstances.
Request Parameters

The following table describes the request parameters for CreateKeyPair. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>keyName</code></td>
<td>A unique name for the key pair. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in CreateKeyPair responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyName</td>
<td>The key pair name provided in the original request. Type: xsd:string</td>
</tr>
<tr>
<td>keyFingerprint</td>
<td>A SHA-1 digest of the DER encoded private key. Type: xsd:string</td>
</tr>
<tr>
<td>keyMaterial</td>
<td>An unencrypted PEM encoded RSA private key. Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

```xml
<CreateKeyPair xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <keyName>example-key-name</keyName>
</CreateKeyPair>
```
Sample Response

<CreateKeyPairResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <keyName>example-key-name</keyName>
</CreateKeyPairResponse>
Related Operations

- DescribeKeyPairs
- DeleteKeyPair
- RunInstances
CreateSecurityGroup

The CreateSecurityGroup operation creates a new security group.

Every instance is launched in a security group. If no security group is specified during launch, the instances are launched in the default security group. Instances within the same security group have unrestricted network access to each other. Instances will reject network access attempts from other instances in a different security group. As the owner of instances you can grant or revoke specific permissions using the AuthorizeSecurityGroupIngress and RevokeSecurityGroupIngress operations.
Request Parameters

The following table describes the request parameters for CreateSecurityGroup. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupName</td>
<td>Name of the new security group. Type: xsd:string</td>
<td>Yes</td>
</tr>
<tr>
<td>groupDescription</td>
<td>Description of the new security group. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in CreateSecurityGroup responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if call succeeded. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

```xml
  <groupName>WebServers</groupName>
  <groupDescription>Web</groupDescription>
</CreateSecurityGroup>
```
Sample Response

```xml
<return>true</return>
</CreateSecurityGroupResponse>
```
Related Operations

- RunInstances
- DescribeSecurityGroups
- AuthorizeSecurityGroupIngress
- RevokeSecurityGroupIngress
- DeleteSecurityGroup
CreateSnapshot

The CreateSnapshot operation creates a snapshot of an Amazon EBS volume and stores it in Amazon S3. You can use snapshots for backups, to make identical copies of instance devices, and to save data before shutting down an instance. For more information, see Amazon Elastic Block Store.
## Request Parameters

The following table describes the request parameters for `CreateSnapshot`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| `volumeId` | The ID of the Amazon EBS volume to snapshot  
Type: xsd:string  
Default: none  
Valid Values: ID of a volume that you own  
Constraints: ID of a volume that you own | Yes      |
# Response Elements

The following table describes the default response tags included in `CreateSnapshot` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| snapshotId | The ID of the snapshot
|           | Type: xsd:string                                                            |
| volumeId  | The ID of the volume
|           | Type: xsd:string                                                            |
| status    | Snapshot state (e.g., pending, completed)
|           | Type: xsd:string                                                            |
| startTime | Time stamp when the snapshot was initiated
|           | Type: xsd:dateTime                                                           |
| progress  | The progress of the snapshot, in percentage
|           | Type: xsd:string                                                            |
Sample Request

<CreateSnapshot xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <volumeId>vol-4d826724</volumeId>
</CreateSnapshot>
Sample Response

```xml
  <snapshotId>snap-78a54011</snapshotId>
  <volumeId>vol-4d826724</volumeId>
  <status>pending</status>
  <startTime>2008-05-07T12:51:50.000Z</startTime>
  <progress/>
</CreateSnapshotResponse>
```
Related Operations

- **DeleteSnapshot**
- **DescribeSnapshots**
CreateVolume

The CreateVolume operation creates a new Amazon EBS volume to which any Amazon EC2 instance can attach within the same availability zone. For more information, see Amazon Elastic Block Store.

**Note**
You must specify an availability zone when creating a volume. The volume and the instance to which it attaches must be in the same availability zone.
## Request Parameters

The following table describes the request parameters for `CreateVolume`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>size</em></td>
<td>The size of the volume, in GiBs. Required if you are not creating a volume from a snapshot. Type: xsd:string Default: none Valid Values: 1 to 1024 Constraints: none Condition: Required if you are not creating a volume from a snapshot.</td>
<td>Conditional</td>
</tr>
<tr>
<td><em>snapshotId</em></td>
<td>The snapshot from which to create the new volume. Type: xsd:string Default: none Valid Values: ID of a snapshot that you own Constraints: none Condition: Required if you are creating a volume from a snapshot.</td>
<td>Conditional</td>
</tr>
<tr>
<td><em>availabilityZone</em></td>
<td>The availability zone in which to create the new volume. Type: xsd:string Default: none Valid Values: A valid availability zone Constraints: none</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in CreateVolume responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>size</td>
<td>The size of the volume, in GiBs</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., creating, available)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>createTime</td>
<td>Time stamp when volume creation was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td>availabilityZone</td>
<td>Availability zone in which the volume was created</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>snapshotId</td>
<td>Snapshot from which the volume was created, if applicable</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

```xml
  <size>800</size>
  <zone>us-east-1a</zone>
</CreateVolume>
```
Sample Response

```
  <volumeId>vol-4d826724</volumeId>
  <size>800</size>
  <statusCreating</status>
  <createTime>2008-05-07T11:51:50.000Z</createTime>
  <zone>us-east-1a</zone>
  <snapshotId></snapshotId>
</CreateVolumeResponse>
```
Related Operations

- DeleteVolume
- DescribeVolumes
- AttachVolume
- DetachVolume
- DescribeAvailabilityZones
DeleteKeyPair

The `DeleteKeyPair` operation deletes a key pair.
Request Parameters

The following table describes the request parameters for DeleteKeyPair. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyName</td>
<td>Name of the key pair to delete. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
# Response Elements

The following table describes the default response tags included in `DeleteKeyPair` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the key was successfully deleted. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

<DeleteKeyPair xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
    <keyName>example-key-name</keyName>
</DeleteKeyPair>
Sample Response

<DeleteKeyPair xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <return>true</return>
</DeleteKeyPair>
Related Operations

- CreateKeyPair
- DescribeKeyPairs
DeleteSecurityGroup

The DeleteSecurityGroup operation deletes a security group.

Note

If you attempt to delete a security group that contains instances, a fault is returned.

If you attempt to delete a security group that is referenced by another security group, a fault is returned. For example, if security group B has a rule that allows access from security group A, security group A cannot be deleted until the allow rule is removed.
Request Parameters

The following table describes the request parameters for DeleteSecurityGroup. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>groupName</code></td>
<td>Name of the security group to delete. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DeleteSecurityGroup responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the group is deleted. Otherwise, false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

<?xml version="1.0" encoding="UTF-8"?>
  <groupName>RangedPortsBySource</groupName>
</DeleteSecurityGroup>
Sample Response

  <return>true</return>
</DeleteSecurityGroupResponse>
Related Operations

- CreateSecurityGroup
- DescribeSecurityGroups
- AuthorizeSecurityGroupIngress
- RevokeSecurityGroupIngress
DeleteSnapshot

The `DeleteSnapshot` operation deletes a snapshot of an Amazon EBS volume that is stored in Amazon S3. For more information, see Amazon Elastic Block Store.
Request Parameters

The following table describes the request parameters for DeleteSnapshot. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshotId</td>
<td>The ID of the Amazon EBS snapshot to delete Type: xsd:string Default: none Valid Values: ID of a snapshot that you own Constraints: none</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in `DeleteSnapshot` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if deletion succeeded. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

```xml
    <snapshotId>snap-78a54011</snapshotId>
</DeleteSnapshot>
```
Sample Response

  <return>true</return>
</DeleteSnapshotResponse>
Related Operations

- CreateSnapshot
- DescribeSnapshots
DeleteVolume

The `DeleteVolume` operation deletes an Amazon EBS volume. For more information about Amazon EBS, see [Amazon Elastic Block Store](https://aws.amazon.com/elasticblockstore/).
Request Parameters

The following table describes the request parameters for DeleteVolume. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume to delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a volume that you own</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Response Elements**

The following table describes the default response tags included in `DeleteVolume` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if deletion succeeded</td>
<td>xsd:boolean</td>
</tr>
</tbody>
</table>

Sample Request

  <volumeId>vol-4282672b</volumeId>
</DeleteVolume>
Sample Response

  <return>true</return>
</DeleteVolumeResponse>
Related Operations

- CreateVolume
- DescribeVolumes
- AttachVolume
- DetachVolume
The **DeregisterImage** operation deregisters an AMI. Once deregistered, instances of the AMI can no longer be launched.
## Request Parameters

The following table describes the request parameters for **DeregisterImage**. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>imageId</code></td>
<td>Unique ID of the AMI which was assigned during registration (see <a href="#">RegisterImage</a>). For information on viewing the IDs of AMIs you own, see <a href="#">DescribeImages</a>. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Response Elements

The following table describes the default response tags included in `DeregisterImage` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if deregistration succeeded; otherwise false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

```xml
  <imageId>ami-61a54008</imageId>
</DeregisterImage>
```
<table>
<thead>
<tr>
<th>Sample Response</th>
</tr>
</thead>
</table>
|     <return>true</return>
| </DeregisterImageResponse> |
Related Operations

- RegisterImage
- DescribeImages
DescribeAddresses

The DescribeAddresses operation lists elastic IP addresses assigned to your account.
# Request Parameters

The following table describes the request parameters for DescribeAddresses. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| `publicIpsSet` | Elastic IP addresses to describe. Type: xsd:string[]  
Default: none  
Valid Values: Can be empty  
Constraints: none | Yes      |
Response Elements

The following table describes the default response tags included in DescribeAddresses responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>publicIp</td>
<td>Elastic IP address assigned to your account. Type: xsd:string</td>
</tr>
<tr>
<td>instanceId</td>
<td>Instance ID to which the IP address is assigned. Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

<DescribeAddresses xmlns="http://ec2.amazonaws.com/doc/2008-02-01">
  <publicIpsSet>
    <item>
    </item>
  </publicIpsSet>
</DescribeAddresses>
Sample Response

```xml
<DescribeAddressesResponse xmlns="http://ec2.amazonaws.com/doc/2008-02-01">
  <addressesSet>
    <item>
      <instanceId>i-28a64341</instanceId>
    </item>
  </addressesSet>
</DescribeAddressesResponse>
```
Related Operations

- AllocateAddress
- ReleaseAddress
- AssociateAddress
- DisassociateAddress
DescribeAvailabilityZones

The DescribeAvailabilityZones operation displays availability zones that are currently available to the account and their states.

Note

Availability zones are not the same across accounts. The availability zone us-east-1a for account A is not necessarily the same as us-east-1a for account B. Zone assignments are mapped independently for each account.
Request Parameters

The following table describes the request parameters for DescribeAvailabilityZones. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>zoneName</td>
<td>Name of an availability zone. Type: xsd:string[]</td>
<td>No</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DescribeAvailabilityZones responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>availabilityZoneInfo</td>
<td>Availability zone information. Type: [AvailabilityZoneItemType]</td>
</tr>
</tbody>
</table>
## Sample Request

```xml
<DescribeAvailabilityZones
xmlns="http://ec2.amazonaws.com/doc/2008-02-01">
    <availabilityZoneSet/>
<DescribeAvailabilityZones>
```
Sample Response

<DescribeAvailabilityZonesResponse
xmlns="http://ec2.amazonaws.com/doc/2008-02-01/">
  <availabilityZoneInfo>
    <item>
      <zoneName>us-east-1a</zoneName>
      <zoneState>available</zoneState>
    </item>
    <item>
      <zoneName>us-east-1b</zoneName>
      <zoneState>available</zoneState>
    </item>
    <item>
      <zoneName>us-east-1c</zoneName>
      <zoneState>available</zoneState>
    </item>
  </availabilityZoneInfo>
</DescribeAvailabilityZonesResponse>
Related Operations

- RunInstances
DescribeImageAttribute

The DescribeImageAttribute operation returns information about an attribute of an AMI. Only one attribute can be specified per call.
# Request Parameters

The following table describes the request parameters for DescribeImageAttribute. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>imageId</code></td>
<td>ID of the AMI for which an attribute will be described.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
<td></td>
</tr>
<tr>
<td><code>launchPermission</code></td>
<td>Describes launch permissions of the AMI.</td>
<td>Choice</td>
</tr>
<tr>
<td></td>
<td>Type: EmptyElementType</td>
<td></td>
</tr>
<tr>
<td><code>productCodes</code></td>
<td>Describes the product code associated with the AMI.</td>
<td>Choice</td>
</tr>
<tr>
<td></td>
<td>Type: EmptyElementType</td>
<td></td>
</tr>
<tr>
<td><code>kernel</code></td>
<td>Describes the ID of the kernel associated with the AMI.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
<td></td>
</tr>
<tr>
<td><code>ramdisk</code></td>
<td>Describes the ID of the RAM disk associated with the AMI.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
<td></td>
</tr>
<tr>
<td><code>blockDeviceMapping</code></td>
<td>Describes the mapping that defines native device names to use</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>when exposing virtual devices.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
<td></td>
</tr>
</tbody>
</table>
# Response Elements

The following table describes the default response tags included in `DescribeImageAttribute` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| `imageId`         | ID of the AMI of which parameters are described.  
Type: xsd:string                                                                                  |
| `launchPermission`| Launch permissions of the AMI. Returned if `launchPermission` is specified.  
Type: [LaunchPermissionItemType]                                                                  |
| `productCodes`    | Product codes of the AMI. Returned if `productCodes` is specified.  
Type: [ProductCodeItemType]                                                                     |
| `kernel`          | ID of the kernel associated with the AMI. Returned if `kernel` is specified.  
Type: xsd:string                                                                                 |
| `ramdisk`         | ID of the RAM disk associated with the AMI. Returned if `ramdisk` is specified.  
Type: xsd:string                                                                                   |
| `blockDeviceMapping` | Mapping that defines native device names to use when exposing virtual  
devices. Returned if `blockDeviceMapping` is specified.  
Type: [BlockDeviceMappingItemType]                                                                |
Sample Request - Launch Permission

```xml
<DescribeImageAttribute xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <imageId>ami-61a54008</imageId>
  <launchPermission />
</DescribeImageAttribute>
```
Sample Response - Launch Permission

```xml
<DescribeImageAttributeResponse
 xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
 <imageId>ami-61a54008</imageId>
 <launchPermission>
  <item>
   <group>all</group>
  </item>
  <item>
   <userId>495219933132</userId>
  </item>
 </launchPermission>
</DescribeImageAttributeResponse>
```
Sample Request - Product Codes

<DescribeImageAttribute xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <imageId>ami-61a54008</imageId>
  <productCodes />
</DescribeImageAttribute>
Sample Response - Product Codes

<DescribeImageAttributeResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <imageId>ami-61a54008</imageId>
  <productCodes>
    <item>
      <productCode>774F4FF8</productCode>
    </item>
  </productCodes>
</DescribeImageAttributeResponse>
Related Operations

- DescribeImages
- ModifyImageAttribute
- ResetImageAttribute
DescribeImages

The DescribeImages operation returns information about AMIs, AKIs, and ARIs available to the user. Information returned includes image type, product codes, architecture, and kernel and RAM disk IDs. Images available to the user include public images available for any user to launch, private images owned by the user making the request, and private images owned by other users for which the user has explicit launch permissions.

Launch permissions fall into three categories:

<table>
<thead>
<tr>
<th>Launch Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td>The owner of the AMI granted launch permissions for the AMI to the all group. All users have launch permissions for these AMIs.</td>
</tr>
<tr>
<td>explicit</td>
<td>The owner of the AMI granted launch permissions to a specific user.</td>
</tr>
<tr>
<td>implicit</td>
<td>A user has implicit launch permissions for all AMIs he or she owns.</td>
</tr>
</tbody>
</table>

The list of AMIs returned can be modified by specifying AMI IDs, AMI owners, or users with launch permissions. If no options are specified, Amazon EC2 returns all AMIs for which the user has launch permissions.

If you specify one or more AMI IDs, only AMIs that have the specified IDs are returned. If you specify an invalid AMI ID, a fault is returned. If you specify an AMI ID for which you do not have access, it will not be included in the returned results.

If you specify one or more AMI owners, only AMIs from the specified owners and for which you have access are returned. The results can include the account IDs of the specified owners, amazon for AMIs owned by Amazon or self for AMIs that you own.

If you specify a list of executable users, only users that have launch permissions for the AMIs are returned. You can specify account IDs (if you own the AMI(s)), self for AMIs for which you own or have explicit permissions, or all for public AMIs.
Note

Deregistered images are included in the returned results for an unspecified interval after deregistration.
## Request Parameters

The following table describes the request parameters for DescribeImages. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>imagesSet</code></td>
<td>AMI IDs to describe</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string[]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: Can be empty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
<tr>
<td><code>ownersSet</code></td>
<td>Owners of AMIs to describe</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string[]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: Can be empty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
<tr>
<td><code>executableBySet</code></td>
<td>AMIs for which specified users have access</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string[]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: Can be empty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
</tbody>
</table>
**Response Elements**

The following table describes the default response tags included in `DescribeImages` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>imagesSet</td>
<td>A list of image descriptions</td>
</tr>
<tr>
<td></td>
<td>Type: [DescribeImagesResponseItemType][]</td>
</tr>
</tbody>
</table>
Sample Request

<DescribeImages xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <executableBySet>
    <item>
      <user>all</user>
    </item>
  </executableBySet>
  <ownersSet />
  <imagesSet>
    <item>
      <imageId>ami-be3adfd7</imageId>
    </item>
  </imagesSet>
</DescribeImages>
Sample Response

  <imagesSet>
    <item>
      <imageId>ami-be3adfd7</imageId>
      <imageLocation>ec2-public-images/fedora-8-i386-base-v1.04.manifest.xml</imageLocation>
      <imageState>available</imageState>
      <imageOwnerId>206029621532</imageOwnerId>
      <isPublic>false</isPublic>
      <architecture>i386</architecture>
      <imageType>machine</imageType>
      <kernelId>aki-4438dd2d</kernelId>
      <ramdiskId>ari-4538dd2c</ramdiskId>
    </item>
  </imagesSet>
</DescribeImagesResponse>
Related Operations

- DescribeInstances
- DescribeImageAttribute
**DescribeInstances**

The DescribeInstances operation returns information about instances that you own.

If you specify one or more instance IDs, Amazon EC2 returns information for those instances. If you do not specify instance IDs, Amazon EC2 returns information for all relevant instances. If you specify an invalid instance ID, a fault is returned. If you specify an instance that you do not own, it will not be included in the returned results.

Recently terminated instances might appear in the returned results. This interval is usually less than one hour.
Request Parameters

The following table describes the request parameters for DescribeInstances. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>instancesSet</td>
<td>Set of instances IDs to get the status of. Type: xsd:string[] Default: none Valid Values: Can be empty Constraints: none</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DescribeInstances responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reservationSet</td>
<td>A list of structures describing the status of all requested instances. Type: ReservationInfoType[]</td>
</tr>
</tbody>
</table>
Sample Request

<DescribeInstances xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <instancesSet>
    <item>
      <instanceId>i-28a64341</instanceId>
    </item>
  </instancesSet>
</DescribeInstances>
Sample Response

<DescribeInstancesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
  <reservationSet>
    <item>
      <reservationId>r-44a5402d</reservationId>
      <ownerId>UYY3TLBUXIE0N5QVUXG60MPWZ1QNFM</ownerId>
      <groupSet>
        <item>
          <groupId>default</groupId>
        </item>
      </groupSet>
      <instancesSet>
        <item>
          <instanceId>i-28a64341</instanceId>
          <imageId>ami-6ea54007</imageId>
          <instanceState>
            <code>0</code>
            <name>running</name>
          </instanceState>
          <privateDnsName>10-251-50-132.ec2.internal</privateDnsName>
          <dnsName>ec2-72-44-33-4.compute-1.amazonaws.com</dnsName>
          <keyName>example-key-name</keyName>
          <amiLaunchIndex>23</amiLaunchIndex>
          <productCodesSet>
            <item><productCode>774F4FF8</productCode></item>
          </productCodesSet>
          <instanceType>m1.large</instanceType>
          <launchTime>2007-08-07T11:54:42.000Z</launchTime>
          <placement>
            <availabilityZone>us-east-1b</availabilityZone>
          </placement>
          <kernelId>aki-ba3adfd3</kernelId>
          <ramdiskId>ari-badbad00</ramdiskId>
        </item>
      </instancesSet>
    </item>
  </reservationSet>
</DescribeInstancesResponse>
Related Operations

- RunInstances
- TerminateInstances
DescribeKeyPairs

The DescribeKeyPairs operation returns information about key pairs available to you. If you specify key pairs, information about those key pairs is returned. Otherwise, information for all registered key pairs is returned.
Request Parameters

The following table describes the request parameters for DescribeKeyPairs. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>keySet</td>
<td>Key pair IDs to describe.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string[]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: Can be empty</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DescribeKeyPairs responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keySet</td>
<td>A list of key pair descriptions</td>
</tr>
<tr>
<td></td>
<td>Type: [DescribeKeyPairsResponseItemType]</td>
</tr>
</tbody>
</table>
Sample Request

<DescribeKeyPairs xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <keySet>
    <item>
      <keyName>example-key-name</keyName>
    </item>
  </keySet>
</DescribeKeyPairs>
<DescribeKeyPairsResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <keySet>
    <item>
      <keyName>example-key-name</keyName>
    </item>
  </keySet>
</DescribeKeyPairsResponse>
Related Operations

- CreateKeyPair
- DeleteKeyPair
- RunInstances
DescribeSecurityGroups

The DescribeSecurityGroups operation returns information about security groups that you own.

If you specify security group names, information about those security group is returned. Otherwise, information for all security group is returned. If you specify a group that does not exist, a fault is returned.
**Request Parameters**

The following table describes the request parameters for DescribeSecurityGroups. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>securityGroupSet</code></td>
<td>List of security groups to describe. Type: xsd:string[]</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DescribeSecurityGroups responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityGroupInfo</td>
<td>Information about security groups. Type: SecurityGroupItemType[]</td>
</tr>
</tbody>
</table>
Sample Request

```xml
  <securityGroupSet>
    <item>
      <groupName>WebServers</groupName>
    </item>
    <item>
      <groupName>RangedPortsBySource</groupName>
    </item>
  </securityGroupSet>
</DescribeSecurityGroups>
```
  <securityGroupInfo>
    <item>
      <ownerId>UYY3TLBUXIEON5NQVUUX6OMPWBZIQNFM</ownerId>
      <groupName>WebServers</groupName>
      <groupDescription>Web</groupDescription>
      <ipPermissions>
        <item>
          <ipProtocol>tcp</ipProtocol>
          <fromPort>80</fromPort>
          <toPort>80</toPort>
        </item>
      </ipPermissions>
    </item>
    <item>
      <ownerId>UYY3TLBUXIEON5NQVUUX6OMPWBZIQNFM</ownerId>
      <groupName>RangedPortsBySource</groupName>
      <groupDescription>A</groupDescription>
      <ipPermissions>
        <item>
          <ipProtocol>tcp</ipProtocol>
          <fromPort>6000</fromPort>
          <toPort>7000</toPort>
        </item>
      </ipPermissions>
    </item>
  </securityGroupInfo>
</DescribeSecurityGroupsResponse>
Related Operations

- CreateSecurityGroup
- AuthorizeSecurityGroupIngress
- RevokeSecurityGroupIngress
- DeleteSecurityGroup
DescribeSnapshots

The DescribeSnapshots operation describes the status of Amazon EBS snapshots. For more information about Amazon EBS, see Amazon Elastic Block Store.
Request Parameters

The following table describes the request parameters for DescribeSnapshots. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| snapshotId.n | The ID of the Amazon EBS snapshot  
Type: xsd:string  
Default: Describes all snapshots that you own  
Valid Values: IDs of one or more snapshots that you own  
Constraints: none | No       |
Response Elements

The following table describes the default response tags included in DescribeSnapshots responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshotId</td>
<td>The ID of the snapshot&lt;br&gt;Type: xsd:string</td>
</tr>
<tr>
<td>volumeId</td>
<td>The ID of the volume&lt;br&gt;Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Snapshot state (e.g., pending, completed)&lt;br&gt;Type: xsd:string</td>
</tr>
<tr>
<td>startTime</td>
<td>Time stamp when the snapshot was initiated&lt;br&gt;Type: xsd:dateTime</td>
</tr>
<tr>
<td>progress</td>
<td>The progress of the snapshot, in percentage&lt;br&gt;Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

<DescribeSnapshots xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <snapshotId>snap-78a54011</snapshotId>
</DescribeSnapshots>
Sample Response

<DescribeSnapshotsResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
  <snapshotId>snap-78a54011</snapshotId>
  <volumeId>vol-4d826724</volumeId>
  <status>pending</status>
  <startTime>2008-05-07T12:51:50.000Z</startTime>
  <progress>80%</progress>
</DescribeSnapshotsResponse>
Related Operations

- CreateSnapshot
- DeleteSnapshot
DescribeVolumes

The DescribeVolumes operation lists the specified Amazon EBS volumes that you own. If you do not specify one or more volume IDs, Amazon EBS lists all volumes that you own. For more information about Amazon EBS, see Amazon Elastic Block Store.
Request Parameters

The following table describes the request parameters for DescribeVolumes. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| `volumeId` | The ID of the volume to list  
Type: xsd:string  
Default: Describes all volumes that you own  
Valid Values: IDs of one or more volumes that you own  
Constraints: none | No       |
**Response Elements**

The following table describes the default response tags included in `DescribeVolumes` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>size</td>
<td>The size of the volume, in GiBs</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., creating, available)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>createTime</td>
<td>Time stamp when volume creation was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td>attachmentSet</td>
<td>Specifies an attachment of a volume to an instance</td>
</tr>
<tr>
<td></td>
<td>Type: AttachmentSetItem</td>
</tr>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Ancestor: attachmentSet</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Ancestor: attachmentSet</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., attaching, attached, detaching, busy)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Ancestor: attachmentSet</td>
</tr>
<tr>
<td>attachTime</td>
<td>Time stamp when the association was created</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td></td>
<td>Ancestor: attachmentSet</td>
</tr>
<tr>
<td>availabilityZone</td>
<td>Availability zone in which the volume is located</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td></td>
<td>Ancestor: item</td>
</tr>
</tbody>
</table>
Sample Request

<DescribeVolumes xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
</DescribeVolumes>
Sample Response

<DescribeVolumesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <volumeSet>
    <item>
      <volumeId>vol-4282672b</volumeId>
      <size>800</size>
      <status>in-use</status>
      <createTime>2008-05-07T11:51:50.000Z</createTime>
      <attachmentSet>
        <item>
          <volumeId>vol-4282672b</volumeId>
          <instanceId>i-6058a509</instanceId>
          <size>800</size>
          <status>attached</status>
          <attachTime>2008-05-07T12:51:50.000Z</attachTime>
        </item>
      </attachmentSet>
    </item>
  </volumeSet>
</DescribeVolumesResponse>
Related Operations

- CreateVolume
- DeleteVolume
- AttachVolume
- DetachVolume
The `DetachVolume` operation detaches an Amazon EBS volume from an instance. For more information about Amazon EBS, see Amazon Elastic Block Store.
# Request Parameters

The following table describes the request parameters for `DetachVolume`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| `volumeId` | The ID of the Amazon EBS volume  
Type: xsd:string  
Default: none  
Valid Values: ID of a volume that you own  
Constraints: none | Yes |
| `instanceId` | The ID of the instance from which the volume will detach  
Type: xsd:string  
Default: none  
Valid Values: ID of the instance attached to the volume  
Constraints: none | No |
| `device` | The device name  
Type: xsd:string  
Default: none  
Valid Values: Valid device ID  
Constraints: none | No |
| `force` | Forces detachment if the previous detachment attempt did not occur cleanly (logging into an instance, unmounting the volume, and detaching normally).  
This option can lead to data loss or a corrupted file system. Use this option only as a last resort to detach an instance from a failed instance. The instance will not have an opportunity to flush file system caches nor file system meta data.  
If you use this option, you must perform file system check and repair procedures.  
Default: none  
Valid Values: none  
Constraints: none | No |
Response Elements

The following table describes the default response tags included in DetachVolume responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>device</td>
<td>The device as it is exposed to the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., detaching, detached)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>attachTime</td>
<td>Time stamp when detaching was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
</tbody>
</table>
Sample Request

```xml
    <volumeId>vol-4d826724</volumeId>
    <instanceId>i-6058a509</instanceId>
</detachVolume>
```
Sample Response

```xml
  <volumeId>vol-4d826724</volumeId>
  <instanceId>i-6058a509</instanceId>
  <device>/dev/sdh</device>
  <status>detaching</status>
  <attachTime>2008-05-08T11:51:50.000Z</attachTime>
</DetachVolumeResponse>
```
Related Operations

- CreateVolume
- DeleteVolume
- DescribeVolumes
- AttachVolume
DisassociateAddress

The **DisassociateAddress** operation disassociates the specified elastic IP address from the instance to which it is assigned. This is an idempotent operation. If you enter it more than once, Amazon EC2 does not return an error.
## Request Parameters

The following table describes the request parameters for `DisassociateAddress`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>publicIp</code></td>
<td>IP address that you are disassociating from the instance. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DisassociateAddress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the IP address is disassociated from the instance. Otherwise, false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

<DisassociateAddress xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
</DisassociateAddress>
Sample Response

  <return>true</return>
</DisassociateAddressResponse>
Related Operations

- AllocateAddress
- DescribeAddresses
- ReleaseAddress
- AssociateAddress
GetConsoleOutput

The GetConsoleOutput operation retrieves console output for the specified instance.

