

**Running an Intelligent Analytical System on AWS**

**Using AWS Services & Solutions in AWS Marketplace**

Step-by-Step Deployment Guide – Part 2

**Table of Contents**

[4.6 Setup R environment for doing Predictive Analysis [R (F)] 3](#_Toc469413278)

[4.7. Setup Kony Mobile Fabric (H) 6](#_Toc469413279)

[4.8. Trend Micro Deep Security (I) 12](#_Toc469413280)

[4.8.1. Launch Instance 12](#_Toc469413281)

[4.8.2. Launch RDS Database 19](#_Toc469413282)

[4.8.3. Create Database in SQL Server 24](#_Toc469413283)

[4.8.4. Install Deep Security Manager 28](#_Toc469413284)

[4.8.5. Modify your AWS Security Group to open required ports on your instances 31](#_Toc469413285)

[4.8.6. Create a dedicated AWS policy and user account for Deep Security to access your cloud account 33](#_Toc469413286)

[4.8.7. Adding your AWS Cloud account to Deep Security 37](#_Toc469413287)

[4.8.8. Deploy Deep Security Agents to your Windows AWS instance 41](#_Toc469413288)

[4.8.9. Deploy Deep Security Agents to your Linux AWS instance 44](#_Toc469413289)

[4.9. Setup demo code tree & datasets [Github repository cloning] 49](#_Toc469413290)

[4.10 Install Tomcat Servers for Web Interfacing 52](#_Toc469413291)

[4.11. Install Apache Maven 55](#_Toc469413292)

[4.12. Cluster & resource setup automation using AWS CloudFormation 58](#_Toc469413293)

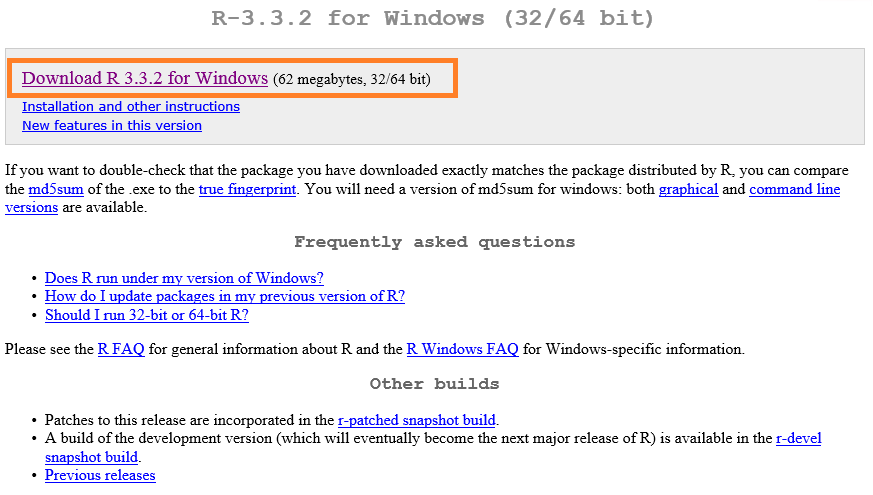
[5. Billing and Cost Management 68](#_Toc469413294)

[6. Next Steps 74](#_Toc469413295)

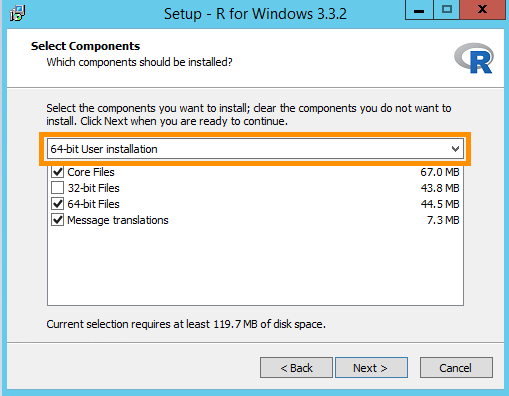
[7. Appendix 74](#_Toc469413296)

* 1. Setup R environment for doing Predictive Analysis [R (F)]

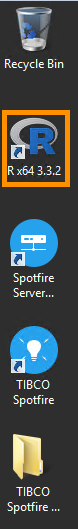
1. Make a remote desktop connection to the **TIBCO Spotfire** instance that is created in **Section 4.5** ofthe **Deployment Guide — Part 1**. (Refer to **Steps 1 through 10 of Section 4.4.2** of **the Deployment Guide — Part 1** to make a remote connection to an EC2 instance.)
2. Click on the link [*https://cran.r-project.org/bin/windows/base*](https://cran.r-project.org/bin/windows/base%20) using the browser inside the TIBCO Spotfire instance.
3. Click on the **“Download R 3.3.2 for Windows”** link to download the R installation package.



1. While performing the installation, select the default settings — except in the **Select Components** window, choose **64-bit User installation**.



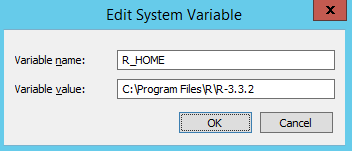
1. After a successful installation, you can find R desktop icons to open the R Console.



1. Add the following System Environment variables for the R installation:

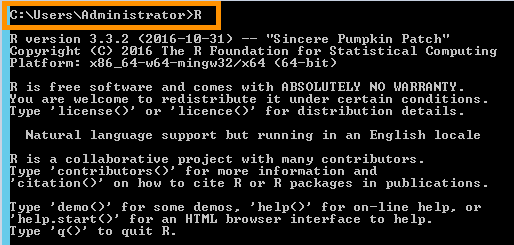
Variable Name: **R\_HOME**

Variable Value: Path to the R installation directory. By default, it is C:\Program Files\R\R-X.X.X, where X.X.X is the version number.



1. Append string **“;%R\_HOME%\bin”** at the end of the existing value of the Path variable. Semicolon “;” acts as a string separator.
2. Execute an **R** command in a new instance of a command prompt to check if R is installed.

The following output signifies a successful installation.



**Benefits:**

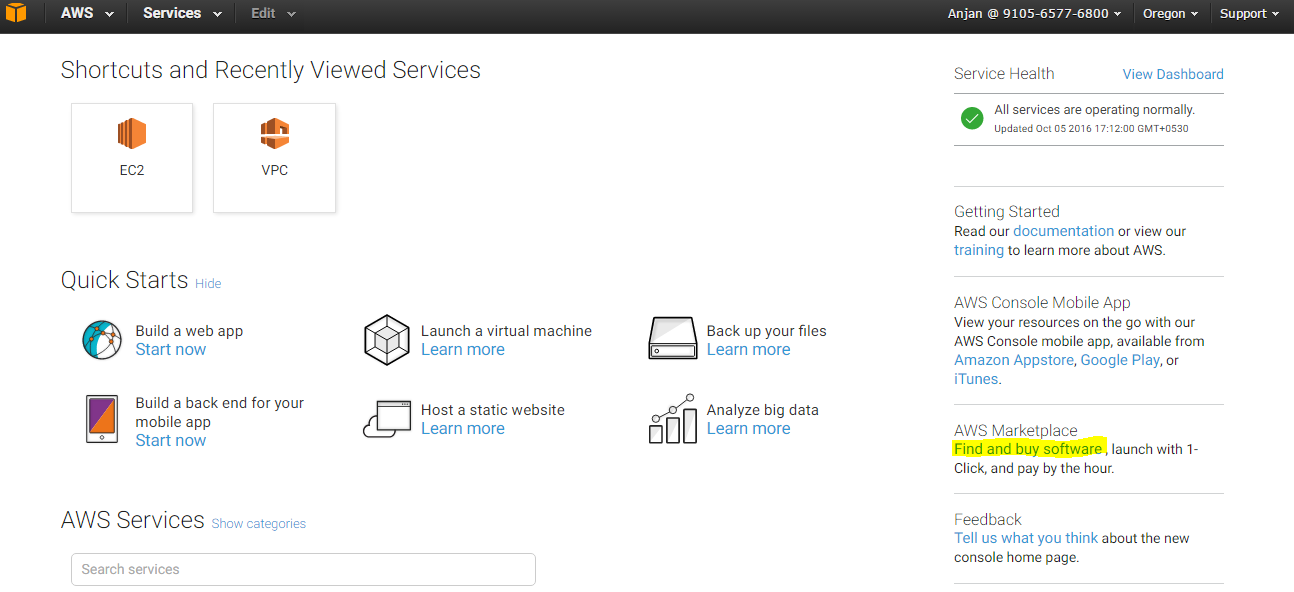
R is a very powerful open source language that comes with thousands of built-in functions. R makes predictive analytics very easy. It also processes thousands of records in seconds and produces the required output.

**Alternatives:**

Python (scipy), Apache Spark ML

4.7. Setup Kony Mobile Fabric (H)

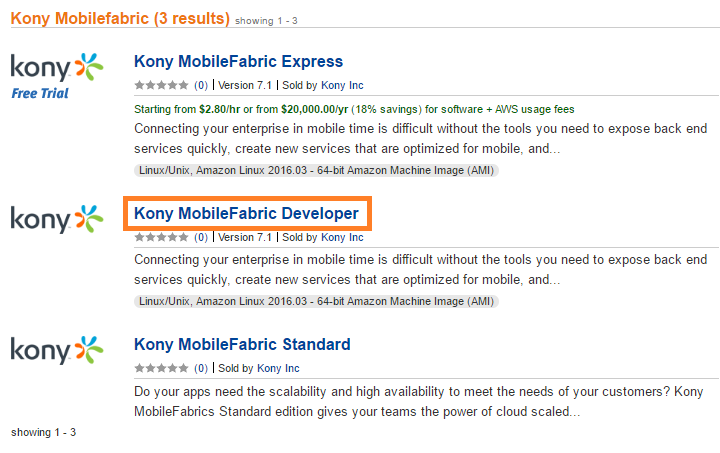
1. Log in to [*https://console.aws.amazon.com/console*](https://console.aws.amazon.com/console).
2. In the right side navigation panel, click on the link **Find and buy software** to open AWS Marketplace.



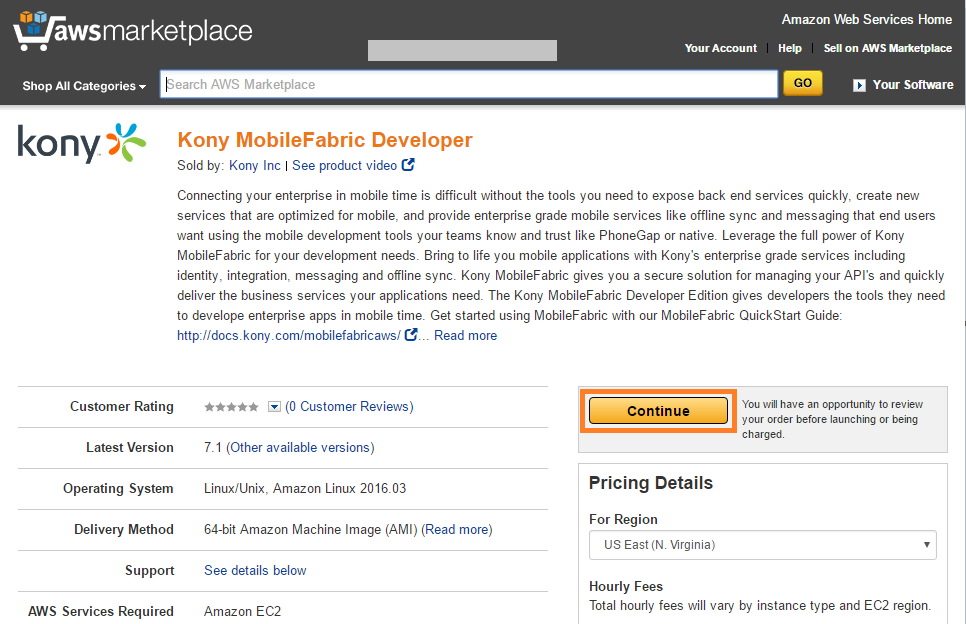
1. Type **Kony MobileFabric** in the search box of AWS Marketplace and click on the **Go** button.



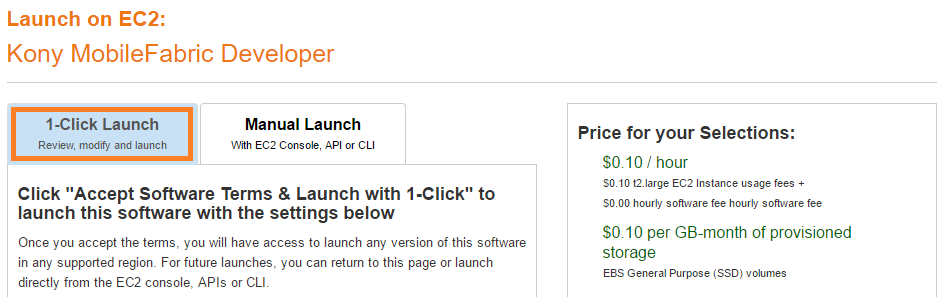
1. Click on **“Kony MobileFabric Developer”** from the search result.



1. Click on the **Continue** button on the product description page of **Kony MobileFabric Developer**.



1. On the Launch on EC2 page, make sure the **1-Click Launch** tab is selected.



1. In the **Version** section, choose the latest version.
2. Select **US-West (Oregon)** as the default region for this project.



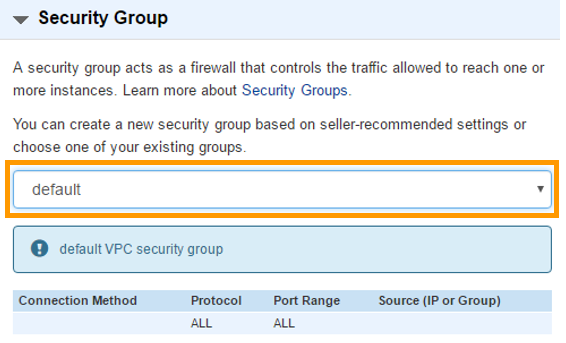
1. Select **t2.large** EC2 Instance type.



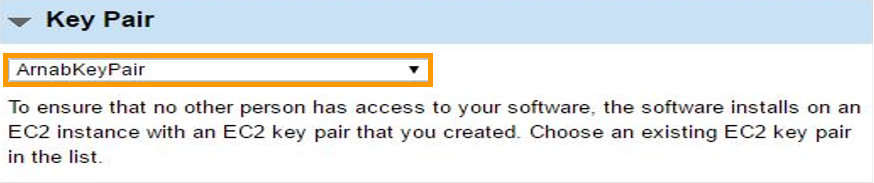
1. Select default **VPC** and default **Subnet**. Default VPC and Subnet are marked with an **asterisk** **“\*”**.



1. Select **default** Security Group.



1. If you haven’t generated your key pair already, follow the steps mentioned in **Section 2 “Generate Your Private Keys” of the Prerequisites** document.
2. Select the generated key pair for **Key Pair** selection box.

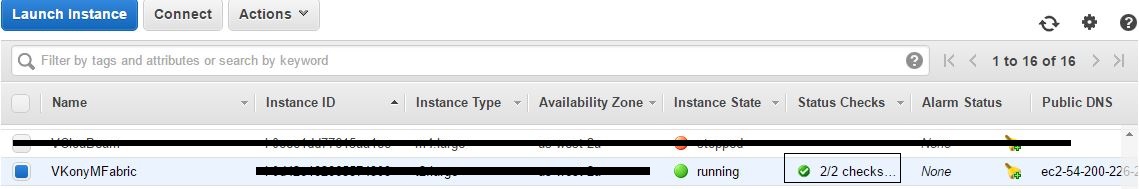


1. Scroll up and click on the **Launch with 1-Click** button to start the **Kony MobileFabric Developer** installation process.

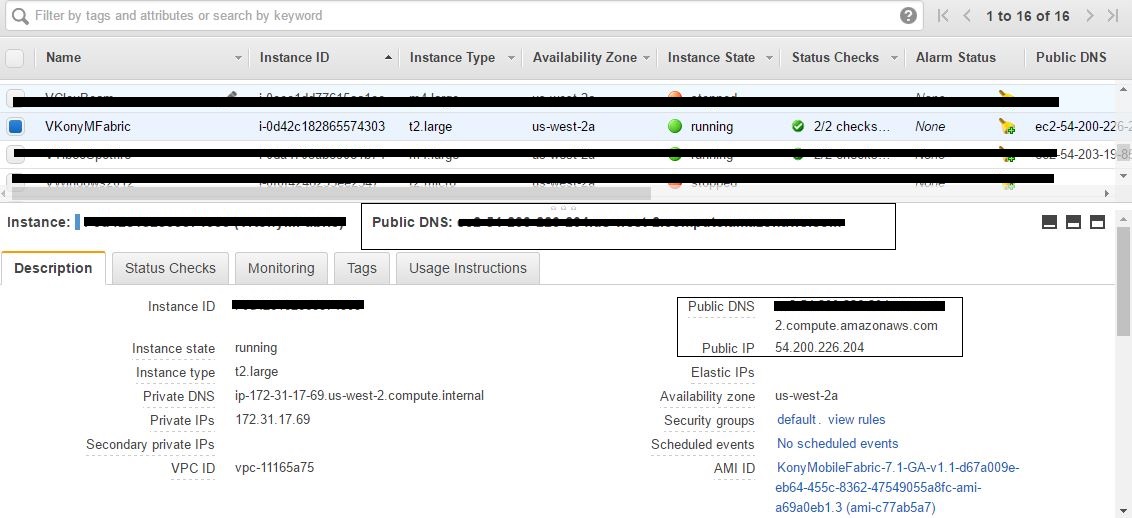


Wait few minutes until the installation completes.

1. Follow the steps mentioned in Section 3 **“Get list of EC2 Instances”** in the **Prerequisites** document to get a newly created **Kony MobileFabric Developer** instance.



1. Click on the instance, then copy the **Public DNS** or **Public IP**.



Check if an SSH client is installed on your local machine by typing **SSH** in the command line of your local machine. Your Linux computer most likely includes an SSH client by default. However, if your computer doesn't recognize the command, the Open SSH project provides a free implementation of the full suite of SSH tools. For more information, go to [http://www.openssh.com](http://www.openssh.com/).

|  |
| --- |
| **For Windows platform**  You can download OpenSSH from the following location:  <https://www.mls-software.com/opensshd.html>.  After installing OpenSSH on a Windows platform, modify the PATH environment variable, by appending the directory path of OpenSSH bin folder. By default, it is C:\Program Files\OpenSSH\bin. |

1. SSH into AWS Linux instance. Execute the command below..

|  |
| --- |
| ssh -i "<Path\_to\_Private\_Key\_File>" ec2-user@<Public\_DNS\_EC2\_Instance> |

* Replace <Path\_to\_Private\_Key\_File> token with the directory path where the Private Key file (file with ‘.pem’ Extention) is stored. Refer to **Section 1.4** of the Prerequisite Document.
* Replace **<Public\_DNS\_EC2\_Instance>** token with Public DNS of AWS Linux Instance that you can obtain from the EC2 dashboard.



1. After a successful connection, you will be asked to provide a Public URL for Kony MobileFabric. Enter the **Public DNS** of Kony EC2 instance and click on the **Enter** button to start the setup of Kony MobileFabric.
2. After a successful setup, the system will provide you with a URL and the credentials details to access the Kony MobileFabric console.

Make a note of the URL for the Kony MobileFabric console for future use.

**Note:** Please do not terminate the Kony MobileFabric instance. If you do, you will need to install and configure the instance again.

