

# IBM Security Guardium Cloud Deployment for Amazon AWS

**Guardium Technical Note**

Updated November 25, 2019

©IBM Corporation 2017, 2019

# IBM Security Guardium Cloud Deployment Guide for Amazon AWS

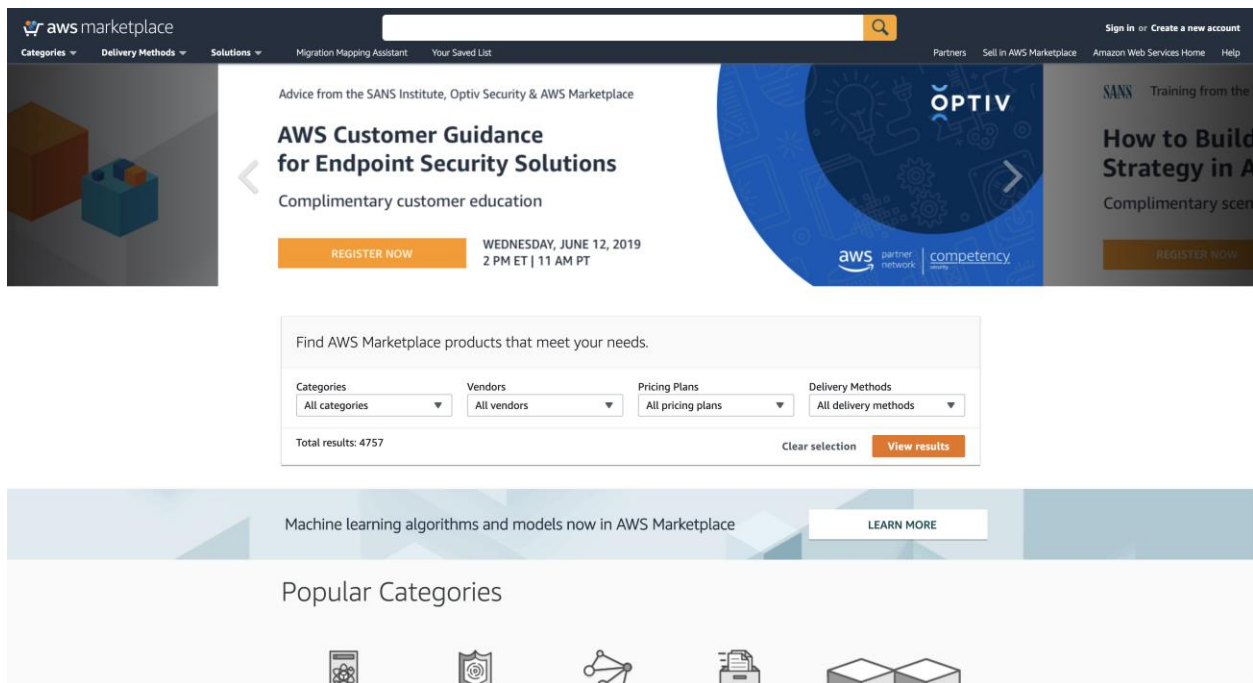
## Introduction

Guardium instances can be deployed on AWS in one of two ways. You can deploy either from the marketplace or from Guardium specific Amazon Machine Images (AMIs).

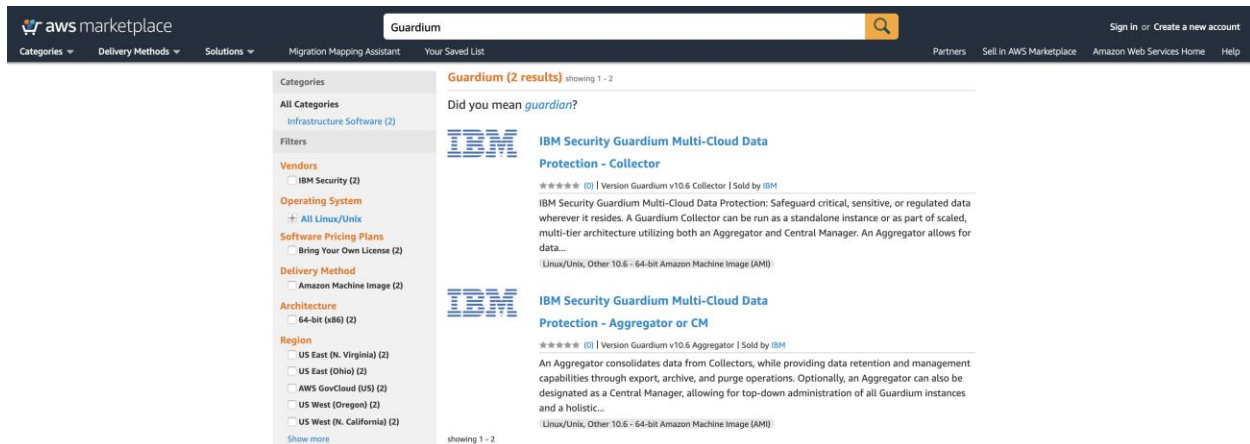
### Method 1: Deploying from the Marketplace