Instance console output is buffered and posted shortly after instance boot, reboot, and termination. Amazon EC2 preserves the most recent 64 KB output which will be available for at least one hour after the most recent post.
Request Parameters

The following table describes the request parameters for GetConsoleOutput. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>instanceId</td>
<td>An instance ID returned from a previous call to RunInstances. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in GetConsoleOutput responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instanceId</td>
<td>The instance ID.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>timestamp</td>
<td>The time the output was last updated.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td>output</td>
<td>The console output, Base64 encoded.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

```xml
  <instanceId>i-28a64341</instanceId>
</GetConsoleOutput>
```
  <instanceId>i-28a64341</instanceId>
  <timestamp>2007-01-03 15:00:00</timestamp>
  <output>TGludXggdmVyc2lvbiAyLjYuMTYteGVuVSAoYnVpbGRlc3ByYXRjaGJhdC5hbWY3dC4wIzI3IDChZWNobyBo
YyB2ZXJzaW9uIDQuMC4xIDIwMDYuMjIwMDIzIDQuLTUpKSAjMSBTTVAgVGh1IE9jdCAyNiAwOQDo0MTToyNiBTQV
NUIwMDYkPUY1Incm92aWRlc3NhZ2UwNnNhbCBQQU0gcm9ycmF0aW9uOiBhY3RpdmUgLSAwMDAwMDAwMDA5MDAwMD
ApQnVuZCBkZXRlY3Rpb24gZGlxYmxlIi4uIGRvbnMuCg==</output>
</GetConsoleOutputResponse>
ModifyImageAttribute

The ModifyImageAttribute operation modifies an attribute of an AMI.
Request Parameters

The following table describes the request parameters for ModifyImageAttribute. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>imageId</td>
<td>AMI ID to modify. Type: xsd:string</td>
<td>Yes</td>
</tr>
<tr>
<td>launchPermission</td>
<td>Adds or removes launch permissions for the AMI. Type: LaunchPermissionOperationType[]</td>
<td>Choice</td>
</tr>
<tr>
<td>productCodes</td>
<td>Attaches a product code to the AMI, allowing developers to charge for the use of their AMIs. Currently only one product code can be associated with an AMI. Once set, the product code cannot be changed or reset. Type: ProductCodeItemType[]</td>
<td>Choice</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in ModifyImageAttribute responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the operation succeeded, otherwise false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request - Launch Permission

<!--ModifyImageAttribute xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <imageId>ami-61a54008</imageId>
  <launchPermission>
    <add>
      <item>
        <group>all</group>
      </item>
      <item>
        <userId>495219933132</userId>
      </item>
    </add>
  </launchPermission>
</ModifyImageAttribute>
<ModifyImageAttribute xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <imageId>ami-61a54008</imageId>
  <productCodes>
    <item>
      <productCode>774F4FF8</productCode>
    </item>
  </productCodes>
</ModifyImageAttribute>
<table>
<thead>
<tr>
<th>Sample Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ModifyImageAttributeResponse xmlns=&quot;http://ec2.amazonaws.com/doc/2008-05-05&quot;&gt;</code></td>
</tr>
<tr>
<td><code>&lt;return&gt;true&lt;/return&gt;</code></td>
</tr>
<tr>
<td><code>&lt;/ModifyImageAttributeResponse&gt;</code></td>
</tr>
</tbody>
</table>
Related Operations

- ResetImageAttribute
- DescribeImageAttribute
RebootInstances

The RebootInstances operation requests a reboot of one or more instances. This operation is asynchronous; it only queues a request to reboot the specified instance(s). The operation will succeed if the instances are valid and belong to the user. Requests to reboot terminated instances are ignored.
Request Parameters

The following table describes the request parameters for RebootInstances. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>instancesSet</td>
<td>One or more instance IDs. Type: xsd:string[]</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in RebootInstances responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>true if the operation succeeded. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

<RebootInstances xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <instancesSet>
    <item>
      <instanceId>i-28a64341</instanceId>
    </item>
  </instancesSet>
</RebootInstances>
Sample Response

<RebootInstancesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <return>true</return>
</RebootInstancesResponse>
RegisterImage

The RegisterImage operation registers an AMI with Amazon EC2. Images must be registered before they can be launched. For more information, see RunInstances.

Each AMI is associated with an unique ID which is provided by the Amazon EC2 service through the RegisterImage operation. During registration, Amazon EC2 retrieves the specified image manifest from Amazon S3 and verifies that the image is owned by the user registering the image.

The image manifest is retrieved once and stored within the Amazon EC2. Any modifications to an image in Amazon S3 invalidates this registration. If you make changes to an image, deregister the previous image and register the new image. For more information, see DeregisterImage.
## Request Parameters

The following table describes the request parameters for `RegisterImage`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>imageLocation</code></td>
<td>Full path to your AMI manifest in Amazon S3 storage. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in RegisterImage responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>imageId</td>
<td>Unique ID of the newly registered machine image. Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

<RegisterImage xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <imageLocation>/mybucket/myimage.manifest.xml</imageLocation>
</RegisterImage>
Sample Response

  <imageId>ami-61a54008</imageId>
</RegisterImageResponse>
Related Operations

- DescribeImages
- DeregisterImage
ReleaseAddress

The `ReleaseAddress` operation releases an elastic IP address associated with your account.

If you run this operation on an elastic IP address that is already released, the address might be assigned to another account which will cause Amazon EC2 to return an error.

**Note**

Releasing an IP address automatically disassociates it from any instance with which it is associated. For more information, see [DisassociateAddress](#).

**Important**

After releasing an elastic IP address, it is released to the IP address pool and might no longer be available to your account. Make sure to update your DNS records and any servers or devices that communicate with the address.
Request Parameters

The following table describes the request parameters for ReleaseAddress. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>publicIp</td>
<td>IP address that you are releasing from your account. Type: xsd:string</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in ReleaseAddress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the IP address is released. Otherwise, false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

```xml
<ReleaseAddress xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
</ReleaseAddress>
```
Sample Response

```xml
  <return>true</return>
</ReleaseAddressResponse>
```
Related Operations

- Allocate Address
- Describe Addresses
- Associate Address
- Disassociate Address
ResetImageAttribute

The ResetImageAttribute operation resets an attribute of an AMI to its default value.

Note
The productCodes attribute cannot be reset.
Request Parameters

The following table describes the request parameters for ResetImageAttribute. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>imageId</td>
<td>ID of the AMI on which the attribute will be reset. Type: xsd:string</td>
<td>Yes</td>
</tr>
<tr>
<td>launchPermission</td>
<td>Resets the AMI's launch permissions. All public and explicit launch permissions for the AMI are revoked. Type: EmptyElementType</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in ResetImageAttribute responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the operation succeeded, otherwise false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

<ResetImageAttribute xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <imageId>ami-61a54008</imageId>
  <launchPermission />
</ResetImageAttribute>
Sample Response

  <return>true</return>
</ResetImageAttributeResponse>
Related Operations

- ModifyImageAttribute
- DescribeImageAttribute
RevokeSecurityGroupIngress

The RevokeSecurityGroupIngress operation revokes permissions from a security group. The permissions used to revoke must be specified using the same values used to grant the permissions.

Permissions are specified by IP protocol (TCP, UDP, or ICMP), the source of the request (by IP range or an Amazon EC2 user-group pair), the source and destination port ranges (for TCP and UDP), and the ICMP codes and types (for ICMP).

Permission changes are quickly propagated to instances within the security group. However, depending on the number of instances in the group, a small delay is might occur.
Request Parameters

The following table describes the request parameters for RevokeSecurityGroupIngress. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>userId</td>
<td>AWS Access Key ID. Type: xsd:string</td>
<td>Yes</td>
</tr>
<tr>
<td>groupName</td>
<td>Name of the group to modify. Type: xsd:string</td>
<td>Yes</td>
</tr>
<tr>
<td>ipPermissions</td>
<td>Set of permissions to remove from the group. Type: IpPermissionType[]</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in RevokeSecurityGroupIngress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if permissions successfully revoked.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

  <groupId/>
  <groupName>RangedPortsBySource</groupName>
  <ipPermissions>
    <item>
      <ipProtocol>tcp</ipProtocol>
      <fromPort>6000</fromPort>
      <toPort>7000</toPort>
      <groups/>
      <ipRanges/>
    </item>
  </ipPermissions>
</RevokeSecurityGroupIngress>
<table>
<thead>
<tr>
<th>Sample Response</th>
</tr>
</thead>
</table>
  <return>true</return>
</RevokeSecurityGroupIngressResponse>` |
Related Operations

- CreateSecurityGroup
- DescribeSecurityGroups
- AuthorizeSecurityGroupIngress
- DeleteSecurityGroup
**RunInstances**

The RunInstances operation launches a specified number of instances.

If Amazon EC2 cannot launch the minimum number AMIs you request, no instances will be launched. If there is insufficient capacity to launch the maximum number of AMIs you request, Amazon EC2 launches the minimum number specified for each AMI and allocate the remaining available instances using round robin.

In the following example, Libby generates a request to launch two images (database and web_server):

1. Libby runs the RunInstances operation to launch database instances (min. 10, max. 15) and web_server instances (min. 30, max. 40).

   Because there are currently 30 instances available and Libby needs a minimum of 40, no instances are launched.

2. Libby adjusts the number of instances she needs and runs the RunInstances operation to launch database instances (min. 5, max. 10) and web_server instances (min. 20, max. 40).

   Amazon EC2 launches the minimum number of instances for each AMI (5 database, 20 web_server).

   The remaining 5 instances are allocated using round robin.

3. Libby adjusts the number of instances she needs and runs the RunInstances operation again to launch database instances (min. 5, max. 10) and web_server instances (min. 20, max. 40).

   ![Note]

   Every instance is launched in a security group (see CreateSecurityGroup). If you do not specify a security group at launch, the instances start in your default security group.

   You can provide an optional key pair ID for each image in the launch request
(for more information, see CreateKeyPair). All instances that are created from images that use this key pair will have access to the associated public key at boot. You can use this key to provide secure access to an instance of an image on a per-instance basis. Amazon EC2 public images use this feature to provide secure access without passwords.

⚠️ **Important**

Launching public images without a key pair ID will leave them inaccessible.

The public key material is made available to the instance at boot time by placing it in the openssh_id.pub file on a logical device that is exposed to the instance as /dev/sda2 (the instance store). The format of this file is suitable for use as an entry within ~/.ssh/authorized_keys (the OpenSSH format). This can be done at boot (e.g., as part of rc.local) allowing for secure access without passwords.

Optional user data can be provided in the launch request. All instances that collectively comprise the launch request have access to this data. For more information, see Instance Metadata.

⚠️ **Note**

If any of the AMIs have a product code attached for which the user has not subscribed, the RunInstances call will fail.

⚠️ **Important**

We strongly recommend using the 2.6.18 Xen stock kernel with the c1.medium and c1.xlarge instances. Although the default Amazon EC2 kernels will work, the new kernels provide greater stability and performance for these instance types. For more information about kernels, see Kernels, RAM Disks, and Block Device Mappings.
# Request Parameters

The following table describes the request parameters for `RunInstances`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>imageId</code></td>
<td>Unique ID of a machine image, returned by a call to <code>RegisterImage</code>. Type: xsd:string</td>
<td>Yes</td>
</tr>
<tr>
<td><code>minCount</code></td>
<td>Minimum number of instances to launch. If <code>minCount</code> is more than Amazon EC2 can launch, no instances are launched at all. Type: xsd:int</td>
<td>Yes</td>
</tr>
<tr>
<td><code>maxCount</code></td>
<td>Maximum number of instances to launch. If <code>maxCount</code> is more than Amazon EC2 can launch, the largest possible number above <code>minCount</code> will be launched instead. Type: xsd:int</td>
<td>Yes</td>
</tr>
<tr>
<td><code>keyName</code></td>
<td>The name of the key pair. Type: xsd:string</td>
<td>No</td>
</tr>
<tr>
<td><code>groupSet</code></td>
<td>Description of the security groups with which to associate the instances. Type: <code>GroupSetType</code></td>
<td>Yes</td>
</tr>
<tr>
<td><code>userData</code></td>
<td>The user data available to the launched instances. Type: <code>UserDataType</code></td>
<td>No</td>
</tr>
<tr>
<td><code>instanceType</code></td>
<td>This specifies the instance type. Options include <code>m1.small</code>, <code>m1.large</code>, <code>m1.xlarge</code>, <code>c1.medium</code>, and <code>c1.xlarge</code>. The default value is <code>m1.small</code>. For more information on instance types, see <a href="#">Instance Types</a>. Type: xsd:string</td>
<td>No</td>
</tr>
<tr>
<td><code>placement</code></td>
<td>Specifies the placement constraints (availability zones) for launching the instances. To display the list of available availability zones, use the <code>DescribeAvailabilityZones</code> operation. Type: <code>PlacementRequestType</code> By default, Amazon EC2 selects an availability zone for you. For more information, see <a href="#">Availability Zones</a>.</td>
<td>No</td>
</tr>
<tr>
<td><code>kernelId</code></td>
<td>The ID of the kernel with which to launch the instance. For information on finding available kernel IDs, see <a href="http://docs.aws.amazon.com/">ec2-describe-images</a>. Example: aki-ba3adfd3</td>
<td>No</td>
</tr>
<tr>
<td><strong>ramdiskId</strong></td>
<td>The ID of the RAM disk with which to launch the instance. Some kernels require additional drivers at launch. Check the kernel requirements for information on whether you need to specify a RAM disk. To find kernel requirements, go to the <a href="#">Resource Center</a> and search for the kernel ID. Example: ari-badbad00</td>
<td>No</td>
</tr>
<tr>
<td><strong>blockDeviceMapping</strong></td>
<td>Specifies how block devices are exposed to the instance. Each mapping is made up of a <code>virtualName</code> and a <code>deviceName</code>. Virtual name example: instancestore0 Device name example: sdb Type: <code>BlockDeviceMappingItemType[]</code></td>
<td>No</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in `RunInstances` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RunInstancesResponse</td>
<td>Status information about the instances launched. Type: ReservationInfoType</td>
</tr>
</tbody>
</table>
Sample Request

```xml
<RunInstances xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <imageId>ami-60a54009</imageId>
  <minCount>1</minCount>
  <maxCount>3</maxCount>
  <keyName>example-key-name</keyName>
  <groupSet/>
  <placement>
    <availabilityZone>us-east-1b</availabilityZone>
  </placement>
  <kernelId>aki-ba3adfd3</kernelId>
  <ramdiskId>ari-badbad00</ramdiskId>
  <blockDeviceMapping>
    <item>
      <virtualName>ami</virtualName>
      <deviceName>sda1</deviceName>
    </item>
    <item>
      <virtualName>root</virtualName>
      <deviceName>/dev/sda1</deviceName>
    </item>
    <item>
      <virtualName>instancestore0</virtualName>
      <deviceName>sdb</deviceName>
    </item>
    <item>
      <virtualName>instance1</virtualName>
      <deviceName>sdc</deviceName>
    </item>
  </blockDeviceMapping>
  <userData version="1.0" encoding="base64">
    <data>VGhpcyBpcyBiYXNlIDY0IQ==</data>
  </userData>
  <addressingType>public</addressingType>
</RunInstances>
```
<RunInstancesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <reservationId>r-47a5402e</reservationId>
  <ownerId>495219933132</ownerId>
  <groupSet>
    <item>
      <groupId>default</groupId>
    </item>
  </groupSet>
  <instancesSet>
    <item>
      <instanceId>i-2ba64342</instanceId>
      <imageId>ami-60a54009</imageId>
      <instanceState>
        <code>0</code>
        <name>pending</name>
      </instanceState>
      <privateDnsName></privateDnsName>
      <dnsName></dnsName>
      <keyName>example-key-name</keyName>
      <amiLaunchIndex>0</amiLaunchIndex>
      <instanceType>m1.small</instanceType>
      <launchTime>2007-08-07T11:51:50.000Z</launchTime>
      <placement>
        <availabilityZone>us-east-1b</availabilityZone>
      </placement>
    </item>
    <item>
      <instanceId>i-2bc64242</instanceId>
      <imageId>ami-60a54009</imageId>
      <instanceState>
        <code>0</code>
        <name>pending</name>
      </instanceState>
      <privateDnsName></privateDnsName>
      <dnsName></dnsName>
      <keyName>example-key-name</keyName>
      <amiLaunchIndex>1</amiLaunchIndex>
      <instanceType>m1.small</instanceType>
      <launchTime>2007-08-07T11:51:50.000Z</launchTime>
      <placement>
        <availabilityZone>us-east-1b</availabilityZone>
      </placement>
    </item>
  </instancesSet>
</RunInstancesResponse>
<instanceId>i-2be64332</instanceId>
<imageId>ami-60a54009</imageId>
<instanceState>
  <code>0</code>
  <name>pending</name>
</instanceState>
<privateDnsName></privateDnsName>
<dnsName></dnsName>
<keyName>example-key-name</keyName>
<amiLaunchIndex>2</amiLaunchIndex>
<instanceType>m1.small</instanceType>
<launchTime>2007-08-07T11:51:50.000Z</launchTime>
<placement>
  <availabilityZone>us-east-1b</availabilityZone>
</placement>
</item>
</instancesSet>
</RunInstancesResponse>
Related Operations

- DescribeInstances
- TerminateInstances
- AuthorizeSecurityGroupIngress
- RevokeSecurityGroupIngress
- DescribeSecurityGroups
**TerminateInstances**

The `TerminateInstances` operation shuts down one or more instances. This operation is idempotent; if you terminate an instance more than once, each call will succeed.

Terminated instances will remain visible after termination (approximately one hour).
### Request Parameters

The following table describes the request parameters for `TerminateInstances`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>instancesSet</code></td>
<td>One or more instance IDs. Type: xsd:string[]</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in TerminateInstances responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instancesSet</td>
<td>A complex type describing the current and new state of each instance specified. Type: TerminateInstancesResponseInfoType[]</td>
</tr>
</tbody>
</table>
Sample Request

<TerminateInstances xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <instancesSet>
    <item>
      <instanceId>i-28a64341</instanceId>
    </item>
  </instancesSet>
</TerminateInstances>
Sample Response

<TerminateInstancesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
  <instancesSet>
    <item>
      <instanceId>i-28a64341</instanceId>
      <shutdownState>
        <code>32</code>
        <name>shutting-down</name>
      </shutdownState>
      <previousState>
        <code>16</code>
        <name>running</name>
      </previousState>
    </item>
  </instancesSet>
</TerminateInstancesResponse>
Related Operations

- DescribeInstances
Amazon EC2 Query API

The Amazon EC2 API consists of web service operations for every task the service can perform. This section describes each operation in detail.

- AllocateAddress
- AssociateAddress
- AttachVolume
- AuthorizeSecurityGroupIngress
- ConfirmProductInstance
- CreateKeyPair
- CreateSecurityGroup
- CreateSnapshot
- CreateVolume
- DeleteKeyPair
- DeleteSecurityGroup
- DeleteSnapshot
- DeleteVolume
- DeregisterImage
- DescribeAddresses
- DescribeAvailabilityZones
- DescribeImageAttribute
- DescribeImages
• DescribeInstances
• DescribeKeyPairs
• DescribeSecurityGroups
• DescribeSnapshots
• DescribeVolumes
• DetachVolume
• DisassociateAddress
• GetConsoleOutput
• ModifyImageAttribute
• RebootInstances
• RegisterImage
• ReleaseAddress
• ResetImageAttribute
• RevokeSecurityGroupIngress
• RunInstances
• TerminateInstances
Common Query Parameters
Request Parameters

All Query operations share a set of common parameters that must be present in each call:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Indicates the action to perform. Example: RunInstances</td>
<td>Yes</td>
</tr>
<tr>
<td>Version</td>
<td>The API version to use, as specified in the WSDL. Example: 2008-05-05</td>
<td>Yes</td>
</tr>
<tr>
<td>AWSAccessKeyId</td>
<td>The Access Key ID for the request sender. This identifies the account which will be charged for usage of the service. The account with which the Access Key ID is associated must be signed up for Amazon EC2, or requests will not be accepted. 10QMXFEV71ZS32XQFT2</td>
<td>Yes</td>
</tr>
<tr>
<td>Timestamp</td>
<td>The date and time at which the request is signed, in the format YYYY-MM-DDThh:mm:ssZ. For more information, go to ISO 8601.  Example: 2006-07-07T15:04:56Z. For more information, go to ISO 8601.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**ISO 8601.**

Example: 2006-07-07T15:04:56Z

Yes

**Expires**

The date and time at which the signature included in the request expires, in the format YYYY-MM-DDThh:mm:ssZ.

Example: 2006-07-07T15:04:56Z

Yes

**Signature**

A request signature is calculated as explained in Request Authentication.

Example: Qnp14Qk/7tINHzfXCiT7VbBatDA=

Yes

**SignatureVersion**

A value of 0 or 1 indicates the method chosen to construct the string to be signed. Currently, only a value of 1 is valid.

Example: 1

Yes

---

**Note**

The Timestamp parameter can be used instead of Expires. Requests must include either Timestamp or Expires, but cannot contain both.
Parameter values must be URL-encoded. This is true for any Query parameter passed to Amazon EC2 and is typically necessary in the Signature parameter. Some clients do this automatically, but this is not the norm.
List of Operations by Function

Images

- RegisterImage
- DescribeImages
- DeregisterImage

Instances

- RunInstances
- DescribeInstances
- TerminateInstances
- ConfirmProductInstance

Key Pairs

- CreateKeyPair
- DescribeKeyPairs
- DeleteKeyPair

Image Attributes

- ModifyImageAttribute
- DescribeImageAttribute
- ResetImageAttribute

Security Groups

- CreateSecurityGroup
- DescribeSecurityGroups
- DeleteSecurityGroup
- AuthorizeSecurityGroupIngress
- RevokeSecurityGroupIngress

Elastic IP Addresses

- AllocateAddress
- DescribeAddresses
- ReleaseAddress
- AssociateAddress
- DisassociateAddress

Availability Zones

- DescribeAvailabilityZones

Amazon EBS

- CreateVolume
- DescribeVolumes
- DeleteVolume
- AttachVolume
- DetachVolume
- CreateSnapshot
- DescribeSnapshots
- DeleteSnapshot
The AllocateAddress operation acquires an elastic IP address for use with your account.
Request Parameters

The AllocateAddress operation does not have any request parameters.
**Response Elements**

The following table describes the default response tags included in AllocateAddress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PublicIp</td>
<td>Returned IP address. Type: xsd:string</td>
</tr>
</tbody>
</table>
## Sample Request

```
https://ec2.amazonaws.com/
?Action=AllocateAddress
&...auth parameters...
```
Sample Response

<AllocateAddressResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
</AllocateAddressResponse>
Related Operations

- DescribeAddresses
- ReleaseAddress
- AssociateAddress
- DisassociateAddress
AssociateAddress

The AssociateAddress operation associates an elastic IP address with an instance.

If the IP address is currently assigned to another instance, the IP address is assigned to the new instance. This is an idempotent operation. If you enter it more than once, Amazon EC2 does not return an error.
Request Parameters

The following table describes the request parameters for AssociateAddress. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceId</td>
<td>The instance to which the IP address is assigned. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td>PublicIp</td>
<td>IP address that you are assigning to the instance. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in AssociateAddress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the IP address is associated with the instance. Otherwise, false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=AssociateAddress
&InstanceId=i-2ea64347
&PublicIp=67.202.55.255
&...auth parameters...
Sample Response

<AssociateAddressResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-09">
  <return>true</return>
</AssociateAddressResponse>
Related Operations

- AllocateAddress
- DescribeAddresses
- ReleaseAddress
- DisassociateAddress
AttachVolume

The AttachVolume operation attaches an Amazon EBS volume to an instance. For more information about Amazon EBS, see Amazon Elastic Block Store.
# Request Parameters

The following table describes the request parameters for AttachVolume. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| VolumeId | The ID of the Amazon EBS volume  
Type: String  
Default: none  
Valid Values: ID of a volume that you own  
Constraints: The volume and instance must be within the same availability zone | Yes      |
| InstanceId | The ID of the instance to which the volume attaches  
Type: String  
Default: none  
Valid Values: ID of an instance that you own  
Constraints: The volume and instance must be within the same availability zone | Yes      |
| Device | Specifies how the device is exposed to the instance (e.g., `/dev/sdh`). For information on standard storage locations, see [Storage Locations](#).  
Type: String  
Default: none  
Valid Values: Valid device ID  
Constraints: The specified device ID cannot be in use by another device or an instance store | Yes      |
Response Elements

The following table describes the default response tags included in AttachVolume responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>device</td>
<td>The device as it is exposed to the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., attaching, attached)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>attachTime</td>
<td>Time stamp when the attachment was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=AttachVolume
&VolumeId=vol-4d826724
&InstanceId=i-6058a509
&Device=/dev/sdh
&...auth parameters...
Sample Response

  <volumeId>vol-4d826724</volumeId>
  <instanceId>i-6058a509</instanceId>
  <device>/dev/sdh</device>
  <status>attaching</status>
  <attachTime>2008-05-07T11:51:50.000Z</attachTime>
</AttachVolumeResponse>
Related Operations

- CreateVolume
- DeleteVolume
- DescribeVolumes
- DetachVolume
AuthorizeSecurityGroupIngress

The AuthorizeSecurityGroupIngress operation adds permissions to a security group.

Permissions are specified by the IP protocol (TCP, UDP or ICMP), the source of the request (by IP range or an Amazon EC2 user-group pair), the source and destination port ranges (for TCP and UDP), and the ICMP codes and types (for ICMP). When authorizing ICMP, -1 can be used as a wildcard in the type and code fields.

Permission changes are propagated to instances within the security group as quickly as possible. However, depending on the number of instances, a small delay might occur.

When authorizing a user/group pair permission, GroupName, SourceSecurityGroupName and SourceSecurityGroupOwnerId must be specified. When authorizing a CIDR IP permission, GroupName, IpProtocol, FromPort, ToPort and CidrIp must be specified. Mixing these two types of parameters is not allowed.
# Request Parameters

The following table describes the request parameters for `AuthorizeSecurityGroupIngress`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GroupName</strong></td>
<td>Name of the group to modify. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SourceSecurityGroupName</strong></td>
<td>Name of security group to authorize access to when operating on a user/group pair. Type: String</td>
<td>When authorizing user/group pair permission.</td>
</tr>
<tr>
<td><strong>SourceSecurityGroupOwnerId</strong></td>
<td>Owner of security group to authorize access to when operating on a user/group pair. Type: String</td>
<td>When authorizing user/group pair permission.</td>
</tr>
<tr>
<td><strong>IpProtocol</strong></td>
<td>IP protocol to authorize access to when operating on a CIDR IP. Type: String</td>
<td>When authorizing CIDR IP permission.</td>
</tr>
<tr>
<td></td>
<td>Valid Values: tcp</td>
<td>udp</td>
</tr>
<tr>
<td><strong>FromPort</strong></td>
<td>Bottom of port range to authorize access to when operating on a CIDR IP. This contains the ICMP type if ICMP is being authorized. Type: Int</td>
<td>When authorizing CIDR IP permission.</td>
</tr>
<tr>
<td><strong>ToPort</strong></td>
<td>Top of port range to authorize access to when operating on a CIDR IP. This contains the ICMP code if ICMP is being authorized. Type: Int</td>
<td>When authorizing CIDR IP permission.</td>
</tr>
<tr>
<td><strong>CidrIp</strong></td>
<td>CIDR IP range to authorize access to when operating on a CIDR IP. Type: String</td>
<td>When authorizing CIDR IP permission.</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in AuthorizeSecurityGroupIngress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if permissions successfully added. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=AuthorizeSecurityGroupIngress
&IpProtocol=tcp
&FromPort=80
&ToPort=80
&CidrIp=0.0.0.0/0
&...auth parameters...
Sample Response

  <return>true</return>
</AuthorizeSecurityGroupIngressResponse>
Related Operations

- CreateSecurityGroup
- CreateSecurityGroup
- CreateSecurityGroup
- CreateSecurityGroup
ConfirmProductInstance

The ConfirmProductInstance operation returns true if the specified product code is attached to the specified instance. The operation returns false if the product code is not attached to the instance.

The ConfirmProductInstance operation can only be executed by the owner of the AMI. This feature is useful when an AMI owner is providing support and wants to verify whether a user's instance is eligible.
# Request Parameters

The following table describes the request parameters for `ConfirmProductInstance`. Parameter names are case-sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ProductCode</em></td>
<td>The product code to confirm. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td><em>InstanceId</em></td>
<td>The instance for which to confirm the product code. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## Response Elements

The following table describes the default response tags included in `ConfirmProductInstance` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td><code>true</code> if the product code is attached to the instance, <code>false</code> if it is not.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:boolean</td>
</tr>
<tr>
<td>ownerId</td>
<td>The instance owner's account ID. Only present if the product code is attached to the instance. Type: xsd:string</td>
</tr>
</tbody>
</table>

Sample Request

https://ec2.amazonaws.com/
?Action=ConfirmProductInstance
&ProductCode=774F4FF8
&InstanceId=i-10a64379
&...auth parameters...
Sample Response

  <result>true</result>
  <ownerId>254933287430</ownerId>
</ConfirmProductInstanceResponse>
Related Operations

- DescribeInstances
- RunInstances
CreateKeyPair

The CreateKeyPair operation creates a new 2048 bit RSA key pair and returns a unique ID that can be used to reference this key pair when launching new instances. For more information, see RunInstances.
# Request Parameters

The following table describes the request parameters for `CreateKeyPair`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>KeyName</code></td>
<td>A unique name for the key pair. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in CreateKeyPair responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyName</td>
<td>The key pair name provided in the original request. Type: xsd:string</td>
</tr>
<tr>
<td>KeyFingerprint</td>
<td>A SHA-1 digest of the DER encoded private key. Type: xsd:string</td>
</tr>
<tr>
<td>KeyMaterial</td>
<td>An unencrypted PEM encoded RSA private key. Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/  
?Action=CreateKeyPair  
&KeyName=example-key-name  
&...auth parameters...
<CreateKeyPairResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <keyName>example-key-name</keyName>
  <keyMaterial>-----BEGIN RSA PRIVATE KEY-----
MIIEoQIBAAKCAQBuLFg5ujHrtm1jnUtSu08Xe56LLT+HM8v/xka39EstM3/aFxTHgElqI:
HungQx929VTc8rc1bw0kdi230H5eqkMHGhvEwqa0HWASUmll4o3o/l+0f2ucPabKCOVR+j:
5AV5U2EfanIn3ZQ8lFW7Edp5a3q4DhjGLUKToHVbicL5E+g45zfb95wIyywZFeW/UUF3LpO:
ebIUIqlqTbHklLbCC2r7RTn8vpWp47BVGYGtGSMpTRP5hnbzuqj3itkiLHjU3S2sJC0:
i8BygR4s3mHKbJ8l+ePQxG1kGbF6R4ygsECmXn17MRQVXODH2ZnAgMBAAECggEAY1t:
9ICXirkYGuvFLyLflXenxfI50mDms/mumTqloH07t80iriHDR5K7wMCYY5YkVXO7mvU:
ZNUJ5s7w9gZRTf77Lyaj58kOcyajw8TsC4e4LPbFaHw51d6K8rXh64o6WqW45r8sB6Ic:
3wcfgt5ecIu4TzfoE9I/Hjn+2eRlsrbJdeOi7KiUINC/pAG23I6MzdOFEQRC5sIGC+j:
4/mciSWS4dMbrpb9FNS1cf9dcLxVM7/6KxgJNFz9XWwU77Jg8x92Zd0fVhHOux5IZC+U:
VeSKWBDq:
etE8C3p9bbU9VGyY5vLCAIb4qQKBgQDL1024GxkIswF32YtBMMuVgL5CwU9bHlo9mK:
jUE5IpRgTeye9IQiIMUTwtpgw42auSCzbeYMURPtDqyQ7p6AojMujP9EPemCVOk9xY:
x9WMC0dtV6iPckN7g0qiZXPRKanFbWADp16p8UAIVS/a5XXk5jwKBgQCKhpH2EISH1:
rhxKL:
iDCiK6JBRSVmpb8v5kWp5a101fmdR5jPAv2qvZ5jCYNPMAy1/ENDT50S1JU+0Kfm:
rdLNLDL4+TcnT7c62/aH01ohYaf/VCBrHttL/bfcG0qC7+sAc8vmKkesnF7CqCEKDyF:
dhrx:
gC01zzNAapayzi1+JcTVwEId6j9qXbBc+ZYZwMi+T0Fv/P/hwxk/ypeOxNiuCw0Ih/YtC:
DQbms7Lc1HqXiIHKYNNvXgwOw+i0ChjxvEkSdsTTfInK4V5ScVU98xDbQHjiNDJb6oar:
rBYvCh3Z7LvUH4yVpaHAOGab2Z77XVoeEO+uZ58/BGKOIGHBbHIlxTzMrhJ15HTY:
gkK+Bz4p4L9bLGDM0Bvft32XPWUtwC8FH+CsWLADZMKSsBagCzh/h1FwmdMgCMcY:
JZKjTu3u17hvx6RzdSedXEMNTZN4qI/XIK3R5ahucKyAGA+Zrvm1F0seQPlbNk7Eq:
P8TTvW/6bdP123ExxzN7K0drfclYRph1LHPmAONV/x24ALif91UB+v5ohyo1DoasL0g:
2ERKXddwz3LZ59Wq6VTdhr/5G949C72fy5WhyeRdbjnUIdHaK3M849JUfSC5so:
------END RSA PRIVATE KEY------
</keyMaterial>
</CreateKeyPairResponse>
Related Operations

- DescribeKeyPairs
- DeleteKeyPair
- RunInstances
CreateSecurityGroup

The CreateSecurityGroup operation creates a new security group.

