exabeam

Amazon Web Services Setup Guide

Exabeam Security Management Platform - Version SMP 2020.1

Publication date October 13, 2020

Exabeam
1051 E. Hillsdale Blvd.
4th Floor
Foster City, CA 944042

1.844.392.2326

Have feedback on this guide? We'd love to hear from you!
Email us at docs@exabeam.com

Table of Contents

1. Launch an Instance in Amazon Web Services

This guide will detail the process necessary for launching an Exabeam product instance in Amazon Web Services (AWS).

We will cover:

- Sizing specifications of your AWS instance
- The Amazon Machine Image (AMI) setup process
- Data Lake or Advanced Analytics installation

2. Request AMIs to Deploy in AWS

Exabeam has created Amazon Machine Images (AMIs) to deploy your solution. To request access to the AWS image files, visit the *Virtual Images* section in the Exabeam Community. You will need to provide the following information:

- Customer email address
- AWS customer account number
- AWS region of deployment
- Exabeam product to be deployed

> **NOTE**
> Please review all specifications for your deployment and ensure you have sufficient resources (CPU, memory, and storage across all the instances that will be deployed in your account) to deploy the Exabeam AMIs. Additionally, please ensure you have valid Exabeam licenses for the product(s) you will implement.

2.1. Exabeam Platform Specification Table for Virtual Platforms

These are the minimum operating specifications needed to run your Exabeam product. We do not support hybrid deployments (cross environment deployments). All nodes must be in the same subnet.

Be aware that vCPU is not the same as the number of CPUs or Cores for the processor. A vCPU is typically equal to the number of threads in the processor. Also, a hard drive GiB unit (used in AWS) is fractionally larger than a standard GB (1 GiB ~ 1.074 GB).

The tables below details the CPU and memory allocation required for Exabeam products to operate optimally, with the following provisioned:

- The host is not shared with any other product or resource

Advanced Analytics Node Type	AWS
Advanced Analytics Master Node	Instance type: r4.16xlarge Core: 64 vCPU Memory: 488 GiB (~ 523 GB) Storage: Our AMI allocates the following hard-drives: • 1 x 120 GiB GP2 (SSD) • 3 x 894 GiB GP2 (SSD) • 6 x 1860 GiB GP2 (SSD)

Advanced Analytics Node Type	AWS
Advanced Analytics Worker Incident Responder Node	Instance Type: r4.4xlarge Core: 16 vCPU Memory: 122 GiB (~ 130 GB) Storage: Our AMI allocates the following hard drives: • 1 x 120 GiB GP2 (SSD) • 3 x 894 GiB GP2 (SSD) • 6 x 1860 GiB GP2 (SSD)

Table 1. Advanced Analytics Node Specifications

Node Type in Exabeam Cluster		AWS
Before I32*	Data Lake Master	Instance type: r4.4xlarge
	Data Lake Worker Nodes	Core: 16 vCPU Memory: 122 GiB Storage: Please ensure you follow the ordering of storage disks as listed below. Our AMI allocates the following hard-drives: • 1 x 150 GiB GP2 (SSD) • 2 x 2000 GiB GP2 (SSD) • 9 X 2000 GiB ST1 (HDD)
I32 or higher	Data Lake Master	Instance type: r4.8xlarge
	Data Lake Worker Nodes	Core: 32 vCPU Memory: 244 GiB Storage: Please ensure you follow the ordering of storage disks as listed below. Our AMI allocates the following hard-drives: • 1 x 150 GiB GP2 (SSD) • 2 x 2000 GiB GP2 (SSD) • 9 X 4 000 GiB ST1 (HDD)

Table 2. Data Lake Node Specifications

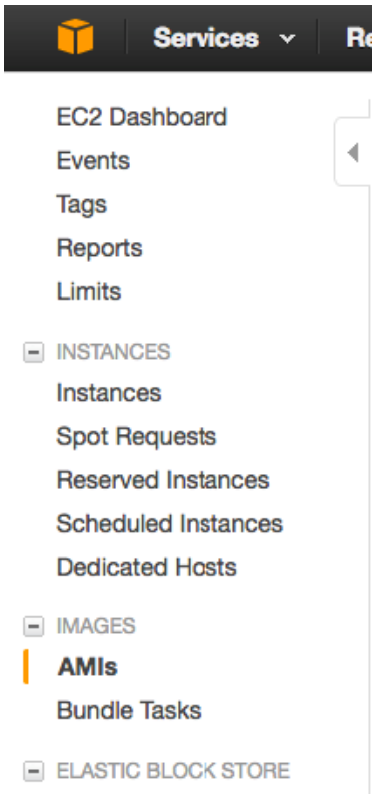
(* If you have an existing Data Lake deployment of 20 nodes or below, we will continue to support the older sizing for up to i32 only. Please contact the Exabeam Technical Account Manager for your team for any questions.)

