exabeam

Google Cloud Platform Setup Guide

Exabeam Security Management Platform - Version SMP 2020.1

Publication date October 16, 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 Google Cloud Platform (GCP) 4
2. Request Images To Deploy In GCP 5
    2.1. Exabeam Platform Specification Table For Virtual Platforms 5
3. Deploying In Google Cloud Platform (GCP) 7
A. Network Ports 10

1. Launch an Instance in Google Cloud Platform (GCP)

This guide details the process necessary for launching an instance in Google Cloud Platform (GCP).

It covers:

- The sizing specifications of your GCP instance
- The GCP setup process

2. Request Images to Deploy in GCP

To request access to the GCP images, visit the Virtual Images section in the Exabeam Community. You will need to provide the following information:

- The name of the member of your organization that will perform the deployment in GCP
- The business email address of that member of your organization

Your credentials will be added to the Exabeam Google Group to access product images.

> **NOTE**
> Please review all specifications for your platform and ensure you have sufficient resources to deploy Exabeam images. 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.

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	GCP
Advanced Analytics Master Node	vCPU: 40 Cores Memory: 256GB Storage: • 1 x 150 GiB (SSD) • 3 x 894 GiB (SSD) • 6 x 1860 GiB (HDD)
Advanced Analytics Worker Incident Responder Node	vCPU: 20 Memory: 128 GB Storage: • 1 x 150 GiB (SSD) • 3 x 894 GiB (SSD) • 6 x 1860 GiB (HDD)

Table 1. Advanced Analytics Node Specifications

Node Type in Exabeam Cluster		GCP
Before I32*	Data Lake Master Data Lake Worker Nodes	vCPU: 20 Memory: 128 GB Storage: • 1 x 240 GiB (SSD) • 2 x 2000 GiB (SSD) • 9 x 2000 GiB (HDD)
I32 or higher	Data Lake Master Data Lake Worker Nodes	vCPU: 20 Memory: 192 GB Storage: • 1 x 240 GiB (SSD) • 2 x 1920 GiB (SSD) • 9 x 4000 GiB (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. Deploying in Google Cloud Platform (GCP)

Before you begin, please ensure you have been added to the Google Group: Exabeam_GoogleCloudPlatform. To do so, you can contact Exabeam Customer Success by opening a case via Community.Exabeam.com.

The following instructions are for creating hosts using the Google Cloud SDK (command-line tool) command `gcloud`. Please see *Google Cloud SDK* for more information.

1. Connect in to your Google Cloud Platform using `gcloud`.
2. Create templates for host instances based on your deployment needs. Please consult an Exabeam technical representative, if you are unsure which host configuration to implement.

   > **NOTE**
   > If launching in a non-default network for project, you may need to supply network arguments when creating the templates. (For more information, consult GCloud documentation.)

   Execute the following commands for your host type:

   Template for EX-2000 Equivalent Host

   ```
   gcloud compute instance-templates create ex2000 --boot-disk-size 150 --boot-
   disk-type pd-ssd --create-disk=auto-delete=yes,size=894GB,type=pd-ssd --
   create-disk=auto-delete=yes,size=1860GB,type=pd-standard --create-disk=auto-
   delete=yes,size=1860GB,type=pd-standard --machine-type custom-20-131072 --
   image-project exabeam-images --image-family exabeam-centos-7 --no-address --
   can-ip-forward
   ```

   Template for EX-4000 Equivalent Host

   ```
   gcloud compute instance-templates create ex4000 --boot-disk-size 150 --boot-
   disk-type pd-ssd --create-disk=auto-delete=yes,size=894GB,type=pd-ssd --
   create-disk=auto-delete=yes,size=894GB,type=pd-ssd --create-disk=auto-
   delete=yes,size=894GB,type=pd-ssd --create-disk=auto-
   delete=yes,size=1860GB,type=pd-standard --create-disk=auto-
   delete=yes,size=1860GB,type=pd-standard --create-disk=auto-
   delete=yes,size=1860GB,type=pd-standard --create-disk=auto-
   delete=yes,size=1860GB,type=pd-standard --create-disk=auto-
   delete=yes,size=1860GB,type=pd-standard --create-disk=auto-
   delete=yes,size=1860GB,type=pd-standard --machine-type custom-40-262144 --
   image-project exabeam-images --image-family exabeam-centos-7 --no-address --
   can-ip-forward
   ```

   Template for EX-3000 Equivalent Host

   ```
   gcloud compute instance-templates create ex3000 --boot-disk-size 240 --boot-
   disk-type pd-ssd --create-disk=auto-delete=yes,size=2000GB,type=pd-ssd --
   create-disk=auto-delete=yes,size=2000GB,type=pd-ssd --create-disk=auto-
   delete=yes,size=2000GB,type=pd-standard --create-disk=auto-
   delete=yes,size=2000GB,type=pd-standard --create-disk=auto-
   delete=yes,size=2000GB,type=pd-standard --create-disk=auto-
   ```

```
delete=yes,size=2000GB,type=pd-standard --create-disk=auto-
delete=yes,size=2000GB,type=pd-standard --create-disk=auto-
delete=yes,size=2000GB,type=pd-standard --create-disk=auto-
delete=yes,size=2000GB,type=pd-standard --create-disk=auto-
delete=yes,size=2000GB,type=pd-standard --create-disk=auto-
delete=yes,size=2000GB,type=pd-standard --machine-type custom-20-131072 --
image-project exabeam-images --image-family exabeam-centos-7 --no-address --
can-ip-forward
```

3. Instantiate your host from a template.
   `gcloud compute instances create --source-instance-template [host_template] [hostname]`
   To instantiate multiple hosts with the same template, separated hostnames by space.
4. Create an SSH key.
   a. Enter the following command

      ```
      ssh-keygen -t rsa
      ```

   b. Enter the file in which you want to save the SSH key

      ```
      (/home/exabeam/.ssh/id_rsa): key.pem
      ```

   c. You will be asked to generate a passphrase. Skip this by hitting "enter" on your keyboard twice.
   d. Enter the following commands.

      ```
      chmod 400 key.pem
      sudo mkdir -p /opt/exabeam_installer/.ssh
      sudo mv key.pem* /opt/exabeam_installer/.ssh/
      cat /opt/exabeam_installer/.ssh/key.pem.pub
      ```

5. Copy the entire output content (generated in the previous step).
6. Add the SSH key.
   a. WIthin your Google Cloud account, navigate to the Exabeam project > **Compute Engine** > **Metadata** > **SSH Keys**.
   b. Click **Edit**.
   c. Click **Add Item**.
   d. Paste the entire contents of the SSH key (copied in the previous step) to the input box.
   e. Click **Save**.
7. Log in to the instance using SSH and <username>@<external ip>.
8. Change user to use the Exabeam account with "sudo su exabeam".
9. Download the .sxb to the `/home/exabeam directory`.

10. Run `chmod +x <release>.sxb`, replacing `<release>` with the name of the .sxb file you are installing. (Download the release you need from the Exabeam Community)

You are now ready to install.

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	✓	