Every instance is launched in a security group. If no security group is specified during launch, the instances are launched in the default security group. Instances within the same security group have unrestricted network access to each other. Instances will reject network access attempts from other instances in a different security group. As the owner of instances you can grant or revoke specific permissions using the AuthorizeSecurityGroupIngress and RevokeSecurityGroupIngress operations.
Request Parameters

The following table describes the request parameters for CreateSecurityGroup. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td>Name of the new security group. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td>GroupDescription</td>
<td>Description of the new security group. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in CreateSecurityGroup responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if call succeeded. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action==CreateSecurityGroup
&GroupName=WebServers
&GroupDescription=Web
&...auth parameters...
Sample Response

```
  <return>true</return>
</CreateSecurityGroupResponse>
```
Related Operations

- RunInstances
- DescribeSecurityGroups
- AuthorizeSecurityGroupIngress
- RevokeSecurityGroupIngress
- DeleteSecurityGroup
CreateSnapshot

The CreateSnapshot operation creates a snapshot of an Amazon EBS volume and stores it in Amazon S3. You can use snapshots for backups, to launch instances from identical snapshots, and to save data before shutting down an instance. For more information, see Amazon Elastic Block Store.
Request Parameters

The following table describes the request parameters for CreateSnapshot. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>VolumeId</td>
<td>The ID of the Amazon EBS volume to snapshot</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a volume that you own</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: ID of a volume that you own</td>
<td></td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in `CreateSnapshot` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshotId</td>
<td>The ID of the snapshot</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Snapshot state (e.g., pending, completed)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>startTime</td>
<td>Time stamp when the snapshot was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td>progress</td>
<td>The progress of the snapshot, in percentage</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=CreateSnapshot
&VolumeId=vol-4d826724
&...auth parameters...
Sample Response

<?xml version="1.0" encoding="UTF-8"?>
  <snapshotId>snap-78a54011</snapshotId>
  <volumeId>vol-4d826724</volumeId>
  <status>pending</status>
  <startTime>2008-05-07T12:51:50.000Z</startTime>
  <progress/>
</CreateSnapshotResponse>
Related Operations

- **DeleteSnapshot**
- **DescribeSnapshots**
CreateVolume

The CreateVolume operation creates a new Amazon EBS volume that you can mount from any Amazon EC2 instance. For more information, see Amazon Elastic Block Store.

Note
You must specify an availability zone when creating a volume. The volume and any instance to which it attaches must be in the same availability zone.
## Request Parameters

The following table describes the request parameters for `CreateVolume`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Size</strong></td>
<td>The size of the volume, in GiB.</td>
<td>Conditional</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: 1 to 1024</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Condition: Required if you are not creating a volume from a snapshot.</td>
<td></td>
</tr>
<tr>
<td><strong>SnapshotId</strong></td>
<td>The snapshot from which to create the new volume.</td>
<td>Conditional</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a snapshot that you own</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Condition: Required if you are creating a volume from a snapshot.</td>
<td></td>
</tr>
<tr>
<td><strong>AvailabilityZone</strong></td>
<td>The availability zone in which to create the new volume.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: A valid availability zone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
</tbody>
</table>
## Response Elements

The following table describes the default response tags included in `CreateVolume` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>volumeId</code></td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td><code>size</code></td>
<td>The size of the volume, in GiBs</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td><code>status</code></td>
<td>Volume state (e.g., creating, available)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td><code>createTime</code></td>
<td>Time stamp when volume creation was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td><code>availabilityZone</code></td>
<td>Availability zone in which the volume was created</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td><code>snapshotId</code></td>
<td>Snapshot from which the volume was created, if applicable</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=CreateVolume
&Size=800
&Zone=us-east-1a
&...auth parameters...
Sample Response

  <volumeId>vol-4d826724</volumeId>
  <size>800</size>
  <status>creating</status>
  <createTime>2008-05-07T11:51:50.000Z</createTime>
  <zone>us-east-1a</zone>
</CreateVolumeResponse>
Related Operations

- DeleteVolume
- DescribeVolumes
- AttachVolume
- DetachVolume
- DescribeAvailabilityZones
DeleteKeyPair

The `DeleteKeyPair` operation deletes a key pair.
Request Parameters

The following table describes the request parameters for `DeleteKeyPair`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>KeyName</strong></td>
<td>Name of the key pair to delete. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in `DeleteKeyPair` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the key was successfully deleted. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
### Sample Request

```
https://ec2.amazonaws.com/
?Action=DeleteKeyPair
&KeyName=example-key-name
&...auth parameters...
```
Sample Response

<DeleteKeyPair xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <return>true</return>
</DeleteKeyPair>
Related Operations

- CreateKeyPair
- DescribeKeyPairs
DeleteSecurityGroup

The `DeleteSecurityGroup` operation deletes a security group.

**Note**
If you attempt to delete a security group that contains instances, a fault is returned.
If you attempt to delete a security group that is referenced by another security group, a fault is returned. For example, if security group B has a rule that allows access from security group A, security group A cannot be deleted until the allow rule is removed.
Request Parameters

The following table describes the request parameters for `DeleteSecurityGroup`. Parameter names are case sensitive.

![Note]

A security group cannot be deleted if it is referenced by another security group. For example, if security group B has a rule that allows access from security group A, security group A cannot be deleted until the allow rule is removed.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>GroupName</code></td>
<td>Name of the security group to delete. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Response Elements**

The following table describes the default response tags included in DeleteSecurityGroup responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the group is deleted. Otherwise, false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/?Action=DeleteSecurityGroup&GroupName=RangedPortsBySource&...auth parameters...
Sample Response

```xml
  <return>true</return>
</DeleteSecurityGroupResponse>
```
Related Operations

- [CreateSecurityGroup](#)
- [DescribeSecurityGroups](#)
- [AuthorizeSecurityGroupIngress](#)
- [RevokeSecurityGroupIngress](#)
DeleteSnapshot

The `DeleteSnapshot` operation deletes a snapshot of an Amazon EBS volume that is stored in Amazon S3. For more information, see [Amazon Elastic Block Store](https://aws.amazon.com/elasticblockstore/).
Request Parameters

The following table describes the request parameters for DeleteSnapshot. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| SnapshotId | The ID of the Amazon EBS snapshot to delete  
Type: String  
Default: none  
Valid Values: ID of a snapshot that you own  
Constraints: none | Yes      |
Response Elements

The following table describes the default response tags included in `DeleteSnapshot` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>return</code></td>
<td>true if deletion succeeded. Type: <code>xsd:boolean</code></td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=DeleteSnapshot
&SnapshotId=snap-78a54011
&...auth parameters...
Sample Response

  <return>true</return>
</DeleteSnapshotResponse>
Related Operations

- CreateSnapshot
- DescribeSnapshots
DeleteVolume

The DeleteVolume operation deletes an Amazon EBS volume. For more information about Amazon EBS, see Amazon Elastic Block Store.
Request Parameters

The following table describes the request parameters for DeleteVolume. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>VolumeId</td>
<td>The ID of the volume to delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a volume that you own</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DeleteVolume responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if deletion succeeded.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=DeleteVolume
&VolumeId=vol-4282672b
&...auth parameters...
Sample Response

  <return>true</return>
</DeleteVolumeResponse>
Related Operations

- CreateVolume
- DescribeVolumes
- AttachVolume
- DetachVolume
DetachVolume

The DetachVolume operation detaches an Amazon EBS volume from an instance. For more information about Amazon EBS, see Amazon Elastic Block Store.
# Request Parameters

The following table describes the request parameters for `DetachVolume`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>VolumeId</td>
<td>The ID of the Amazon EBS volume</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of a volume that you own</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
<tr>
<td>InstanceId</td>
<td>The ID of the instance from which the volume will detach</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: ID of the instance attached to the volume</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
<tr>
<td>Device</td>
<td>The device name</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: Valid device ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
<tr>
<td>Force</td>
<td>Forces detachment if the previous detachment attempt did not occur cleanly</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>(logging into an instance, unmounting the volume, and detaching normally).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This option can lead to data loss or a corrupted file system. Use this option</td>
<td></td>
</tr>
<tr>
<td></td>
<td>only as a last resort to detach an instance from a failed instance. The</td>
<td></td>
</tr>
<tr>
<td></td>
<td>instance will not have an opportunity to flush file system caches nor file</td>
<td></td>
</tr>
<tr>
<td></td>
<td>system meta data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you use this option, you must perform file system check and repair</td>
<td></td>
</tr>
<tr>
<td></td>
<td>procedures.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type: Boolean</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: none</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Constraints: none</td>
<td></td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in `DetachVolume` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>device</td>
<td>The device as it is exposed to the instance</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., detaching, detached)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>attachTime</td>
<td>Time stamp when detaching was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=DetachVolume
&VolumeId=vol-4d826724
&InstanceId=i-6058a509
&...auth parameters...
Sample Response

```xml
  <volumeId>vol-4d826724</volumeId>
  <instanceId>i-6058a509</instanceId>
  <device>/dev/sdh</device>
  <status>detaching</status>
  <attachTime>2008-05-08T11:51:50.000Z</attachTime>
</DetachVolumeResponse>
```
Related Operations

- CreateVolume
- DeleteVolume
- DescribeVolumes
- AttachVolume
DeregisterImage

The DeregisterImage operation deregisters an AMI. Once deregistered, instances of the AMI can no longer be launched.
## Request Parameters

The following table describes the request parameters for DeregisterImage. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ImageId</td>
<td>Unique ID of a machine image, returned by a call to <a href="https://docs.aws.amazon.com/AmazonS3/latest/API/Welcome.html">RegisterImage</a> or <a href="https://docs.aws.amazon.com/AmazonS3/latest/API/Welcome.html">DescribeImages</a>. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DeregisterImage responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if deregistration succeeded; otherwise false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/?Action=DeregisterImage
&ImageId=ami-61a54008
&...auth parameters...
Sample Response

```xml
  <return>true</return>
</DeregisterImageResponse>
```
Related Operations

- RegisterImage
- DescribeImages
DescribeAddresses

The DescribeAddresses operation lists elastic IP addresses assigned to your account.
Request Parameters

The following table describes the request parameters for DescribeAddresses. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>PublicIp.n</td>
<td>Elastic IP addresses to describe. Type: String</td>
<td>Yes (but can be empty)</td>
</tr>
</tbody>
</table>
**Response Elements**

The following table describes the default response tags included in DescribeAddresses responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>publicIp</td>
<td>Elastic IP address assigned to your account. Type: xsd:string</td>
</tr>
<tr>
<td>instanceId</td>
<td>Instance ID to which the IP address is assigned. Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=DescribeAddresses
&PublicIp.1=67.202.55.255
&...auth parameters...
## Sample Response

```xml
<DescribeAddressesResponse xmlns="http://ec2.amazonaws.com/doc/2008-02-01">
    <addressesSet>
        <item>
            <instanceId>i-28a64341</instanceId>
        </item>
    </addressesSet>
</DescribeAddressesResponse>
```
Related Operations

- AllocateAddress
- ReleaseAddress
- AssociateAddress
- DisassociateAddress
DescribeAvailabilityZones

The `DescribeAvailabilityZones` operation describes availability zones that are currently available to the account and their states.

**Note**
Availability zones are not the same across accounts. The availability zone `us-east-1a` for account A is not necessarily the same as `us-east-1a` for account B. Zone assignments are mapped independently for each account.
**Request Parameters**

The following table describes the request parameters for DescribeAvailabilityZones. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZoneName.n</td>
<td>Name of an availability zone.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DescribeAvailabilityZones responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>availabilityZoneInfo</td>
<td>Availability zone information.</td>
</tr>
<tr>
<td></td>
<td>Type: <code>AvailabilityZoneItemType[]</code></td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=DescribeAvailabilityZones
&ZoneName.0=us-east-1a
&ZoneName.1=us-east-1b
&...auth parameters...
Sample Response

<DescribeAvailabilityZonesResponse
  xmlns="http://ec2.amazonaws.com/doc/2008-02-01/">
  <availabilityZoneInfo>
    <item>
      <zoneName>us-east-1a</zoneName>
      <zoneState>available</zoneState>
    </item>
    <item>
      <zoneName>us-east-1b</zoneName>
      <zoneState>available</zoneState>
    </item>
    <item>
      <zoneName>us-east-1c</zoneName>
      <zoneState>available</zoneState>
    </item>
  </availabilityZoneInfo>
</DescribeAvailabilityZonesResponse>
Related Operations

- RunInstances
DescribeImageAttribute

The DescribeImageAttribute operation returns information about an attribute of an AMI. Only one attribute can be specified per call.
## Request Parameters

The following table describes the request parameters for `DescribeImageAttribute`. Parameter names are case-sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ImageId</td>
<td>ID of the AMI for which an attribute will be described. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td>Attribute</td>
<td>Specifies the attribute to describe. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Valid Value: <code>launchPermission</code></td>
<td></td>
</tr>
</tbody>
</table>
## Attributes

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>launchPermission</td>
<td>The AMIs launch permissions.</td>
<td></td>
</tr>
<tr>
<td>ImageId</td>
<td>ID of the AMI for which an attribute will be described.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td>productCodes</td>
<td>The product code attached to the AMI.</td>
<td>No</td>
</tr>
<tr>
<td>kernel</td>
<td>Describes the ID of the kernel associated with the AMI.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td>ramdisk</td>
<td>Describes the ID of RAM disk associated with the AMI.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td>blockDeviceMapping</td>
<td>Defines native device names to use when exposing virtual devices.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
</tbody>
</table>
## Response Elements

The following table describes the default response tags included in `DescribeImageAttribute` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>imageId</code></td>
<td>ID of the AMI described. Type: xsd:string</td>
</tr>
<tr>
<td><code>launchPermission</code></td>
<td>Launch permissions of the AMI. Returned if <code>launchPermission</code> is specified. Type: <code>LaunchPermissionItemType[]</code></td>
</tr>
<tr>
<td><code>productCodes</code></td>
<td>Product codes of the AMI. Returned if <code>productCodes</code> is specified. Type: <code>ProductCodeItemType[]</code></td>
</tr>
<tr>
<td><code>kernel</code></td>
<td>ID of the kernel associated with the AMI. Returned if <code>kernel</code> is specified. Type: xsd:string</td>
</tr>
<tr>
<td><code>ramdisk</code></td>
<td>ID of the RAM disk associated with the AMI. Returned if <code>ramdisk</code> is specified. Type: xsd:string</td>
</tr>
<tr>
<td><code>blockDeviceMapping</code></td>
<td>Mapping that defines native device names to use when exposing virtual devices. Returned if <code>BlockDeviceMapping</code> is specified. Type: <code>BlockDeviceMappingItemType[]</code></td>
</tr>
</tbody>
</table>
Sample Request - Launch Permission

https://ec2.amazonaws.com/
?Action=DescribeImageAttribute
&ImageId=ami-61a54008
&Attribute=launchPermission
&...auth parameters...
Sample Response - Launch Permission

<DescribeImageAttributeResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
    <imageId>ami-61a54008</imageId>
    <launchPermission>
        <item>
            <group>all</group>
        </item>
        <item>
            <userId>495219933132</userId>
        </item>
    </launchPermission>
</DescribeImageAttributeResponse>
Sample Request - Product Codes

https://ec2.amazonaws.com/
?Action=DescribeImageAttribute
&ImageId=ami-61a54008
&Attribute=productCodes
&...auth parameters...
Sample Response - Product Codes

  <imageId>ami-61a54008</imageId>
  <productCodes>
    <item>
      <productCode>774F4FF8</productCode>
    </item>
  </productCodes>
</DescribeImageAttributeResponse>
Related Operations

- DescribeImages
- ModifyImageAttribute
- ResetImageAttribute
DescribeImages

The DescribeImages operation returns information about AMIs, AKIs, and ARIs available to the user. Information returned includes image type, product codes, architecture, and kernel and RAM disk IDs. Images available to the user include public images available for any user to launch, private images owned by the user making the request, and private images owned by other users for which the user has explicit launch permissions.

Launch permissions fall into three categories:

<table>
<thead>
<tr>
<th>Launch Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>public</td>
<td>The owner of the AMI granted launch permissions for the AMI to the all group. All users have launch permissions for these AMIs.</td>
</tr>
<tr>
<td>explicit</td>
<td>The owner of the AMI granted launch permissions to a specific user.</td>
</tr>
<tr>
<td>implicit</td>
<td>A user has implicit launch permissions for all AMIs he or she owns.</td>
</tr>
</tbody>
</table>

The list of AMIs returned can be modified by specifying AMI IDs, AMI owners, or users with launch permissions. If no options are specified, Amazon EC2 returns all AMIs for which the user has launch permissions.

If you specify one or more AMI IDs, only AMIs that have the specified IDs are returned. If you specify an invalid AMI ID, a fault is returned. If you specify an AMI ID for which you do not have access, it will not be included in the returned results.

If you specify one or more AMI owners, only AMIs from the specified owners and for which you have access are returned. The results can include the account IDs of the specified owners, Amazon for AMIs owned by Amazon or self for AMIs that you own.

If you specify a list of executable users, only users that have launch permissions for the AMIs are returned. You can specify account IDs (if you own the AMI(s)), self for AMIs for which you own or have explicit permissions, or all for public AMIs.
Note

Deregistered images are included in the returned results for an unspecified interval after deregistration.
Request Parameters

The following table describes the request parameters for DescribeImages. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ImageId.&lt;n&gt;</td>
<td>A list of image descriptions&lt;br&gt;Type: String</td>
<td>No</td>
</tr>
<tr>
<td>Owner.&lt;n&gt;</td>
<td>Owners of AMIs to describe.&lt;br&gt;Type: String</td>
<td>No</td>
</tr>
<tr>
<td>ExecutableBy.&lt;n&gt;</td>
<td>AMIs for which specified users have access.&lt;br&gt;Type: String</td>
<td>No</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DescribeImages responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>imagesSet</td>
<td>A list of image descriptions.</td>
</tr>
<tr>
<td></td>
<td>Type: DescribeImagesResponseItemType[]</td>
</tr>
</tbody>
</table>
**Sample Request**

```plaintext
https://ec2.amazonaws.com/?Action=DescribeImages
&ImageId.1=ami-be3adfd7
&...auth parameters...
```
Sample Response

  <imagesSet>
    <item>
      <imageId>ami-be3adfd7</imageId>
      <imageLocation>ec2-public-images/fedora-8-i386-base-v1.04.manifest.xml</imageLocation>
      <imageState>available</imageState>
      <imageOwnerId>206029621532</imageOwnerId>
      <isPublic>false</isPublic>
      <architecture>i386</architecture>
      <imageType>machine</imageType>
      <kernelId>aki-4438dd2d</kernelId>
      <ramdiskId>ari-4538dd2c</ramdiskId>
    </item>
  </imagesSet>
</DescribeImagesResponse>
Related Operations

- DescribeInstances
- DescribeImageAttribute
DescribeInstances

The DescribeInstances operation returns information about instances that you own.

If you specify one or more instance IDs, Amazon EC2 returns information for those instances. If you do not specify instance IDs, Amazon EC2 returns information for all relevant instances. If you specify an invalid instance ID, a fault is returned. If you specify an instance that you do not own, it will not be included in the returned results.

Recently terminated instances might appear in the returned results. This interval is usually less than one hour.
Request Parameters

The following table describes the request parameters for DescribeInstances. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceId.&lt;n&gt;</td>
<td>Set of instances IDs of which to get the status. Type: String</td>
<td>No</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DescribeInstances responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reservationSet</td>
<td>A list of structures describing the status of all requested instances. Type: ReservationInfoType</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=DescribeInstances
&InstanceId.1=i-28a64341
&...auth parameters...
Sample Response

<DescribeInstancesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
  <reservationSet>
    <item>
      <reservationId>r-44a5402d</reservationId>
      <ownerId>UYY3TLBUXIEON5NQVUX60MPWBZIQNFM</ownerId>
      <groupSet>
        <item>
          <groupId>default</groupId>
        </item>
      </groupSet>
      <instancesSet>
        <item>
          <instanceId>i-28a64341</instanceId>
          <imageId>ami-6ea54007</imageId>
          <instanceState>
            <code>0</code>
            <name>running</name>
          </instanceState>
          <privateDnsName>10-251-50-75.ec2.internal</privateDnsName>
          <dnsName>ec2-72-44-33-4.compute-1.amazonaws.com</dnsName>
          <keyName>example-key-name</keyName>
          <productCodesSet>
            <item><productCode>774F4FF8</productCode></item>
          </productCodesSet>
          <InstanceType>m1.small</InstanceType>
          <launchTime>2007-08-07T11:54:42.000Z</launchTime>
          <placement>
            <availabilityZone>us-east-1b</availabilityZone>
            <kernelId>aki-ba3adfd3</kernelId>
            <ramdiskId>ari-badbad00</ramdiskId>
          </placement>
        </item>
        </instancesSet>
    </item>
  </reservationSet>
</DescribeInstancesResponse>
Related Operations

- RunInstances
- TerminateInstances
**DescribeKeyPairs**

The `DescribeKeyPairs` operation returns information about key pairs available to you. If you specify key pairs, information about those key pairs is returned. Otherwise, information for all registered key pairs is returned.
Request Parameters

The following table describes the request parameters for DescribeKeyPairs. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;KeyName.r&gt;</td>
<td>Key pair IDs to describe. Type: String</td>
<td>No</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DescribeKeyPairs responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keySet</td>
<td>A list of key pair descriptions. Type: [1] DescribeKeyPairsResponseItemType]</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=DescribeKeyPairs
&KeyName.1=example-key-name
&...auth parameters...
Sample Response

<DescribeKeyPairsResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
  <keySet>
    <item>
      <keyName>example-key-name</keyName>
    </item>
  </keySet>
</DescribeKeyPairsResponse>
Related Operations

- CreateKeyPair
- DeleteKeyPair
- RunInstances
DescribeSecurityGroups

The DescribeSecurityGroups operation returns information about security groups that you own.

If you specify security group names, information about those security group is returned. Otherwise, information for all security group is returned. If you specify a group that does not exist, a fault is returned.
# Request Parameters

The following table describes the request parameters for DescribeSecurityGroups. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName.n</td>
<td>List of security groups to describe. Type: String</td>
<td>No</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in DescribeSecurityGroups responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>securityGroupInfo</td>
<td>Information about security groups. Type: SecurityGroupItemType[]</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=DescribeSecurityGroups
&GroupName.1=WebServers
&GroupName.2=RangedPortsBySource
&...auth parameters...
Sample Response

<DescribeSecurityGroupsResponse xmlns="http://ec2.amazonaws.com/doc/2008/01/security-groups/">
  <securityGroupInfo>
    <item>
      <ownerId>UYY3TLBUXIEON5NQVUX60MPWBZIQNF</ownerId>
      <groupName>WebServers</groupName>
      <groupDescription>Web</groupDescription>
      <ipPermissions>
        <item>
          <ipProtocol>tcp</ipProtocol>
          <fromPort>80</fromPort>
          <toPort>80</toPort>
        </item>
        <ipRanges/>
      </ipPermissions>
    </item>
    <item>
      <ownerId>UYY3TLBUXIEON5NQVUX60MPWBZIQNF</ownerId>
      <groupName>RangedPortsBySource</groupName>
      <groupDescription>A</groupDescription>
      <ipPermissions>
        <item>
          <ipProtocol>tcp</ipProtocol>
          <fromPort>6000</fromPort>
          <toPort>7000</toPort>
        </item>
        <ipRanges/>
      </ipPermissions>
    </item>
  </securityGroupInfo>
</DescribeSecurityGroupsResponse>
Related Operations

- CreateSecurityGroup
- AuthorizeSecurityGroupIngress
- RevokeSecurityGroupIngress
- DeleteSecurityGroup
DescribeSnapshots

The DescribeSnapshots operation describes the status of Amazon EBS snapshots. For more information about Amazon EBS, see Amazon Elastic Block Store.
Request Parameters

The following table describes the request parameters for `DescribeSnapshots`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| `SnapshotId` | The ID of the Amazon EBS snapshot  
Type: String  
Default: Describes all snapshots that you own  
Valid Values: IDs of one or more snapshots that you own  
Constraints: none | No       |
Response Elements

The following table describes the default response tags included in DescribeSnapshots responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshotId</td>
<td>The ID of the snapshot</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>status</td>
<td>Snapshot state (e.g., pending, completed)</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
<tr>
<td>startTime</td>
<td>Time stamp when the snapshot was initiated</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:dateTime</td>
</tr>
<tr>
<td>progress</td>
<td>The progress of the snapshot, in percentage</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:string</td>
</tr>
</tbody>
</table>
## Sample Request

<table>
<thead>
<tr>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://ec2.amazonaws.com/">https://ec2.amazonaws.com/</a></td>
</tr>
<tr>
<td>?Action=DescribeSnapshots</td>
</tr>
</tbody>
</table>
Sample Response

<DescribeSnapshotsResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
  <snapshotId>snap-78a54011</snapshotId>
  <volumeId>vol-4d826724</volumeId>
  <status>pending</status>
  <startTime>2008-05-07T12:51:50.000Z</startTime>
  <progress>80%</progress>
</DescribeSnapshotsResponse>
Related Operations

- CreateSnapshot
- DeleteSnapshot
DescribeVolumes

The DescribeVolumes operation lists one or more Amazon EBS volumes that you own. If you do not specify any volumes, Amazon EBS returns all volumes that you own. For more information about Amazon EBS, see Amazon Elastic Block Store.
Request Parameters

The following table describes the request parameters for DescribeVolumes. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| VolumeId.\(n\) | The ID of the volume to list  
Type: String  
Default: Describes all volumes that you own  
Valid Values: IDs of one or more volumes that you own  
Constraints: none | No       |
**Response Elements**

The following table describes the default response tags included in DescribeVolumes responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td>size</td>
<td>The size of the volume, in GiBs</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., creating, available)</td>
</tr>
<tr>
<td>createTime</td>
<td>Time stamp when volume creation was initiated</td>
</tr>
<tr>
<td>snapshotId</td>
<td>The ID of the snapshot from which the volume was created</td>
</tr>
<tr>
<td>zone</td>
<td>Availability zone in which the volume launched</td>
</tr>
<tr>
<td>attachmentSet</td>
<td>Specifies an attachment of a volume to an instance</td>
</tr>
<tr>
<td>volumeId</td>
<td>The ID of the volume</td>
</tr>
<tr>
<td>instanceId</td>
<td>The ID of the instance</td>
</tr>
<tr>
<td>device</td>
<td>The name of the device</td>
</tr>
<tr>
<td>status</td>
<td>Volume state (e.g., creating, available)</td>
</tr>
<tr>
<td>attachTime</td>
<td>Time stamp when the association was created</td>
</tr>
<tr>
<td>availabilityZone</td>
<td>Availability zone in which the volume is located</td>
</tr>
</tbody>
</table>
# Sample Request

<table>
<thead>
<tr>
<th>Sample Request</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://ec2.amazonaws.com/?Action=DescribeVolumes">https://ec2.amazonaws.com/?Action=DescribeVolumes</a> &amp;...auth parameters...</td>
</tr>
</tbody>
</table>
<DescribeVolumesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <volumeSet>
    <item>
      <volumeId>vol-4282672b</volumeId>
      <size>800</size>
      <status>in-use</status>
      <createTime>2008-05-07T11:51:50.000Z</createTime>
      <attachmentSet>
        <item>
          <volumeId>vol-4282672b</volumeId>
          <instanceId>i-6058a509</instanceId>
          <size>800</size>
          <status>attached</status>
          <attachTime>2008-05-07T12:51:50.000Z</attachTime>
        </item>
      </attachmentSet>
    </item>
  </volumeSet>
</DescribeVolumesResponse>
Related Operations

- CreateVolume
- DeleteVolume
- AttachVolume
- DetachVolume
DisassociateAddress

The `DisassociateAddress` operation disassociates the specified elastic IP address from the instance to which it is assigned. This is an idempotent operation. If you enter it more than once, Amazon EC2 does not return an error.
Request Parameters

The following table describes the request parameters for DisassociateAddress. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>PublicIp</td>
<td>IP address that you are disassociating from the instance. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in `DisassociateAddress` responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the IP address is disassociated from the instance. Otherwise, false.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:boolean</td>
</tr>
</tbody>
</table>
## Sample Request

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>DisassociateAddress</td>
</tr>
<tr>
<td>PublicIp</td>
<td>67.202.55.255</td>
</tr>
<tr>
<td>...auth parameters...</td>
<td></td>
</tr>
</tbody>
</table>
**Sample Response**

```
  <return>true</return>
</DisassociateAddressResponse>
```
Related Operations

- AllocateAddress
- DescribeAddresses
- ReleaseAddress
- AssociateAddress
GetConsoleOutput

The `GetConsoleOutput` operation retrieves console output for the specified instance.

