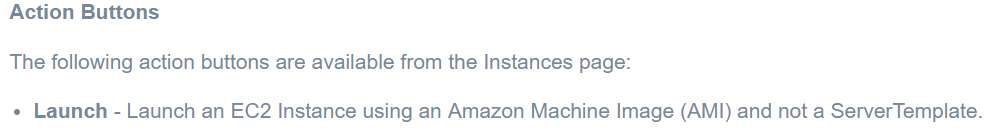
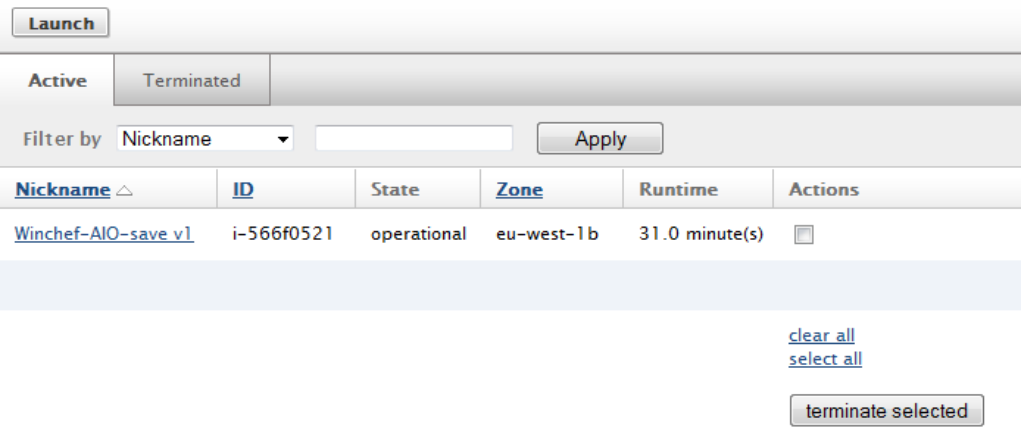
**EC2 Instances**

Overview

A cloud *instance* refers to a Virtual Machine Instance (VMI) that runs within a cloud infrastructure. Conceptually, an instance is simply a dedicated machine in your desired cloud infrastructure that you can configure for your own purposes. Two of the more important concepts with respect to instances in the cloud are instance type and state. Both of which can differ from cloud to cloud. An instance type is basically the size of the instance. That is, the amount of compute resources when provisioned such as the amount of CPU, memory, and ephemeral storage. RightScale maps these back to generic terms which are easier to understand across all cloud infrastructures. It's the cloud provider's responsibility to make sure that an instance is provisioned which meets the requirements you specify from the RightScale Dashboard (or API).

Navigating to **Clouds** > *AWS Region* > **Instances** displays a list of all active and inactive (terminated) server instances of Amazon's EC2. It's an exhaustive list of all instances that were launched/terminated within the selected cloud/region. Click the **Active** or **Terminated** tabs to toggle the view.

page lists unmanaged instances in addition to servers that were launched from Deployments using ServerTemplates.



## View EC2 Instance Details

Use the following procedure to view the details of a running EC2 Instance from the RightScale Dashboard.

1. Navigate to **Clouds** > AWS Region > **Instances**
2. Select the Instance Nickname you want to view (Hint: use the Filter by option if there are many running Instances). This page shows you detailed information about your Instance.
3. Action buttons and Instance details are displayed.

## Terminate an Instance

Use the following procedure to terminate an Instance.

1. Navigate to **Clouds** > AWS Region > **Instances**
2. Select the Instance you want to terminate.
3. Click the **Terminate** button.

EC2 SSH Keys

SSH Keys are used to establish secure client-server connections via SSH (shell acces) to running instances in the cloud. An SSH Key pair consists of both public and private material. EC2 SSH Keys are also region-specific. When you launch an EC2 instance, you must use an SSH Key that's located in the same region as where you're going to launch the instance.

Create a unique SSH Key (secure shell) so that you can SSH directly into a machine. The SSH key is passed directly into an instance in order to provide root login access to the machine via SSH. Once an instance is launched, you can typically find it inserted into **/root/.ssh/authorized\_keys**.

For security reasons, when an SSH Key is created, Amazon will only send the key material of the SSH Key to the user once. Therefore, SSH Keys that are generated inside the Dashboard will have key material, whereas SSH Keys generated outside of RightScale will not have any key material. However, you can manually add the key material for one of your SSH keys inside the Dashboard. The Dashboard will always display all SSH Keys associated with an account, regardless of whether or not they have key material. You can still launch an instance inside the Dashboard using an SSH key that does not have any key material, but you will not be able to SSH into the instance or use any of RightScale's convenient features such as bundling, backups, automation, etc. Without knowing the contents of the SSH Keys, RightScale will not be able to access your instance to perform such tasks.

The **Key Fingerprint** is the public key fingerprint. It is shorter than the private key, and is used to authenticate or lookup the longer private key. **Key Material** refers to the encrypted portion of the private key. For security reasons, the private key material is only visible in the RightScale Dashboard to the user who created the SSH Key and users with 'admin' user role privileges. Since Amazon will only send you the private key material once when you create an SSH Key, it's important that you create your SSH Keys from the RightScale Dashboard/API, otherwise RightScale will not be able to capture the private key material. Without key material, you will not be able to SSH into an instance if it's using v4 RightImages. If you've created SSH keys outside of RightScale, they will appear in the list below and you'll be able to assign them to an instance at launch time. However, since RightScale does not have its private key material, you will not be able to SSH into the instance from the RightScale Dashboard. To solve this problem, simply edit the key and manually add its key material.

RightScale's Managed SSH feature will be used to establish SSH access and RightLink will be used to run RightScripts on the instance. You can either use the unique SSH Key that RightScale generates for each user or upload your own SSH Key.

**Note:**

When you launch an instance, be sure to select an SSH Key that contains key material. (Key material = yes)

**Action Buttons**

The following action buttons are available on the SSH Keys page:

* **New** - Create a new SSH Key pair where Amazon will generate the key pair for you.
* **Import** - Create a new SSH Key pair by using an existing RSA key pair.

Actions

* [Create a New SSH Key](http://docs.rightscale.com/cm/dashboard/clouds/aws/actions/ec2_ssh_keys_actions.html#create-a-new-ssh-key)
* [Add Private SSH Key Material](http://docs.rightscale.com/cm/dashboard/clouds/aws/actions/ec2_ssh_keys_actions.html#add-private-ssh-key-material)
* [Create an RSA Key Pair](http://docs.rightscale.com/cm/dashboard/clouds/aws/actions/ec2_ssh_keys_actions.html#create-an-rsa-key-pair)
* [Create a New SSH Key by Importing an RSA Key Pair](http://docs.rightscale.com/cm/dashboard/clouds/aws/actions/ec2_ssh_keys_actions.html#create-a-new-ssh-key-by-importing-an-rsa-key-pair)
* [Delete an SSH Key](http://docs.rightscale.com/cm/dashboard/clouds/aws/actions/ec2_ssh_keys_actions.html#delete-an-ssh-key)