**Benefits:**

MobileFabric provides the most robust, comprehensive mobile middleware solution in the industry. It allows customers to rapidly build mobile backend applications that reduce development time, improve reuse, and optimize the mobile client performance. Key features include:

* Object Services
* Backend Services
* API Management
* Integration
* Logic APIs.
* Client SDKs
* Analytics
* Management
* Security

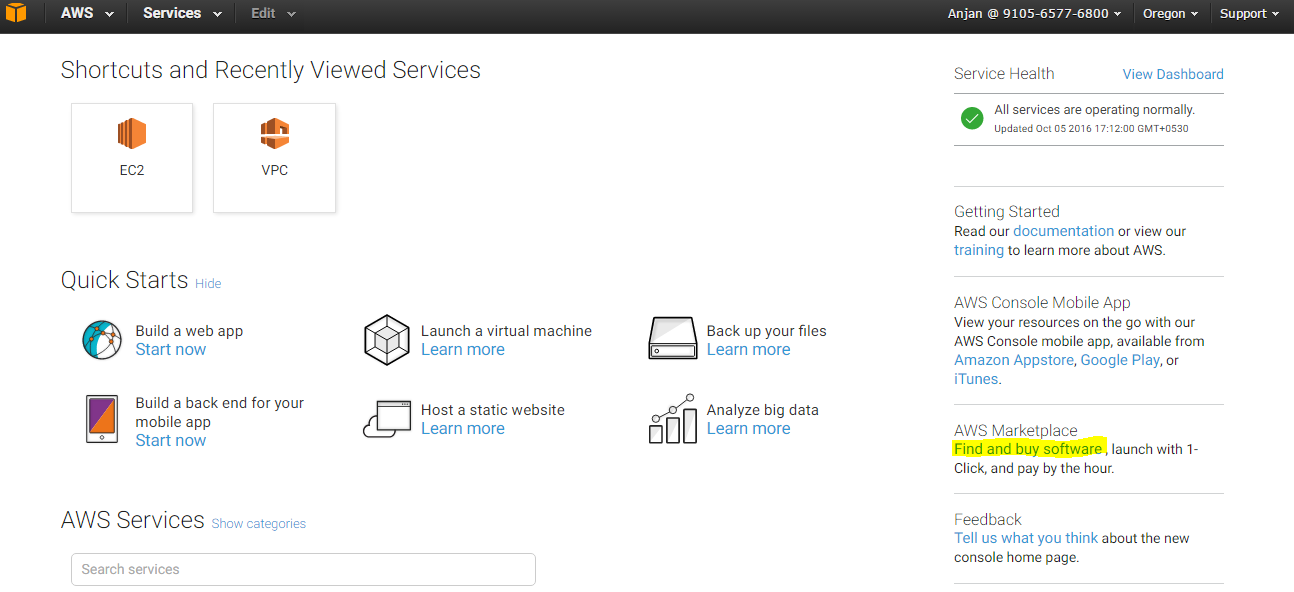
**Alternatives:**

Kumulos, Kinley, Backendless, Google Mobile Backend

4.8. Trend Micro Deep Security (I)

4.8.1. Launch Instance

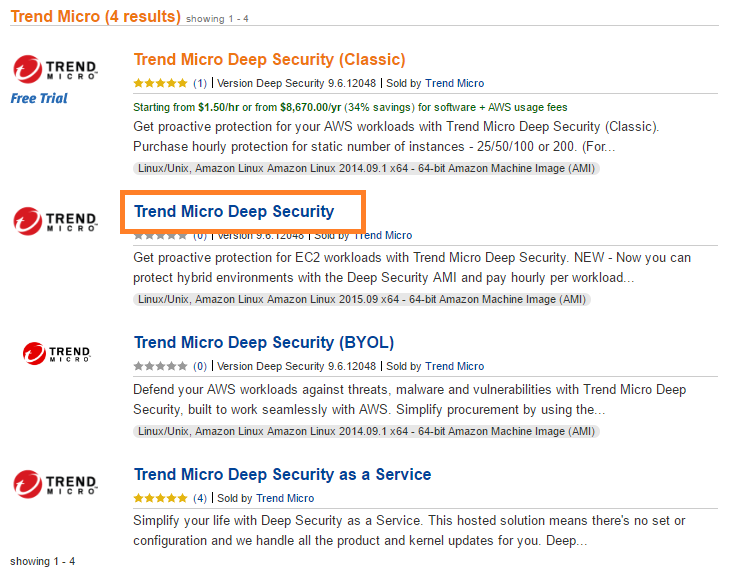
1. Log in to [*https://console.aws.amazon.com/console*](https://console.aws.amazon.com/console).
2. In the right navigation panel, click on the link **Find and buy software** to open AWS Marketplace.



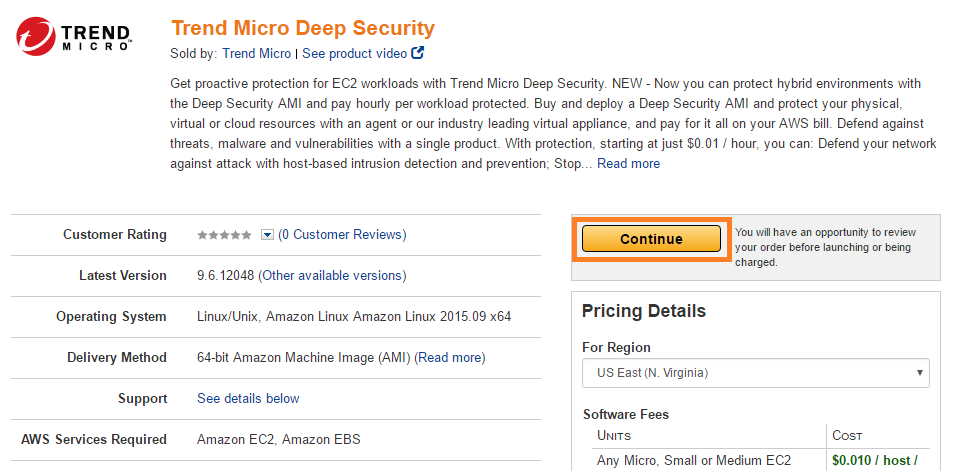
1. Type **Trend Micro** in the search box of AWS Marketplace and click on the **Go** button.



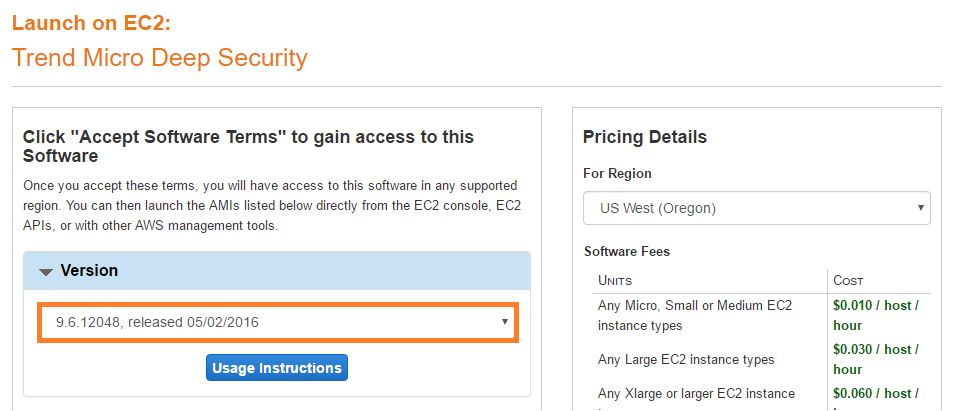
1. Click on **“Trend Micro Deep Security”** from the search result.



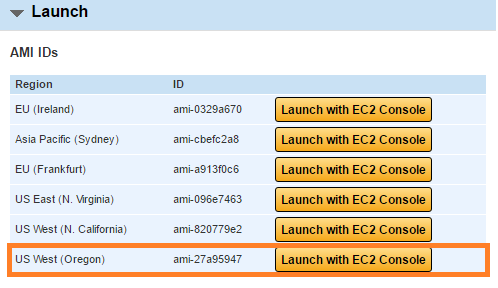
1. Click on the **Continue** button on the product description page of **Trend Micro Deep Security**.



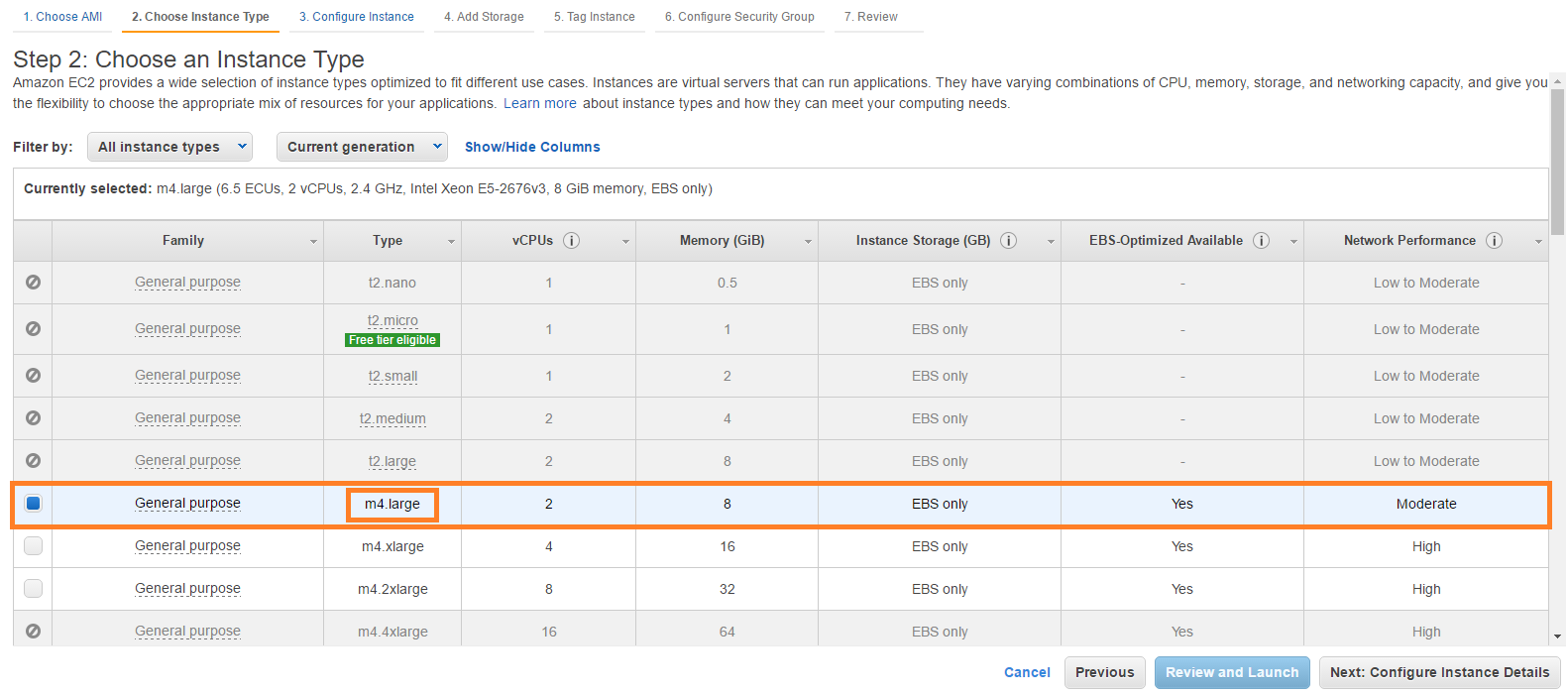
1. On the **Launch on EC2** page select the latest version of **Trend Micro Deep Security**.



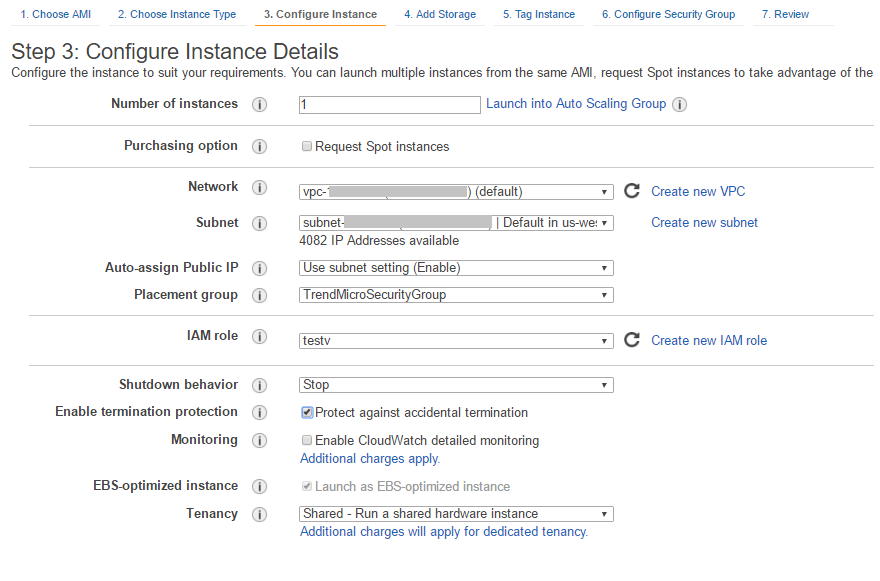
1. In the Launch section, click on the **Launch with EC2 Consol**e button next to the region **US West (Oregon)**.



1. On the Launch Instance Wizard page, **Choose an Instance Type** tab will be opened.
2. Check the check box next to the **m4.large** instance type.

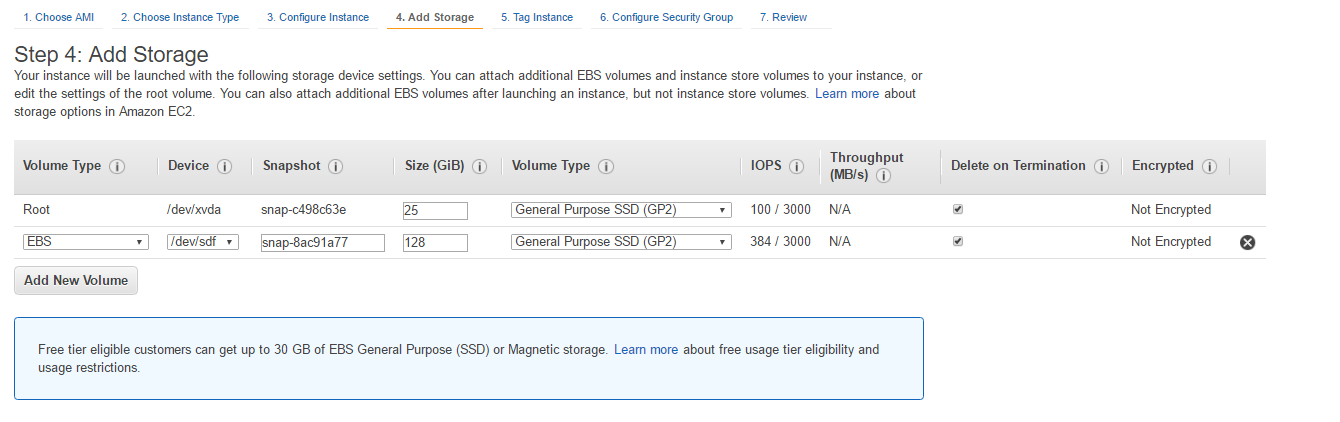


1. Click on the **Next: Configure Instance Details** button located in the lower right corner of the page.
2. Set the properties as shown below on the **Configure Instance** tab:



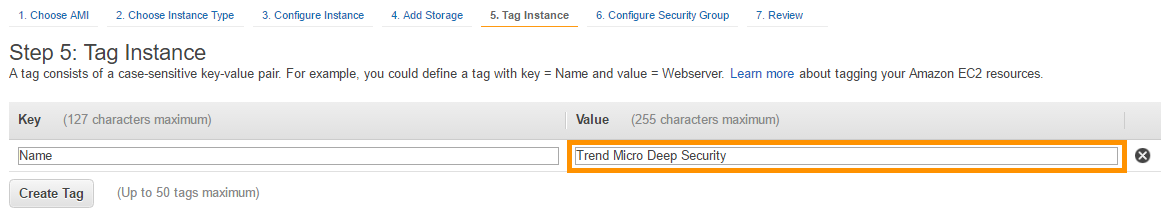
* Number of instances: **1**
* Network: **Default VPC**
* Subnet: **Default subnet**
* Auto-assign Public IP: Select **Use subnet setting (Enable)**
* Placement Group: Create new Placement group or create new
* IAM Role: Assign existing role or create new appropriate role
* Shutdown Behavior: Select **Stop** option for this property
* Enable termination protection: Check the check box **Protect against accidental termination**
* Tenancy: Select **Shared –- Run a shared hardware**

1. Click on the **Next: Add Storage** button located at the bottom of the page.
2. On the **Add Storage** tab, you can extend storage capacity by adding a new Volume Size. Click on the **Add New Volume** button.



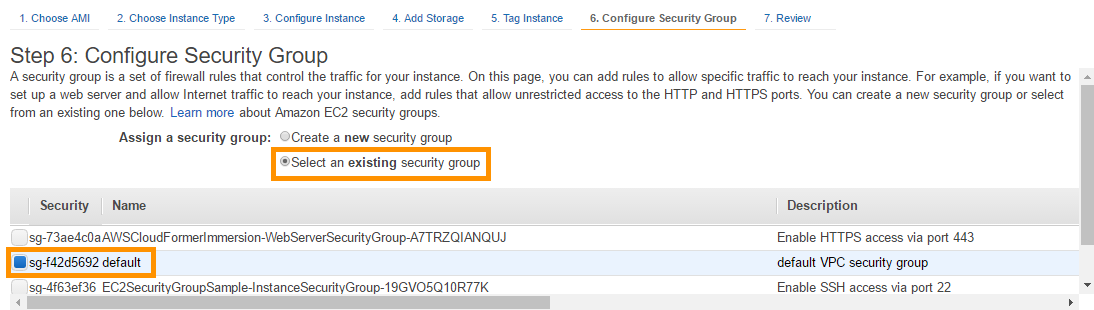
1. Click on the **Next: Tag Instance** button located at the bottom of the page.
2. The **Tag Instance** tab allows you to provide additional metadata to resource.

Type in the appropriate name for the Key and a Value. Click on the **Create Tag** button.

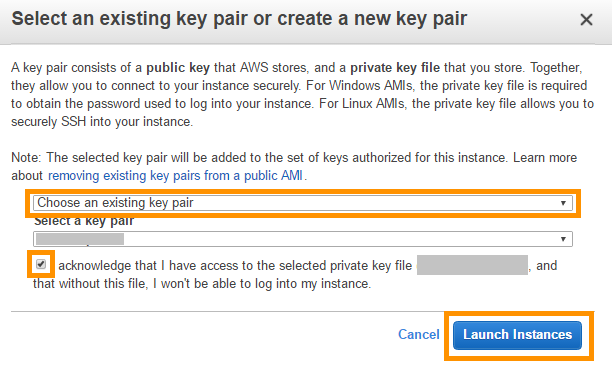


1. Click on the **Next: Configure Security Group** button located at the bottom of the page.
2. On the **Configure Security Group** tab you can assign an existing Security Group or create a new Security Group.

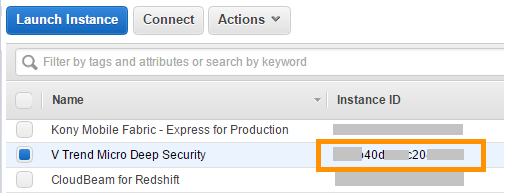
Now set the existing **Default** Security Group for this instance.