Instance console output is buffered and posted shortly after instance boot, reboot, and termination. Amazon EC2 preserves the most recent 64 KB output which will be available for at least one hour after the most recent post.
## Request Parameters

The following table describes the request parameters for GetConsoleOutput. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceId</td>
<td>An instance ID returned from a previous call to RunInstances. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in GetConsoleOutput responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instanceId</td>
<td>The instance ID. Type: xsd:string</td>
</tr>
<tr>
<td>timestamp</td>
<td>The time the output was last updated. Type: xsd:dateTime</td>
</tr>
<tr>
<td>output</td>
<td>The console output, Base64 encoded. Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=GetConsoleOutput
&InstanceId=i-2ea64347
&...auth parameters...
  <instanceId>i-28a64341</instanceId>
  <timestamp>2007-01-03 15:00:00</timestamp>
  <output>TGludXggdmVyc2lvbiAyLjYuMTYteGVuVSAoYnVpbGRlc3BwYXRjaGJhdc5hbwYyb2ZxJzaW9uIDQuMC4xIDUwNzI3IC1hS2ZvQWQgSFQIDQuMC4xLTUpKSAjMSBTTVVTA5VhBhMbCAyNiwODo0MTY0BITZVNUwMDYKkIilSU0gbWFwOgpYZW46IDAwMDAwMDAwMDAwMDAwMDAgLSAwMDAwMDAwMDZhNDAwMDAwICh1c2FibGUpCjk4ME1C
R0hNRU0gYXZhaWxyYmxlLGo3MjdNQidMT1dKRU0gYXZhaWxyYmxlLgo3MjdNQiBMT1dKRU0gYXZhaWxyYmxlLgpOWCAoRXhlY3V0ZSBEB7YmxlKSUwcm90ZWN0aW9uOziBhY3RpdgoWKSJUJjRJIGxvY2t1cCBoZXN0b3JlLi4uIGRvbmUcCg==</output>
</GetConsoleOutputResponse>
The `ModifyImageAttribute` operation modifies an attribute of an AMI.
# Attributes

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>launchPermission</code></td>
<td>List</td>
<td>Controls who has permission to launch the AMI. Launch permissions can be granted to specific users by adding userIds. To make the AMI public, add the <code>all</code> group.</td>
</tr>
<tr>
<td><code>productCodes</code></td>
<td>List</td>
<td>Associates a product code with AMIs. This allows developers to charge users for using AMIs. The user must be signed up for the product before they can launch the AMI. This is a write once attribute; after it is set, it cannot be changed or removed.</td>
</tr>
</tbody>
</table>
# Request Parameters

The following table describes the request parameters for `ModifyImageAttribute`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ImageId</code></td>
<td>AMI ID to modify. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td><code>Attribute</code></td>
<td>Specifies the attribute to modify. See the preceding attributes table for supported attributes. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td><code>OperationType</code></td>
<td>Specifies the operation to perform on the attribute. See the preceding attributes table for supported operations for attributes. Type: String</td>
<td>Conditional</td>
</tr>
<tr>
<td><code>UserId.n</code></td>
<td>User IDs to add to or remove from the <code>launchPermission</code> attribute. Type: String</td>
<td>Conditional</td>
</tr>
<tr>
<td><code>UserGroup.n</code></td>
<td>User groups to add to or remove from the <code>launchPermission</code> attribute. Currently, the <code>all</code> group is available, which will make it a public AMI. Type: String</td>
<td>Conditional</td>
</tr>
<tr>
<td><code>ProductCode.n</code></td>
<td>Attaches a product code to the AMI. Currently only one product code can be associated with an AMI. Once set, the product code cannot be changed or reset. Type: String</td>
<td>Conditional</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in ModifyImageAttribute responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the operation succeeded, otherwise false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request - Launch Permission

https://ec2.amazonaws.com/?Action=ModifyImageAttribute
&ImageId=ami-61a54008
&Attribute=launchPermission
&OperationType=add
&Group.1=all
&UserId.1=495219933132
&...auth parameters...
Sample Request - Product Codes

https://ec2.amazonaws.com/
?Action=ModifyImageAttribute
&ImageId=ami-61a54008
&Attribute=productCodes
&ProductCode.1=774F4FF8
&...auth parameters...
Sample Response

  <return>true</return>
</ModifyImageAttributeResponse>
Related Operations

- ResetImageAttribute
- DescribeImageAttribute
RebootInstances

The RebootInstances operation requests a reboot of one or more instances. This operation is asynchronous; it only queues a request to reboot the specified instance(s). The operation will succeed if the instances are valid and belong to the user. Requests to reboot terminated instances are ignored.
Request Parameters

The following table describes the request parameters for `RebootInstance`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceId.n</td>
<td>One or more instance IDs. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in RebootInstances responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>result</td>
<td>true if the operation succeeded.</td>
</tr>
<tr>
<td></td>
<td>Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=RebootInstances
&InstanceId.1=i-2ea64347
&InstanceId.2=i-21a64348
&...auth parameters...
Sample Response

<RebootInstancesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <return>true</return>
</RebootInstancesResponse>
**ReleaseAddress**

The `ReleaseAddress` operation releases an elastic IP address associated with your account.

If you run this operation on an elastic IP address that is already released, the address might be assigned to another account which will cause Amazon EC2 to return an error.

**Note**

Releasing an IP address automatically disassociates it from any instance with which it is associated. For more information, see [DisassociateAddress](#).

**Important**

After releasing an elastic IP address, it is released to the IP address pool and might no longer be available to your account. Make sure to update your DNS records and any servers or devices that communicate with the address.
Request Parameters

The following table describes the request parameters for ReleaseAddress. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>PublicIp</td>
<td>IP address that you are releasing from your account. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in ReleaseAddress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the IP address is released. Otherwise, false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=ReleaseAddress
&PublicIp=67.202.55.255
&...auth parameters...
Sample Response

  <return>true</return>
</ReleaseAddressResponse>
Related Operations

- AllocateAddress
- DescribeAddresses
- AssociateAddress
- DisassociateAddress
RegisterImage

The `RegisterImage` operation registers an AMI with Amazon EC2. Images must be registered before they can be launched. For more information, see `RunInstances`.

Each AMI is associated with an unique ID which is provided by the Amazon EC2 service through the `RegisterImage` operation. During registration, Amazon EC2 retrieves the specified image manifest from Amazon S3 and verifies that the image is owned by the user registering the image.

The image manifest is retrieved once and stored within the Amazon EC2. Any modifications to an image in Amazon S3 invalidates this registration. If you make changes to an image, deregister the previous image and register the new image. For more information, see `DeregisterImage`. 
Request Parameters

The following table describes the request parameters for RegisterImage. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>ImageLocation</td>
<td>Full path to your AMI manifest in Amazon S3 storage. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in RegisterImage responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>imageId</td>
<td>Unique ID of the newly registered machine image. Type: xsd:string</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=RegisterImage
&ImageLocation=mybucket-myimage.manifest.xml
&...auth parameters...
Sample Response

  <imageId>ami-61a54008</imageId>
</RegisterImageResponse>
Related Operations

- DescribeImages
- DeregisterImage
ResetImageAttribute

The ResetImageAttribute operation resets an attribute of an AMI to its default value.

Note

The `productCodes` attribute cannot be reset.
**Request Parameters**

The following table describes the request parameters for `ResetImageAttribute`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ImageId</strong></td>
<td>ID of the AMI for which an attribute will be described. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Attribute</strong></td>
<td>Specifies the attribute to reset. Currently, only <code>launchPermission</code> is supported. In the case of <code>launchPermission</code>, all public and explicit launch permissions for the AMI are revoked. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in ResetImageAttribute responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if the operation succeeded, otherwise false. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/?Action=ResetImageAttribute&ImageId=ami-61a54008&Attribute=launchPermission&...auth parameters...
Sample Response

<ResetImageAttributeResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
    <return>true</return>
</ResetImageAttributeResponse>
Related Operations

- ModifyImageAttribute
- DescribeImageAttribute
**RevokeSecurityGroupIngress**

The RevokeSecurityGroupIngress operation revokes permissions from a security group. The permissions used to revoke must be specified using the same values used to grant the permissions.

Permissions are specified by IP protocol (TCP, UDP, or ICMP), the source of the request (by IP range or an Amazon EC2 user-group pair), the source and destination port ranges (for TCP and UDP), and the ICMP codes and types (for ICMP).

Permission changes are quickly propagated to instances within the security group. However, depending on the number of instances in the group, a small delay is might occur, .

When revoking a user/group pair permission, `GroupName`, `SourceSecurityGroupName` and `SourceSecurityGroupOwnerId` must be specified. When authorizing a CIDR IP permission, `GroupName`, `IpProtocol`, `FromPort`, `ToPort` and `CidrIp` must be specified. Mixing these two types of parameters is not allowed.
# Request Parameters

The following table describes the request parameters for `RevokeSecurityGroupIngress`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GroupName</strong></td>
<td>Name of the group to modify. Type: String</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SourceSecurityGroupName</strong></td>
<td>Name of security group to revoke access to when operating on a user/group pair. Type: String Condition: Required when revoking user/group pair permission.</td>
<td>Conditional</td>
</tr>
<tr>
<td><strong>SourceSecurityGroupOwnerId</strong></td>
<td>Owner of security group to revoke access to when operating on a user/group pair. Type: String Condition: Required when revoking user/group pair permission.</td>
<td>Conditional</td>
</tr>
<tr>
<td><strong>IpProtocol</strong></td>
<td>IP protocol to revoke access to when operating on a CIDR IP. Type: String Valid Values: tcp</td>
<td>udp</td>
</tr>
<tr>
<td><strong>FromPort</strong></td>
<td>Bottom of port range to revoke access to when operating on a CIDR IP. This contains the ICMP type if ICMP is being authorized. Type: Int Condition: Required when revoking CIDR IP permission.</td>
<td>Conditional</td>
</tr>
<tr>
<td><strong>ToPort</strong></td>
<td>Top of port range to revoke access to when operating on a CIDR IP. This contains the ICMP code if ICMP is being authorized. Type: Int Condition: Required when revoking CIDR IP permission.</td>
<td>Conditional</td>
</tr>
<tr>
<td><strong>CidrIp</strong></td>
<td>CIDR IP range to revoke access to when operating on a CIDR IP. Type: String Condition: Required when revoking CIDR IP permission.</td>
<td>Conditional</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in RevokeSecurityGroupIngress responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>return</td>
<td>true if permissions successfully revoked. Type: xsd:boolean</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=AuthorizeSecurityGroupIngress
&IpProtocol=tcp
&FromPort=80
&ToPort=80
&CidrIp=0.0.0.0/0
&...auth parameters...
Sample Response

```xml
   <return>true</return>
</RevokeSecurityGroupIngressResponse>
```
Related Operations

- CreateSecurityGroup
- DescribeSecurityGroups
- AuthorizeSecurityGroupIngress
- DeleteSecurityGroup
RunInstances

The RunInstances operation launches a specified number of instances.

**Note**
The Query version of RunInstances only allows instances of a single AMI to be launched in one call. This is different from the SOAP API version of the call, but similar to the `ec2-run-instances` command line tool.

If Amazon EC2 cannot launch the minimum number AMIs you request, no instances launch. If there is insufficient capacity to launch the maximum number of AMIs you request, Amazon EC2 launches as many as possible to satisfy the requested maximum values.

Every instance is launched in a security group. If you do not specify a security group at launch, the instances start in your default security group. For more information on creating security groups, see [CreateSecurityGroup](#).

An optional instance type can be specified. For information about instance types, see [Instance Types](#).

You can provide an optional key pair ID for each image in the launch request (for more information, see [CreateKeyPair](#)). All instances that are created from images that use this key pair will have access to the associated public key at boot. You can use this key to provide secure access to an instance of an image on a per-instance basis. Amazon EC2 public images use this feature to provide secure access without passwords.

**Important**
Launching public images without a key pair ID will leave them inaccessible.

The public key material is made available to the instance at boot time by placing it in the `openssh_id.pub` file on a logical device that is exposed to the instance as `/dev/sda2` (the instance store). The format of this file is suitable for use as an entry within `~/.ssh/authorized_keys` (the OpenSSH format). This can be done at boot (e.g., as part of `rc.local`) allowing for secure access without passwords.
Optional user data can be provided in the launch request. All instances that collectively comprise the launch request have access to this data. For more information, see Instance Metadata.

Note
If any of the AMIs have a product code attached for which the user has not subscribed, the RunInstances call will fail.

Important
We strongly recommend using the 2.6.18 Xen stock kernel with the c1.medium and c1.xlarge instances. Although the default Amazon EC2 kernels will work, the new kernels provide greater stability and performance for these instance types. For more information about kernels, see Kernels, RAM Disks, and Block Device Mappings.
# Request Parameters

The following table describes the request parameters for `RunInstances`. Parameter names are case sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ImageId</strong></td>
<td>ID of the AMI with which to launch instances.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td><strong>MinCount</strong></td>
<td>Minimum number of instances to launch.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: Int</td>
<td></td>
</tr>
<tr>
<td><strong>MaxCount</strong></td>
<td>Maximum number of instances to launch.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Type: Int</td>
<td></td>
</tr>
<tr>
<td><strong>KeyName</strong></td>
<td>Name of the key pair with which to launch instances.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td><strong>SecurityGroup.n</strong></td>
<td>Names of the security groups with which to associate the instances.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td><strong>UserData</strong></td>
<td>The user data available to the launched instances. This should be Base64 encoded. For more information on encoding details, see <strong>UserDataType</strong>.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Type: String</td>
<td></td>
</tr>
<tr>
<td><strong>InstanceType</strong></td>
<td>Specifies the instance type. Options include m1.small, m1.large, m1.xlarge, c1.medium, and c1.xlarge. The default value is m1.small. For more information on instance types, see <strong>Instance Types</strong>. Type: xsd:string</td>
<td>No</td>
</tr>
<tr>
<td><strong>Placement.AvailabilityZone</strong></td>
<td>Specifies the availability zone in which to launch the instance(s). To display a list of availability zones in which you can launch the instances, use the DescribeAvailabilityZones operation. For more information, see <strong>DescribeAvailabilityZones</strong>. For more information on instance types, see <strong>Availability Zones</strong>. Type: xsd:string By default, Amazon EC2 selects an availability zone for you.</td>
<td>No</td>
</tr>
<tr>
<td><strong>KernelId</strong></td>
<td>The ID of the kernel with which to launch the instance. For information on finding available kernel IDs, see <strong>ec2-</strong></td>
<td>No</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><code>RamdiskId</code></td>
<td>The ID of the RAM disk with which to launch the instance. Some kernels require additional drivers at launch. Check the kernel requirements for information on whether you need to specify a RAM disk. To find kernel requirements, go to the Resource Center and search for the kernel ID. Example: ari-badbad00</td>
<td>No</td>
</tr>
<tr>
<td><code>BlockDeviceMapping. n.VirtualName</code></td>
<td>Specifies the virtual name to map to the corresponding device name. For example: instancestore0. This parameter must be used in conjunction with <code>BlockDeviceMapping. n.DeviceName</code>.</td>
<td>No</td>
</tr>
<tr>
<td><code>BlockDeviceMapping. n.DeviceName</code></td>
<td>Specifies the device to which you are mapping a virtual name. For example: sdb. This parameter must be used in conjunction with <code>BlockDeviceMapping. n.VirtualName</code>.</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**describe-images**

Example: aki-ba3adf3
Response Elements

The following table describes the default response tags included in RunInstances responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RunInstancesResponse</td>
<td>Status information about the instances launched. Type: ReservationInfoType</td>
</tr>
</tbody>
</table>
Sample Request

https://ec2.amazonaws.com/
?Action=RunInstances
&ImageId=ami-60a54009
&MaxCount=3
&MinCount=1
&AddressingType=public
&Placement.AvailabilityZone=us-east-1b
&...auth parameters...
Sample Response

<RunInstancesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-05">
  <reservationId>r-47a5402e</reservationId>
  <ownerId>495219933132</ownerId>
  <groupSet>
    <item>
      <groupId>default</groupId>
    </item>
  </groupSet>
  <instancesSet>
    <item>
      <instanceId>i-2ba64342</instanceId>
      <imageId>ami-60a54009</imageId>
      <instanceState>
        <code>0</code>
        <name>pending</name>
      </instanceState>
      <privateDnsName></privateDnsName>
      <dnsName></dnsName>
      <keyName>example-key-name</keyName>
      <amiLaunchIndex>0</amiLaunchIndex>
      <InstanceType>m1.small</InstanceType>
      <launchTime>2007-08-07T11:51:50.000Z</launchTime>
      <placement>
        <availabilityZone>us-east-1b</availabilityZone>
      </placement>
    </item>
    <item>
      <instanceId>i-2bc64242</instanceId>
      <imageId>ami-60a54009</imageId>
      <instanceState>
        <code>0</code>
        <name>pending</name>
      </instanceState>
      <privateDnsName></privateDnsName>
      <dnsName></dnsName>
      <keyName>example-key-name</keyName>
      <amiLaunchIndex>1</amiLaunchIndex>
      <InstanceType>m1.small</InstanceType>
      <launchTime>2007-08-07T11:51:50.000Z</launchTime>
      <placement>
        <availabilityZone>us-east-1b</availabilityZone>
      </placement>
    </item>
  </instancesSet>
</RunInstancesResponse>
<instanceId>i-2be64332</instanceId>
<imageId>ami-60a54009</imageId>
<instanceState>
  <code>0</code>
  <name>pending</name>
</instanceState>
<privateDnsName></privateDnsName>
<dnsName></dnsName>
<keyName>example-key-name</keyName>
<amiLaunchIndex>2</amiLaunchIndex>
<InstanceType>m1.small</InstanceType>
<launchTime>2007-08-07T11:51:50.000Z</launchTime>
<placement>
  <availabilityZone>us-east-1b</availabilityZone>
</placement>
</item>
</instancesSet>
</RunInstancesResponse>
Related Operations

- DescribeInstances
- TerminateInstances
- AuthorizeSecurityGroupIngress
- RevokeSecurityGroupIngress
- DescribeSecurityGroups
**TerminateInstances**

The `TerminateInstances` operation shuts down one or more instances. This operation is idempotent; if you terminate an instance more than once, each call will succeed.

Terminated instances will remain visible after termination (approximately one hour).
Request Parameters

The following table describes the request parameters for TerminateInstances. Parameter names are case-sensitive.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstanceId.n</td>
<td>One or more instance IDs returned. Type: String</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Response Elements

The following table describes the default response tags included in TerminateInstances responses.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instancesSet</td>
<td>A complex type describing the current and new state of each instance specified. Type: TerminateInstancesResponseInfoType[]</td>
</tr>
</tbody>
</table>
**Sample Request**

```
https://ec2.amazonaws.com/
?Action=TerminateInstances
&InstanceId.1=i-2ea64347
&InstanceId.2=i-21a64348
&...auth parameters...
```
Sample Response

<TerminateInstancesResponse xmlns="http://ec2.amazonaws.com/doc/2008-05-01">
  <instancesSet>
    <item>
      <instanceId>i-28a64341</instanceId>
      <shutdownState>
        <code>32</code>
        <name>shutting-down</name>
      </shutdownState>
      <previousState>
        <code>16</code>
        <name>running</name>
      </previousState>
    </item>
    <item>
      <instanceId>i-21a64348</instanceId>
      <shutdownState>
        <code>32</code>
        <name>shutting-down</name>
      </shutdownState>
      <previousState>
        <code>16</code>
        <name>running</name>
      </previousState>
    </item>
  </instancesSet>
</TerminateInstancesResponse>
Related Operations

- DescribeInstances
Command Line Tools Reference

Topics

- Introduction
- Errors
- Common Options
- AMI Tools
- API Tools
Introduction

The Amazon EC2 command line tools provide a command line interface to the web service API. This section describes each tool and its command line arguments in detail.

Command line options and arguments are based on the GNU getopt conventions. Parameters are invoked using flags, which typically come in short and long form. In their short form, flags use a single character preceded by a dash. In their long form, flags use a more expressive name preceded by two dashes.

Note

Some common options apply to all command line tools. These are described in Common Options, and are not included in the description of the specific tools.
Errors

Any service errors encountered by the command line tools are passed straight through from the API. For more information about these errors, see API Error Codes.
# Common Options

Most command line tools described in this section accept the set of optional parameters described in the following table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-U URL</code></td>
<td><em>URL</em> is the uniform resource locator of the Amazon EC2 web service entry point. Default: The <code>EC2_URL</code> environment variable, or <a href="http://ec2.amazonaws.com">http://ec2.amazonaws.com</a> if the environment variable is not set. Example: <code>-U http://ec2.amazonaws.com</code></td>
</tr>
<tr>
<td><code>-K EC2-PRIVATE-KEY</code></td>
<td>The private key to use when constructing requests to Amazon EC2. Default: The value of the <code>EC2_PRIVATE_KEY</code> environment variable. Example: <code>-K pk-HKZYKTAIG2ECMXYIBH3HXV4ZBQ55CL0.pem</code></td>
</tr>
<tr>
<td><code>-C EC2-CERT</code></td>
<td>The X.509 certificate to use when constructing requests to Amazon EC2. Default: The value of the <code>EC2_CERT</code> environment variable. Example: <code>-C cert-HKZYKTAIG2ECMXYIBH3HXV4ZBQ55CL0.pem</code></td>
</tr>
<tr>
<td><code>-v</code></td>
<td>Displays verbose output by showing the SOAP request and response on the command line. This is particularly useful if you are building tools to talk directly to our SOAP API.</td>
</tr>
<tr>
<td><code>--show-empty-fields</code></td>
<td>Shows empty columns as (nil).</td>
</tr>
<tr>
<td><code>--debug</code></td>
<td>Prints internal debugging information. This is useful to assist us when troubleshooting problems.</td>
</tr>
<tr>
<td><code>-?</code></td>
<td>Displays help.</td>
</tr>
<tr>
<td><code>.</code></td>
<td>If <code>-</code> is specified as an argument to one of the parameters, a list of arguments are read from standard input. This is useful for piping the output of one command into the input of another. Example: `ec2-describe-instances</td>
</tr>
</tbody>
</table>
AMI Tools

Topics

- ec2-bundle-image
- ec2-bundle-vol
- ec2-delete-bundle
- ec2-download-bundle
- ec2-unbundle
- ec2-upload-bundle

This section describes each tool used to create AMIs and its command line arguments in detail.
ec2-bundle-image
Syntax

text

`ec2-bundle-image` -k `private_key` -c `ec2_cert` -u `user_id` -i `image_path` -r `{i386 | x86_64}` [-d `destination`] [-p `ami_prefix`] [-b, --batch] [--kernel `kernel-id`] [--ramdisk `ramdisk_id`] [--block-device-mapping `block_device_mapping`]

Description

Create a bundled AMI from an operating system image created in a loopback file. For more information, see

Creating an AMI through a Loopback File.

Note

Scripts that require a copy of the public key from the launch key pair must obtain the key from the instance's metadata (not the key file in the instance store) for instances bundled with the 2007-08-29 AMI tools and later. AMIs bundled before this release will continue to work normally.
## Options

### Note
This tool does not support the Common Options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-k, --privatekey</code></td>
<td>The path to the user's PEM-encoded RSA key file.</td>
<td>Yes</td>
</tr>
<tr>
<td><code>private_key</code></td>
<td>Example: <code>-k pk-HKZYKTAIG2ECMX43H4ZBZQ55CL0.pem</code></td>
<td></td>
</tr>
<tr>
<td><code>-c, --cert</code></td>
<td>The user's PEM encoded RSA public key certificate file.</td>
<td>Yes</td>
</tr>
<tr>
<td><code>ec2_cert</code></td>
<td>Example: <code>-c cert-HKZYKTAIG2ECMX43H4ZBZQ55CL0.pem</code></td>
<td></td>
</tr>
<tr>
<td><code>-u, --user</code></td>
<td>The user's AWS account number without dashes. Do not use the Access Key ID.</td>
<td>Yes</td>
</tr>
<tr>
<td><code>user_id</code></td>
<td>Example: <code>-u 495219933132</code></td>
<td></td>
</tr>
<tr>
<td><code>-i, --image</code></td>
<td>The path to the image to bundle.</td>
<td>Yes</td>
</tr>
<tr>
<td><code>image_path</code></td>
<td>Example: <code>-i /var/spool/my-image/version-2/debian.img</code></td>
<td></td>
</tr>
<tr>
<td><code>-r, --arch</code></td>
<td>Specifies 32-bit (m1.small) or 64-bit architecture (m1-large and m1-xlarge).</td>
<td>Yes</td>
</tr>
<tr>
<td>`{i386</td>
<td>x86_64}`</td>
<td>Default: None</td>
</tr>
<tr>
<td><code>-d, --destination</code></td>
<td>The directory in which to create the bundle.</td>
<td>No</td>
</tr>
<tr>
<td><code>destination</code></td>
<td>Default: The current directory</td>
<td></td>
</tr>
<tr>
<td><code>-p, --prefix</code></td>
<td>The filename prefix for bundled AMI files.</td>
<td>No</td>
</tr>
<tr>
<td><code>ami_prefix</code></td>
<td>Default: <code>image</code></td>
<td></td>
</tr>
<tr>
<td><code>--help</code></td>
<td>Display the help message.</td>
<td>No</td>
</tr>
<tr>
<td><code>--manual</code></td>
<td>Display the manual entry.</td>
<td>No</td>
</tr>
<tr>
<td><code>-b, --batch</code></td>
<td>Runs without interaction and suppresses all warnings.</td>
<td>No</td>
</tr>
<tr>
<td><code>--kernel</code></td>
<td>The ID of the kernel to select.</td>
<td>No</td>
</tr>
<tr>
<td><code>kernel_id</code></td>
<td>For information on finding available kernel IDs, see <code>ec2-describe-images</code>.</td>
<td></td>
</tr>
<tr>
<td><code>--ramdisk</code></td>
<td>The ID of the RAM disk to select.</td>
<td>No</td>
</tr>
<tr>
<td><code>ramdisk_id</code></td>
<td>Some kernels require additional drivers at launch. Check the kernel</td>
<td></td>
</tr>
<tr>
<td></td>
<td>requirements for information on whether you need to specify a RAM disk.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To find kernel requirements, go to the Resource Center and search for the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>kernel ID.</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| --block-device-mappings mappings | Specifies how block devices are exposed. | Virtual name example: instancestore0
Device name example: sdb |

Example: ari-badbad00

No
Output

Status messages describing the stages and status of the bundling process.
**Example**

This example creates a bundled AMI from an operating system image that was created in a loopback file.

```bash
$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXVIB3H4VZBZQ55CL0.pem -c cert-HK
Splitting bundled/fred.gz.crypt...
Created fred.part.00
Created fred.part.01
Created fred.part.02
Created fred.part.03
Created fred.part.04
Created fred.part.05
Created fred.part.06
Created fred.part.07
Created fred.part.08
Created fred.part.09
Created fred.part.10
Created fred.part.11
Created fred.part.12
Created fred.part.13
Created fred.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
Bundle Image complete.
```
Related Topics

- ec2-bundle-vol
- ec2-unbundle
- ec2-upload-bundle
- ec2-download-bundle
- ec2-delete-bundle
ec2-bundle-vol
Syntax

```
ec2-bundle-vol -k private_key -u user_id -c ec2_cert -r {i386 | x86_64} [-s size][-d destination][-e exclude_directory_1,exclude_directory_1,...] [-p ami_prefix][-v volume][-c ec2cert ami_path][-f stab fstab_path][-generate-fstab][-k kernel kernel-id][-r disk ramdisk_id][-b, --batch]
```
Description

Creates a bundled AMI by compressing, encrypting and signing a snapshot of the local machine's root file system.

✏️ Note

Scripts that require a copy of the public key from the launch key pair must obtain the key from the instance's metadata (not the key file in the instance store) for instances bundled with the 2007-08-29 AMI tools and later. AMIs bundled before this release will continue to work normally.