For clusters with 21 nodes or more, an additional three management nodes are required for cluster management operations, health monitoring and other critical functions.

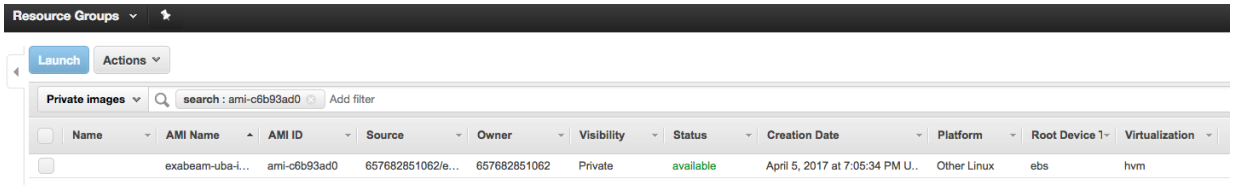
3. Deploy in Amazon Web Services (AWS)

Instantiate each virtual machine in your cluster.

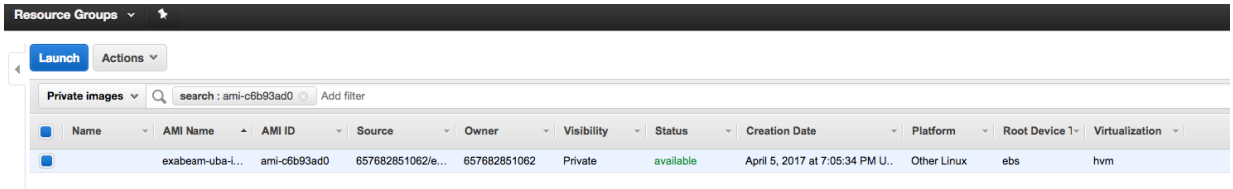
1. In the EC2 Console select **Images** > **AMI** from the menu on the left.



2. Select **Private Images** from the drop-down menu to the left of the search field, then enter your AMI ID in the search field.



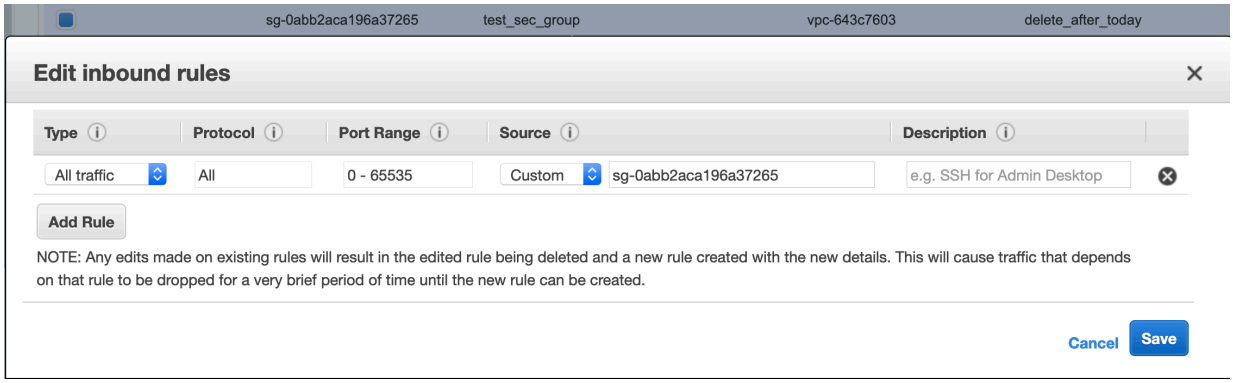
3. In the search results, select the AMI you want to launch by ticking the box to the left. Click **Launch** at the upper left.



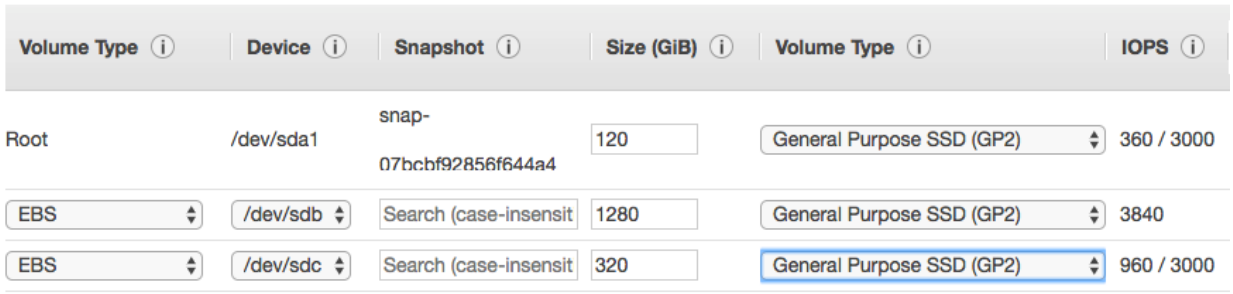
4. The **Choose an Instance Type** window will open.
5. Using the virtual machine specifications guidelines at the beginning of this document, choose an instance that meets your requirements. For example, if your are instantiating a master node, select

the EX-4000 instance for Advanced Analytics. For example, if your are instantiating a master node, select the EX-3000 instance for Data Lake.

