Copyright

All content in this document, including text, graphics, logos, icons, images, and video clips, is the exclusive property of Exabeam or its content suppliers and is protected by U.S. and international copyright laws. The compilation (meaning the collection, arrangement, and assembly) of all content in this document is the exclusive property of Exabeam and is also protected by U.S. and international copyright laws. The content in this document may be used as a resource. Any other use, including the reproduction, modification, distribution, transmission, republication, display, or performance, of the content in this document is strictly prohibited.

Copyright ©2020 Exabeam, Inc. All Rights Reserved.

Trademarks

Exabeam, the Exabeam logo, Threat Hunter, Smarter SIEM, Smart Timelines and Security Management Platform are service marks, trademarks or registered marks of Exabeam, Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. The marks and logos displayed in this document may not be used without the prior written consent of Exabeam or their respective owners.

Patents

Exabeam owns, and reserves all rights for, patents for Exabeam products and services, which may be protected under registered patents as well as patents pending.

Other Policies

For information regarding Exabeam’s treatment of personally identifiable information, please review Exabeam’s current privacy policy at www.exabeam.com/privacy.
# Table of Contents

1. Exabeam Data Lake Architecture Overview ................................................................. 6
   1.1. How Exabeam Data Lake Works ............................................................................... 7
   1.2. Exabeam Log Collectors In Data Lake ................................................................. 7
      1.2.1. Exabeam Data Lake Agent Collector ................................................................ 8
      1.2.2. Exabeam Data Lake Server Side Collector ....................................................... 8
   1.3. Exabeam Data Lake Ingestion ............................................................................... 9
   1.4. Exabeam Data Lake Indexer ............................................................................... 9
      1.4.1. Parsing ........................................................................................................... 9

2. Exabeam Product Deployment In On-Premises Or Virtual Environments .................... 10
   2.1. Considerations For Installing And Deploying Exabeam Products ......................... 10
      2.1.1. Hardware And Virtual Deployments Only ....................................................... 10
      2.1.2. Supported Exabeam Deployment Configurations ........................................... 11
   2.2. Installation Pre-Check For Exabeam Products ....................................................... 12
   2.3. Install Exabeam Software .................................................................................. 12
   2.4. Upgrade An Exabeam Product ........................................................................... 20
      2.4.1. Upgrading For Data Lake Large Clusters ....................................................... 21
      2.4.2. Updating Data Lake Parsers And Event Categories ....................................... 22
      2.4.3. Disk Usage Automatic Clean Up For Upgrades .............................................. 22
   2.5. Troubleshooting An Installation ......................................................................... 23
      2.5.1. Ansible Failure ............................................................................................. 23
      2.5.2. Error: Multiple Interfaces Detected ............................................................... 23

3. Administrator Operations ............................................................................................ 24
   3.1. Exabeam Licenses ............................................................................................. 24
      3.1.1. License Lifecycle ............................................................................................ 24
      3.1.2. Types Of Exabeam Product Licenses ............................................................. 25
      3.1.3. License Versions ............................................................................................. 25
      3.1.4. Download An On-Premises Or Cloud Exabeam License .................................. 26
   3.2. Exabeam Hardening ............................................................................................ 26
      3.2.1. How To Enable Cross-Site Request Forgery Protection .................................. 27
      3.2.2. How To Enable Cross-Origin Resource Sharing Protection ............................ 28
   3.3. Adding Nodes To A Cluster .................................................................................. 30
      3.3.1. Add Nodes ..................................................................................................... 30
   3.4. Replicating Logs Across Exabeam Data Lake Clusters ............................................ 31
   3.5. Ingesting Logs Into Exabeam Data Lake ............................................................. 32
   3.6. Exabeam Data Lake Retention Settings ................................................................ 33
      3.6.1. Exabeam Data Retention And Enforcement .................................................. 33
   3.7. Remote Archiving NAS And AWS S3 From Data Lake ........................................... 34
      3.7.1. Archiving Prerequisites ................................................................................. 34
      3.7.2. Archive And Restoration Performance .......................................................... 34
      3.7.3. Set Retention Policies For Exabeam Data Lake Logs ..................................... 35
      3.7.4. Set Up An Archive Destination For Exabeam Data Lake Logs ....................... 35
      3.7.5. Archive Destination Management For Exabeam Data Lake Logs .................... 38
      3.7.6. Restore Data To Exabeam Data Lake ............................................................ 41
   3.8. Set Up LDAP Import ........................................................................................... 43
9. Cross-Cluster Search In Exabeam Data Lake ................................................................. 112
  9.1. Prerequisites For Exabeam Data Lake Cross-Cluster Search ................................. 112
  9.2. Remote Cluster Management For Exabeam Data Lake Cross-Cluster Search .......... 112
  9.3. Register A Remote Cluster In Exabeam Data Lake For Cross-Cluster Search .............. 113
  9.4. Exabeam Data Lake Cross-Cluster Health Monitoring And Handling .................. 115
  9.5. How To Enable/Disable/Delete Exabeam Data Lake Remote Clusters For Cross-Cluster Search ................................................................................................................. 116
  9.6. Exabeam Data Lake Remote Cluster Data Access Permissions For Cross-Cluster Search ............................................................................................................................ 116
    9.6.1. Role-Based Permissions ............................................................................... 116
    9.6.2. Cluster-Based Permissions ........................................................................... 117
10. Exabeam Cloud Telemetry Service .................................................................................. 118
  10.1. Prerequisites ....................................................................................................... 118
  10.2. Types Of Telemetry Data In Exabeam Cloud Telemetry Service ................................. 118
    10.2.1. Metrics ........................................................................................................ 118
    10.2.2. Events ........................................................................................................ 119
    10.2.3. Environment .............................................................................................. 119
  10.3. Data Collected By Exabeam Cloud Telemetry Service ........................................... 119
    10.3.1. How To Disable Exabeam Cloud Telemetry Service ....................................... 121
11. System Health Page ....................................................................................................... 123
  11.1. Proactive And On-Demand System Health Checks ................................................. 123
    11.1.1. Data Lake Specific Health Checks ................................................................. 124
    11.1.2. How To Configure System Health Alert Notifications .................................... 125
  11.2. Data Lake Cluster Health Status ......................................................................... 125
  11.3. ElasticSearch Status In Exabeam Data Lake ......................................................... 126
    11.3.1. ElasticSearch Details .................................................................................. 127
    11.3.2. Shard Stats ............................................................................................... 127
  11.4. Get To Know The Exabeam Data Lake Indexing Metrics Tab ............................... 127
    11.4.1. Data Lake Flow ......................................................................................... 127
    11.4.2. Available Indexes ...................................................................................... 128
    11.4.3. Host Metrics ............................................................................................. 129
A. Technical Support Information ....................................................................................... 130
B. List Of Exabeam Services ............................................................................................ 131
C. Network Ports ............................................................................................................. 132
D. Supported Browsers ..................................................................................................... 134
1. Exabeam Data Lake Architecture Overview

Data Lake is one of three elements in Exabeam's Security Management Platform (SMP) and the data ingested by Data Lake can be used by Advanced Analytics for analysis and Incident Responder while investigating incidents.

At a high level, Data Lake involves four main processes:

- Log collection
- Log processing
- Data presentation (searching, visualizing, reporting, dashboards, etc)

The system flow begins with the log collectors, which deployed either on the Data Lake server (for example, agent collector, Exabeam Site Collector, Exabeam Cloud Connector, database collector, Cisco eStreamer) or at local machines, collecting operational data, system metrics, and more. The Log Collectors then send those logs to the Log Ingestor.

The Log Ingestor can consume events from log collectors, syslog sources, or an existing SIEM. The log ingestor provides flow control and pushes the logs to the log indexer.

The log indexer is the piece that is responsible for parsing and enriching before indexing and storing the logs in a distributed search cluster.

Data Lake is offered for hardware and virtual deployments as well as for SaaS.

Figure 1. Exabeam Data Lake Hardware and Virtual Architecture
### 1.1. How Exabeam Data Lake Works

Data Lake indexes data from the servers, applications, databases, network devices, virtual machines, and so on, that make up your IT infrastructure. Data Lake can collect the data from machines located anywhere, whether it is local, remote, or cloud. Most users connect to Data Lake through a web browser to run searches and create dashboards. Other forms to connect to Data Lake include API streams from log collectors and ingesters. Additionally, Data Lake can push parsed logs to Exabeam Advanced Analytics or your SIEM.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exabeam Log Collectors</td>
<td>Agent/Server-based log collectors, SaaS collectors, and cloud connectors</td>
</tr>
<tr>
<td>Exabeam Log Ingestor</td>
<td>Consumes events from Syslog and Connectors, providing flow control before pushing to Log Indexer</td>
</tr>
<tr>
<td>Exabeam Log Processor</td>
<td>Responsible for parsing, enriching, and indexing log events that are then stored in a distributed cluster</td>
</tr>
<tr>
<td>Exabeam Data Lake UI</td>
<td>The Web interface used for searching log events, creating charts, and viewing dashboards</td>
</tr>
</tbody>
</table>

**Table 1. Exabeam Data Lake Components**

### 1.2. Exabeam Log Collectors in Data Lake

Data Lake can collect the data from machines located anywhere, whether it is local, remote, or cloud. It provides an out-of-the-box, file-based collector and Windows event collector. It also supports organizations that collect:

- Data from devices communicating via the Cisco eStream protocol
- Logs via cloud applications (PaaS, IaaS, and SaaS)
• Logs via databases

Most customer environments will utilize a combination of both server-side and agent connectors.

We can deploy and run local agents on machines from which logs must be collected and aggregated. We can also receive Syslogs that are sent to our Log Ingestor from your SIEM or another third-party security service such as FireEye, Symantec, and many others.

Regardless of the method by which Data Lake collects logs, once they are accepted by the Log Ingestor they are treated exactly the same.

**NOTE**

Data Lake is optimized to support up to 1,500 collectors for clusters with 2 or more hosts. For single host clusters, up to 700 collectors is supported. There may be up to a 10% EPS performance degradation and up to a 20% increase in search latency, based on the number of collectors.

### 1.2.1. EXABEAM DATA LAKE AGENT COLLECTOR

Exabeam supports three types of agents for log collection:

- **Windows Log Collectors** – Installed on Windows machines.
- **File Log Collectors** – Installed on Windows or Linux machines.
- **Gzip Log Collectors** – Installed on Windows or Linux machines.

These are lightweight processes that are installed on machines (i.e. workstations, servers) to capture operational data such as hardware events, security system events, application events, operating system metrics, network packets, health metrics, etc. The connectors read from one or more event logs and Gzipped logs. The connectors watch the event logs and send any new events in real time. The read position is persisted in order to allow the connectors to resume after restarts.

While file log collectors can be installed on Windows machines, they will only collect file inputs and will not collect windows event logs. If you would like to capture Windows event logs you must install Windows Event collectors.

Gzip file collectors process Gzipped files and publish them to Exabeam Data Lake.

### 1.2.2. EXABEAM DATA LAKE SERVER SIDE COLLECTOR

Direct log collection is supported on Data Lake. Essentially, as long as there is a way to send syslog from a device (such as Windows or Unix servers) or a security solution (such as a DLP solution), Data Lake can ingest them. Alternatively, Data Lake can remotely connect to databases and Cisco eStream to fetch logs. In addition, Data Lake can also ingest logs from any device capable of sending Syslog (e.g. DLP, Firewall).

Data Lake supports data collection from the following log sources:

- Syslog
- DB Collectors for MySQL, MS-SQL, Oracle, PostgreSQL
• eStreamer

Through Cisco eStreamer Collectors, Data Lake provides the ability for organizations to collect data from their Cisco FireSight systems. Like the three collectors mentioned above, the eStreamer collector is a service that runs on the Data Lake appliance and connects to the remote servers communicating over the Cisco eStreamer protocol.

1.3. Exabeam Data Lake Ingestion

The Data Lake Ingestion Engine serves as an aggregator, accepting logs via Syslog or via Log Collectors. It supports a variety of inputs that simultaneously pull in events from a multitude of common sources, unifying your data regardless of format or schema.

Data Lake processes streams of records as they occur and builds real-time streaming data pipelines that reliably move data between systems. It organizes all the incoming logs and builds a message queue to the Indexer, buffering and controlling the volume of logs coming into the Indexer.

⚠️ WARNING

Data Lake architecture is optimized to ingest log events that are less than 1 MB per event. This is a high safety limit that many customers will never hit. Please contact Exabeam Customer Success to assist in fine tuning this value.

• Syslog- The Ingestor will accept syslog via a syslog ingestor instance listening on multiple ports and protocols. The messages will be written to a Kafka message queue. We highly recommend the use of a load balancer to distribute your syslog data across your various nodes in the Data Lake cluster. The collector will accept syslog via TLS on ports 515/TCP and 514/TCP or /UDP. The messages will be forwarded to a message queue.

• Collectors- These are deployed on customer systems or Data Lake clusters and will send messages to Data Lake directly.

1.4. Exabeam Data Lake Indexer

The Data Lake Indexer accepts raw logs from the Ingestor and then parses relevant information from each log, enriches the data with contextual information, then indexes each log for full-text searching in near real time. The indexer dynamically transforms and prepares your data regardless of format or complexity.

1.4.1. PARSING

One of the purposes of indexing data is to turn verbose messages into user-readable data structures. Data Lake extracts pre-defined fields from the logs by running them through a series of parsers. Log events are “typed” as defined by the parsers. For example, a Windows 4624 event from any collector such as Splunk or Exabeam Cloud Connector would be “typed” as windows-4624.

The original log data, along with the parsed fields, are searchable.
2. Exabeam Product Deployment in On-premises or Virtual Environments

Hardware and Virtual Deployments Only

Before installing Exabeam products, ensure you have deployed the supported operating system and configurations. Please review all instructions for setting up hosts that will run Exabeam tasks. See the setup guides that apply to your operating environment.

There are a series of prerequisites to implement before installing Exabeam products. There are a number of ports, protocols, and URLs that must be opened and white-listed. We highly recommend reading through the Considerations for Installing and Deploying Exabeam Products and tackling these requirements early. This will ensure that the setup goes smoothly and quickly.

2.1. Considerations for Installing and Deploying Exabeam Products

2.1.1. HARDWARE AND VIRTUAL DEPLOYMENTS ONLY

Before you install and deploy an Exabeam product, ensure you have set up your physical, virtual machine, or Cloud Exabeam appliance. For more information on setting up your environment, please refer to our appliance, virtual machine, and Cloud appliance setup guides.

The installation prompts ask a series of questions regarding how you want your node cluster and distributed file system configured.

Have the following prepared before starting:

- exabeam user account credentials with installation privileges. DO NOT ATTEMPT TO RUN THIS INSTALLATION AS ROOT. If this is an upgrade, go to the last bullet item below.
- SSH key for authenticating sessions between hosts. (Authentication using SSH password method is not preferred. SSH password method is not supported for AWS and GCP deployments.)
- If you are using an external Certificate Authority (CA), please consult an Exabeam technical representative before installation.
- IP address(es) and hostname(s) of new node servers.
- Preferred NTP and DNS hostnames and addresses.
- Docker BIP and Calico subnet (cannot be an existing IP space or in use), if not using default settings
- For virtual or cloud installations, obtain access to instance images or configurations for your platform. Contact your Exabeam representative for more information.
- If you are setting up a disaster recovery scheme, please consult Disaster Recovery Deployment.
- A terminal/screen session (SSH access).

Run deployment scripts only on the master node host. The deployment process will automatically install to worker hosts from the master node/host.

Repeat the deployment process at standby nodes. Secondary sites and standby nodes should have the same resources and capacities as the primary site and its nodes.
If you are installing new or upgrading from Data Lake i24 or earlier, you must meet the following requirements before installing or upgrading to this release:

- **AWS deployments**: All nodes MUST have src/dest (source/destination) checks turned off.
- **GCP deployments**: The firewall rules must allow IP protocol 4 (IP-in-IP or IPIP) traffic within the cluster. While setting up your TCP/UDP ports, ensure the Other protocols box is checked and in the input box type ipip, and then save the setting.

- Nodes allow traffic to and from security group to itself.
- For Data Lake, use a load balancer in front of your cluster and use TCP (not UDP) as a transmission protocol between the load balancer and the Exabeam Data Lake hosts. A load balancer is required (customer-provided) in front of Data Lake in order to have no downtime for Syslog ingestion during the upgrade.

If you have questions about the prerequisites or installation approaches, please create a support ticket at Exabeam Community to connect with a technical representative who can assist you.

### 2.1.2. SUPPORTED EXABEAM DEPLOYMENT CONFIGURATIONS

#### Hardware and Virtual Deployments Only

The tables below show the supported deployment configurations for Exabeam products and modules. When running the installation scripts, the various packages will be referred to by Exabeam module names.

#### 2.1.2.1. Data Lake Deployment Configurations

For deployments with a cluster of 21 or more hosts, it is mandatory to have three management nodes in the worker node pool. Designating three worker nodes as host management nodes is a prerequisite to ensure that the cluster maintains optimal processing performance.

- **lms = Data Lake**
  - lms_master = Data Lake master host; orchestration and console/API node
  - lms_slave = Data Lake worker host; data and processing node

<table>
<thead>
<tr>
<th>Node Host</th>
<th>lms_master</th>
<th>lms_slave</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Node</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Worker Node 1</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Worker Node 2</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>


2.2. Installation Pre-Check for Exabeam Products

Hardware and Virtual Deployments Only

When deploying your Exabeam product, a series of automated pre-checks test your platform to ensure servers meet Exabeam's requirements in terms of available resources (memory, CPU, disks), OS configuration, etc. Any failures or warnings indicate your system will likely fail to deploy, and should be remedied before continuing.

A successful pre-check will conclude with **All checks passed.**

```
| => cd /opt
| => python exa_pre_check.py
INFO exa_pre_check.py 2018-08-07 21:42:39,921 verify_precheck_results 111:Pre-check SSHDPrecheck passed at host: localhost . OK
INFO exa_pre_check.py 2018-08-07 21:42:39,921 verify_precheck_results 111:Pre-check OSVersionPrecheck passed at host: localhost . OK
INFO exa_pre_check.py 2018-08-07 21:42:39,921 verify_precheck_results 111:Pre-check FreeRootSpacePrecheck passed at host: localhost . OK
INFO exa_pre_check.py 2018-08-07 21:42:39,921 verify_precheck_results 111:Pre-check FreeExabeamDataSpacePrecheck passed at host: localhost . OK
INFO exa_pre_check.py 2018-08-07 21:42:39,921 verify_precheck_results 111:Pre-check FreeMongoSpacePrecheck passed at host: localhost . OK
INFO exa_pre_check.py 2018-08-07 21:42:39,921 verify_precheck_results 121:All checks passed.
```

An **unsuccessful** pre-check will conclude the following messages and it is advised you do not upgrade until checks have passed.

```
WARNING exa_pre_check.py 2018-08-09 22:06:48,353 verify_precheck_results 103:Precheck FreeMongoSpacePrecheck failed at host: 10.10.2.81 . Please make sure you have enough disk spaces at /opt/exabeam/data/mongo .
ERROR exa_pre_check.py 2018-08-09 22:06:48,353 verify_precheck_results 105:There are problems with your environment, but deployment may still continue. It is recommended that you correct the above problems if possible.
```

2.3. Install Exabeam Software

Hardware and Virtual Deployments Only

The instructions below are for new installations using the fresh_install steps. Installations should only run on Exabeam supported or approved hardware and platforms. For upgrades, please see Upgrading Exabeam Software

**To install Exabeam software:**

1. Download Exabeam_[product]_[build_version].sxb file from Exabeam Community that you want to install. Transfer the downloaded SXB to /home/exabeam or anywhere on the master node except /opt/exabeam_installer.

---

**NOTE**

For AWS, disable source/destination checks on all cluster hosts. This is necessary for the network technology in Data Lake.
2. Start a new terminal session using the `exabeam` credentials (do not run as ROOT).
3. Initiate a screen session. This is mandatory and will prevent accidental termination of your session.
   
   ```
   screen -LS [yourname]_[todaysdate]
   ```
4. Change the permission of the file using:
   
   ```
   chmod +x Exabeam_[product]_[build_version].sxb
   ```
5. Execute the following command:
   
   ```
   ./Exabeam_[product]_[build_version].sxb fresh_install
   ```

**NOTE**

If your installation is disrupted and needs to be resumed, execute the following:

```
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

Then select the "Deploy Cluster" menu option. If the network connection to the Exabeam host is dropped at any point during the installation, type `screen -r [yourname]_[todaysdate]` to reattach the screen session.

6. The following are prompts based on the product you are installing.
   a. **For Advance Analytics, Case Manager, and Incident Responder**:
      
      Indicate how your nodes should be configured. There are many possible deployment combinations.
      
      For example, to configure a multi-node environment with Advanced Analytics installed on the master node (node 1) and Case Manager installed on the worker node (node 2):

      ```
      Which product(s) do you wish to add? ['uba', 'ml', 'dl', 'cm'] uba cm
      How many nodes do you wish to add? (minimum: 2) 2
      What is the IP address of node 1 (localhost/127.0.0.1 not allowed)? [node1_address]
      What are the roles of node 1? ['uba_master', 'uba_slave']: uba_master
      What is the IP address of node 2 (Localhost/127.0.0.1 not allowed)? [node2_address]
      What are the roles of node 2? ['cm', 'uba_slave']: cm
      ```

      To configure an environment with multiple ingestion nodes, with Advanced Analytics installed on the master node (node 1), three ingestion nodes (node 2, 3, and 4), and a worker node (node 5):

      ```
      Which product(s) do you wish to add? ['uba', 'ml', 'dl', 'cm'] uba
      How many nodes do you wish to add? (minimum: 2) 5
      What is the IP address of node 1 (localhost/127.0.0.1 not allowed)? [node1_address]
      What are the roles of node 1? ['uba_master', 'uba_slave','uba_lime']: uba_master
      ```
What is the IP address of node 2 (localhost/127.0.0.1 not allowed)?
[node2_address]
What are the roles of node 2? ['uba_slave', 'uba_lime']:
[uba_lime]
What is the IP address of node 3 (localhost/127.0.0.1 not allowed)?
['uba_slave', 'uba_lime']:
[node3_address]
What are the roles of node 3? ['uba_slave', 'uba_lime']:
[uba_lime]
What is the IP address of node 4 (localhost/127.0.0.1 not allowed)?
['uba_slave', 'uba_lime']:
[node4_address]
What are the roles of node 4? ['uba_slave', 'uba_lime']:
[uba_lime]
What is the IP address of node 5 (localhost/127.0.0.1 not allowed)?
['uba_slave', 'uba_lime']:
[node5_address]
What are the roles of node 5? ['uba_slave', 'uba_lime']:
[uba_slave]

This IP assign step will repeat until all nodes are assigned addresses.

To configure a single-node environment, follow the same process but input the IP address of just one node.

b. **For Data Lake**: The minimum number of nodes you need must match your product selection and sizing. The example below is for a large multi-node environment where Node 1 (master), Node 2 (worker) and Node 3 (worker) are designated for management functions. Node 4 onwards are worker nodes that process data. A single-node environment will be the same process, except you will only be asked for the IP address of one node.

⚠️ **WARNING**

If you are deploying a cluster with 21 nodes or more, three of the nodes will be automatically assigned as the role of host management node. The first three nodes will be designated host management nodes.

Which product(s) do you wish to add? ['uba', 'ml', 'dl', 'cm']
[dl]
How many nodes do you wish to add? (minimum: 2) 3
What is the IP address of node 1 (localhost/127.0.0.1 not allowed)?
[node1_address]
What are the roles of node 1? ['lms_master', 'lms_slave']:
[lms_master]
What is the IP address of node 2 (localhost/127.0.0.1 not allowed)?
[node2_address]
What is the IP address of node 3 (localhost/127.0.0.1 not allowed)?
[node3_address]
What is the IP address of node 4 (localhost/127.0.0.1 not allowed)?
[node4_address]

This IP assign step will repeat until all nodes are assigned addresses.

7. **Valid credentials (SSH Keys) are needed for inter-node communications.** The example below uses an internal path for the path to the SSH Private Key, which you must replace with your own. The path to the SSH Private Key must be an absolute path. Follow instructions:

⚠️ **NOTE**

If you have set up the instance in AWS or GCP, you must use the same private key shared across all the instances.
a. Follow these instructions if you already have an SSH Private Key. This is the preferred method. Contact your Exabeam representative if you need assistance.

The nodes within the Exabeam cluster communicate with each other regarding the processing status of the jobs, health status of the services etc. Valid credentials (ssh keys) are needed for secure inter-node communications.

Do you have a ssh private key that can be used for internode communications? (If you don't have one, answer 'n' and we will create one for you. If you are running Exabeam on Amazon Web Services, you need to use the SSH key that the instance was launched with.) [y/n] y

What's the path to the ssh private key? [/opt/exabeam_installer/.ssh/key.pem] /home/exabeam/.ssh/key.pem

What's the user name used to deploy the public ssh key? This user must exist and have sudo power. [exabeam] exabeam

Does Exabeam need password or SSH key to log in to all hosts? (This credential is needed only to put the SSH key on the machines. All communications moving forward will use the SSH key.)
1) password
2) SSH key
['1','2']: default (none): 2

What's the path to the ssh private key? [/opt/exabeam_installer/.ssh/key.pem] /opt/exabeam_installer/.ssh/key.pem

b. Follow these instructions if you need to generate an SSH Private Key. This method is not supported for AWS and GCP deployments.

The nodes within the Exabeam cluster communicate with each other regarding the processing status of the jobs, health status of the services etc. Valid credentials (ssh keys) are needed for secure inter-node communications.

Do you have a ssh private key that can be used for internode communications? (If you don't have one, answer 'n' and we will create one for you. If you are running Exabeam on Amazon Web Services, you need to use the SSH key that the instance was launched with.) [y/n] n

We will generate a new ssh key for the deployment at /opt/exabeam_installer/.ssh/key.pem

What's the user name used to deploy the publish ssh key? This user must exist and have sudo power. [exabeam] exabeam

Does Exabeam need password or SSH key to log in to all hosts? (This credential is needed only to put the SSH key on the machines. All communications moving forward will use the SSH key.)
1) password
2) SSH key
['1', '2']: default (None): 1
You will be prompted several times for password.
Password: [password]

8. The installation will automatically partition your drives. However, if auto-detection fails, you will be prompted to manually configure your partitions.
You will be given a suggested storage layout, which you can accept or override.

Unable to autodetect drive types for host
Check if drive configuration/override is needed.

You will be given a suggested storage layout, which you can accept or override. If you choose to accept the auto-suggested drive mapping, type `y` and then proceed to the next step. If you choose to map the drives yourself, type `n` and follow the prompts to configure your drives to match the parameters in the table below.

<table>
<thead>
<tr>
<th>Exabeam Equivalent</th>
<th>/dev/xvdb</th>
<th>/dev/xvdc</th>
<th>/dev/xvdd</th>
<th>Remainder Drives</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX-3000 Data Lake nodes</td>
<td>LVM (1)</td>
<td>LVM (1)</td>
<td>Dedicated Mount (2)</td>
<td>Dedicated Mount (2)</td>
</tr>
</tbody>
</table>

To manually configure your drives, apply the parameters for the role and node you have assigned your host:

EX[appliance_type] mapping applied.

```
{
    [suggested drive mappings]
    ...
    [suggested drive mappings]
}
```
Please review the above, would you like to apply this drive mapping automatically to the host? (Use lsblk or fdisk to verify on a separate screen) [y/n] n

To map an EX3000:

Please specify the drive purpose.
We typically put SSDs on the LVM for services requiring fast I/O (data, mongo, es_hot), and HDDs for dedicated services like hadoop, elasticsearch, kafka.
Ideally your host should have a mix of SSDs (fast) and HDDs (slow), so you should set your drive purpose accordingly to the Exabeam appliance specs.
Important: If your host has all SSDs mounted, please mark the drive purpose for dedicated mounts, and the rest for the LVM.
The size of the drive should be a good indicator as to which purpose it should be assigned to (larger sizes go to the dedicated mounts).
Important: you should not provision all your disks to the LVM, or the
dedicated mounts, there should be a mix.

```json
{ 'device': '/dev/xvdb',
  'driver': 'xvd',
  'model': 'Xen Virtual Block Device',
  'size': '1031GB',
  'table': 'unknown'}
```

1) Provision device /dev/xvdb to LVM (for data, mongo, or es_hot)
2) Provision device /dev/xvdb to dedicated mounts (for hadoop, kafka, or elastic search)
   [{'1', '2'}]: default (None): 1

```json
{ 'device': '/dev/xvdc',
  'driver': 'xvd',
  'model': 'Xen Virtual Block Device',
  'size': '1031GB',
  'table': 'unknown'}
```

1) Provision device /dev/xvdc to LVM (for data, mongo, or es_hot)
2) Provision device /dev/xvdc to dedicated mounts (for hadoop, kafka, or elastic search)
   [{'1', '2'}]: default (None): 1

```json
{ 'device': '/dev/xvdd',
  'driver': 'xvd',
  'model': 'Xen Virtual Block Device',
  'size': '2147GB',
  'table': 'unknown'}
```

1) Provision device /dev/xvdd to LVM (for data, mongo, or es_hot)
2) Provision device /dev/xvdd to dedicated mounts (for hadoop, kafka, or elastic search)
   [{'1', '2'}]: default (None): 2

Select Option 2 for the remainder drives.

9. The following values are recommended.
   a. **For Advanced Analytics**:

   How many elasticsearch instances per host? [2] 1
   What's the replication factor for elasticsearch? 0 means no replication. [0] 0
   How much memory in GB for each elasticsearch for each instance? [16] 16

   b. **For Data Lake**:

   [NOTE]
   If you are choosing an instance type where the memory is greater than 120 GB, we require 4 warm nodes. Otherwise, you will receive a warning message during the deployment process.
How many elasticsearch instances per host? [4] 4
How much memory in GB for each elasticsearch hot node? [16] 16
How much memory in GB for each elasticsearch warm node? [22] 22

The following values are recommended for AWS and GCP deployments.

How many elasticsearch instances per host? [4] 4
How much memory in GB for each elasticsearch hot node? [16] 16
How much memory in GB for each elasticsearch warm node? [22] 11

10. NTP is important for keeping the clocks in sync. If you have a local NTP server please input that information. If you do not have a local NTP server, but have internet access, use the default pool.ntp.org. Only choose none if there is no local NTP server and no internet access.

What's the NTP server to synchronize time with? Type 'none' if you don't have an NTP server and don't want to sync time with the default NTP server group from ntp.org. [pool.ntp.org] pool.ntp.org

11. The installation will automatically detect and assign a default route for your cluster.

Let us determine the right network interface name for the deployment. Discovered network interface name: eno1. This will be used as the default nic in the cluster.

12. If you would like to add internal DNS servers, select y and add them here. If not, select n. Name resolution here impacts only Docker containers.

Would you like to add any DNS servers? [y/n] n

13. If there are any conflicting networks in the user's domain, override the Docker BIP and Calico subnets. Answer y if you want to override (example is given below) and n if you do not.

NOTE
The docker_bip must have an IP actually in the subnet (i.e., the value cannot end in .0).

Would you like to override the docker_bip IP/CIDR (172.17.0.1/16)? [y/n] y
Enter the new docker_bip IP/CIDR (minimum size /25, recommended size /16): [docker_bip_ip/CIDR]
Would you like to override the calico_network_subnet IP/CIDR (10.50.48.0/20)? [y/n] n

CAUTION
IP addresses are given in the form [ip]/[CIDR]. Please apply the correct subnet CIDR block. Otherwise, network routing may fail or produce an unforeseen impact.
14. **For Data Lake** installations with clusters of 21 or more nodes, the installation will automatically designate the first three nodes as host management nodes (including master). The remainder of the nodes are marked as worker nodes that process data. For example, in a cluster of 24 nodes, nodes 1, 2, and 3, will be designated as host management nodes (including master). The remainder 21 nodes will be worker nodes that will process data.

If you do not have enough nodes to deploy the host management feature, the following message will appear:

```
Not enough nodes to deploy management nodes.
```

15. If the RPM (YUM) packages delivered with your installation have aged 3 months, you will be prompted to update your packages. You can also choose the option to **Install pre-approved CentOS package updates** from the main menu. **ONLY UPDATE USING RPM (YUM) packages provided by Exabeam inside your SXB package.**

```
NOTE
You have the option to perform a rolling update or update all hosts at once. Choosing to perform a rolling update prevents log ingestion downtime. This option still requires the use of TCP and a load balancer in front of any Syslog source. Only update all hosts at once if you are doing a fresh install.
```

While this update process will exit the original fresh_install script, once you have run the YUM updates and your hosts have been rebooted, you can return to and complete the deployment process by logging into your master host and apply:

```
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

Then select the "Deploy Cluster" menu option.

Your product is now deployed.

- If you wish to disable the **Exabeam Cloud Telemetry Service**, please refer to **Disabling Telemetry During a Product Installation**.

- If you purchased the Cloud Connectors cloud connector service, please refer to the “**Install SkyFormation app on an Exabeam Appliance**” guide at [support.skyformation.com](http://support.skyformation.com) to install the service.

Once you have deployed your purchased products, go to your host UI to configure features and services:

```
https://[master host IP]:8484
```

Log in using the credentials for the **admin user**, using the default password **changeme**, to make configurations. Please change the default password as soon as possible.

```
NOTE
Data Lake uses Elastalert Service to perform correlation rules. It is installed on the second host of the cluster.
```

Data Lake Administration Guide - Version SMP 2020.3 (DL I35)

Published Dec 11, 2020
2.4. Upgrade an Exabeam Product

Hardware and Virtual Deployments Only

If you are upgrading from Data Lake i24 or Advanced Analytics i46, you must meet the following requirements before installing or upgrading to this release:

- AWS deployments: All nodes MUST have src/dest (source/destination) checks turned off.
- GCP deployments: Network open to IP protocol 4 (IP in IP) traffic within the cluster.
- Nodes allow traffic to and from security group to itself.
- For Data Lake, use a load balancer in front of your cluster and use TCP (not UDP) as a transmission protocol between the load balancer and the Data Lake hosts. A load balancer is required (customer-provided) in front of Data Lake in order to have no downtime for Syslog ingestion during the upgrade.

If you have questions about the prerequisites, please create a support ticket at Exabeam Community to connect with a technical representative who can assist you.

**NOTE**
The current disaster recovery setup requires that both the primary and secondary clusters are on the same release version at all times. For more information, see Disaster Recovery.

**WARNING**
If you have an existing custom UI port, please set the `web_common_external_port` variable. Otherwise, access at the custom UI port may be lost after upgrading. Ensure the variable is set in `/opt/exabeam_installer/group_vars/all.yml`:

```
web_common_external_port: <UI_port_number>
```

1. If you wish to disable the Exabeam Cloud Telemetry Service before upgrading your product, please refer to *Disabling Telemetry Product During Upgrade or Patch Installation*.

2. If you are using the SkyFormation cloud connector service, please stop the service before you start the upgrade of your Exabeam product by applying one of these commands:
   a. For SkyFormation v.2.1.18 and higher, please run the command below:
      ```
sudo systemctl stop sk4compose
      ```
   b. For SkyFormation v.2.1.17 and lower, please run the command below:
      ```
sudo systemctl stop sk4tomcat
sudo systemctl stop sk4postgres
      ```

**NOTE**
The SkyFormation service automatically starts after you complete the upgrade steps of the Exabeam product. To upgrade to the latest version of SkyFormation, please refer to the *Update SkyFormation app on an Exabeam Appliance* guide at support.skyformation.com.
3. Download `Exabeam_[product]_[build_version].sxb` version file from Exabeam Community that you want to upgrade to. Place it on the master node in a temporary directory. Do not place the SXB file in the `/opt/exabeam_installer` directory.

4. Run the command below to start a new screen session:

   ```bash
   screen -LS [yourname]_[todaysdate]
   ```

5. Change the permission of the SXB file.

   ```bash
   chmod +x Exabeam_[product]_[build_version].sxb
   ```

6. Start a new terminal session using your `exabeam` credentials (do not run as ROOT).

7. Initiate a screen session. This is mandatory and will prevent accidental termination of your session.

   ```bash
   screen -LS [yourname]_[todaysdate]
   ```

8. Execute the following command:

   ```bash
   ./Exabeam_[product]_[build_version].sxb upgrade
   ```

   The system will auto-detect your existing version. If it cannot, then you will be asked to enter the existing version that you are upgrading from.

   **NOTE**

   If you are upgrading from Data Lake i22 or Advanced Analytics i41 or earlier, then you must apply your updated license after completing your upgrade. You do not need an updated license for any later release version. For more information on actuating your license, see [Applying a License](#).

---

2.4.1. UPGRADING FOR DATA LAKE LARGE CLUSTERS

For clusters with 21 or more nodes, the first three nodes of the cluster will be designated as host management nodes for Data Lake Host Management. It is mandatory to have three dedicated node for this feature. These host management nodes help ensure that the cluster maintains optimal processing and performance capabilities. They will not store log data.

The Data Lake Host Management feature is not applied automatically after running an upgrade. Please follow these steps to migrate nodes after you have completed your upgrade, if you have not established host management nodes.

1. Start a new terminal session using your `exabeam` credentials (do not run as ROOT).

2. Initiate a screen session. This is mandatory and will prevent accidental termination of your session.

   ```bash
   screen -LS [yourname]_[todaysdate]
   ```

3. Execute the following command:

   ```bash
   /opt/exabeam_mulitnode/init/exabeam-multinode-deployment.sh
   ```
4. Select the option, **Run migration service to move ES data off host1,2,3 (dl_management)**.

5. You will be prompted to confirm whether you are willing to add 3 nodes. Here, you can add new nodes to your cluster if you do not have hosts set aside from host management.

   Are you willing to add another 3 or more hosts for management nodes?

   a. If you answer yes, the script will exit to allow you the opportunity to add three additional nodes to your cluster. (See Adding Nodes to a Cluster.)

   When you have added your nodes, re-run `exabeam-multinode-deployment.sh` and then select **Run migration service to move ES data off host1,2,3 (dl_management)** which will migrate logs from the first three nodes of your cluster to other nodes. There is no loss of logs. The cluster's retention setting is adjusted automatically to compensate for the newly designated nodes.

   b. If you answer no, you will be prompted within:

      Do you accept a reduction in EPS and/or a reduction in storage capacity [percent]% resulting in a lower retention policy?

      i. Answer yes, if you have hosts set aside to operate as host management nodes. The migration will proceed for the first three nodes in your cluster. Logs from the first three nodes of your cluster to other nodes. The cluster's retention setting is adjusted automatically to compensate for the newly designated nodes.

      ii. Answer no, if you do not want to proceed with implementing host management.

2.4.2. UPDATING DATA LAKE PARSERS AND EVENT CATEGORIES

Hardware and Virtual Deployments Only

Please see Parser Configuration Update for steps to incorporate new or revised parsers.

For questions or additional assistance with updating parsers and event categories, please contact Exabeam Customer Success by opening a case via Community.Exabeam.com.

2.4.3. DISK USAGE AUTOMATIC CLEAN UP FOR UPGRADES

Hardware and Virtual Deployments Only

Obsolete installation files and backups are automatically deleted by the Exabeam upgrade process at the end of a successful installation session. The installation script runs a search on files and directories with the labels below:

```
/opt/exabeam_installer*

/opt/exabeam/data/backup/*
```

All contents that are older than three installations previous will be automatically deleted, including folders suffixed with old timestamps, such as:

```
/opt/exabeam_installer.backup[old_timestamp]

/opt/exabeam_installer.future[old_timestamp]
```
2.5. Troubleshooting an Installation
Hardware and Virtual Deployments Only

2.5.1. ANSIBLE FAILURE
If the installer fails during an ansible script (when all of the timestamped tasks are cascading down the screen), the steps to restart the deployment after fixing are:

1. Navigate to the Menu:
   /opt/exabeam_installer/init/exabeam-multinode-deployment.sh

2. Select option: Deploy cluster.

2.5.2. ERROR: MULTIPLE INTERFACES DETECTED
Root Cause: multiple interfaces are defined on boot

Steps to re-mediate:

1. Examine the output of the following command. Look for the iface of the current box for reference (helps know what iface not to touch)
   ip a

2. Look at the defined interfaces:
   cat /etc/sysconfig/network-scripts/ifcfg*

3. Only one interface (excluding the loopback interface ifc-lo) should have 'ONBOOT=yes'. Change the extra interface files from ONBOOT=yes to ONBOOT=no
   Requires sudo access to edit these files.

4. Run
   sudo systemctl restart network

5. Confirm consul is running
   sudo systemctl status consul

6. Restart the deployment process
   /opt/exabeam_installer/init/exabeam-multinode-deployment.sh
3. Administrator Operations

3.1. Exabeam Licenses
All Exabeam products require a license in order to function. These licenses determine which Exabeam products and features you can use. You are not limited by the amount of external data you can ingest and process.

There are multiple types of Exabeam product licenses available, which you can add to your Exabeam instance. For example, separate licenses are required to operate Incident Responder and Case Manager with your Advanced Analytics platform. Exabeam bundles these licenses together and issues you one key to activate all purchased products. For more information on the different product licenses, please see Types of Exabeam Product Licenses.

3.1.1. LICENSE LIFECYCLE
When you first install Exabeam, the installed instance uses a 30 day grace period license. This license allows you to try out all of the features in Exabeam for 30 days.

Grace Period

Exabeam provides a 30-day grace period for expired licenses before products stop processing data. During the grace period, you will not experience any change in product functionality. There is no limit to the amount of data you can ingest and process.

When the license or grace period is 14 days away from expiring, you will receive a warning alert on the home page and an email.

You can request a new license by contacting your Exabeam account representative or by opening a support ticket.

Expiration Period

When your grace period has ended, you will start to experience limited product functionality.

For Data Lake, health alerts and health checks will continue to work. Exabeam Threat Intelligence Services (TIS) and Telemetry will stop working.

You will receive a critical alert on the home page and an email.

License Alerts

License alerts are sent via an alert on the home page and in email when the license or grace period is 14 days away from expiring and when the grace period expires.

NOTE
The email alert is sent to the address linked in the notifications setting page at Settings > Additional Settings > Notifications > Setup Notifications.
The home page alert is permanent until resolved. You must purchase a product license or renew your existing license to continue using Exabeam.

You can also check the status and details of your license any time by visiting **Settings > ADMIN OPERATIONS > Licenses or System Health > Health Alerts.**

### 3.1.2. TYPES OF EXABEAM PRODUCT LICENSES
Exabeam licenses specify which products you have access to and for how long. We bundle your product licenses together into one license file. Therefore, all products that fall under your Exabeam platform share the same expiration dates.

**Data Lake product licenses:**

- **Data Lake** – The Data Lake license provides you with unlimited collection, ingestion, and secure data storage without volume-based pricing. The data ingested by Data Lake can be used by Advanced Analytics for analysis and Incident Responder during incident investigations.

- **Exabeam Threat Intelligence Services (TIS)** – TIS provides real-time actionable intelligence into potential threats to your environment by uncovering indicators of compromise (IOC). It comes fully integrated with the purchase of a Data Lake license. TIS also allows access to telemetry.

After you have purchased or renewed your product licenses, proceed to **Download a License.**

### 3.1.3. LICENSE VERSIONS
Currently, Exabeam has three versions of our product licenses (V1, V2, and V3). License versions are not backward compatible. If you are upgrading from / Data Lake I22 or earlier you must apply the V3 license version. The table below summarizes how the different license versions are designed to work:

<table>
<thead>
<tr>
<th>Products Supported</th>
<th>V1</th>
<th>V2</th>
<th>V3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Analytics</strong></td>
<td>• Advanced Analytics</td>
<td>• Advanced Analytics</td>
<td>• Advanced Analytics</td>
</tr>
<tr>
<td><strong>Threat Hunter</strong></td>
<td>• Threat Hunter</td>
<td>• Threat Hunter</td>
<td>• Threat Hunter</td>
</tr>
<tr>
<td><strong>Entity Analytics</strong></td>
<td>• Entity Analytics</td>
<td></td>
<td>• Entity Analytics</td>
</tr>
<tr>
<td><strong>Incident Responder</strong></td>
<td></td>
<td></td>
<td>• Incident Responder</td>
</tr>
<tr>
<td><strong>Case Manager</strong></td>
<td></td>
<td></td>
<td>• Case Manager</td>
</tr>
<tr>
<td><strong>Data Lake</strong></td>
<td></td>
<td></td>
<td>• Data Lake</td>
</tr>
<tr>
<td><strong>Threat Intelligence Service</strong> (ExaCloud authentication)</td>
<td></td>
<td></td>
<td>• Threat Intelligence Service (ExaCloud authentication)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product Version</th>
<th>V1</th>
<th>V2</th>
<th>V3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Analytics</strong></td>
<td>Advanced Analytics I38 and below</td>
<td>Advanced Analytics I41</td>
<td>Advanced Analytics I46 and above</td>
</tr>
</tbody>
</table>

Data Lake Administration Guide - Version SMP 2020.3 (DL I35)
Published Dec 11, 2020
<table>
<thead>
<tr>
<th></th>
<th>V1</th>
<th>V2</th>
<th>V3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses unique customer ID</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Federal License Mode</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Available to customers through the Exabeam Community</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Licensed enforced in Advanced Analytics</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Licensed enforced in Data Lake</td>
<td>NA</td>
<td>NA</td>
<td>No</td>
</tr>
<tr>
<td>Applied through the UI</td>
<td>No, the license must be placed in a path in Tequila</td>
<td>No, the license must be placed in a path in Tequila</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 2. License Version Details

**NOTE**
Licenses for / Data Lake I24 and later must be installed via the GUI on the license management page.

### 3.1.4. DOWNLOAD AN ON-PREMISES OR CLOUD EXABEAM LICENSE
You can download your unique customer license file from the Exabeam Community.

To download your Exabeam license file:

1. Log into the Exabeam Community with your credentials.
2. Click on your username.
3. Click on **My Account**.
4. Click on the text file under the **License File** section to start the download

After you have downloaded your Exabeam license, proceed to **Apply a License**.

### 3.2. Exabeam Hardening
The Exabeam Security Management Platform (SMP) has enabled security features by default that provide stricter controls and data protection. Two examples of what Exabeam has built protection against include Cross-Site Request Forgery (CSRF) and Cross-Origin Resource Sharing (CORS). A default set of filters are defined and enabled in Exabeam configurations. This improves the default security of the environment for all Exabeam services.
For Exabeam SaaS deployments that use Exabeam Advanced Analytics as your Exabeam Cloud Connector identity provider (IdP), Exabeam will update Cloud Connector to v.2.5.86 or later.

No manual configuration is needed for deployments with the following versions or later, as these protections are enabled by default:

- Exabeam Advanced Analytics i53.6
- Exabeam Data Lake i34.6

### IMPORTANT
This security enhancement has been enabled by default:

- Data Lake i34.6 and i35
- Advanced Analytics i53.6 and i54.5

It is not enabled by default in:

- Data Lake i33 or earlier
- Advanced Analytics i52 or earlier

Please follow the hardening guidelines. At the earliest opportunity, please upgrade to a currently supported version of Advanced Analytics and Data Lake.

### 3.2.1. HOW TO ENABLE CROSS-SITE REQUEST FORGERY PROTECTION

Cross-Site Request Forgery (CSRF) attacks are web-based vulnerabilities where attackers trick users with trusted credentials to commit unintended malicious actions. CSRF attacks change the states of their targets rather than steal data. Examples include changing account emails and changing passwords.

CSRF protection is available for Exabeam Advanced Analytics and Data Lake and previously inactive. Older versions of Advanced Analytics and Data Lake may manually harden or upgrade to a hardened supported version (Advanced Analytics i53.6 or later and Data Lake i34.6 or later) to enable the security configuration by default.

For information about enabled versions, see Exabeam Hardening.

These protections may affect API calls to the Exabeam SMP; please review customs scripts and APIs used by your organization. Please follow instructions given in Step 1c to conform your scripts.

To enable CSRF protection, apply the following:

1. For all deployments, the `/opt/exabeam/config/common/web/custom/application.conf` file at each master host needs to be configured to enable CSRF protection at service startup.
   a. Edit the following parameters in the CONF file:
b. Restart web-common to enable CSRF protection.

```bash
. /opt/exabeam/bin/shell-environment.bash
web-common-restart
```

**NOTE**
Log ingestion will not be interrupted during the restart. web-common can take up to 1 minute to resume services.

c. API calls to Exabeam that utilize POST requests using types application/x-www-form-urlencoded, multipart/form-data and text/plain are affected by CSRF configurations. Ensure API clients have headers that has Csrf-Token set to value nocheck. Continue with the next step.

2. For Advanced Analytics using Case Manager or Incident Responder, edit /opt/exabeam/code/soar-python-action-engine/soar/integrations/exabeamaa/connector.py.

a. Find the entry `self._session = SoarSession(base_url=apiurl, timeout=timeout, verify=False)` and replace with:

```python
self._session = SoarSession(base_url=apiurl, timeout=timeout, verify=False, headers={'Csrf-Token': 'nocheck'})
```

b. Restart services.

```bash
sudo systemctl restart exabeam-soar-python-action-engine-web-server
sudo systemctl restart exabeam-soar-python-action-engine
```

3. If SAML is configured, the IdP’s domain needs to be explicitly added to the CORS origins and then apply the new configuration. Please follow steps given in How to Enable Cross-Origin Resource Sharing Protection.

### 3.2.2. HOW TO ENABLE CROSS-ORIGIN RESOURCE SHARING PROTECTION

Cross-Origin Resource Sharing (CORS) is a browser standard which allows for the resources or functionality of a web application to be accessed by other web pages originating from a different domain -- specifically, the origin. An origin is defined by the scheme (protocol), host (domain), and port of the URL used to access a resource. CORS is a policy that allows a server to indicate any origins other than its own from which a browser should permit loading of resources.

CORS protection is available for Exabeam Advanced Analytics and Data Lake and enabled by default in Data Lake i34.6 or Advanced Analytics i53.6 and later versions. Older versions of Advanced Analytics and Data Lake may manually harden or upgrade to a hardened supported version (Advanced Analytics i53.6 or later and Data Lake i34.6 or later) to enable the security configuration by default.
For information about enabled versions, see Exabeam Hardening.

To manually enable CORS protection when it is not enabled by default, apply the following:

1. For all deployments, the `/opt/exabeam/config/common/web/custom/application.conf` file at each master host needs to be configured to enable CORS protection at service startup. Edit `webcommon.service.origins` parameter the CONF file to match your Exabeam service domain:

   ```
   webcommon.service.origins = ["https://
   *.exabeam.<your_organization>.com:<listener_port>",
   <...additional_origins...>]
   ```

   Here’s an example with 2 service origins:

   ```
   webcommon.service.origins = ["https://*.exabeam.org-name.com", "https://
   *.exabeam.org-name.com:8484"]
   ```

2. Restart `web-common` to enable CORS protection.

   ```
   . /opt/exabeam/bin/shell-environment.bash
   web-common-restart
   ```

   **NOTE**
   Log ingestion will not be interrupted during the restart. `web-common` can take up to 1 minute to resume services.

3.2.2.1. How to Verify Origin and CORS Enforcement with cURL

   The verification method presented here uses cURL to test CORS protection once it has been implemented.

   You can verify that your environment is enforcing CORS policy with the following (using `www.example.com` as an origin):

   ```
   curl -H "Origin: http://www.example.com" --verbose <exabeam_ip_or_hostname>
   ```

   The response should be 403 Forbidden with the error message Invalid Origin - http://www.example.com.

   To verify that CORS is working as intended, modify the origin:

   ```
   curl -H "Origin: <exabeam_ip_or_hostname>" --verbose <exabeam_ip_or_hostname>
   ```

   The response should be 200 OK with the Exabeam home page's HTML.
3.3. Adding Nodes to a Cluster

Hardware and Virtual deployments only

The steps below walk through the process of adding nodes to an existing cluster or upgrading from a standalone to multi-node deployment. The prompts ask a series of questions regarding how you want your node cluster configured.

Before you begin, ensure you have:

- Your Exabeam credentials
- IP addresses of your Master and Worker nodes
- Credentials for inter-node communication (Exabeam can create these during fresh installation if they do not already exist).

⚠️ CAUTION

Before adding nodes to your cluster, please ensure the current storage capacity for these items are below the following thresholds:

- **For Data Lake:**
  - 85% on Elasticsearch hot node
  - 85% on Elasticsearch warm nodes
  - 70% on Kafka service

⚠️ NOTE

Exabeam does not support removing nodes from a cluster.

⚠️ WARNING

Do not increase the number of nodes in a cluster by more than 50% during any given batch of node additions. For example, if you want to have a cluster of 100 nodes grown from a cluster of 20 nodes, run the operation by starting with a batch of 10 nodes and then incrementally add nodes in batches no larger than 50% of the node count.

Review cluster performance before adding more nodes. Ensure that the cluster status is healthy, and nodes have completed rebalancing.

3.3.1. ADD NODES

1. Run the following:

```
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

2. Menu options will appear. Select **Add new nodes to the cluster**. The following example adds 2 nodes to an existing cluster:

```
How many nodes do you wish to add? 2
```
3. Enter the IP(s) of the new node(s). The following example assigns the IP to 2 nodes, where there is a Master Node (existing), and two new Worker Nodes (node 11 and node 12):

```
NOTE
Any given cluster cannot have more than one master node. Please enter lms_slave as the role.
```

What is the IP address of node 11 (localhost/127.0.0.1 not allowed)?
10.10.2.88

What are the roles of node 11? ['lms_master', 'lms_slave']:
lms_slave

What is the IP address of node 12 (localhost/127.0.0.1 not allowed)?
10.10.2.89

What are the roles of node 12? ['lms_master', 'lms_slave']:
lms_slave

This step repeats until all nodes have IP addresses assigned.

4. NTP is important for keeping the clocks in sync. If a local NTP server exists, please input that information. If no local NTP server exists, but the servers do have internet access, use the default pool.ntp.org. Only choose none if there is no local NTP server and no internet access.

What's the NTP server to synchronize time with? Type 'none' if you don't have an NTP server and don't want to sync time with the default NTP server group from ntp.org. [pool.ntp.org] pool.ntp.org

5. If the user has internal DNS servers, add them here. If not, select No.

Would you like to add any DNS servers? [y/n] n

6. Override the Docker and Calico default subnets if there are any conflicting networks in the user's domain. If not, answer no to both.

```
NOTE
If you change any of the docker networks, the product will automatically be uninstalled prior to being redeployed.
```

Would you like to override the default docker BIP (172.17.0.1/16)? [y/n] n
Enter the new docker_bip IP/CIDR (minimum size /25, recommended size /16):
172.18.0.1/16

Would you like to override the calico_network_subnet IP/CIDR (10.50.48.0/20)? [y/n] n

The cluster is now configured.

3.4. Replicating Logs Across Exabeam Data Lake Clusters
You can configure Data Lake so that your primary Data Lake cluster is replicated to a backup system.
Before proceeding, ensure you have two independent Data Lake clusters (the primary and a backup). These clusters must have the same number of nodes, running the same version of Data Lake, and enough storage capacity to hold the same amount of data based on retention settings.

为了安全起见，确保你有两个独立的Data Lake集群（主和备用）。这些集群必须有相同的节点数，运行相同的Data Lake版本，并有足够的存储容量来存储相同的数据，基于保留设置。

### NOTE
All steps below refer to the backup cluster.

1. Establish a CLI session with the backup cluster of your deployment.

2. Set the primary IP address (where 10.10.2.88 is the primary Data Lake IP) as the environment variable in the terminal.

   ```bash
   export PrimaryDataLakeMaster=10.10.2.88
   ```

3. Copy the Keystore and Truststore files from the primary system to the backup system.

   ```bash
   scp exabeam@${PrimaryDataLakeMaster}:/opt/exabeam/config/common/kafka/ssl/kafka-host1.keystore.jks ~/primary.kafka.keystore.jks
   scp exabeam@${PrimaryDataLakeMaster}:/opt/exabeam/config/common/kafka/ssl/kafka-host1.truststore.jks ~/primary.kafka.truststore.jks
   ```

4. Add the DR location:

   ```bash
   /opt/exabeam/bin/lms/add-dr-location.py --dl-master $PrimaryDataLakeMaster \
   --kafka-keystore-path ~/primary.kafka.keystore.jks \
   --kafka-keystore-password exabeam \
   --kafka-truststore-path ~/primary.kafka.truststore.jks \
   --kafka-truststore-password exabeam
   ```

### 3.5. Ingesting Logs into Exabeam Data Lake

Ingestion via syslog is automatically enabled by default. However, you must configure your syslog source host to send logs to the proper Data Lake destination IP/port.

#### IMPORTANT
If you are running a multi-node Data Lake cluster with any Syslog sources, Exabeam strongly recommends having a load balancer with two site collectors behind it to mitigate any potential data loss.

Additionally, you must use the cert `<alias>-exa-ca.pem` provided in the customer artifacts package, which is provided during onboarding, if using TLS.

If you are sending logs via syslog over TCP/UDP, then use ports 515/TCP and 514/TCP or UDP.
3.6. Exabeam Data Lake Retention Settings
This feature provides the ability to remove old data based on a customizable retention policy so that the storage on the cluster can be reclaimed for newer data. Events in indices that exceed the retention period are deleted automatically and when an index is empty, the index is deleted as well.

⚠️ WARNING
Once the data deleted, it is lost permanently. Please implement archiving to prevent data loss.

For example, an index was created for events ingested on 01/01/2020 and events in the system are retained for 90 days. With this retention policy, all events and the index are deleted on 03/31/2018 at midnight GMT.

⚠️ NOTE
The default setting is 90 days retention. The minimum retention period that you can configure is 30 days.

For auditing purposes, the system keeps a trail of deletions.

In order to set a retention policy, users must navigate to Settings > Index Management > Advanced Settings. There they can enter the number of days that logs are to be retained, as seen in the screenshot below.

3.6.1. EXABEAM DATA RETENTION AND ENFORCEMENT
A number of triggers have been implemented in Data Lake to enforce data retention policy in order to ensure log ingestion continuity.

- Data retention by time is the most common criteria for retaining logs. Retention based on a set period cannot be disabled.
  - The default retention period is 90 days. The minimum retention period is 30 days.
  - Data purging is strictly enforced once data aging has reached the expiration point.
  - Archiving can be configured for the data set to be purged. (Options are available to archive to AWS S3 or NAS.) If archiving is not configured, Data Lake will purge expired indices regardless.

- Data retention by space implements purging based on low and high watermarks, meaning, storage limits that trigger archiving and purging. To adjust watermarks for your clusters, navigate to Settings > Index Management > Advanced Settings. Watermarks cannot be disabled.
  - Low watermark – Data storage capacity is approaching undesirable or unsafe levels when the low watermark is exceeded. The oldest data (even if it is not 90 days old) is archived and then purged to return storage capacity to an acceptable level. The default low watermark is 75% of storage capacity.
• High watermark – Data storage capacity has approached a level considered unsafe for operation. This is indicative of under-provisioned worker nodes. Purging of old indexes is triggered in order to ensure ingestion continuity. The default high watermark is 80% of storage capacity.

• Data purge by day
  • Purge a whole day’s index will be archived and purged based on a date schedule. Please implement archiving first before committing a data purge.

3.7. Remote Archiving NAS and AWS S3 from Data Lake
Hardware and Virtual Deployments Only
Logs from Data Lake can be offloaded to a remote archive destination based on a data retention policy. This is especially helpful in certain scenarios, such as:

• Retaining data for audit, compliance, and incident investigations
• Intermediate storage location during system migration
• Storage cost benefits and optimization of hot/warm cluster

You can use an AWS S3 bucket (provided by customer) or NAS appliance (provided by customer) as destinations for sending snapshots of your daily indices for long-term archiving. Logs can be archived in JSON and/or default Elasticsearch snapshot formats.

In order to leverage remote archives, please note the following limitations:

• Only one destination can be active, either AWS S3 or NAS
• Only one snapshot or retrieval job can run at a time
• Data Lake automatically creates and archives one snapshot per retention policy

The external archive destination is owned, managed, and provided by the customer.

3.7.1. ARCHIVING PREREQUISITES
The following tasks must be run to deploy remote archiving in your environment:

• Ensure network access to the remote archive destination
• Obtain AWS S3 credential keys (if applicable)
• Set up a retention policy
• Set up an archive destination

3.7.2. ARCHIVE AND RESTORATION PERFORMANCE
Without network connectivity considerations, these are the approximate processing times for:

• Archive for 1 TB index = 8-10 hours
• Restoration for 1 TB index = 2 hours
3.7.3. SET RETENTION POLICIES FOR EXABEAM DATA LAKE LOGS
Hardware and Virtual Deployments Only
Data Lake data retention policy dictates when the data will be automatically moved to an archive destination.

Archiving will run when a retention policy is in place. It is mandatory to set a retention policy for archiving to be enabled.

The default retention policy is set to 90 days. If the retention policy is shortened while archiving is enabled, then the new retention policy is applied. For an example on shortening the policy from 90 to 60 days, the system begins archiving logs 50 days or older. This 10-day lead is to ensure that archiving is completed before data is deleted.

3.7.4. SET UP AN ARCHIVE DESTINATION FOR EXABEAM DATA LAKE LOGS
Hardware and Virtual Deployments Only
Data Lake logs can be archived to an AWS S3 bucket or a NAS mount point. However, only one destination is supported at a time. You cannot schedule multiple archive tasks to multiple destinations.

Moving snapshots off hosts will consume significant amounts of system resources. It is advised that on-premise deployments use local NAS mount points while deployments in AWS use S3.
NOTE
Data Lake archiving, with the exception of ensuring archive task completion, does not include archive monitoring and purging archive destination. You will not be notified when your archive destination has reached its critical disk capacity. Please review the monitoring options for your archive destination from your vendor.

3.7.4.1. Set Up AWS S3 Archive Destination
Before configuring an AWS S3 archive destination, ensure you have the following:

- Each Data Lake node must have read/write permissions on the AWS S3 bucket
- Each Data Lake node must be included in its security group for accepted network traffic
- AWS S3 bucket name and region
- AWS access key ID
- AWS secret access key
- Base path of the AWS S3 bucket

To configure and enable an AWS archive destination:

1. Navigate to **Settings > Data Management > Archive**.

2. Click **Add Archive**.

3. Select **S3**.

4. You need to use a pre-existing Amazon S3 bucket. If you do not have one, click **CANCEL** to close the window. Come back to this flow once you have created an Amazon S3 bucket.

5. Go to **Archive Destination Management** to edit and enable your archive destination.

### 3.7.4.2. Set Up NAS Archive Destination

Before configuring a NAS archive destination, ensure you have the following:

- Each Data Lake node must have read/write permissions on the NAS mountpoint
- Each Data Lake node must be included in its security group for accepted network traffic
- Hostname or IP of the NAS endpoint
- Mount path at the destination host
- Destination must be in NFSv4 filesystem format

To configure and enable an NAS archive destination:

1. Navigate to **Settings > Data Management > Archive**.

![Image of Settings > Data Management > Archive](image)

2. Click **Add Archive**.

3. Select **NAS**.

![Image of Select NAS](image)

4. Copy the prerequisite script displayed in the UI and then run it from the master node.

5. Click **NEXT** to proceed to the configuration menu.
6. Fill in the required fields.

7. Click **TEST CONNECTION**.

8. Once testing returns **Test was successful!**, click **SAVE** to apply the configuration.

### 3.7.5. ARCHIVE DESTINATION MANAGEMENT FOR EXABEAM DATA LAKE LOGS

**Hardware and Virtual Deployments Only**

Assuming your Data Lake archive source and destination has been configured, this section details archive destination management, including steps to enable, edit, or delete your archive destination.

#### 3.7.5.1. Enable Archiving

Once you have set up an archive destination, enable a destination for your archive and thereby activate the retention policy and archiving. Only destinations that are correctly configured will produce an actionable **Enable** toggle.

To enable archiving:

1. Navigate to **Settings > Data Management > Archive**.

2. If this is the initial setup, it is important to first click on “How to enable?” which will generate the following prompts.
3. You need to execute the commands via SSH to the master node host, if you meet any of the following conditions:
   a. Setting up the archive destination for the first time (for Archive purposes)
   b. Setting up the archive destination for the first time (for Restore purposes)
   c. AWS credentials were updated for this destination (for either Archive or Restore)

4. After the above command finishes on the command line, you need to click How to enable? and follow its instructions to activate the archive destination. (This step is only needed for Archive. Please DO NOT enable this for Restore.)

3.7.5.2. Edit Archive Destination

You may on occasion change the destination repository. Your archive NAS may be at maximum capacity and a new NAS is introduced, or your organization needs to use a different S3 bucket. If you do not have a destination already, use this menu to create one.

To edit an archive destination:

1. Navigate to Settings > Data Management > Archive.
2. Click the vertical ellipsis to expand the submenu and then click Edit.
3. In the **Edit Destination** menu, fill in the required fields and select **Archive Format** you want supported.

![Edit Destination](image1)

**NOTE**
Archive Format: Optionally, select the JSON checkbox to enable Data Lake logs archiving. JSON logs cannot be restored. They are solely for use outside of Data Lake.

4. Click **TEST CONNECTION**.

5. Once testing returns **Test was successful!**, click **SAVE** to apply the configuration.

6. Click **How to enable?** and follow its instructions to activate the archive destination.
3.7.5.3. Delete Archive Destination
As only one destination can be configured for archiving, you will need to delete any existing archive
destination in order to configure a new destination (e.g. a new S3 bucket).

1. Navigate to Settings > Data Management > Archive.

2. At ARCHIVE MANAGEMENT, click Delete.

3. Click DELETE to confirm the cluster deletion.

3.7.6. RESTORE DATA TO EXABEAM DATA LAKE
Hardware and Virtual Deployments Only
Snapshots should be restored on a separate dedicated cluster, as it is critical not to disrupt the
performance of the ingestion cluster. Restoration assumes the restore cluster has sufficient disk space to
restore the data.

⚠️ WARNING
Restoring snapshots to the ingestion cluster is not supported as there could be a significant impact on
cluster performance. Also, restored indices may be unexpectedly deleted due to retention policy
configuration on the ingestion cluster.

3.7.6.1. Prerequisites

- A separate Data Lake cluster has been set up for restoring archived data
- The cluster status is green
- The cluster is not ingesting any logs
- Using the UI, set up the archive destination (the destination from which the data can be restored) with
the right credentials. This is the destination from which the data can be restored
- You can only restore from an archive destination that was created by a different Data Lake cluster
using the automatic archive policy
- Configure the archive destination and follow the prompts to ensure that the data can be listed and
read from the archive destination
• Leave the toggle in the Archive destination setup, to **off** or **Disabled** state (as this is applicable only for Archive scenario)

### 3.7.6.2. Restore Snapshots

There is one snapshot per index per day. The snapshot name contains the date of the index.

To restore a snapshot:

1. Log into the Data Lake UI and then navigate to the **Settings > Archive**.
2. Click **ADD DESTINATION**.
3. Select **NAS** for the Destination Type and run the command shown via SSH on the master node of the restore cluster. Be sure to update `<nas_ip>` with the IP of the NAS server and `<nas_mount_path>` (last field in command) with the mount point on the NFS server. When the command completes on the restore cluster, it will restart Data Lake services.

![Destination Type](image1)

4. Back in the Data Lake UI select **NEXT**. At **CREATE NEW DESTINATION**, give the destination a name and then enter the NAS IP and NAS mount path (as in previous step).

![Create New Destination](image2)

5. Click **TEST CONNECTION** and then **SAVE** if the test was successful.

6. A message will display once the destination is added. Click **OK** to close the window.
7. At the Archive Management UI, do not enable the destination.

8. Via SSH to the master node host, run the following:

```bash
cd /opt/exabeam
&& source bin/shell-environment.bash && clear && /opt/exabeam/bin/lms/es_archive_keystore.py
```

9. List the available indices to restore.

```bash
# If you are not sure about the es_commands.py, use the '--help' switch for all available options for the archive command
python /opt/exabeam/bin/lms/es_commands.py archive --help
# To list available snapshots
python /opt/exabeam/bin/lms/es_commands.py archive -l
```

10. To restore an index, run the command below using the index name from the list of available indices.

```bash
python /opt/exabeam/bin/lms/es_commands.py archive -r <index_name>
```

### 3.8. Set Up LDAP Import

During this stage of the setup, Exabeam will connect to your LDAP servers and query them for user and computer information. We then store the attributes to our own database. Going forward Exabeam will poll your LDAP servers once every 24 hours and update the local copy to reflect the latest state changes.

1. Navigate to Settings > Import LDAP > LDAP Server.

2. At the Import LDAP UI, you can add servers.

   Or, float your pointer to the right of existing LDAP server to click **edit** (pencil icon) or **delete** (trash can icon) records.
4. User Management

4.1. Exabeam Data Lake Role-based Access Control

Customers are able to control the responsibilities and activities of their SOC team members with Role-based Access Control (RBAC). Local users, LDAP users or SAML authenticated users will be assigned roles within Exabeam.

Each user can be assigned one or more roles and the responsibilities of those roles are determined by the permissions their role allows. If users are assigned more than one role, that user receives the permissions of both roles.

In conjunction with RBAC, Data Lake also uses object-based access control which manages the viewing and editing of objects. For more information, see Exabeam Data Lake Object-based Access Control.

**NOTE**

If a user is assigned multiple roles with conflicting permissions, Exabeam enforces the role having more permission. For example, if a role with lighter permission and a role with full permission are both assigned to a user, then the user will have full permission.

To access the Roles page, navigate to **Settings > User Management > Roles.**
CAUTION
The Exabeam-created managed users in Web Common that appear as native users on the Users tabs of Settings > User Management. These accounts are service accounts that are necessary for Exabeam’s basic functionality and should not be altered or deleted. These particular accounts are Common Access Card (CAC) accounts. They login through encryption certificates only and resetting or changing their passwords is not possible.

Figure 3. Data Lake service accounts

Below is a table listing the CAC service accounts and their functions. These accounts cannot be disabled or deleted.

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>exabeam</td>
<td>Used for out of the box content.</td>
</tr>
<tr>
<td>lm-collector-api-user</td>
<td>This is account allows log/remote agent collectors to connect to Data Lake. Connecting to Data Lake is necessary for management and collector metrics, and the authentication is based on highly secure TLS authentication using secured certificates.</td>
</tr>
<tr>
<td>lms-server</td>
<td>Reserved user for core Data Lake service.</td>
</tr>
</tbody>
</table>

Table 3. CAC Service Accounts

4.1.1. OUT-OF-THE-BOX ACCESS ROLES
Exabeam provides pre-configured access roles that restrict a user's tasks, actions, and views. A user may have more than one role. When a task, action, or view has more than one role associated to a user, the role with the greater access is applied.

Administrator: This role is intended for administrative access to Exabeam. Users assigned to this role can perform administrative operations on Exabeam, such as configuring the appliance to fetch logs from the SIEM, connecting to Active Directory to pull in contextual information, and restarting the analytics engine. The default admin credential belongs to this role. This is a predefined role provided by Exabeam and cannot be deleted.

Default permissions include:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[default Data Lake permissions]</td>
<td>By default, all users of the Data Lake have the following permissions: Perform Search, View and Edit Saved Searches, View and Edit Saved Visualizations, View and Edit Saved Dashboards.</td>
</tr>
<tr>
<td>Manage context tables</td>
<td>Manage users, assets or other objects within Context Tables.</td>
</tr>
<tr>
<td>Permission</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Manage Users and Context Sources</td>
<td>Manage users and roles in the Exabeam Security Intelligence Platform, as well as the context sources used to enhanced the logs ingested (e.g. assets, peer groups, service accounts, executives).</td>
</tr>
<tr>
<td>Manage Correlation Rules</td>
<td>Create and Edit Correlation Rules.</td>
</tr>
<tr>
<td>Manage Collectors</td>
<td>Perform all collector-related operations, such as managing and configuring collectors, changing template assignments, as well as performing start/stop operations.</td>
</tr>
<tr>
<td>Manage Exabeam Reports</td>
<td>Update and reload the list of the Exabeam reports.</td>
</tr>
<tr>
<td>Manage Data Retention</td>
<td>Modify Data Retention configuration.</td>
</tr>
<tr>
<td>Manage Data Access</td>
<td>Create and Edit Data Access Rules.</td>
</tr>
<tr>
<td>Manage Indices</td>
<td>Reparse and reindex the logs of one or several indices.</td>
</tr>
<tr>
<td>Manage Saved Objects</td>
<td>Create, edit, share saved object (such as dashboards, visualizations, searches).</td>
</tr>
<tr>
<td>View Saved Objects</td>
<td>View-only saved object (such as dashboards, visualizations, searches).</td>
</tr>
</tbody>
</table>

**Auditor**: Users assigned to this role have only view privileges within the Exabeam UI. They can view all activities within the Exabeam UI, but cannot make any changes such as add comments or approve sessions. This is a predefined role provided by Exabeam.

Default permissions include:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Saved Objects</td>
<td>Create and edit saved searches, visualizations, dashboards, and reports.</td>
</tr>
<tr>
<td>View Saved Objects</td>
<td>View saved searches, visualizations, dashboards, and reports.</td>
</tr>
</tbody>
</table>

**Tier 1 Analyst**: Users assigned to this role are junior security analysts or incident desk responders who supports the day-to-day enterprise security operation and monitoring. This type of role will not be authorized to make any changes to Exabeam system except for making user, session and lockout comments. Users in this role cannot approve sessions or lockout activities. This is a predefined role provided by Exabeam.

Default permissions include:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[default Data Lake permissions]</td>
<td>By default, all users of the Data Lake have the following permissions: Perform Search, View and Edit Saved Searches, View and Edit Saved Visualizations, View and Edit Saved Dashboards.</td>
</tr>
</tbody>
</table>

### 4.1.2. CREATING CUSTOM ROLES

Roles assigned to Exabeam users determine the level of access to tasks and data. Exabeam provides standard out-of-the-box roles that cannot be edited. However, you create new roles using the same access features and adjust accordingly.

1. To create a new role, navigate to **Settings > User Management > Roles**, and then click **Create Role**.
User Management

or

Settings > User Management > Users > Add User, and then click Create a new role.

2. Fill in the fields and enable features in the DATA LAKE tab, as needed.

3. Click the CORE tab and enable the listed features, as needed.
4. Click **Save** to make the role available to add or associate with users.

### 4.1.3. EXABEAM DATA LAKE SECURED RESOURCES OVERVIEW

Secured resources allow you to control access to logs based on a search filter. For example, a secured resource can define logs from sensitive applications, sources, or geographies. Once configured, users are only able to view and utilize specific sets of data for their searches, visualizations, dashboards, scheduled reports, or correlation rules.

For example, restrict data access based on:

- **Log feeds from specific sources** (e.g., Application logs from a business sensitive app can only be accessed by the SOC team).
- **Host, source or sourcetype** (e.g., Access to logs of a specific database is restricted to a role).
- **Search keywords or fields** (e.g., Logs of the executive users can only be accessed by specific roles).

This section walks through adding and managing secured resources within the Data Lake UI.

#### 4.1.3.1. Configure Exabeam Data Lake Log Access with Secured Resources

Secured resources allow you to control access to logs based on a search filter. Use the **Secured Resources** page to add, manage, and make additional changes to your secured resources.

The top-right of the page provides helpful management actions, including:

- **Manage Access** – Open the **Manage Data Access Control** page to limit access to roles within your organization.
- **Add** – Add a new secured resource.
- **Search** – Search for a secured resource.
The secured resources table displays information regarding your secured resources, including:

- **Name** – Name of the secured resource.
- **Description** – Brief description of the secured resource.
- **Query** – Search query matching the log events for the secured resource.
- **Roles** – Role(s) allowed to view the secured resource.

Filter the table according to roles by clicking the lined-triangle next to the **Roles** column header.

Hover over a secured resource in the table to edit (name, description, and query) or delete it.

Additionally, you can delete resources by selecting them in the table and then clicking **Delete**.
4.1.3.2. Adding a Secured Resource in Exabeam Data Lake

Secured resources is a role-base search filter that applies restrictions to the data being searched. Before applying which roles have access, you must define the secured resource being filtered.

To add a secured resource:

1. Navigate to Settings > Secured Resources > Data. This link takes you to the Secured Resources page.
2. On the secured resources page, click Add.

**NOTE**

If this is your first secured resource, the Add button appears in the middle of the secured resources page. If this is not your first secured resource, the Add button appears at the top-right of the secured resources table.
3. Enter a name and description for the new secured resource, and then click **Next**.

4. Enter the search query that matches the log events you want to secure, and then press enter on your keyboard to run the query.

   **WARNING**
   Typing "*" prevents access to any logs by anyone unless they are granted permission.

5. Review the query results. Edit and re-run the query (step 4, above) until you receive the desired results.
6. Once your query is ready, click **Create**.

Your new secured resource(s) appear in the secured resource table in the Secured Resources page. Now, you can manage access to the secured resource(s) for users in your organization.

**4.1.3.3. Managing Exabeam Data Lake Data Access to Secured Resources**

Secured resources allow you to control access to logs based on a search filter. Access to secured resources is based on a user's role. To grant roles access secured resources, configure associations on the Secure Resources page:

1. **Navigate to Settings > User Management > Roles.**

2. **Select any role from the list of default and custom roles.**
3. Click the **Secured Resources** link. This link takes you to the **Secured Resources** page.

4. On the secured resources page, click **Manage Access**.

5. Select a role from the **Roles** panel, and then select secured resource(s) by clicking the appropriate checkbox(es).
6. Click **Save**.

**IMPORTANT**

To constrain access to the data for specific users, enable the **Limit access to these selections** toggle. When this toggle is turned on, any user assigned to that role is restricted to access the selected secured resources in this list. They cannot access resources which are not explicitly allowed.

4.1.4. EXABEAM DATA LAKE VIEW-ONLY ACCESS CONTROL

A role that has **View Saved Objects** permission does not automatically have the right to **Manage Saved Objects** (create, edit, and delete). The two permissions are independent of each other and a role must have both permissions in order to manage a saved object. A role with **View Saved Object** permission but without Manage Saved Objects permission will not be able to manage the object.
However, by default out-of-the-box roles provided by Exabeam have View and Manage Saved Objects permissions, and cannot be edited.

NOTE
Role-based permissions override Object-based permissions. For example, if Manage Saved Objects is off in all the roles associated with a user, then the user is limited to running searches (without the ability to save, create, etc.). If one role of a collection of roles associated with a user has Manage Saved Objects, then the user has permission to search, save, create, and view objects. (For more information on object-based permissions, see Exabeam Data Lake Object-based Access Control.) Users with view-only privileges will receive a banner message on the Search page:

For more information on configuring access for saved objects, see Data Lake User Guide > Access Restrictions for Saved Objects.

4.2. Exabeam Data Lake Object-based Access Control

4.2.1. OBAC VS RBAC
Object-based access control (OBAC) manages the viewing and editing of tangible output products such as searches, visualizations, dashboards, and reports. Workflow is shared amongst user groups (defined by roles). Exabeam Data Lake Role-based Access Control (RBAC) manages execution (task-based) permissions within the Exabeam platform. Both forms of access control can restrict access dependent on roles. OBAC can be implemented in conjunction with RBAC, where objects can be displayed but executing tasks on those objects are managed or limited based on role privileges. OBAC is independent from role management in that objects can allow all actions based on RBAC, but OBAC can limit certain operations to the given role. OBAC manages objects by granting and restricting view and/or edit abilities to roles. OBAC permissions are not inherited from parent objects nor are they shared with child objects.

4.2.2. MANAGING DATA MIGRATION OF EXISTING OBJECTS
Pre-existing objects (created before Data Lake 2019.1) will be converted to the OBAC scheme, with public view and edit permissions within registered users. To view saved objects, your must have View
**Saved Objects** permission selected in at least one of the roles assigned to you. Additionally, you must change access permissions per each object by setting configurations in **Manage Saved Objects**. Access permissions must be changed for each saved object individually.

**NOTE**

New objects are by default saved with **Private** settings (managed and viewed only by the object originator). Only the object originator can change Share settings to **Public** or **Role-based** access, where **None**, **View and Edit**, and **View-only** are managed.

### 4.3. Single Sign-on and Multi-factor Authentication Using SAML

Exabeam users may have a single sign on vendor in their environment, such as Okta, Ping, Duo, Google, or Microsoft Active Directory Federation Services. Exabeam integrates with them, allowing administrators and users to sign on to Exabeam using their existing credentials.

With SAML Authentication enabled, there is no need for users to enter credentials and/or remember/renew a password with Exabeam.

#### 4.3.1. CONFIGURING SINGLE SIGN-ON AND MULTI-FACTOR AUTHENTICATION

Exabeam users may have a single sign on vendor in their environment, such as Okta, Ping, Microsoft Active Directory Federated Services (ADFS), or Google. You may also implement a custom or generic identity provider (IdP). Exabeam integrates with them, allowing administrators and users to sign on to Exabeam using their existing credentials. With SAML authentication enabled, there is no need for users to enter credentials and/or remember/renew a password with Exabeam.

**WARNING**

If your instance of Exabeam is running in a private network, you must ensure `webscommon.service.externalAddress` is pointing to the correct external IP address and is the same as `<exabeam_master_host>`, which was specified in configuration for IdP. The property is pointing to `EXABEAM_IP` environment variable, which is assigned during Exabeam deployment.

When Exabeam is deployed on AWS, there should not be any issues. When Exabeam is deployed on Google Cloud Platform, you may need to set the property in `/optz/exabeam/config/common/web/default/application_default.conf`.

**IMPORTANT**

For Exabeam SaaS deployments, additional restrictions have been applied to enforce security cross origin resource sharing (CORS) practices. Please add the origin of your SSO provider by following the Exabeam Operational Hardening guidelines to ensure SSO works when CORS protection is enabled.

**Single sign-on:** If your organization uses Okta, Ping Identity, Microsoft Active Directory Federated Services (ADFS), or Google as an IdP, you can configure single sign-on directly within the UI. Once configured, your users are automatically authenticated into the UI and will not be asked to create and/or enter specific login credentials.
**Multi-factor authentication:** Similarly, Exabeam products automatically support your multi-factor authentication (MFA, including two-factor authentication and/or two-step verification) through Okta, Ping Identity, and Google.

**4.3.1.1. Configure SAML Identity Provider**
Configure your identity service provider to produce credentials. The following instructions are for identity providers supported by Exabeam.

**Google**

1. Log onto Google Admin, then go to **Home > SAML apps.**

![Google Admin interface](image)

2. Click the + icon to enable SSO for a SAML application.

3. Click **SETUP MY OWN CUSTOM APP.**

![SETUP MY OWN CUSTOM APP](image)

4. Click **Next.**

5. Set the **Application** name, and then click **Next.**
6. Set the following properties **ACS URL** and **Entity ID**.

**ACS URL**: `https://<exabeam_master_host>:8484/api/auth/saml2/google/handle-assertion`

**Entity ID**: `https://<exabeam_master_host>:8484/api/auth/saml2/google/login`

where the `<exabeam_master_host>` is either an external IP address or hostname of the UI accessible by Google.

7. Click **Attribute Mapping** to create a mapping. Fill in the fields. The values in the first column are keys and should correspond to those which will be provided in web-common SAML SP config later. In this example First Name of the user from IdP is used for grouping.

8. Click **Next** and then click **OK**.

9. Click the **vertical ellipse** icon and then click **ON for everyone**.
10. Open **Service Provider Details > Manage Certificates**. Then, select the **DOWNLOAD IDP METADATA** file. Put the file in an easily accessible location. Hold this file for later configuration. Go to **Configure Identity Providers in Exabeam** to set up SSO.

![Manage identity provider certificates](image)

**Microsoft ADFS**

The instructions that follow are based on Windows 2019 Server.

1. Ensure that the identity provider (IdP) initiated SSO is enabled in ADFS. Verify using the PowerShell cmdlets `Get-AdfsProperties` and `Set-AdfsProperties`.

   ```powershell
   Get-AdfsProperties | Select EnableIdpInitiatedSignonPage
   # EnableIdpInitiatedSignonPage
   # ----------------------------
   #                        False
   Set-AdfsProperties –EnableIdpInitiatedSignonPage $True
   ```

   **NOTE**
   For more information on enabling IdP SSO, see
   
   
   https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties

2. Configure Microsoft ADFS Relying Party Trust by going to the **Server Manager > Tools > ADFS > ADFS Management**.

3. Go to the **Relying Party Trusts** branch and click **Add Relying Party Trust**.

4. Select **Claims aware** and then click **Start**.
5. Select **Enter data about the relying party manually** and then click **Next**.

6. Enter a **Display name**. Exabeam SAML SSO, for example, and then click **Next**.

7. Click **Next** at the **Configure Certificate** menu.

8. Select **Enable support for the SAML 2.0 WebSSO protocol**.

9. At **Relying party SAML 2.0 SSO service URL**, enter the ACS link `https://<exabeam master host>:8484/api/auth/saml2/adfs/handle-assertion`, and then click **Next**.

10. At **Relying party trust identifier**, enter the Exabeam Entity ID, `https://<exabeam master host>:8484/api/auth/saml2/adfs/login`. Click **Add** to enter it into the list of trusted identifiers.
11. At the **Choose Access Control Policy** menu, choose an access control policy from the list that adheres to your organization’s policies. Then click **Next**.

12. Leave **Configure claims issuance policy for this application** selected. Click **Close**.

13. Verify that a new record was created in the **Rely Party Trusts** list.

14. Select the new record. Right-click and then select **Edit Claim Issuance Policy**.
15. Select **Add Rule** and choose the template **Send LDAP Attributes as Claims**.
16. In the Edit Rule menu, enter a **Claim rule name**. Select **Choose Active Directory** as the **Attribute store**, and add the following attribute mappings:
   - **E-Mail-Addresses > EmailAddress**
     Set to user email
   - **Display-Name > FirstName**
     First name of exabeam user
   - **Display-Name > Username**
Username with prefix added (For example, if username is Jackyl it becomes [saml]Jackyl, username of exabeam user.)

- **Surname > LastName**
  Last name of exabeam user

- **Display-Name > ExaGroup**
  Associated user group for retrieving role and permissions. The display name will be set as the value **ExaGroup** attribute inside IdP response and must exist among all group mappings on the Exabeam side.

17. Click **Finish** to save the configuration. Click **Okay** to close the menu.

18. Select the record again. Right-click and then select **Edit Claim Issuance Policy**.

19. Click **Add Rule** and then select the template **Transform an Incoming Claim**. Click **Next**.

20. Set a rule to transform **Username** to **Name ID** in an unspecified format. Click **View Rule Language** to see the resultant rule. Here is an example:

   ```plaintext
```


22. Go to **Configure Identity Providers in Exabeam** to set up SSO. In the setup, use the following Exabeam-to-IdP attribute mappings:
User Management

- **Email Address** > EmailAddress
- **Username** > Username
- **First Name** > FirstName
- **Last Name** > LastName
- **Group** > ExaGroup
  Exagroup is used here as an example of a group name.

**Okta**

1. Log into the Okta console for your organization. The instructions that follow are based on the Okta Classic UI.
2. Click **Admin**.
3. Click **Add Applications**.
4. Click **Create New App**.
5. Select **SAML 2.0**.
6. Enter the **App name** and then click **Next**.

7. Enter the following properties:
   - **Single sign on URL**: https://<exabeam_master_host>:8484/api/auth/saml2/okta/handle-assertion
   - Click **Next** to go to the confirmation menu.

9. Select **I'm an Okta customer adding an internal app** and the checkbox **This is an internal app that we have created**.

10. Press **Finish** to apply the configuration.

11. Click on the **Assignments** section of the Exabeam test application and select **Assign to People**.
12. Press **Assign**.

13. Leave the username as-is and press **Save and Go Back**.

14. Press **Done**.

15. Click on the **Sign On** section of the Exabeam test application and press **View Setup Instructions**.
16. In the new page that opens, you can find the SSO URL, certificate file, metadata file content. Hold this information for later configuration. Go to Configure Identity Providers in Exabeam to set up SSO.

Ping

1. Log into the Ping console for your organization.
2. Go to Applications and press Add Application.
3. Choose **New SAML Application**.

4. Enter **Application Name**, **Application Description** and choose **Other** category. Press **Continue to Next Step**.

5. Set mandatory properties:
   - **Assertion Consumer Service (ACS)**: https://<exabeam_master_host>:8484/api/auth/saml2/ping/handle-assertion
   - **Entity ID**: https://<exabeam_master_host>:8484/api/auth/saml2/ping/login
   where the `<exabeam_master_host>` is either an external IP address or hostname of the UI accessible by Ping.

6. Press **Continue to Next Step**.

7. Specify attribute mapping. Mark each property as **Required**. The **SAML_SUBJECT** attribute is required for Ping to function correctly.
8. For the attribute SAML_SUBJECT attribute press **Advanced**.

9. **Set Name ID Format to send to SP** to the value shown in the example below, then press **Save**.

10. **Pay attention to this.**

11. **On the Preview settings page, download the Certificate file and Metadata file.** Hold these files for later configuration.

12. The SSO URL is found in the Metadata file, with the tag **md:SingleSignOnService**, where **Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"**.

13. **Press Finish.** Make sure the created application is enabled.

14. **Go to Configure Identity Providers in Exabeam to set up SSO.**

**4.3.1.2. Configure Identity Providers in Exabeam**

Once you have collected authentication metadata or certificate files from your IdP, you will associate the IdP to your Exabeam product. These instructions assumes you have created an identity service provider record. (See **Configure SAML Identity Provider**).
1. Log into your Exabeam product
2. Navigate to Settings > Admin Operations > Configure SAML.

3. Select the IdP in the list and click the Edit icon to configure the record to open the Edit Identity Provider menu.

   a. Click the IdP Enable toggle to activate the service.

   b. Ensure the correct SAML Provider is shown.

   c. If you have a metadata file from your IdP, select Upload the XML file metadata file provided by your IdP and then click CHOOSE FILE to upload the file.

   d. If you have a certificate file and SSO URL, select Configure SSO manually and then click CHOOSE FILE to upload the certificate and enter the SSO URL.

   e. You can optionally specify the Authentication Method, if you are uploading SSO assets.

   f. Configure the Query Attributes mappings.

   g. Click SAVE to apply the configurations.
4. Go to Map SAML Groups to Exabeam User Roles to associate user roles to your IdP service.

4.3.1.3. **Enable SAML Credentialing**

To configure an identity provider in your Exabeam deployment:

1. Log in to your instance of the UI.
2. Navigate to **Settings**.
3. On the **Settings** page, go to **User Management > Configure SAML**.
4. Click **Add Identity Provider**.

This step assumes you have already configured the IdP service provider. If not, configure your IdP service before proceeding.

- Google
- Microsoft ADFS
- Okta
- Ping
- Custom or generic SSO IdP are to include: (Please refer to the IdP vendor for additional instructions.)
  - IdP vendor name (15 characters or less)
  - Idp logo (PNG file size of 1Mb or less and in 3:4 or 9:16 aspect ratio)
5. The IdP is enabled by default upon saving. It can be disabled by toggling the **IdP Disabled** button.

![IdP Disabled button](image)

**NOTE**
You can configure multiple identity providers for your organization, but you can enable only one at a time. For information on configuring your SAML Identity Provider, see [Configure SAML Identity Provider](#).

6. Select your **SAML Identity Provider**. All supported IdPs are listed in the drop-down.

![SAML Identity Provider drop-down](image)

7. Complete the SSO Configuration by choosing one of the two options below. If you have an XML metadata file from your IdP, choose the first option. If you do not, you will need to manually configure SSO.

   - **Upload the XML file metadata provided by your IdP** – Click the Choose File button to locate and upload the XML file from your computer. SAML metadata is used to share configuration information between the Identity Provider (IdP) and the Service Provider (SP).

   ![Upload XML file metadata](image)

   - **Configure SSO manually** – Click the Choose File button to locate and upload the IdP certificate from your computer, and then enter the **Single Sign-on URL** and select either **HTTP Post** or **HTTP Redirect**. Optionally, configure the **Single Log-Out URL** and **Redirect to URL after Log-Out**.

   ![Configure SSO manually](image)

8. Select the **Authentication Method** or leave the field blank to accept the default configuration.

9. **For Custom/Generic IdP**, configure the **Name of IdP** and **Upload IdP logo**.

![Custom/Generic IdP](image)
10. **For ADFS**, configure the encryption. Select the option(s) that applies to your environment.

- **Encryption Enabled** -- Users are able to fill data for signature request and decryption response.

- **Signature Enabled** -- Adds a signature to the SAML authorization requests. Encryption keys (private key and certificate) are required.

- **Internal Keys** -- User internal Exabeam encryption key-pair (located in the trust store). To download the internal certificate, click the **Download certificate** link.

- **Custom Keys** -- User the key-pair from your organization.

11. **Configure the Query Attributes** to map your identity provider attributes to Exabeam's attributes.
12. Click Save. Your identity provider now appears in the **Identity Providers** table.

You can also continue customizing the configuration by mapping your SAML groups to Exabeam user roles.

**4.3.1.4. Map SAML Groups to Exabeam User Roles**

Once you have configured a SAML identity provider, the Group Mappings options appears below the **Identity Providers** table.

To map your existing SAML groups to Exabeam user roles:

1. **Click Add Group.**

2. **Select your configured Identity Provider.**

3. **Enter a SAML Group Name.** The name must match the Group value that comes from the IdP response in the group attribute; meaning, `<Attribute name="Group" value="[saml_group_name]">`.

4. Use the checkboxes to select default and custom roles.
5. Click **Save**.

Your SAML user groups are now mapped to Exabeam user roles.

### 4.3.1.5. Enable/Disable SAML Authentication

You can dictate how SAML authentication is handled within Exabeam products. There are two ways to implement SAML as well as disabling it entirely.

1. Navigate to **Settings > User Management > Configure SAML**.

2. In the **SAML Status** box has setting your organization is to support. To change the status, click **EDIT**.

3. The **SAML Status** box shows the current condition of how your users are permitted to log in to the UI. Click **Edit** to configure how your users are permitted to log in, including:

   - **Disabled** – SAML was configured, but it is not currently enabled. Consequently, users from your organization can only log in with their Exabeam credentials, but they will not be automatically authorized based on the their SAML credentials.

   - **Allowed** – Users can log in with their SAML or Exabeam credentials. If they have Exabeam credentials, they will also be able to use them to log in.
• **Mandatory** – Users can log in with their SAML credentials, but they cannot log in with their Exabeam credentials.

Select **Allowed** or **Mandatory** to implement SAML credentialing, and then click **SAVE** to apply changes.

### 4.4. Common Access Card (CAC) Authentication and Limitations

Exabeam supports Common Access Card (CAC) authentication. CAC is the principal card used to enable physical spaces, and provides access to computer networks and systems. Analysts have CAC readers on their workstations that read their Personal Identity Verification (PIV) and authenticates them to use various network resources.

Exabeam allows CAC authentication in combination with other authentication mechanisms (Kerberos, Local authentication, etc.).

Please note the following restrictions:

• Configure CAC users that are authorized to access Exabeam from the Exabeam User Management page.

• During the user provisioning, the CAC analysts must be assigned roles. The roles associated with a CAC user will be used for authorization when they login.

**Figure 4. Add User menu**

#### 4.4.1. CONFIGURE A CAC USER

1. Generate Certificate and add to the cluster by running the shell script below. Fill in the fields pertinent to your organization.

```bash
#!/bin/bash
# Main variables
Country="[country]"
CommonName="[cac_username_hostname]"
State="[state]"
Locality="[locality]"
Organization="[organization]"
OrganizationalUnit="[organizational_unit]"
EmailAddress="[email_address]"

# C = Country Name (2 letter code)
# ST = State or Province Name (full name)
# L = Locality Name (eg, city)
```

Data Lake Administration Guide - Version SMP 2020.3 (DL I35)

Published Dec 11, 2020
# O = Organization Name (eg, company)
# OU = Organizational Unit Name (eg, section)
# CN = Common Name (eg, your name or your server's hostname)
# emailAddress = Email Address
SubjString="/C=$Country/CN=$CommonName/emailAddress=$EmailAddress/ST=$State/L=$Locality/O=$Organization/OU=$OrganizationalUnit"

# Run the following commands on Exabeam server to create Client Certificate
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -aes-128-cbc -out ca.key -pass pass:test
openssl req -new -x509 -days 365 -sha256 -key ca.key -out ca.pem -subj "$SubjString" -passin pass:test

# Create client cert that will be signed by CA
cCountry="[country]"
cCommonName="[cac_username]"
cState="[state]"
cLocality="[locality]"
cOrganization="[organization]"
cOrganizationalUnit="[organization_unit]"
cEmailAddress="[email]"

cSubjString="/C=$cCountry/CN=$cCommonName/emailAddress=$cEmailAddress/ST=$cState/L=$cLocality/O=$cOrganization/OU=$cOrganizationalUnit"
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out client.key
openssl req -new -key client.key -sha256 -out client.csr -subj "$cSubjString" -passin pass:test
openssl x509 -req -days 365 -in client.csr -CA ca.pem -CAkey ca.key -CAcreateserial -out client.pem -passin pass:test
openssl pkcs12 -export -in client.pem -inkey client.key -name "Sub-domain certificate for some name" -out client.p12 -passout pass:test

2. Upload the generated ca.pem file to the CAC user home directory at the master node.
3. Execute the following commands at the master node:
   ```
   source /opt/exabeam/bin/shell-environment.bash
docker cp ca.pem exabeam-web-common:/
docker exec exabeam-web-common keytool -import -trustcacerts -alias cacbundle -file ca.pem -keystore /opt/exabeam/web-common/config/custom/truststore.jks -storepass changeit -noprompt
   ```
4. To associate the credentials to a login, create a CAC user by navigating to Settings > User Management > Users > Add User and select CAC in User type.

### 4.4.2. CONFIGURATION OF CLIENT CERTIFICATES
Located in /opt/exabeam/config/common/web/custom/application.conf the sslClientAuth flag must be set to true. Example below.

```
tequila {
  service {
...
```
4.5. Adding a User to Exabeam Data Lake

Data Lake users must be added in a separate process from your organization’s LDAP service. User permissions to view and execute tasks are based on the role(s) a user is assigned. Actions and views where a user has more than one role designation will follow the permission with the greatest access privilege.

To add a new user in Data Lake:

1. Log in to your instance of the UI.
2. Click the settings icon at the top-right corner of any page, and then click Settings.
3. In the **User Management** section, click **Users**.

4. Click **+ Add User**.

5. Enter the user details.
6. Select applicable roles.

7. Click **SAVE**.

The new user now appears on the **User Management** page.

### 4.6. Exabeam User Password Policy

Exabeam users must adhere to security requirements for forming passwords. The Exabeam Security Management Platform (SMP) adheres to the following for user passwords:

- **Passwords must:**
  - Be between 8 to 32 characters
  - Contain at least one uppercase, lowercase, numeric, and special character
  - Contain no blank space
- **User must change password every 90 days**
- **New passwords cannot match last 5 passwords**
- **SHA256 hashing is applied to store passwords**
- **Only administrator user can rest passwords and unblock users who have been locked out due to too many consecutive failed logins**

The management policies that are adjustable:

- **Strong password policy can be changed by editing the webcommon block in** `/opt/exabeam/config/common/web/custom/application.conf`. 
• Default idle session timeout is 4 hours. Edit the `silhouette.authenticator.cookieIdleTimeout` value (in seconds) in `/opt/exabeam/config/common/web/custom/application.conf`.

`silhouette.authenticator.cookieIdleTimeout = 14400`

### 4.7. Audit Log Management in Data Lake

There are a host of reasons to audit user activity. Insider threat show up in the form of unusual queries to sensitive information or unauthorized configuration changes. Perhaps your organization is undergoing an internal audit. Data Lake’s audit mechanism centralizes important and useful data for generating reports or help fill gaps in an investigation.

#### 4.7.1. WHAT IS IN THE AUDIT DATA

Audit data in Data Lake contains event logs for user activity committed within the product. In the same manner as other event logs, audit event logs can be forwarded to Exabeam Advanced Analytics via Syslog Forwarding. Personally Identifiable Information (PII) is not stored.

The default retention time for audit data is 90 days.

The following table lists the fields for each event being stored.
<table>
<thead>
<tr>
<th>Element</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>app</td>
<td>&quot;Exabeam Data Lake&quot;</td>
</tr>
<tr>
<td>event_type</td>
<td>Type categories:</td>
</tr>
<tr>
<td></td>
<td>• dl-search-activity</td>
</tr>
<tr>
<td></td>
<td>• dl-filtered-search-activity</td>
</tr>
<tr>
<td></td>
<td>• dl-correlation-rules-activity</td>
</tr>
<tr>
<td></td>
<td>• dl-secured-resource-activity</td>
</tr>
<tr>
<td></td>
<td>• dl-reports-activity</td>
</tr>
<tr>
<td>event_subtype</td>
<td>&quot;Exabeam Audit Event&quot;</td>
</tr>
<tr>
<td>time</td>
<td>Time of event</td>
</tr>
<tr>
<td>src_ip</td>
<td>Currently authenticated user's IP address</td>
</tr>
<tr>
<td>user</td>
<td>Currently authenticated user's username</td>
</tr>
<tr>
<td>activity</td>
<td>Type categories:</td>
</tr>
<tr>
<td></td>
<td>• Search query</td>
</tr>
<tr>
<td></td>
<td>• Visualization query</td>
</tr>
<tr>
<td></td>
<td>• Correlation rule [ruleId] deletion</td>
</tr>
<tr>
<td></td>
<td>• Secured resource [Sid] was updated</td>
</tr>
<tr>
<td></td>
<td>• Secured resource [Sid] was deleted</td>
</tr>
<tr>
<td></td>
<td>• Import reports from file</td>
</tr>
<tr>
<td>host</td>
<td>Host IP address</td>
</tr>
<tr>
<td>additional_info</td>
<td>The activity containing the search, query, etc.</td>
</tr>
<tr>
<td>sent_to_syslog</td>
<td>Indicates whether the message has been sent to Syslog</td>
</tr>
</tbody>
</table>

**4.7.2. HOW TO ENABLE AUDIT LOGGING**

Audit logging is not enabled by default. Syslog notification must configured with it messages sent to the Data Lake host.

1. Navigate to **Settings > Notifications > Setup Notifications**.

2. Click 🔳 to expand the menu and then select **Syslog notifications**.
3. In the configuration menu, use the IP or FQDN of your Data Lake master host in the **IP/Hostname** field.

4. Select **DL Audit**.

![Configuration menu for DL Audit](image)

5. Click **ADD NOTIFICATION** to create the record.

Audit event logs will start writing to Data Lake immediately.

**4.7.3. HOW TO ACCESS AUDIT DATA**

You can view, create reports, export, etc. audit data like you would for any event log in Data Lake. Apply queries with the event subtype **Exabeam Audit Event** as a filter.

![Audit data access](image)

**4.8. User Engagement Analytics Policy**

Exabeam uses user engagement analytics to provide in-app walkthroughs and anonymously analyze user behavior, such as page views and clicks in the UI. This data informs user research and improves the overall user experience of the Exabeam Security Management Platform (SMP). Our user engagement analytics sends usage data from the web browser of the user to a cloud-based service called Pendo.

There are three types of data that our user engagement analytics receives from the web browser of the user. This data is sent to a cloud-based service called Pendo:

- **Metadata** – User and account information that is explicitly provided when a user logs in to the Exabeam SMP, such as:
  - User ID or user email
  - Account name
• IP address
• Browser name and version

• **Page Load Data** – Information on pages as users navigate to various parts of the Exabeam SMP, such as root paths of URLs and page titles.

• **UI Interactions Data** – Information on how users interact with the Exabeam SMP, such as:
  • Clicking the Search button
  • Clicking inside a text box
  • Tabbing into a text box

### 4.8.1. OPT OUT OF USER ENGAGEMENT ANALYTICS

**NOTE**
For customers with a Federal license, we disable user engagement analytics by default.

To prevent Exabeam SMP from sending your data to our user analytics:

1. Access the config file at

   ```bash
   /opt/exabeam/config/common/web/custom/application.conf
   ```

2. Add the following code snippet to the file:

   ```bash
   webcommon {
     app.tracker {
       appTrackerEnabled = false
       apiKey = ""
     }
   }
   ```

3. Run the following command to restart Web Common and apply the changes:

   ```bash
   . /opt/exabeam/bin/shell-environment.bash web-common-restart
   ```
5. Index Management

5.1. Index Patterns
Exabeam provides out-of-the-box search indices, labeled with the prefix exabeam-*. You can view their details in the Index Patterns menu. All ingested logs go into exabeam-* indices, as well as correlation rule alerts by default.

**NOTE**
Though you can adjust parameters, we strongly recommend that you do not edit Exabeam supplied indices.

New filtered data (for example, after importing updated parsers) and contexts introduced to an existing data set will not display in graphs and search results until the next refresh cycle of a maximum 5 minutes. If you wish to see results immediately post, use **Refresh** to initiate a refresh of all graphs and search results.

**5.2. Reindex Operations**
Existing data can be reindexed when a new or revised parser is introduced. This is a manual initiated process. Apply this process only if you need to have new parsed valued in your historical/older data.

**CAUTION**
The reindexing operation is an expensive operation and might compete for resources with ongoing ingestion. Additionally, reindexing time is directly proportional to the volume of data being reindexed. This means the larger the time window selected for reindexing, the more expensive the operation and the longer the time it takes.
1. Navigate to Settings > Index Management > Reindex.

2. Select the start and end dates in the Timeframe for which the data time block you want to reindex.

3. Narrow the batch to process by selecting the Index and the data set to reprocess with a Search Query.

4. Click Reindex to initiate reindexing.

5.3. Saved Objects in Exabeam Data Lake
Customized objects are objects you can build using examples and templates provided by Exabeam. "Saved objects" are customized objects stored in the objects library during the build process that can be passed between clusters. Customized objects do not automatically synchronize between clusters. Distributing objects between clusters is a manual process.

To see objects available for export as well as access the import tool, navigate to Settings > Index Management > Saved Objects.

The Edit Saved Objects menu provides helpful actions, including:

- **Export Everything** – Generates and downloads a JSON file to your computer.
• **Import** – Deliver saved objects (JSON files) to your cluster.

Click *Save dashboard Object* to make the new object available for export. Additionally, you can *Delete dashboard Object* or *View Dashboard*.

• **Edit** – Reconfigure object properties.

• **View** – See the output from a given object.

In this example, the object is a visualization. Selecting its view displays in the *Chart Builder*.
5.4. Exabeam Data Lake Parser Configuration Update

Parsers are log ingest filters that sift for known threat indicators. Any changes to the parser categories file (API/logs/categories) will be picked up at most within 15 minutes due to automated re-caching. To apply parser changes immediately, restart the parsing service using the command `dl-mojito-restart`.

If any parsers have been disabled and need to be re-enabled, you can re-enable them and restart the parsing service by using the following commands:

```
sos
dl-mojito-restart
```
6. Parser Management

Parsers are individually managed for performance and can be paused by Exabeam Data Lake. Automated Data Lake action is based on the performance thresholds from a holistic standpoint to maintain system operability.

6.1. How to Set Parser Policy

You can select the parsing policy that determines whether Exabeam Data Lake prioritizes parsing of all ingested raw logs, events per second throughput, or a balance of both.

For custom parsers, you can adjust the threshold for pausing parsers based on resource priority:

1. Navigate to **Settings > Parsers Management > Parsers Management**.

2. In the **Parser Policy** panel, the currently active parser policy is shown at the bottom of the text. Click **EDIT** to expand the configuration options. Select the performance preference that best suites your operation and less likely to trigger the parser to be paused. The categories are defined by the parser’s impact to performance.
The thresholds are:

**Optimized for parsing** -- The parser has consumed more than 80% of Data Lake performance.

**Balanced** -- The parser has consumed more than 50% of Data Lake performance.

**System Focused** -- The parser has consumed more than 30% of Data Lake performance.

3. Click **APPLY** to implement your preference. The parsing policy takes effect immediately. There is no need to restart services.

### 6.2. How to Re-enable Paused Parsers

Parsers may be paused by based on the performance threshold set by the **Parser Policy**. Parsers can be manually resumed but be aware they can be re-paused if poor performance persists.

To resume a paused parser:

1. Navigate to **Settings > Parsers Management > Parsers Management**.

2. Review the list of **Paused Parsers**. If you have resolved the cause of the slow parser, you may re-enable the paused parser by clicking **START** or the hyperlink (shown as **Start 3 Parsers** in this example) for a batch start.
**PARSERS MANAGEMENT**

**Parser Policy**

The parser policy determines whether the system prioritizes parsing of all ingested raw logs, events per second throughput, or a balance of both. Select the policy that matches your goals.

- Optimize for parsing
- Balanced
- System focused

**Learn more about parser policies**

**Start 3 Paused Parsers**

Data Lake automatically pauses overloaded parsers to maintain optimal system performance. Click **Start** to restart a paused parser. If Data Lake pauses the parser again, you can update the parser’s configuration to improve its efficiency, making it less likely to be overloaded and paused.

**Learn more about automatic parser pausing**

<table>
<thead>
<tr>
<th>Parser Name</th>
<th>Start</th>
<th>Start</th>
<th>Start</th>
</tr>
</thead>
<tbody>
<tr>
<td>bro-notice</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bro-mysql</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>bro-httpd0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7. Forwarding to Other Destinations

7.1. Syslog Forwarding Management in Exabeam Data Lake

**NOTE**
SaaS Cloud deployments only support TCP 515 with TLS.

SaaS Cloud deployments support Syslog forwarding but must be configured by an Exabeam technical representative. Please gather the relevant sources and destinations and then contact your Exabeam technical representative to enable Syslog forwarding.

Data Lake can be configured to send all, or a subset of, ingested logs to Advanced Analytics or other destinations via Syslog. This capability allows you to send your logs to an Advanced Analytics instance and/or third-party destination.

If you also have deployed an instance of Advanced Analytics, we strongly recommend using this functionality, as logs ingested by Data Lake can be consumed immediately by Advanced Analytics for threat detection.

Follow the instructions in Syslog Forwarding to Advanced Analytics to forward logs ingested from Data Lake to Advanced Analytics. Or, follow the instructions in Syslog Forwarding to External Destinations to forward all logs ingested from Data Lake to external destinations.

Then follow the instructions in Selective Forwarding via Conditions.

7.1.1. SYSLOG FORWARDING PAGE

The **Syslog Forwarding** page provides details and settings for Data Lake log forwarding. The **Destinations** section lets you add a new syslog destination (either internal or external destinations) and access a list of your configured syslog destinations.
Hover over any syslog destination to enable additional actions, such as:

- **Reconnect** – If the destination is disconnected, attempt to manually reconnect the destination.

  ![NOTE]
  
  **NOTE**
  
  If the configured destination is Exabeam Advanced Analytics, then forwarding automatically reconnects when Advanced Analytics service returns.

- **Disable** – Disable syslog forwarding to the destination.
- **Edit** – Edit the destination (name, hostname or IP, port, and protocol).
- **Delete** – Remove the destination and all associated conditions.

The **Conditions** section lets you add a new log filters (or "conditions") and access a list of your configured filters.

Hover over any condition to enable additional actions, such as:
7.1.2. HOW TO FORWARD SYSLOG TO EXABEAM ADVANCED ANALYTICS FROM EXABEAM DATA LAKE

This process will configure your Data Lake product to forward ingested logs to your Advanced Analytics product via syslog. A best practice is to forward only necessary logs to Advanced Analytics.

**Required:**

Before you begin, please ensure you have the following:

- Permissions to adjust log ingestion settings in Advanced Analytics
- Permissions to adjust log forwarding settings in Data Lake

1. **Enable Syslog Ingestion in Advanced Analytics.**
   
   a. Log in to the Advanced Analytics product, and then navigate to **Admin Settings > Log Management > Log Ingestion Settings.**

   ![Admin Settings](image)

   b. Toggle the **Enable Syslog Ingestion** setting to **ON.**

   ![Log Ingestion Settings](image)

   c. If you previously added Data Lake as a server, then delete it. Otherwise, skip to step 1d.
d. Click **Next**.

2. Configure Advanced Analytics as your syslog destination.
   a. Log in to the Data Lake product, and then navigate to **Settings > Log Forwarding > Log Destinations**.

   b. Click **Add** in the Destinations box.

   c. Enter a **Name**, **Hostname or IP**, and **Port**, and then select a **Protocol**.
d. Click **Add**.

![Add Destination](image)

e. Optionally, configure any forwarding Conditions.

![Add Condition](image)

3. Verify that the Advanced Analytics instance is receiving logs by running the following:

```
sudo tcpdump -i eno1 'port Syslog_port'
```

### 7.1.3. HOW TO FORWARD SYSLOG FROM EXABEAM DATA LAKE TO NON-EXABEAM EXTERNAL DESTINATIONS

This process will configure your Data Lake product to forward ingested logs to external non-Exabeam destinations via syslog.

**Required:**

- An external destination configured to ingest syslog data
- Permissions to adjust log forwarding settings in Data Lake

1. Log in to the Data Lake product, and then navigate to **Settings > Log Forwarding > Log Destinations.**
2. Click **Add** in the Destinations box.

3. Enter a **Name**, **Hostname or IP**, and **Port**, and then select a **Protocol**.

4. Click **ADD**.
5. Optionally, configure any forwarding Conditions.

Verify that the external destination is receiving logs.

7.1.4. EXABEAM DATA LAKE SELECTIVE FORWARDING USING CONDITIONS

Conditions let you filter and then forward the logs that are ingested into Data Lake to your Syslog destination via Syslog for threat detection.

Conditions are based on log types. When you create a filter, select the type of log that you wish to forward from a predefined menu.

To add a new condition:

1. Log in to the Data Lake product, and then navigate to Settings > Log Forwarding > Log Destinations.

2. 

3. Select an existing destination, or click ADD to create a new destination (either Advanced Analytics or external).
4. Click **Add Condition**.

5. Select the log type that you want to forward. The default filter condition is automatically entered into the **Filter Expression** box.

6. Optionally, edit the filter condition according to your business needs. See *Editing Condition Filters*.

7. Click **Add**.
8. The condition will appear in the condition list and is automatically enabled.

**Editing Condition Filters**

In condition filters, string matching is applied to raw log text. There is no distinction between field names and content.

Consider the following when creating condition filters:

- Regular expressions are not supported
- Text strings in condition filters need to be braced with double-quotes
- The or operator will be used when combining multiple conditions in the filter
- Destinations will additionally need an escape character '\\' for literal text filtering
- Parenthesis is not supported
- The and Boolean takes precedence over or in the logic order

Here are some examples:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;s1&quot;</td>
<td>event must contain s1</td>
</tr>
<tr>
<td>&quot;s1&quot; and &quot;s2&quot;</td>
<td>event must contain both s1 and s2</td>
</tr>
<tr>
<td>&quot;s1&quot; and &quot;s2&quot; or &quot;s3&quot;</td>
<td>event must contain both s1 and s2, or contains s3</td>
</tr>
<tr>
<td>&quot;s1&quot; or &quot;s2&quot; and &quot;s3&quot;</td>
<td>event must contain s1 or both s2 and s3</td>
</tr>
<tr>
<td>&quot;s1&quot; and &quot;\s2&quot;</td>
<td>event must contain both s1 and &quot;s2&quot;</td>
</tr>
</tbody>
</table>

7.1.5. HOW TO CONFIGURE EXABEAM DATA LAKE LOG DESTINATIONS FOR CORRELATION RULE OUTCOMES

In addition to syslog forwarding to multiple recipients, you can filter the content further using correlation rules.

To incorporate correlation rules with log forwarding:

1. Create a Destination Record.
   a. Navigate to **Settings > Log Forwarding > Log Destinations** and then click **Add**.
   
      ![SYSLOG FORWARDING](image)

      - **Add** button highlighted

   b. Fill in the destination fields and then select **Receive Correlation Rules Outcome**.
c. Click **ADD**. Your new record should appear in the **Syslog Forwarding** list of destinations.

2. Direct the outcome of a correlation rule to your destination. The following is an example of creating a new correlation rule.
   
   a. Navigate to **Settings > Correlation Rules > Correlation Rules**, and then click **CREATE**.

   ![Correlation Rules](image)

   b. Select the correlation rule type that will activate log forwarding to your destination.

   ![Select Rule Type](image)

   c. At the **Determine Rule Outcomes** step, enable **ADD RISK TO ENTITIES**. Click **User** and/or **Assets** as the entity timeline to append data to, if your destination is an **Advanced Analytics** platform.
d. Click **NEXT** to the **Save Rule** step to complete the correlation rule creation.

### 7.2. How to Forward Exabeam Data Lake Incident to Exabeam Incident Responder

**Hardware and Virtual Deployments Only**

If you have Exabeam Incident Responder in your environment, you can produce incidents directly into it using triggers generated by correlation rules.

⚠️ **WARNING**

It is required that your Incident Responder host has parsers to receive payloads from Data Lake. Otherwise, Data Lake forwarded items will not produce incidents.

ℹ️ **NOTE**

Ensure routing and access is enabled to and from port 9875 for data transport at the Data Lake and Incident Responder hosts.

To Setup Incident Forwarding, you must establish an Incident Responder destination:

1. Navigate to **Settings > Index Management > Advanced Settings**.
2. Click the Edit icon to change the status of `incidentResponderAlerts`. A status of “false” indicates that incident forwarding is disabled.

3. Click the Enable checkbox and then the Save icon to enable forwarding to Exabeam Incident Responder.

4. Edit the `ir.outcome` setting in `/opt/exabeam/config/lms/server/default/application.conf` at the Data Lake master host with the Incident Responder host and port information.

   ```
   ir.outcome {
     enabled = true
     syslogservers = [
       {
         host = "<hostname>"
         port = 9875
       }
     ]
   }
   ```

5. Restart Data Lake to apply incident forwarding changes.

   ```
   lms-server-stop; sleep 5; lms-server-start
   ```

6. In the Data Lake UI, create a rule to utilize the incident forwarding:
   a. Navigate to Settings > Correlation Rules.
   b. Click Create to build a new rule or select an existing rule to edit.
   c. During rule creation in the Rule Outcomes menu, click CREATE AN INCIDENT and fill in the incident descriptors based on your organization’s security policies.
d. Proceed with the remainder of rule creation process.
8. Cluster Operations

8.1. Configuring Exabeam Data Services Data Retention in Exabeam Data Lake
Hardware and Virtual Deployments Only

NOTE
To configure this feature, please contact your Exabeam technical representative.

By default, the retention policy for Exabeam Data Services (EDS) data is 30 days. Therefore, LDIF (LDAP Data Interchange Format) files collected daily from the LDAP (Lightweight Directory Access Protocol) server(s) are retained for 30 days.

In general, the 30-day default period is suitable for the average customer and does not affect product behavior performance. However, some customers may need to reprocess older events, which may include events related to users or assets that are no longer active, and won't be found in the current context tables. In this specific case, the events will be reprocessed but might not be able to leverage the historical contextual information.

To configure the EDS data retention period:

1. Access the EDS custom application.conf file:
   `/opt/exabeam/config/common/eds/custom/application.conf`
2. Add the value here, where N is the total number of retention days:
   
   ```
   EDS.Defaults.RetentionPeriod = N days
   ```
3. Stop, and then start EDS again:
   ```
   eds-stop
   eds-start
   ```

8.2. Re-Assign to a New IP (Appliance Only)
Hardware Deployments Only

NOTE
These instructions apply to Exabeam appliances only. For instructions on re-assigning IPs in virtual deployments, please contact Exabeam Customer Success by opening a case at Exabeam Community.

1. Set up a named session to connect to the host. This will allow the process to continue in the event you lose connection to the host.
   ```
   screen -LS [session_name]
   ```
2. Enter the cluster configuration menu.
source /opt/exabeam_installer/init/exabeam-multinode-deployment.sh

3. From the list of options, choose Change network settings.
5. Choose Change IP(s) of the cluster - Part I (Before changing IP).
6. You will go through a clean up of any previous Exabeam installations.

    Do you want to continue with uninstalling the product? [y/n] y

7. Acknowledge the Exabeam requisites.

    ***********************************************
    Part I completed. Nuke successful. Product has been uninstalled.
    ***Important***
    Before running Part II, please perform these next steps below (Not optional!):
    - Step 1 (Manual): Update the IPs (using nmtui or tool of choice)
    - Step 2 (Manual): Restart network (e.g., systemctl restart network)
    ***********************************************

    Please enter 'y' if you have read and understood the next steps: [y/n] y

8. Open the nmtui to change IP addresses of each host in the cluster where the IP address will be changed.

    sudo nmtui

9. Go to Edit Connection and then select the network interface.

10. The example below shows the menu for the network hardware device eno1. Go to ETHERNET > IPv4 CONFIGURATION.
**WARNING**

Please apply the correct subnet CIDR block when entering [ip]/[subnet]. Otherwise, network routing will fail or produce unforeseen circumstances.

11. Set the configuration to **MANUAL**, and then modify the IP address in **Addresses**.
12. Click **OK** to save changes and exit the menu.
13. Restart the network services.

```bash
sudo systemctl restart network
```

14. Enter the cluster configuration menu again.

```bash
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

15. Choose **Change network settings**.
16. Choose **Change IP of cluster hosts**.
17. Choose **Change IP(s) of the cluster - Part II (Before changing IP)**
18. Acknowledge the Exabeam requisites.

```
**********************************************************************
Please make sure you have completed all the items listed below:
- Complete Part I successfully (nuke/uninstall product)
- (Manual) Update the IPs (using nmtui or tool of choice)
- (Manual) Restart network (e.g., systemctl restart network)
**********************************************************************
Do you want to continue with Part II? [y/n] **y**
```

19. Provide the new IP of the host.

```
What is the new IP address of [hostname]? (Previous address was 10.70.0.14) [new_host_ip]
```

20. Update your DNS and NTP server information, if they have changed. Otherwise, answer **n**.

```
Do you want to update your DNS server(s)? [y/n] **n**
Do you want to update your NTP server? [y/n] **n**
```

**8.3. Display a Custom Login Message**

You can create and display a custom login message for your users. The message is displayed to all users before they can proceed to login.

To display a custom login message:

1. On a web browser, log in to your Exabeam web console using an account with administrator privileges.
2. Navigate to **Settings > Admin Operations > Additional Settings.**

3. Under **Admin Operations**, click **Login Message.**

4. Navigate to **Settings > Admin Operations > Login Message.**

5. Click **EDIT.**
6. Enter a login message in **Message Content**.

**NOTE**
The message content has no character limit and must follow UTF-8 format. It supports empty lines between text. However, it does not support special print types, links, or images.

A common type of message is a warning message. The following example is a sample message:

**Usage Warning**

This computer system is for authorized use only. Users have no explicit or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to an authorized site. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of the authorized site.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

**NOTE**
This sample warning message is intended to be used only as an example. Do not use this message in your deployment.

7. Click **SAVE**.
8. Click the **Display Login Message** toggle to enable the message.

![Login Message Toggle]

**NOTE**
You can hide your message at any time without deleting it by disabling the message content.

Your custom login message is now shared with all users before they proceed to the login screen.

---

**8.4. Exabeam Cluster Authentication Token**

Hardware and Virtual Deployments Only

The cluster authentication token is used to verify identities between clusters that have been deployed in phases as well as HTTP-based log collectors. Each peer cluster in a query pool must have its own token. You can set expiration dates during token creation or manually revoke tokens at any time.
To generate a token:


2. At the Cluster Authentication Token menu:
   a. To configure a new token, click.
   b. Or to edit an existing configuration, click.

3. In the Setup Token menu, fill in the Token Name, Expiry Date, and select the Permission Level(s).
NOTE
Token names may contain letters, numbers, and spaces only.

4. Click **ADD TOKEN** or **SAVE** to apply the configuration.

Use this generated file to allow your API(s) to authenticated by token. Ensure that your API uses ExaAuthToken in its requests. For curl clients, the request structure resembles:

```bash
curl -H "ExaAuthToken:<generated_token>" https://<external_host>:<api_port>/
<api_request_path>
```
9. Cross-cluster Search in Exabeam Data Lake

Cross-cluster searches enable queries across one or more trusted and connected clusters at a time. Any cluster can be used to issue a search across multiple clusters accessible to it. The querying cluster can execute search requests across a list of selected clusters for each search query. These searches allow you to comprehensively examine data across all clusters.

Cross-cluster search is well suited to customers who have multiple Data Lake clusters, especially those with:

- Geographically distributed data centers
- Regional clusters (such as satellite offices) with their own clusters alongside a central cluster
- A need to manage smaller clusters instead of a single large cluster

**WARNING**

Cross cluster search results export is limited to 10,000 events per search query. For local clusters, up to 1,000,000 events per search query can be exported in CSV format.

9.1. Prerequisites for Exabeam Data Lake Cross-cluster Search

Cross-cluster searches can run only between configured trusted clusters within a routable network. For cross-cluster searches to work, the following requirements must be met:

- Peer clusters must have secure routing. The CA (Certificate Authority) certificate must be shared amongst querying and remote clusters to enable encrypted communication across clusters.
- There must be sufficient bandwidth between clusters to support network traffic from results aggregation.
- The path between peer clusters must be routable, with necessary firewall traversal. (Firewall ports should have network subnet or whitelist restrictions to protect access to the clusters.)
- Opening of port 9300 on participating clusters to be accessible for searches. For more information about port configurations, see Network Ports.
- Necessary permissions are set up for users and roles on each participating cluster.

9.2. Remote Cluster Management for Exabeam Data Lake Cross-cluster Search

Data Lake allows the Administrator to add clusters to perform cross-cluster searches. The cluster list must have:

- Only registered clusters can be queried.
- All member clusters must have CA credentials.

Each participating cluster must be set up to allow searches to be issued from it. You need to provide the remote cluster IP address and cross-cluster permissions for cross-cluster connections to work correctly.
9.3. Register a Remote Cluster in Exabeam Data Lake for Cross-cluster Search

Hardware and Virtual Deployments Only

For remote clusters to be queried using cross-cluster search, each remote cluster must:

- Have a CA certificate file.
- Be registered individually in that cluster's registry.

To download a certificate on a remote cluster:

1. Navigate to **Settings > Cluster Management**.
2. Select **Download certificate**. A download will automatically initiate. See your downloads directory for the certificate file.

To register a remote cluster:

1. Navigate to **Settings > Cluster Management > Clusters**.
2. Click **ADD CLUSTERS**.

3. Fill in the cluster **Name** and **Hostname or IP** of the master node, then click **UPLOAD THE CERTIFICATE** to attach the CA certificate to the cluster.

**NOTE**

Up to 2 hostnames and IP addresses are supported. Two hostnames or IPs are recommended for mid-sized clusters of less than 10 nodes. To determine the identities of the first and second hosts, see host1.yml and host2.yml in /opt/exabeam_installer/host_vars.
4. Click **ADD** to apply the configuration.

5. Repeat steps 2-4 for all remote clusters before proceeding to step 6.

6. After adding all remote clusters, click **APPLY ALL** to apply the changes. Some nodes will be restarted; therefore the current cluster may be slow for roughly 10-30 minutes depending on the cluster size. It is recommended to add all the remote clusters first before clicking on APPLY ALL. This way the restart will pick up all the new configs in one step. It is also recommended to do this during a downtime period.

### 9.4. Exabeam Data Lake Cross-cluster Health Monitoring and Handling

**Hardware and Virtual Deployments Only**

The availability of a participating remote cluster is shown with color indicators on the cluster list. At the time of a cross-cluster query, only active clusters are queried. Clusters with less than available status are not queried for results. The status of each cluster is shown in the Availability column and is updated at the time of querying.

- **Green** = enabled and available cluster
- **Grey** = disabled and unavailable cluster and will be passed over during querying
- **Red** = enabled cluster but is not available and will be passed over during querying
- **Yellow** = enabled and the availability is unknown.

**NOTE**

The **yellow** cluster status will usually change to the actual status of **green**/**red** within 5 seconds after first setting up a cluster.

Clusters with less than available status are those that did not respond to health checks in a timely manner. This can be a delayed response due to load issues or no response at all due to an outage. In either case, such clusters should be investigated. The statuses of restored or repaired clusters are upgraded in the health check before the next cross-cluster search is run.
9.5. How to Enable/Disable/Delete Exabeam Data Lake Remote Clusters for Cross-cluster Search
Hardware and Virtual Deployments Only

In a cross-cluster search list, a registered cluster can be taken out of or reinstated into the query pool at
the Clusters submenu manually, regardless of the health of the cluster.

To change the availability of a cluster:

1. Navigate to **Settings > Cluster Management > Clusters**.
2. Click the **vertical ellipsis** to open the status menu.
3. Select the cluster status:

   - **Enable** -- Reinstate a cluster into the query pool. Use this status if the cluster has been returned to
     working order and was previously removed.
   - **Disable** -- Take a cluster out of use in the query pool. You may use this status to prevent the use of a
     cluster that is under repair or maintenance.
   - **Delete** -- Permanently disassociate the cluster from the query pool. You may use this status to
     remove clusters that will no longer participate in the query pool. The cluster is not delete and can be
     reregistered.

9.6. Exabeam Data Lake Remote Cluster Data Access Permissions for Cross-cluster Search
Hardware and Virtual Deployments Only

To run cross-cluster searches, in addition to registering remote clusters, access permissions need to
configured. Tiers of access is managed globally and at the clusters locally. Permission to execute cross-
cluster searches is configured in two parts:

9.6.1. ROLE-BASED PERMISSIONS
You can restrict the user roles that are allowed to perform a cross-cluster search. By default, only users
with Administrator role have full permissions to create and configure which roles can perform cross-
cluster searches. Role-based permissions must be configured at each cluster.

⚠️ WARNING
Cross-cluster searches are performance intensive, so Exabeam highly recommends limiting the
number of users and roles who can perform cross-cluster searches.
For more information on role-based permissions and configuration, see User Management > Role-based Access Control.

9.6.2. CLUSTER-BASED PERMISSIONS
Each cluster in the cluster list is configured individually and is independent of its peers. You can control which user roles are allowed to execute a cross-cluster search on each individual cluster.

NOTE
Cluster permissions supersede role permissions. Even if your role has permission to execute a cross-cluster search, clusters that are not configured with access for your role will not grant permission for you to perform a search.

To configure access per cluster:

1. Navigate to Settings > Cluster Management > Clusters.
2. Select the cluster to configure in the left panel. The corresponding Access Management menu will appear to the right.
3. Select the checkboxes to the user roles that can run to cross-cluster searches.
4. Click SAVE to save the configuration.

When remote clusters have been successfully incorporated, you will see them selectable in the cluster menu above the Search field.
10. Exabeam Cloud Telemetry Service

Exabeam telemetry service provides valuable quality and health metrics to Exabeam. System events, metrics, and environment health data are collected and sent to Exabeam Cloud, enabling insight into system issues, such as processing downtime (such as processing delays and storage issues) and UI/application availability.

Learn about the different types of telemetry data, possible telemetry data, and disabling this feature.

NOTE
If you do not wish to send any data to the Exabeam Cloud, please follow the opt-out instructions listed in the How to Disable Exabeam Cloud Telemetry Service.

10.1. Prerequisites
For Exabeam to successfully collect telemetry data, please ensure the following prerequisites are met:

- Advanced Analytics I48.4 or later with a valid license
- Data Lake I32 or later with a valid license
- Access to *.cloud.exabeam.com over HTTPS port 443.

10.2. Types of Telemetry Data in Exabeam Cloud Telemetry Service
At a high level, telemetry data falls into one of three categories:

- Metrics (for example, CPU, events-per-second, and processing delay)
- Events (for example, machine restart, user login, and configuration changes)
- Environment (for example, versions, products, nodes, and configuration)

IP addresses and hostnames are masked before being sent to Exabeam Cloud. For example, {"host": "*.*.0.24"}.

10.2.1. METRICS
The example below shows the metrics data sent from the master node to the telemetry service in Exabeam Cloud:

NOTE
The example below is only a partial example and does not show the full payload.

```json
{ "metrics": [ { "points": [[1558614965, 0.29]], "name": "tm.plt.service_cpu.exabeam-web-common-host1"}, {"points": [[1558614965, 0.3457]], "name": "tm.plt.service_memory.exabeam-web-common-host1"}, {"points": [[1558614965, 0.77]], "name": "tm.plt.service_cpu.mongodb-shard-host1"}, {"points": [[1558614965, 0.04947]], "name": "tm.plt.service_memory.mongodb-shard-host1"} ] }
```
10.2.2. EVENTS
The example below shows the events data sent from the master node to the telemetry service in Exabeam Cloud:

```
{ "events": [ { "dateHappened": 1558614965, "title": "Device /dev/shm S.M.A.R.T health check: FAIL", "text": "S.M.A.R.T non-compatible device" } ] }
```

10.2.3. ENVIRONMENT
The example below shows the environment data sent from the master node to the telemetry service in Exabeam Cloud:

```
{ "environment": { "versions": { "uba": { "build": "4", "branch": "I46.2"}, "common": { "build": "7", "branch": "PLT-i12.5"}, "exa_security": { "build": "33", "branch": "cI80815.1" } }, "hosts": { "host3": { "host": "*.*.0.24", "roles": ["oar","cm"] }, "host2": { "host": "*.*.0.72", "roles": ["uba_slave"] }, "host1": { "host": "*.*.0.70", "roles": ["uba_master"] } }, "licenseInfo": { "customer": "EXA-1234567", "gracePeriod": 60, "expiryDate": "10-11-2021", "version": "3", "products": ["User Analytics","Entity Analytics"], "uploadedAt": 1557740839325 } }
```

10.3. Data Collected by Exabeam Cloud Telemetry Service
Exabeam telemetry service provides valuable quality and health metrics to Exabeam. System events, metrics, and environment health data are collected and sent to Exabeam Cloud, enabling insight into system issues, such as processing downtime (such as processing delays and storage issues) and UI/application availability. The table below lists the possible metrics, events, and environment telemetry data.

<table>
<thead>
<tr>
<th>Environment Name</th>
<th>Description</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Nodes, masked IPs, and roles of each node.</td>
<td>Once a day</td>
</tr>
<tr>
<td>Product Version</td>
<td>Versions of each product in your deployment.</td>
<td>Once a day</td>
</tr>
<tr>
<td>License information</td>
<td>License information for each product in your deployment.</td>
<td>Once a day</td>
</tr>
</tbody>
</table>

You can also view a full list of product metrics and events sent to the Exabeam cloud (including when the requests were made and the full payload) by accessing the audit log file located at /opt/exabeam/data/logs/common/cloud-connection-service/telemetry.log.
### Metrics for Advanced Analytics

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>tm.aa.processing_delay_sec</td>
<td>An Advanced Analytics processing delay (if applicable) in seconds.</td>
<td>5 mins</td>
</tr>
<tr>
<td>tm.plt.service_status.&lt;service-name&gt;</td>
<td>Per-service status.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.ssh_logins</td>
<td>Number of SSH logins.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.service_memory.&lt;service-name&gt;</td>
<td>Per-service memory.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.service_cpu.&lt;service-name&gt;</td>
<td>Per-service CPU.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.load_avg_1m</td>
<td>Load average (CPU) per 1-minute, 5-minute, and 10-minute period.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.load_avg_5m</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.plt.load_avg_10m</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.aa.compressed_logs_bytes</td>
<td>Log volume of the last hour.</td>
<td>1 hour</td>
</tr>
<tr>
<td>tm.aa.compressed_events_bytes</td>
<td>Events volume of the last hour.</td>
<td>1 hour</td>
</tr>
<tr>
<td>tm.aa.notable_users</td>
<td>Notable users.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.disk_usage.mongo</td>
<td>Disk usage per partition.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.disk_usage.data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.plt.disk_usage.root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.plt.total_users</td>
<td>Total users.</td>
<td>1 hour</td>
</tr>
<tr>
<td>tm.plt.total_assets</td>
<td>Total assets.</td>
<td>1 hour</td>
</tr>
</tbody>
</table>

### Metrics for Data Lake

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>tm.plt.service_status.&lt;service-name&gt;</td>
<td>Per-service status.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.ssh_logins</td>
<td>Number of SSH logins.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.service_memory.&lt;service-name&gt;</td>
<td>Per-service memory.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.service_cpu.&lt;service-name&gt;</td>
<td>Per-service CPU.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.load_avg_1m</td>
<td>Load average (CPU) broken per 1-minute, 5-minute, and 10-minute period.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.load_avg_5m</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.plt.load_avg_10m</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.plt.disk_usage.mongo</td>
<td>Disk usage per partition.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.plt.disk_usage.data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.plt.disk_usage.root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.plt.disk_usage.es_hot</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.plt.disk_usage.kafka</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.plt.total_users</td>
<td>Total users.</td>
<td>1 hour</td>
</tr>
<tr>
<td>tm.plt.total_assets</td>
<td>Total assets.</td>
<td>1 hour</td>
</tr>
<tr>
<td>tm.dl.es.cluster_status</td>
<td>Elasticsearch cluster status.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.dl.es.number_of_nodes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.dl.es.number_of_data_nodes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.dl.es.active_shards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.dl.es.active_primary_shards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>tm.dl.kafka.total_lag</td>
<td>A Kafka delay if detected.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.dl.kafka.connectors_lag</td>
<td>A Kafka connector lag if detected.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.dl.avg_doc_size_bytes</td>
<td>Average document size.</td>
<td>15 min</td>
</tr>
</tbody>
</table>
### Metrics for Data Lake

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>tm.dl.avg_msg_size_bytes</td>
<td>Average message size.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.dl.index_delay</td>
<td>Index delay if detected.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.dl.connectors_send_rate_bytes</td>
<td>Total connector ingestion rate in bytes.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.dl.ingestion_queue</td>
<td>Kafka topic delay if detected.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.dl.indexing_rate</td>
<td>Average indexing rate.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.dl.shards_today</td>
<td>Elasticsearch shards today.</td>
<td>5 min</td>
</tr>
<tr>
<td>tm.dl.shards_total</td>
<td>Elasticsearch shards total.</td>
<td>5 min</td>
</tr>
</tbody>
</table>

#### 10.3.1. HOW TO DISABLE EXABEAM CLOUD TELEMETRY SERVICE

**Hardware and Virtual Deployments Only**

Cloud Telemetry Service will be enabled by default, following the installation of the relevant product versions. Exabeam highly recommends to connect to the Telemetry Service, in order to enjoy the benefits of future enhancements that will be built using this data.

If you do not wish to send any data to the Exabeam Cloud, the steps required vary depending on your deployment scenario:

- Product Upgrade or Patch Installation
- Product Installation
- Any time after Product Upgrade

#### 10.3.1.1. Disabling Telemetry Before Product Upgrade or Patch Installation

To disable the hosting of telemetry data in the Exabeam Cloud before upgrading your Exabeam product(s):

1. Access the Cloud Connection Service (CCS) configuration files at:

   `/opt/exabeam/config/common/cloud-connection-service/custom/application.conf`

2. Add a new line:

   ```
   cloud.plugin.Telemetry.enabled = false
   ```

3. Perform the upgrade steps described in the Upgrade an On-Premises or Cloud Exabeam Product section.

#### 10.3.1.2. Disabling Telemetry During a Product Installation

To disable the hosting of telemetry data in the Exabeam Cloud while installing your Exabeam product(s):

1. Perform the installation steps described in the product installation section, but do not upload the product license. You will upload the product license later in this process.

2. Access the Cloud Connection Service (CCS) configuration files at:

   `/opt/exabeam/config/common/cloud-connection-service/custom/application.conf`
3. Add a new line:

```bash
cloud.plugin.Telemetry.enabled = false
```

4. Restart CCS by running the following command:

```bash
./opt/exabeam/bin/shell-environment.bash
cloud-connection-service-stop && cloud-connection-service-start
```

5. Upload the product license by following the steps provided in the Download an On-premises or Cloud Exabeam License and ??? sections.

### 10.3.1.3. Disabling Telemetry After Product Upgrade

To disable the hosting of telemetry data in the Exabeam Cloud after upgrading your Exabeam product(s):

1. Access the Cloud Connection Service (CCS) configuration files at:

   ```bash
   /opt/exabeam/config/common/cloud-connection-service/custom/application.conf
   ```

2. Add a new line:

   ```bash
cloud.plugin.Telemetry.enabled = false
   ```

3. Restart CCS by running the following command:

   ```bash
   ./opt/exabeam/bin/shell-environment.bash
cloud-connection-service-stop && cloud-connection-service-start
   ```
11. System Health Page

System Health can be used to check the status of critical functionality across your Data Lake system. Navigate to the System Health page from the Settings tab at the top right corner of any page. System Health monitors various back-end processes of Data Lake and assists Exabeam engineers with troubleshooting. Graphs and tables on the page visually represent the health status for all of the key systems, as well as indexes and the appliance, so you are always able to check statuses at a glance and track health over time.

11.1. Proactive and On-Demand System Health Checks

System Health is used to check the status of critical functionality across your system and assists Exabeam engineers with troubleshooting. Exabeam provides visibility on the backend data pipeline via Health Checks. Graphs and tables on the page visually represent the health status for all of the key systems, as well as indexes and the appliance, so you are always able to check statuses at a glance and track health over time.

Proactive health checks run automatically and periodically in the background.

On-demand health checks can be initiated manually and are run immediately. All newly gathered health check statuses and data is updated in the information panes on the page. All proactive and on-demand health checks are listed on the Health Checks page. Proactive health checks are visible by any user in your organization. Only users with administrator permission can reach the page.

![Exabeam Notification Icon](image)

When a health check is triggered, a notification message is displayed in the upper right corner of the UI. Select the alert icon to open a side panel that lists the alerts and provides additional detail. A panel listing all notifications is expanded.
These alerts are also listed under the Health Alerts tab in the System Health page. In general:

- **Warning**: There is an issue that should be brought to the attention of the user.
- **Critical**: Immediate action is recommended. In all cases, if an alert is raised on your system, please contact Exabeam Customer Success.

To reach the **Health Checks** page, navigate to the **System Health** page from the Settings tab at the top right corner of any page, then select the **Health Checks** tab.

Health check categories are:

- **Service Availability** – License expiration, database, disaster recovery, Web Common application engine, directory service, aggregators, and external connections
- **Node Resources** – Load, performance, and retention capacity
- **Service Availability** (Incident Processors and Repositories) - IR, Hadoop, and Kafka performance metrics

### 11.1.1. DATA LAKE SPECIFIC HEALTH CHECKS

- **Service Availability** (Context Processors and Repositories) - API server, connectors, and collectors
- **Log storage** - Log repository health and utilization
- **Ingestion Limit** - Ingestion queue health and performance
• **Data Lake Archive** - Archive health
• **Data Lake Migrations** - Migration task status
• **Data Lake Index creation** - Last index creation task status
• **Data Lake Index merge** - Merge task status
• **Data Lake Log Forwarding** - Log forwarding task health
• **Data Lake Index Reindex** - Reindex task status and performance

![System Health - Data Lake Health Checks page](image)

**Figure 10. System Health - Data Lake Health Checks page**

11.1.2. **HOW TO CONFIGURE SYSTEM HEALTH ALERT NOTIFICATIONS**
System health alert notifications can be configured for delivery to recipients via email or Syslog.

Navigate to the **Settings > Notifications > Setup Notifications**. This will be where all of your email and Syslog notifications are listed. If you have not yet set up any notifications, this page will be empty. This is where you can configure health alerts to be sent via Email and/or Syslog. You can set up the details of the SMTP server for email notifications and Syslog destination server for alerts to be sent via Syslog.

11.2. **Data Lake Cluster Health Status**
There are components unique to Data Lake that impact health status of clusters overall. It is important to distinguish which part is involved in Data Lake's performance. Health statuses indicate:
<table>
<thead>
<tr>
<th>Status Color</th>
<th>State</th>
<th>Interface Services</th>
<th>Ingestion</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Healthy</td>
<td>All services performing as expected:</td>
<td>Ingestion lag is less than 30 minute</td>
<td>No significant performance issue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• lms-server</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• web-common</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• lms-ui</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>Operational with degraded performance</td>
<td>All services operational with minor performance impact</td>
<td>Ingestion lag is greater than 30 minutes</td>
<td>No significant performance issue</td>
</tr>
<tr>
<td>Red</td>
<td>Severely degraded performance</td>
<td>One or more service is not operating</td>
<td>Ingestion lag is more than 60 minutes and less than 50% of incoming events per second (EPS) is processed</td>
<td>Storage performance is impacted</td>
</tr>
</tbody>
</table>

Table 4. Health Status Indicators

**NOTE**

To further protect Data Lake performance, Exabeam implemented circuit breakers to quash excessively heavy queries. For example, a query that returns billions of results does not reflect a useful search. Circuit breakers would be tripped to cancel such a query to avoid it from drawing Data Lake resources.

11.3. ElasticSearch Status in Exabeam Data Lake

ElasticSearch is the data repository engine in Data Lake. Exabeam provides specific monitoring to its inner workings to assist you with optimization and determining when and how to apply preventive measures.

The **Cluster Status** breaks down the shard status in each Data Lake cluster and will tell you if the cluster is re-balancing. If the number of unassigned shards is increasing or constant, then the status will likely be a yellow warning.

You can view the health of your data repositories by navigating to **Settings > System Health > Cluster Details**.

![Figure 11. Data Lake System Health - Cluster Details page](image)

The status is indicated with the following:
• Good = Healthy condition
• Warning = There is an issue that should be brought to the attention of the user.
• Critical = Immediate action is recommended.

Scroll down the Cluster Details page to view ElasticSearch status and information.

11.3.1. ELASTICSEARCH DETAILS
This table breaks down the memory and number of shards per node. The percentage of memory used here is an important metric and should not go higher than 80%. This will also tells you if there are too many shards in the cluster.

![ElasticSearch Details Table]

Figure 12. Cluster Details page - ElasticSearch

11.3.2. SHARD STATS
Statistical information for shards in your clusters can outputted to a file for further examination. Go to the Shard Stats panel and then click shard stats file to export a shards information file.

![Shard Stats Panel]

Figure 13. Cluster Details page - Shards Stats Download

11.4. Get to Know the Exabeam Data Lake Indexing Metrics Tab
The status of indexes reflects the health of data ingestion for your clusters. You can reach the Indexing Metric tab by navigating to Settings > System Health > Indexing Metrics.

The Indexing Metrics tab is broken into three sections:

11.4.1. DATA LAKE FLOW
The Flow begins with Syslog and Collectors. This lets you know the number of logs coming into the system via Syslog or the Log Collectors, which are agent based, running locally on user's machines, and collecting operational data, system metrics, etc.

The Ingestion Queue shows the number of logs in the Log Ingestor. The Log Ingestor consumes events from the Log Collectors as well as any syslog data sent from the Syslog Forwarder and your SIEM, if you have either. The Log Ingestor provides flow control and pushes the logs to the Log Indexer.
The **Indexer** is the piece that is responsible for parsing and enriching before indexing and storing the logs in a distributed search cluster.

At the top right you can select the time-frame over which you want to see the metrics. The below example shows the metrics for the past 2 hours.

If you hover over the graph with your mouse, a line indicating a 1 minute interval will appear. This reflects the number of events (or GB, depending on which measurement is selected at the bottom left) for each system within that minute.

### 11.4.2. AVAILABLE INDEXES

Logs are stored in a distributed search cluster and indexed for many types of searches. These can be structured, unstructured, geographic, metric, etc. in real-time. Data Lake stores all of the logs for each day in separate indexes, as indicated by the date in the name.

Under the Available Indexes section are lists all of the system’s indexes along with the date that index was created, the volume of data contained in that index, the number of events in that index, and when the Volume and Event data was last updated.
11.4.3. HOST METRICS
The Host Metrics panel shows the disk metrics of each host, including CPU, memory usage, used and available Storage. You can view CPU and memory usage over time by changing the View at the top right of the panel.
Appendix A. Technical Support Information

To contact Exabeam Customer Success, please open a case via Community.Exabeam.com.
Appendix B. List of Exabeam Services

The following table lists all services that comprise functional Data Lake nodes. Please refer to this table if you are unsure whether the necessary service is running or is associated with your deployment.

<table>
<thead>
<tr>
<th>Host1 (lms_master)</th>
<th>Host2 (lms_slave)</th>
<th>Host3 (lms_slave)</th>
<th>Host4 (lms_slave)</th>
</tr>
</thead>
<tbody>
<tr>
<td>exabeam-lms-server</td>
<td>exabeam-dl-elastalert</td>
<td>exabeam-dl-elastalert</td>
<td>exabeam-ganglia</td>
</tr>
<tr>
<td>exabeam-web-common</td>
<td>exabeam-ganglia</td>
<td>exabeam-ganglia</td>
<td>exabeam-dl-kafka</td>
</tr>
<tr>
<td>exabeam-logstash</td>
<td>exabeam-web-common</td>
<td>exabeam-web-common</td>
<td>exabeam-dl-kafka</td>
</tr>
<tr>
<td>exabeam-lms-ui</td>
<td>exabeam-dl-kafka</td>
<td>exabeam-dl-kafka</td>
<td>exabeam-dl-kafka</td>
</tr>
<tr>
<td>exabeam-ganglia</td>
<td>exabeam-dl-kafka</td>
<td>exabeam-dl-kafka</td>
<td>exabeam-elasticsearch</td>
</tr>
<tr>
<td>exabeam-web-common</td>
<td>exabeam-dl-kafka</td>
<td>exabeam-dl-kafka</td>
<td>exabeam-elasticsearch</td>
</tr>
<tr>
<td>exabeam-dl-kafka</td>
<td>exabeam-elasticsearch</td>
<td>exabeam-elasticsearch</td>
<td>exabeam-logstash</td>
</tr>
<tr>
<td>exabeam-lms-server</td>
<td>exabeam-elasticsearch</td>
<td>exabeam-elasticsearch</td>
<td>exabeam-calico-node</td>
</tr>
<tr>
<td>exabeam-dl-data-management</td>
<td>exabeam-logstash</td>
<td>exabeam-logstash</td>
<td></td>
</tr>
<tr>
<td>exabeam-dl-kafka</td>
<td>exabeam-zookeeper</td>
<td>exabeam-zookeeper</td>
<td></td>
</tr>
<tr>
<td>exabeam-dl-kafka</td>
<td>exabeam-load-balancer</td>
<td>exabeam-load-balancer</td>
<td></td>
</tr>
<tr>
<td>exabeam-elasticsearch</td>
<td>exabeam-mongo</td>
<td>exabeam-mongo</td>
<td></td>
</tr>
<tr>
<td>exabeam-elasticsearch</td>
<td>exabeam-mongo</td>
<td>exabeam-mongo</td>
<td></td>
</tr>
<tr>
<td>exabeam-elasticsearch</td>
<td>exabeam-mongo</td>
<td>exabeam-mongo</td>
<td></td>
</tr>
<tr>
<td>exabeam-logstash</td>
<td>exabeam-calico-node</td>
<td>exabeam-calico-node</td>
<td></td>
</tr>
<tr>
<td>exabeam-cloud-connection-service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>exabeam-edsexabeam-ganglia</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>exabeam-zookeeper</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>exabeam-load-balancer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>exabeam-mongo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>exabeam-mongo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>exabeam-mongo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>exabeam-calico-node</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table B.1. Services per Node Role
Appendix C. 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.

<table>
<thead>
<tr>
<th>Service</th>
<th>Hosts</th>
<th>Port</th>
<th>TCP</th>
<th>UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>All Cluster Hosts</td>
<td>22</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>BGP</td>
<td>All Cluster Hosts</td>
<td>179</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam Web UI (HTTPS)</td>
<td>All Cluster Hosts</td>
<td>8484</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Docker</td>
<td>All Cluster Hosts</td>
<td>2376</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Docker</td>
<td>All Cluster Hosts</td>
<td>2377</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Docker</td>
<td>All Cluster Hosts</td>
<td>4789</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Docker</td>
<td>All Cluster Hosts</td>
<td>7946</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Docker Registry</td>
<td>Master Host</td>
<td>5000</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Kafka Connector</td>
<td>All Cluster Hosts</td>
<td>8083</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Kafka</td>
<td>All Cluster Hosts</td>
<td>9092</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Kafka</td>
<td>All Cluster Hosts</td>
<td>9093</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Kafka</td>
<td>All Cluster Hosts</td>
<td>9094</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>MongoDB</td>
<td>All Cluster Hosts</td>
<td>27017</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>MongoDB</td>
<td>All Cluster Hosts</td>
<td>27018</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>etcd</td>
<td>First 1 or 3 nodes up to highest odd number</td>
<td>2379</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>etcd</td>
<td>First 1 or 3 nodes up to highest odd number</td>
<td>2380</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Ping</td>
<td>All Cluster Hosts</td>
<td>ICMP</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Elastalert</td>
<td>All Cluster Hosts</td>
<td>3030</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>NTP</td>
<td>Master Host</td>
<td>123</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>DNS</td>
<td>All Cluster Hosts</td>
<td>53</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>Master and Failover Hosts</td>
<td>25</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SMTPS</td>
<td>Master and Failover Hosts</td>
<td>587</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Syslog Forwarder</td>
<td>Target Host</td>
<td>514</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Syslog Forwarder</td>
<td>All Cluster Hosts</td>
<td>515</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam Coordination Service (Zookeeper)</td>
<td>All Cluster Hosts</td>
<td>2181</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam Coordination Service (Zookeeper)</td>
<td>All Cluster Hosts</td>
<td>2888</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam Coordination Service (Zookeeper)</td>
<td>All Cluster Hosts</td>
<td>3888</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam Data LakeUI</td>
<td>Master Host</td>
<td>5601</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam Health Agent</td>
<td>All Cluster Hosts</td>
<td>8659</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam SOAR Syslog</td>
<td>Case Manager Host</td>
<td>9875</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>All Cluster Case Manager Hosts</td>
<td>9200</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Elasticsearch</td>
<td>All Cluster Case Manager Hosts</td>
<td>9300</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Datadog and Threat Intelligence Service</td>
<td>Master and Failover Hosts</td>
<td>443</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>TCP</th>
<th>UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP (Non-secure Connection)</td>
<td>389</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>LDAP (Secure Connection)</td>
<td>636</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Ganglia</td>
<td>8081</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>eStreamer</td>
<td>8000</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Java Management Extensions (JMX)</td>
<td>9999</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Appendix D. Supported Browsers

Exabeam products support the latest versions of:

- Chrome
- Internet Explorer
- Firefox
- Safari