On a running instance, Amazon EC2 attempts to inherit product codes, kernel settings, RAM disk settings, and block device mappings with which the instance launched.
Options

**Note**

This tool does not support the

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>-k, --privatekey</td>
<td>The path to the user's PEM-encoded RSA key file.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: -k pk-HKZYKTA1G2ECMXY1B3H3HV4ZBZQ55CL0.pem</td>
<td></td>
</tr>
<tr>
<td>-c, --cert ec2_cert</td>
<td>The user's PEM encoded RSA public key certificate file.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: -c cert-HKZYKTA1G2ECMXY1B3H3HV4ZBZQ55CL0.pem</td>
<td></td>
</tr>
<tr>
<td>-u, --user user_id</td>
<td>The user's AWS account number without dashes. Do not use the Access Key ID.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: -u 495219933132</td>
<td></td>
</tr>
<tr>
<td>-r, --arch {i386</td>
<td>x86_64}</td>
<td>Specifies 32-bit (m1.small) or 64-bit architecture (m1-large and m1-xlarge).</td>
</tr>
<tr>
<td></td>
<td>Example: -r i386</td>
<td></td>
</tr>
<tr>
<td>-s, --size size</td>
<td>The size, in MB (1024 * 1024 bytes), of the image file to create. The maximum size is 10240 MB. Default: 10240</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: -s 2048</td>
<td></td>
</tr>
<tr>
<td>-d, --destination</td>
<td>The directory in which to create the bundle.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default: /tmp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: -d /var/run/my-bundle</td>
<td></td>
</tr>
<tr>
<td>-e, --exclude</td>
<td>A list of absolute directory paths to exclude from the bundle operation.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>This overrides the --all parameter. Example: -e /tmp, /home/secret-data</td>
<td></td>
</tr>
<tr>
<td>-p, --prefix ami_prefix</td>
<td>The filename prefix for bundled AMI files.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default: image</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: -p my-image-is-special</td>
<td></td>
</tr>
<tr>
<td>-v, --volume volume</td>
<td>The absolute path to the mounted volume from which to create the bundle.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default: The root directory (/)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: -v /mnt/my-customized-ami</td>
<td></td>
</tr>
<tr>
<td>-a, --all</td>
<td>Bundle all directories, including those on remotely mounted filesystems.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: -a</td>
<td></td>
</tr>
<tr>
<td>--ec2cert ami_path</td>
<td>The path to the Amazon EC2 X509 public key</td>
<td>No</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>--cert</strong> Certificate</td>
<td>Default: /etc/aes/amiutil/cert-ec2.pem Example: --ec2cert /etc/aes/amiutil/cert-ec2.pem</td>
<td>No</td>
</tr>
<tr>
<td><strong>--help</strong></td>
<td>Display the help message. Example: --help</td>
<td>No</td>
</tr>
<tr>
<td><strong>--manual</strong></td>
<td>Display the manual entry. Example: --manual</td>
<td>No</td>
</tr>
<tr>
<td><strong>--fstab fstab_path</strong></td>
<td>The path to the fstab to bundle into the image. If this is not specified, Amazon EC2 bundles /etc/fstab. Example: --fstab /etc/fstab</td>
<td>No</td>
</tr>
<tr>
<td><strong>--generate-fstab</strong></td>
<td>Causes Amazon EC2 to bundle the volume using an Amazon EC2-provided fstab. Example: --fstab /etc/fstab</td>
<td>No</td>
</tr>
<tr>
<td><strong>-b, --batch</strong></td>
<td>Runs without interaction and suppresses all warnings. Will attempt to automatically determine architecture. Example: -b</td>
<td>No</td>
</tr>
<tr>
<td><strong>--kernel kernel_id</strong></td>
<td>The ID of the kernel to select. For information on finding available kernel IDs, see ec2-describe-images. Example: aki-ba3adfd3</td>
<td>No</td>
</tr>
<tr>
<td><strong>--ramdisk ramdisk_id</strong></td>
<td>The ID of the RAM disk to select. Some kernels require additional drivers at launch. Check the kernel requirements for information on whether you need to specify a RAM disk. To find the kernel requirements, go to the Resource Center and search for the kernel ID. Example: ari-badbad00</td>
<td>No</td>
</tr>
<tr>
<td><strong>--block-device-mappings</strong></td>
<td>Specifies how block devices are exposed. Virtual name example: instancestore0 Device name example: sdb</td>
<td>No</td>
</tr>
</tbody>
</table>
Output

Status messages describing the stages and status of the bundling
**Example**

This example creates a bundled AMI by compressing, encrypting and signing a snapshot of the local machine's root file system.

```
$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CL0.pem -c c

Copying / into the image file /mnt/image.img...
Excluding:
    sys
    dev/shm
    proc
    dev/pts
    proc/sys/fs/binfmt_misc
    dev
    media
    mnt
    proc
    sys
    tmp/image.img
    mnt/img-mnt
1+0 records in
1+0 records out
mke2fs 1.38 (30-Jun-2005)
warning: 256 blocks unused.

Splitting /mnt/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
...
Created image.part.22
Created image.part.23
Generating digests for each part...
Digests generated.
Creating bundle manifest...
Bundle Volume complete.
```
Related Topics

- ec2-bundle-image
- ec2-unbundle
- ec2-upload-bundle
- ec2-download-bundle
- ec2-delete-bundle
ec2-delete-bundle
Syntax

```
ec2-delete-bundle -b s3_bucket -a access_key_id -s secret_key [-m manifest_path] [-p ami_prefix] [--url url] [--retry] [-y] [--clear]
```
**Description**

Deletes the specified bundle from Amazon S3 storage.
### Options

**Note**
This tool does not support the

**Common Options.**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>-b, --bucket</td>
<td>The name of the Amazon S3 bucket containing the bundled AMI</td>
<td>Yes</td>
</tr>
<tr>
<td>s3_bucket</td>
<td>Example: -b aes-cracker-ami-bucket</td>
<td></td>
</tr>
<tr>
<td>-a, --access-key</td>
<td>The AWS access key ID.</td>
<td>Yes</td>
</tr>
<tr>
<td>access_key_id</td>
<td>Example: -a 10QMXFEV71ZS32XQFTR2</td>
<td></td>
</tr>
<tr>
<td>-s, --secret-key</td>
<td>The AWS secret access key.</td>
<td>Yes</td>
</tr>
<tr>
<td>secret_key</td>
<td>Example: -s DMADSSfPfdaDjbK+RRUhs/aDrjsiZadgAUm8gRU2</td>
<td></td>
</tr>
<tr>
<td>-m, --manifest</td>
<td>The path to the unencrypted manifest file.</td>
<td>No</td>
</tr>
<tr>
<td>manifest_path</td>
<td>Example: -m /var/spool/my-first-bundle/Manifest</td>
<td></td>
</tr>
<tr>
<td>-p, --prefix</td>
<td>The bundled AMI filename prefix.</td>
<td>No</td>
</tr>
<tr>
<td>ami_prefix</td>
<td>Example: -p eos-</td>
<td></td>
</tr>
<tr>
<td>--url url</td>
<td>The Amazon S3 service URL.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default: <a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: --url <a href="https://s3.amazonaws.ie">https://s3.amazonaws.ie</a></td>
<td></td>
</tr>
<tr>
<td>--retry</td>
<td>Automatically retries failed uploads. Use with caution.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: --retry</td>
<td></td>
</tr>
<tr>
<td>-y, --yes</td>
<td>Automatically assumes the answer to all prompts is 'yes'.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: -y</td>
<td></td>
</tr>
<tr>
<td>--help</td>
<td>Display the help message.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: --help</td>
<td></td>
</tr>
<tr>
<td>--manual</td>
<td>Display the manual entry.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: --manual</td>
<td></td>
</tr>
<tr>
<td>--clear</td>
<td>Deletes the specified bundle from the Amazon S3 bucket and deletes the bucket, if empty.</td>
<td>No</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 displays status messages indicating the stages and status of the delete process.
Example

This example deletes a bundle from Amazon S3.

```bash
$ ec2-delete-bundle -b my-s3-bucket -a 10QMXFEV71ZS32XQFTR2 -s DMADSSfPf
Deleting files:
my-s3-bucket/fred.manifest.xml
my-s3-bucket/fred.part.00
my-s3-bucket/fred.part.01
my-s3-bucket/fred.part.02
my-s3-bucket/fred.part.03
my-s3-bucket/fred.part.04
my-s3-bucket/fred.part.05
my-s3-bucket/fred.part.06
Continue? [y/n] y
Deleted my-s3-bucket/fred.manifest.xml
Deleted my-s3-bucket/fred.part.00
Deleted my-s3-bucket/fred.part.01
Deleted my-s3-bucket/fred.part.02
Deleted my-s3-bucket/fred.part.03
Deleted my-s3-bucket/fred.part.04
Deleted my-s3-bucket/fred.part.05
Deleted my-s3-bucket/fred.part.06
ec2-delete-bundle complete.
```
Related Topics

- ec2-bundle-image
- ec2-bundle-vol
- ec2-unbundle
- ec2-upload-bundle
- ec2-download-bundle
ec2-download-bundle
Syntax

`ec2-download-bundle -b s3_bucket -m manifest -a access_key_id -s secret_key -k private_key [-p ami_prefix] [-d directory] [--url url]`
Description

Download the specified bundles from S3 storage.
Options

Note

This tool does not support the

Common Options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>b, --bucket -s3_bucket</td>
<td>The name of the Amazon S3 bucket where the bundle is located.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: -b aes-cracked</td>
<td></td>
</tr>
<tr>
<td>-m, --manifest manifest</td>
<td>The manifest path and filename.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: -m /var/spool/my-first-bundle/Manifest</td>
<td></td>
</tr>
<tr>
<td>-a, --access-key access_key_id</td>
<td>Your AWS access key ID.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: -a 10QMXFEV71ZS32XQFTR2</td>
<td></td>
</tr>
<tr>
<td>-s, --secret-key secret_key</td>
<td>Your AWS secret access key.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: -s DMADSSFpdfaDjbjk+RRUhs/aDrjsiZadgAum8gRU2</td>
<td></td>
</tr>
<tr>
<td>-k, --privatekey private_key</td>
<td>The private key used to decrypt the manifest.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: -k pk-HKZYKTAIG2ECMXYIB3HXV4ZBZQ5CL0.pem</td>
<td></td>
</tr>
<tr>
<td>-p, --prefix ami_prefix</td>
<td>The filename prefix for the bundled AMI files.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default: image</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: -p my-image</td>
<td></td>
</tr>
<tr>
<td>-d, --directory directory</td>
<td>The directory where the downloaded bundles are saved. The directory must exist.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default: The current working directory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: -d /tmp/my-downloaded-bundle</td>
<td></td>
</tr>
<tr>
<td>--url url</td>
<td>The S3 service URL.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Default: <a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: --url <a href="https://s3.amazonaws.ie">https://s3.amazonaws.ie</a></td>
<td></td>
</tr>
<tr>
<td>--help</td>
<td>Display the help message.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: --help</td>
<td></td>
</tr>
</tbody>
</table>
Output

Status messages indicating the various stages of the download process are displayed.
Example

This example downloads creates the `bundled` directory and downloads the bundle from the `my-s3-bucket` Amazon S3 bucket.

```bash
$ mkdir bundled
$ ec2-download-bundle -b my-s3-bucket -m fred.manifest.xml -a 10QMXFEV71

downloading manifest https://s3.amazonaws.com/my-s3-bucket/image.manifest.xml to bundled/image.manifest.xml...
downloading part https://s3.amazonaws.com/my-s3-bucket/image.part.00 to bundled/image.part.00...
downloading part https://s3.amazonaws.com/my-s3-bucket/image.part.01 to bundled/image.part.01...
downloading part https://s3.amazonaws.com/my-s3-bucket/image.part.02 to bundled/image.part.02...
downloading part https://s3.amazonaws.com/my-s3-bucket/image.part.03 to bundled/image.part.03...
downloading part https://s3.amazonaws.com/my-s3-bucket/image.part.04 to bundled/image.part.04...
downloading part https://s3.amazonaws.com/my-s3-bucket/image.part.05 to bundled/image.part.05...
downloading part https://s3.amazonaws.com/my-s3-bucket/image.part.06 to bundled/image.part.06...

downloaded image.part.00 from https://s3.amazonaws.com/my-s3-bucket...
downloaded image.part.01 from https://s3.amazonaws.com/my-s3-bucket...
downloaded image.part.02 from https://s3.amazonaws.com/my-s3-bucket...
downloaded image.part.03 from https://s3.amazonaws.com/my-s3-bucket...
downloaded image.part.04 from https://s3.amazonaws.com/my-s3-bucket...
downloaded image.part.05 from https://s3.amazonaws.com/my-s3-bucket...
downloaded image.part.06 from https://s3.amazonaws.com/my-s3-bucket...

download Bundle complete.
```
Related Topics

- ec2-bundle-image
- ec2-bundle-vol
- ec2-unbundle
- ec2-upload-bundle
- ec2-delete-bundle
ec2-unbundle
Syntax

```
ec2-unbundle -m manifest -k private_key [-d destination_directory] [-s source_directory]
```
Description

Recreates the AMI from the bundled AMI parts.
## Options

**Note**

This tool does not support the **Common Options**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>-m, --manifest <code>manifest</code></td>
<td>The path to the unencrypted AMI manifest file. Example: <code>-m /var/spool/my-first-bundle/Manifest</code></td>
<td>Yes</td>
</tr>
<tr>
<td>-k, --privatekey <code>private_key</code></td>
<td>The path to your PEM-encoded RSA key file. Example: <code>-k $HOME/pk-234242DEADCAFE.pem</code></td>
<td>Yes</td>
</tr>
<tr>
<td>-d, --destination <code>destination_directory</code></td>
<td>The directory in which to unbundle the AMI. The destination directory must exist. Default: The current directory Example: <code>-d /tmp/my-image</code></td>
<td>No</td>
</tr>
<tr>
<td>-s, --source <code>source_directory</code></td>
<td>The directory containing the bundled AMI parts. Default: The current directory Example: <code>-s /tmp/my-bundled-image</code></td>
<td>No</td>
</tr>
<tr>
<td>--help</td>
<td>Display the help message. Example: <code>--help</code></td>
<td>No</td>
</tr>
</tbody>
</table>
Example

This example unbundles the AMI specified in the `fred.manifest.xml` file.

```
$ mkdir unbundled
$ ec2-unbundle -m fred.manifest.xml -s bundled -d unbundled
Unbundle complete.
$ ls -l unbundled
 total 1025008
   -rw-r--r-- 1 root root 1048578048 Aug 25 23:46 fred.img
```
Output

Status messages indicating the various stages of the unbundling process are displayed.
Related Topics

- ec2-bundle-image
- ec2-bundle-vol
- ec2-upload-bundle
- ec2-download-bundle
- ec2-delete-bundle
ec2-upload-bundle
Syntax

```
```
Description

Upload a bundled AMI to Amazon S3 storage.
Options

**Note**
This tool does not support the Common Options.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>-b, --bucket s3_bucket</td>
<td>The name of the Amazon S3 bucket in which to store the bundle. If the bucket doesn't exist it will be created (if the bucket name is available). Example: -b aes-cracker-ami</td>
<td>Yes</td>
</tr>
<tr>
<td>-m, --manifest manifest</td>
<td>The path to the manifest file. The manifest file is created during the bundling process and can be found in the directory containing the bundle. Example: -m /var/spool/my-first-bundle/Manifest</td>
<td>Yes</td>
</tr>
<tr>
<td>-a, --access-key access_key_id</td>
<td>Your AWS access key ID. Example: -a 10QMXFEV71ZS32XQFTR2</td>
<td>Yes</td>
</tr>
<tr>
<td>-s, --secret-key secret_key</td>
<td>Your AWS secret access key. Example: -s DMADSSFPfdaDjbK+RRUhS/aDrjsiZadgAUm8gRU2</td>
<td>Yes</td>
</tr>
<tr>
<td>--acl acl</td>
<td>The access control list policy of the bundled image. Valid Values: public-read</td>
<td>aws-exec-read  Default: aws-exec-read</td>
</tr>
<tr>
<td>--ec2cert certificate</td>
<td>The path to the Amazon EC2 X509 public key certificate. Default: /etc/aes/amiutil/cert-ec2.pem</td>
<td>No</td>
</tr>
<tr>
<td>-d, --directory directory</td>
<td>The directory containing the bundled AMI parts. Default: The directory containing the manifest file (see the -m option). Example: -d /var/run/my-bundle</td>
<td>No</td>
</tr>
<tr>
<td>--part part</td>
<td>Starts uploading the specified part and all subsequent parts. Example: --part</td>
<td>No</td>
</tr>
<tr>
<td>--url url</td>
<td>The S3 service URL. Default: <a href="https://s3.amazonaws.com">https://s3.amazonaws.com</a></td>
<td>No</td>
</tr>
<tr>
<td>--retry</td>
<td>Automatically retries failed uploads. Use with caution. Example: --retry</td>
<td>No</td>
</tr>
<tr>
<td>--skipmanifest</td>
<td>Does not upload the manifest. Example: --skipmanifest</td>
<td>No</td>
</tr>
<tr>
<td>--help</td>
<td>Display the help message. Example: --help</td>
<td>No</td>
</tr>
</tbody>
</table>
| **--manual** | Display the manual entry.  
Example: **--manual** | No |
Output

Amazon EC2 displays status messages that indicate the stages and status of the upload process.
Example

This example uploads the bundle specified by the bundled/fred.manifest.xml manifest.

```
s ec2-upload-bundle -b my-s3-bucket -m bundled/fred.manifest.xml -a 10QMF
Encrypting bundle manifest...  
Completed encryption.  
Uploading encrypted manifest... 
Uploaded encrypted manifest to http://s3.amazonaws.com:80/alpowell-images/fred.manifest.xml
Uploading bundled AMI parts to http://s3.amazonaws.com:80/alpowell-images...  
Uploaded fred.part.00 to http://s3.amazonaws.com:80/alpowell-images/fred.part.00.  
Uploaded fred.part.01 to http://s3.amazonaws.com:80/alpowell-images/fred.part.01.  
Uploaded fred.part.03 to http://s3.amazonaws.com:80/alpowell-images/fred.part.03.  
Uploaded fred.part.05 to http://s3.amazonaws.com:80/alpowell-images/fred.part.05.  
Uploaded fred.part.06 to http://s3.amazonaws.com:80/alpowell-images/fred.part.06.  
Uploaded fred.part.08 to http://s3.amazonaws.com:80/alpowell-images/fred.part.08.  
Upload Bundle complete.
```
Related Topics

- ec2-bundle-image
- ec2-bundle-vol
- ec2-unbundle
- ec2-download-bundle
- ec2-delete-bundle
API Tools

Topics

- List of Operations by Function
  - ec2-add-group
  - ec2-add-keypair
  - ec2_allocate-address
  - ec2_associate-address
  - ec2_attach-volume
  - ec2_authorize
  - ec2_confirm-product-instance
  - ec2_create-snapshot
  - ec2_create-volume
  - ec2_delete-group
  - ec2_delete-keypair
  - ec2_delete-snapshot
  - ec2_delete-volume
  - ec2_deregister
  - ec2_describe-addresses
  - ec2_disassociate-address
  - ec2_describe-availability-zones
  - ec2_describe-group
  - ec2_describe-image-attribute
  - ec2_describe-images
  - ec2_describe-instances
  - ec2_describe-keypairs
  - ec2_detach-volume
  - ec2_describesnapshots
  - ec2_describe-volumes
  - ec2_fingerprint-key
  - ec2_get-console-output
  - ec2_modify-image-attribute
  - ec2_reboot-instances
  - ec2_release-address
  - ec2_register
- `ec2-reset-image-attribute`
- `ec2-revoke`
- `ec2-run-instances`
- `ec2-terminate-instances`

This section describes each API tool and its command line arguments in detail.
List of Operations by Function

Images

- ec2-register
- ec2-deregister
- ec2-describe-images

Instances

- ec2-run-instances
- ec2-describe-instances
- ec2-terminate-instances
- ec2-confirm-product-instance

Key Pairs

- ec2-add-keypair
- ec2-describe-keypairs
- ec2-delete-keypair
- ec2-fingerprint-key

Image Attributes

- ec2-modify-image-attribute
- ec2-describe-image-attribute
- ec2-reset-image-attribute
Security Groups

- **ec2-add-group**
- **ec2-delete-group**
- **ec2-describe-group**
- **ec2-authorize**
- **ec2-revoke**

Elastic IP Addresses

- **ec2-allocate-address**
- **ec2-describe-addresses**
- **ec2-release-address**
- **ec2-associate-address**
- **ec2-disassociate-address**

Availability Zones

- **ec2-describe-availability-zones**

Amazon EBS

- **ec2-create-volume**
- **ec2-describe-volumes**
- **ec2-delete-volume**
- **ec2-attach-volume**
- **ec2-detach-volume**
- **ec2-create-snapshot**
- **ec2-describe-snapshots**
- **ec2-delete-snapshot**
ec2-add-group
Syntax

`ec2-add-group group -d description`
Description

Creates a new security group. Group names must be unique per account.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Name of the security group. Example: web servers</td>
<td>Yes</td>
</tr>
<tr>
<td>-d description</td>
<td>Description of the group. This is informational only. If the description contains spaces, you must enclose it in single quotes ('). Example: -d 'web servers'</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("GROUP")
- Group name
- Group description

Amazon EC2 displays errors on stderr.
Example

This example creates the `websrv` security group.

```
$ ec2-add-group websrv -d 'Web servers'
GROUP websrv Web servers
```
Related Topics

- CreateSecurityGroup
- ec2-describe-group
- ec2-delete-group
- ec2-authorize
- ec2-revoke
ec2-add-keypair
Syntax

d2-add-keypair \textit{key}
Description

Creates a new 2048 bit RSA key pair with the specified name. The public key is stored by Amazon EC2 and the private key is displayed on the console. The private key is returned as an unencrypted PEM encoded PKCS#8 private key. If a key with the specified name already exists, Amazon EC2 returns an error.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>Name of the key pair. Example: mysecretkey</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("KEYPAIR")
- Key pair name
- Private key fingerprint
- Private key. This value is displayed on a new line.

Amazon EC2 displays errors on stderr.
Example

This example creates a key pair named gsg-keypair.

```
$ ec2-add-keypair gsg-keypair
d-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQBuLFg5ujHrtm1jnutSuo08Xe56L1t+HM0v/xkaa39EstM3/aFxTHgElqiJLChp
HungXQ29V7c8rciBw01kd213OH5eqkMHGhEwqaoHWASUM1403o/IX+0f2ucpKCOVUR+jx71Sg
5AU52EqfanIn3Q81lf7Edp5a3q04hj61UKToHvB1cL5E+e45z9B95wiyyWZFeuw/UUF3plG2ygq
ee1ulqrTbHkLbC2r7R7n8vPQwp47QoVY6tgSGBQpTRP5hnbbzqj3tikILHjU39S2sJcJ3TrJ3x
i8ByqR43smHkBj81+ePQx61kGBF6R4yg6sECmXn17MRQVXODNHZBaGMBAAEcgEAYtsiUsIwD15
91CXiKyGvFylfLIFxenxfsISmDFms/mumTqIoH07tr8or1HDRSK7wMcy/YY5YkcxN07mVUVDipm
ZNUIs7rw9Qz2RTr7Lyla1S5khcya2wts0e4LpBh4w51d6K8rXh6406WXP45RsB6ICm1k6Q17
3wcigTesJcu47ZfoE9Hjr+2eR1rslrjBde0Ri7kUINC/pAG23I6MdDOFE9c86sCigCj4++4/mciUSA
WS4sdMbrrpb9FNSIScf9dcLxVM7/6XkgJNfZc9XwzuW7773g8x92Zd0fVhH0uxSIZC+UvSKWb4ydfcI
TeB3C3p9bU9GVyY5vLCAiB4qKQBgQDLi024GXrIKswF32ytBBMuVgLGwvU9h9H109mkAc2m8c1m
jUE5IpzRJted9lIqiZUMTgtwnq2auSCzbUeYMURPtDqyQ7p6AJMujp9PEpcmSVOK9xyL0PcO
xW9MCodtv6IPcN7g0iqizXPRKafbWAdp16P8UAIs/v5XXS5jwKBqCCkphIzEISh1uRhx1jyWC
iDCIk6JRsMvplbc0V5dKwP5a10fmdR5Pa2vqzS5jCNyPn2a1/EDNTY5OISJU+0KfKmyhsbmn
rdLNL4L+TcnT7C62/ahH0ikoYaf/VCBRhL1BfgoQ0C7+sAc8vKkesnF7CqCEKDYf/dhrxYdKB
qCG1zzZNaapayz1+JcTVwEid6j9jQXbM+XXyWHi+tOFv/P/hwky/epeX01ucw0Ih/YtGBVAC
Qbqsz7Lyc1hXqix1HkYWrvNxQwgr0+oi1chjxyEksDSTTfnK4VSCVU9BDbQHdjidNDbL60ar92UN7V
rBByChZJF7LvUH4YmpvHApAgAbZ2X7vvoEo+uZ58/BGKOIGHByHBD1XtMhdJR15HTYjjK70gTzm
gK+8zp4L9ibvLDmJ08vf32wPEWvU18twCZFH+SsWLQADZMKSsB50Z/h1FwhMdMgMCYq+Qld4
JZKjTsu317vVx6RzdSed1XMTN2W4q1L1x3K5aHucKcgya9T+Zrvm10fseQPbLknn7EqhX1lJxAT
BPTTWv/6dPp23ExzzJ0Kdrtfc1YRhph1LMPA01Nv/x2xALIf91UB+v50hylIoDoasL6gij1houRe
2E1Kkdwh2E2L9Swq6FTdhr/5S994CK72fy5WhatsRbdjUIdhaK3Mb49JJu6cSrvSb4g==
-----END RSA PRIVATE KEY-----
Related Topics

- CreateKeyPair
- `ec2-describe-keypairs`
- `ec2-delete-keypair`
ec2-allocate-address
Syntax

c2-allocate-address
Description

Acquires an elastic IP address for use with your account.
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("ADDRESS")
- Elastic IP address for use with your account

Amazon EC2 displays errors on stderr.
Example

This example returns an elastic IP address for use with the account.

$ ec2-allocate-address
ADDRESS 67.262.55.255
Related Topics

- ec2-describe-addresses
- ec2-release-address
- ec2-associate-address
- ec2-disassociate-address
ec2-associate-address
Syntax

d2-associate-address -i instance_id ip_address
Description

Associates an elastic IP address with an instance. If the IP address is currently assigned to another instance, the IP address is assigned to the new instance. This is an idempotent operation. If you enter it more than once, Amazon EC2 does not return an error.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance_id</td>
<td>The instance to which the IP address is assigned. Example: i-43a4412a</td>
<td>Yes</td>
</tr>
<tr>
<td>ip_address</td>
<td>The IP address that you are assigning to the instance. Example: 67.202.55.255</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("ADDRESS")
- Elastic IP address that you are assigning to the instance
- Instance to which the IP address is assigned

Amazon EC2 displays errors on stderr.
Example

This example assigns the 67.202.55.255 IP address to the i-43a4412a instance.

```
$ ec2-associate-address -i i-43a4412a 67.202.55.255
 ADDRESS 67.202.55.255  i-43a4412a
```
Related Topics

- ec2-allocate-address
- ec2-describe-addresses
- ec2-release-address
- ec2-disassociate-address
ec2-attach-volume
Syntax

**ec2-attach-volume** *volume_id* --instance *instance_id* --device *device*
Description

Attaches an Amazon EBS volume to an instance and exposes it as the specified device.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>volume_id</td>
<td>The ID of the Amazon EBS volume&lt;br&gt;Example: vol-4d826724</td>
<td>Yes</td>
</tr>
<tr>
<td>--instance_instance_id</td>
<td>The ID of the instance to which the volume will attach Volumes can only attach to instances in the same availability zone.&lt;br&gt;Example: i-6058a509</td>
<td>Yes</td>
</tr>
<tr>
<td>--device_device</td>
<td>Specifies how the device is exposed to the instance. This value is operating system dependent.&lt;br&gt;Example: /dev/sdh (Linux)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EBS returns a table that contains the following information:

- ATTACHMENT identifier
- ID of the volume
- ID of the instance
- The device as it is exposed to the instance
- Volume state (e.g., attaching, attached)
- Time stamp when attachment initiated

Amazon EBS displays errors on stderr.
Example

This example attaches volume vol-4d826724 to instance i-6058a509 and exposes it as /dev/sdh. For information on standard storage locations, see Storage Locations.

```bash
$ ec2-attach-volume vol-4d826724 --instance i-6058a509 --device /dev/SDH
ATTACHMENT vol-4d826724 i-6058a509 /dev/SDH attaching 2008-02-14T00:15:00+0000
```
Related Topics

- ec2-create-volume
- ec2-delete-volume
- ec2-describe-volumes
- ec2-detach-volume
ec2-authorize
Syntax

ec2-authorize group [-P protocol] (-p port_range | -t icmp_type_code) [-u source_group_user ...] [-o source_group ...] [-s source_subnet ...]
Description

Adds a rule to the specified security group. If no source host, group or subnet is provided, requests from any source address will be honored.
# Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>The group to which this rule will apply.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: webservers</td>
<td></td>
</tr>
<tr>
<td>-P protocol</td>
<td>The protocol to allow.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Condition: Applies when specifying a CIDR subnet as the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Valid Values: tcp</td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>Example: -P tcp</td>
<td></td>
</tr>
<tr>
<td>-p port_range</td>
<td>For the TCP or UDP protocols, this specifies the range of ports to allow.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>You specify a single integer or a range (min-max).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Condition: Applies when specifying a CIDR subnet as the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: -p 80</td>
<td></td>
</tr>
<tr>
<td>-t icmp_type_code</td>
<td>For the ICMP protocol, the ICMP type and code must be specified.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>This must be specified in the format type:code where both are integers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Type, code, or both can be specified as -1, which is a wildcard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Condition: Applies when specifying a CIDR subnet as the source.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: -t 2:5</td>
<td></td>
</tr>
<tr>
<td>-u source_group_user</td>
<td>The owner of a group specified using -o. If this is not specified, all groups will refer to the current user. If specified more than once, there must be exactly one -u per -o and each user will be mapped to the corresponding group.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: -u 495219933132</td>
<td></td>
</tr>
<tr>
<td>-o source_group</td>
<td>The network source from which traffic will be authorized specified as a security Group. See the description of the -u option for group owner information.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: -o headoffice</td>
<td></td>
</tr>
<tr>
<td>-s source_subnet</td>
<td>The network source from which traffic is to be authorized specified as a CIDR subnet range.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: -s 205.192.8.45/24</td>
<td></td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("GROUP", "PERMISSION")
- Group name. Currently, this will report an empty string
- Type of rule. Currently, only ALLOW rules are supported
- Protocol to allow
- Start of port range
- End of port range
  - FROM
  - Source

Amazon EC2 displays errors on stderr.
Example

This example grants TCP port 80 access from the 205.192.0.0/16 address range to the `websrv` security group.

```
$ ec2-authorize websrv -P tcp -p 80 -s 205.192.0.0/16
GROUP websrv ""
PERMISSION websrv ALLOWS tcp 80 80 FROM CIDR 205.192.0.0/16
```
Related Topics

- AuthorizeSecurityGroupIngress
- ec2-add-group
- ec2-describe-group
- ec2-delete-group
- ec2-revoke
ec2-confirm-product-instance
Syntax

`ec2-confirm-product-instance product_code -i instance_id`
Description

Returns a boolean indicating whether the specified product code is attached to the specified instance. If it is attached, it returns true. Otherwise, it returns false.

This command can only be executed by the AMI owner. This is useful when an AMI owner is providing support and wants to verify whether a user's instance is eligible.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance_id</td>
<td>Instance identifier that was generated when the instance launched. Example: i-10a64379</td>
<td>Yes</td>
</tr>
<tr>
<td>product_code</td>
<td>The product code. Example: 774F4FF8</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Product code.
- Instance ID.
- Boolean indicating if the product code is attached to the instance.
- The instance owner's account ID (if the product code is attached).

Amazon EC2 displays errors on stderr.
Example

This example confirms whether the 774F4FF8 product code is attached to the i-10a64379 instance.

```
$ ec2-confirm-product-instance 774F4FF8 -i i-10a64379
774F4FF8 i-10a64379 true
```
Related Topics

- DescribeInstances
- ec2-modify-image-attribute
ec2-create-snapshot
Syntax

e2-create-snapshot \textit{volume_id}
Description

Creates a snapshot of the current state of an Amazon EBS volume and stores it in Amazon S3. You can use snapshots for backups, to make identical copies of instance devices, and to save data before shutting down an instance.

When taking a snapshot of a file system, we recommend unmounting it first. This ensures the file system metadata is in a consistent state, that the 'mounted indicator' is cleared, and that all applications using that file system are stopped and in a consistent state. Some file systems, such as xfs, can freeze and unfreeze activity so a snapshot can be made without unmounting.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>$volume_{id}$</td>
<td>The ID of the volume to snapshot. Example: vol-4d826724</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Output**

Amazon EBS returns a table that contains the following information:

- SNAPSHOT identifier
- ID of the snapshot
- ID of the volume
- Snapshot state (e.g., pending, completed)
- Time stamp when the snapshot was initiated

Amazon EBS displays errors on stderr.
Example

This example creates a snapshot of volume `vol-4d826724`.

```
$ ec2-create-snapshot vol-4d826724
SNAPSHOT snap-78a54011 vol-4d826724 pending 2008-02-15T09:58+0000
```
Related Topics

- ec2-delete-snapshot
- ec2-describe-snapshots
ec2-create-volume
Syntax

`ec2-create-volume [--size `size` | --snapshot `snapshot`] --availability-zone `zone``
Description

Creates an Amazon EBS volume of a size you specify or from a snapshot.

Note
You must specify an availability zone when creating a volume. The volume and the instance to which it attaches must be in the same availability zone.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>--size size</td>
<td>The size of the Amazon EBS volume, in GiB. Required if you are not creating a volume from a snapshot. Example: 800</td>
<td>Conditional</td>
</tr>
<tr>
<td>--snapshot snapshot</td>
<td>The snapshot from which to create the new volume. Required if you do not specify a volume size. Example: snap-78a54011</td>
<td>Conditional</td>
</tr>
<tr>
<td>--availability-zone zone</td>
<td>The availability zone in which to create the new volume. Example: us-east-1a</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EBS returns a table that contains the following information:

- VOLUME identifier
- ID of the volume
- Size of the volume, in GiBs
- Snapshot from which the volume was created, if applicable
- Availability zone in which the volume was created
- Volume state (e.g., creating, available)
- Time stamp when volume creation was initiated

Amazon EBS displays errors on stderr.
Example

This example creates a new 800 GiB volume in availability zone `us-east-1a`.

```
$ ec2-create-volume --size 800 --availability-zone us-east-1a
VOLUME vol-4d826724 800 us-east-1a creating 2008-02-14T00:00:00+0000
```
Related Topics

- ec2-delete-volume
- ec2-describe-volumes
- ec2-attach-volume
- ec2-detach-volume
- ec2-describe-availability-zones
ec2-delete-group
Syntax

`ec2-delete-group group`
Description

Deletes the specified security group.

⚠️ Note
If you attempt to delete a security group that contains instances, a fault is returned.
If you attempt to delete a security group that is referenced by another security group, a fault is returned. For example, if security group B has a rule that allows access from security group A, security group A cannot be deleted until the allow rule is removed.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Name of the security group. Example: webservers</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("GROUP")
- Name of the deleted security group

Amazon EC2 displays errors on stderr.
Example

This command deletes the `websrv` security group.

```bash
$ ec2-delete-group websrv
GROUP websrv
```
Related Topics

- DeleteSecurityGroup
- ec2-add-group
- ec2-describe-group
- ec2-authorize
- ec2-revoke
ec2-delete-keypair
Syntax

ec2-delete-keypair *key_pair*
Description

Deletes the specified key pair, by removing the public key from Amazon EC2
# Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>key_pair</code></td>
<td>Name of the key pair. Example: <code>primary_keypair</code></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("KEYPAIR")
- Name of the deleted key pair
- Private key fingerprint

Amazon EC2 displays errors on stderr.
Example

This example deletes the *gsg-keypair* key pair.

```bash
$ ec2-delete-keypair gsg-keypair
```
Related Topics

- DeleteKeyPair
- ec2-add-keypair
- ec2-describe-keypairs
ec2-delete-snapshot
Syntax

e2-delete-snapshot snapshot_id
Description

Deletes an Amazon EBS snapshot.
Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshot_id</td>
<td>The ID of the snapshot to delete. Example: snap-78a54011</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EBS returns a table that contains the following information:

- SNAPSHOT identifier
- ID of the snapshot

Amazon EBS displays errors on stderr.
Example

This example deletes snapshot snap-78a54011.

```bash
$ ec2-delete-snapshot snap-78a54011
SNAPSHOT snap-78a54011
```
Related Topics

- ec2-create-snapshot
- ec2-describe-snapshots
ec2-delete-volume
Syntax

`ec2-delete-volume volume_id`
Description

Deletes the specified Amazon EBS volume.
Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>volume_id</td>
<td>The ID of the Amazon EBS volume to delete.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Note**

The volume remains in the deleting state for several minutes after entering this command.

Example: `vol-4282672b`
Output

Amazon EBS returns a table that contains the following information:

- VOLUME identifier
- ID of the volume you deleted

Amazon EBS displays errors on stderr.
Example

This example deletes volume `vol-4282672b`.

```
$ ec2-delete-volume vol-4282672b
VOLUME vol-4282672b
```
Related Topics

- ec2-create-volume
- ec2-describe-volumes
- ec2-attach-volume
- ec2-detach-volume
ec2-deregister
Syntax

`ec2-deregister ami_id`
Description

Deregisters the specified AMI. Once deregistered, the AMI cannot be used to launch new instances.

Note
This command does not delete the AMI from Amazon S3.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ami_id</code></td>
<td>AMI identifier. Example: <code>ami-4fa54026</code></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- A record type identifier ("IMAGE")
- The image identifier that was deregistered

Amazon EC2 displays errors on stderr.
Example

This example deregisters the *ami-4fa54026* AMI.

```
$ ec2-deregister ami-4fa54026
IMAGE ami-4fa54026
```
Related Topics

- DeregisterImage
- ec2-register
- ec2-describe-images
ec2-describe-addresses
Syntax

```bash
c2-describe-addresses [public_ip ...]
```
**Description**

Lists elastic IP addresses assigned to your account.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
</table>
| **public_ip** | Elastic IP addresses to describe
Example: 67.202.55.255 | No       |
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("ADDRESS")
- Elastic IP address assigned to your account
- Instance ID to which the IP address is assigned

Amazon EC2 displays errors on stderr.
Example

This example returns elastic IP addresses assigned to the account.

```
$ ec2-describe-addresses
```

Amazon EC2 returns 67.202.55.255 which is assigned to instance i-f15ebb98 and 67.202.55.233 which is not assigned to an instance.
Related Topics

- ec2-allocate-address
- ec2-release-address
- ec2-associate-address
- ec2-disassociate-address
ec2-disassociate-address
Syntax

e2c-disassociate-address \textit{ip\_address}
Description

Disassociates the specified elastic IP address from the instance to which it is assigned. This is an idempotent operation. If you enter it more than once, Amazon EC2 does not return an error.
Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ip_address</em></td>
<td>The IP address that you are disassociating from the instance. Example: 67.202.55.255</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("ADDRESS")
- Elastic IP address you are disassociating from the instance

Amazon EC2 displays errors on stderr.
Example

This example disassociates the 67.202.55.255 IP address from the instance to which it is assigned.

```
$ ec2-disassociate-address 67.202.55.255
ADDRESS 67.202.55.255
```
Related Topics

- ec2-allocate-address
- ec2-describe-addresses
- ec2-release-address
- ec2-associate-address
ec2-describe-availability-zones
Syntax

ec2-describe-availability-zones [zone-name...]

Description

Describes availability zones that are currently available to the account and their states.

**Note**
Availability zones are not the same across accounts. The availability zone us-east-1a for account A is not necessarily the same as us-east-1a for account B. Zone assignments are mapped independently for each account.
### Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>zone-name</td>
<td>Name of an availability zone.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: <code>us-east-1a</code></td>
<td></td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("AVAILABILITYZONE")
- Availability zone name
- State

Amazon EC2 displays errors on stderr.
Example

This example displays the availability zones that are available to the account.

```plaintext
$ ec2-describe-availability-zones
  AVAILABILITYZONE           us-east-1a   available
  AVAILABILITYZONE           us-east-1b   available
  AVAILABILITYZONE           us-east-1c   available
```
Related Topics

ec2-run-instances
ec2-describe-group
Syntax

ec2-describe-group [group ...]
Description

Describes the current state of each specified security group. If no security groups are explicitly listed, Amazon EC2 displays all security groups owned by the current user.
# Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Name of the security group. Example: webservers</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("GROUP", "PERMISSION")
- User ID of security group owner
- Security group name
- Description of the security group
- Firewall rule

Amazon EC2 displays errors on stderr.
Example

This example displays the state of the `websrv` security group.

```
$ ec2-describe-group websrv
GROUP 495219933132 websrv Web servers
PERMISSION 495219933132 websrv ALLOWS tcp 80 80 FROM CIDR 0.0.0.0/0
```
Related Topics

- DescribeSecurityGroups
- ec2-add-group
- ec2-delete-group
- ec2-authorize
- ec2-revoke
ec2-describe-image-attribute
Syntax

`ec2-describe-image-attribute ami_id (-l | -p)`
Description

Describes an attribute for the specified AMI.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ami_id</code></td>
<td>AMI identifier. Example: ami-4fa54026</td>
<td>Yes</td>
</tr>
<tr>
<td><code>-B, --block-device-mapping</code></td>
<td>Describes the mapping that defines native device names to use when exposing virtual devices. Type: String</td>
<td>No</td>
</tr>
<tr>
<td><code>-l, --launch-permission</code></td>
<td>Describes the <code>launchPermission</code> attribute. Example: -l</td>
<td>Choice</td>
</tr>
<tr>
<td><code>-p, --product-code</code></td>
<td>Describes the <code>productCodes</code> attribute. Example: -p</td>
<td>Choice</td>
</tr>
<tr>
<td><code>--kernel</code></td>
<td>Describes the ID of the kernel associated with the AMI. Type: String</td>
<td>No</td>
</tr>
<tr>
<td><code>--ramdisk</code></td>
<td>Describes the ID of the RAM disk associated with the AMI. Type: String</td>
<td>No</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Attribute type identifier
- ID of the AMI.
- Attribute value type or attribute list item value type.
- Attribute or attribute list item value.

Amazon EC2 displays errors on stderr.
Examples

This example lists the launch permissions for the ami-2bb65342 AMI.

```
$ ec2-describe-image-attribute ami-2bb65342 -l
launchPermission ami-2bb65342 group all
launchPermission ami-2bb65342 userId 495219933132
```

This example lists the product code for the ami-2bb65342 AMI.

```
$ ec2-describe-image-attribute ami-2bb65342 -p
productCodes ami-2bb65342 productCode 774F4FF8
```
Related Topics

- DescribeImageAttribute
- ec2-modify-image-attribute
- ec2-reset-image-attribute
- Sharing AMIs
ec2-describe-images
Syntax

d2-describe-images [ami_id ...] [-a] [-o owner ...] [-x user_id]
Description

Returns information about AMIs, AKIs, and ARIs available to the user. Information returned includes image type, product codes, architecture, and kernel and RAM disk IDs. Images available to the user include public images available for any user to launch, private images owned by the user making the request, and private images owned by other users for which the user has explicit launch permissions.

The list of AMIs returned can be modified by specifying AMI IDs, AMI owners, or users with launch permissions. If no options are specified, Amazon EC2 returns all AMIs for which the user has launch permissions.

If you specify one or more AMI IDs, only AMIs that have the specified IDs are returned. If you specify an invalid AMI ID, a fault is returned. If you specify an AMI ID for which you do not have access, it will not be included in the results.

If you specify one or more AMI owners, only AMIs from the specified owners and for which you have access are returned. The results can include the account IDs of the specified owners, amazon for AMIs owned by Amazon or self for AMIs that you own.

If you specify a list of executable users, only users that have launch permissions for the AMIs are returned. You can specify account IDs (if you own the AMI(s)), self for AMIs for which you own or have explicit permissions, or all for public AMIs.

**Note**

If you do not specify any optional parameters, Amazon EC2 returns images you own or images for which you have explicit access. Public images are not returned.

Machine images returned by this command include their kernel and RAM disk IDs.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-a</code></td>
<td>Returns AMIs that the user owns and for which the user has execution permissions. Example: <code>-a</code></td>
<td>No</td>
</tr>
<tr>
<td><code>-o owner</code></td>
<td>Returns AMIs owned by the specified owner. Multiple owners can be specified. Owners are specified with AWS user account ID, without dashes. The IDs <code>amazon</code>, <code>self</code>, and <code>explicit</code> can be used to include AMIs owned by Amazon, AMIs owned by the user, and AMIs for which the user has explicit launch permissions, respectively. Example: <code>-o 495219933132</code></td>
<td>No</td>
</tr>
<tr>
<td><code>-x user_id</code></td>
<td>Returns AMIs for which the specified user has explicit launch permissions. The user ID can be a user's account ID, <code>self</code> to return AMIs for which the sender of the request has explicit launch permissions, or <code>all</code> to return AMIs with public launch permissions. Example: <code>-x self</code></td>
<td>No</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- A record type identifier ("IMAGE")
- Image identifier
- Manifest location
- User identifier of the user that registered the image
- Image status
- Image visibility (public or private)
- Product codes, if any, that are attached to the instance
- Image architecture (i386 or x86_64)
- Image type (machine, kernel, or ramdisk)
- ID of the kernel associated with the image (machine images only)
- ID of the RAM disk associated with the image (machine images only)

Amazon EC2 displays errors on stderr.
Example

This example describes the ami-78a54011 AMI.

```
$ ec2-describe-images ami-78a54011
  IMAGE  ami-78a54011  powerdns/image.manifest.xml  495219933132  available  private  774F4FF8  i386
```

This example describes the Amazon 64-bit AMI.

```
$ ec2-describe-images --o amazon | grep x86_64
  IMAGE  ami-78a54034  ec2-public-images/fedora-core6-base-x86_64.manifest.xml
  amazon  available  public  x86_64  machine  aki-a2d732cb  ari-a3d732ca
```
Related Topics

- DescribeImages
- ec2-register
- ec2-deregister
ec2-describe-instances
Syntax

```
ec2-describe-instances [instance_id|availability-zone ...]
```
Description

Describes the current state of the specified instance(s). If you do not specify instances, all your instances are included in the output.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>instance_id</code></td>
<td>Instance identifier that was generated when the instance launched.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: <code>r-15a4417c</code></td>
<td></td>
</tr>
<tr>
<td><code>availability-zone</code></td>
<td>Returns instances within the specified availability zone.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: <code>us-east-1a</code></td>
<td></td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("RESERVATION", "INSTANCE")
- Instance ID for each running instance
- AMI ID of the image on which the instance is based
- Public DNS name associated with the instance. This is only present for instances in the running state
- Private DNS name associated with the instance. This is only present for instances in the running state
- Instance state
- Key name. If a key was associated with the instance at launch, its name will appear
- AMI launch index. For more information, see Instance Metadata

- Product codes attached to the instance
- Instance type. The type of the instance. For more information, see Instance Types
- Instance launch time. The time the instance launched
- Availability zone. The availability zone in which the instance is located

Amazon EC2 displays errors on stderr.
Example

This example describes the current state of the instances (currently one) owned by this user.

```
$ ec2-describe-instances
RESERVATION r-15a4417c 495219933132
INSTANCE i-3ea74257 ami-6ba54002 ec2-72-44-33-4.compute-1.amazonaws.com 10-251-50-154.ec2.internal running 0 774F4FF8 m1.small 2007-07-11T16:40:44+0000	sky
INSTANCE i-31a74258 ami-6ba54002 ec2-72-44-34-23.compute-1.amazonaws.com 10-251-50-156.ec2
```
Related Topics

- DescribeInstances
- ec2-run-instances
- ec2-terminate-instances
ec2-describe-keypairs
Syntax

`ec2-describe-keypairs [key_id ...]`
Description

Describes the current state of each specified key. If no keys are specified, all keys owned by the current user are included in the output.
Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>key_id</td>
<td>Names of one or more keys.</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Example: gsg-keypair</td>
<td></td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- A output type identifier ("KEYPAIR")
- Key pair identifier
- Private key fingerprint

Amazon EC2 displays errors on stderr.
Example

This example describes the state of the current keys.

```
$ ec2-describe-keypairs gsg-keypair
```
Related Topics

- DescribeKeyPairs
- ec2-add-keypair
- ec2-delete-keypair
ec2-detach-volume
Syntax

```
ec2-detach-volume volume_id [--instance instance_id [--device device]] [--force]
```
Description

Detaches an Amazon EBS volume from an instance.

⚠️ Important
Make sure to unmount any filesystems on the device within your operating system before detaching the volume. Failure to unmount file systems, or otherwise properly release the device from use, can result in lost data and will corrupt the file system.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>volume_id</code></td>
<td>The ID of the Amazon EBS volume. Example: <code>vol-4d826724</code></td>
<td>Yes</td>
</tr>
<tr>
<td><code>instance_id</code></td>
<td>The ID of the instance. Example: <code>i-6058a509</code></td>
<td>No</td>
</tr>
<tr>
<td><code>device</code></td>
<td>The device name. Example: <code>/dev/sdh</code></td>
<td>No</td>
</tr>
<tr>
<td><code>--force</code></td>
<td>Forces detachment if the previous detachment attempt did not occur cleanly (logging into an instance, unmounting the volume, and detaching normally). This option can lead to data loss or a corrupted file system. Use this option only as a last resort to detach an instance from a failed instance. The instance will not have an opportunity to flush file system caches nor file system meta data. If you use this option, you must perform file system check and repair procedures.</td>
<td>No</td>
</tr>
</tbody>
</table>
Output

Amazon EBS returns a table that contains the following information:

- ATTACHMENT identifier
- ID of the volume
- ID of the instance
- Device as which the volume is exposed within the instance
- Attachment state (e.g., detaching)
- Time stamp when detaching was initiated

Amazon EBS displays errors on stderr.
Example

This example detaches volume vol-4d826724.

```bash
$ ec2-detach-volume vol-4d826724
ATTACHMENT vol-4d826724 i-6058a509 /dev/sdh detaching 2008-02-14T00:00:17+0000
```
Related Topics

- ec2-create-volume
- ec2-delete-volume
- ec2-describe-volumes
- ec2-attach-volume
ec2-describe-snapshots
Syntax

ect2-describe-snapshots [snapshot_id ...]
Description

Describes the status of one or more snapshots. If no snapshots are specified, Amazon EBS returns information on all snapshots owned by you.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>snapshot_id</td>
<td>The IDs of the snapshots owned by you. If no snapshots are specified, Amazon EBS returns all snapshots owned by you. Example: snap-78a54011</td>
<td>No</td>
</tr>
</tbody>
</table>
Output

Amazon EBS returns a table that contains the following information:

- SNAPSHOT identifier
- ID of the snapshot
- ID of the volume
- Snapshot state (e.g., pending, completed)
- Time stamp when the snapshot request was initiated
- Percentage of completion

Amazon EBS displays errors on stderr.
Example

This example describes snapshot snap-78a54011.

$ ec2-describe-snapshots snap-78a54011
SNAPSHOT snap-78a54011 vol-4d826724 pending 2008-02-15T09:03:58+0000 60%
Related Topics

- ec2-create-snapshot
- ec2-delete-snapshot
ec2-describe-volumes
Syntax

ec2-describe-volumes [volume_id ...]
Description

Lists specified Amazon EBS volumes that you own. If no volumes are specified, Amazon EBS lists all volumes that you own.
# Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>volume_id</td>
<td>The IDs of the Amazon EBS volume to describe. If you do not specify a value, Amazon EBS returns information about all volumes owned by you. Example: vol-4282672b</td>
<td>No</td>
</tr>
</tbody>
</table>
Output

Amazon EBS returns a table that contains the following volume information:

- **VOLUME** identifier
- **ID** of the volume
- **Size** of the volume, in GiBs
- **Snapshot** from which the volume was created, if applicable
- **Availability zone** in which the instance launched
- **Volume state** (e.g., creating, available, in-use)
- **Time stamp** when volume creation was initiated

For volumes that are attached to instances, Amazon EBS returns a table that contains the following attachment information:

- **ATTACHMENT** identifier
- **ID** of the volume
- **ID** of the instance to which the volume is attached
- **Device** as which the volume is exposed within the instance
- **Attachment state** (e.g., attached)
- **Time stamp** when the attachment was initiated

Amazon EBS displays errors on stderr.
Example

This example describes all volumes associated with your account.

```
$ ec2-describe-volumes
VOLUME vol-4d826724 800 us-east-1a in-use 2008-02-14T00:00:00+0000
ATTACHMENT vol-4d826724 i-6058a509 /dev/sdh attached 2008-02-14T00:17+0000
VOLUME vol-50957039 13 us-east-1a available 2008-02-09T00:00:00+0000
ATTACHMENT vol-6682670f i-69a54000 /dev/sdh attached 2008-02-11T13:56:00+0000
```

This example describes volume vol-4d826724 and vol-50957039.

```
$ ec2-describe-volumes vol-4d826724 vol-50957039
VOLUME vol-4d826724 800 us-east-1a in-use 2008-02-14T00:00:00+0000
ATTACHMENT vol-4d826724 i-6058a509 /dev/sdh attached 2008-02-14T00:17+0000
VOLUME vol-50957039 13 us-east-1a available 2008-02-09T00:00:00+0000
```
Related Topics

- ec2-create-volume
- ec2-delete-volume
- ec2-attach-volume
- ec2-detach-volume
ec2-fingerprint-key
Syntax

ec2-fingerprint-key keyfile
Description

Computes and displays the fingerprint for a private key produced by Amazon EC2.

This operation is performed entirely on the client-side. Network access is not required.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyfile</td>
<td>The path to a file containing an unencrypted PEM-encoded PKCS#8 private key. Example: mykey.pem</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

A key fingerprint. This is formatted as a hash digest with each octet separated by a colon.

Amazon EC2 displays errors on stderr.
Example

This example computes and displays the fingerprint for the mykey.pem private key.

```
s ec2-fingerprint-key mykey.pem
```
Related Topics

- ec2-add-keypair
- ec2-describe-keypairs
ec2-get-console-output
Syntax

`ec2-get-console-output instance_id [-r]`
Description

Retrieves the console output that was displayed during startup for specified instance, if available, and displays it to std out.

In addition to standard startup information, this includes the SSH host key fingerprints which you can use to verify the host to which you are connecting.
Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance_id</td>
<td>Instance identifier generated when the instance launched. Example: i-10a64379</td>
<td>Yes</td>
</tr>
<tr>
<td>-r</td>
<td>Raw output. Do not escape the output to facilitate reading.</td>
<td>No</td>
</tr>
</tbody>
</table>
Output

- A timestamp indicating the time of the last update.
- The instance console output. By default the ^ESC character is escaped and duplicate new-lines are removed to facilitate reading.

Amazon EC2 displays errors on stderr.
## Example

This example retrieves the console output for the `i-10a64379` instance.

```
$ ec2-get-console-output i-10a64379
2007-01-03 12:00:00
Linux version 2.6.16-xenU (builder@patchbat.amazonsa) (gcc version 4.0.1 20050727 (Red Hat)
BIOS-provided physical RAM map:
Xen: 0000000000000000 - 000000006a400000 (usable)
980MB HIGHMEM available.
727MB LOWMEM available.
NX (Execute Disable) protection: active
IRQ lockup detection disabled
Built 1 zonelists
Kernel command line: root=/dev/sda1 ro 4
Enabling fast FPU save and restore... done.
...
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 2048 fc:8d:0c:eb:0e:a6:4a:61:50:00:c4:d2:51:78:66 /etc/ssh/ssh_host_rsa_key.pub
ec2: -----END SSH HOST KEY FINGERPRINTS-----
Fedora release 8 (Werewolf)
Kernel 2.6.21.7-2.fc8xen on an i686
```
ec2-modify-image-attribute
Syntax

ec2-modify-image-attribute ami_id -l (-a item_value | -r item_value)

ec2-modify-image-attribute ami_id -p product_code [-p product_code ...]
Description

Modifies an attribute for the specified AMI.
Attributes

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>launchPermission</code></td>
<td>List</td>
<td>Controls who has permission to launch the AMI. You can grant launch permissions by adding user IDs or make the AMI public by adding the all group. To learn more about sharing AMIs see</td>
</tr>
</tbody>
</table>

**Sharing AMIs.**

![Note](image)

If another user launches your AMI there is no mechanism to prevent that user from rebundling the image and registering it as a new AMI.

**productCodes**

List

Associates a product code with an AMI. This allows a developer to charge a user for using the AMI.

![Note](image)

The user must be signed up for the product before they can launch the AMI.

The product code attribute is a write-once attribute. After a product code is set for an AMI it cannot be altered or removed. AMIs are limited to one product code.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>-l</td>
<td>Modifies the <code>launchPermission</code> property. Example: <code>-l</code></td>
<td>Yes</td>
</tr>
<tr>
<td><code>-a item_value</code></td>
<td>Adds or removes an attribute item. The type of the item is inferred from the item value. For <code>launchPermission</code> there are two item types:</td>
<td></td>
</tr>
<tr>
<td><code>-a all</code></td>
<td>group: The only group currently supported is the all group. Adding this group sets public launch permissions for the AMI.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>userId: The user ID is an AWS account ID, without dashes. Adding user IDs grants explicit launch permissions for the AMI.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: <code>-a all</code></td>
<td></td>
</tr>
<tr>
<td><code>-p product_code</code></td>
<td>Sets the <code>productCodes</code> property. Example: <code>-p 774F4FF8</code></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Attribute type identifier.
- ID of the AMI on which attributes are being modified.
- Action performed on the attribute.
- Attribute or attribute list item value type.
- Attribute or attribute list item value.

Amazon EC2 displays errors on stderr.
Examples

The following example modifies launch permission attributes for the ami-2bb65342 AMI:

```
$ ec2-modify-image-attribute ami-2bb65342 -l -a 495219933132
```

The following example adds the 774F4FF8 product code to the ami-2bb65342 AMI:

```
$ ec2-modify-image-attribute ami-2bb65342 -p 774F4FF8
```
Related Topics

- ModifyImageAttribute
- ec2-reset-image-attribute
- ec2-describe-image-attribute
- Sharing AMIs
ec2-reboot-instances
Syntax

`ec2-reboot-instances instance_id [instance_id ...]`
Description

Reboots one or more specified instances. You must specify at least one instance ID.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>instance_id</code></td>
<td>Instance identifier that was assigned to the instance at launch. Example: i-3ea74257</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

This command displays no output on success.

Amazon EC2 displays errors on stderr.
Example

This example reboots the i-3ea74257 instance.

```
$ ec2-reboot-instances i-3ea74257
```
ec2-release-address
Syntax

d2-release-address  ip_address
Description

Releases an elastic IP address associated with your account.

If you run this operation on an elastic IP address that is already released, the address might be assigned to another account which will cause Amazon EC2 to return an error.

Note
Releasing an IP address automatically disassociates it from any instance with which it is associated. For more information, see ec2-disassociate-address.

Important
After releasing an elastic IP address, it is released to the IP address pool and might no longer be available to your account. Make sure to update your DNS records and any servers or devices that communicate with the address.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>ip_address</em></td>
<td>The IP address that you are releasing from your account. Example: <em>67.202.55.255</em></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("ADDRESS")
- Elastic IP address that you are releasing

Amazon EC2 displays errors on stderr.
Example

This example releases an elastic IP address associated with the account.

```
$ ec2-release-address 67.202.55.255
ADDRESS 67.262.55.255
```
Related Topics

- ec2-allocate-address
- ec2-describe-addresses
- ec2-associate-address
- ec2-disassociate-address
ec2-register
Syntax

`ec2-register manifest`
Description

Registers the Amazon Machine Image (AMI) specified in the manifest file and generates a new Amazon Machine Image (AMI) ID.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>manifest</strong></td>
<td>Location and filename of the manifest file. The manifest file must be located in Amazon S3 and must be in the bucket/object form. Example: mybucket/image.manifest.xml</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 assigns and returns an AMI ID.

Amazon EC2 displays errors on stderr.
Example

This example registers the AMI specified in the `image.manifest.xml` manifest file.

```
$ ec2-register mybucket/image.manifest.xml
IMAGE ami-78a54011
```
Related Topics

- RegisterImage
- `ec2-deregister`
- `ec2-describe-images`
ec2-reset-image-attribute
Syntax

ec2-reset-image-attribute ami_id -l
Description

Resets an attribute for the specified AMI.

The productCodes attribute cannot be reset.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ami_id</code></td>
<td>The identifier that was assigned to the AMI when it was registered.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: <code>r-15a4417c</code></td>
<td></td>
</tr>
<tr>
<td>-1</td>
<td>Resets the <code>launchPermission</code> attribute.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Example: <code>-1</code></td>
<td></td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Attribute type identifier
- ID of the AMI on which the attribute is being reset
- Action identifier ("RESET")

Amazon EC2 displays errors on stderr.
Example

This example resets the launchPermission attribute.

```
$ ec2-reset-image-attribute ami-6ba54002 -l
launchPermission ami-6ba54002 RESET
```
Related Topics

- ResetImageAttribute
- ec2-modify-image-attribute
- ec2-describe-image-attribute
- Sharing AMIs
ec2-revoke
Syntax

```
ec2-revoke group [-P protocol] (-p port_range | -t icmp_type_code) [-u source_group_user ...] [-o source_group ...] [-s source_subnet ...]
```
Description

Revokes a rule from the security group named GROUP. To identify the rule to be removed you must provide exactly the same set of options used to create that rule (see `ec2-add-group`).
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>The group to which this rule will apply. Example: webservers</td>
<td>Yes</td>
</tr>
<tr>
<td>-P protocol</td>
<td>The protocol to revoke. Condition: Applies when specifying a CIDR subnet as the source. Valid Values: tcp</td>
<td>Yes</td>
</tr>
<tr>
<td>-p port_range</td>
<td>For the TCP or UDP protocols, this specifies the range of ports to revoke. Condition: Applies when specifying a CIDR subnet as the source. Example: -p 80</td>
<td>Yes</td>
</tr>
<tr>
<td>-t icmp_type_code</td>
<td>For the ICMP protocol, you must specify the ICMP type and code. Use the type:code format, where both are integers. To specify a wildcard for either or both, enter -1. Condition: Applies when specifying a CIDR subnet as the source. Example: -t 2:5</td>
<td>Yes</td>
</tr>
<tr>
<td>-u source_group_user</td>
<td>The owner of a group specified using -o. If this is not specified, all groups will refer to the current user. If specified more than once, there must be exactly one -u per -o and each user will be mapped to the corresponding group. Example: -u 495219933132</td>
<td>No</td>
</tr>
<tr>
<td>-o source_group</td>
<td>The network source from which traffic will be revoked specified as a security Group. See the description of the -u option for group owner information. Example: -o headoffice</td>
<td>No</td>
</tr>
<tr>
<td>-s source_subnet</td>
<td>The network source from which traffic is to be revoked specified as a CIDR subnet range. Example: -s 205.192.8.45/24</td>
<td>No</td>
</tr>
</tbody>
</table>
Output

A table containing the following information is returned:

- Output type identifier ("GROUP", "PERMISSION")
- Group name. Currently, this will report an empty string
- Type of rule. Currently, only ALLOW rules are supported
- Protocol to allow
- Start of port range
- End of port range
- FROM
- Source

Amazon EC2 displays errors on stderr.
Example

This example revokes TCP port 80 access from the 205.192.0.0/16 address range for the `websrv` security group.