6. Select **Next: Configure Instance Details**.
7. For **Configure Instance Details** use the default settings unless there is a need to change the Network and Subnet.
8. Select **Security Group**.
9. At the **Configure Security Group** page, select **Inbound Rules**, and then click **Add Rule** to create a rule with:
   - **Type** - `All traffic`
   - **Source** - Set to your Security Group ID for your pool of peer hosts. (Security group ID is an alpha-numeric string; for example, `sg-asd9867asdf8768`.)



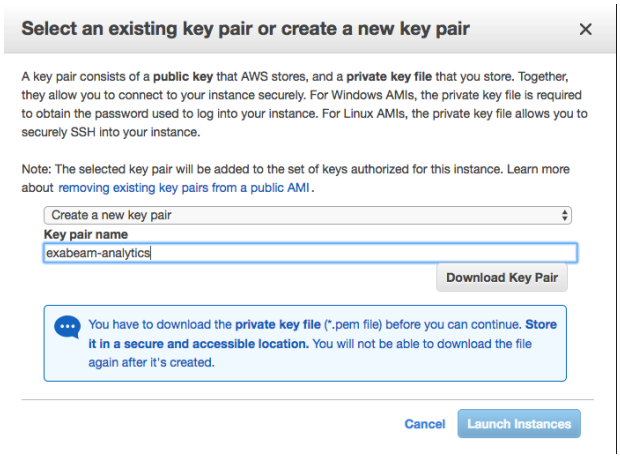
10. Select **Next: Add Storage**. Accept the default configuration.



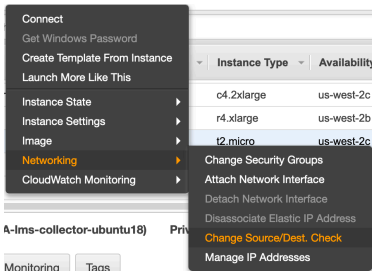
11. Select **Next: Add Tag**.
12. At the **Add Tags** screen, select the **Add Tag** button and give your instance a name. A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value, both of which you define. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. This is useful when you have many resources of the same type—you can quickly identify a specific resource based on the tags you've assigned to it
13. Accept the default values in the remainder fields and select **Review and Launch**.

14. After reviewing your settings, click **Launch**.
15. When prompted to select an existing key pair or create a new key pair, select **Create a new key pair** and name it.

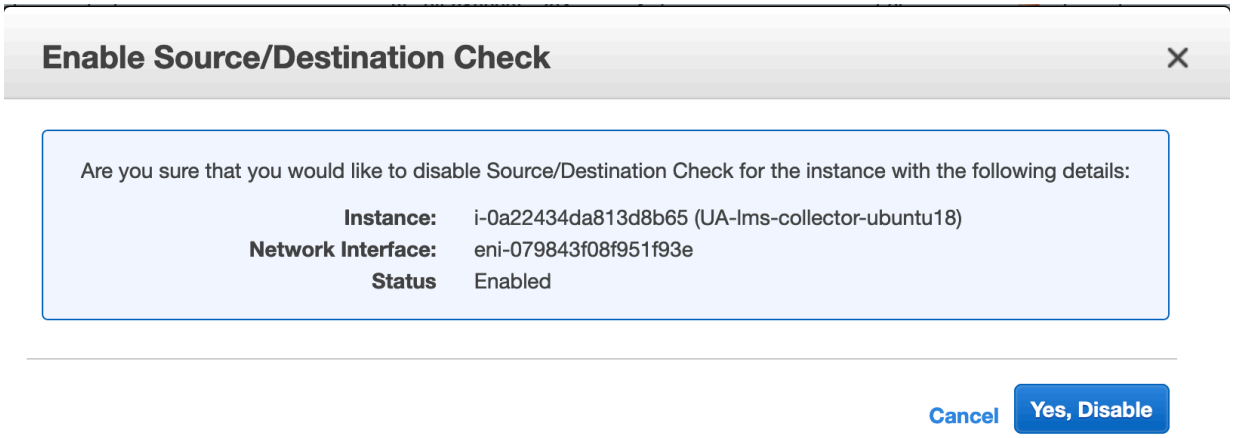
> **NOTE**
> If you saved the key to a *nix system, the key must have 400 permission.



16. Select **Launch Instance**.
17. The instance will take some time to initialize. To check on the status, find the instance in the **Running Instances** page.
18. Disable source and destination checks by selecting your instance and then right-click to select **Networking** > **Change Source/Dest. Check**.



19. Click **Yes, Disable**.



You are now ready to deploy your product. Please refer to your product's Exabeam *Administration Guide* for installation and configuration steps. Use a terminal application, such as Moba Xterm, to connect to the host via SSH.

Appendix A. Network Ports

The table below shows all the ports that Exabeam either connects to or receives connections from. Ensure these ports are configured appropriately for data and communications traversal.

Service	Hosts	Port	TCP	UDP
SSH	All Cluster Hosts	22	✓	
BGP	All Cluster Hosts	179	✓	
Exabeam Web UI (HTTPS)	All Cluster Hosts	8484	✓	
Docker	All Cluster Hosts	2376	✓	
Docker	All Cluster Hosts	2377	✓	
Docker	All Cluster Hosts	4789		✓
Docker	All Cluster Hosts	7946	✓	✓
Docker Registry	Master Host	5000	✓	
Kafka Connector	All Cluster Hosts	8083	✓	
Kafka	All Cluster Hosts	9092	✓	
Kafka	All Cluster Hosts	9093	✓	
Kafka	All Cluster Hosts	9094	✓	
MongoDB	All Cluster Hosts	27017	✓	
MongoDB	All Cluster Hosts	27018	✓	
MongoDB	All Cluster Hosts	27019	✓	
Hadoop	All Cluster Hosts	9000	✓	
Hadoop	All Cluster Hosts	50010	✓	
Hadoop	All Cluster Hosts	50020	✓	
etcd	First 1 or 3 nodes up to highest odd number	2379	✓	
etcd	First 1 or 3 nodes up to highest odd number	2380	✓	
Ping	All Cluster Hosts	ICMP		
Elastalert	All Cluster Hosts	3030	✓	
Disaster Recovery Socks Proxy	Master and Failover Hosts	10022	✓	
NTP	Master Host	123		✓
DNS	All Cluster Hosts	53		✓
SMTP	Master and Failover Hosts	25	✓	
SMTPS	Master and Failover Hosts	587	✓	
Syslog Forwarder	Target Host	514	✓	✓
Syslog Forwarder	All Cluster Hosts	515	✓	
Disaster Recovery MongoDb	Master and Failover Hosts	5123	✓	
Exabeam Coordination Service (Zookeeper)	All Cluster Hosts	2181	✓	
Exabeam Coordination Service (Zookeeper)	All Cluster Hosts	2888	✓	
Exabeam Coordination Service (Zookeeper)	All Cluster Hosts	3888	✓	
Exabeam Data LakeUI	Master Host	5601	✓	
Exabeam SOAR Metrics UI	Case Manager Host	5850	✓	
Exabeam SOAR Server	Case Manager Host	7999	✓	
Exabeam SOAR Server	Case Manager Host	8097	✓	
Exabeam SOAR Server	Case Manager Host	9998	✓	

Service	Hosts	Port	TCP	UDP
Exabeam SOAR Server	Case Manager Host	9999	✓	
Exabeam Advanced Analytics Engine	All Advanced Analytics Martini Hosts	8090	✓	
Exabeam Advanced Analytics API	Master/Main Advanced Analytics Node	8482	✓	
Exabeam Advanced Analytics UI	Master Host	8483	✓	
Exabeam Health Agent	All Cluster Hosts	8659	✓	
Exabeam SOAR-LEMON	Case ManagementHost	8880	✓	
Exabeam SOAR-LEMON	Case Manager Host	8888		
Exabeam SOAR-LEMON	Case ManagementHost	8889	✓	
Exabeam SOAR Syslog	Case Manager Host	9875	✓	✓
Exabeam SOAR Action Controller	OAR Host	9978	✓	
Exabeam Advanced Analytics Engine JMX	All Advanced Analytics Martini Hosts	9003	✓	
Exabeam Advanced Analytics LIME JMX	All LIME Hosts	9006	✓	
Exabeam Replicator	Master Host	9099	✓	
Elasticsearch	All Cluster Case Manager Hosts	9200	✓	
Elasticsearch	All Cluster Case Manager Hosts	9300	✓	
Datadog and Threat Intelligence Service	Master and Failover Hosts	443	✓	

Ensure ports for third-party products allow traffic from Exabeam Hosts.

Service	Port	TCP	UDP
LDAP (Non-secure Connection)	389	✓	
LDAP (Secure Connection)	636	✓	
QRadar	443	✓	
ArcSight ESM	3306	✓	
Ganglia	8081	✓	
Splunk	8089	✓	
ArcSight Logger	9000	✓	
RSA	50105	✓	
eStreamer	8000	✓	