1. Click on the **Review and Launch** button located at the bottom of the page.
2. Check all the properties set for this instance on **Review** tab; click on the **Launch** button if everything is correctly set to create a new instance of Trend Micro Security.
3. In the popup window, to set the Private Key for an instance, select an **existing key pair** created in the **Prerequisite** document.

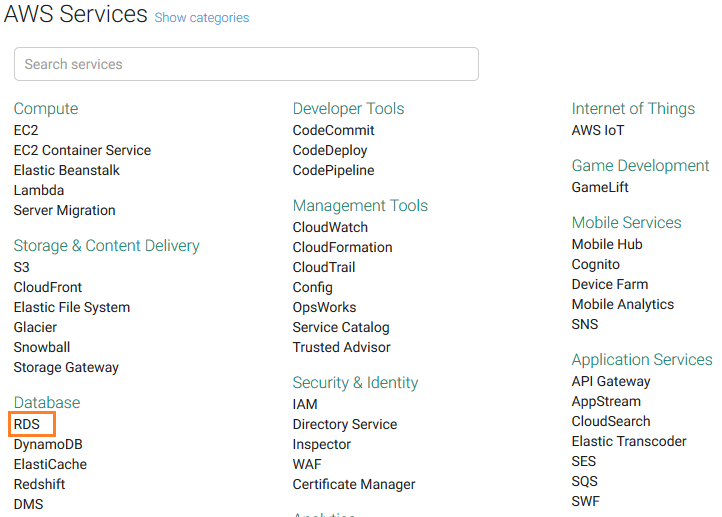


1. Check the box for acknowledging you have access to the private key file of the selected key pair.
2. Click on the **Launch Instances** button to launch the instance. Wait for a few minutes to get this instance initialized.
3. Go to the EC2 instance list and make note of the Instance ID of the Trend Micro Deep Security instance created in this section.

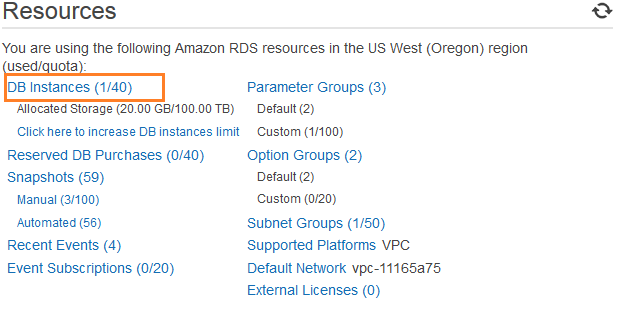


4.8.2. Launch RDS Database

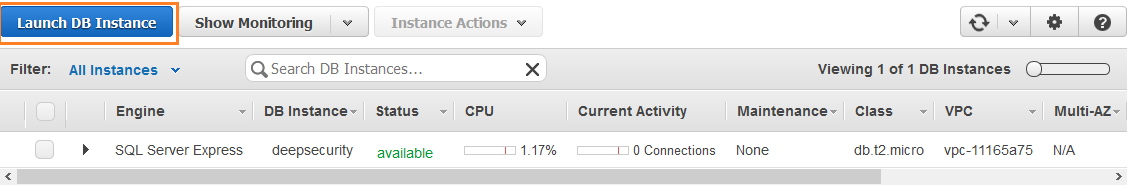
1. Log in to [*https://console.aws.amazon.com/console*](https://console.aws.amazon.com/console).
2. Select **RDS** under Database in the **AWS Services** window.



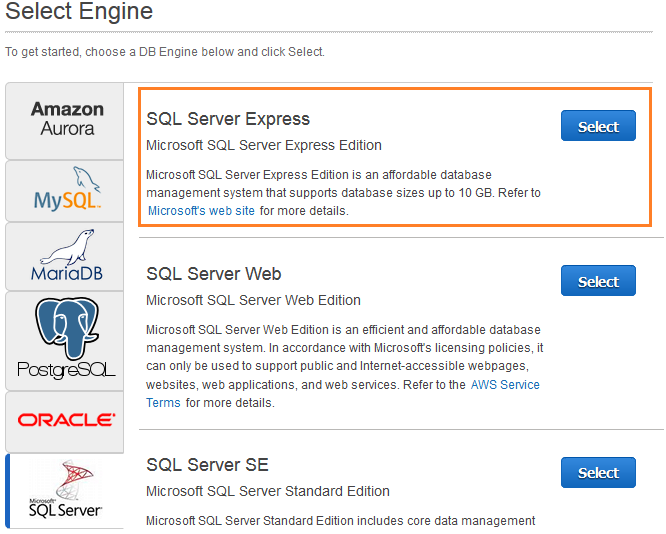
1. Click on the link **DB Instances** in the **Resources** section of the RDS Dashboard.



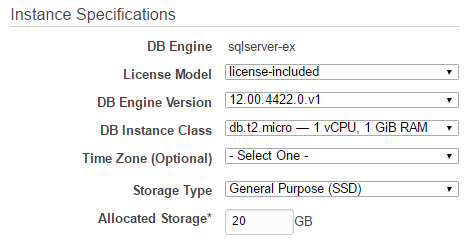
1. Click on the **Lunch DB Instance** button.



1. Select **SQL Server** **Express** and Select the **SQL Server Express** Edition to deploy.

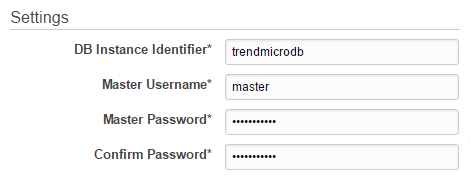


1. On **the Specify DB Details tab**, set Instance Specifications:

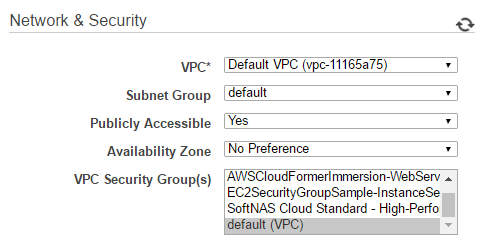


* License Model: license-included
* DB Engine Version: 12.00.4422.0.v1
* DB Instance Class: db.t2.micro
* Storage Type: General Purpose (SSD)
* Allocated Storage: 20 GB

1. On the **Specify DB Details** tab, set the value for the DB Instance Identifier, Master Username, and Master Password. Then click on the **Next Step** button located at the bottom of the page.

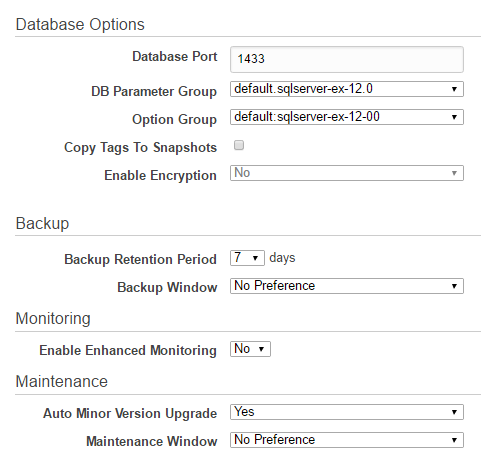


1. On the **Configure Advanced Settings** tab, set the **Network and Security** settings:

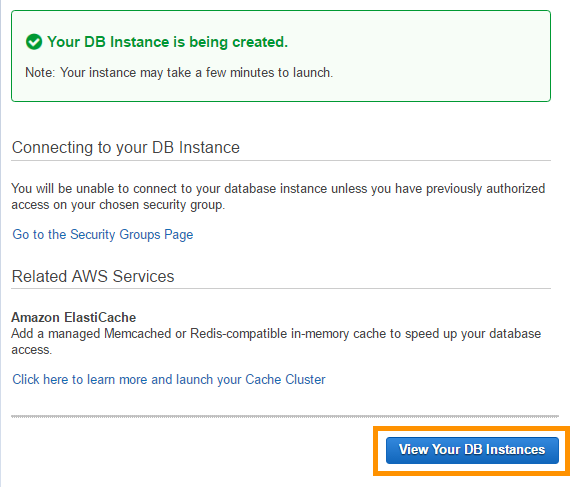


* VPC: **Default**
* Subnet Group: **default**
* Publicly Accessible: **Yes**
* Availability Zone: **No Preference**
* VPC Security Group(s): **default (VPC)**

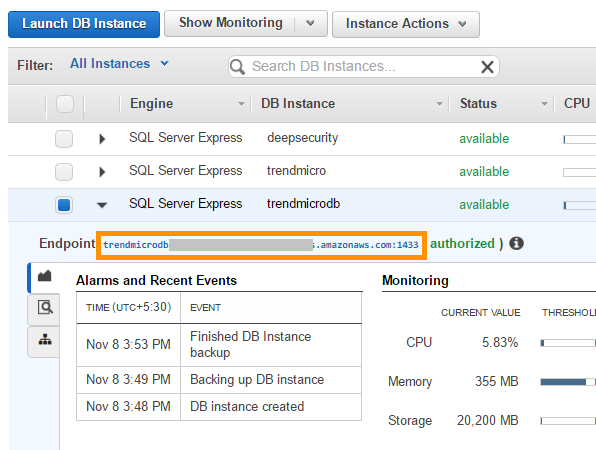
1. Keep the **default values** for the settings in the Database Options, Backup, Monitoring, and Maintenance sections.



1. Click on the **Launch DB Instance** button located at the bottom of the tab to launch the instance of the **SQL Server**.
2. Wait a few minutes to launch the instance and click on **View Your DB Instance** to check its status.



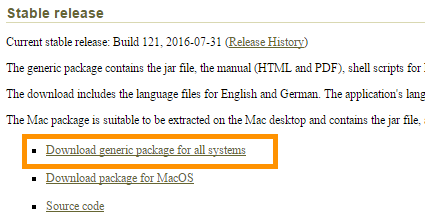
1. Select and expand the SQL Server instance created in this section.
2. Copy the **Endpoint** of the SQL Server instance.



4.8.3. Create Database in SQL Server

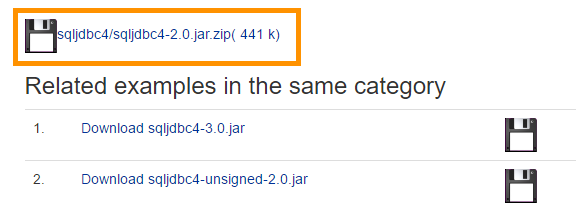
**The SQL Workbench** tool can be used to create a Database in the SQL Server

1. Click on the URL <http://www.sql-workbench.net/downloads.html> in the browser of your local machine to download the SQL Workbench installation package.
2. Select the **Download generic package for all systems** located in the **Stable Release** section to start downloading the installation package.

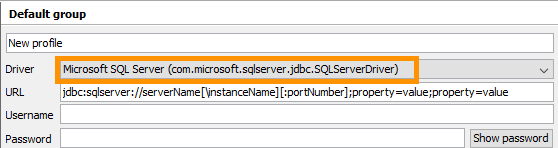


The generic package contains the jar file, the manual (HTML and PDF), shell scripts for Linux/Unix systems to start the application, as well as a Windows® [launcher](http://www.sql-workbench.net/manual/install.html#launcher-using) and sample [XSLT](http://www.sql-workbench.net/xslt.html) scripts.

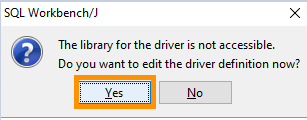
1. Unzip the compressed file.
2. Click on the URL <http://www.java2s.com/Code/Jar/s/Downloadsqljdbc420jar.htm> in your browser to open the download page for **sqljdbc4-2.0.jar**.
3. Scroll down to the bottom of the page.
4. Click on the link for downloading the compressed file containing **sqljdbc4-2.0.jar**.



1. **Unzip** the compressed file.
2. Open the **SQL Workbench** tool using the appropriate file according to your Operating System.
3. In the Connect Window, select the **Microsoft SQL Server** driver.



10. Click on the **Yes** button in the Message Box to set the definition for the driver.

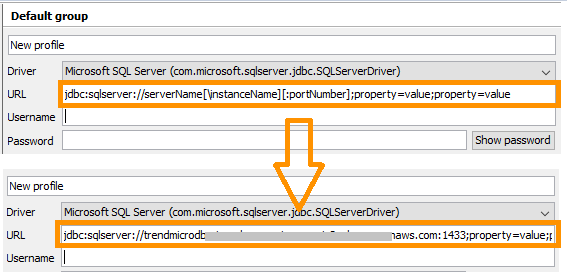


11. Click on the **Browse** button in the Manage Drivers window. Select the **sqljdbc4-2.0.jar** file present in the folder that was obtained in **Step 7** of this section.



12. Click on the **OK** button to close the Manage Drivers window.

13. In the Connection Window, replace the substring **serverName[\instanceName][:portNumber]** in the URL box with the **Endpoint string of SQL Server** (refer to **Step 13** of **Section** **4.8.2. Launch RDS Database).**



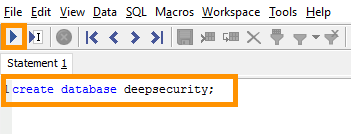
14. Type in the **Username** and **Password** of the SQL Server that you set in **Step 7 of Section 4.8.2. Launch RDS Database**.

15. Click on the **Test** button at the bottom of the Connection Window to confirm the connection settings.

16. Click on the **OK** button.

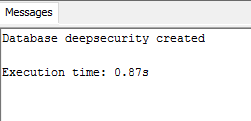
17. In the SQL Query window, type in the statement below and execute it to create the database.

create database deepsecurity;



Make note of the name of the database for future use.

18. The message below in the Message pane shows the successful creation of a database.



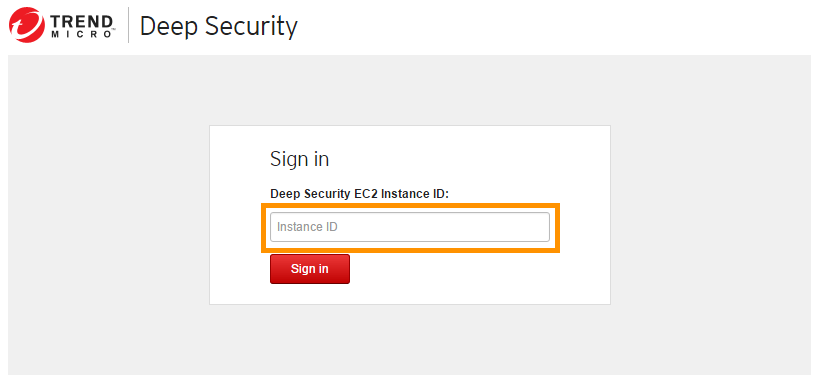
4.8.4. Install Deep Security Manager

1. Click on the URL below in the browser of your local machine. However, replace the token **<Public\_IP\_Trend\_Micro\_Deep\_Security\_Instance>** with the Public IP of Trend Micro Deep Security instance created in **Section 4.8.1: Launch Instance**

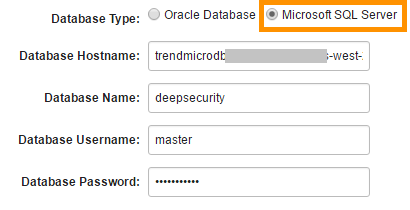
*https://****<Public\_IP\_Trend\_Micro\_Deep\_Security\_Instance>****:8080*

Generally, a privacy error warning due to a self-signed SSH certificate will pop up. Bypass this for now and continue browsing.

1. Type in the Instance ID of the Micro Trend Deep Security instance (created in **section 4.8.1: Launch Instance**) in the input box of the Sign In page for the Deep Security instance and click on the **Sign In** button.

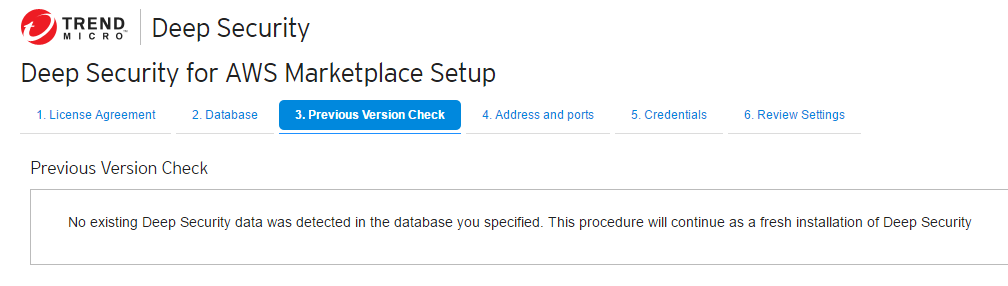


1. Accept the **License Agreement** after a successful login. Click on the **Next** button.
2. On the Database tab, set the connection properties for the SQL Server you created in **Section 4.8.2. Launch RDS Database.**



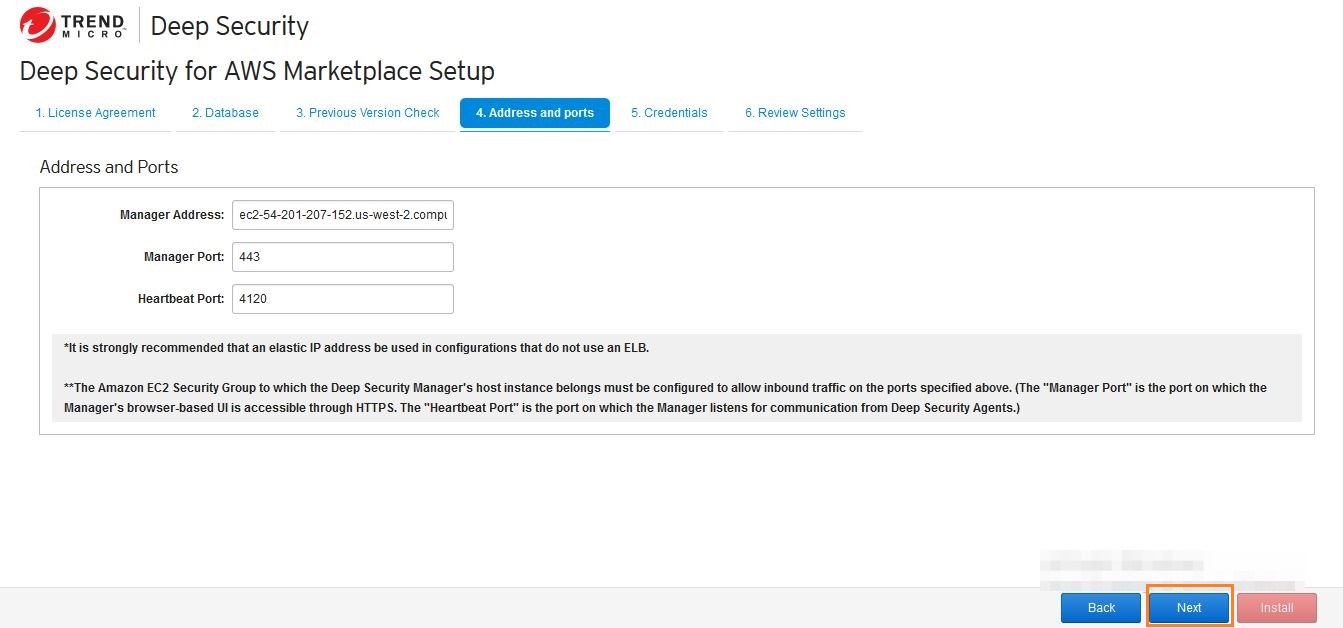
* Database Type: **Microsoft SQL Server**
* Database Hostname: Enter **Endpoint of SQL Server** (refer to **Step 13 of Section 4.8.2 of Launch RDS Database**), but remove colon **“:”** and Port Number present at the end of string.
* Database Name: Enter the name of the database created in **Step 17 of Section 4.8.3: Create Database in SQL Server.**
* Enter the Username and Password of the SQL Server (that was setup in **Step 7 of Section 4.8.2. Launch RDS Database**) in **Database Username** and **Database Password** fields respectively.

1. Click on the **Next** button.
2. Skip the Previous Version Check tab and move to the next tab.

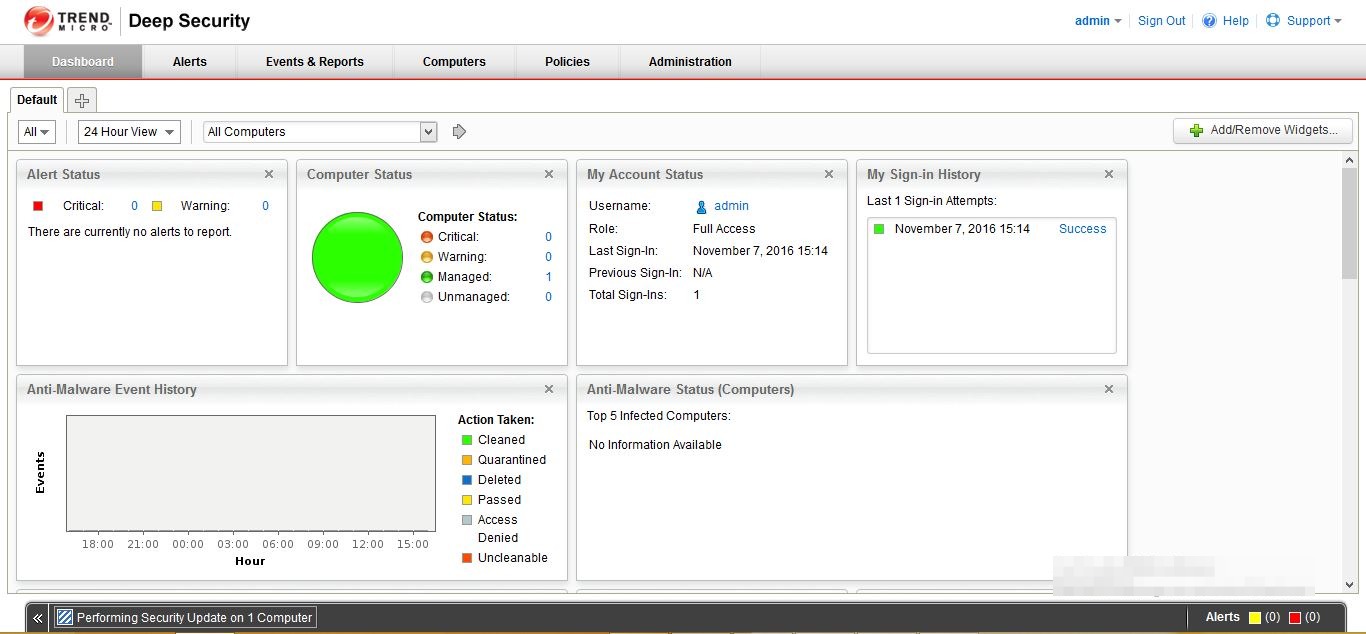


1. On the **Address & Ports** tab**,** keep the default properties.

Make note of the **Manager Address**, **Manager Port,** and **Heartbeat Port.** Click on the **Next** button.

****

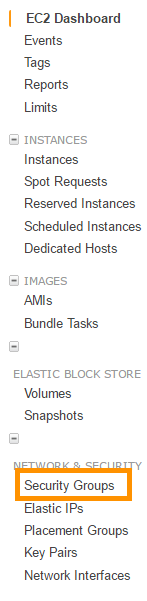
1. On the **Credentials** tab, type in the appropriate Username and Password. Make note of these credentials for future use and go to the next tab.
2. On the **Review Settings** tab, check all the properties and, if all properties are set correctly, click on the **Install** button at the bottom.
3. Wait for a few minutes until the Deep Security Manager gets installed.
4. After a successful installation, a new page will open with the message “**Your Connection is not secure**”. Ignore this message and continue browsing.
5. On the **Sign In** page, type in the credentials of the Deep Security Manager set in **Step 7** of this section. Sign In.
6. The **Deep Security** dashboard will open in your browser.



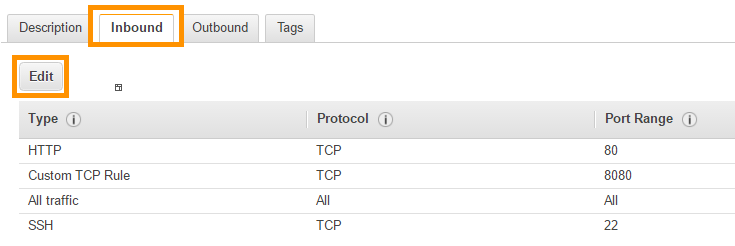
4.8.5. Modify your AWS Security Group to open required ports on your instances

This section modifies the Security Group so that instances attached to a group can be protected with Deep Security. Add the Inbound Rule for **Manager Port** and **Heartbeat Port** in the Security Group, obtained in **Step 7** of **Section 4.8.4: Install Deep Security Manager**.

1. Go to **EC2 Dashboard** and click on the **Security Groups** link that is grouped under **NETWORK & SECURITY** in the left navigation pane.



1. Select the existing Security Group or create a new Security Group.
2. On the **Inbound** tab, choose **Edit**.



1. In the dialog box, choose **Add Rule**.
2. Select **HTTPS** from the **Type** drop down list and leave the source as **Anywhere** (0.0.0.0/0).



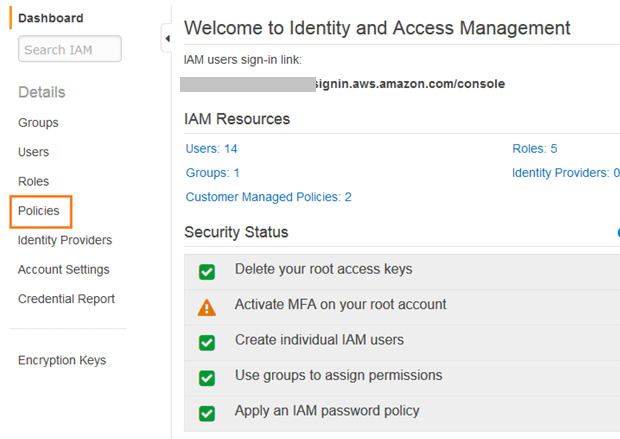
1. In the dialog box, choose **Add Rule**.
2. Select Custom TCP Rule from Type drop down list. Type in the port number of **HeartBeat** **Port** and select **Anywhere** from the Source list.



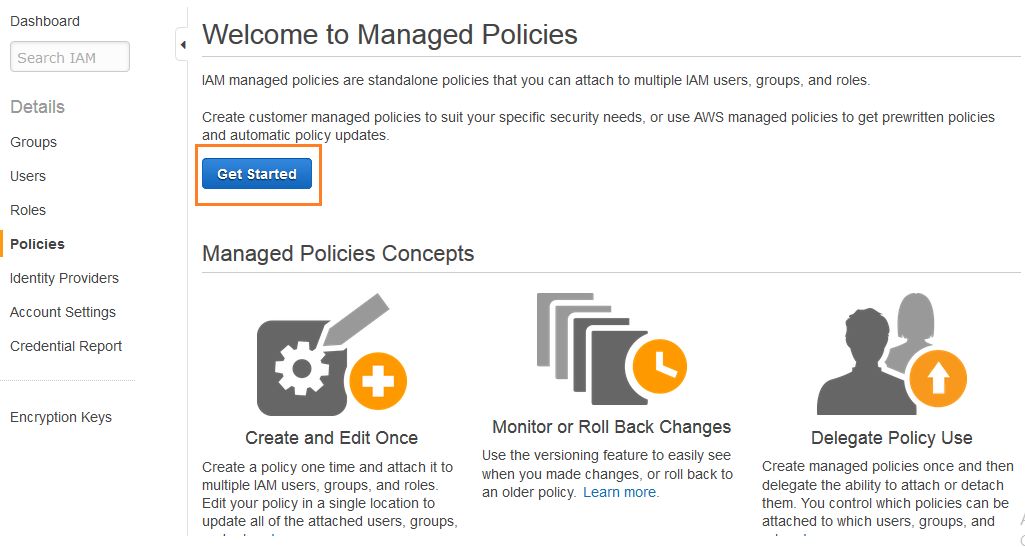
1. Click on the **Save** button to finalize your editing and save the added rules.

4.8.6. Create a dedicated AWS policy and user account for Deep Security to access your cloud account

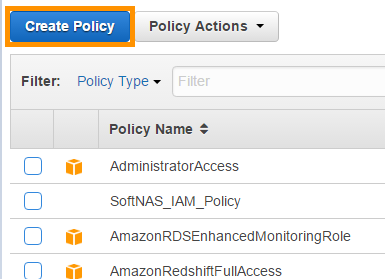
1. Log in to the **IAM Dashboard** <*https://console.aws.amazon.com/iam/home>*
2. In the left navigation pane, click on **Policies**.



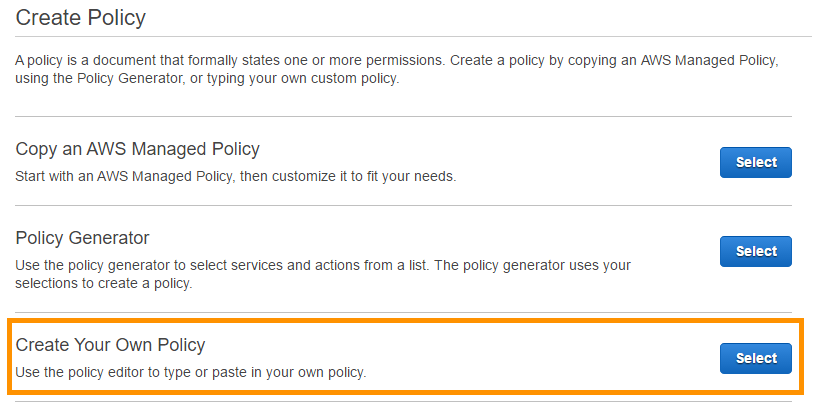
1. If this is your first time on this page, you'll need to click on Get Started.



1. Click on the **Create Policy** button.



1. Select **Create Your Own Policy**.



1. Give the policy a name and description, then copy the following JSON code into the **Policy Document** area:

{

"Version":"2012-10-17",

"Statement":[

{

"Sid":"cloudconnector",

"Effect":"Allow",

"Action":[

"ec2:DescribeImages",

"ec2:DescribeInstances",

"ec2:DescribeRegions",

"ec2:DescribeSubnets",

"ec2:DescribeTags",

"ec2:DescribeVpcs",

"iam:ListAccountAliases",

"sts:AssumeRole"

],

"Resource":[

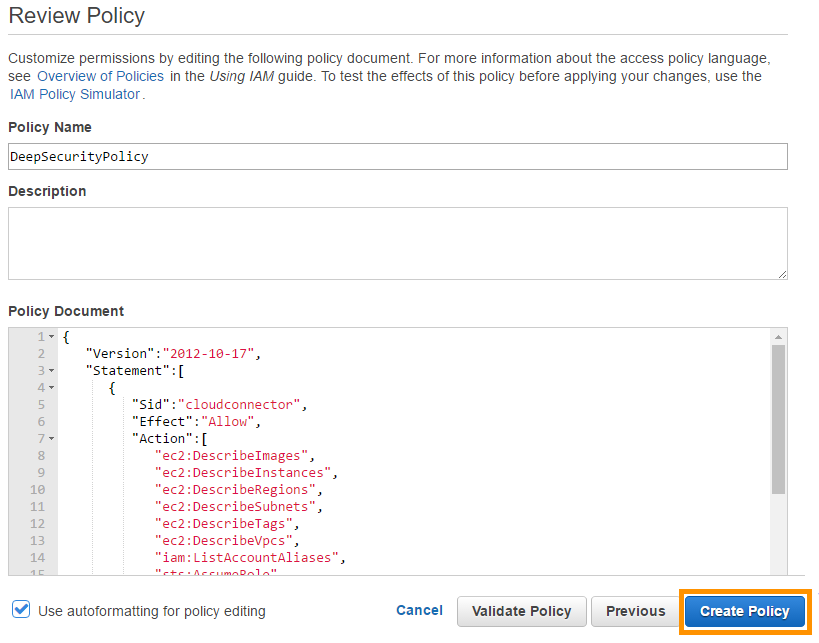
"\*"

]

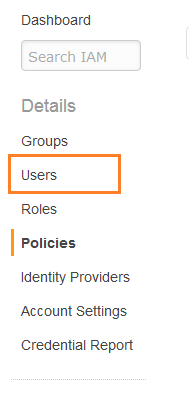
}

]

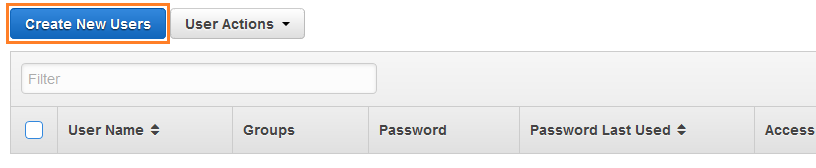
}



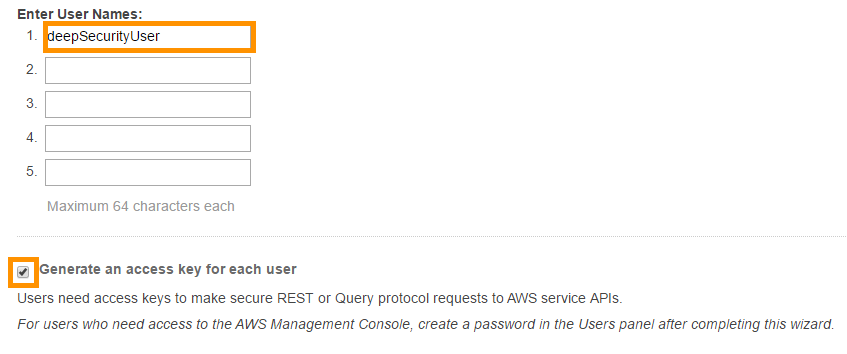
1. Click on the **Create Policy button.** Your policy is now ready to use.
2. On the Identity and Access Management page's navigation pane, click on **Users**.



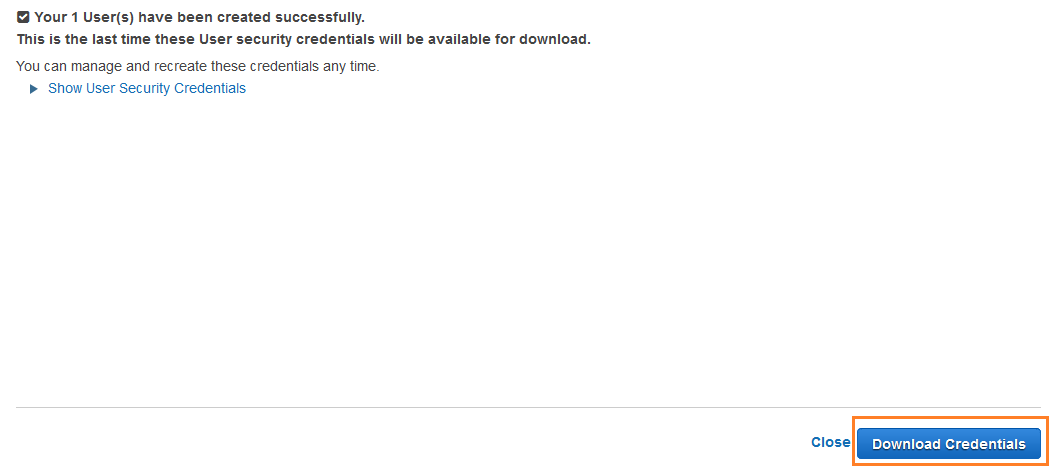
1. Click **Create New Users** to display the **Create User** page.



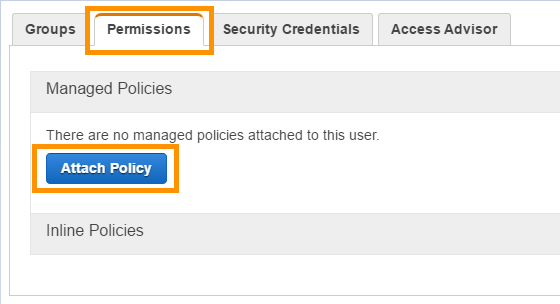
1. Enter a username and select the **Generate an access key for each User** option.



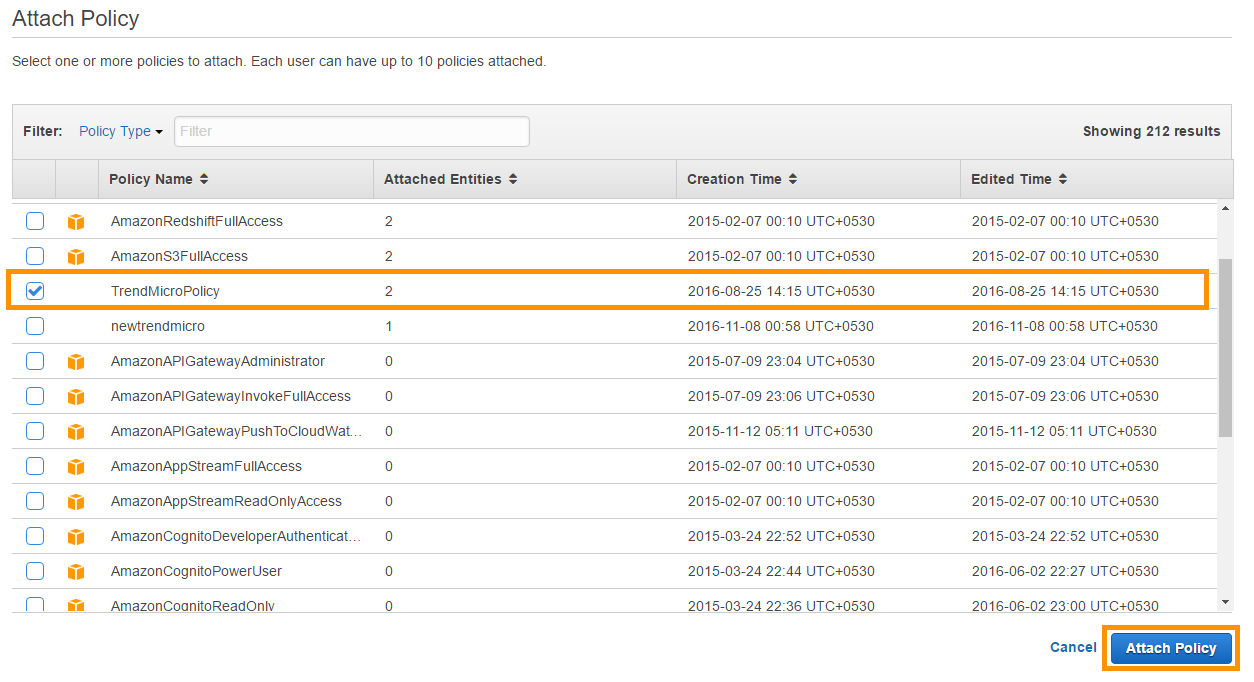
1. Click on the **Create** button located at the bottom of the Create User window.
2. Click on **Download Credentials** to download the generated User Security credentials (Access Key and Secret Key) and then click on the **Close** button to close the dialog window.



1. Back on the Users page, click on the User created in previous steps to display the User properties, then select the **Permissions** tab.



1. In the expanded **Permissions** section, click on **Attach Policy** at the bottom of the window to display the **Attach Policy** page.
2. Select the Policy you just created and click **Attach Policy** to apply the policy to the new user account.

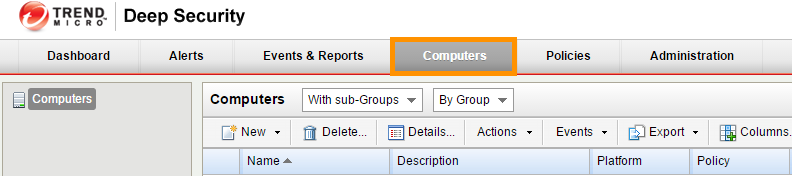


The Amazon Web Services account is now ready for access by a Deep Security Manager.

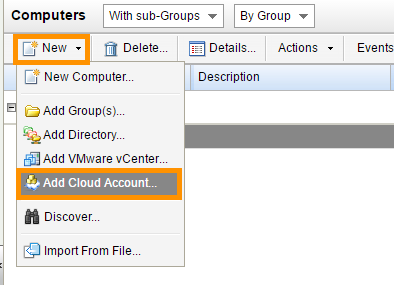
4.8.7. Adding your AWS Cloud account to Deep Security

1. Sign in to the Trend Micro Deep Security Manager and click on the Computers tab.

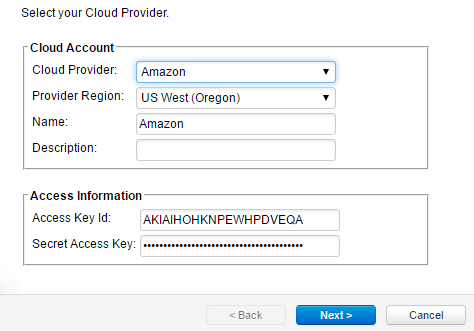
(For the URL of Trend Micro Deep Security Manager refer to **Step 8** of **section 4.8.4: Install Deep Security Manager)**



1. Click on the **New** dropdown menu and select **Add Cloud Account**.

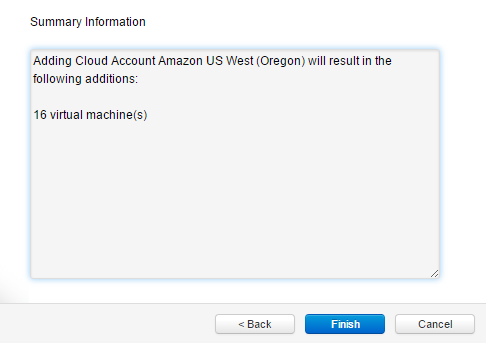


In **Add Cloud Account Wizard** enter the following information, then click **Next**.

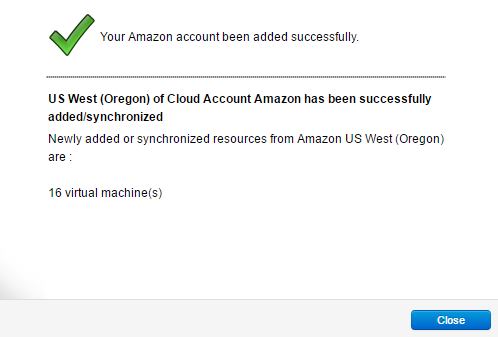


* **Cloud Provider**: Amazon
* **Provider Region:** Select the region where your AWS instances are hosted. (If you have instances hosted in multiple regions, you'll have to add a Cloud Account for each region.)
* **Name and Description:** Enter the name and description of the resources you are adding. These are only used for display purposes in the Deep Security Manager.
* **Access Key Id and Secret Access Key:** These are the credentials generated for the AWS user account you created specifically for Deep Security. Get these keys from the file downloaded in **Step 12** of **Section 4.8.6,** and **create** a dedicated AWS policy and user account for Deep Security to access your cloud account.

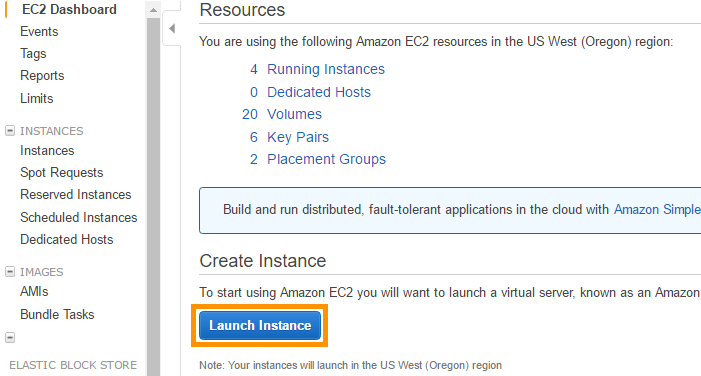
1. Deep Security Manager will verify the connection to the AWS cloud account and display a summary of the import action. Click on the **Finish button**.



1. When it's done importing your AWS instances, the wizard will display the results of the action.



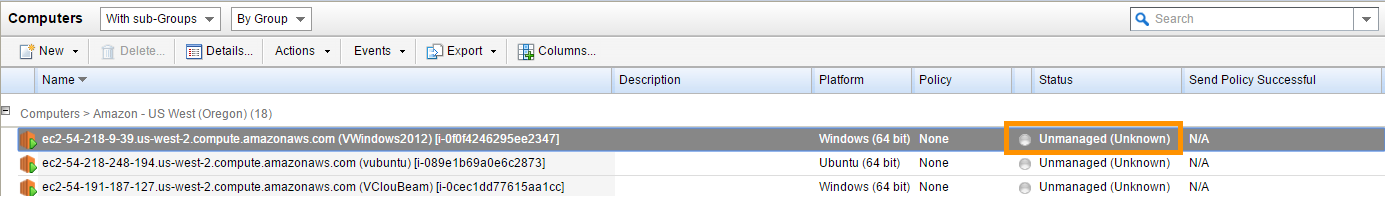
1. Your AWS instances now appear in the Deep Security Manager under their own branch under the Computers tab in the navigation panel.
   * 1. Deploy Deep Security Agents to your Windows AWS instance
2. Create a Windows AWS Instance
3. Navigate to [*https://console.aws.amazon.com/ec2*](https://console.aws.amazon.com/ec2).
4. Click on the **Launch Instance** button on the EC2 dashboard page.



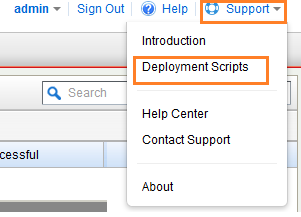
1. Launch a new windows instance with the following properties:

* **Operating System**: Microsoft Windows Server 2012 R2 Base (64 bit)
* **VPC and Subnet:** Default
* **Security Group:** The same Security Group specifically modified for Deep Security

1. This newly-created windows instance will appear in the Computers List of the Deep Security Manager with status Unmanaged (Unknown).

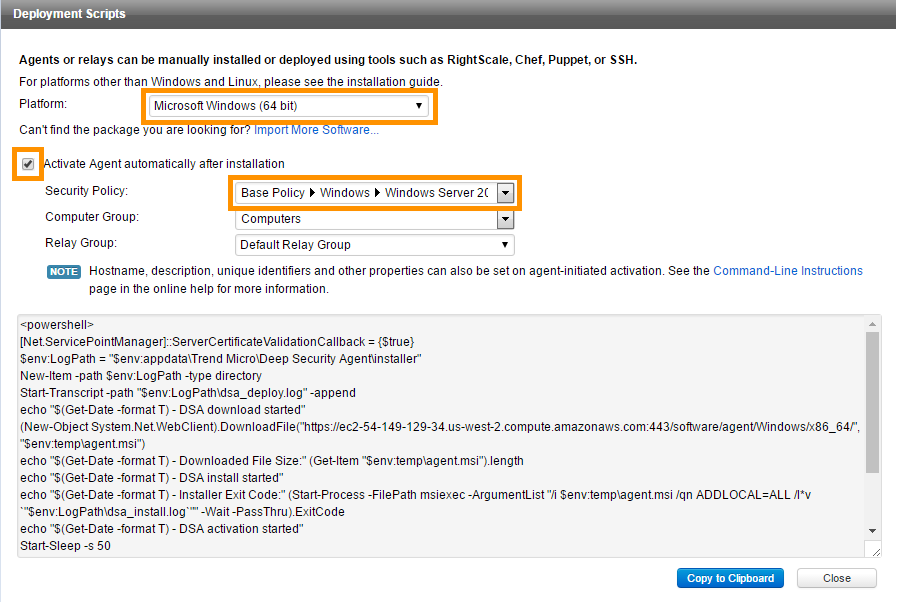


1. In the top right corner of Deep Security Manager, click on the **Support** dropdown menu and select the **Deployment Scripts** link.

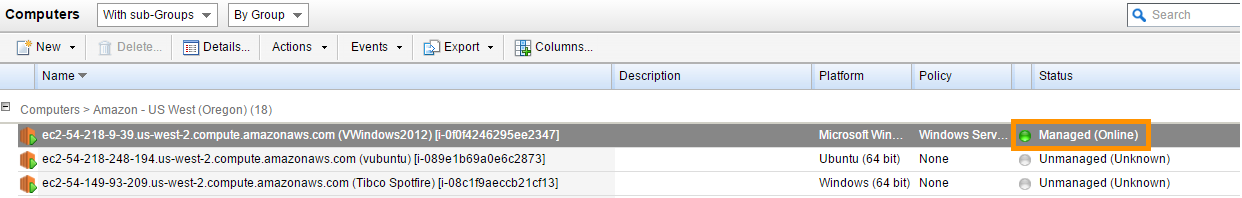
****

1. In the Deployment Scripts window:

* Select **Platform** Microsoft Windows (64 bit)
* Select the **Activate Agent Automatically** option
* Select **Security** **Policy** for Windows Server 2012 Operating System
* Leave the other options at their default settings. As you make the selections, the Deployment Script Generator will generate a PowerShell script for Windows that you will run on your Deep Security instance.



1. Click on the **Copy to Clipboard** button to copy the script to your clipboard.
2. Use the Remote Desktop Connection to AWS Windows Instance launched in **Step 1 of this section**.
3. Start Windows PowerShell ISE (in administrator mode) on a remotely-connected AWS Windows Instance.
4. Paste the script from your clipboard into PowerShell and run it.
5. After a successful execution of the script, wait a few minutes and check the status of the AWS Windows Instance in the Computers list of Deep Security Manager. It will change to Managed (Online).

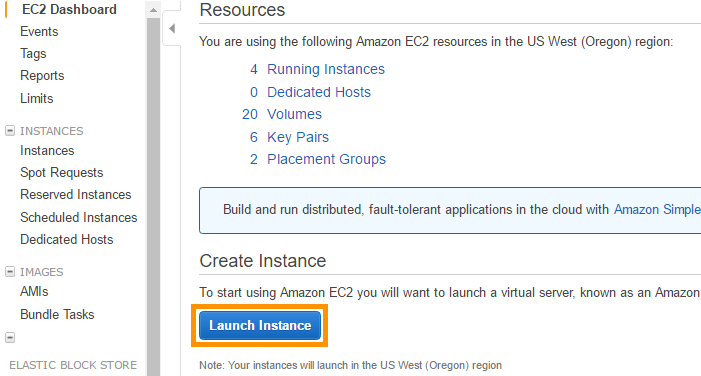


Likewise, you can secure other existing and new AWS Windows instances by using the PowerShell script generated according to the Platform and Operating System of instance.

* + 1. Deploy Deep Security Agents to your Linux AWS instance

Create a Linux AWS Instance.

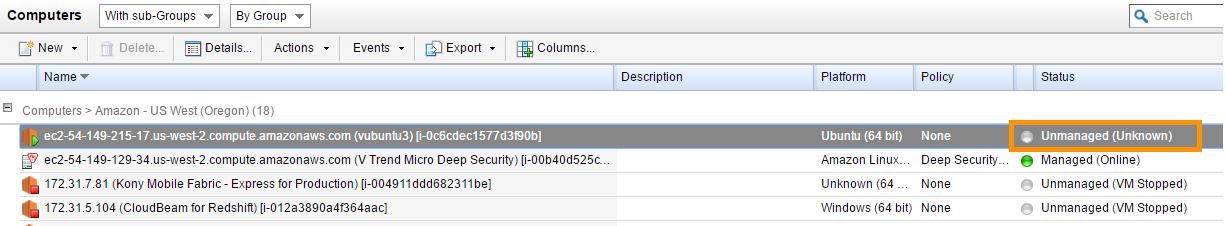
1. Navigate to [*https://console.aws.amazon.com/ec2*](https://console.aws.amazon.com/ec2)
2. Click on the **Launch Instance** button on the EC2 Dashboard Page.



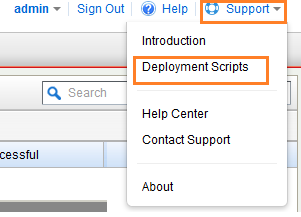
1. Launch a New Linux instance with the following properties:

* **Operating System**: Ubuntu Server 14.04 LTS (HVM) (64 bit).
* **VPC and Subnet:** Default.
* **Security Group:** The same Security Group specifically modified for Deep Security.

1. This newly-created Linux instance will appear in the Computers List of the Deep Security Manager with a status of Unmanaged (Unknown).



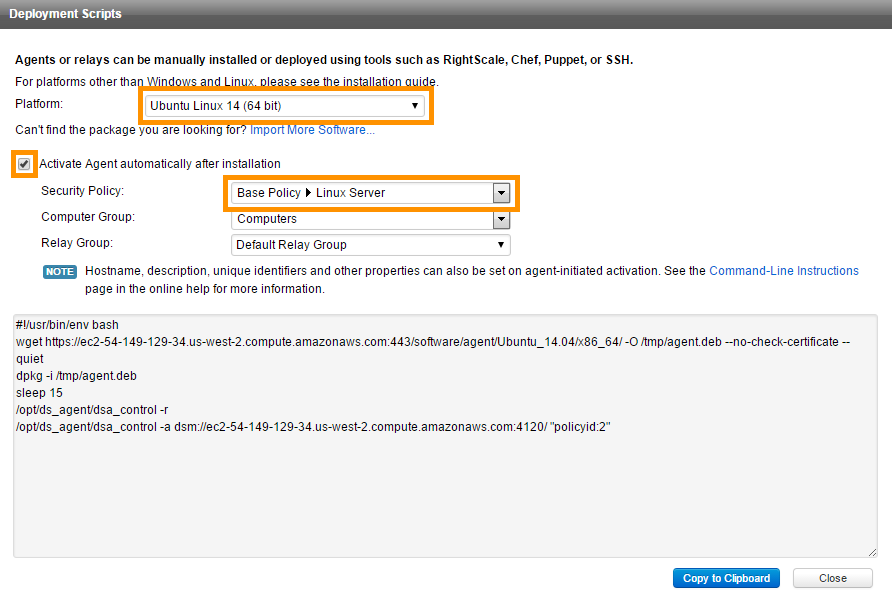
1. In the top right corner of the Deep Security Manager, click on the **Support** dropdown menu and select the **Deployment Scripts** link.

****

1. In the Deployment Scripts window:

* Select **Platform** Ubuntu Linux 14 (64 bit).
* Select the **Activate Agent Automatically** option.
* Select **Security** **Policy** for Linux Server Operating System.

Leave the other options with their default settings. As you make the selections, the Deployment Script Generator will generate a Shell script for Linux that you will run on your Deep Security instance.



1. Click on the **Copy to Clipboard** button to copy the script to clipboard.

Check if the SSH client is installed on your local machine by typing **SSH** in the command line of your local machine. Your Linux computer most likely includes an SSH client by default. However, if your computer doesn't recognize the command, the Open SSH project provides a free implementation of the full suite of SSH tools. For more information, see [http://www.openssh.com](http://www.openssh.com/).

|  |
| --- |
| **For windows platform**  You can download OpenSSH from following location: <https://www.mls-software.com/opensshd.html>  After installing OpenSSH on a Windows platform, modify the environment PATH variable, by appending the directory path of OpenSSH bin folder. By default, it is C:\Program Files\OpenSSH\bin. |

1. SSH into AWS Linux instance. Execute the command below.

|  |
| --- |
| ssh -i "<Path\_to\_Private\_Key\_File>" ubuntu@<Public\_DNS\_EC2\_Instance> |

* Replace <Path\_to\_Private\_Key\_File> token with the directory path where the Private Key file (file with ‘.pem’ Extention) is stored..
* Replace **<Public\_DNS\_EC2\_Instance>** token with Public DNS of AWS Linux Instance that you can obtain from EC2 dashboard.



1. You will see a response similar to the following.

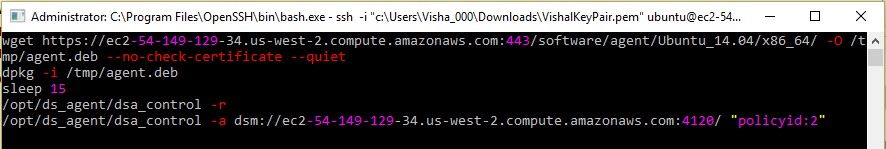
|  |
| --- |
| The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'can't be established.  RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.  Are you sure you want to continue connecting (yes/no)? |

1. Type **yes** to connect to the AWS Linux Instance.
2. In the same console window, execute the command below to create a shell script file. Open it in the **vi** editor.

|  |
| --- |
| vi deep\_security.sh |

10. Paste the shell script, copied from the Deployment Script window in **Step 6** of this **section** **4.8.8** into the **vi editor**.

11. Make sure all the content is copied.



12. Click the **Esc** key on your keyboard to change the mode.

13. Type **:x** in the vi editor and click on the **Enter** button to save and close the vi editor.

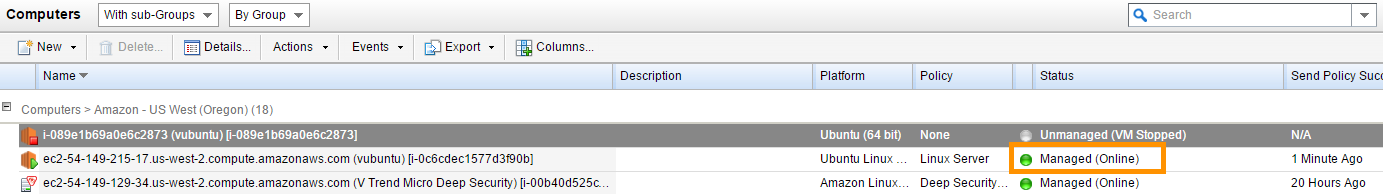
14. Execute the command below in the console window to convert the shell script file to an executable file.

|  |
| --- |
| chmod 777 deep\_security.sh |

15. Execute the command below in the console window to start the execution of the shell script file.

|  |
| --- |
| sudo ./deep\_security.sh |

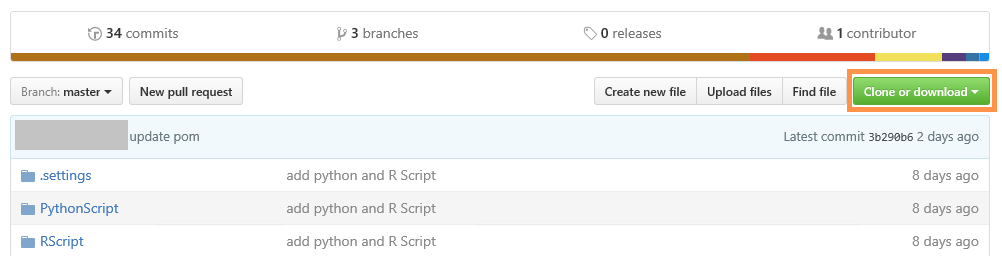
16. After a successful execution of the script, the Deep Security agent will get installed in the AWS Linux Instance. You can verify this in the Deep Security manager where the status of the AWS Linux Instance will be changed to Managed (Online).



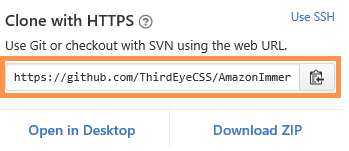
You can secure the other existing and new AWS Linux instances by executing the Shell script generated, according to the Platform and Operating System of the instance.

4.9. Setup solution code tree & datasets [Github repository cloning]

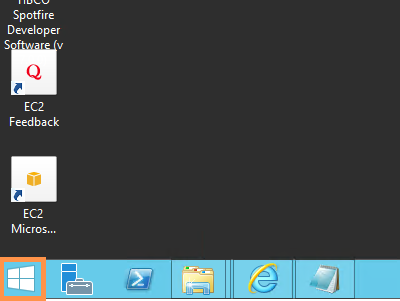
1. Take the RDP of the **TIBCO Spotfire** EC2 instance and perform following:
2. Download and install the Git client for windows with default settings from [*https://git-scm.com/*](https://git-scm.com/).
3. Click on the link [*https://github.com/ThirdEyeCSS/AmazonImmersion*](https://github.com/ThirdEyeCSS/AmazonImmersion) on the web browser of TIBCO Spotfire EC2 instance to access the repository containing project code and datasets.
4. Click on the **Clone or download** menu button located on the repository page.



1. Copy the web URL to access the repository on the Git client, from the popup window.



1. Click on the **Start** button located on the taskbar.

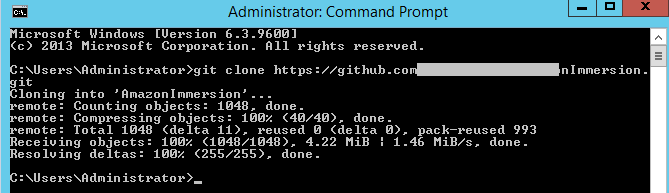


1. Type **‘cmd’** on the Start window and select **Command Prompt** from the search results.

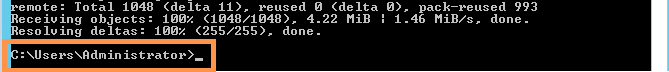


1. Replace **<Repository\_URL>** token from the command below with the URL of the repository you copied in **Step 5** of this section. Execute it on the Command Prompt to start cloning the project code.

|  |
| --- |
| git clone **<Repository\_URL>** |



Now the entire code from the project repository is copied to your TIBCO Spotfire EC2 instance in the current directory of the Command Prompt. Example: C:\Users\Administrator directory according to the above image.



4.10 Install Tomcat Servers for Web Interfacing

Follow the steps in this section to install the Tomcat Server on ATTUNITY CloudBeam and TIBCO Spotfire EC2 instances.

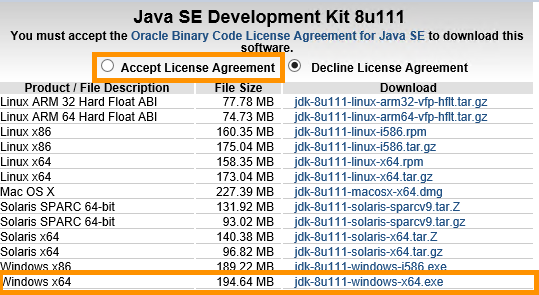
1. Take the RDP of the TIBCO Spotfire EC2 instance.
2. Click on the following URL in the browser of the EC2 instance.

[*http://www.oracle.com/technetwork/java/javase/downloads/index.html*](http://www.oracle.com/technetwork/java/javase/downloads/index.html)

1. Click on the Java icon to navigate to the JDK download page.



1. Accept the license agreement on JDK download page. Click on the download link for Windows x64.



1. Save and execute the downloaded file. Make note of the destination folder while installing the JAVA SE Development kit.
2. Follow the steps below to set the Path environment variable for the installed JAVA Development Kit:

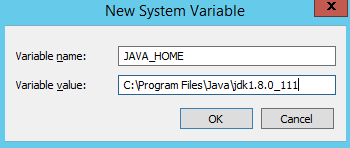
* For **Windows Server 2012** follow the path below to open the Advanced System Settings

Select Start > Control Panel > System and Security > System > Advanced System Settings.

For **Windows Server 2008** follow the path below to open the Advanced System Settings

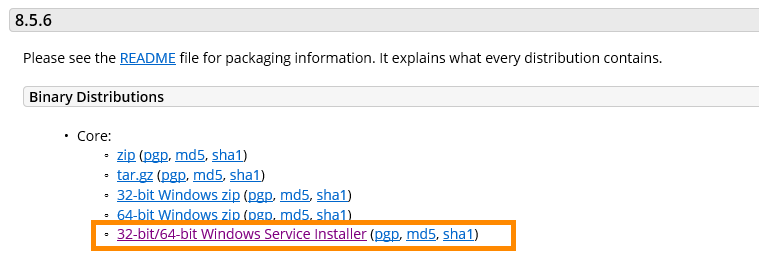
Select Start > Control Panel > System > Advanced System Settings.

* In the System Properties dialog window, select the **Advanced** tab and click on the **Environment Variable** button.
* In the Environment Variables dialog window, click on the **New** button in System Variables section to add a variable.
* In the New System Variable window, type **JAVA\_HOME** as a Variable name and type the **path to the JDK directory** as a Variable value. (The JDK directory is located in the destination folder used when JAVA was installed)



* Click on the **OK** button to save the variable.

1. Restart the instance and use RDP again to install the Tomcat server.
2. Click on the URL [*http://tomcat.apache.org/download-80.cgi*](http://tomcat.apache.org/download-80.cgi) in the browser of a connected EC2 instance to get the latest installation package for the Tomcat server.
3. Scroll down the web page to reach the **Binary Distributions** section and click on the link **32-bit/64-bit Windows Service Installer** to download the binary executable file.



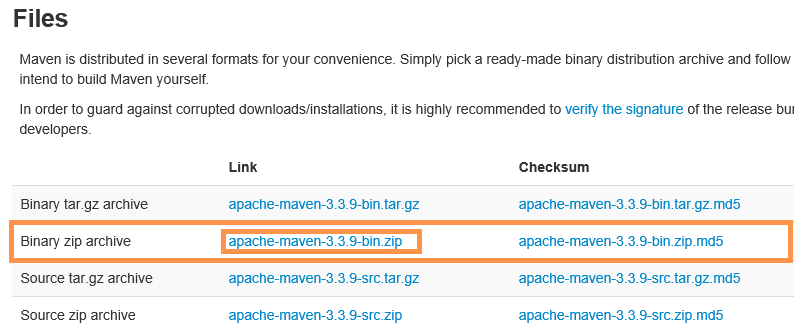
1. Run the downloaded executable file to install Tomcat Server on the EC2 instance.

11. Follow Steps 1 through 10 to install the Tomcat server on ATTUNITY CloudBeam EC2 instance.

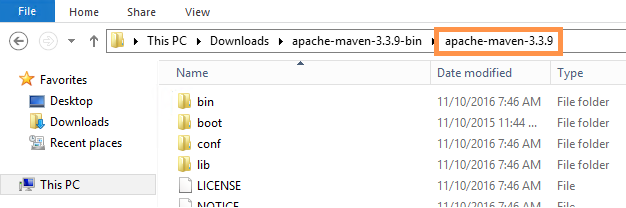
4.11. Install Apache Maven

This section guides you on to how to install Apache Maven on ATTUNITY CloudBeam and TIBCO Spotfire EC2 instances.

1. Take the RDP of the **TIBCO Spotfire** EC2 instance.
2. Click on [*http://maven.apache.org/download.cgi*](http://maven.apache.org/download.cgi) on the web browser to download Apache maven.
3. Scroll down the page to reach the Files section and click on the link next to the **Binary zip archive** to start downloading the installation package.



1. Unzip the downloaded compressed file and copy the directory containing bin, boot, and conf, etc. folder in the C drive of the EC2 instance.



1. Follow the steps below to set the Path environment variables for the Maven installation:

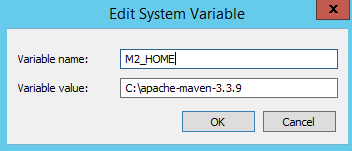
* For **Windows Server 2012** follow the path below to open Advanced System Settings

Select Start > Control Panel > System and Security > System > Advanced System Settings

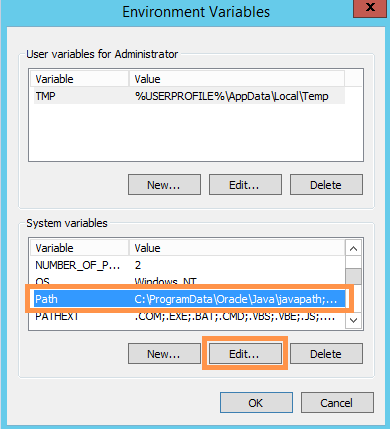
For **Windows Server 2008** follow the path below to open Advanced System Settings

Select Start > Control Panel > System > Advanced System Settings

* In the System Properties dialog window, select the **Advanced** tab and click on the **Environment Variable** button.
* In the **Environment Variables** dialog window, click on the **New** button in the System Variables section to add a variable.
* In the **New System Variable** window, enter **M2\_HOME** as a Variable name and type the **path to Maven installation directory** as a Variable value.

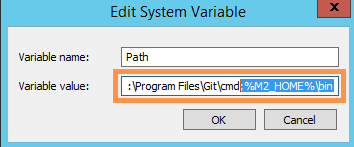


* Click on the **OK** button to save.
* Now select a **Path** System variable and click on the **Edit** button to modify it.



* Append string “**;%M2\_HOME%\bin**” at the end of the existing value of the Path variable.

Semicolon “;” acts as a string separator.



* Click on the **OK** button to save the modification.
* Click on the **OK** button on the System Variable window.

1. Open a new Command Prompt instance and execute the command below to check if Maven has successfully been installed.

|  |
| --- |
| mvn –version |



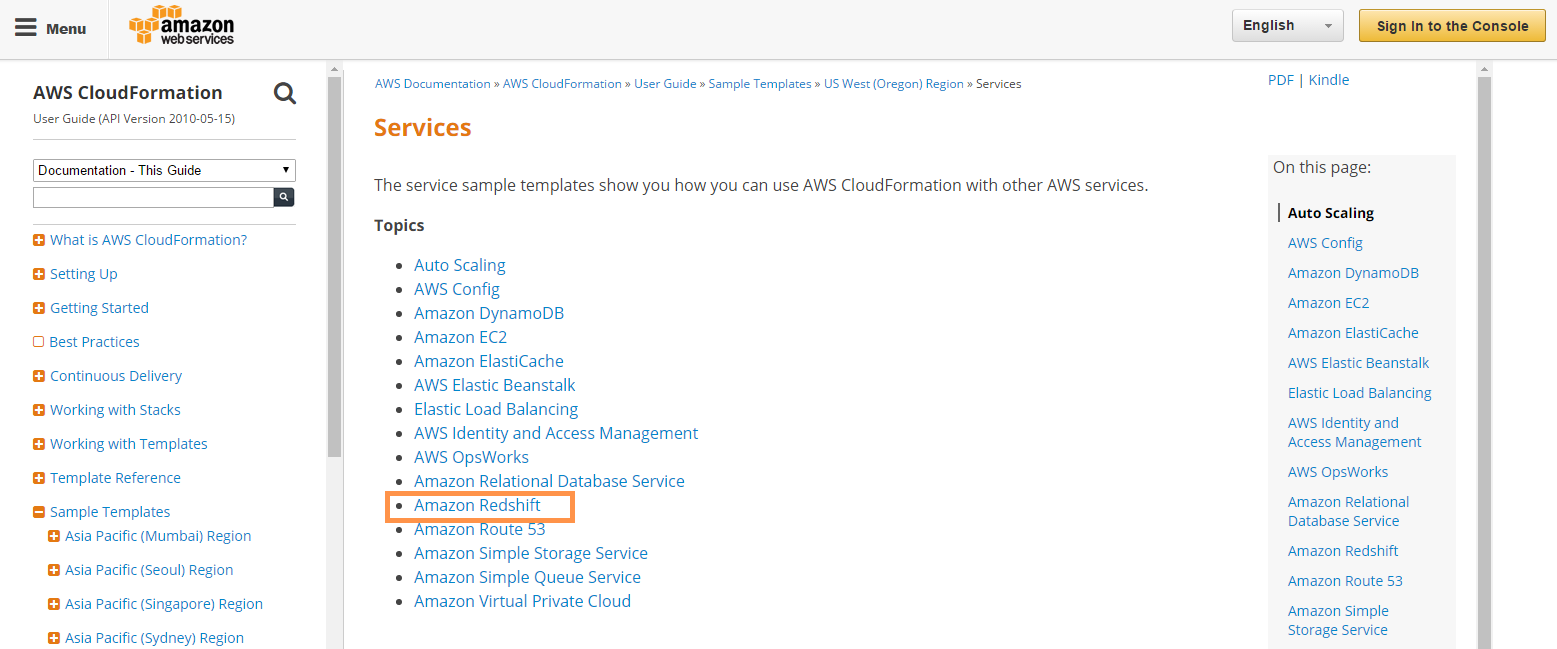
Output similar to the above screenshot signifies a successful Maven installation.

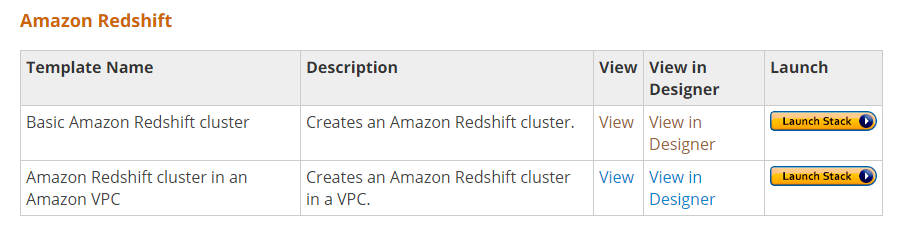
1. Repeat Steps 1 through 6 to install Maven on ATTUNITY CloudBeam EC2 instance.

4.12. Cluster & resource setup automation using AWS CloudFormation

AWS CloudFormation is a service that helps you model and set up your Amazon Web Services resources so that you can spend less time managing those resources and more time focusing on your applications that run in AWS. You create a template that describes all the AWS resources that you want (like Amazon EC2 instances or Amazon RDS DB instances), and AWS CloudFormation takes care of provisioning and configuring those resources for you. You don't need to individually create and configure AWS resources and figure out what's dependent on what. AWS CloudFormation handles all of that.

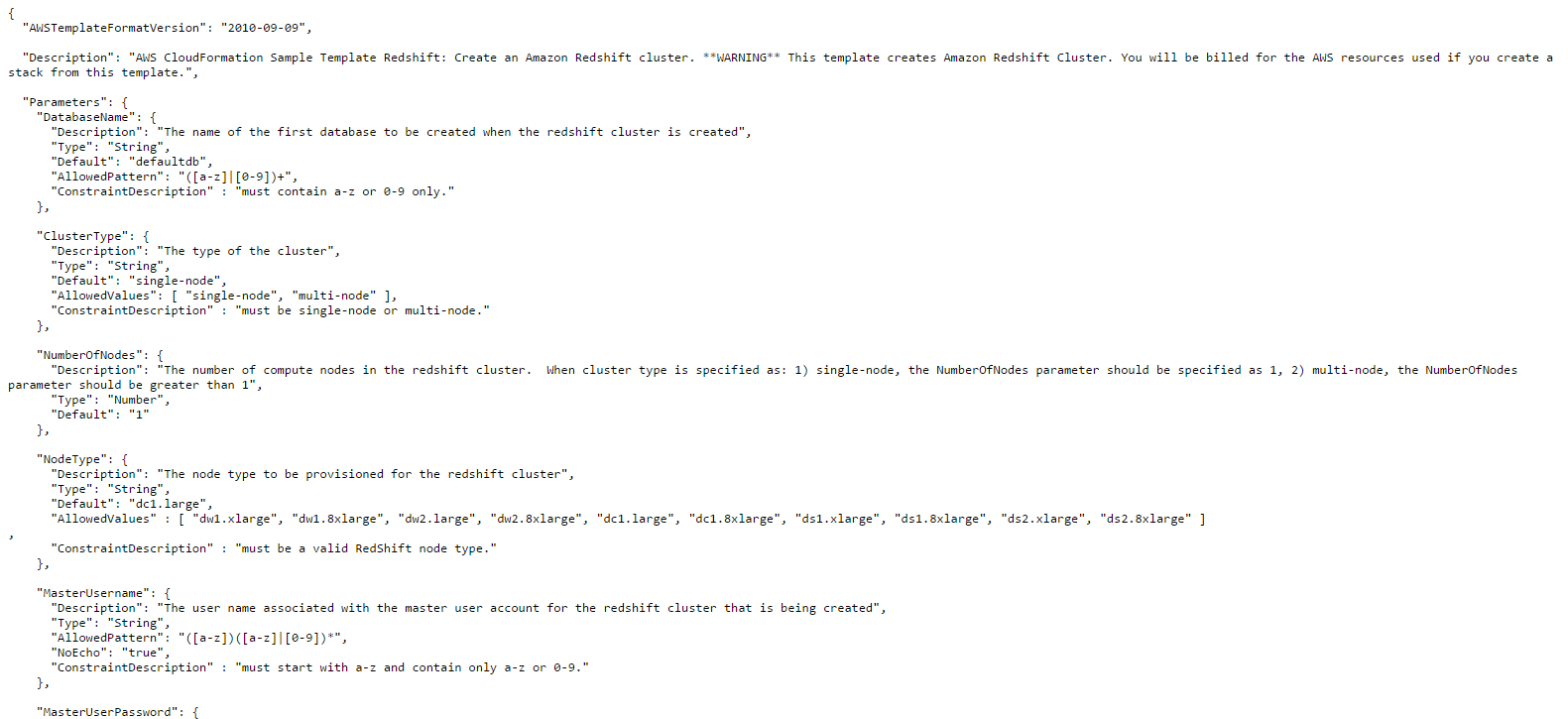
The following steps will show you how to setup Amazon redshift using an AWS Cloud Formation template.

Click on the link [*http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/sample-templates-services-us-west-2.html*](http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/sample-templates-services-us-west-2.html)and select **Amazon Redshift** in the **Topics** list to bring up the template list for Amazon Redshift. 



The Header row of this table contains Template Name, Description, View, View in Designer, and Launch.

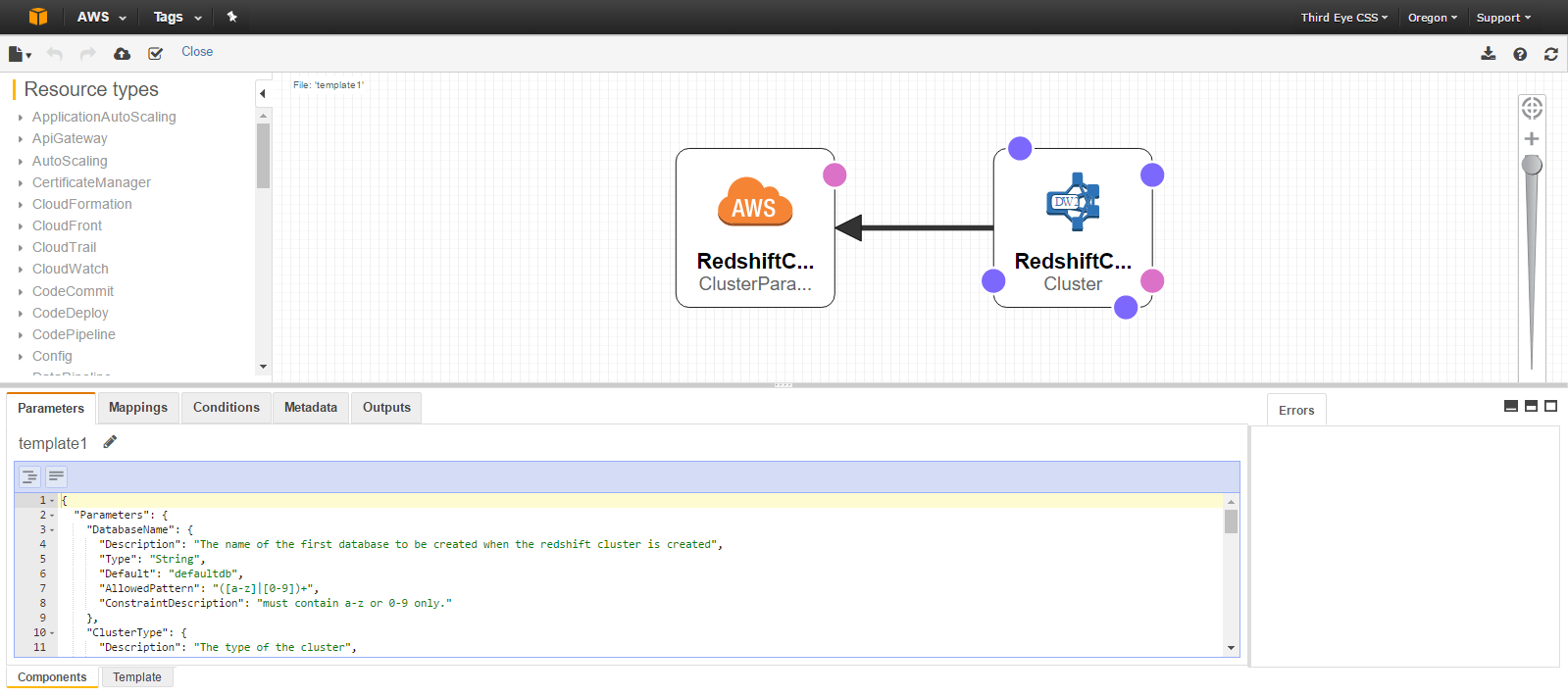
1. Click the **View** link next to **Basic Amazon Redshift cluster** template to view the template in a browser.



The template is in Json format and contains various nodes required to create a cluster.

1. Click on the **View in Designer** link next to **Basic Amazon Redshift cluster** template.

It opens up Designer to manage the template. Designer visualizes the template so that AWS resources can be easily recognized and connected. Designer helps to create a new template, modifies existing templates, and helps to store them locally or in the AWS storage.



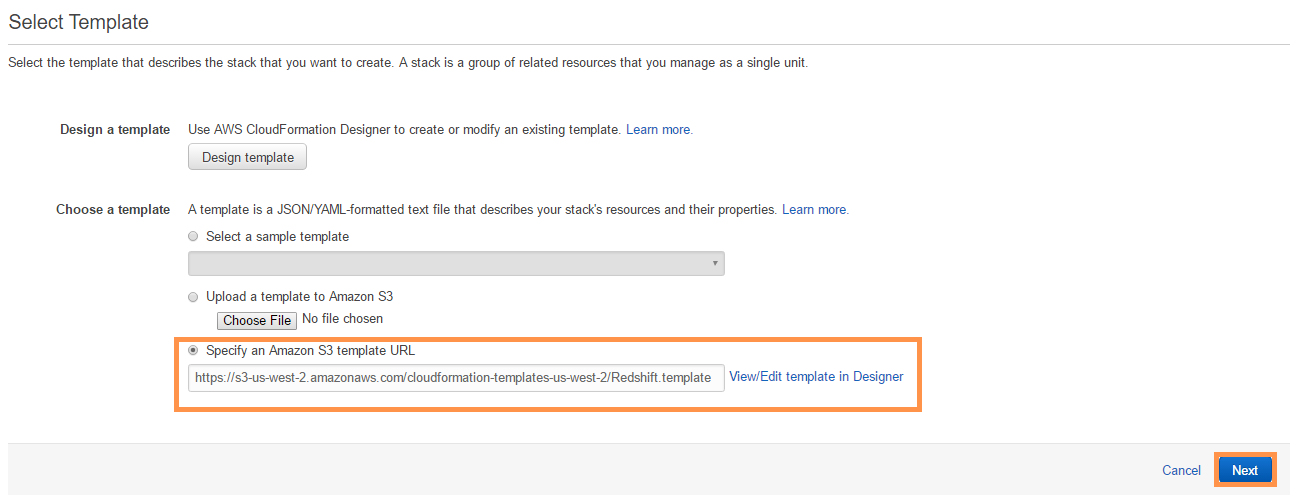
1. Click on the **Launch Stack** button to open the Create stack page.

On the Create Stack page, AWS CloudFormation uses the defined template, and makes underlying service calls to AWS in order to provision and configure your resources.

Use the Amazon’s **Basic Amazon Redshift cluster** template to launch a new cluster.

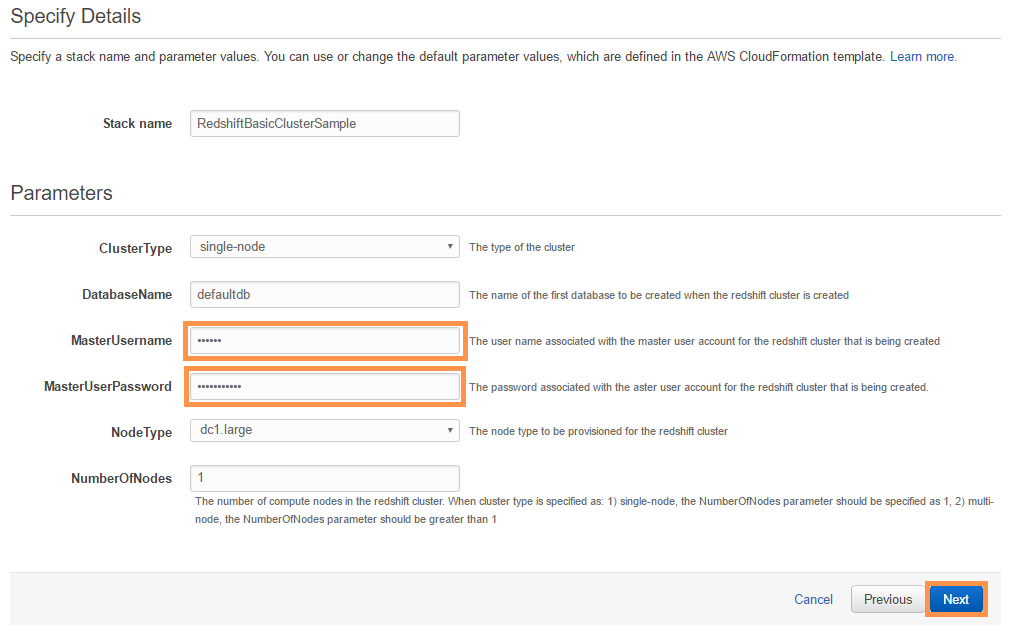
1. Do not make any changes on the **Select Template** tab of the Create Stack page.

By default, **Specify an Amazon S3 template URL** option will be selected, which lets you use the template published on the Internet. The URL field contains the location of Amazon’s sample **Basic Amazon Redshift cluster** template.

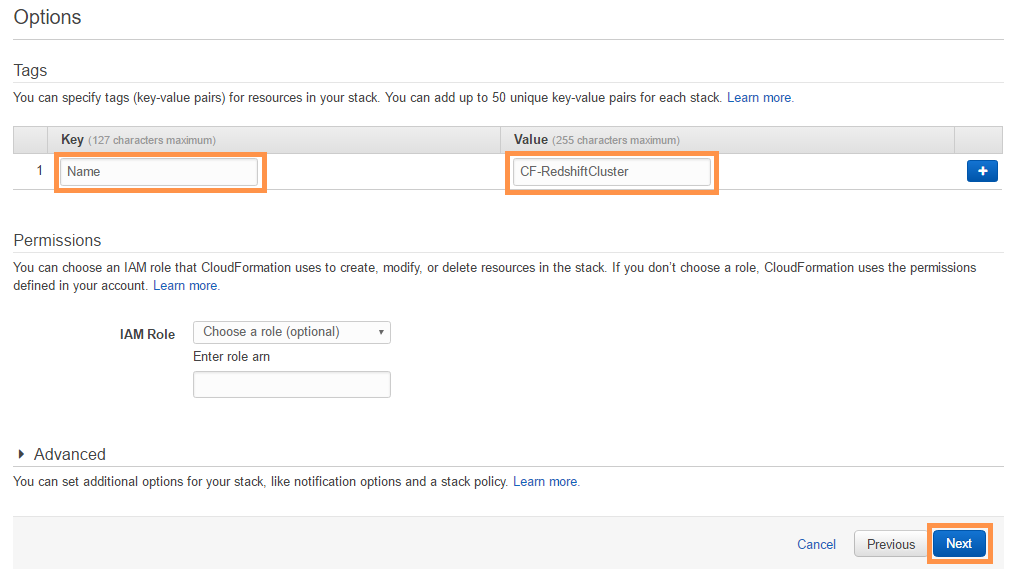


1. Click on the **Next** button to move to the **Specify Details** tab.
2. Keep all default values on the **Specify Details** tab, but enter the appropriate values for MasterUsername and MasterUserPassword.

Make note of the **DatabaseName**, **MasterUsername,** and **MasterUserPassword** for future use.



1. Click on the **Next** button to move to the next tab.
2. On the **Options** tab, go to the **Tags** section and enter the following values for a new tag:

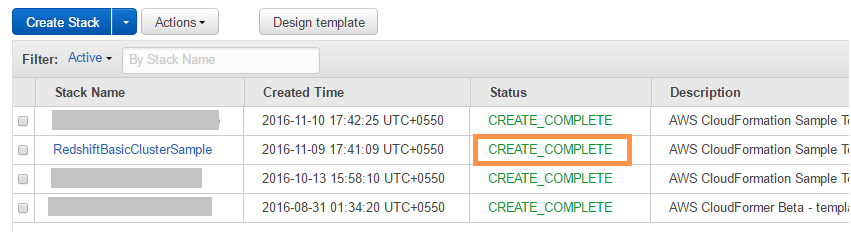


**Key**: Name

**Value**: CF-RedshiftCluster, or enter the name for the cluster of your choice.

Keep the IAM Role blank. If you don’t choose a role, CloudFormation uses the permissions defined in your account.

1. Click on the **Next** button to move to the Review tab.
2. Confirm all the properties on the Review tab and click on the **Create** button at the bottom to launch Amazon Redshift cluster.
3. Wait until the status of the new stack becomes **CREATE\_COMPLETE** in the stack list.



1. Click on the URL <https://us-west-2.console.aws.amazon.com/redshift> in your browser to open the Redshift Dashboard.
2. Click on the **Clusters** link to open the clusters list.



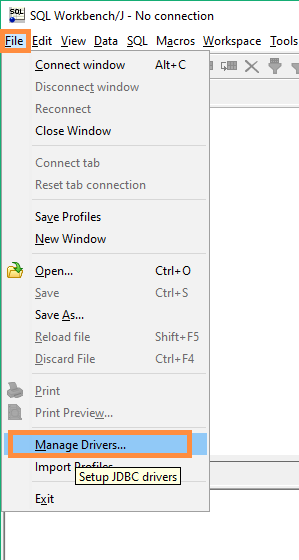
1. Click on the cluster name from the clusters list (created in an earlier step) to open the clusters details page.
2. Scroll down to reach **Cluster Database Properties** and copy the **JDBC URL**.



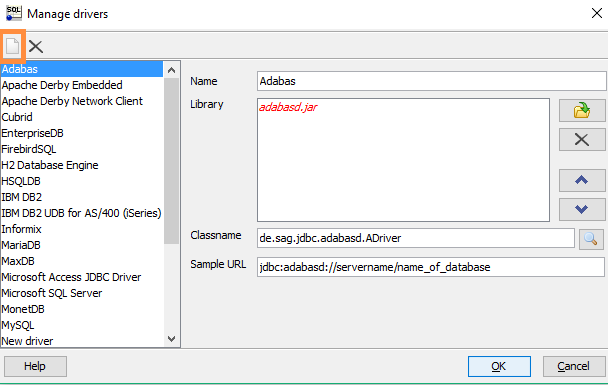
1. Copy and paste the link [http://docs.aws.amazon.com/redshift/latest/mgmt/configure-jdbc-connection.html#download-jdbc-driver](http://docs.aws.amazon.com/redshift/latest/mgmt/configure-jdbc-connection.html%23download-jdbc-driver) in the browser of your local machine to Download the Amazon Redshift JDBC Driver.
2. Click on the download link for the latest driver jar file to download it, and to copy the class for the same driver.



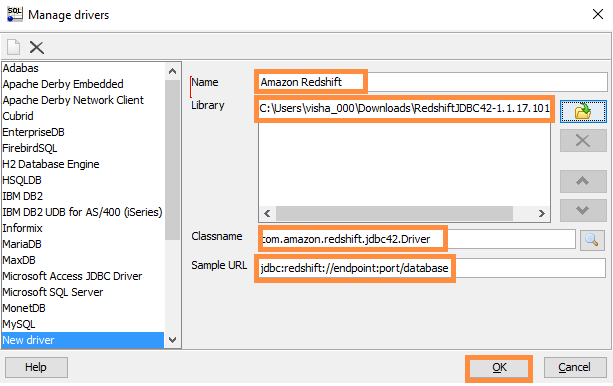
1. Open the **SQL Workbench** tool.
2. Close **Select Connection Profile** window if it’s open.
3. Select the **File > Manage** Drivers menu.



1. In the **Manage Drivers** dialog window, click on the **Create New Entry** button located in the upper left corner.

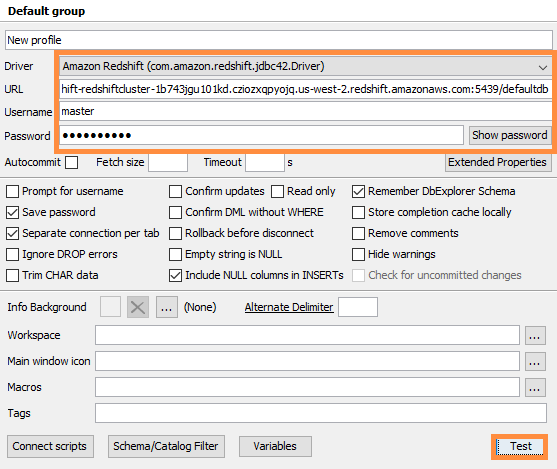


1. Enter the following properties, and click on the **OK** button to register the new driver.



* **Name**: Amazon Redshift (or you can enter the name of your choice)
* **Library:** Browse and select the downloaded Amazon Redshift JDBC drivers jar file.
* **Classname:** The class name for Amazon Redshift JDBC driver
* **Sample URL:** jdbc:redshift://endpoint:port/database

1. Select **File > Connect** Window.
2. In the Select Connection Profile window, enter the following connection properties to connect to the Amazon Redshift database.

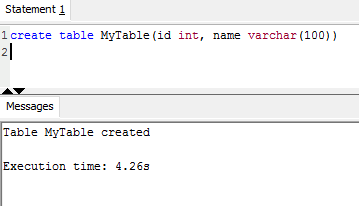


* Driver: Select the driver from the **Driver** list (registered in **Step 23** of this section).
* URL: JDBC URL for Amazon Redshift Cluster (copied in **Step 16** of this section).
* Username and Password: Enter **MasterUsername** and **MasterUserPassword** (specified while provisioning the Redshift cluster in **Step 7** of this section).

Click on the **Test** button at the bottom to confirm the connection properties.

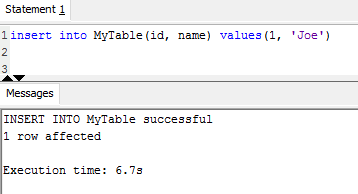
1. After a successful test connection, click on the **OK** button to make the connection.
2. Execute the statements below in the query window to create a new table in the database.

|  |
| --- |
| create table MyTable(id int, name varchar(100)) |



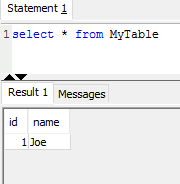
1. Insert a row into the table.

|  |
| --- |
| insert into MyTable(id, name) values(1, 'Joe') |

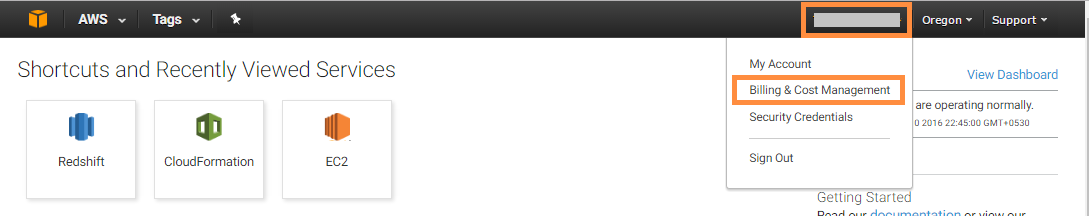


1. Select a query on the created table.

|  |
| --- |
| select \* from MyTable |

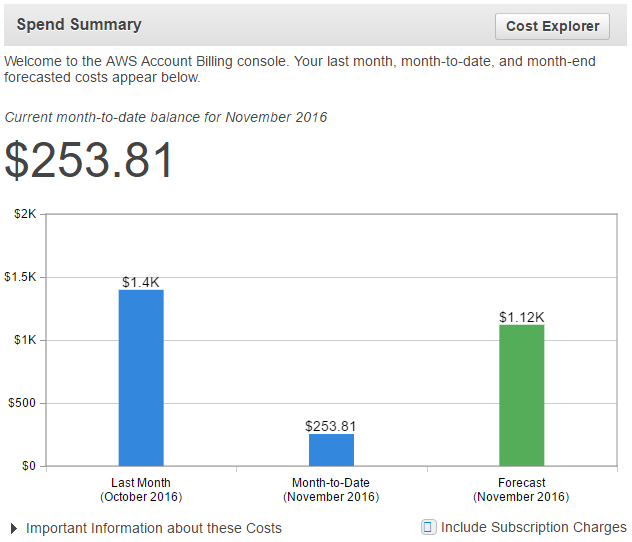


1. Billing and Cost Management
2. Log in to your **AWS Management Console** using your account credentials.
3. Click on the drop down menu attached to your account name in the upper left corner of the page and select the **Billing & Cost Management** menu.



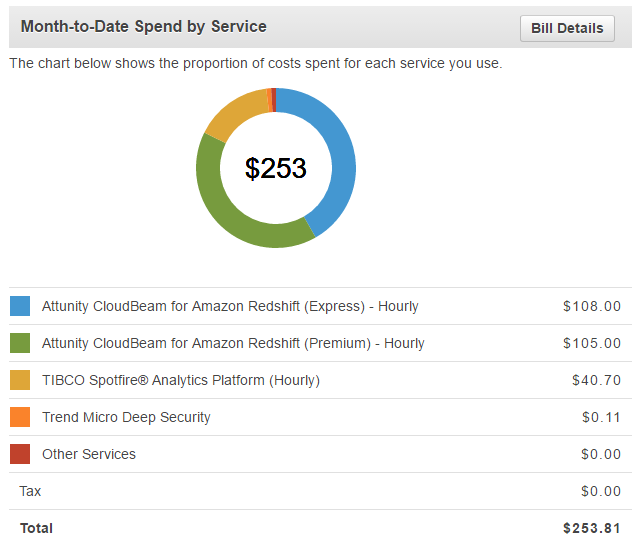
1. The Billing & Cost Management Dashboard page contains two charts:

* **Spend Summary**



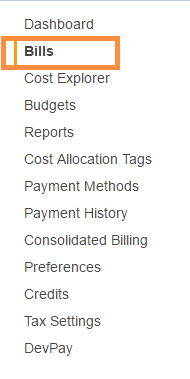
This chart visualizes Last Month, Month-to-Date, and Month-End-Forecasted costs in the form of a bar chart that helps to make the comparison with ease.

* **Month-to-Date Spend by Service**

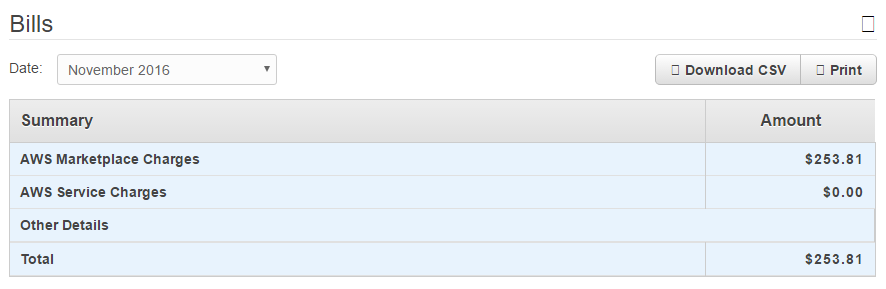


This pie chart shows the proportion of costs spent for each service in Month-to-Date. You can easily identify which service is consuming the most.

1. In the navigation pane, select the **Bills** tab to open the Bills section.



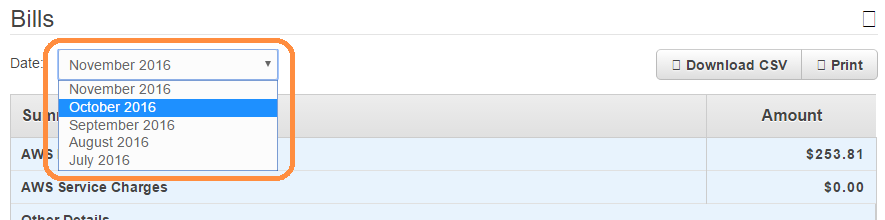
The Bills section provides detailed information of bills for the current month-to-date, by default.



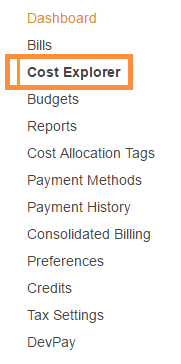
It also provides details of bills by service, used in the current month-to- date, by default.



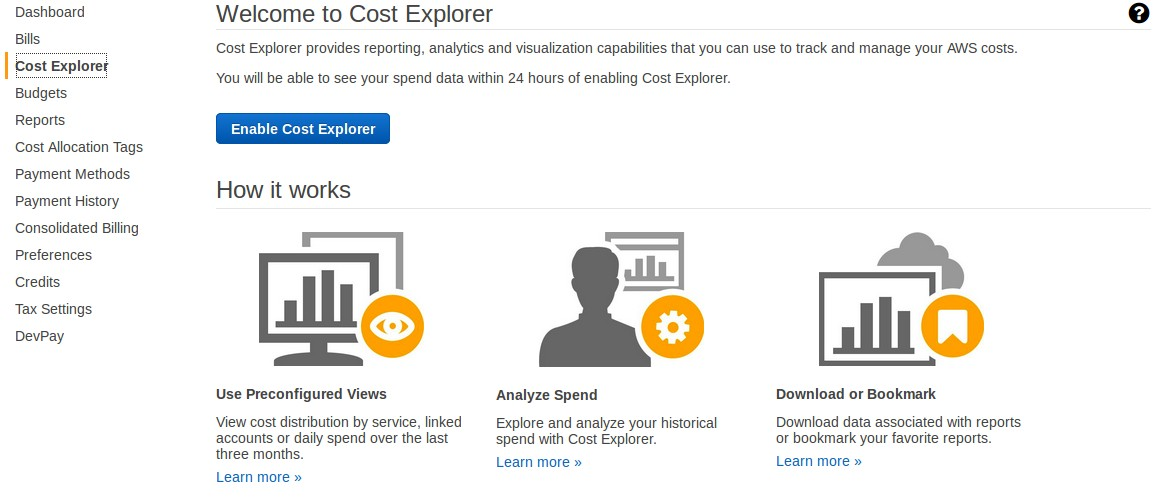
You can get Bill information for previous months by changing the months in the **Date** list.



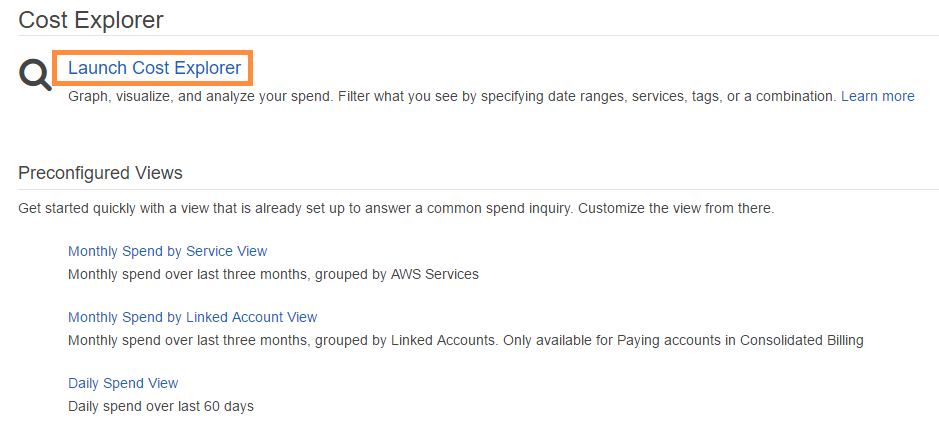
1. Select the **Cost Explorer** tab in the navigation pane.



1. Cost Explorer lets you create our own charts to analyze costs in our own way. It provides various filters such as date ranges, services, tags, or combinations of all. Using these filters, a user can analyze costs from different perspectives.
2. If you are a first-time user of Cost Explorer, you can see the **Enable Cost Explorer** button in the Cost Explorer window.

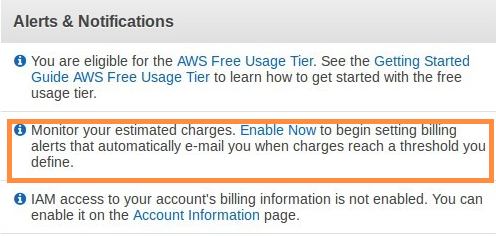


1. By default, Cost Explorer doesn’t come enabled with your account; you have to click on the **Enable Cost Explorer** button to enable it. It takes 24 hours to get it enabled after you press this button.
2. After Cost Explorer is enabled, the **Launch Cost Explorer** link appears in Cost Explorer.

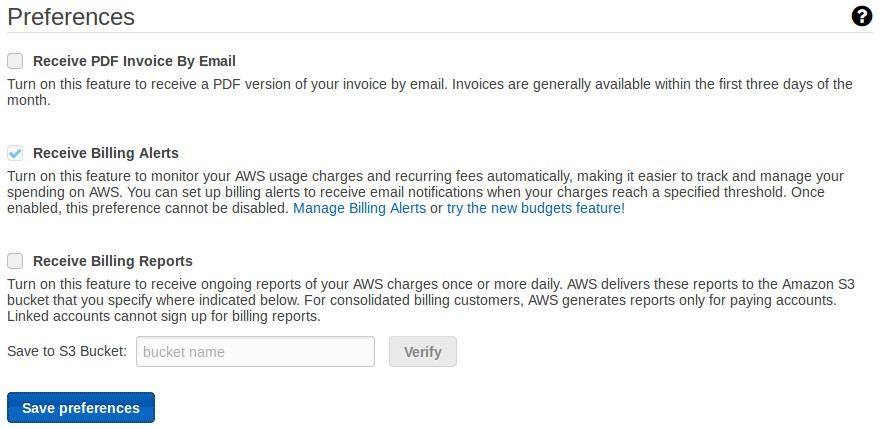


Click on this link to open Designer which lets you create your own visualizations, modify existing reports, or delete unwanted reports.

1. Follow the steps below to set your billing alerts.
2. Click on the **Dashboard** tab in the navigation pane to open the Dashboard again.
3. Scroll down the page to reach the **Alerts & Notifications** section.



1. Click on the **Enable Now** link in the highlighted area, to enable alerts that will get triggered when the cost-threshold is reached. The cost-threshold can be set through the **Amazon CloudWatch** service.
2. Once you click on this link you will be asked to set your preferences to receive alerts.



1. Check the box **Receive Billing Alerts** to receive email notifications when your charges reach a specified threshold.

Note: Once enabled, this preference **cannot** be disabled.

1. Click on the **Save** preferences button at the bottom to finalize.

You are now subscribed to receive cost alerts for your AWS account.

6. Next Steps

**Execute Project 2**: **Data Pipeline**. This document for the next Project can be found in the following Git repository:

The document’s name is: *Step-by-Step Guide for Data pipeline from AWS Marketplace.pdf*

7. Appendix

The following table provides cost estimates for various components.

However, these are sample prices only, which are subject to change.

|  |  |  |
| --- | --- | --- |
| **Components Name** | **EC2 Servers** | **EC2 Charges Hourly** |
| **SoftNAS** | m3.xlarge | $1.616/hr |
| **Attunity CloudBeam** | m4.large | $2.646/hr |
| **TIBCO Spotfire** | m4.large | $2.646/hr |
| **Kony Mobile Fabric** | t2.large | $0.104/hr |
| **Trend Micro** | m4.large | $1.62/hr |
| **AWS RedShift** | NA | $0.250/hr |

The following links are for the Amazon market place components. Please go through the list to get more details.

|  |  |  |
| --- | --- | --- |
| **Component #** | **Component Name** | **EC2 Server Type** |
| B | SoftNAS | <https://aws.amazon.com/marketplace/pp/B00PJ9FGVU?qid=1475145771249&sr=0-2&ref_=srh_res_product_title> |
| C | Attunity CloudBeam | <https://aws.amazon.com/marketplace/pp/B00LBH6GCC?qid=1475145807428&sr=0-3&ref_=srh_res_product_title> |
| G | TIBCO Spotfire | <https://aws.amazon.com/marketplace/pp/B00PB74KYY?qid=1475145882225&sr=0-9&ref_=srh_res_product_title> |
| H | Kony Mobile Fabric | Developer: <https://aws.amazon.com/marketplace/pp/B010TV3U2E?qid=1475145908555&sr=0-2&ref_=srh_res_product_title>  Express: <https://aws.amazon.com/marketplace/pp/B010PHCVO0?qid=1475145908555&sr=0-1&ref_=srh_res_product_title> |
| I | Trend Micro Security | <https://aws.amazon.com/marketplace/pp/B01AVYHVHO?qid=1475145958660&sr=0-2&ref_=srh_res_product_title> |

|  |  |  |
| --- | --- | --- |
| **Seller / ISV Name** | **Listing Title** | **Marketplace URL** |
| MapR | MapR Enterprise Database Edition Plus | <https://aws.amazon.com/marketplace/pp/B01256C2XE> |
| MapR | MapR Enterprise Database Edition Plus Spark | <https://aws.amazon.com/marketplace/pp/B01256C07M> |
| MapR | MapR Enterprise Edition Plus | <https://aws.amazon.com/marketplace/pp/B01256BSVQ> |
| MapR | MapR Enterprise Edition Plus Spark | <https://aws.amazon.com/marketplace/pp/B01255WKW8> |
| NetApp | OnCommand Cloud Manager on Linux | <https://aws.amazon.com/marketplace/pp/B018REK8QG> |
| Sophos | Sophos UTM 9 Autoscaling | <https://aws.amazon.com/marketplace/pp/B0166NB8RI> |
| Sophos | Sophos UTM 9 Autoscaling (BYOL) | <https://aws.amazon.com/marketplace/pp/B0166P65JW> |
| TIBCO | TIBCO Jaspersoft for AWS with Multi-Tenancy (Hourly) | <https://aws.amazon.com/marketplace/pp/B00G9PRRDS> |
| TIBCO | TIBCO Jaspersoft Reporting and Analytics for AWS | <https://aws.amazon.com/marketplace/pp/B00B527JQ0> |
| TIBCO | TIBCO Jaspersoft Reporting and Analytics for AWS (BYOL) | <https://aws.amazon.com/marketplace/pp/B00E8ON93Y> |
| MapR | MapR Community Edition | <https://aws.amazon.com/marketplace/pp/B010GJS5WO> |
| Barracuda | Barracuda Web Application Firewall | <https://aws.amazon.com/marketplace/pp/B014GEC526> |
| MapR | MapR Enterprise Edition Plus BYOL | <https://aws.amazon.com/marketplace/pp/B018T2N8P4> |
| Unisys | Unisys Stealth(cloud) Enterprise Manager | <https://aws.amazon.com/marketplace/pp/B018JDUT9G> |
| Unisys | Unisys Stealth(cloud) on Red Hat Enterprise Linux 6 | <https://aws.amazon.com/marketplace/pp/B018JEE9NW> |
| Unisys | Unisys Stealth(cloud) on Red Hat Enterprise Linux 7 | <https://aws.amazon.com/marketplace/pp/B0195P1O7S> |
| Unisys | Unisys Stealth(cloud) on SUSE Linux Enterprise Server 11 | <https://aws.amazon.com/marketplace/pp/B0195OWOKK> |
| Unisys | Unisys Stealth(cloud) on Ubuntu Linux 14.04 | <https://aws.amazon.com/marketplace/pp/B0195PEU0G> |
| Unisys | Unisys Stealth(cloud) on Windows Server 2008 R2 | <https://aws.amazon.com/marketplace/pp/B0195OPMAE> |
| Unisys | Unisys Stealth(cloud) on Windows Server 2012 R2 | <https://aws.amazon.com/marketplace/pp/B018JEEDVU> |
| Aerospike | Aerospike 3 Database | <https://aws.amazon.com/marketplace/pp/B00LW9382A> |
| Zend | Zend PHP 5.6 Enterprise RHEL | <https://aws.amazon.com/marketplace/pp/B00SG8YOFK> |
| Zend | Zend PHP 5.6 Enterprise Ubuntu | <https://aws.amazon.com/marketplace/pp/B00SG8MHWW> |
| Zend | Zend PHP 5.6 Professional RHEL | <https://aws.amazon.com/marketplace/pp/B00SG8SDO8> |
| Zend | Zend PHP 5.6 Professional Ubuntu | <https://aws.amazon.com/marketplace/pp/B00SG8MCR2> |
| HP Vertica | HP Vertica Analytics Platform | <https://aws.amazon.com/marketplace/pp/B010ETKZKG> |
| Sirqul | Sirqul | <https://aws.amazon.com/marketplace/pp/B01BZEABOE> |
| Data Resolution | SharePoint Enterprise 2013 for AWS Advanced - BYOL | <https://aws.amazon.com/marketplace/pp/B01C0VFNZI> |
| Data Resolution | SharePoint Enterprise 2013 for AWS Advanced | <https://aws.amazon.com/marketplace/pp/B01C0VAZMO> |
| Data Resolution | SharePoint Enterprise 2013 for AWS Business - BYOL | <https://aws.amazon.com/marketplace/pp/B01C0VFP9W> |
| Data Resolution | SharePoint Enterprise 2013 for AWS Business | <https://aws.amazon.com/marketplace/pp/B01C0PTYWC> |
| Data Resolution | SharePoint Enterprise 2013 for AWS Basic "All in One" | <https://aws.amazon.com/marketplace/pp/B01BXJ8FSK> |
| Digital Cube | WordPress powered by AMIMOTO (HVM) | <https://aws.amazon.com/marketplace/pp/B00LWHVJH8> |
| Checkpoint | Security Gateway Virtual Edition NGTP (PAYG) | <https://aws.amazon.com/marketplace/pp/B01CEYZ5S6> |
| Checkpoint | Security Gateway Virtual Edition (BYOL) | <https://aws.amazon.com/marketplace/pp/B01CEYZMB6> |
| Digital Cube | WordPress Powered by AMIMOTO (Apache HTTPD PHP7) | <https://aws.amazon.com/marketplace/pp/B01B3ZE1NC> |
| Teradata | Teradata Server Management | <https://aws.amazon.com/marketplace/pp/B01DFZ2ZG8> |
| Hyperglance | Hyperglance - up to 500 Nodes | <https://aws.amazon.com/marketplace/pp/B01DJZLUWO> |
| Hyperglance | Hyperglance - up to 250 Nodes | <https://aws.amazon.com/marketplace/pp/B01DJZLVPU> |
| Hyperglance | Hyperglance - up to 100 Nodes | <https://aws.amazon.com/marketplace/pp/B01DJZLU2O> |
| Saviynt | Saviynt Security Manager | <https://aws.amazon.com/marketplace/pp/B01CPOTDWO> |
| Digital Cube | WooCommerce Powered by AMIMOTO (HHVM) | <https://aws.amazon.com/marketplace/pp/B00ZGTRMVU> |
| Sungard | Sungard | <https://aws.amazon.com/marketplace/pp/B01CIWY4UO> |
| Omnibond | CloudyCluster RHEL 7 v1.01 | <https://aws.amazon.com/marketplace/pp/B018506W1C> |
| ClickBerry | ClickBerry | <https://aws.amazon.com/marketplace/pp/B0179ZISCK> |
| Fortinet | FortiGate | <https://aws.amazon.com/marketplace/pp/B00PCZSWDA> |
| Digital Cube | WordPress Powered by AMIMOTO (HHVM) | <https://aws.amazon.com/marketplace/pp/B00V5JYXTO> |
| Thinkparq | BeeGFS | <https://aws.amazon.com/marketplace/pp/B01D5CMU66> |
| Thinkparq | BeeGFS - Support Included | <https://aws.amazon.com/marketplace/pp/B01EVXGRH6> |
| Bitfusion | Bitfusion Boost Ubuntu 14 Cuda 7 | <https://aws.amazon.com/marketplace/pp/B01AT7S6CC> |
| Digital Cube | Mautic Powered by AMIAGE | <https://aws.amazon.com/marketplace/pp/B00YAY9OX6> |