1. Navigate to the AWS Marketplace:

<https://aws.amazon.com/marketplace>



## 2. Search for Guardium.



## 3. Click on the IBM Security Guardium Collector or the IBM Security Guardium Aggregator offering.

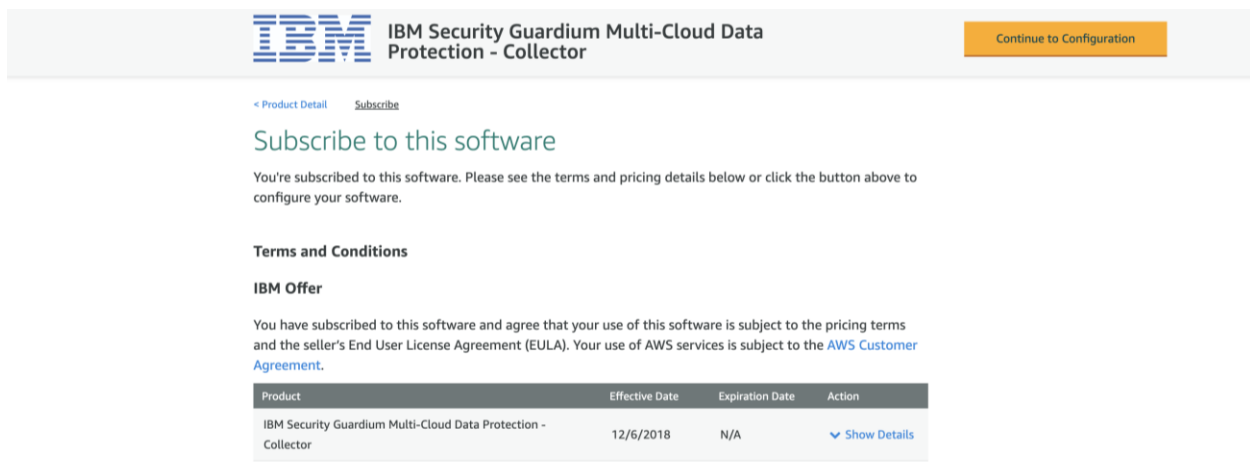
## 4. Click Continue to Subscribe to subscribe to the offering.




## 5. You are prompted to log into your AWS account if not logged in already

## 6. Review the terms and conditions.

## 7. Click Continue to Configuration.



## 8. Review the fulfillment option and then click Continue to Launch.

**IBM Security Guardium Multi-Cloud Data Protection - Collector**

[< Product Detail](#) [Subscribe](#) [Configure](#)

### Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

**Fulfillment Option**  
64-bit (x86) Amazon Machine Image (AMI)

**Software Version**  
Guardium v10.6 Collector (Jan 10)

**Region**  
US East (N. Virginia) Ami Id: ami-06c0e9f33d4f5b15b

**Pricing information**

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

**Software Pricing**


IBM Security Guardium Multi-Cloud Data Protection - Collector	\$0/hr
---	--------

**BYOL**  
*running on m4.2xlarge*

**Infrastructure Pricing**

EC2:	1 * m4.2xlarge
Monthly Estimate:	\$288.00/month

## 9. Click Usage Instructions to review the instructions.

**IBM Security Guardium Multi-Cloud Data Protection - Collector**

[< Product Detail](#) [Subscribe](#) [Configure](#) [Launch](#)

### Launch this software

Review your configuration and choose how you wish to launch the software.