```
$ ec2-revoke websrv -P tcp -p 80 -s 205.192.0.0/16
GROUP websrv ""
PERMISSION websrv ALLOWS tcp 80 80 FROM CIDR 205.192.0.0/16
```
Related Topics

- RevokeSecurityGroupIngress
- ec2-add-group
- ec2-describe-group
- ec2-delete-group
- ec2-authorize
ec2-run-instances
Syntax

```
ec2-run-instances ami_id [-n instance_count] [-g group [-g group ...]] [-k keyname] [-d user_data | -f user_data_file] [ --addressing addressing_type] [ --instance-type instance_type] [ --availability-zone zone] [ --kernel kernel_id] [ --ramdisk ramdisk_id] [ --block-device-mapping block_device_mapping]
```
**Description**

Launches one or more instances of the specified AMI.

Every instance is launched in a security group. If you do not specify a security group at launch, the instances start in your default security group. For more information on creating security groups, see [CreateSecurityGroup](#).

An optional instance type can be specified. For information about instance types, see [Instance Types](#).

You can provide an optional key pair ID for each image in the launch request (for more information, see [CreateKeyPair](#)). All instances that are created from images that use this key pair will have access to the associated public key at boot. You can use this key to provide secure access to an instance of an image on a per-instance basis. Amazon EC2 public images use this feature to provide secure access without passwords.

⚠️ **Important**

Launching public images without a key pair ID will leave them inaccessible.

The public key material is made available to the instance at boot time by placing it in the `openssh_id.pub` file on a logical device that is exposed to the instance as `/dev/sda2` (the instance store). The format of this file is suitable for use as an entry within `~/.ssh/authorized_keys` (the OpenSSH format). This can be done at boot (e.g., as part of `rc.local`) allowing for secure access without passwords.

Optional user data can be provided in the launch request. All instances that collectively comprise the launch request have access to this data. For more information, see [Instance Metadata](#).

⚠️ **Note**

If the AMI has a Amazon DevPay product code attached for which the user has not subscribed, the `ec2-run-instances` call will fail.
Important

We strongly recommend using the 2.6.18 Xen stock kernel with the c1.medium and c1.xlarge instances. Although the default Amazon EC2 kernels will work, the new kernels provide greater stability and performance for these instance types. For more information about kernels, see Kernels, RAM Disks, and Block Device Mappings.
## Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ami_id</code></td>
<td>The identifier that was assigned to the AMI when it was registered. Example: <code>r-15a4417c</code></td>
<td>Yes</td>
</tr>
<tr>
<td><code>-n instance_count</code></td>
<td>The number of instances to launch. If Amazon EC2 cannot launch the specified number of instances, no instances will launch. If this is specified as a range (min-max), Amazon EC2 will try to launch the maximum number, but no fewer than the minimum number. Default: 1 Example: <code>-n 5</code></td>
<td>No</td>
</tr>
<tr>
<td><code>-g group</code></td>
<td>The security group(s) within which to launch the instances. This determines the ingress firewall rules applied to the instances. If you specify more than one group, the security policy will be the union of the security policies of the specified groups. Default: The default group. Example: <code>-g fooGroup</code></td>
<td>No</td>
</tr>
<tr>
<td><code>-k keyname</code></td>
<td>The key pair to make available to these instances at boot. Example: <code>-k fooKeyPair</code></td>
<td>No</td>
</tr>
<tr>
<td><code>-d user_data</code></td>
<td>Data to make available to the instances. This data is read from the command line of the <code>USER_DATA</code> argument. If you want the data to be read from a file, see the <code>-f</code> option. Example: <code>-d &quot;my user data&quot;</code></td>
<td>No</td>
</tr>
<tr>
<td><code>-f user_data_file</code></td>
<td>Data to make available to these instances. The data is read from the file specified by <code>FILE_NAME</code>. To specify user data on the command line, use the <code>-d</code> option. Example: <code>-f data.zip</code></td>
<td>No</td>
</tr>
<tr>
<td><code>--instance-type</code></td>
<td>The type of instance to launch. For more information, see <a href="#">Instance Types</a>. Example: <code>--instance-type m1.small</code></td>
<td>No</td>
</tr>
<tr>
<td><code>--availability-zone</code></td>
<td>The availability zone in which to launch the instance(s). For more information, see <a href="#">ec2-describe-availability-zones</a>. Example: <code>us-east-1a</code></td>
<td>No</td>
</tr>
<tr>
<td><code>--kernel kernel_id</code></td>
<td>The ID of the kernel with which to launch the instance. For information on finding available kernel IDs, see <a href="#">ec2-describe-images</a>. Example: <code>aki-ba3adfd3</code></td>
<td>No</td>
</tr>
<tr>
<td><code>--ramdisk ramdisk_id</code></td>
<td>The ID of the RAM disk with which to launch the instance. Some kernels require additional drivers at launch. Check the kernel requirements for information on whether you need to specify a RAM disk. To find kernel requirements, go to the <a href="#">Resource Center</a> and search for the kernel ID.</td>
<td>No</td>
</tr>
<tr>
<td>Example: ari-badbad00</td>
<td>--block-device-mappings mappings</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------</td>
<td></td>
</tr>
<tr>
<td>Specifies how block devices are exposed to the instance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual name example: instancestore0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device name example: sdb</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("INSTANCE").

- Instance ID which uniquely identifies each running instance.

- AMI ID of the image on which the instance(s) are based.

- DNS name associated with the instance (only present for instances in the running state).

- Instance state. This is usually pending, which indicates that the instance(s) are preparing to launch.

- Key name. If a key was associated with the instance at launch its name is displayed.

- AMI launch index. For more information, see Instance Metadata.

- Instance type. For more information on instance types, see Instance Types.

- Instance launch time. Specifies when the instance launched.

- Availability zone. Specifies the zone in which the instance launched.

Amazon EC2 displays errors on stderr.
Example

This example launches five instances of the ami-6ba54002 AMI.

```bash
$ ec2-run-instances ami-6ba54002 -n 5 --availability-zone us-east-1a -- 
RESERVATION r-0ea54067 495219933132 default 
INSTANCE i-3ea74257 ami-6ba54002 pending 0 m1.small 2007-07-11T16:40:44+ 
INSTANCE i-31a74258 ami-6ba54002 pending 1 m1.small 2007-07-11T16:40:44+ 
INSTANCE i-31a74259 ami-6ba54002 pending 2 m1.small 2007-07-11T16:40:44+ 
INSTANCE i-31a7425a ami-6ba54002 pending 3 m1.small 2007-07-11T16:40:44+ 
INSTANCE i-31a7425b ami-6ba54002 pending 4 m1.small 2007-07-11T16:40:44+ 
INSTANCE i-31a7425c ami-6ba54002 pending 5 m1.small 2007-07-11T16:40:44+
```
Related Topics

- RunInstances
- ec2-terminate-instances
- ec2-describe-instances
- ec2-add-keypair
- Instance Metadata
ec2-terminate-instances
Syntax

d2-terminate-instances  instance_id [instance_id ...]
Description

Terminates the specified instances.
# Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>instance_id</em></td>
<td>ID of the instance that was assigned at launch. Example: i-3ea74257</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Output

Amazon EC2 returns a table that contains the following information:

- Output type identifier ("INSTANCE")
- The instance ID of the instance being terminated
- The state of the instance prior to being terminated
- The new state of the instance

Amazon EC2 displays errors on stderr.
Example

This example terminates the i-3ea74257 instance.

```
$ ec2-terminate-instances i-3ea74257
INSTANCE i-3ea74257 running shutting-down
```
Related Topics

- TerminateInstances
- ec2-run-instances
- ec2-describe-instances
Technical FAQ

Topics

- General Information
- Operation Information
- Instance Types and Architectures
- IP Information
- Availability Zones
- Monitoring, Errors, and Unexpected Behavior
- Error Messages
- Paid AMIs
- Kernels, RAM Disks, and Block Device Mappings
- Miscellaneous

This section contains answers to commonly asked questions.
General Information

How many instances can I launch?

Each user has a concurrent running instance limit. For new users, this limit is 20. If you need more than 20 instances, please complete the Amazon EC2 Instance Request Form and your request will be considered.

How do I sign a request?

Information on signing SOAP requests is provided in Request Authentication. Information on signing Query requests is provided in Query API Authentication.

What username do I use for the various Amazon EC2 tools?

When you sign up with Amazon Web Services, you are provided an AWS Account ID. This is your username. For more information, refer to the Amazon Elastic Compute Cloud Getting Started Guide.

Why do my instances take so long to start?

Amazon EC2 must move the images around the network before they can be launched. For big images and/or congested networks, this can take several minutes. To improve performance, images are cached. As you launch your images more frequently, it should be less noticeable.

How durable are the instance stores?

Instance stores appear to an instance as a local disk. They will survive intentional and unintentional reboots of the instance unless the instance terminates or the underlying drive fails.

You should always backup or replicate important data.

What happens to my running instances if the machines on which they are running go down?

The instances will terminate and will need to be relaunched. The data on the instances' hard drives will be lost.
Always replicate important data or store it in Amazon S3.

*Can I get a bigger/smaller/differently optimized virtual machine?*

Yes. For more information, see [Instance Types](#).

*Is there a REST interface to Amazon EC2?*

Not at present. You can use the SOAP API, Query API, or the command-line tools.

*How does Amazon EC2 handle load balancing?*

With a service as flexible as Amazon EC2, you can use many types of load balancing systems. The load balancing instances can forward traffic to other systems. There are several open source solutions that are in wide use.

*Does Amazon perform system maintenance?*

Yes. Periodically, Amazon might perform maintenance that requires a reboot of your system. Make sure your instances can recover and restart after being rebooted.
Operation Information

*How do I handle time synchronization between instances?*

You can set up NTP (Network Time Protocol). For more information, go to [www.ntp.org](http://www.ntp.org). NTP is particularly important if you plan on using any Amazon web services (such as Amazon S3 or Amazon EC2) from within an instance, since requests to these services must be timestamped.

*Is there a method for an instance to discover its own instance ID?*

From within your instance you can use REST-like queries to [http://169.254.169.254/2008-05-05/](http://169.254.169.254/2008-05-05/) to retrieve various instance-specific metadata, including the instance ID. For more information, see [Instance Metadata](#).

*Can I pass arbitrary configuration values to an instance at launch time?*

Yes, although the size of the data is limited to 16K. For more information, see [Instance Metadata](#).

*Is there a way to run a script on instance termination?*

Not with any reliability. Amazon EC2 tries to shut an instance down cleanly (running system shutdown scripts), but there is only a short time available. In some cases (e.g., hardware failure), this does not happen.

Since there is no way to ensure shutdown scripts run, have a strategy to deal with abnormal terminations.

*How can I allow other people to launch my AMIs?*

You can allow other users to launch your AMIs by modifying the AMI's launchPermission attribute. You can grant public launch permissions or explicit permissions to specific users. For more information, see [Sharing AMIs](#).

*Why do I need to reregister a rebundled AMI? Can I keep the same AMI ID?*

An AMI ID is associated with the physical bits in an image. To protect users
from images being modified, we require you to reregister AMIs after rebundling.

*Can I pass JVM properties to the command line tools?*

Yes. By setting the environment variable `EC2_JVM_ARGS`, you can pass arbitrary JVM properties to the command line tools.

*Can I use a proxy with the command line tools?*

Yes. By passing in JVM properties through the `EC2_JVM_ARGS` environment variable, you can specify proxy settings for the command line tools. For example, in Linux:

```
export EC2_JVM_ARGS="-Dhttp.proxyHost=http://my.proxy.com -Dhttp.proxyPort=8080"
```

Properties for configuring a proxy are described in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>https.proxyHost</td>
<td>HTTPS proxy host</td>
</tr>
<tr>
<td>https.proxyPort</td>
<td>HTTPS proxy port</td>
</tr>
<tr>
<td>http.proxyHost</td>
<td>HTTPS proxy host</td>
</tr>
<tr>
<td>http.proxyPort</td>
<td>HTTPS proxy port</td>
</tr>
<tr>
<td>http.proxyRealm</td>
<td>Proxy realm (https and http)</td>
</tr>
<tr>
<td>http.proxyUser</td>
<td>Proxy username (https and http)</td>
</tr>
<tr>
<td>http.proxyPass</td>
<td>Proxy password (https and http)</td>
</tr>
</tbody>
</table>

*Note*

`https.proxyHost` should be used when `EC2_URL` points to an https host, and `http.proxyHost` when `EC2_URL` points to an http host.
Instance Types and Architectures

What happened to the original instance type?

The original instance type is still available. It is called the small instance (m1.small) and it has the same technical specifications.

Will the original instance type be retired soon?

There are no plans to retire the original instance type.

If I do not specify an instance type at launch, what type of instance will I get?

You will get a m1.small Amazon EC2 instance type.

Does my instance limit apply to all instance types or is there a separate limit for each type?

The instance limit applies to the sum of all instances, regardless of type. There is no separate instance limit per type.

Can I mix instance types, or do I have to use the same type for all of my instances?

You can launch any combination of instance types. Choose the instance types that have the most appropriate memory, CPU, and storage for each function within your application.

How do I select the right instance type?

Amazon EC2 instances are grouped into two families: standard and High-CPU. Standard instances have memory to CPU ratios suitable for most general purpose applications; High-CPU instances have proportionally more CPU resources than memory (RAM) and are well suited for compute-intensive applications. When selecting instance types, you might want to use less powerful instance types for your web server instances and more powerful instance types for your database instances. Additionally, you might want to run CPU instance types for CPU-intensive data processing tasks.
For most applications, the standard instance types are appropriate. These instance types include the small instance (m1.small), large instance (m1.large), and extra large instance (m1.xlarge). High-CPU instances are well suited for compute-intensive applications such as rendering, search indexing, and computational analysis. The High-CPU instance types are the High-CPU medium instance (c1.medium) and the High-CPU extra large instance (c1.xlarge). For more information, refer to Instance Types.

One of the advantages of Amazon EC2 is that you pay by the instance hour, which makes it convenient and inexpensive to test the performance of your application on different instance families and types. One good way to determine the most appropriate instance family and instance type is to launch test instances and benchmark your application.

When should I use High-CPU instance types (c1.medium and c1.xlarge)?

High-CPU instance types have a proportionately higher ratio of CPU to memory and are well suited for compute-intensive applications. To determine whether they are appropriate for you, launch an instance and benchmark your own application on different instance types and calculate which is most appropriate.

Which instance types are 32-bit and which are 64-bit?

The small (m1.small) and High-CPU medium (c1.medium) instances are 32-bit. The large (m1.large), extra large (m1.xlarge), and High-CPU extra large (c1.xlarge) instances are 64-bit.

Can I launch any AMI on any type of instance?

No. You must use 64-bit AMIs on large (m1.large), extra large (m1.xlarge) and High-CPU extra large (c1.xlarge) instances. You must use 32-bit AMIs on small (m1.small) and High-CPU medium (c1.medium) instances.

Can I use my own kernel?

Not at present. However, as of version 2008-02-01 of the Amazon EC2 API you can use any of the kernels published by Amazon EC2 or selected vendors.

Do I have to do anything special to bundle the large or extra large instances?
Make sure to use the latest AMI Tools.

*Can I build an AMI that works on both 32-bit and 64-bit instances?*

No, an AMI is either a 32-bit AMI or a 64-bit.

*Can I run 32-bit applications on 64-bit AMIs?*

You can run a 32-bit application on a 64-bit host if the Linux kernel is compiled with IA32 emulation and the correct 32-bit libraries are available.

By default, the Amazon DomU Kernel has IA32 emulation enabled and there are many public AMIs that include pre-installed 32-bit libraries. If the library you require is not included with the AMI, you can install it using standard tools (e.g., yum).

*How fast is the disk?*

The large and extra large instances have higher and more consistent I/O performance than the original (small) instance.

![Note]

The first write to any given block of the disk will be slower than subsequent writes. For more information, see [Disk Performance Optimization](#).

*Can I RAID the spindles exposed on large and extra large instances?*

Yes, you can use software RAID on top of the exposed spindles.

![Note]

The initial RAID setup might take a long time. For more information, see [Disk Performance Optimization](#).
IP Information

How do I host a public domain if I have to DHCP an IP address?

You can use a dynamic DNS service, such as DynDNS or ZoneEdit. Alternatively, you can map an elastic IP address to your instance and avoid the propagation delays possible with a dynamic DNS solution.

Why do I get an internal (RFC 1918) IP address when I look up a DNS name that I expect to map to my instance's external IP address?

The Amazon EC2 DNS servers return the internal IP address when asked about an instance's public DNS name. In this way, DNS lookups that would resolve to a public Amazon EC2 IP address will be translated to the correct internal IP address. This only works when using the Amazon EC2 DNS servers from an Amazon EC2 instance.

Why is Amazon EC2 Using NAT?

Public IP space is a limited resource. Amazon EC2 is adopting NAT to ensure that we are able to efficiently make use of our public Internet addresses.

Furthermore, the new NAT networking will enable Amazon to deliver new features in the future. For example, some users might not want external addresses. This would allow for non-Internet routable clusters, which will further preserve IPs and increase security for those not running public facing servers.

Can I use a static IP in my instances?

Not at present. Your image must be configured as a DHCP client and it will be assigned an IP address. Currently, all instances come with Internet-addressable IP addresses. If you enable access through the firewall from the "world", you can address them from anywhere.

How does the instance know its public and private addresses?

From within the instance, issue the following HTTP queries:

To obtain the internal IP address:
To obtain the public IP address:


*Why am I limited to 5 elastic IP addresses?*

Public (IPV4) Internet addresses are a scarce public resource. Amazon EC2 is committed to helping use that space efficiently.

By default, all accounts are limited to 5 elastic IP addresses. If you need more than 5 Elastic IP addresses, please complete the [Amazon EC2 Elastic IP Address Request Form](https://console.aws.amazon.com/ec2/elasticip). We will ask you to think through your use case and help us understand your need for additional addresses.

*Is my elastic IP addressed fixed to a single instance?*

Unlike a traditional dedicated IP addresses, an elastic IP can be assigned to many different instances over time.

*Is there a minimum usage required for elastic IP addresses?*

When operating within the 5 address limit, you can leave addresses unattached as you need. However, we reserve the right to reclaim elastic IP addresses that are chronically underutilized.

*Is there a charge for elastic IP addresses?*

To ensure our customers are efficiently using elastic IP addresses, we impose the a small hourly charge when these IP addresses are not mapped to an instance. When these IP addresses are mapped to an instance, they are free of charge. To avoid charges for elastic IP addresses that you are not using, use ReleaseAddress.

*Do I need one elastic IP address for every instance that I have running?*

You do not need an elastic IP address for all your instances. By default, every
instance comes with a private IP address and an Internet routable public IP address. These addresses are fixed for the life of the instance. We believe this should be adequate for many applications where you do not need a long lived Internet routable end point (e.g., compute clusters, web crawling, and backend services).

Why don't you use IPV6 addresses?

Because of the scarcity of IPV4 Internet address, Amazon EC2 will be actively investigating the use of IPV6 addresses. We believe this is the only tenable long term solution. We don't yet have a timeline for introducing IPV6 addresses, but when we do support IPV6 addresses, we will be able to remove the friction we have imposed with IPV4 address.

Can I launch an instance with no public IP address?

You cannot currently launch an instance without a public IP address. We understand that for many applications, it is desirable to have no Internet routable IP address (e.g., internal databases).

How long does it take to remap an elastic IP address?

After you successfully make an API call to remap an IP address, it will usually occur within a few minutes.

Will I be charged for the time when my IP address is unattached because my instance failed?

You are not charged until your elastic IP address has been unattached for a full hour. As long as you are monitoring your instances, you will have plenty of time to reattach your instance before the charge is metered.

Am I limited to 100 elastic IP remaps per month?

No. The first 100 remaps per account are free. After that, there will be a charge for each remap.
Availability Zones

Can I assume that my availability zone us-east-1a is the same location as someone else's availability zone us-east-1a?

No. Currently, we do not support cross-account proximity. Each account's availability zones are independent. There is no assurance that your availability zone us-east-1a will be the same as any other account's availability zone us-east-1a.

How can I make sure that I am in the same availability zone as another developer?

We do not currently support the ability to coordinate availability groups between developer accounts. We are seeking customer feedback to understand the types of use cases for proximity control between accounts. We will use this feedback to determine how and when we can provide availability zone control between accounts.

Regional data transfer seems like such a small charge, why are you complicating my bill with this?

We anticipate that for most common use cases, regional data transfer will only constitute a very small portion of your monthly usage charges. There are valid use cases that involve moving large amounts of data between availability zones. In these cases, the regional data transfer can be a significant cost.

We try to enable as many use cases as possible while charging you only for what you use. Because of the large potential differences in the way developers will use regional data transfer, we think it is appropriate to break this cost out rather than amortize it across other charges.

If I have two instances in different availability zones, how will I be charged for regional data transfer?

Each instance is charged for its data in and data out. Therefore, if data is transferred between these two instances, it is charged out for the first instance and in for the second instance.
If I transfer data between availability zones using public IP addresses, will I be charged twice for Regional Data Transfer (once because it’s across zones, and a second time because I’m using public IP addresses)?

No. Regional Data Transfer rates apply if at least one of the following is true, but is only charged once for a given instance even if both are true:

- The other instance is in a different availability zone, regardless of which type of address is used
- Public or Elastic IP addresses are used, regardless of which zone the other instance is in.
Monitoring, Errors, and Unexpected Behavior

How do I monitor my systems?

Amazon EC2 provides basic monitoring. You can use DescribeInstances to check whether an instance appears to be running. However, if you are using Amazon EC2 as your data center, you might want to set up for sophisticated monitoring on your instances, such as SNMP.

Why can't I "talk" to my instances?

There are a few common reasons for broken connectivity to your instance.

Amazon EC2 changes the state of your instance to running after your operating system starts booting. Depending on your AMI, there will be a delay before the instance is fully set up and functional.

If your instance has been running for several minutes, you verify you authorized the appropriate access to your host through the Amazon EC2 firewall. If you have launched your instances without specifying a security group, the default group is used. Permissions on the default group are very strict and disallow all access from the Internet and other groups. You will need to modify the permissions of your default group or set up a new group with appropriate permissions. For more information, see Network Security

If this doesn't solve your issue, make sure you authorized port 22 and try to open an SSH connection with verbose output. Use the man page for the exact syntax of your system, but the command is likely to be similar to ssh -vv root@[hostname]. This output is very useful if you are posting to the forum.

Why did my instance terminate immediately after launch?

Launch errors can be the result of an internal error during launch or a corrupt Amazon EC2 image. Internal errors are rare, as we actively test for and isolate suspect hosts. Consult the DescribeInstances operation for details on why your instance failed to launch.
Note

The `ec2-describe-instances` command line tool does not provide this information. Use the `-v` flag to read the detailed SOAP response and get detailed information.

You can also attempt to launch the image again. If this proves to be a persistent problem (especially with a shared image), post to the AWS forums.

I ran `shutdown` from within an `ssh` session, but my instance still shows up as running when I query it with `DescribeInstances` and I can't shell into it.

To shut down an instance, use the `TerminateInstances` call (`ec2-terminate`) on the command line. You can also use `shutdown -h`, but must verify the instance shut down using the `DescribeInstances` call.

Why are my instances stuck in a pending state (or a shutting-down state)?

This situation is rare and might be the result of a software error or misconfiguration.

We actively monitor for this; please contact us if it occurs.

Why do I get an "AuthFailure: User is not AMI creator" error when I try to register an image?

Make sure that you are using the correct user ID and certificate to create and upload the image. You must use the same ID and certificate to register the image with Amazon EC2.
Error Messages

Why do I get an "InsufficientInstanceCapacity" error when I try to launch an instance?

This error indicates that we do not currently have enough available capacity to service your request.

If you are requesting a large number of instances, there might not be enough server capacity to host them. You can try again later or specify a smaller number of instances.

Why do I get an "InstanceLimitExceeded" error when I try to launch an instance?

This error indicates you reached your concurrent running instance limit. For new users during the public beta, the limit is 20.

If you need additional capacity, please contact us at aws@amazon.com.

Why can't I retrieve my instance-specific data from within a running instance when querying http://169.254.169.254/2008-05-05/?

The Parameterized Launches feature is available to instances that were launched after the feature was released. If you launched your instance before this, the data will not be available. If you want to use this functionality, relaunch your instances.

If you still experience problems retrieving the data after relaunching your instance, check the following:

- Verify you are using the correct base URI (http://169.254.169.254/2008-05-05/)

- Verify you are using the correct URI for the data you are trying to retrieve. Depending on the data, a trailing "/" might be required

- Verify you specified launch data when launching your instances. If not, you will get a HTTP error response (404) when trying to retrieve the user data
Why do I get keep getting "Request has expired" errors?

To reduce the risk of replay attacks, our requests include a timestamp. This and the most important parts of the request are signed to ensure the message (including the timestamp) cannot be modified without detection.

If the difference between the timestamp in the request and the time on our servers is larger than 5 minutes, the request is too old (or too new) and an error is returned.

You need to ensure that your system clock is accurate and configured to use the correct time zone. For more information, go to NTP.
Paid AMIs

Note
You can still share AMIs without charging. Public and paid AMIs can be listed in the Resource Center.

How can I determine if a particular AMI is a paid AMI?

By describing images (ec2dim) with the "-a" flag and looking for AMIs that have a product code. For example, if you run `ec2dim -a`, the result contains an AMI with the ID `ami-bd9d78d4`. This is our Demo Paid AMI with product code `A79EC0DB`.

How can I determine if a public AMI is paid?

By describing images (ec2dim). An AMI is a paid AMI if a product code is returned. Example: run `ec2dim -a amazon`, and the AMI `ami-bd9d78d4` will be returned with a product code (A79EC0DB).

Is there anything that prevents a paid AMI from being rebundled? How can this be restricted?

Paid AMIs are comparable to shared AMIs with regards to rebundling and trying to restrict rebundling. If you allow a user running the AMI to see all of its contents (e.g. by giving root access to the AMI), the user could rebundle these into their own AMI.

Why can't I query a particular AMI's attributes to see if the AMI is paid?

Only the owner of an AMI can query the AMI attributes. However, anyone can tell if an AMI is paid by describing images (ec2dim). An AMI is paid if a product code is returned. Example: run `ec2dim -a amazon`, and the AMI with ID `ami-bd9d78d4` will be returned with a product code (A79EC0DB).

Who can use the confirm-product-instance command?

Only the owner of the AMI can use this command. Owners use this command with supported AMIs to determine if a supported instance with a given product
code attached is up and running.

Will the product code be inherited by the rebundled AMI?

If your customer uses AWS tools to rebundle the AMI, the product code associated with the AMI is inherited by the rebundled AMI. When launching the rebundled AMI the customer is still billed for usage based on your price.

Note
This is a convenience feature and not a guarantee that the product code will always be attached to rebundled AMIs.

Note that the customer's workflow could bundle the AMI outside of Amazon EC2, or the customer could use modified versions of the AWS tools, preventing the product code from being inherited.

Will the kernel/RAM disk be inherited by the rebundled AMI?

If you rebundle an AMI, it inherits the kernel and RAM disk from the source AMI unless you specify a different kernel and RAM disk.

Note
This is a convenience feature and not a guarantee that the kernel/RAM disk will always be attached to rebundled AMIs.

I created my paid AMIs with one AWS developer account, but I want to sell them using a different AWS developer account. Can I transfer them?

No, you can't automatically transfer AMIs from one account to another. You would have to upload them again using the second AWS developer account and then register them with DevPay using that account. Alternately, you could leave the AMIs with the original account (the AMI owner account) and register them with DevPay using another AWS developer account (the product owner account). You could then use the AMI owner account to associate the product code with the AMIs. However, keep in mind that only the product owner (and not the AMI owner in this case) can use the ec2-confirm-product-instance command, which confirms that an instance is running an AMI associated with the product owner's product code.
How do I prevent someone from stripping the product code from my paid AMI?

If you do not provide root access to your AMI, it cannot be rebundled. If you provide root access, our tools attempt to preserve the product code.

To increase security, we recommend that you configure your application to check the instance metadata to verify that the product code is intact.
Kernels, RAM Disks, and Block Device Mappings

What are user selectable kernels?

Amazon EC2 provides user selectable kernels which enables you to select a kernel when bundling an AMI or launching an instance. User selectable kernels are useful for keeping your instances up to date with security fixes and updates, being able to use functionality provided by new distributions, and for using specialty applications that have unique timing requirements.

How do I find user selectable kernels?

Use the describeInstances operation with the --kernel option. This lists all public kernels that are currently available. After locating a kernel to launch or bundle with your AMI, go to the Resource Center and search for it to determine whether there are any known issues and whether it has any dependencies.

Can I use my own kernel?

Not at present. However, as of version 2008-02-01 of the Amazon EC2 API you can use any of the kernels published by Amazon EC2 or selected vendors.

What type of dependencies do kernels have?

Kernels are most likely to require a RAM disk that contains required drivers (e.g., Xen drivers, video drivers, and so on). If you launch a kernel without a required RAM disk, it will not work properly.

How do I know a kernel/AMI combination will work together?

If you are concerned about whether the kernel/image combination will work well together, Amazon provides several AMIs that have tested combinations that you can use as a starting point for your AMIs or AMIs that you can use as a foundations for a public AMIs. If you require a certified kernel/ AMI combination, you can find them as paid AMIs through organizations such as RedHat. For more information, see Paying for AMIs.
Are there any special requirements to use FTP?

The File Transfer Protocol (FTP) has a PORT command by which a client sends its address back to the server. The server then connects to the client at that address to send the file data. If the client looks up its own internal address and sends this to the server, the connection will fail. In this specific case, there are two solutions to the problem. First, configure the client to send its public IP address. Second, the client can use "passive FTP" which makes connections only to the server, rather than from the server to the client. In general, applications which encode local addresses and port numbers in data sent to external servers might have problems with NAT. Care must always be taken to send the public address, rather than the internal one. We recommend using passive mode unless it is not supported by the FTP server.
Glossary
Amazon machine image (AMI)

An Amazon Machine Image (AMI) is an encrypted machine image stored in Amazon S3. It contains all the information necessary to boot instances of your software.

ephemeral store

See *instance store*.

explicit launch permission

Launch permission granted to a specific user.

gibibyte (GiB)

A contraction of giga binary byte, a gibibyte is $2^{30}$ bytes or 1,073,741,824 bytes. A gigabyte is $10^9$ or 1,000,000,000 bytes. So yes, Amazon has bigger bytes.

instance

Once an AMI has been launched, the resulting running system is referred to as an instance. All instances based on the same AMI start out identical and any information on them is lost when the instances are terminated or fail.

instance store

The disk storage associated with an instance. In the event an instance fails or is terminated, all content on the instance store is deleted.

group

Also known as a security group, groups define firewall rules that can be shared among a group of instances that have similar security requirements. The group is specified at instance launch.

launch permission

AMI attribute allowing users to launch an AMI
public AMI

An AMI that all users have launch permissions for.

reservation

A collection of instances started as part of the same launch request.

shared AMI

AMIs that developers build and make available for other AWS developers to use.

tebibyte (TiB)

a contraction of tera binary byte, a tebibyte is $2^{40}$ bytes or 1,099,511,627,776 bytes. A terabyte is $10^{12}$ or 1,000,000,000,000 bytes. So yes, Amazon has bigger bytes.
Document Conventions

This section lists the common typographical and symbol use conventions for AWS technical publications.
## Typographical Conventions

This section describes common typographical use conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description/Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Call-outs</strong></td>
<td>A call-out is a number in the body text to give you a visual reference. The reference point is further discussion elsewhere. You can use this resource regularly.</td>
</tr>
<tr>
<td><strong>Code in text</strong></td>
<td>Inline code samples (including XML) and commands are identified with a special font. You can use the command <code>java -version</code>.</td>
</tr>
<tr>
<td><strong>Code blocks</strong></td>
<td>Blocks of sample code are set apart from the body and marked accordingly.</td>
</tr>
<tr>
<td></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td># ls -l /var/www/html/index.html</td>
</tr>
<tr>
<td></td>
<td># date</td>
</tr>
<tr>
<td></td>
<td>Wed Jun 21 09:33:42 EDT 2006</td>
</tr>
<tr>
<td><strong>Emphasis</strong></td>
<td>Unusual or important words and phrases are marked with a special font. You must sign up for an account before you can use the service.</td>
</tr>
<tr>
<td><strong>Internal cross references</strong></td>
<td>References to a section in the same document are marked. See <a href="#">Document Conventions</a>.</td>
</tr>
<tr>
<td><strong>Logical values, constants, and regular expressions, abstracta</strong></td>
<td>A special font is used for expressions that are important to identify, but are not code. If the value is null, the returned response will be false.</td>
</tr>
<tr>
<td><strong>Product and feature names</strong></td>
<td>Named AWS products and features are identified on first use. Create an <em>Amazon Machine Image</em> (AMI).</td>
</tr>
<tr>
<td><strong>Operations</strong></td>
<td>In-text references to operations. Use the <code>GetHITResponse</code> operation.</td>
</tr>
<tr>
<td><strong>Parameters</strong></td>
<td>In-text references to parameters. The operation accepts the parameter <code>AccountID</code>.</td>
</tr>
<tr>
<td><strong>Response elements</strong></td>
<td>In-text references to responses. A container for one <code>CollectionParent</code> and one or more <code>CollectionItems</code>.</td>
</tr>
<tr>
<td><strong>Technical publication</strong></td>
<td>References to other AWS publications. If the reference is hyperlinked, it is also underscored. For detailed conceptual information, see the <em>Amazon Mechanical Turk Developer Guide</em>.</td>
</tr>
<tr>
<td>references</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>User entered values</td>
<td>A special font marks text that the user types. At the password</td>
</tr>
<tr>
<td></td>
<td>prompt, type <strong>MyPassword.</strong></td>
</tr>
<tr>
<td>User interface controls and</td>
<td>Denotes named items on the UI for easy identification. On the</td>
</tr>
<tr>
<td>labels</td>
<td>File menu, click Properties.</td>
</tr>
<tr>
<td>Variables</td>
<td>When you see this style, you must change the value of the</td>
</tr>
<tr>
<td></td>
<td>content when you copy the text of a sample to a command line.</td>
</tr>
<tr>
<td></td>
<td>% ec2-register <code>&lt;your-s3-bucket&gt;/image.manifest</code></td>
</tr>
<tr>
<td></td>
<td>See also <a href="#">Symbol Conventions</a>.</td>
</tr>
</tbody>
</table>
## Symbol Conventions

This section describes the common use of symbols.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Symbol</th>
<th>Description/Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutually exclusive parameters</td>
<td>(Parentheses</td>
<td>and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% data = hdfread (start</td>
</tr>
<tr>
<td>Optional parameters</td>
<td>[square brackets]</td>
<td>Within a code description, square brackets denote completely optional commands or parameters.</td>
</tr>
<tr>
<td>XML variable text</td>
<td></td>
<td>% sed [-n, -quiet]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use square brackets in XML examples to differentiate them from tags.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;CustomerId&gt;[ID]&lt;CustomerId&gt;</td>
</tr>
<tr>
<td>Variables</td>
<td>&lt;arrow brackets&gt;</td>
<td>Within a code sample, arrow brackets denote a variable that must be replaced with a valid value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>% ec2-register &lt;your-s3-bucket&gt;/image.manifest</td>
</tr>
</tbody>
</table>
Index

A

actions, Actions
addressing, Instance Addressing and Network Security
AllocateAddress, AllocateAddress, AllocateAddress
allocating elastic IP addresses, AllocateAddress, AllocateAddress, ec2_allocate_address
Amazon DevPay, Creating Paid AMIs
AMI tools
   ec2-add-keypair, ec2-upload-bundle
   ec2-bundle-image, ec2-bundle-image
   ec2-bundle-vol, ec2-bundle-vol
   ec2-delete-bundle, ec2-delete-bundle
   ec2-download-bundle, ec2-download-bundle
   ec2-unbundle, ec2-unbundle
AMIs
   bundling, Bundling an AMI
   creating, Creating an AMI
   paid, Paying for AMIs
   shared, Using Shared AMIs
      finding, Finding Shared AMIs
      security, Safe Use of Shared AMIs
   sharing, Sharing AMIs
API
   actions, Actions
   common data types, Common Data Types
   conventions, API Conventions
   data types, Data Types and the Amazon EC2 WSDL
   Query, Using the Query API
   reference, API Reference
   SOAP, Using the SOAP API
APIs, using, Using the APIs
AssociateAddress, AssociateAddress, AssociateAddress
associating elastic IP addresses, AssociateAddress, AssociateAddress, ec2_associate_address
attaching EBS volumes, `ec2-attach-volume`
attaching volumes, `AttachVolume`, `AttachVolume`
AttachVolume, `AttachVolume`, `AttachVolume`
AttachVolumeResponseType, `AttachVolumeResponseType`
AttachVolumeType, `AttachVolumeType`
audience, `Audience`
authentication
    Query, `Query API Authentication`
    SOAP, `Request Authentication`
AuthorizeSecurityGroupIngress, `AuthorizeSecurityGroupIngress`
authorizeing security group ingress, `AuthorizeSecurityGroupIngress`
Availability Zones, `Availability Zones`, `Availability Zones`
    describing, `DescribeAvailabilityZones`, `DescribeAvailabilityZones`, `ec2-describe-availability-zones`
AvailabilityZoneItemType, `AvailabilityZoneItemType`

B

batch processing, `Introduction to Amazon Elastic Compute Cloud`
best practices, `Instance Usage`
block device mapping, `Kernels, RAM Disks, and Block Device Mappings`
block storage
    attach volume, `ec2-attach-volume`
    create snapshot, `ec2-create-snapshot`
    create volume, `ec2-create-volume`
    delete snapshot, `ec2-delete-snapshot`
    delete volume, `ec2-delete-volume`
    describe volumes, `ec2-describe-volumes`
    describing snapshots, `ec2-describe-snapshots`
    detach volume, `ec2-detach-volume`
BlockDeviceMappingItemType, `BlockDeviceMappingItemType`
bundling AMIs, `Bundling an AMI`

C

categories, `Categories of Available Data`
changes to Amazon EC2, What's New

CLI

ec2-add-group, ec2-add-group
ec2-add-keypair, ec2-upload-bundle, ec2-add-keypair
ec2-allocate-address, ec2-allocate-address
ec2-associate-address, ec2-associate-address
ec2-attach-volume, ec2-attach-volume
ec2-authorize, ec2-authorize
ec2-bundle-image, ec2-bundle-image
ec2-bundle-vol, ec2-bundle-vol
ec2-confirm-product-instance, ec2-confirm-product-instance
ec2-create-snapshot, ec2-create-snapshot
ec2-create-volume, ec2-create-volume
ec2-delete-bundle, ec2-delete-bundle
ec2-delete-group, ec2-delete-group
ec2-delete-keypair, ec2-delete-keypair
ec2-delete-snapshot, ec2-delete-snapshot
ec2-delete-volume, ec2-delete-volume
ec2-deregister, ec2-deregister
ec2-describe-addresses, ec2-describe-addresses
ec2-describe-availability-zones, ec2-describe-availability-zones
ec2-describe-group, ec2-describe-group
ec2-describe-image-attribute, ec2-describe-image-attribute
ec2-describe-images, ec2-describe-images
ec2-describe-instances, ec2-describe-instances
ec2-describe-keypairs, ec2-describe-keypairs
ec2-describe-snapshots, ec2-describe-snapshots
ec2-describe-volumes, ec2-describe-volumes
ec2-detach-volume, ec2-detach-volume
ec2-disassociate-address, ec2-disassociate-address
ec2-download-bundle, ec2-download-bundle
ec2-fingerprint-key, ec2-fingerprint-key
ec2-get-console-output, ec2-get-console-output
ec2-modify-image-attribute, ec2-modify-image-attribute
ec2-reboot-instances, ec2-reboot-instances
ec2-register, ec2-register
ec2-release-address, ec2-release-address
ec2-reset-image-attribute, ec2-reset-image-attribute
ec2-revoke, ec2-revoke
ec2-run-instances, ec2-run-instances
ec2-terminate-instances, ec2-terminate-instances
ec2-unbundle, ec2-unbundle
list of operations, List of Operations by Function
client error codes, API Error Codes
command line tools, Command Line Tools Reference
AMI tools, AMI Tools
API tools, API Tools
errors, Errors
options, Common Options
common data types, Common Data Types
computation building block, Instance Usage
compute resources, measuring, Measuring Compute Resources
confirming instances, ConfirmProductInstance, ConfirmProductInstance, ec2-confirm-product-instance
ConfirmProductInstance, ConfirmProductInstance, ConfirmProductInstance
console output, Get Console Output and Reboot Instances
getting, GetConsoleOutput, GetConsoleOutput, ec2-get-console-output
conventions
API, API Conventions
CPU, I/O Resources
CreateKeyPair, CreateKeyPair, CreateKeyPair
CreateSecurityGroup, CreateSecurityGroup, CreateSecurityGroup
CreateSnapshot, CreateSnapshot, CreateSnapshot
CreateSnapshotResponseType, CreateSnapshotResponseType
CreateSnapshotType, CreateSnapshotType
CreateVolume, CreateVolume, CreateVolume
CreateVolumeResponseType, CreateVolumeResponseType
CreateVolumeType, CreateVolumeType
creating AMIs, Creating an AMI
creating EBS snapshots, ec2-create-snapshot
creating EBS volumes, ec2-create-volume
creating keypairs, CreateKeyPair, CreateKeyPair
creating paid AMIs, Creating Paid AMIs
creating snapshots, CreateSnapshot, CreateSnapshot
creating volumes, CreateVolume, CreateVolume

D
data retrieval, [Data Retrieval](#)
data types, [Data Types and the Amazon EC2 WSDL](#)
   - AttachVolumeResponseType, [AttachVolumeResponseType](#)
   - AttachVolumeType, [AttachVolumeType](#)
   - AvailabilityZoneItemType, [AvailabilityZoneItemType](#)
   - BlockDeviceMappingItemType, [BlockDeviceMappingItemType](#)
   - CreateSnapshotResponseType, [CreateSnapshotResponseType](#)
   - CreateSnapshotType, [CreateSnapshotType](#)
   - CreateVolumeResponseType, [CreateVolumeResponseType](#)
   - CreateVolumeType, [CreateVolumeType](#)
   - DeleteSnapshotResponseType, [DeleteSnapshotResponseType](#)
   - DeleteSnapshotType, [DeleteSnapshotType](#)
   - DeleteVolumeResponseType, [DeleteVolumeResponseType](#)
   - DeleteVolumeType, [DeleteVolumeType](#)
   - DescribeImagesResponseItemType, [DescribeImagesResponseItemType](#)
   - DescribeKeyPairsResponseItemType, [DescribeKeyPairsResponseItemType](#)
   - DescribeSnapshotsResponseType, [DescribeSnapshotsResponseType](#)
   - DescribeSnapshotsType, [DescribeSnapshotsType](#)
   - DescribeVolumesResponseType, [DescribeVolumesResponseType](#)
   - DescribeVolumesType, [DescribeVolumesType](#)
   - DetachVolumeResponseType, [DetachVolumeResponseType](#)
   - DetachVolumeType, [DetachVolumeType](#)
   - EmptyElementType, [EmptyElementType](#)
   - GroupSetType, [GroupSetType](#)
   - InstanceStateType, [InstanceStateType](#)
   - IpPermissionType, [IpPermissionType](#)
   - LaunchPermissionItemType, [LaunchPermissionItemType](#)
   - LaunchPermissionOperationType, [LaunchPermissionOperationType](#)
   - PlacementRequestType, [PlacementRequestType](#)
   - PlacementResponseType, [PlacementResponseType](#)
   - ProductCodeItemType, [ProductCodeItemType](#)
   - ProductInstanceResponseItemType, [ProductInstanceResponseItemType](#)
   - ReservationInfoType, [ReservationInfoType](#)
   - RunningInstancesItemType, [RunningInstancesItemType](#)
   - SecurityGroupItemType, [SecurityGroupItemType](#)
   - TerminateInstancesResponseInfoType, [TerminateInstancesResponseInfoType](#)
   - UserType, [UserDataType](#)
   - UserIdGroupPairType, [UserIdGroupPairType](#)
DeleteKeyPair, DeleteKeyPair, DeleteKeyPair
DeleteSecurityGroup, DeleteSecurityGroup, DeleteSecurityGroup
DeleteSnapshot, DeleteSnapshot, DeleteSnapshot
DeleteSnapshotResponseType, DeleteSnapshotResponseType
DeleteSnapshotType, DeleteSnapshotType
DeleteVolume, DeleteVolume, DeleteVolume
DeleteVolumeResponseType, DeleteVolumeResponseType
DeleteVolumeType, DeleteVolumeType
deleting EBS snapshots, ec2-delete-snapshot
deleing EBS volumes, ec2-delete-volume
deleing keypairs, DeleteKeyPair, DeleteKeyPair, ec2-delete-keypair
deleing security groups, DeleteSecurityGroup, DeleteSecurityGroup, ec2-delete-group
deleing snapshots, DeleteSnapshot, DeleteSnapshot
deleing volumes, DeleteVolume, DeleteVolume
DeregisterImage, DeregisterImage, DeregisterImage
deregistering images, DeregisterImage, DeregisterImage, ec2-deregister
DescribeAddresses, DescribeAddresses, DescribeAddresses
DescribeAvailabilityZones, DescribeAvailabilityZones,
DescribeAvailabilityZones
DescribeImageAttribute, DescribeImageAttribute, DescribeImageAttribute
DescribeImages, DescribeImages, DescribeImages
DescribeImagesResponseItemType, DescribeImagesResponseItemType
DescribeInstances, DescribeInstances, DescribeInstances
DescribeKeyPairs, DescribeKeyPairs, DescribeKeyPairs
DescribeKeyPairsResponseItemType, DescribeKeyPairsResponseItemType
DescribeSecurityGroups, DescribeSecurityGroups, DescribeSecurityGroups
DescribeSnapshots, DescribeSnapshots, DescribeSnapshots
DescribeSnapshotsResponseType, DescribeSnapshotsResponseType
DescribeSnapshotsType, DescribeSnapshotsType
DescribeVolumes, DescribeVolumes, DescribeVolumes
DescribeVolumesResponseType, DescribeVolumesResponseType
DescribeVolumesType, DescribeVolumesType
describing availability zones, DescribeAvailabilityZones,
DescribeAvailabilityZones, ec2-describe-availability-zones
describing EBS snapshots, ec2-describe-snapshots
describing EBS volumes, ec2-describe-volumes
describing elastic IP addresses, DescribeAddresses, DescribeAddresses, ec2-describe-addresses
describing image attributes, DescribeImageAttribute, DescribeImageAttribute, DescribeImageAttribute, DescribeImageAttribute

describing images, DescribeImages, DescribeImages, DescribeImages, DescribeImages

describing instances, DescribeInstances, DescribeInstances, DescribeInstances, DescribeInstances

describing keypairs, DescribeKeyPairs, DescribeKeyPairs, DescribeKeyPairs, DescribeKeyPairs


describing snapshots, DescribeSnapshots, DescribeSnapshots, DescribeSnapshots

describing volumes, DescribeVolumes, DescribeVolumes

detaching EBS volumes, ec2-detach-volume, DetachVolume, DetachVolume, DetachVolume, DetachVolume

detaching volumes, DetachVolume, DetachVolume

device mapping, Kernels, RAM Disks, and Block Device Mappings

DevPay, Creating Paid AMIs

DisassociateAddress, DisassociateAddress, DisassociateAddress

disassociating elastic IP addresses, DisassociateAddress, DisassociateAddress, DisassociateAddress

disk performance, Disk Performance Optimization

RAID, RAID Configuration

DNS, internal, Internal DNS Name

E

disk performance, Disk Performance Optimization

RAID, RAID Configuration

DNS, internal, Internal DNS Name

E

ec2-add-group, ec2-add-group

dc2-add-keypair, ec2-upload-bundle, ec2-add-keypair

dc2-allocate-address, ec2-allocate-address

dc2-associate-address, ec2-associate-address

dc2-attach-volume, ec2-attach-volume

dc2-authorize, ec2-authorize

dc2-bundle-image, ec2-bundle-image

dc2-bundle-vol, ec2-bundle-vol

dc2-confirm-product-instance, ec2-confirm-product-instance

dc2-create-snapshot, ec2-create-snapshot

dc2-create-volume, ec2-create-volume
ec2-delete-bundle, ec2-delete-bundle
ec2-delete-group, ec2-delete-group
ec2-delete-keypair, ec2-delete-keypair
ec2-delete-snapshot, ec2-delete-snapshot
ec2-delete-volume, ec2-delete-volume
ec2-deregister, ec2-deregister
ec2-describe-addresses, ec2-describe-addresses
ec2-describe-availability-zones, ec2-describe-availability-zones
ec2-describe-group, ec2-describe-group
ec2-describe-image-attribute, ec2-describe-image-attribute
ec2-describe-images, ec2-describe-images
ec2-describe-instances, ec2-describe-instances
ec2-describe-keypairs, ec2-describe-keypairs
ec2-describe-snapshots, ec2-describe-snapshots
ec2-describe-volumes, ec2-describe-volumes
ec2-detach-volume, ec2-detach-volume
ec2-disassociate-address, ec2-disassociate-address
ec2-download-bundle, ec2-download-bundle
ec2-fingerprint-key, ec2-fingerprint-key
ec2-get-console-output, ec2-get-console-output
ec2-modify-image-attribute, ec2-modify-image-attribute
ec2-reboot-instances, ec2-reboot-instances
ec2-register, ec2-register
ec2-release-address, ec2-release-address
ec2-reset-image-attribute, ec2-reset-image-attribute
ec2-revoke, ec2-revoke
ec2-run-instances, ec2-run-instances
ec2-terminate-instances, ec2-terminate-instances
ec2-unbundle, ec2-unbundle
elastic block storage
  attach volume, ec2-attach-volume
  create snapshot, ec2-create-snapshot
  create volume, ec2-create-volume
  delete snapshot, ec2-delete-snapshot
  delete volume, ec2-delete-volume
  describe volumes, ec2-describe-volumes
  describing snapshots, ec2-describe-snapshots
detach volume, ec2-detach-volume
elastic IP addresses, Instance Addressing and Network Security
allocating, AllocateAddress, AllocateAddress, ec2-allocate-address
associating, AssociateAddress, AssociateAddress, ec2-associate-address
describing, DescribeAddresses, DescribeAddresses, ec2-describe-addresses
disassociating, DisassociateAddress, DisassociateAddress, ec2-disassociate-address
releasing, ReleaseAddress, ReleaseAddress, ec2-release-address

EmptyElementType, EmptyElementType
error codes, API Error Codes
eroors, Monitoring, Errors, and Unexpected Behavior
messages, Error Messages
example Query request, Example Request

F

FAQs, Technical FAQ
availability zones, Availability Zones
block device mapping, Kernels, RAM Disks, and Block Device Mappings
eroors, Monitoring, Errors, and Unexpected Behavior
geneneral, General Information
instance types, Instance Types and Architectures
IP addresses, IP Information
kernels, Kernels, RAM Disks, and Block Device Mappings
miscellaneous, Miscellaneous
monitoring, Monitoring, Errors, and Unexpected Behavior
operations, Operation Information
paid AMIs, Paid AMIs
proximity, Availability Zones
RAM disk, Kernels, RAM Disks, and Block Device Mappings
unexpected behaviors, Monitoring, Errors, and Unexpected Behavior
firewall
concepts, Concepts

G

general information, General Information
GetConsoleOutput, GetConsoleOutput, GetConsoleOutput
g getopt, Command Line Tools Reference
g getting console output, GetConsoleOutput, GetConsoleOutput, ec2-get-console-
output
glossary, Glossary
groups, Concepts
GroupSetType, GroupSetType

I

I/O resources, I/O Resources
images
deregistering, DeregisterImage, DeregisterImage, ec2-deregister
describing, DescribeImages, DescribeImages, ec2-describe-images
describing attributes, DescribeImageAttribute, DescribeImageAttribute, ec2-describe-image-attribute
modifying attributes, ModifyImageAttribute, ModifyImageAttribute, ec2-modify-image-attribute
registering, RegisterImage, RegisterImage, ec2-register
resetting attributes, ResetImageAttribute, ResetImageAttribute, ec2-reset-image-attribute
instance store, Instance Storage
instance types, Instance Types and Architectures
instances
addressing, Instance Addressing and Network Security
confirming, ConfirmProductInstance, ConfirmProductInstance, ec2-confirm-product-instance
describing, DescribeInstances, DescribeInstances, ec2-describe-instances
launching, Launching and Using Instances
metadata, Instance Metadata
rebooting, Get Console Output and Reboot Instances, RebootInstances, RebootInstances, ec2-reboot-instances
running, RunInstances, RunInstances, ec2-run-instances
security, Instance Addressing and Network Security
sizes, Instance Types
storage, Instance Storage
terminating, TerminateInstances, TerminateInstances, ec2-terminate-instances
types, Instance Types
usage, Instance Usage
InstanceStateType, InstanceStateType
introduction, Introduction to Amazon Elastic Compute Cloud
IP address information, **IP Information**

IP addresses
- allocating, **AllocateAddress**, **AllocateAddress**, **ec2-allocate-address**
- associating, **AssociateAddress**, **AssociateAddress**, **ec2-associate-address**
- describing, **DescribeAddresses**, **DescribeAddresses**, **ec2-describe-addresses**
- disassociating, **DisassociateAddress**, **DisassociateAddress**, **ec2-disassociate-address**
- releasing, **ReleaseAddress**, **ReleaseAddress**, **ec2-release-address**

IpPermissionType, **IpPermissionType**

K

kernels, **Kernels, RAM Disks, and Block Device Mappings**
keypairs
- creating, **CreateKeyPair**, **CreateKeyPair**
- deleting, **DeleteKeyPair**, **DeleteKeyPair**, **ec2-delete-keypair**
- describing, **DescribeKeyPairs**, **DescribeKeyPairs**, **ec2-describe-keypairs**

L

launch data, security, **Security of Launch Data**
launch index, example, **Use Case: AMI Launch Index Value**
LaunchPermissionItemType, **LaunchPermissionItemType**
LaunchPermissionOperationType, **LaunchPermissionOperationType**
listing EBS volumes, **ec2-describe-volumes**
locality, **Availability Zones**

M

mapping, block device, **Kernels, RAM Disks, and Block Device Mappings**
memory, **I/O Resources**
metadata, **Instance Metadata**
- categories, **Categories of Available Data**
- retrieval, **Retrieving Metadata**
miscellaneous FAQs, **Miscellaneous**
ModifyImageAttribute, **ModifyImageAttribute**, **ModifyImageAttribute**
modifying image attributes, **ModifyImageAttribute**, **ModifyImageAttribute**, **ec2-modify-image-attribute**
monitoring information, Monitoring, Errors, and Unexpected Behavior

N

NAT, Instance Addressing and Network Security
network security, Instance Addressing and Network Security
new features, What's New

O

operations
    CLI, List of Operations by Function
    information, Operation Information
    Query, List of Operations by Function, Amazon EC2 Query API, List of Operations by Function
    SOAP, Amazon EC2 SOAP API
output, console, Get Console Output and Reboot Instances
overview, Introduction to Amazon Elastic Compute Cloud

P

paid AMIs
    creating, Creating Paid AMIs
    information, Paid AMIs
Paid AMIs, Paying for AMIs
parameters, Query, Common Query Parameters
performance, optimization, Disk Performance Optimization
permissions, Instance Usage
PlacementRequestType, PlacementRequestType
PlacementResponseType, PlacementResponseType
private addresses, Instance Addressing and Network Security
ProductCodeItemTypex, ProductCodeItemTypex
ProductInstanceResponseItemTypex, ProductInstanceResponseItemTypex
programming language support, Programming Language Support in Amazon EC2
proximity, Availability Zones, Availability Zones
public addresses, Instance Addressing and Network Security
Query
AllocateAddress, AllocateAddress
Using the Query API
AssociateAddress, AssociateAddress
AttachVolume, AttachVolume
authentication, Query API Authentication
AuthorizeSecurityGroupIngress, AuthorizeSecurityGroupIngress
common parameters, Common Query Parameters
ConfirmProductInstance, ConfirmProductInstance
CreateKeyPair, CreateKeyPair
CreateSecurityGroup, CreateSecurityGroup
CreateSnapshot, CreateSnapshot
CreateVolume, CreateVolume
DeleteKeyPair, DeleteKeyPair
DeleteSecurityGroup, DeleteSecurityGroup
DeleteSnapshot, DeleteSnapshot
DeleteVolume, DeleteVolume
DeregisterImage, DeregisterImage
DescribeAddresses, DescribeAddresses
DescribeAvailabilityZones, DescribeAvailabilityZones
DescribeImageAttribute, DescribeImageAttribute
DescribeImages, DescribeImages
DescribeInstances, DescribeInstances
DescribeKeyPairs, DescribeKeyPairs
DescribeSecurityGroups, DescribeSecurityGroups
DescribeSnapshots, DescribeSnapshots
DescribeVolumes, DescribeVolumes
DetachVolume, DetachVolume
DisassociateAddress, DisassociateAddress
example request, Example Request
GetConsoleOutput, GetConsoleOutput
list of operations, List of Operations by Function, List of Operations by Function
ModifyImageAttribute, ModifyImageAttribute
operations, Amazon EC2 Query API
parameters, Query Parameters
RebootInstances, RegisterImage, ReleaseAddress, ResetImageAttribute, RevokeSecurityGroupIngress, RunInstances, TerminateInstances

RAID, RAID Configuration
RAM disk, Kernels, RAM Disks, and Block Device Mappings
reboot, Get Console Output and Reboot Instances
rebooting instances, RebootInstances, RegisterImage, RegisterImage, RebootInstances, RebootInstances, RebootInstances
reference, API, API Reference
RegisterImage, RegisterImage, RegisterImage
registering images, RegisterImage, RegisterImage, RegisterImage, RegisterImage, RegisterImage, RegisterImage, RegisterImage, RegisterImage, RegisterImage
ReleaseAddress, ReleaseAddress, ReleaseAddress
releasing elastic IP addresses, ReleaseAddress, ReleaseAddress, ReleaseAddress
required knowledge, Required Knowledge and Skills
ReservationInfoType, ReservationInfoType
ResetImageAttribute, ResetImageAttribute, ResetImageAttribute
resetting image attributes, ResetImageAttribute, ResetImageAttribute, ResetImageAttribute, ResetImageAttribute
resources, Related Resources
I/O, I/O Resources
measuring, Measuring Compute Resources
response structure, The Response Structure
response structure, SOAP, The Response Structure
retrieving metadata, Retrieving Metadata
retrieving user data, Retrieving User Data
revoking security group ingress, RevokeSecurityGroupIngress, RevokeSecurityGroupIngress, RevokeSecurityGroupIngress, ec2-revoke
RunInstances, RunInstances, RunInstances, RunInstances, RunInstances, RunInstances
running instances, RunInstances, RunInstances, ec2-run-instances
RunningInstancesItemType, RunningInstancesItemType

S

scalable applications, Introduction to Amazon Elastic Compute Cloud
security, Instance Addressing and Network Security
security groups, Concepts
  authorizing ingress, AuthorizeSecurityGroupIngress, AuthorizeSecurityGroupIngress, ec2-authorize
deleting, DeleteSecurityGroup, DeleteSecurityGroup, ec2-delete-group
describing, DescribeSecurityGroups, DescribeSecurityGroups, ec2-describe-group
  revoking ingress, RevokeSecurityGroupIngress, RevokeSecurityGroupIngress, ec2-revoke
SecurityGroupItemType, SecurityGroupItemType
server error codes, API Error Codes
service overview, Introduction to Amazon Elastic Compute Cloud
shared AMIs, Using Shared AMIs
  finding, Finding Shared AMIs
security, Safe Use of Shared AMIs
sharing AMIs, Sharing AMIs
sizes of instances, Instance Types
snapshots
  creating, CreateSnapshot, CreateSnapshot
deleting, DeleteSnapshot, DeleteSnapshot
describing, DescribeSnapshots, DescribeSnapshots
SOAP
AllocateAddress, AllocateAddress
API, Using the SOAP API
AssociateAddress, AssociateAddress
AttachVolume, AttachVolume
authentication, Request Authentication
AuthorizeSecurityGroupIngress, AuthorizeSecurityGroupIngress
ConfirmProductInstance, ConfirmProductInstance
CreateKeyPair, CreateKeyPair
CreateSecurityGroup, CreateSecurityGroup
CreateSnapshot, CreateSnapshot
CreateVolume, CreateVolume
DeleteKeyPair, DeleteKeyPair
DeleteSecurityGroup, \texttt{DeleteSecurityGroup}
DeleteSnapshot, \texttt{DeleteSnapshot}
DeleteVolume, \texttt{DeleteVolume}
DeregisterImage, \texttt{DeregisterImage}
DescribeAddresses, \texttt{DescribeAddresses}
DescribeAvailabilityZones, \texttt{DescribeAvailabilityZones}
DescribeImageAttribute, \texttt{DescribeImageAttribute}
DescribeImages, \texttt{DescribeImages}
DescribeInstances, \texttt{DescribeInstances}
DescribeKeyPairs, \texttt{DescribeKeyPairs}
DescribeSecurityGroups, \texttt{DescribeSecurityGroups}
DescribeSnapshots, \texttt{DescribeSnapshots}
DescribeVolumes, \texttt{DescribeVolumes}
DetachVolume, \texttt{DetachVolume}
DisassociateAddress, \texttt{DisassociateAddress}
GetConsoleOutput, \texttt{GetConsoleOutput}
ModifyImageAttribute, \texttt{ModifyImageAttribute}
operations, \texttt{Amazon EC2 SOAP API}
RebootInstances, \texttt{RebootInstances}
RegisterImage, \texttt{RegisterImage}
ReleaseAddress, \texttt{ReleaseAddress}
ResetImageAttribute, \texttt{ResetImageAttribute}
response structure, \texttt{The Response Structure}
RevokeSecurityGroupIngress, \texttt{RevokeSecurityGroupIngress}
RunInstances, \texttt{RunInstances}
TerminateInstances, \texttt{TerminateInstances}
WSDL, \texttt{WSDL and Schema Definitions}
static IPs, \texttt{Instance Addressing and Network Security}
storage, I/O Resources, \texttt{Instance Storage}
locations, Storage Locations
suggestions, \texttt{Instance Usage}

T

temporary events, \texttt{Introduction to Amazon Elastic Compute Cloud}
TerminateInstances, \texttt{TerminateInstances}, \texttt{TerminateInstances}
TerminateInstancesResponseInfoType, \texttt{TerminateInstancesResponseInfoType}
terminating instances, \texttt{TerminateInstances}, \texttt{TerminateInstances}, \texttt{ec2-terminate-instances}
types of instances, Instance Types

unexpected behavior information, Monitoring, Errors, and Unexpected Behavior
user data, retrieval, Retrieving User Data
UserDataType, UserDataType
UserIdGroupPairType, UserIdGroupPairType
using, Using Amazon EC2

volumes
attaching, AttachVolume, AttachVolume
creating, CreateVolume, CreateVolume
deleting, DeleteVolume, DeleteVolume
describing, DescribeVolumes, DescribeVolumes
detaching, DetachVolume, DetachVolume

web services references, Web Services References
WSDL, WSDL and Schema Definitions

zones, availability, Availability Zones