**Configuration Details**

Fulfillment Option	64-bit (x86) Amazon Machine Image (AMI) IBM Security Guardium Multi-Cloud Data Protection - Collector <i>running on m4.2xlarge</i>
Software Version	Guardium v10.6 Collector
Region	US East (N. Virginia)

Usage Instructions

## 10. Choose to launch the software from the Website or EC2.

Note: You can also opt to copy the Guardium offering to your AWS Service Catalog to manage your organization's cloud resources

## 11. Choose an EC2 Instance Type

Note: Guardium recommends that you configure instances as described in [IBM Guardium System Requirements and Supported Platforms..](#)

## 12. Configure VPC settings.

## 13. Configure Subnet settings.

Note: By default, a public IP address is associated with the instance on deployment. To prevent this, modify the subnet settings in EC2 in order to disable auto-assign IP settings

## 14. Configure your security group settings

Note: Specify ports 22 and 8443 on launch in order to access SSH and the Guardium UI. Additional ports can be specified depending on user needs. For port requirements, see [Guardium Port Requirements.](#)

## 15. Configure Key Pair settings.

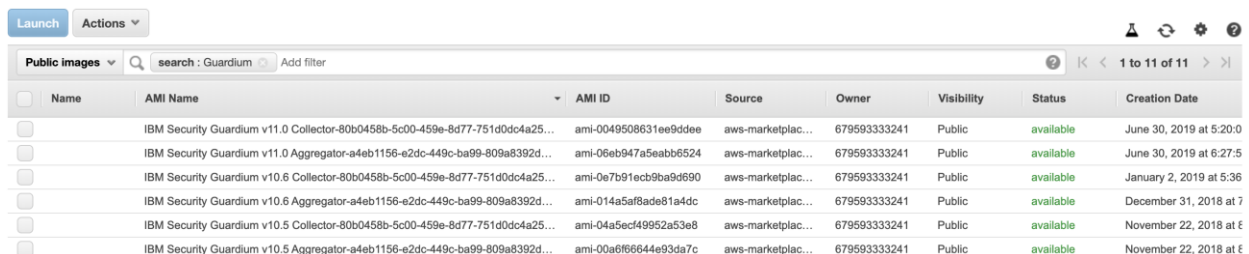
Note: Access to Guardium instances is limited to using a EC2 key pair. Password based authentication is not supported

## 16. Click Launch to launch your Guardium instance.

### *Method 2: Deploying from an Amazon Machine Image (AMI)*

The official Guardium AMIs are listed publicly and are accessible to all other AWS accounts. To access the images, go to the AMIs page and search for “Guardium”.

1. Log in to the AWS EC2 console page at <https://console.aws.amazon.com/ec2/>
2. Under Images click AMIs.
3. Next to the search bar select Public Images, then search for “Guardium.”



The screenshot shows the AWS Management Console interface for the Amazon Machine Images (AMIs) page. At the top, there are tabs for 'Launch' and 'Actions'. Below the tabs is a search bar with the text 'search: Guardium' and an 'Add filter' button. To the right of the search bar, there are icons for help, refresh, settings, and a user profile. Below the search bar, there is a table listing several Guardium AMIs. The table has columns for Name, AMI Name, AMI ID, Source, Owner, Visibility, Status, and Creation Date. The first five rows of the table are visible, showing various Guardium v11.0 and v10.5 Collector and Aggregator AMIs.

Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date
	IBM Security Guardium v11.0 Collector-80b0458b-5c00-459e-8d77-751d0dc4a25...	ami-0049508631ee9ddee	aws-marketplac...	679593333241	Public	available	June 30, 2019 at 5:20:0
	IBM Security Guardium v11.0 Aggregator-a4eb1156-e2dc-449c-ba99-809a8392d...	ami-06eb947a5eabb6524	aws-marketplac...	679593333241	Public	available	June 30, 2019 at 6:27:5
	IBM Security Guardium v10.6 Collector-80b0458b-5c00-459e-8d77-751d0dc4a25...	ami-0e7b91ecb9ba9d690	aws-marketplac...	679593333241	Public	available	January 2, 2019 at 5:36
	IBM Security Guardium v10.6 Aggregator-a4eb1156-e2dc-449c-ba99-809a8392d...	ami-014a5af8ade81a4dc	aws-marketplac...	679593333241	Public	available	December 31, 2018 at 7
	IBM Security Guardium v10.5 Collector-80b0458b-5c00-459e-8d77-751d0dc4a25...	ami-04a5ecf49952a53e8	aws-marketplac...	679593333241	Public	available	November 22, 2018 at 6
	IBM Security Guardium v10.5 Aggregator-a4eb1156-e2dc-449c-ba99-809a8392d...	ami-00a6f66644e93da7c	aws-marketplac...	679593333241	Public	available	November 22, 2018 at 6

4. Select from either the Collector or Aggregator Guardium AMIs.
5. Click Launch to start the Instance creation wizard.

### Create the Guardium Instance

1. On the Choose an Instance Type page select the instance size General Purpose m4.2xlarge (Guardium recommends a minimum of 4 vCPUs and 24GB RAM). Click Next to configure the instance details.
2. Next to network select a VPC.
3. Next to subnet select a subnet from the list.
4. Under Network Interfaces enter an IP address in primary IP address.

Network interfaces ⓘ			
Device	Network Interface	Subnet	Primary IP
eth0	New network interface▼	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	172.31.64.100

5. Click Next to go to the Storage Configuration page.
6. Review the configuration for Storage, then click Next.
7. Add a tag name for the instance, then click Next to configure the Security Group.

### Configure the Security Groups

1. In the Security Configuration Page click on Assign a Security Group.
2. Next to Security Group Name enter a name for the Security Group.
3. Next to Description write a short description for the Security Group.
4. Guardium uses port 8443 to connect to the web UI and port 22 to connect to the CLI. Create these 2 rules:
  - a. Type: SSH, Protocol: TCP, Port Range: 22, Source: Custom
  - b. Type: Custom TCP, Protocol: TCP, Port Range: 8443, Source: CustomNote: Guardium recommends that security group rules allow access from known IP addresses only.

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
SSH ▼	TCP	22	Custom ▼ CIDR, IP or Security Group
Custom TCP Rule ▼	TCP	8443	Custom ▼ CIDR, IP or Security Group

Security Group rules can also be configured for the following on an as needed basis:

- For GIM: “tcp:8444-8446; tcp:8081”
- For FAM: “tcp:16022-16023”
- For Unix STAP: “tcp:16016-16018”
- For Windows STAP: “tcp:9500-9501”
- For Quick Search: “tcp:8983; tcp:9983”
- For MySQL: “tcp:3306”

For a complete list of ports that are used in IBM Security Guardium, see [Guardium port requirements](#).

5. Click Review and Launch.
6. Review the configuration settings then click Launch.
7. Select the Secret Key pair from the drop-down list , then click Launch Instances.

### *Configuration and Settings*

Once the Guardium instance is deployed, the steps below outline how to connect to the instance and how to configure the network settings.

#### *Connect to the instance*

1. Connect to the Guardium GUI: In a browser, go the URL: https://<instance-ip>:8443. The default password for admin, accessmgr, and Guardium UI users is the instance-id.
2. Connect to the CLI. From a terminal, connect via ssh to the command line interface using the private key corresponding to the public key selected when launching the instance:

```
>ssh -i /path/to/private-key cli@<ip-of-gmachine>
```

#### *Set up the Network*

1. From the EC2 > Instances page, find the values for the private IP, subnet mask, internal gateway IP and Internal FQDN of the instance, then run the following CLI network commands to configure the appliance. Answer “yes” to the question “Is it a newly cloned appliance?”..
  - a. Setup the primary (eth0) IP

```
>store net interface ip <instance-ip>
```

- b. Setup the Netmask
    - >store net interface mask <netmask>
  - c. Setup the Gateway
    - >store network route defaultroute <default-router-ip>
  - d. Set the DNS resolver
    - >store network resolver 1 <resolver-ip>
  - e. Setup the system hostname
    - >store system hostname <instance-hostname>
  - f. Setup the system domain
    - >store system domain <instance-domain>
2. Restart the network for all changes to take effect restart network:
- >restart network

IBM Security Guardium Licensed Materials - Property of IBM. © Copyright IBM Corp. 2017, 2019. US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml))