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.
# Exabeam Advanced Analytics Administration Guide - Version SMP 2020.3 (I54)

Published Dec 31, 2020

## Table of Contents

1. Advanced Analytics .................................................................................................................. 6
2. Understand The Basics Of Advanced Analytics ........................................................................ 7
   2.1. Advanced Analytics High-Level Overview ........................................................................ 7
2.2. How Advanced Analytics Works .......................................................................................... 7
   2.2.1. Fetch And Ingest Logs ............................................................................................. 8
   2.2.2. Add Context .......................................................................................................... 8
   2.2.3. Detect Anomalies ................................................................................................... 8
   2.2.4. Assess Risk Using The Risk Engine ......................................................................... 8
2.3. The Advanced Analytics Architecture ................................................................................. 9
3. Deploy Exabeam Products ..................................................................................................... 11
   3.1. Considerations For Installing And Deploying Exabeam Products .................................... 11
   3.1.1. Hardware And Virtual Deployments Only ............................................................... 11
   3.1.2. Supported Exabeam Deployment Configurations .................................................... 12
   3.2. Things You Need To Know About Deploying Advanced Analytics .................................... 13
   3.2.1. Network Ports ....................................................................................................... 13
   3.2.2. Configure Your SIEM ............................................................................................ 14
   3.2.3. Guidelines For Integrating Your LDAP Server ......................................................... 16
   3.2.4. Network Zones ..................................................................................................... 16
   3.3. Pre-Check Scripts For An On-Premises Or Cloud Deployment ......................................... 16
   3.3.1. Run The Installation Pre-Check Script For An On-Premises Or Cloud Deployment ......... 18
   3.4. Install Exabeam Software ............................................................................................. 19
   3.5. Upgrade An Exabeam Product ...................................................................................... 29
   3.5.1. Upgrading Advanced Analytics And Case Manager ................................................ 31
   3.6. Add Ingestion (LIME) Nodes To An Existing Advanced Analytics Cluster ....................... 31
   3.7. Apply Pre-Approved CentOS Updates ......................................................................... 33
4. Configure Advanced Analytics ............................................................................................... 34
   4.1. Set Up Admin Operations ............................................................................................. 34
   4.1.1. Access Exabeam Advanced Analytics ..................................................................... 34
   4.1.2. Set Up Log Management ....................................................................................... 34
   4.1.3. Set Up Training & Scoring ..................................................................................... 35
   4.1.4. Set Up Log Feeds ................................................................................................... 35
   4.1.5. Draft/Published Modes For Log Feeds ..................................................................... 35
   4.1.6. Get Notifications About Important Events .............................................................. 36
   4.1.7. Advanced Analytics Transaction Log And Configuration Backup And Restore ......... 37
   4.1.8. Exabeam Licenses ............................................................................................... 40
   4.1.9. Exabeam Cluster Authentication Token ................................................................... 43
   4.2. Set Up Authentication And Access Control ................................................................... 44
   4.2.1. What Are Accounts & Groups? .............................................................................. 44
   4.2.2. What Are Assets & Networks? ............................................................................... 45
   4.2.3. Common Access Card (CAC) Authentication And Limitations ................................. 46
   4.2.4. Role-Based Access Control .................................................................................... 48
   4.2.5. Out-Of-The-Box Access Roles .............................................................................. 49
   4.2.6. Set Up User Management ....................................................................................... 53
4.9. Disaster Recovery (Advanced Analytics, Case Manager, And Incident Responder) .......................... 140
  4.9.1. Deploy Disaster Recovery .................................................................................................. 140
  4.9.2. Failover To Passive Cluster .............................................................................................. 143
  4.9.3. Replicate Specific Files Across Clusters ............................................................................. 146
  4.9.4. Add Case Manager And Incident Responder To Advanced Analytics Disaster Recovery .................................................................................................................. 149
4.10. Enable Settings To Detect Email Sent To Personal Accounts ................................................ 153
4.11. Manage Security Content In Advanced Analytics ................................................................ 154
  4.11.1. Manually Install A Content Package ............................................................................... 154
  4.11.2. Automatically Install Content Packages ......................................................................... 155
  4.11.3. Manually Check For New Content Packages .................................................................. 155
  4.11.4. Automatically Check For New Content Packages ............................................................ 156
  4.11.5. Upload A Content Package ............................................................................................ 156
  4.11.6. Uninstall A Custom Content Package .......................................................................... 157
4.12. Exabeam Hardening ............................................................................................................... 157
  4.12.1. How To Enable Cross-Site Request Forgery Protection .................................................. 158
  4.12.2. How To Enable Cross-Origin Resource Sharing Protection ........................................... 159
5. Health Status Page ....................................................................................................................... 161
  5.1. Proactive And On-Demand Health Checks ......................................................................... 161
    5.1.1. Configure Alerts For Worker Node Lag .......................................................................... 162
  5.2. System Health Checks .......................................................................................................... 163
  5.3. Alerts For Storage Use ......................................................................................................... 164
    5.3.1. Default Data Retention Settings ..................................................................................... 164
  5.4. System Health Alerts For Disabled Parsers ......................................................................... 164
  5.5. View Storage Usage And Retention Settings ....................................................................... 164
  5.6. Set Up System Optimization ............................................................................................... 165
    5.6.1. Disabled Models .............................................................................................................. 165
    5.6.2. Disabled Parsers ............................................................................................................. 167
    5.6.3. Disabled Event Types .................................................................................................... 168
    5.6.4. Manually Redistribute System Load .............................................................................. 170
    5.6.5. Automatically Redistribute System Load ........................................................................ 172
  5.7. Automatic Shutdown ............................................................................................................ 172
6. Generate Technical Support Information ..................................................................................... 173
7. View Version Information .......................................................................................................... 174
8. Syslog Notifications Key-Value Pair Definitions ........................................................................... 175
1. Advanced Analytics

Exabeam collects and processes data from a log management system and other external context data sources in order to identify advanced security attacks.

Advanced Analytics can identify compromised, malicious insiders, and advanced threats by leveraging logs and contextual information. High risk behaviors in your organization are tracked across networks and assets then articulated into comprehensive timelines so you can focus your investigation from point to point of action rather than manually amassing and sifting data.
2. Understand the Basics of Advanced Analytics

Get to know the foundations of Advanced Analytics, such as Context, Logs, and the Risk Engine. Understand the overall architecture, and how all the parts work together.

2.1. Advanced Analytics High-level Overview

Exabeam Advanced Analytics provides user and entity behavior intelligence on top of existing SIEM and log management data repositories to detect compromised and rogue insiders and present a complete picture of the user session and lateral movement use in the attack chain.

Exabeam pulls logs from a variety of data sources (Domain Controller, VPN, security alerts, DLP etc.) through your existing SIEM, as well as direct ingestion via Syslog, and enriches this data with identity information collected from Active Directory (LDAP). This provides an identity context for credential use. Using behavior modeling and analytics, Exabeam learns normal user credential activities, access characteristics, and automatically asks questions of the data to expose anomalous activities.

Finally, Exabeam places all user credential activities and characteristics on a timeline with scores assigned to anomalous access behavior. Traditional security alerts are also scored, attributed to identities, and placed on the activity timeline. All systems touched by compromised credentials of insiders are identified to reveal the attacker’s path through the IT environment.

The figure below gives a visual representation of the high-level components of the Exabeam solution.

2.2. How Advanced Analytics Works

Exabeam has a two-level approach to identifying incidents. The first layer collects data from log management systems and external context data sources. The second layer consists of a risk engine and Exabeam’s Stateful User Tracking™.

The first layer normalizes the events and enriches them with contextual information about the users and assets in order to understand the entity activities within the environment across a variety of dimensions. At this layer, the statistical modeling profiles the behaviors of the network entities and machine learning is applied in the areas of context estimation, for example, to distinguish between users and service accounts.
In the second layer, as events flow through the processing engine, Exabeam uses Stateful User Tracking™ to connect user activities across multiple accounts, devices and IP addresses and places all user credential activities and characteristics on a timeline with scores assigned to anomalous access behavior. Traditional security alerts are also scored, attributed to identities, and placed on the activity timeline. The risk engine updates risk scores based on input from the anomaly detection layer as well as from other external data sources. The risk engine brings in the security knowledge and expertise in order to bubble up anomalies that are significant security-wise. Incidents are generated when some scores exceed defined thresholds.

2.2.1. FETCH AND INGEST LOGS
Exabeam can fetch logs from SIEM log repositories and also ingest logs via Syslog. We currently support log ingestion from Splunk, Microfocus ArcSight, IBM QRadar, McAfee ESM and RSA Security Analytics, as well as other data sources such as Exabeam Data Lake. For Splunk and QRadar log ingestion is via external API's and Syslog is used for all others. For SIEM solutions, such as LogRhythm, McAfee ESM, and LogLogic, we ingest via Syslog forwarding.

2.2.2. ADD CONTEXT
Logs tell us what the users and entities are doing while context tells us who the users and entities are. These are data sources that typically come from identity services such as Active Directory. They enrich the logs to help with the anomaly detection process or are used directly by the risk engine layer for fact-based rules. Regardless of where these external feeds are used, they all go through the anomaly detection layer as part of an event. Examples of context information potentially used by the anomaly detection layer are the location for a given IP address, ISP name for an IP address, and department for a user. We can also feed contextual information from HR Management Systems, Configuration Management Databases, Identity Systems, etc. Another example of contextual information would be threat intelligence feeds, which would be used by the anomaly detection layer to check if a specific IP is listed in a threat intelligence feed.

2.2.3. DETECT ANOMALIES
This component uses machine learning algorithms to identify users, sessions, and devices and more that are behaving in an anomalous way. The anomalies may be relative to a single user, session, or device or relative to various groups of them. For example, some anomalies may refer to a behavior that is anomalous for a user relative to his past history and other anomalies may take into account anomalous behaviors relative to people with roles similar to the individual (peer group), location, or other grouping mechanisms.

The algorithms are constantly improved upon to increase the speed and accuracy of numerical data calculations. This in turn improves the performance of Advanced Analytics.

2.2.4. ASSESS RISK USING THE RISK ENGINE
The risk engine treats each session as a container and assigns risk scores to the events that are flagged as anomalous. As the sum of event risk scores reach a threshold (a default value of 90), incidents are automatically generated within the Case Management module or escalated as incidents to an existing SIEMs or ticketing systems. The event scores are also available for the user to query through the user interface. In some cases, the scores reflect not only information considered as anomalous by Exabeam based only on behavior log feeds, but it can provide an Exabeam score in connection to other security alerts that may be generated by third-party sources (for example, FireEye or CrowdStrike alerts). These security alerts are integrated into user sessions and scored as factual risks.
2.3. The Advanced Analytics Architecture

Exabeam has a scale-out architecture that is a cluster of nodes that meets the needs of small to global organizations. Customers can start with a single node Exabeam appliance or a cluster of multiple nodes based on the number of active users and the volume of logs processed by the Exabeam engine. Smaller organizations can function on a single node appliance while for larger organizations we can scale horizontally by adding multiple nodes as needed. A node can be a physical appliance or a virtual appliance. Distributing the processing across multiple CPU cores and nodes allows Exabeam to support not only environments with many employees but also high-volume feeds, such as end-point logs or web activity (proxy) logs. Figure 1 shows the Exabeam architecture and the components that run inside the cluster.

LIME (Log Ingestion and Message Extraction): LIME runs on the Master node or a standalone node (depending on the log volume). It is the Exabeam process that interfaces with Exabeam Data Lake or an alternative customer log repository; it fetches the data or receives via Syslog and stores it on HDFS. In addition, it also normalizes the raw logs into events that the rest of the Exabeam pipeline can process. After parsing the events, it places the parsed events into HDFS, where the Master and Slave Nodes will retrieve them for pipeline processing.

HDFS (Hadoop Distributed File System): This is a distributed file system, which organizes file and directory services of individual servers into a global directory in such a way that remote data access is not location-specific but is identical from any client. All files are accessible to all users of the global file system and organization is hierarchical and directory-based. Distributed file systems typically use file or database replication (distributing copies of data on multiple servers) to protect against data access failures. HDFS provides high throughput access to application data and is suitable for applications that have large data sets. It is highly fault-tolerant and enables streaming access to file system data. This is where Exabeam stores the raw logs that are fetched from the SIEM and Syslog, as well as the parsed events that are accessed by the nodes for processing. These files are available to all nodes.

Docker Containers: Each major component of Exabeam (such as LIME, Analytics Engine, HDFS, etc.) is contained within a Docker container. Docker containers wrap up a piece of software in a complete filesystem that contains everything it needs to run: code, run-time, system tools, system libraries – anything
you can install on a server. This guarantees that it will always run the same, regardless of the environment it is running in.

**Master Node:** The master node is the powerful node of the cluster - it runs the processing pipeline and in a multi-node environment also coordinates the activities of the node cluster. The session manager runs on the master node and identifies all logs that belong to a session by putting together all the activities of a user from the time they logon to the time they logoff.

**Worker Nodes:** In a multi-node environment the Worker Nodes are responsible for processing all of the logs generated by high-volume feeds. The Worker Nodes run the Sequence Manager which processes all logs that belong to high volume feeds, such as proxy or endpoint logs.

Exabeam customers can begin with a Master node and add worker nodes as needed. If a cluster has only one node (which is the Master Node), then the node runs both the Session Manager and the Sequence Manager (if needed).

**Distributed Database:** All session, user, asset, and event metadata is sorted in a distributed Mongo database. The database is sharded in order to handle the higher volume of data and the logs stored in each shard are available to all nodes.

**User Interface:** Web Services for the user interface runs on the Master Node, though technically it can run on any. It retrieves data from the database.
3. Deploy Exabeam Products

3.1. Considerations for Installing and Deploying Exabeam Products

3.1.1. 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 or Advanced Analytics i46 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.

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.

3.1.2. SUPPORTED EXABEAM DEPLOYMENT CONFIGURATIONS
Hardware and Virtual Deployments Only
The tables below shows 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.

3.1.2.1. Advanced Analytics Deployment Configurations

- uba = Advanced Analytics
  - uba_master = Advanced Analytics master host
  - uba_slave = Advanced Analytics worker host
  - uba_lime = Advanced Analytics dedicated LIME host
- cm = Case Manager and Incident Responder bundle
- ml = Machine Learning

If more than 1TB worth of logs ingested a day, it is recommended that a standalone LIME node be deployed.

<table>
<thead>
<tr>
<th>Node Host</th>
<th>uba_master</th>
<th>uba_slave</th>
<th>cm</th>
<th>ml</th>
<th>uba_lime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master Node</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Case Manager/Incident Responder Node 1</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Worker Node 2</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dedicated LIME Node 3</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

**IMPORTANT**

Single-node clusters can have `uba_master` configuration only and cannot be combined with Case Manager/Incident Responder. Two-node cluster configuration must have a `uba_master` and Case Manager/Incident Responder, not `uba_slave`. Worker nodes may be deployed in cluster with more than two nodes.
3.2. Things You Need to Know About Deploying Advanced Analytics

Hardware and Virtual Deployments Only

Review considerations for installing and upgrading Advanced Analytics, including network ports, SIEM configurations, setting up your .conf file, the default Syslog template, LDAP server integration, and network zones.

3.2.1. 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 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>Hadoop</td>
<td>All Cluster Hosts</td>
<td>9000</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Hadoop</td>
<td>All Cluster Hosts</td>
<td>50010</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Hadoop</td>
<td>All Cluster Hosts</td>
<td>50020</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>Disaster Recovery Socks Proxy</td>
<td>Master and Failover Hosts</td>
<td>10022</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>Disaster Recovery MongoDb</td>
<td>Master and Failover Hosts</td>
<td>5123</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam Coordination Service</td>
<td>All Cluster Hosts</td>
<td>2181</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam Coordination Service</td>
<td>All Cluster Hosts</td>
<td>2888</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Exabeam Coordination Service</td>
<td>All Cluster Hosts</td>
<td>3888</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
Ensure ports for third-party products allow traffic from Exabeam Hosts.

### 3.2.2. CONFIGURE YOUR SIEM

Depending on which SIEM your organization uses, take these basic configuration steps to connect seamlessly with Exabeam. You will need the IP Address and TCP Port of your SIEM.

#### Site Collector

Exabeam SaaS Cloud uses site collectors to enable you to upload log data from your data centers or VPCs to Exabeam. Site collectors in the Exabeam SaaS Cloud were designed to support most data centers with a single Site Collector.
You can configure more than one site collector for your deployment. For example, if you need to collect logs from multiple data centers or VPCs and upload them to Exabeam.

**Splunk**

Exabeam fetches logs by querying the Splunk Search Head on TCP port 8089. It is possible to distribute search across multiple search heads by manually specifying the different search head IPs. The logs are fetched by leveraging the Splunk APIs.

You can configure your Splunk Cloud connection to fetch logs from Splunk Cloud by setting and configuring a proxy.

To do so, specify the parameters `ProxyHost` and `ProxyPort` in `/opt/exabeam/config/custom/custom_lime_config.conf`.

```
NOTE
The ProxyHost and ProxyPort are optional parameters. When provided, the connection goes through the proxy. If not provided, the connection goes directly to Splunk.
```

Sample configuration for the proxy:

```
Hosts = {
    Splunk1 = {
        Hostname = "10.10.2.123"
        Password = "password"
        Port = 8089
        Username = "admin"
        ProxyHost = "192.158.8.12"
        ProxyPort = 3123
    }
}
```

**IBM QRadar**

Exabeam makes API calls to the QRadar SIEM on TCP port 443 to fetch the logs.

**Syslog**

Exabeam supports direct syslog ingestion. SIEM platforms not listed above can send data to Exabeam in the form of syslogs. Syslog messages may be sent directly by security devices or forwarded by a SIEM. Enabling Syslog collection is recommended in environments where fetching from the SIEM is too slow or where the log sources of interest to the customer aren't all in the SIEM. Syslog ingestion can be enabled for certain log feeds while other log feeds are fetched directly from the SIEM.

**Syslog Server Configuration**

Located at `/opt/exabeam/config/rsyslog/exabeam_rsyslog.conf` this file specifies which protocols to use (TCP, UDP), which ports to open, the layout of the syslog messages we receive, as well as filtering options.
Syslog ingestion can be turned on and off through the Settings page.

### 3.2.3. GUIDELINES FOR INTEGRATING YOUR LDAP SERVER

The Global Catalog server is a domain controller that enables searching for Active Directory objects without requiring replication of the entire contents of Active Directory to every domain controller. It is important to point Exabeam to a Global Catalog server (port 3268) so that they system can gather comprehensive user information.

**NOTE**

Before integrating an LDAP server, please ensure you have installed and properly configured the Exabeam Site Collector.

You will need the IP Address or Hostname, TCP Port (defaults to 389), Base Distinguished Name, Bind Distinguished Name and password to connect to the domain controller (Active Directory). The Base Distinguished Name is the starting point for directory server searches, and the Bind Distinguished Name is the Active Directory user account that has privileges to search for users.

We need the complete Distinguished Name, for example: `CN=exabeam,OU=Service Accounts,OU=Administration,dc=NA,dc=Acme,dc=net`

If there are multiple domains in your environment, you can use the IP address or host name of the domain controller that serves as the Global Catalog server. The Global Catalog server is a domain controller that enables searching for Active Directory objects without requiring replication of the entire contents of Active Directory to every domain controller. It is important to point Exabeam to a Global Catalog server (port 3268) so that Exabeam can gather comprehensive user and asset information across multiple domains. On the other hand, you can configure Exabeam to connect to multiple domain controllers to pull in information from different domains.

### 3.2.4. NETWORK ZONES

You will need the CIDR Range and names of your network zones. Please limit these to networks greater than or equal to /24, as smaller zones may create an excess of unnecessary information.

### 3.3. Pre-Check Scripts for an On-Premises or Cloud Deployment

The table below lists the pre-checks run when you deploy your Exabeam product:

**NOTE**

If a critical pre-check fails, the deployment stops and cannot proceed. If a warning message is displayed on the CLI, a non-critical pre-check failed and the deployment can proceed. You MUST fix unsuccessful pre-checks, those tagged as `FAIL`, before electing to proceed with your deployment.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Critical</th>
<th>First Advanced Analytics Version</th>
<th>First Data LakeVersion</th>
</tr>
</thead>
<tbody>
<tr>
<td>CheckSubnet</td>
<td>Checks if all hosts in the cluster are in the same subnet.</td>
<td>Yes</td>
<td>i46</td>
<td>i20</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong> This pre-check is excluded on Google Cloud Platform deployments.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CheckInstalledPackages</td>
<td>Checks if the following required packages are installed (RPM):</td>
<td>Yes</td>
<td>i46</td>
<td>i22</td>
</tr>
<tr>
<td></td>
<td>• bind-utils</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• curl</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• dmidecode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• git</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• lvm2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• openldap-clients</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• policycoreutils-python</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• rsync</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• screen</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• telnet</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• wget</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• firewalld (v.0.4.4.4 or later)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ipset</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• yum-utils</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CheckSSHDConfig</td>
<td>Checks if SSHD configure file (/etc/ssh/sshd_config) has the following configuration:</td>
<td>No</td>
<td>i46</td>
<td>i22</td>
</tr>
<tr>
<td></td>
<td>• PermitRootLogin no</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• GSSAPIAuthentication no</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• UseDNS no</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CheckInterfaceNames</td>
<td>Checks if the interface names are properly detected.</td>
<td>Yes</td>
<td>i46</td>
<td>i22</td>
</tr>
<tr>
<td>CheckPermissions</td>
<td>Checks for existence and permission of the system key directory.</td>
<td>Yes</td>
<td>i46</td>
<td>i22</td>
</tr>
<tr>
<td>CheckRpmPackAge</td>
<td>Checks if the cluster has packages older than 90 days.</td>
<td>No</td>
<td>i46</td>
<td>i22</td>
</tr>
<tr>
<td>CheckPartitions</td>
<td>Checks if drives are mounted and partitioned correctly.</td>
<td>No</td>
<td>i46</td>
<td>i24</td>
</tr>
</tbody>
</table>
### 3.3.1. RUN THE INSTALLATION PRE-CHECK SCRIPT FOR AN ON-PREMISES OR CLOUD DEPLOYMENT

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. The pre-check script collects and verifies the following information:

- sshd config
- Sufficient disk space
- OS and kernel version
- Networking interfaces
- Memory
- Number of CPUs
- Time zone (UTC is currently the only supported time zone)

**NOTE**

It is strongly recommended that deployment does not proceed if pre-checks do not pass.

**Preconditions:** Linux users should be able to run sudo without password.

Download the `exa_pre_check.py` script from Exabeam Community.

**CAUTION**

Make sure you download the script that corresponds to your current version number of Advanced Analytics. If you are running a multi-node system, you may need to run the script on either all hosts on master node and all worker nodes, or just the master node, depending on the version.
Start a terminal session on a node. You must run the pre-check on all nodes in your deployment.

Run `exa_pre_check.py` and check the output.

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.
```

### 3.4. 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:**

**NOTE**

These instructions will walk you through installing Advanced Analytics and Case Manager (with Incident Responder). If you are installing only Advanced Analytics, please take note of and disregard Case Manager-Incident Responder-related prompts where applicable.
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.

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

4. Change the permission of the file using:

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

5. Execute the following command:

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

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

   ```bash
   /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).

      ```bash
      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 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-2000 (base) Advanced Analytics worker node</td>
<td>LVM (1)</td>
<td>Dedicated Mount (2)</td>
<td>Dedicated Mount (2)</td>
<td>[n/a]</td>
</tr>
<tr>
<td>EX-2000 PLUS Advanced Analytics and Incident Responder worker node</td>
<td>LVM (1)</td>
<td>LVM (1)</td>
<td>LVM (1)</td>
<td>Dedicated Mount (2)</td>
</tr>
<tr>
<td>EX-4000 Advanced Analytics master node</td>
<td>LVM (1)</td>
<td>LVM (1)</td>
<td>LVM (1)</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]}

To manually configure your drives, apply the parameters for the role and node you have assigned your host:
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 EX2000 (base):

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.

{'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 elasticsearch)

[['1', '2']]: default (None): 1

{'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 elasticsearch)

[['1', '2']]: default (None): 1

{'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 elasticsearch)

[['1', '2']]: default (None): 1

To map an EX2000 PLUS:

Deploy Exabeam Products
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.

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 elasticsearch)

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 elasticsearch)

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 elasticsearch)

1) Provision device /dev/xvde to LVM (for data, mongo, or es_hot)
2) Provision device /dev/xvde to dedicated mounts (for hadoop, kafka, or
elasticsearch)
['1', '2']: default (None): 2

Select Option 2 for the remainder drives.

**To map an EX4000:**

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
elasticsearch)
['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
elasticsearch)
['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
elasticsearch)
['1', '2']: default (None): 1
1) Provision device /dev/xvde to LVM (for data, mongo, or es_hot)
2) Provision device /dev/xvde to dedicated mounts (for hadoop, kafka, or elasticsearch)

[['1', '2']: default (None): 2

Select Option 2 for the remainder drives.

9. The following values are recommended.
   a. **For Advanced Analytics** when Case Manager is being deployed:

   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] 22

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 Advanced Analytics, if setting up disaster recovery, configure it here. Please refer to Deploy Disaster Recovery.

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/exabean_installer/init/exabean-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 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.

### 3.5. 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.

<table>
<thead>
<tr>
<th>NOTE</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>WARNING</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you have an existing custom UI port, please set the <code>web_common_external_port</code> variable. Otherwise, access at the custom UI port may be lost after upgrading. Ensure the variable is set in <code>/opt/exabeam_installer/group_vars/all.yml</code>:</td>
</tr>
</tbody>
</table>

```
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:

   ```bash
   sudo systemctl stop sk4compose
   ```

   b. For SkyFormation v.2.1.17 and lower, please run the command below:

   ```bash
   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.

9. When the upgrade finishes, the script will then ask the following questions.

   Upgrade completed. Do you want to start exabeam-analytics now? [y/n] y
   Upgrade completed. Do you want to start lime now? [y/n] y
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.

3.5.1. UPGRADING ADVANCED ANALYTICS AND CASE MANAGER

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:
      ```bash
      sudo systemctl stop sk4compose
      ```
   b. For SkyFormation v.2.1.17 and lower, please run the command below:
      ```bash
      sudo systemctl stop sk4tomcat
      ```

3. SSH to the primary Advanced Analytics machine.

4. Run the command below to start a new screen session:
   ```bash
   screen -LS new_screen
   ```

5. Download the new `Exabeam_[product]_[build_version].sxb` from the Exabeam Community. Place it anywhere on the master node except `/opt/exabeam_installer`.

6. In the same file directory where you saved the `.sxb` file in step 3, run the command below to upgrade Advanced Analytics and Case Manager:
   ```bash
   ./Exabeam_SOAR_SOAR-iyy_zzz.UBA_iyy_zzz.PLATFORM.PLT-iyy_zzz.EXA_SECURITY_cyyyyyy_zz.sxb upgrade
   ```

Use these instructions if you are upgrading a bundled Advanced Analytics and Case Manager deployment.

3.6. Add Ingestion (LIME) Nodes to an Existing Advanced Analytics Cluster

Hardware and Virtual Deployments Only

When you add ingestion nodes to an existing cluster, you boost your ingesting power so you can ingest and parse more logs.

If you have a Log Ingestion Message Extraction (LIME) engine on your master node or you already have dedicated ingestion nodes, which you may have added when you first installed Advanced Analytics, you can add a dedicated ingestion node.

You are prompted to answer questions about how your node should be configured. After answering these questions, please wait twenty minutes to two hours for the process to finish, depending on how many nodes you deployed.

If you have a LIME engine on your master node and you want to add multiple dedicated ingestion nodes, you must first add just one dedicated ingestion node. The LIME engine is disabled on the master node.
and moves to the dedicated ingestion node. After you add this first ingestion node, you can continue to add more as needed.

You can add ingestion nodes only if you ingest logs from Syslog. If you ingest logs from a SIEM, you can use only one LIME engine, on either a master or dedicated node. If you ingest logs from both a SIEM and Syslog, you ingest your SIEM logs using one LIME engine, on either a master or dedicated node, then distribute your Syslog traffic across your other ingestion nodes.

Each ingestion node should handle no more than 11k EPS. This upper limit depends on log mixture and type, how many custom parsers you have, and how complex the parsers are. To follow best practices, use a load balancer to evenly distribute the traffic across the nodes.

Once you add a node to a cluster, you can’t remove it.

Have the following available and provisioned:

- Exabeam credentials
- IP addresses of your ingestion nodes
- Credentials for inter-node communication (Exabeam can create these if they do not already exist)
- A load balancer
- Ensure that you ingest logs from Syslog and your load balancer is configured to send no more than 11k EPS to each node

To add an ingestion node:

1. Start a new screen session:
   ```
   screen -LS new_screen
   ```

2. Run the command below to start the deployment:
   ```
   /opt/exabeam_installer/init/exabeam-multinode-deployment.sh
   ```

3. Menu options appear. Select Add new nodes to the cluster.

4. Indicate how the nodes should be configured:
   ```
   How many nodes do you wish to add? 1
   What is the IP address of node 1 (localhost/127.0.0.1 not allowed)? 10.10.2.88
   What are the roles of node 1? ['uba_slave', 'uba_lime']: uba_lime
   ```

5. Network Time Protocol (NTP) keeps your computer’s clocks in sync. Indicate how this should be configured:
   - If you have a local NTP server, input that information.
   - If you don’t have a local NTP server but your server has Internet access, input the default
     pool.ntp.org.
• If you don't have an NTP server or want to sync with the default NTP server, input `none`.

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**

6. Indicate whether to configure internal DNS servers:
   • If you would like to configure internal DNS servers, input `y`.
   • If you don't want to configure internal DNS servers, input `n`.

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

7. If there are any conflicting networks in the user's domain, override the docker_bip/CIDR value. If you change any of the docker networks, the product automatically uninstalls before you deploy it.
   • To override the value, input `y`.
   • If you don't want to override the value, input `n`.

   **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`

8. To move your Rsyslog filters to the new node, note your ingestion node's host number at `/opt/exabeam_installer/inventory`, then run the command, replacing `[host]` with the host number:

   ```
   scp /etc/rsyslog.d/exabeam_rsyslog.conf exabeam@[host]:/etc/rsyslog.d/
   ```

3.7. **Apply Pre-approved CentOS Updates**
Hardware and Virtual Deployments Only
There may be CentOS patches on released on a periodic basis. These patches are included as part of the upgrade package. Applying the patches would typically require a system reboot.

1. To apply these CentOS updates, execute the below command:

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

2. Select the option **Install pre-approved CentOS package updates.**
4. Configure Advanced Analytics

Everything administrators need to know about setting up and operating Advanced Analytics.

4.1. Set Up Admin Operations

Everything administrators need to know about setting up and operating Advanced Analytics.

4.1.1. ACCESS EXABEAM ADVANCED ANALYTICS

Navigate, log in, and authenticate into your Advanced Analytics environment.

If you have an hardware or virtual deployment of Advanced Analytics, enter the IP address of the server and port number 8484:

https://[IP address]:8484 or https://[IP address]:8484/uba

If you have the SaaS deployment of Advanced Analytics, navigate to https://[company].aa.exabeam.com.

Use your organization credentials to log into your Advanced Analytics product.

These login credentials were established when Advanced Analytics was installed. You can authenticate into Advanced Analytics using LDAP, SAML, CAC, or SSO through Okta. To configure and enable these authentication types, contact your Technical Account Manager.

If you work for a federal agency, you can authenticate into Advanced Analytics using Common Access Card (CAC). United States government personnel use the CAC to access physical spaces, computer networks, and systems. You have readers on your workstations that read your Personal Identity Verification (PIV) and authenticate you into various network resources.

You can authenticate into Advanced Analytics using CAC combined with another authentication mechanism, like Kerberos or local authentication. To configure and enable other authentication mechanisms, contact your Technical Account Manager.

4.1.2. SET UP LOG MANAGEMENT

Large enterprise environments generally include many server, network, and security technologies that can provide useful activity logs to trace who is doing what and where. Log ingestion can be coupled with your Data Lake data repository, that can forward syslogs to Advanced Analytics. (See Data Lake Administration Guide > Syslog Forwarding to Advanced Analytics.)

Use the Log Ingestion Settings page to configure the following log sources:

**NOTE**

The Syslog destination is your site collector IP/FQDN, and only TLS connections are accepted in port TCP/515.
4.1.2.1. View Insights About Syslog Ingested Logs

Advanced Analytics has the ability to test the data pipeline of logs coming in via Syslog.

NOTE
This option is only available if the Enable Syslog Ingestion button is toggled on.

Click the Syslog Stats button to view the number of logs fetched, the number of events parsed, and the number of events created. A warning will also appear that lists any event types that were not created within the Syslog feed that was analyzed.

In this step you can also select Options to limit the time range and number of log events tested.

4.1.3. SET UP TRAINING & SCORING

To build a baseline, Advanced Analytics extensively profiles the people, asset usage, and sessions. For example, in a typical deployment, Advanced Analytics begins by examining typically 60-90 days of an organization's logs. After the initial baseline analysis is done, Advanced Analytics begins assigning scores to each session based on the amount and type of anomalies in the session.

4.1.4. SET UP LOG FEEDS

Advanced Analytics can be configured to fetch log data from a SIEM. Administrators can configure log feeds that can be queried during ingestion. Exabeam provides out-of-the-box queries for various log sources; or you can edit them and apply your own.

Once the log feed is setup, you can perform a test query that fetches a small sample of logs from the log management system. You can also parse the sample logs to make sure that Advanced Analytics is able to normalize the logs. If the system is unable to parse the logs, reach out to Customer Success and the Exabeam team will create a parser for those logs.

4.1.5. DRAFT/PUBLISHED MODES FOR LOG FEEDS

There are two different modes when it comes to adding log feeds under Settings > Log Feeds. When you create a new log feed and complete the workflow you will be asked if you would like to publish the feed. Publishing the feed lets the Analytics Processing Engine know that the respected feed is ready for consumption.

If you choose to not publish the feed then it will be left in draft mode and will not be picked up by the processing engine. You can always publish a feed that is in draft mode at a later time.

This allows you to add multiple feeds and test queries without worrying about the feed being picked up by the processing engine or having the processing engine encounter errors when a draft feed is deleted.

Once a feed is in published mode it will be picked up by the processing engine at the top of the hour.
4.1.6. GET NOTIFICATIONS ABOUT IMPORTANT EVENTS

Configure Advanced Analytics to send Syslog or email notifications about system health, notable sessions, anomalies, and other important events to your external log repository or ticketing system.

Notifications sent with Syslog include useful event fields and their associated values. These event fields are unique to each event type. If the field has an empty value, it isn't included in the notification. Notifications also include reason rule templates. If the UI template changes then the output changes too.

The Email Notification configuration also affects the email actions within Incident Responder playbooks. If this is not configured to a valid SMTP server, you can't send email notifications from within the playbook. Once this has been configured, the Incident Responder service automatically populates as 'IRNotificationSMTPService' for send email actions, including:

- Notify User By Email Phishing
- Phishing Summary Report
- Send Email
- Send Template Email
- Send Indicators via Email

1. Click the Menu, select Settings, then navigate to Log Management > Incident Notification.
2. Click add, then select how you want to be notified. To be notified by Syslog, select Syslog Notification. To be notified by email, select Email Notification.
3. Configure your notification settings.
   If you selected Syslog Notification:
   - IP / Hostname – Enter the IP or host name of your Syslog server.
   - Port – Enter the port for your Syslog server.
   - Protocol – Select the network protocol your Syslog server uses to send messages: TCP, SSL_TCP, or UDP.
   - Syslog Security Level – Select the severity of the event for which you want to be notified:
     - Informational – Normal operational events, no action needed.
     - Debug – Useful information for debugging, sent after an error occurs.
     - Error –
     - Warning – Events that will lead to an error if you don’t take action.
     - Emergency – Your system is unusable.
     - Alert – Events that should be corrected immediately.
     - Notice – Unusual events.
     - Critical –
Notifications by Product – Select all the events for which you want to be notified:
  - System Health –
  - Notable Sessions –
  - Anomalies –
  - AA/CM/OAR Audit –
  - Job Start –
  - Job End –
  - Job Failure –

If you selected Email Notification:
  - Port – Enter 587.
  - SSL – Select this box. Your email notifications are sent using Secure Sockets Layer (SSL) protocol.
  - Username Required –
  - Password Required –
  - Sender Email Address – Enter [yourinstance]@notify.exabeam.com.
  - Recipients – List the email addresses to receive these email notifications, separated by a comma.
  - E-mail Signature – Enter text that’s automatically added to the end of all email notifications.

Notifications by Product – Select all the events for which you want to be notified.

Incident Responder:
  - System Health –

Advanced Analytics:
  - System Health –
  - Notable Sessions –
  - Anomalies –
  - AA/CM/OAR Audit –
  - Job Start –
  - Job End –
  - Job Failure –

4. If you configured Syslog notifications, restart the Analytics Engine.

4.1.7. ADVANCED ANALYTICS TRANSACTION LOG AND CONFIGURATION BACKUP AND RESTORE
Hardware and Virtual Deployments Only
Rebuilding a failed worker node host (from a failed disk for on-premise appliance) or shifting a worker node host to new resources (such as in AWS) takes significant planning. One of the more complex
steps and most prone to error is migrating the configurations. Exabeam has provide a backup mechanism for layered data format (LDF) transaction log and configuration files to minimize the risk of error. To use the configuration backup and restore feature, you must have:

- Amazon Web Services S3 storage or an active Advanced Analytics worker node
- Cluster with two or more worker nodes
- Have read and write permission for the credentials you will configure to access the base path at the storage destination
- A scheduled task in Advanced Analytics to run backup to the storage destination

**NOTE**
To rebuild after a cluster failure, it is recommended that a cloud-based backups be used. To rebuild nodes from disk failures, backup files to a worker node or cloud-based destination.

**WARNING**
Master nodes cannot be backed up and restored. Only worker nodes.

### 4.1.7.1. Set Up Backup Storage
If you want to save the generate backup files to your first worker node, then no further configuration is needed to configure an external storage destination. A worker node destination addresses possible disk failure at the master node appliance. This is not recommended as the sole method for disaster recovery.

If you are storing your configurations at an AWS S3 location, you will need to define the target location before scheduling a backup.

1. Go to **Settings > Additional Settings > Admin Operations > External Storage**.
2. Click **Add** to register an AWS backup destination.
3. Fill all field and then click **TEST CONNECTION** to verify connection credentials.
4. Once a working connection is confirmed **Successful**, click **SAVE**.

### 4.1.7.2. Schedule Up a Configuration Back
Once you have a verified destination to store your files, configure and schedule a recurring backup.

1. Go to **Settings > Additional Settings > Backup & Restore > Backups**.
2. Click **CREATE BACKUP** to generate a new schedule record. If you are changing the destination, click the edit icon on the displayed record.
3. Fill all fields and then click **SAVE** to apply the configuration.

**WARNING**
Time is given in UTC.
A successful backup will place a `backup.exa` file at either the base path of the AWS destination or `/opt/exabeam/data/backup` at the worker node. In the case that the scheduled backup fails to write files to the destination, confirm there is enough space at the destination to hold the files and that the `exabeam-web-common` service is running. (If `exabeam-web-common` is not running, review its `application.log` for hints as to the possible cause.)

### 4.1.7.3. Restore a Host from Configuration Backup

In order to restore a node host using files store off-node, you must have:

- administrator privileges to run tasks a the host
- SSH access to the host
- free space at the restoration partition at the master node host that is greater than 10 times the size of `backup.exa` backup file

1. Copy the backup file, `backup.exa`, from the backup location to the restoration partition. This should be a temporary work directory `<restore_path>` at the master node.
2. Run the following to unpack the EXA file and repopulate files.

   ```bash
   sudo /opt/exabeam/bin/tools/exa-restore <restore_path>/backup.exa
   ```

   `exa-restore` will stop all services, restore files, and then start all services. Monitor the console output for error messages. See Troubleshooting a Restoration if `exa-restore` is unable to run to completion.

3. Remove `backup.exa` and the temporary work directory when restoration is completed.

#### Troubleshooting a Restoration

If restoration does not succeed, the try following below solutions. If the scenarios listed do not match your situation,

**Not Enough Disk Space**

Select a different partition to restore the configuration files to and try to restore again. Otherwise, review files stored in to target destination and offload files to create more space.

**Restore Script Cannot Stop All Services**

Use the following to manually stop all services:

```bash
source /opt/exabeam/bin/shell-environment.bash & & everything-stop
```

**Restore Script Cannot Start All Services**

Use the following to manually start all services:

```bash
source /opt/exabeam/bin/shell-environment.bash & & everything-start
```

**Restore Script Could Not Restore a Particular File**

Use `tar` to manually restore the file:

```bash
```
# Determine the task ID and base directory (<base_dir>) for the file restoration that failed.
# Go to the <base_id>/<task_id> directory and apply following command:

```bash
sudo tar -xzpvf backup.tar backup.tgz -C <baseDir>
```

# Manually start all services.

```bash
source /opt/exabeam/bin/shell-environment.bash && everything-start
```

## 4.1.8. 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](#).

### 4.1.8.1. 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 Advanced Analytics, the Log Ingestion Engine will continue to ingest data, but the Analytics Engine will stop processing. Threat Hunter and telemetry will also 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.

4.1.8.2. 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 Advanced Analytics I41 / 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>V1</th>
<th>V2</th>
<th>V3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Products Supported</strong></td>
<td>• Advanced Analytics</td>
<td>• Advanced Analytics</td>
</tr>
<tr>
<td></td>
<td>• Threat Hunter</td>
<td>• Threat Hunter</td>
</tr>
<tr>
<td></td>
<td>• Entity Analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Product Version</strong></th>
<th>Advanced Analytics I38 and below</th>
<th>Advanced Analytics I41 and below</th>
<th>Advanced Analytics I46 and above</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Uses unique customer ID</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Federal License Mode</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Available to customers through the Exabeam Community</strong></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Licensed enforced in Advanced Analytics</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Licensed enforced in Data Lake</strong></td>
<td>NA</td>
<td>NA</td>
<td>No</td>
</tr>
<tr>
<td><strong>Applied through the UI</strong></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 1. License Version Details
4.1.8.3. 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.

Advanced Analytics product licenses:

• **User Analytics** – This is the core product of Advanced Analytics. Exabeam’s user behavioral analytics security solution provides modern threat detection using behavioral modeling and machine learning.

• **Threat Hunter** – Threat Hunter is a point and click advanced search function which allows for searches across a variety of dimensions, such as Activity Types, User Names, and Reasons. It comes fully integrated with User Analytics.

• **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 an Advanced Analytics V3 license. TIS also allows access to telemetry.

• **Entity Analytics (EA)** – Entity Analytics offers analytics capabilities for internet-connected devices and entities beyond users such as hosts and IP addresses within an environment. Entity Analytics is available as an add-on option. If you are adding Entity Analytics to your existing Advanced Analytics platform, you will be sent a new license key. Note that you may require additional nodes to process asset oriented log sources.

• **Incident Responder** – Also known as Orchestration Automation Response. Incident Responder adds automation to your SOC to make your cyber security incident response team more productive. Incident Responder is available as an add-on option. If you are adding Incident Responder to your existing Advanced Analytics platform, you will be sent a new license key. Note that you may require additional nodes to support automated incident responses.

• **Case Manager** – Case Manager can fully integrate into Advanced Analytics enabling you to optimize analyst workflow by managing the life cycle of your incidents. Case Manager is available as an add-on option. If you are adding Case Manager to your existing Advanced Analytics platform, you will be sent a new license key. Note that you may require additional nodes to support this module extension.

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

4.1.8.4. 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

![My Account](image)

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

### 4.1.9. 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:

1. Navigate to **Settings > Admin Operations > Cluster Authentication Token**.

![Admin Operations](image)

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)**.

![Setup Token Menu](image)

**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>
```

4.2. Set Up Authentication and Access Control

4.2.1. WHAT ARE ACCOUNTS & GROUPS?

**Peer Groups**

Peer groups can be a team, department, division, geographic location, etc. and are defined by the organization. Exabeam uses this information to compare a user's behavior to that of their peers. For example, when a user logs into an application for the first time Exabeam can evaluate if it is normal for a member of their peer group to access that application. When Dynamic Peer Grouping is enabled, Exabeam will use machine learning to choose the best possible peer groups for a user for different activities based on the behaviors they exhibit.

**Executives**

Exabeam watches executive movements very closely because they are privileged and have access to sensitive and confidential information, making their credentials highly desirable for account takeover.
Identifying executives allows the system to model executive assets, thereby prioritizing anomalous behaviors associated with them. For example, we will place a higher score for an anomaly triggered by a non-executive user accessing an executive workstation.

**Service Accounts**

A service account is a user account that belongs to an application rather than an end user and runs a particular piece of software. During the setup process, we work with an organization to identify patterns in service account labels and uses this information to classify accounts as service accounts based on their behavior. Exabeam also adds or removes points from sessions based on service account activity. For example, if a service account logs into an application interactively, we will add points to the session because service accounts should not typically log in to applications.

**4.2.2. WHAT ARE ASSETS & NETWORKS?**

**Workstations & Servers**

Assets are computer devices such as servers, workstations, and printers. During the setup process, we will ask you to review and confirm asset labels. It is important for Exabeam to understand the asset types within the organization - are they Domain Controllers, Exchange Servers, Database Servers or workstations? This adds further context to what Exabeam sees within the logs. For example, if a user performs interactive logons to an Exchange Server on a daily basis, the user is likely an Exchange Administrator. Exabeam automatically pulls in assets from the LDAP server and categorizes them as servers or workstations based on the OS property or the Organizational Units they belong to. In this step, we ask you to review whether the assets tagged by Exabeam are accurate. In addition to configuration of assets during setup, Exabeam also runs an ongoing classifier that classifies assets as workstations or servers based on their behavior.

**Network Zones**

Network zones are internal network locations defined by the organization rather than a physical place. Zones can be cities, business units, buildings, or even specific rooms. For example, "Atlanta" can refer to a network zone within an organization rather than the city itself (all according to an organization’s preference). Administrators can upload information regarding network zones for their internal assets via CSV or add manually one at a time.

**Asset Groups**

Asset Groups are a collection of assets that perform the same function in the organization and need to be treated as a single entity from an anomaly detection perspective. An example of an asset group would be a collection of Exchange Servers. Grouping them this way is useful to our modeling processing because it allows us to treat an asset group as a single entity, reducing the amount of false positives that are generated when users connect to multiple servers within that group. As a concrete example, if a user regularly connects to email exchange server #1 then Exabeam builds a baseline that says this is their normal behavior. But exchange servers are often load-balanced, and if the user then connects to email exchange server #2 we can say that this is still normal behavior for them because the exchange servers are one Asset Group. Other examples of asset groups are SharePoint farms, or Virtual Desktop Infrastructure (VDI).
4.2.3. 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 1. Add User menu](image)

4.2.3.1. 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.

```
#!/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)
# 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"
openssl x509 -req -days 365 -in client.csr -CA ca.pem -CAkey ca.key -set_serial 0x`openssl rand 16 -hex` -sha256 -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.

4.2.3.2. 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 {
        interface = "0.0.0.0"
        #hostname = "<hostname>"
        port = 8484
        https = true
        sslKeystore = "$EXABEAM_HOME/config/custom/keystore.jks"
        sslKeypass = "password"
# The following property enables Two-Way Client SSL Authentication
sslClientAuth = true

To install client certificates for CAC, add the client certificate bundle to the trust store on the master host. Example below (replace the name of the file with the bundle you are installing):

```
# For Exabeam Data Lake
sudo docker exec exabeam-web-common-host1 /bin/bash -c "cd /opt/exabeam/config/custom; keytool -import -trustcacerts -alias cacbundle -file ca.pem -keystore truststore.jks -storepass changeit -noprompt"

# For Exabeam Advanced Analytics
sudo docker exec exabeam-web-common /bin/bash -c "cd /opt/exabeam/config/custom; keytool -import -trustcacerts -alias cacbundle -file ca.pem -keystore truststore.jks -storepass changeit -noprompt"
```

To verify the contents of the trust store on the master host, run the following:

```
# For Exabeam Data Lake
sudo docker exec exabeam-web-common-host1 /bin/bash -c "keytool -list -v -keystore /opt/exabeam/config/custom/truststore.jks -storepass changeit"

# For Exabeam Advanced Analytics
sudo docker exec exabeam-web-common /bin/bash -c "keytool -list -v -keystore /opt/exabeam/config/custom/truststore.jks -storepass changeit"
```

After configuration changes, restart `web-common`.

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

### 4.2.4. 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.

**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.**
4.2.5. 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.

**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>View Comments</td>
<td>View comments</td>
</tr>
<tr>
<td>View Activities</td>
<td>View all notable users, assets, sessions, and related risk reasons in the organization.</td>
</tr>
<tr>
<td>View Global Insights</td>
<td>View the organizational models built by Exabeam. The histograms that show the normal behavior for all entities in the organization can be viewed.</td>
</tr>
<tr>
<td>View Executive Info</td>
<td>View the risk reasons and the timeline of the executive users in the organization. You will be able to see the activities performed by executive users along with the associated anomalies.</td>
</tr>
<tr>
<td>View Incidents</td>
<td>View incidents.</td>
</tr>
<tr>
<td>View Infographics</td>
<td>View all the infographics built by Exabeam. You will be able to see the overall trends for the organization.</td>
</tr>
<tr>
<td>View Insights</td>
<td>View the normal behaviors for specific entities within the organization. The histograms for specific users and assets can be viewed.</td>
</tr>
<tr>
<td>Search Incidents</td>
<td>Can search keywords in Incident Responder via the search bar.</td>
</tr>
<tr>
<td>Basic Search</td>
<td>Perform basic search on the Exabeam homepage. Basic search allows you to search for a specific user, asset, session, or a security alert.</td>
</tr>
<tr>
<td>View Search Library</td>
<td>View the Search Library provided by Exabeam and the corresponding search results associated with the filters.</td>
</tr>
<tr>
<td>Threat Hunting</td>
<td>Perform threat hunting on Exabeam. Threat hunting allows you to query the platform across a variety of dimension such as find all users whose sessions contain data exfiltration activities or a malware on their asset.</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>View Executive Info</td>
<td>View the risk reasons and the timeline of the executive users in the organization. You will be able to see the activities performed by executive users along with the associated anomalies.</td>
</tr>
<tr>
<td>Permission</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>View Activities</td>
<td>View all notable users, assets, sessions and related risk reasons in the organization.</td>
</tr>
<tr>
<td>View Executive Info</td>
<td>View the risk reasons and the timeline of the executive users in the organization. You will be able to see the activities performed by executive users along with the associated anomalies.</td>
</tr>
<tr>
<td>View Global Insights</td>
<td>View the organizational models built by Exabeam. The histograms that show the normal behavior for all entities in the organization can be viewed.</td>
</tr>
<tr>
<td>View Insights</td>
<td>View the normal behaviors for specific entities within the organization. The histograms for specific users and assets can be viewed.</td>
</tr>
<tr>
<td>Add AA Comments</td>
<td>Add comments for the various entities (users, assets and sessions) within Exabeam.</td>
</tr>
<tr>
<td>Sending Incidents to Incident Responder</td>
<td>Send incidents to Incident Responder.</td>
</tr>
<tr>
<td>Basic Search</td>
<td>Perform basic search on the Exabeam homepage. Basic search allows you to search for a specific user, asset, session, or a security alert.</td>
</tr>
</tbody>
</table>

**Tier 3 Analyst:** Users assigned to this role will be performing more complex investigations and remediation plans. They can review user sessions, account lockouts, add comments, approve activities and perform threat hunting. 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>View Activities</td>
<td>View all notable users, assets, sessions and related risk reasons in the organization.</td>
</tr>
<tr>
<td>View Executive Info</td>
<td>View the risk reasons and the timeline of the executive users in the organization. You will be able to see the activities performed by executive users along with the associated anomalies.</td>
</tr>
<tr>
<td>View Global Insights</td>
<td>View the organizational models built by Exabeam. The histograms that show the normal behavior for all entities in the organization can be viewed.</td>
</tr>
<tr>
<td>View Insights</td>
<td>View the normal behaviors for specific entities within the organization. The histograms for specific users and assets can be viewed.</td>
</tr>
<tr>
<td>Approve Lockouts</td>
<td>Accept account lockout activities for users. Accepting lockouts indicates to Exabeam that the specific set of behaviors for that lockout activity sequence are whitelisted and are deemed normal for that user.</td>
</tr>
<tr>
<td>Accept Sessions</td>
<td>Accept sessions for users. Accepting sessions indicates to Exabeam that the specific set of behaviors for that session are whitelisted and are deemed normal for that user.</td>
</tr>
<tr>
<td>Add AA Comments</td>
<td>Add comments for the various entities (users, assets and sessions) within Exabeam.</td>
</tr>
<tr>
<td>Manage Rules</td>
<td>Create/Edit/Reload rules that determine how security events are handled.</td>
</tr>
<tr>
<td>Manage Watchlist</td>
<td>Add or remove users from the Watchlist. Users that have been added to the Watchlist are always listed on the Exabeam homepage, allowing them to be scrutinized closely.</td>
</tr>
<tr>
<td>Sending incidents to Incident Responder</td>
<td>Send incidents to Incident Responder.</td>
</tr>
<tr>
<td>Manage Search Library</td>
<td>Create saved searches as well as edit them.</td>
</tr>
<tr>
<td>Basic Search</td>
<td>Perform basic search on the Exabeam homepage. Basic search allows you to search for a specific user, asset, session, or a security alert.</td>
</tr>
<tr>
<td>View Search Library</td>
<td>View the Search Library provided by Exabeam and the corresponding search results associated with the filters.</td>
</tr>
<tr>
<td>Threat Hunting</td>
<td>Perform threat hunting on Exabeam. Threat hunting allows you to query the platform across a variety of dimensions such as find all users whose sessions contain data exfiltration activities or a malware on their asset.</td>
</tr>
</tbody>
</table>
Data Privacy Officer: This role is needed only when the data masking feature is turned on within Exabeam. Users assigned to this role are the only users that can view personally identifiable information (PII) in an unmasked form. They can review user sessions, account lockouts, add comments, approve activities and perform threat hunting. This is a predefined role provided by Exabeam.

See the section in this document titled Mask Data Within the Advanced Analytics UI on the next page for more information on this feature.

Default permissions include:

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Activities</td>
<td>View all notable users, assets, sessions and related risk reasons in the organization.</td>
</tr>
<tr>
<td>View Executive Info</td>
<td>View the risk reasons and the timeline of the executive users in the organization. You will be able to see the activities performed by executive users along with the associated anomalies.</td>
</tr>
<tr>
<td>View Global Insights</td>
<td>View the organizational models built by Exabeam. The histograms that show the normal behavior for all entities in the organization can be viewed.</td>
</tr>
<tr>
<td>View Infographics</td>
<td>View all the infographics built by Exabeam. You will be able to see the overall trends for the organization.</td>
</tr>
<tr>
<td>View Insights</td>
<td>View the normal behaviors for specific entities within the organization. The histograms for specific users and assets can be viewed.</td>
</tr>
<tr>
<td>Basic Search</td>
<td>Perform basic search on the Exabeam homepage. Basic search allows you to search for a specific user, asset, session, or a security alert.</td>
</tr>
<tr>
<td>View Search Library</td>
<td>View the Search Library provided by Exabeam and the corresponding search results associated with the filters.</td>
</tr>
<tr>
<td>Threat Hunting</td>
<td>Perform threat hunting on Exabeam. Threat hunting allows you to query the platform across a variety of dimensions such as find all users whose sessions contain data exfiltration activities or a malware on their asset.</td>
</tr>
</tbody>
</table>

4.2.5.1. Mask Data Within the Advanced Analytics UI

NOTE
To enable/disable and configure data masking, please contact your Exabeam technical representative.

NOTE
Data masking is not supported in Case Management or Incident Responder modules.

Data masking within the UI ensures that personal data cannot be read, copied, modified, or removed without authorization during processing or use. With data masking enabled, the only user able to see a user's personal information will be users assigned to the permission "View Clear Text Data". The default role "Data Privacy Officer" is assigned this permission out of the box. Data masking is a configurable setting and is turned off by default.

To enable data masking in the UI, the dataMaskingEnabled field needs to be set to true. This is located in /opt/exabeam/config/tequila/custom/application.config.

PII {
   # Globally enable/disable data masking on all the PII configured fields.
   Default value is false.
   dataMaskingEnabled = true
}
You’re able to fully customize which PII data is masked or shown in your deployment. The following fields are available when configuring PII data masking:

- **Default** – This is the standard list of PII values controlled by Exabeam. If data masking is enabled, all of these fields are encrypted.
- **Custom** – Encrypt additional fields beyond the default list by adding them to this custom list. The default is empty.
- **Excluded** – Do not encrypt these fields. Adds that are in the default list to expose their values in your deployment. The default is empty.

For example, if you want to mask all default fields other than "task name" and also want to mask the "address" field, then you would configure the lists as shown below:

```plaintext
PII {
  # Globally enable/disable data masking on all the PII configured fields.
  Default value is false.
  dataMaskingEnabled = true
  dataMaskingSuffix = ":M"
  encryptedFields = {
    #encrypt fields
    event {
      default = [
        #EventFieldName
        "user",
        "account",
        ...
        "task_name"
      ]
      custom="["address"]"
      excluded="["task_name"]"
    }
    ...
  }
}
```

### 4.2.5.2. Mask Data for Notifications

You can configure Advanced Analytics to mask specific fields when sending notable sessions and/or anomalous rules via email, Splunk, and QRadar. This prevents exposure of sensitive data when viewing alerts sent to external destinations.

**NOTE**

Advanced Analytics activity log data is not masked or obfuscated when sent via Syslog. It is your responsibility to upload the data to a dedicated index which is available only to users with appropriate privileges.

Before proceeding through the steps below, ensure your deployment has:

- Enabled data masking (instructions below)
• Configured a destination for Notable Sessions notifications sent from Advanced Analytics via Incident Notifications

By default, all fields in a notification are unmasked. To enable data masking for notifications, the Enabled field needs to be set to true. This is located in the application.conf file in the path /opt/exabeam/config/tequila/custom.

```
NotificationRouter {
    ...
    Masking {
        Enabled = true
        Types = [...]  
        NotableSessionFields = [...]  
        AnomaliesRulesFields = [...]  
    }
}
```

Use the Types field to add the notification destinations (Syslog, Email, QRadar, and/or Splunk). Then, use the NotableSessionFields and AnomaliesRulesFields to mask specific fields included in a notification.

For example, if you want to mask the user, source host and IP, and destination host and IP for notifications sent via syslog and Splunk, then you would configure the lists as shown below:

```
NotificationRouter {
    ...
    Masking {
        Enabled = true
        Types = [Syslog, Splunk]
        NotableSessionFields = ["user", "src_host", "src_ip", "dest_host", "dest_ip"]
    }
}
```

4.2.6. SET UP USER MANAGEMENT
Users are the analysts that have access to the Exabeam UI to review and investigate activity. These analysts also have the ability to accept sessions. Exabeam supports local authentication or authentication against an LDAP server.

4.2.6.1. Roles
Exabeam supports role-based access control. Under Default Roles are the roles that Exabeam has created; these cannot be deleted or modified. Selecting a role displays the permissions associated with that role.

Users can also create custom roles by selecting Create a New Role. In this dialogue box you will be asked to name the role and select the permissions associated with it.
4.2.6.2. Add an Exabeam Role

Exabeam’s default roles include Administrator, Auditor, and Tier (1 and 3) Analyst. If you do not want to use these default roles or edit their permissions, create ones that best suit your organization.

To add a new role:

1. Navigate to Settings > Exabeam User Management > Roles.
2. Click Create Role.
3. Fill the Create a new role fields and click SAVE. The search box allows you to search for specific permissions. Your newly created role should appear in the Roles UI under Custom Roles and can be assigned to any analyst.
4. To start assigning users to the role, select the role and click Next, which will direct you to the Users UI to edit user settings. Edit the configuration for the users you wish to add the role to and click Next to apply the changes.

4.2.6.3. Supported Permissions

Administration

- All Admin Ops: Perform all Exabeam administrative operations such as configuring the appliance, connecting to the log repository and Active Directory, setting up log feeds, managing users and roles that access the Exabeam UI, and performing system health checks.
- Manage Users and Context Sources: 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)
- Manage context tables: Manage users, assets or other objects within Context Tables.

Comments

- Add Advanced Analytics Comments: Add comments for the various entities (users, assets and sessions) within Exabeam.
- Add Incident Responder Comments

Create

- Create incidents
- Upload Custom Services: Upload custom actions or services.

Delete

- Delete incidents

Manage

- Manage Bi-directional Communication: Configure inbound and outbound settings for Bi-Directional Communications.
• Manage Data Ingest: Configure log sources and feeds and email-based ingest.
• Manage Playbooks: Create, update, or delete playbooks.
• Manage Services: Configure, edit, or delete services (3rd party integrations).
• Manage Triggers: Create, update, or delete playbook triggers.
• Run Playbooks: Run a playbook manually from the workbench.
• Manage Checklist Definitions: Configure checklist definitions.
• Manage ingest rules: Add, edit, or delete rules for how incidents are assigned, restricted, and prioritized on ingest.
• Manage Queues: Create, edit, delete, and assign membership to queues
• Manage Templates: Create, edit, or delete playbook templates.
• Run Actions: Launch individual actions from the user interface.

View

• Manage Incident Configs: Manage Incident Incident Responder Configs
• View API
• View Executive Info: View the risk reasons and the timeline of the executive users in the organization. You will be able to see the activities performed by executive users along with the associated anomalies.
• View health
• View Raw Logs: View the raw logs that are used to built the events on AA timeline.
• View Infographics: View all the infographics built by Exabeam. You will be able to see the overall trends for the organization.
• View Metrics: View the Incident Responder Metrics page.
• View Activities: View all notable users, assets, sessions and related risk reasons in the organization.
• View comments
• View Global Insights: View the organizational models built by Exabeam. The histograms that show the normal behavior for all entities in the organization can be viewed.
• View incidents
• View Insights: View the normal behaviors for specific entities within the organization. The histograms for specific users and assets can be viewed.
• View Rules: View configured rules that determine how security events are handled

Edit & Approve

• Approve Lockouts: Accept account lockout activities for users. Accepting lockouts indicates to Exabeam that the specific set of behaviors for that lockout activity sequence are whitelisted and are deemed normal for that user.
• Bulk Edit: Users can edit multiple incidents at the same time.
• Edit incidents: Edit an incident's fields, edit entities & artifacts.
• Manage Watchlist: Add or remove users from the Watchlist. Users that have been added to the Watchlist are always listed on the Exabeam homepage, allowing them to be scrutinized closely.
• Accept Sessions: Accept sessions for users. Accepting sessions indicates to Exabeam that the specific set of behaviors for that session are whitelisted and are deemed normal for that user.
• Delete entities and artifacts: Users can delete entities and artifacts.
• Manage Rules: Create/Edit/Reload rules that determine how security events are handled
• Sending incidents to Incident Responder

Search

• Manage Search Library: Create saved searches as well as edit them.
• Basic Search: Perform basic search on the Exabeam homepage. Basic search allows you to search for a specific user, asset, session, or a security alert.
• Threat Hunting: Perform thread hunting on Exabeam. Query the platform across a variety of dimensions such as find all users whose sessions contain data exfiltration activities or a malware on their asset.
• Manage Threat Hunting Public searches: Create, update, delete saved public searches
• Search Incidents: Can search keywords in Incident Responder via the search bar.
• View Search Library: View the Search Library provided by Exabeam and the corresponding search results associated with the filters.

Data Privacy

• View Unmasked Data (PII): Show all personally identifiable information (PII) in a clear text form. When data masking is enabled within Exabeam, this permission should be enabled only for select users that need to see PII in a clear text form.

4.2.7. MANAGE USERS

Understand the difference between Roles and Users. Configure the analysts that have access to the Exabeam User Interface, add the analyst's information, assign them roles, and set up user permissions and access based on your organization's needs.

4.2.7.1. Users

Users are the analysts that have access to the Exabeam UI to review and investigate activity. These analysts have specific roles, permissions, and can be assigned Exabeam objects within the platform. They also have the ability to accept sessions. Exabeam supports local authentication or authentication against an LDAP server.

4.2.7.2. Add an Exabeam User

1. Navigate to Settings > Exabeam User Management > Users.
2. Click Add User.
3. Fill the new user fields and select role(s), and then click SAVE.

Your newly created user should appear in the Users UI.

### 4.2.7.3. 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`.

```plaintext
webcommon {
  ...
  auth {
    defaultAdmin {
      username = "admin"
      password = "changeme"
    }
    ...
    passwordConstraints {
      minLength = 8
      maxLength = 32
      lowerCaseCount = 1
      upperCaseCount = 1
      numericCount = 1
      specialCharCount = 1
      spacesAllowed = false
      passwordHistoryCount = 5 # 0 to disable password history checking
    }
    failedLoginLockout = 0  # 0 to disable loginLockout
    passwordExpirationDays = 90 # 0 to disable password expiration
    passwordHashing = "sha256" # accept either sha256 or bcrypt as options
  }
}
```

Configure Advanced Analytics

Exabeam Advanced Analytics Administration Guide - Version SMP 2020.3 (I54)
Published Dec 31, 2020
• 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
```

### 4.2.8. SET UP LDAP SERVER

If you are adding an LDAP server for the first time, then the Add LDAP Server page displays when you reach the Import LDAP page. Otherwise, if you have already added an existing LDAP server, click Add LDAP Server to add more.

The add/edit LDAP Server page displays the fields necessary to query and pull context information from your LDAP server(s), including:

- **Server Type** – Select either Microsoft Active Directory (default) or NetIQ eDirectory.
- **Primary IP Address or Hostname** – Enter the LDAP IP address or hostname for the primary server of the given server type.

**NOTE**

For context retrieval in Microsoft Active Directory environments, we recommend pointing to a Global Catalog server. To list Global Catalog servers, enter the following command in a Windows command prompt window:

```
nslookup -querytype=srv gc.tcp.acme.local
```

Replace `acme.local` with your company's domain name.

- **I have a secondary server** – If the primary LDAP server is unavailable, Exabeam falls back to the secondary LDAP server if configured. Click this checkbox to add a secondary LDAP server and display a **Secondary IP Address or Hostname** field.
- **TCP Port** – Enter the TCP port of the LDAP server. Optionally, select Enable SSL (LDAPS) and/or Global Catalog to auto-populate the TCP port information accordingly.
- **Bind DN** – Enter the bind domain name, or leave blank for anonymous bind.
- **Bind Password** – Enter the bind password, if applicable.
- **Base DN** – Enter the base domain name. For example, DC=acme, DC=local, etc.

For Microsoft Active Directory:

- **LDAP attributes for Account Name** – This field auto-populated with the value `sAMAccountName`. Please modify the value if your AD deployment uses a different value.

For NetIQ eDirectory:
• **LDAP Attributes** – The list of all attributes to be queried by the Exabeam Domain Service (EDS) component is required. When testing the connection to the eDirectory server, EDS will collect from the server a list of the available attributes and display that list as a drop down menu. Select the name of the attribute from that list or provide a name of your own. Only names for the LDAP attributes you want EDS to poll are required (i.e., not necessarily the full list). Additionally, EDS does not support other types of attributes, therefore you cannot add “new attributes” on the list below.

Click **Validate Connection** to test the LDAP settings.

If you selected **Global Catalog**, this button displays as **Connect & Get Domains**.

**4.2.9. SET UP LDAP AUTHENTICATION**
In addition to local authentication Exabeam can authenticate users via an external LDAP server.

When you arrive at this page, by default the ‘Enable LDAP Authentication’ is selected and the LDAP attribute name is also populated. To change the LDAP attribute, enter the new account name and click Save. To add an LDAP group, select Add LDAP Group and enter the DN of the group you would like to add. Test Settings will tell you how many analysts Exabeam found in the group. From here you can select which role(s) to assign. It is important to note that these roles are assigned to the group and not to the individual analysts; if an analyst changes groups their role will automatically change to the role(s) associated with their new group.

**4.2.10. 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.

**4.2.10.1. 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 `webcommon.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`.

---

Configure Advanced Analytics

Exabeam Advanced Analytics Administration Guide - Version SMP 2020.3 (I54)
Published Dec 31, 2020

59
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.

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.
2. Click the + icon to enable SSO for a SAML application.
3. Click SETUP MY OWN CUSTOM APP.
4. Click Next.
5. Set the **Application** name, and then click **Next**.

![Application name](image)

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.

![Attribute Mapping](image)

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

![Next and OK](image)

9. Click the **vertical ellipse** icon and then click **ON for everyone**.

![Vertical ellipse](image)
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 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 > AD FS > AD FS 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 Jacky1 it becomes [saml]Jacky1, 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:

\[
\]


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

- **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**.

   ![Admin](image)

3. Click **Add Applications**.

   ![Add Applications](image)

4. Click **Create New App**.

   ![Create New App](image)

5. Select **SAML 2.0**.
6. Enter the **App name** and then click **Next**.

![App configuration screen](image)

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

8. Click **Next** to go to the confirmation menu.

![Next button](image)

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

![Selection screen](image)

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 \texttt{md:SingleSignOnService}, where \texttt{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.

**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**)

---

Exabeam Advanced Analytics Administration Guide - Version SMP 2020.3 (I54)
Published Dec 31, 2020

71
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.
EDIT IDENTITY PROVIDER

Use this Identity Provider for SSO
Only one IdP can be enabled at a time.

SAML Provider

SSO Configuration
- Upload the XML file metadata file provided by your IdP
- Configure SSO manually

IdP Certificate

Single Sign-on URL

Single Log-Out URL

Redirect to URL after Log-Out

Query Attributes

<table>
<thead>
<tr>
<th>Exabeam Attributes</th>
<th>IdP Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Address</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td></td>
</tr>
<tr>
<td>First Name</td>
<td></td>
</tr>
<tr>
<td>Last Name</td>
<td></td>
</tr>
<tr>
<td>Group</td>
<td></td>
</tr>
</tbody>
</table>

CANCEL SAVE
Configure Advanced Analytics

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.

**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.

![NEW IDENTITY PROVIDER](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 PROVIDER](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).

![SSO CONFIGURATION](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**.
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.**

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** -- Use internal Exabeam encryption key-pair (located in the trust store). To download the internal certificate, click the **Download certificate** link.
   - **Custom Keys** -- Use the key-pair from your organization.
11. Configure the **Query Attributes** to map your identity provider attributes to Exabeam's attributes.

![Query Attributes](image)

12. Click Save. Your identity provider now appears in the **Identity Providers** table.

![Identity Providers](image)

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

**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**.

![Add Group](image)

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.

**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 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.

### 4.2.10.2. Configure an Identity Provider

Please contact your Technical Account Manager.

1. Click the **Menu**, then navigate to **Settings > Admin Operations > Additional Settings**.
2. Under **User Management**, select **Configure SAML**.
3. Click **Add Identity Provider**.
4. You can configure multiple identity providers for your organization, but enable only one at a time. By default, the IdP is enabled when you save. To disable it, toggle the **IdP Disabled** button.
5. Under **SAML Identity Provider**, select a provider from the list of all supported providers.
6. Decide how you want to configure the SSO:
   - If you have an XML metadata file from your IdP, select **Upload the XML metadata file provided by your IdP**. Click **CHOOSE FILE**, then upload the XML file.
   - If you don't have an XML metadata file, select **Configure SSO manually**. Click **CHOOSE FILE**, upload the IdP certificate, then enter the single sign-on URL. If applicable, enter a single log-out URL or a URL to redirect to after logging out.

7. To map the identity provider attributes to Exabeam attributes, configure the query attributes:

8. Click **SAVE**. Your identity provider appears in the **Identity Providers** table.

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

**4.2.10.3. 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**.

4. Use the checkboxes to select default and custom roles.

5. Click **Save**.

### 4.2.11. SET UP CONTEXT MANAGEMENT

Logs tell Exabeam what the users and entities are doing while context tells us who the users and entities are. These are data sources that typically come from identity services such as Active Directory. They enrich the logs to help with the anomaly detection process or are used directly by the risk engine layer for fact-based rules. Regardless of where these external feeds are used, they all go through the anomaly detection layer as part of an event. Examples of context information potentially used by the anomaly detection layer are the location for a given IP address, ISP name for an IP address, and department for a user.

Analysts are able to view and edit Exabeam's out-of-the-box context tables as well as create their own custom tables. They can select a specific table, such as Executive Users, Service Accounts, etc. and see the details of the table and all of the objects within the table. Edits can be performed on objects individually or through CSV uploads.

#### 4.2.11.1. Out-of-the-Box Context Tables

<table>
<thead>
<tr>
<th>Context Table</th>
<th>Source</th>
<th>Available Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>email_user</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam. Administrators cannot add, edit, or delete the entries in this context table.</td>
</tr>
<tr>
<td>fullname_user</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam. Administrators cannot add, edit, or delete the entries in this context table.</td>
</tr>
<tr>
<td>user_account</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam and add regular expression through the Advanced Analytics tab. Administrators can add entries manually via CSV or AD filters. Where Administrators have manually added users, they can also edit or delete entries.</td>
</tr>
<tr>
<td>Context Table</td>
<td>Source</td>
<td>Available Actions</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>user_department</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam and add regular expression through the Advanced Analytics tab. Administrators can add entries manually via CSV or Active Directory filters. Where Administrators have manually added users, they can also edit or delete entries.</td>
</tr>
<tr>
<td>user_division</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam and add regular expression through the Advanced Analytics tab. Administrators can add entries manually via CSV or Active Directory filters. Where Administrators have manually added users, they can also edit or delete entries.</td>
</tr>
<tr>
<td>user_manager</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam and add regular expression through the Advanced Analytics tab. Administrators can add entries manually via CSV or Active Directory filters. Where Administrators have manually added users, they can also edit or delete entries.</td>
</tr>
<tr>
<td>user_department_number</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam and add regular expression through the Advanced Analytics tab. Administrators can add entries manually via CSV or Active Directory filters. Where Administrators have manually added users, they can also edit or delete entries.</td>
</tr>
<tr>
<td>user_country</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam and add regular expression through the Advanced Analytics tab. Administrators can add entries manually via CSV or Active Directory filters. Where Administrators have manually added users, they can also edit or delete entries.</td>
</tr>
<tr>
<td>user_location</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam and add regular expression through the Advanced Analytics tab. Administrators can add entries manually via CSV or Active Directory filters. Where Administrators have manually added users, they can also edit or delete entries.</td>
</tr>
<tr>
<td>user_title</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam and add regular expression through the Advanced Analytics tab. Administrators can add entries manually via CSV or Active Directory filters. Where Administrators have manually added users, they can also edit or delete entries.</td>
</tr>
<tr>
<td>user_fullname</td>
<td>LDAP</td>
<td>This table is automatically populated when administrators integrate their LDAP system with Exabeam. Administrators cannot add, edit, or delete the entries in this context table.</td>
</tr>
</tbody>
</table>
4.2.11.2. Threat Intelligence Service Context Tables

The table below shows the description of each available threat intelligence feed to a context table in Advanced Analytics:

<table>
<thead>
<tr>
<th>Context Table</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is_ip_threat</td>
<td></td>
<td>IP addresses identified as a threat.</td>
</tr>
<tr>
<td>is_ip_ransomeware_ip</td>
<td></td>
<td>IP addresses associated with ransomware traffic.</td>
</tr>
<tr>
<td>is_tor_ip</td>
<td></td>
<td>Known Tor IP addresses.</td>
</tr>
<tr>
<td>reputation_domains</td>
<td></td>
<td>Domains associated with malware traffic</td>
</tr>
<tr>
<td>web_phishing</td>
<td></td>
<td>Domains associated with phishing attacks.</td>
</tr>
</tbody>
</table>

For more information on Exabeam threat intelligence service, please see the section Threat Intelligence Service Overview.

4.2.12. CUSTOM CONTEXT TABLES

Exabeam provides several filters and lookups to get your security deployment running immediately. However, there may be assets and users within your organization that need particular attention and cannot be fully addressed out of the box. Custom context tables allow you the flexibility to create watchlists or reference lists for assets, threat intelligence indicators, and users/groups that do not fit in the typical deployment categories. Custom context tables let you put parts of your organization under extra monitoring or special scrutiny, such as financial servers, privileged insiders, and high-level departed employees.

Within Advanced Analytics, you can create watchlists using context tables. When creating the table, the Label attribute allows you to attach tags to records that match entries in your context table. This provides quick access to query your results and/or focus your tracking using a global characteristic.

You can also build rules based on entries in your context tables. Set up alerts, actions, or playbooks to trigger when conditions match records, such as access to devices in a special asset group.
4.2.12.1. Context Data

Prepare Context Data

You can upload data as CSV files with either key and value columns or key-only column. All context tables include a Label to tag matching records into groups during parsing and filtering.

**Key-value CSV** – Two-field data file with a header row. This lookup lists correlations between the two fields, such as:

<table>
<thead>
<tr>
<th>Key Fieldname</th>
<th>Value Fieldname</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC1Group</td>
<td>Accounts Receivable</td>
</tr>
<tr>
<td>AC2Group</td>
<td>Accounts Payable</td>
</tr>
</tbody>
</table>

**Key-only CSV** – Single-field data file with no header row. Items on this list are compared to as being present or not during data filtering. For example, a watchlist context table, SpecialGroup, consists of user groups of special interest:

- “Accounts Receivable”
- “Accounts Payable”
- “Accounting Database Admin”

You can create a correlation rule that sends an alert when the monitoring data contains a user having the group name that matches any in the SpecialGroup table.

**Label** – The named tag associated with a record. This allows you to filter groups of records during parsing or filtering. You can also use labels to assemble watchlists based on groupings rather than by individual asset or user record.

---

**NOTE**

You can opt not to use labels by selecting **No Label** during table creation. Otherwise, labels are associated with tables and its records. For key-value context tables, the Label is drawn from the value field of the matching context table entry. For key-only context tables, the **Label** is the table attribute you enter in the **Manual Assignment** field during table creation and is used to tag all matching records.
4.2.12.2. Create Custom Lookups
You must first create a table object to add contextual data to. Create the table with key-only or key-value field and whether labels will used based on the needs of your organization. Use the various methods to add content into your table depending on your data source.

4.2.12.3. Create a Context Table
To introduce context data into your environment, create a table object to contain your data and reference it in queries and lookups.

1. Navigate to Settings > Accounts & Groups > Context Tables.
2. At the top right of the UI, click the blue + to open the New Context Table dialogue box.

3. Fill in the details of the type of context table that this will be.

Fill in table attribute fields:

**Name** – A unique name identifying the table in queries and in the context of your organization.

**Object Type** – The type gives the table additional tagging (with information on the potential data source, such as LDAP for users or user groups).

- **Users** – This object type is associated with users and user group context tables. LDAP data sources can be used to fill its content.
- **Assets** – These are itemizable objects of value to your organization. These can be devices, files, or workstations/servers.
- **Miscellaneous** – These are reference objects of interest, such as tags for groups of objects within a department or network zones.

**Type** – Select the field structure in the table as Key Value or Key Only. See Prepare Context Data for more information. If you are creating a correlation context table, use Key Only.
**Label Assignment** – Click the text source for creating the label or use no label. See *Prepare Context Data* for more information.

4. Click **Save** to advance to the table details UI for the newly created context table.

Your table is ready to store data. The following sections describe ways to add data to your table. Each method is dependent on the data source and intended use of the table.

**4.12.4. Import Data into a Context Table Using CSV**

This is the most flexible method to create unconventional context tables as the CSV file can contain any category or type of data that you wish to monitor.

1. Select your desired context table.
2. Select the **Upload Table** icon.
3. Click **Upload CSV**. From your file system, select the CSV file you wish to import, then select **Next**.

**NOTE**

Key and value (2 fields) tables require a header first row. Do not include a header for keys-only CSV files (1 field). Table names may be alpha-numeric with no blank spaces. (Underscore is acceptable.)

4. Inspect the contents that will be added to your table. Select **Apply Changes**, when you are done.

Once context has been integrated, it is displayed in the table. You can use the lookup tables in rules as required.
For assistance in creating custom context tables, contact Exabeam Customer Success by opening a case at Exabeam Community.

4.2.12.5. Import Data into a Context Table Using an LDAP Connection

This section details the steps required to create context tables to customize your lookups. In this example, we are creating a lookup table with two fields: the userAccountControl field and the User ID field. This allows the event enricher to map one to the other. For example, let’s say you have a log that does not include the username, but instead included the userAccountControl field. This would map the two together. A similar use case would be badge logs: you could create a lookup table that maps the badge ID to the actual username, assuming the badge ID is contained in LDAP.

1. Navigate to the Settings > Accounts & Groups > Context Tables.
2. Click the ‘+’ icon to add a new table.
3. In this example, we use these settings:
   
   Name – useraccountcontrol_user
Object Type – Users

Type – Key Value

Label Assignment – Automatic Assignment from value

4. Click **Save**.
   Click **No Label** if you do not want to add a label to matching records during parsing or filtering.

   The context table now appears in the **Context Management** tables list.

5. Select the name of the context table you created in Step 4 to configure it with values.

   After clicking on `useraccountcontrol_user` you will be presented with the setup page for the `useraccountcontrol_user` context table.

6. Click **+ Add Connection** to connect the context table to an LDAP domain server.
7. Select the **LDAP Server(s)**, **Key**, and **Value** to populate the context table. Optionally, filter the attribute source with conditions by clicking **ADD CONDITION**.

8. Click **TEST CONNECTION** to view and validate the test results, and then click **SAVE**.
Once context has been integrated, it is displayed in the table. You can use the lookup table in rules as required.

For assistance in creating custom context tables, contact Exabeam Customer Success by opening a case at Exabeam Community

4.3. Audit Actions Using Logs

Specific activities related to Exabeam product administrators and users are logged, including activities within the UI as well as configuration and server changes. This is especially useful for reviewing activities of departed employees as well as for audits (for example, GDPR).

The following events are logged:
These audit logs are stored in MongoDB. You can find them at `exabeam_audit_db` inside the `audit_events` collection. The collection stores the entire auditing history. You cannot purge audit logs or set retention limits.

### 4.3.1. AUDIT LOG RETENTION

#### 4.3.1.1. Hardware and Virtual Deployments Only

The Exabeam audit logs are activity logs for user and asset activity in your organization. The logs are held for 90 days by default and retention can be extended up to 365 days.

Retention time is found in `/opt/exabeam/config/common/web/custom/application.conf`, where `webcommon.audit.retentionPeriod` determines the number of days logs are held. The range may be 1 to 365 days.

#### 4.3.2. SEND ADVANCED ANALYTICS ACTIVITY LOG DATA VIA SYSLOG

Access activity data via Syslog. Audit logs of administrative and analyst actions can be forwarded to an existing SIEM or Data Lake via Syslog. Exabeam sends the Advanced Analytics activity data every five minutes.

**NOTE**

Advanced Analytics activity log data is not masked or obfuscated when sent via Syslog. It is your responsibility to upload the data to a dedicated index which is available only to users with appropriate privileges.

To access activity data via Syslog:

1. Navigate to **Settings > Log Management > Incident Notification**.
2. Edit an existing Syslog destination, or create a new Syslog destination.
3. Configure any applicable Syslog settings.
4. After completing the applicable fields, click **TEST CONNECTION**.
   a. If the test fails, validate the configured fields and re-test connectivity until successful.
   b. If the test succeeds, continue to the next step.
5. Click the **AA/CM/OAR Audit** checkbox.

6. Click **Add Notification**.

### 4.4. Starting the Analytics Engine

Once the setup is complete, the administrator can start the Exabeam Analytics Engine. The engine will start fetching the logs from the SIEM, parsing, and then analyzing them. On the **Settings** page, go to **Admin Operations** then **Exabeam Engine** to access controls.

Actions can be restarted from a specific point in time - Exabeam will re-fetch and reprocess all the logs going forward from that time. Note that date and time is given in UTC and starts at epoch (i.e. 00:00:00 hour).

When **Ingest Log Feeds** (and logs are selected) or **Restart Processing** is selected, a **settings** menu is presented.

**Restart the engine** – Select this option if this is the first time the engine is run.

**Restart from the initial training period** – Restart engine using data initially collected.

**Restart from a date** – Reprocess based on specific date (UTC).

### 4.5. Additional Configurations

#### 4.5.1. CONFIGURE STATIC MAPPINGS OF HOSTS TO/FROM IP ADDRESSES

**Hardware and Virtual Deployments Only**

**NOTE**

To configure this feature, please contact your Technical Account Manager.

You can configure static mappings from hosts to IP addresses, and vice versa. This is especially useful for mapping domain controllers (DCs). Since DCs do not often change IPs, you can tie the DC hostname to a specific IP address. Additionally, if there is user activity that isn't tied to a hostname but is tied to an IP address, then you can map the user to their specific, static IP address. This helps maintain and enrich information in events that may be lost or unknown since the system cannot tie events to dynamic IP addresses.

**Map IP addresses to hosts**

Add them to the file: `/opt/exabeam/data/context/dynamic_objects/static_ip_host_mapping.csv`

CSV Format: [ip], [host]

**Map hosts to IP addresses**

Add them to the file: `/opt/exabeam/data/context/dynamic_objects/static_host_ip_mapping.csv`

CSV Format: [host], [ip]
4.5.2. ASSOCIATE MACHINE ORIENTED LOG EVENTS TO USER SESSIONS
Hardware and Virtual Deployments Only
Proxy and other generic sequence events (such as, web, database, file activity, endpoint) as well as some security and DLP alerts may generate logs that contain only machine names or IP addresses without the user names. In Advanced Analytics, you can automatically associate these events with users by IP/host-to-user mapping.

NOTE
This feature is currently only available for sequence events in multi-node deployments.

4.5.2.1. User-Host/IP Association
Exabeam will create an IP/host-to-user association based on specific configurable events. (See example below.) The logic to associate users and hosts is flexible and is configurable by using the UserPresentOnHostIf parameter. For example, you can choose to associate a user and host in Kerberos logon events only if the IP is in a specific network zone.

The configuration also allows you to associate the user with any field based on event type. For example, you can associate the user in a Kerberos logon event with dest_host (destination host) and dest_ip (destination IP), and the user in a remote-access event with src_host (source host) and src_ip (source IP). The user of a remote logon event can be associated with both src_host and dest_host because the events indicates they are present on both.

User-Host Example
The example configuration below shows an association between user and IP event. Edits are made to /opt/exabeam/config/custom/custom_exabeam_config.conf:

```plaintext
UserPresentOnHostIf {
    kerberos-logon = {
        Condition = "not (EndsWith(user, '$') OR InList(user, 'system', 'local service', 'network service', 'anonymous logon'))"
        UserPresentOn = ['dest_host', 'dest_ip']
    }
    remote-logon = {
        Condition = "not (EndsWith(user, '$') OR InList(user, 'system', 'local service', 'network service', 'anonymous logon'))"
        UserPresentOn = ['dest_host', 'src_host', 'dest_ip', 'src_ip']
    }
    remote-access = {
        Condition = "InList(ticket_options, '0x40800000', '0x60810010') && not (EndsWith(user, '$') OR InList(user, 'system', 'local service', 'network service', 'anonymous logon'))"
        UserPresentOn = ['src_host', 'src_ip']
    }
}
```

After editing the configuration file, restart services to apply changes:
4.5.2.2. **User-Event Association**

Based on the host/IP-to-user association described above, Exabeam can associate an event with a host/IP to a user. This is done via the HostToUserMerger parameter. This configuration enables you to determine which events will utilize the created associations as well as which fields should be used to make it.

A user will be resolved from the host/IP only if one user is associated with this host/IP. If more than one user is associated, no user will be resolved.

**User-event example**

The example configuration below defines which events should be considered for resolving the user. The events web-activity-allowed and web-activity-denied are event types that will be associated with the user.

```yaml
HostToUserMerger {
  Enabled = true
  EventTypes = [
    {
      EventType = "web-activity-allowed"
      MergeFields = ["src_host", "src_ip"]
    },
    {
      EventType = "web-activity-denied"
      MergeFields = ["src_host"]
    }
  ]
}
```

After editing the configuration file, restart services to apply changes:

```bash
exabeam-analytics-stop
exabeam-analytics-start
```

4.5.2.3. **Alert-User Association**

The host/IP-to-user association will also be used to resolve the user in security and DLP alerts that do not have one. If one user is on the host during the alert trigger, then the user is associated with a host/IP when resolving a user in security. If there is more than one user on the host, no DLP alerts are associated.

4.5.3. **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.
Configure Advanced Analytics

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.

**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.

4.5.4. **CONFIGURE THREAT HUNTER MAXIMUM SEARCH RESULT LIMIT**

You can configure the maximum search result limit when using Threat Hunter’s search capabilities. By default, the result limit is set to 10,000 sessions.
The default result limit is located in the `application_default.conf` file at `/opt/exabeam/config/tequila/default/application_default.conf`.

All changes should be made to

`/opt/exabeam/config/tequila/custom/application.conf`.

To configure the default result limit, enter an acceptable value in place of `10000` at `tequila.data.criteria`:

```
finalQueryResultLimit = 10000
```

There is no restriction on the limit value, however, for very large intermediate results you should input at least 30,000 sessions.

### 4.5.5. CHANGE DATE AND TIME FORMATS

**Hardware and Virtual Deployments Only**

Change the way dates and times are displayed in Advanced Analytics, Case Manager, and Incident Responder.

---

**NOTE**

To configure this feature, please contact your Technical Account Manager.

Dates and times may appear slightly different between Advanced Analytics, Case Manager, and Incident Responder.

1. Navigate to `/opt/exabeam/config/tequila/custom/`, then open the `application.conf` file.
2. Enter a supported format value:
   - To configure how dates are formatted, enter a supported value after `tequila.data.criteria.dateFormat =`, in quotation marks:
     ```
     tequila.data.criteria.dateFormat = "[value]"
     ```
   - To configure how times are formatted, enter a supported value after `tequila.data.criteria.timeFormat =`, in quotation marks:
     ```
     tequila.data.criteria.timeFormat = "[value]"
     ```
3. Save the `application.conf` file.
4. Restart Advanced Analytics Restful Web Services:
4.5.5.1. Supported Date and Time Formats

View all the ways you can format dates and times displayed in Advanced Analytics, Case Manager, and Incident Responder.

**Date Formats**

By default, dates are displayed in the "default" format, DD Month Year; for example, 27 September 2012.

Depending on the format, some areas of the product, like watchlists and user or asset profiles, may display a shortened or year-less version.

<table>
<thead>
<tr>
<th>Value</th>
<th>Format</th>
<th>Example</th>
<th>Shortened Example</th>
<th>Year-less Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;default&quot;</td>
<td>DD Month YYYY</td>
<td>27 September 2012</td>
<td>27 Sep 2012</td>
<td>27 Sep</td>
</tr>
<tr>
<td>&quot;default-short&quot;</td>
<td>DD Mo YYYY</td>
<td>27 Sep 2012</td>
<td>n/a</td>
<td>27 Sep</td>
</tr>
<tr>
<td>&quot;default-num&quot;</td>
<td>DD-MM-YYYY</td>
<td>27-09-2012</td>
<td>n/a</td>
<td>27-09</td>
</tr>
<tr>
<td>&quot;default-num-short&quot;</td>
<td>DD-MM-YY</td>
<td>27-09-12</td>
<td>n/a</td>
<td>27-09</td>
</tr>
<tr>
<td>&quot;us&quot;</td>
<td>Month DD YYYY</td>
<td>September 27 2012</td>
<td>Sep 27 2012</td>
<td>Sep 27</td>
</tr>
<tr>
<td>&quot;us-short&quot;</td>
<td>Mo DD YYYY</td>
<td>Sep 27 2012</td>
<td>n/a</td>
<td>Sep 27</td>
</tr>
<tr>
<td>&quot;us-num&quot;</td>
<td>MM-DD-YYYY</td>
<td>09-27-2012</td>
<td>n/a</td>
<td>09-27</td>
</tr>
<tr>
<td>&quot;us-num-short&quot;</td>
<td>MM-DD-YY</td>
<td>09-27-12</td>
<td>n/a</td>
<td>09-27</td>
</tr>
<tr>
<td>&quot;ISO&quot;</td>
<td>YYYY-MM-DD</td>
<td>2012-09-27</td>
<td>n/a</td>
<td>09-27</td>
</tr>
<tr>
<td>&quot;ISO-slash&quot;</td>
<td>YYYY/MM/DD</td>
<td>2012/09/27</td>
<td>n/a</td>
<td>09/27</td>
</tr>
</tbody>
</table>

**Time Formats**

By default, times are displayed in 24hr format.

<table>
<thead>
<tr>
<th>Value</th>
<th>Format</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;24hr&quot;</td>
<td>13:45</td>
<td>This is the default value in the configuration file. For chart labels, the time appears as 13 instead of 1pm. Minutes aren't displayed.</td>
</tr>
<tr>
<td>&quot;12hr&quot;</td>
<td>1:45pm</td>
<td>Leading zeros aren't displayed. For example, the time appears as 1:45pm instead of 01:45pm. Some areas of the product use a and p to indicate am and pm.</td>
</tr>
</tbody>
</table>

4.5.6. SET UP MACHINE LEARNING ALGORITHMS (BETA)

Machine Learning (ML) algorithms require a different infrastructure than regular deployments. This infrastructure is necessary to run data science algorithms. ML infrastructure will install two new docker-powered services: Hadoop YARN and Advanced Analytics API.

NOTE These machine learning algorithms are currently available as beta features.

Installation is only supported on EX4000 powered single- or multi-node deployments running Advanced Analytics i35 or later due to the high system resources needed for these jobs. ML infrastructure is a
requirement for algorithms that drive the Personal Email Detection, Daily Activity Change Detection, and Windows Privileged Command Monitoring features.

4.5.6.1. Install and Deploy Machine Learning
Installation is done through the unified installer by specifying the ml product after Advanced Analytics has already been deployed. The build version needs to be identical to the version used for Advanced Analytics.

4.5.6.2. When asked for the docker tag of the image to be used for ML, make sure to use the same tag which was used for Advanced Analytics.

1. Optionally, run this process in screen: screen -LS [yourname]_[todaysdate]
2. Run the following script: /opt/exabeam_installer/init/exabeam-multinode-deployment.sh
3. Select your inputs based on the following prompts:
   - Add Product(s)
     Which product(s) do you wish to add? ['ml', 'lms', 'ir']: ml
     What is the docker tag for new ml images? <AA version_build>
     Would you like to override the default docker_gwbridge IP/CIDR? n
     Do you want to setup disaster recovery? n

4. Stop the Log Ingestion Engine and the Analytics Engine at the shell, make configuration changes, and then restart services.
   a. exa-lime-stop; exa-martini-stop
   b. Edit EventStore parameters in /opt/exabeam/config/custom/custom_exabeam_config.conf:
      
      EventStore.Enabled = true
      EventStore.UseHDFS = true
   c. Navigate to /opt/exabeam/config/custom/custom_exabeam_config.conf and make sure that Event Store is disabled:
      
      EventStore.Enabled = false
   d. Restart the DS server, and then start the Log Ingestion Engine and the Analytics Engine:
      
      ds-server-stop; ds-server-start
      exa-lime-start; exa-martini-start

5. Check the state of the DS server by inspecting the log
   /opt/exabeam/data/logs/ds-server.log
6. Check the DS server logs to ensure the algorithms have been enabled.
   
   grep enabled /opt/exabeam/data/logs/ds-server.log
You should be able to see a list of all algorithms, along with their statuses and configurations.

![NOTE]

Navigate to `/opt/exabeam/ds-server/config/custom/algorithms.conf` and set
 Enabled = true on the DS algorithms you want to implement. If the custom
 algorithms.conf does not contain the DS algorithm you want to implement, copy over the
 corresponding algorithm block from `/opt/exabeam/ds-server/config/default/
 algorithms_default.conf`.

7. Navigate to `/opt/exabeam/data/logs` and enable EventStore:

```yaml
} EventStore {
  UserHDFS = true
  Enabled = true
}
```

8. Restart the Log Ingestion Engine and the Analytics Engine to apply any updates:

```bash
exa-lime-stop
exa-lime-start
exa-martini-stop
exa-martini-start
```

9. Continue to each module to complete your configurations

### 4.5.6.3. Configure Machine Learning

All Machine Learning algorithms use EventStore and expect the data to be stored on HDFS, which
must be manually activated by adding this line to `/opt/exabeam/config/custom/
 custom_exabeam_config.conf`:

```yaml
EventStore.Enabled = true
EventStore.UseHDFS = true
```

All other algorithm-specific configurations should be done in `/opt/exabeam/ds-server/
 config/custom/algorithms.conf`.

The defaults for each algorithm can be found in `/opt/exabeam/ds-server/config/default/
 algorithms_default.conf`. As with other configuration changes, only the options which are
changed should be overwritten in the custom algorithms.conf file.

LogFetcher.LogDir in `/opt/exabeam/config/custom/custom_exabeam_config.conf`
is the path for Martini to find events. DS algorithms use this path as well. Therefore, make sure that you
have SDK.EventStoreHDFSPathTemplates in `/opt/exabeam/ds-server/config/
default/script.conf`, which corresponds to LogFetcher.LogDir.

For example:
4.5.6.4. Upgrade Machine Learning Deployment
ML deployments have to be updated together with the underlying Advanced Analytics version. If Machine Learning is installed, the upgrade tool will ask both for a tag for Advanced Analytics and a tag for ML. Make sure to use the same tag for Advanced Analytics and ML. The format for the tag is `<version>_<build #>`.

4.5.6.5. Upgrading ML Custom Configurations
In i50.6 we have changed the source of processing events. Now, EventStore is no longer needed and should not be enabled to run DS algorithms. Instead, all ML algorithms read events from LogDir. Therefore, if you are upgrading from a version pre-i50.6, make sure EventStore.Type has been removed from these files:

- `ds-server/config/default/algorithms_default.conf`
- `ds-server/config/custom/algorithms.conf`
- `ds-server/config/default/script.conf`

If you have custom settings, you must also make sure that you edit them correctly in order to preserve them. Custom configurations are not automatically updated.

See details on the required edits below:

**In script.conf**

Make sure that you remove EventStore.Type, and change EventStoreHDFSPathTemplates accordingly. Instead of an output generated by Martini, you should connect it to the Lime output.

**Previous version of script.conf:**

```
{
EventStoreHDFSPathTemplates = [
"hdfs://hadoop-master:9000/opt/exabeam/data/output/(YYYY-MM-dd)/(HH).*evt.gz",
]
```

**NOTE**
You can free up space by removing data in hdfs://hadoop-master:9000/opt/exabeam/data/output, which is not required for DS deployments.
"hdfs://hadoop-master:9000/opt/exabeam/data/output/(YYYY-MM-dd)/(HH).[type]-events-{m,s?}.[category].evt.gz"
]
EventStore {
  # Event type. Can be Raw, Container or Any
  Type = "Container"
  # Event category. All available categories are in event_categories.conf
  Categories = ["all"]
}

New version of script.conf:

{
  EventStoreHDFSPathTemplates = [
    "hdfs://hadoop-master:9000/opt/exabeam/data/input/(YYYY-MM-dd)/(HH).*.[category].evt.gz"
  ]
  EventStore {
    # Event category. All available categories are in event_categories.conf
    Categories = ["all"]
  }
}

To check that everything runs correctly, check custom_exabeam_config.conf LogFetcher.LogDir for a path to events folder: /opt/exabeam/config/custom/custom_exabeam_config.conf

LogFetcher {
  UseHDFS = true
  # this path to events folder in HDFS should be the same as in
  # script.conf EventStoreHDFSPathTemplates, main difference
  LogDir = "/opt/exabeam/data/input"
  # this values by default, you don’t have to override it in this config
  HDFSHost = "hadoop-master"
  HDFSPort = 9000
}

This path should be the same as in script.conf EventStoreHDFSPathTemplates:

EventStoreHDFSPathTemplates = [
  "hdfs://hadoop-master:9000/opt/exabeam/data/input/(YYYY-MM-dd)/(HH).*.[category].evt.gz"
]
LogDir = "/opt/exabeam/data/input"

In algorithms.conf

If you customized EventStore.EventType for the personal-email-identification algorithm, daily-activity-change algorithm, or wincli-command-centric algorithm, then you must ensure that you remove parameter EventStore.EventType from the configuration:

Previous version of algorithms.conf:
personal-email-identification {
  ...
  EventStore {
    Type = “Container”
    Categories = ["alerts"]
  }
  ...
}

New version of algorithms.conf:

personal-email-identification {
  ...
  EventStore {
    Categories = ["alerts"]
  }
  ...
}

To check that everything runs correctly, check the log files after launching exabeam-analytics. AA- API: /opt/exabeam/data/logs/aa-api.log DS server: /opt/exabeam/data/logs/ds-server.log # spark log files for all algorithms are located in the folder: /opt/exabeam/data/logs/ds-server Exabeam: /opt/exabeam/data/logs/exabeam.log Also, you can check Processed events: tail -f -n 300 /opt/exabeam/data/logs/exabeam.log | grep Processed You should not see “0 events” for Processed events. If “0 events” persists, then that means that the paths to event files are configured improperly. If you run into this issue, check: /opt/exabeam/config/custom/custom_exabeam_config.conf LogFetcher.LogDir. You should have the same specifications in the HDFS folder as in LogFetcher.LogDir. Also, the folder should contain folders with date and files, such as 00.*.evt.gz – 23.*.evt.gz.

4.5.6.6. Checking ML Status
You can check the status of DS algorithms in the mongo data_science_db. There is a separate collection with the states for each algorithm. You can also check the progress in the Martini logs: tail -f /opt/exabeam/data/logs/exabeam.log

4.5.6.7. Deactivate ML
To deactivate all ML components, shut down the respective services:

ds-server-stop
aa-api-stop
hadoop-yarn-stop

4.5.6.8. Detect Daily Activity Change
Daily activity change detection identifies significant changes in a user’s overall behavior across both sessions (eg: Windows, VPN) and sequence events (eg: web activity, endpoint activity).

In addition to examining individual activities, Advanced Analytics also looks at anomalies in the overall patterns of the daily activities of a user. For example, taken individually it might not be anomalous for a
user to access a server remotely that has been accessed before or download files from Salesforce, but a combination of activities could be anomalous based on the user’s daily activity behavior.

The daily activity change will generate an event. If today’s behavior is significantly different from past behavior, then that event will also generate a triggered rule (DAILY-ACTIVITY-CHANGE) for the event. The risk score from daily activity change is transferred to the user’s session just like any other web or endpoint sequence.

Daily activity change detection is available as a beta capability and by default the feature is turned off.

**Configuration Prerequisites**

Ensure that you have the Machine Learning infrastructure (beta) installed. If you do not, follow the instructions in the section Machine Learning Algorithms (Beta). Then return to these configuration instructions.

**Configuration**

1. Machine Learning Algorithms (Beta) must be deployed in order for the feature to work. Installation is done through the unified installer by specifying the ml product. The build version needs to be identical to the version used for Advanced Analytics.

2. To enable Daily Activity Change add the following line to `/opt/exabeam/ds-server/config/custom/algorithms.conf`:

   ```
   Algorithms.daily-activity-change.Enabled = true
   ```

3. To enable Daily Activity Change, in `/opt/exabeam/ds-server/config/custom/algorithms.conf` set:

   ```
   daily-activity-change {
   ...
   Enabled = true
   ```

4. **EventStore must be disabled:**

   Make sure that in `/opt/exabeam/config/custom/custom_exabeam_config.conf`:

   ```
   EventStore.Enabled = false
   ```

5. **EventStore must also be active for the feature to work:**

   Add the following lines to `/opt/exabeam/config/custom/custom_exabeam_config.conf`:

   ```
   EventStore.Enabled = true
   EventStore.UseHDFS = true
   ```

**Daily Activity Change Parameters**

You can customize configuration parameters for the algorithm under `daily-activity-change` within `algorithms.conf` (/opt/exabeam/ds-server/config/custom/algorithms.conf). Refer to `algorithms_default.conf` (/opt/exabeam/ds-server/config/default/algorithms_default.conf) for default settings.

---

Exabeam Advanced Analytics Administration Guide - Version SMP 2020.3 (I54)
Published Dec 31, 2020
- **VarianceThreshold = 0.95** – variance threshold used by PCA
- **ResidueThreshold = 1** – above this threshold is considered anomalous
- **MinTrainingPeriod = 30** – a minimum period of historic data required to detect daily activity change
- **TrainingPeriod = 90** – data from eventTime - trainingPeriod to eventTime will be taken to train the algorithm
- **RetentionPeriod = 180** – keep historic data for this period
- **RuleId = "DAILY-ACTIVITY-CHANGE"** – in mongo triggered_rule_db triggered_rule_collection all triggered rules by this algorithm will be saved with rule_id = “DAILY-ACTIVITY-CHANGE”
- **RuleEventType = "daily-activity"** – in mongo triggered_rule_db.triggered_rule_collection all triggered rules by this algorithm will be saved with rule_event_type = “daily-activity”
- **DistinctCountIntervalMs = 600000** – time in events from EventStore will be rounded down to 600000 Ms = 10 minutes.
  - For example: 1406877142000 = Friday, August 1, 2014 7:12:22 AM
  - Becomes: 1406877000000 = Friday, August 1, 2014 7:10:00 AM

**Verify Intermediate Results**

This algorithm saves results in the Mongo database. You can check database ds_dac_db. It should have two collections: event_weight and user_activity. They should not be empty while processing.

You can also check triggered_rule_db in collection triggered_rule_collection. There should be some events with rule_id = DAILY-ACTIVITY-CHANGE if there are suspicious users.

**Enable Daily Activity Change**

Ensure that you have the installed. If you do not, follow the instructions in the section *Machine Learning Infrastructure*. Then return to these configuration instructions.

1. Machine Learning Infrastructure must be deployed in order for the feature to work. Installation is done through the unified installer by specifying the ml product. The build version needs to be identical to the version used for Advanced Analytics.

2. Add the following line to /opt/exabeam/ds-server/config/custom/algorithms.conf:

```
Algorithms.daily-activity-change.Enabled = true
```

3. EventStore must also be active for the feature to work.

Add the following lines to /opt/exabeam/config/custom/custom_exabeam_config.conf:
EventStore.Enabled = true
EventStore.UseHDFS = true

4.5.6.9. Monitor Windows Privileged Commands

NOTE
To configure this feature, please contact your Technical Account Manager.

Advanced Analytics now identifies anomalous behaviors around Windows privileged commands performed via command line by privilege users. Attackers move through a network using native Windows commands in order to collect information, perform reconnaissance, spread malware, etc. The pattern of the Windows command usage by attackers is statistically and behaviorally different from that of legitimate users and therefore it is possible to detect anomalous behaviors involving command execution. Exabeam performs an offline machine learning algorithm to detect anomalous Windows command execution and assigns risk scores to users performing them.

Associated Rules:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPA-F-CLI</td>
<td>Suspicious</td>
<td>A native Windows command has been executed which is suspicious for this type of user. For example, a non-technical user is executing complicated powershell commands. Check with the user if they are aware of this and who/what is behind it.</td>
</tr>
</tbody>
</table>

Configuration Prerequisites
Ensure that you have the Machine Learning infrastructure (beta) installed. If you do not, follow the instructions in the section Machine Learning Algorithms. Then return to these configuration instructions.

Configuration
Configuration changes should be made in /opt/exabeam/config/custom/exabeam_custom.config. To enable CLI detection set Enabled = true.

Field Descriptions:

- **Enabled** – Set to true to enable detection; set to false to disable.
- **CmdFlagsRegex** – Regular expressions used for flag extraction.
- **CasheSize** – Number of process IDs to be stored.
- **CacheExpirationTime** – The number of days after which CasheSize is reset.
- **Commands** – List of the CLI commands that the algorithm will monitor.

1. Machine Learning Algorithms (Beta) must be deployed in order for the feature to work. Installation is done through the unified installer by specifying the ml product. The build version needs to be identical to the version used for Advanced Analytics.

2. To enable Windows Command Line Algorithm, in /opt/exabeam/ds-server/config/custom/algorithms.conf set:
wincli-command-centric {
  ...
  Enabled = true
}

Commands and CmdFlagsRegex should be the same as in the custom_exabeam_config.conf.

3. EventStore must be disabled:
   Make sure that in /opt/exabeam/config/custom/custom_exabeam_config.conf:
     EventStore.Enabled = false

Windows Privileged Command Monitoring Parameters

You can customize configuration parameters for the algorithm under wincli-command-centric within algorithms.conf (/opt/exabeam/ds-server/config/custom/algorithms.conf). Refer to algorithms_default.conf (/opt/exabeam/ds-server/config/default/algorithms_default.conf) for default settings.

- TrainingPeriod = 40 - data from trainingPeriod to eventTime will be taken to train the algorithm
- BinThresholds - bins with size above the threshold are ignored. By default:

```
BinThresholds {
  flag = 100
  directory = 100
  parent = 100
}
```

- Commands = ["at.exe", "bcdedit.exe", "cscript.exe", "csvde.exe"...] - list of the CLI commands that the algorithm will monitor
- CmdFlagsRegex = \s(--|-|/)[a-zA-Z0-9-]+ - regular expressions used to extract flags from the command
- HistoricStatsCollection = "command_centric_historic_stats" - collection in ds_wincli_db which will retain statistics for Martini rule behaviour

Verify Intermediate Results

To verify the intermediate results, you can look for data in ds_wincli_db collections:

command_centric_historic_stats
command_centric_daily_stats

Support Information

This feature is supported in single and multi-node environments on the EX4000 but not on the EX2000 single-node environment.
4.5.7. DETECT PHISHING

NOTE
To configure this feature, please contact your Technical Account Manager.

Advanced Analytics now detects users who visit suspected phishing websites. Phishing often starts with a domain name string that has the look-and-feel of a legitimate domain, but is not. Phishers target the Internet’s most recognizable domain names (google.com, yahoo.com, etc.) and make slight changes on these domain names in order to fool unassuming eyes. Phishing detection uses lexical analysis to identify whether a domain is a variant of popular domain names. In addition, it also checks URLs against a white-list of popular legitimate domains and a blacklist of identified suspicious domains. It also uses substring searches to identify domains that contain the domain name of a popular site as a substring within the suspect domain. For example, www.gmail.com-hack.net contains the recognizable "gmail.com" within the top level domain.

Associated Rules:

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WA-Phishing</td>
<td>Web activity to a phishing domain</td>
<td>Web activity to a suspected phishing domain has been detected. The domain is suspected as Phishing based on Exabeam data science algorithms.</td>
</tr>
</tbody>
</table>

Configuration

Configuration should be made in /opt/exabeam/config/custom/custom_exabeam_config.conf.

To enable Phishing Detection, set PhishingDetector.Enabled = true.

Support Information

Supported in single and multi-node environments with EX2000 and EX4000.

4.5.8. RESTART THE ANALYTICS ENGINE

Administrators typically need to restart the Analytics Engine when configuration changes are made to the system such as adding new log feeds to be analyzed by Exabeam or changing risk scores to an existing rule.

Exabeam will store time-based records in the database for recovery and granular reprocessing. The histograms and the processing state of the Exabeam Analytics Engine are time-stamped by week and stored in the database. This allows the Exabeam Analytics Engine to be able to go back to any week in the past and continue processing.

To illustrate, let's say that the Exabeam Analytics Engine started processing logs from January 1, 2016, and is currently processing today, April 15, 2016. The administrator would like to ingest new Cloud application log feeds into Exabeam and start reprocessing from a time in the past, say March 30, 2016. The administrator would stop the Exabeam Analytics Engine and then restart processing from March 30, 2016. The system will go back to find the weekly boundary where the state of the nodes and the models...
are consistent - which might mean a few days before March 30, 2016 - and start processing all the configured log feeds from that point in time.

Navigate to **Settings > Admin Operations > Exabeam Engine**.

Upon clicking **Restart Processing**, the **Processing Feeds** page appears. You can choose to:

- Restart the engine from where it left off.
- Restart and reprocess all the configured log feeds from the initial training period
- Restart from a specific date. The Analytics Engine will choose the nearest snapshot available for the date chosen and reprocess from this date.

**NOTE**

Reprocessing can take a considerable amount of time depending on the volume of data that needs to be reprocessed.

**CAUTION**

Upon clicking **Process**, a success page loads. If you are reconfiguring a secondary appliance, DO NOT click **Start Exabeam Engine** on the success page. Rather, please contact your administrator.

**NOTE**

If a Log Ingestion Engine restart is required when you attempt to restart the Analytics Engine, you will be prompted with a dialog box to also restart the Log Ingestion Engine. Advanced Analytics will intelligently handle the coordination between the two Engines. The Log Ingestion Engine will restart from the same time period as the Analytics Engine. You can choose to cancel the restart if you would like the Log Ingestion Engine to finish its current process, but this will also cancel the Analytics Engine restart procedure.

If you have made configuration changes then the system will check for any inadvertent errors in the configuration files before performing the restart. If the **custom configuration validation** does identify errors in the config files then it will list the errors and not perform the restart. Otherwise, it will restart the analytics engine as usual.

**4.5.9. CUSTOM CONFIGURATION VALIDATION**

**Hardware and Virtual Deployments Only**

Any edits you make to your Exabeam custom configuration files are validated before you are able to restart the analytics engine to apply them to your system. This helps prevent Advanced Analytics system failures due to inadvertent errors introduced to the config files.

The system validates Human-Optimized Configuration Object Notation (HOCON) syntax, for example, missing a quotes or wrong caps ("SCOREMANAGER" instead of "ScoreManager"). The validation also checks for dependencies such as extended rules in custom config files that are missing dependencies within default config files. Some additional supported validation examples are:

- Value validity and ranges
• Operators
• Brackets
• Date formats
• Rule expressions
• Model dependencies

If found, errors are listed by file name during the analytics engine restart attempt.

From here you can fix the configuration errors, Cancel the modal, and retry the restart.

Only the config files related to Advanced Analytics are validated:

• custom_exabeam_config.conf (includes default config)
• cluster.conf
• custom_lime_config.conf
• event_builder.conf
• models.conf
• parsers.conf (includes both default and custom)
• rule_labels.json
• rules.conf
• custom_event_categories.conf

In addition to helping you troubleshoot your custom config edits, Advanced Analytics also saves the last known working config files. Every time the system successfully restarts, a backup is made and stored for you.

The backups are collected and zipped in /opt/exabeam/config/backup under custom_configuration_backups_martini. All zipped files are named as follows custom_config_backup_<date>_<time> with time in UTC server time. The last ten backups are stored, and the oldest copy is deleted to make room for a new backup.

You may choose to Roll Back to the latest backup if you run into configuration errors that you are unable to fix. If you do so the latest backup is restored and the analytics engine is not restarted.

4.5.10. ADVANCED ANALYTICS TRANSACTION LOG AND CONFIGURATION BACKUP AND RESTORE
Hardware and Virtual Deployments Only

Rebuilding a failed worker node host (from a failed disk for on-premise appliance) or shifting a worker node host to new resources (such as in AWS) takes significant planning. One of the more complex steps and most prone to error is migrating the configurations. Exabeam has provide a backup mechanism for layered data format (LDF) transaction log and configuration files to minimize the risk of error. To use the configuration backup and restore feature, you must have:

• Amazon Web Services S3 storage or an active Advanced Analytics worker node
• Cluster with two or more worker nodes
• Have read and write permission for the credentials you will configure to access the base path at the storage destination
• A scheduled task in Advanced Analytics to run backup to the storage destination

**NOTE**
To rebuild after a cluster failure, it is recommended that a cloud-based backups be used. To rebuild nodes from disk failures, backup files to a worker node or cloud-based destination.

**WARNING**
Master nodes cannot be backed up and restored. Only worker nodes.

### 4.5.10.1. Set Up Backup Storage
If you want to save the generate backup files to your first worker node, then no further configuration is needed to configure an external storage destination. A worker node destination addresses possible disk failure at the master node appliance. This is not recommended as the sole method for disaster recovery.

If you are storing your configurations at an AWS S3 location, you will need to define the target location before scheduling a backup.

1. Go to **Settings > Additional Settings > Admin Operations > External Storage**.
2. Click **Add** to register an AWS backup destination.
3. Fill all field and then click **TEST CONNECTION** to verify connection credentials.
4. Once a working connection is confirmed **Successful**, click **SAVE**.

### 4.5.10.2. Schedule Up a Configuration Back
Once you have a verified destination to store your files, configure and schedule a recurring backup.

1. Go to **Settings > Additional Settings > Backup & Restore > Backups**.
2. Click **CREATE BACKUP** to generate a new schedule record. If you are changing the destination, click the edit icon on the displayed record.
3. Fill all fields and then click **SAVE** to apply the configuration.

**WARNING**
Time is given in UTC.

A successful backup will place a `backup.exa` file at either the base path of the AWS destination or `/opt/exabeam/data/backup` at the worker node. In the case that the scheduled backup fails to write files to the destination, confirm there is enough space at the destination to hold the files and that the `exabeam-web-common` service is running. (If `exabeam-web-common` is not running, review its `application.log` for hints as to the possible cause.)
4.5.10.3. Restore a Host from Configuration Backup

In order to restore a node host using files store off-node, you must have:

- administrator privileges to run tasks at the host
- SSH access to the host
- free space at the restoration partition at the master node host that is greater than 10 times the size of backup.exa backup file

1. Copy the backup file, backup.exa, from the backup location to the restoration partition. This should be a temporary work directory (<restore_path>) at the master node.

2. Run the following to unpack the EXA file and repopulate files.

```
sudo /opt/exabeam/bin/tools/exa-restore <restore_path>/backup.exa
```

`exa-restore` will stop all services, restore files, and then start all services. Monitor the console output for error messages. See Troubleshooting a Restoration if `exa-restore` is unable to run to completion.

3. Remove `backup.exa` and the temporary work directory when restoration is completed.

**Troubleshooting a Restoration**

If restoration does not succeed, the try following below solutions. If the scenarios listed do not match your situation,

**Not Enough Disk Space**

Select a different partition to restore the configuration files to and try to restore again. Otherwise, review files stored in to target destination and offload files to create more space.

**Restore Script Cannot Stop All Services**

Use the following to manually stop all services:

```
sudo /opt/exabeam/bin/shell-environment.bash & & everything-stop
```

**Restore Script Cannot Start All Services**

Use the following to manually start all services:

```
sudo /opt/exabeam/bin/shell-environment.bash & & everything-start
```

**Restore Script Could Not Restore a Particular File**

Use `tar` to manually restore the file:

```
# Determine the task ID and base directory (<base_dir>) for the file restoration that failed.
# Go to the <base_id>/<task_id> directory and apply following command:
sudo tar -xzpvf backup.tar backup.tgz -C <baseDir>

# Manually start all services.
sudo /opt/exabeam/bin/shell-environment.bash & & everything-start
```
4.5.11. REPROCESS JOBS
Access the Reprocessing Jobs tab to view the status of jobs (for example, completed, in-progress, pending, and canceled), view specific changes and other details regarding a job, and cancel a pending or in-progress job.

If you wish to cancel a reprocessing job for any reason, select the job in the Reprocessing Jobs table and then click Cancel Job.

4.5.11.1. Configure Notifications About Reprocessing Job Status Changes
You can configure email and Syslog notifications for certain reprocessing job status changes, including start, end, and failure.

To configure notifications for reprocessing job status changes:

1. Navigate to Settings > Log Management > Incident Notification.
2. Select an existing notification or create a new notification. You can choose either Syslog or email.
3. Select the reprocessing jobs notifications according to your business needs (Job status changes and/or Job failures).
4. Save your changes.

4.5.12. 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.
   ```bash
   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.
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.
   ```bash
   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**.
   ```bash
   Do you want to update your DNS server(s)? [y/n] **n**  
   Do you want to update your NTP server? [y/n] **n**
   

### 4.5.13. HADOOP DISTRIBUTED FILE SYSTEM (HDFS) NAMENODE STORAGE REDUNDANCY

There is a safeguard in place for the HDFS NameNode (master node), storage to prevent data loss in the case of data corruption. Redundancy is automatically set up for you when you install or upgrade Advanced Analytics and include at least three nodes.

**NOTE**

Deployments may take longer if redundancy is enabled.
These nodes can include the common LIME and master node in the EX2003 appliance (excluding single-node deployments), or the standalone/dedicated LIME and Master Node in the EX4003. The Incident Responder node does not factor into the node count.

Redundancy requires two NameNodes that are both operating at all times. The second NameNode is always on the next available Advanced Analytics host, which in most cases is the first worker node. It constantly replicates the primary NameNode.

With this feature enabled in the case of the Master NameNode failing the system can still move forward without data loss. In such cases, you can use this redundancy to fix the state of Hadoop (such as installing a new SSD if there was an SSD failure) and successfully restart it.

![NOTE]

Disaster recovery deployments mirror the NameNode duplicated environment.

4.5.14. 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


![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

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

2. Add the following code snippet to the file:

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

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

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

### 4.6. Set Up Rules Administration

Administrators are able to create and modify rules from within the Advanced Analytics UI in order to meet their needs. From the Rules Administration page, Administrators can:

- View all the rules configured in the system, arranged categorically.
- Change the risk scores for a rule.
- Edit an existing Exabeam Rule. This will overwrite Exabeam's original rule of the same name with the option to 'Revert to Default', which negates any changes made.
- Create a new fact-based rule.
- Clone any existing Exabeam Rule. After cloning, an administrator can edit the cloned rule and save. Cloning preserves the original rule.
- Disable any rule.
- Reload the rules. New rules or changes made to existing rules will not take effect until the rules are reloaded.

**NOTE**

Modified or newly added rules that need to be reloaded are highlighted with an orange triangle.

**All Rules**: A comprehensive list of all rules existing in Advanced Analytics's system.

**Exabeam Rules**: These are all of the out-of-the-box Exabeam rules.

**Custom Rules**: All rules that have been created, cloned, or edited and saved by an administrator.

**Disabled Rules**: All the rules that have been disabled and are not being triggered.

Expanding a category will list all the rules in that category and offer more details about each rule.
• The icon to the left of the rule indicates that the rule has been edited by an administrator.
• The Rule Name and Description are displayed.
• The Trigger Frequency is a measure of how often the rule has been flagged in User Sessions.
• The Risk Level indicates the number of points that are allocated to a User Session when the rule is triggered.

Selecting the vertical ellipsis to the right offers four options:
• Disable - Disables the rule. The rule will not trigger. This option will read 'Enable' for a rule that has already been disabled.
• Advanced Editor - Launches the JSON style Advanced Editor.
• Clone - This option makes a copy of the rule. You can save the copy under a new name and edit the new rule in the Advanced Editor.
• Revert to Default - This option only appears for rules that have been edited by an administrator. Selecting this option clears all changes that have been made to the rule and restore it to the default settings.

4.6.1. WHAT IS AN EXABEAM RULE?
So what exactly is a rule anyway? There are two types of Exabeam rules:

• Model-based
• Fact-based

Model-based rules rely on a model to determine if the rule should be applied to an event in a session, while fact based rules do not.

For example, a Fireye malware alert is fact based and does not require a model in order to be triggered. On the other hand, a rule such as an abnormal volume of data moved to USB is a Model-based rule.

Model-based rules rely on the information modeled in a histogram to determine anomalous activities. A rule is triggered if an event is concluded to be anomalous, and points are allocated towards the user session in which the event occurred. Each individual rule determines the criticality of the event and allocates the relevant number of points to the session associated with that event.

Taken together, the sum of scores from the applied rules is the score for the session. An example of a high-scoring event is the first login to a critical system by a specific user – which allocates a score of 40 to a user's session. Confidence in the model must be above a certain percentage for the information to be used by a rule. This percentage is set in each rule, though most use 80%. When there is enough reliable information for the confidence to be 80% or higher, this is called convergence. If convergence is not reached, the rule cannot be triggered for the event.

4.6.2. HOW EXABEAM MODELS WORK
Since anomaly-based rules depend on models, it is helpful to have a basic understanding of how Exabeam's models work.

Our anomaly detection relies on statistical profiling of network entity behavior. Our statistical profiling is not only about user-level data. In fact, Exabeam profiles all network entities, including hosts and
machines, and this extends to applications or processes, as data permits. The statistical profiling is histogram frequency based. To perform the histogram-based profiling, which requires discrete input, we incorporate a variety of methods to transform and to condition the data. Probability distributions are modeled using histograms, which are graphical representations of data. There are three different model types – categorical, numerical clustered, and numerical time-of-week.

**Categorical** is the most common. It models a string with significance: number, host name, username, etc. Where numbers fall into specific categories which cannot be quantified. When you model which host a user logs into, it is a categorical model.

**Numerical Clustered** involves numbers that have meaning – it builds clusters around a user’s common activities so you can easily see when the user deviates from this norm. For example, you can model how many hosts a user normally accesses in a session.

**Numerical Time-of-Week** models when users log into their machines in a 24-hour period. It models time as a cycle so that the beginning and end of the period are close together, rather than far apart. For example, if a user logs into a machine Sunday at 11:00 pm, it is closely modeled to Monday at 12:00am.

4.6.3. **MODEL AGING**
Over time, models built in your deployment naturally become outdated. For example, if an employee moves to a different department or accepts a promotion and they do not adhere to the same routines, access points, or other historical regularities.

We automatically clean up and rebuild all models on a regular basis (default is every 16 weeks) to ensure your models are as accurate and up-to-date as possible. This process also enhances system performance by cleaning out unused or underutilized models.

4.6.4. **RULE NAMING CONVENTION**
Exabeam has an internal Rule ID naming convention that is outlined below. This system is used for Exabeam created rules and models only. When a rule is created or cloned by a customer, the system will automatically create a Rule ID for the new rule that consists of `customer-created`, followed by a random hash. For example, a new rule could be called, `customer-created-4Ef3DDYqsQ`.

The Exabeam convention for model and rule names is: **ET-SF-A/F-Z**

- **ET**: The event types that the model or rule addresses. For example,
  - RA = remote-access
  - NKL = NTLM/Kerberos-logon
  - RL = remote-logon

- **SF**: Scope and Feature of the model. For example,
  - HU = Scope=Host, Feature=User
  - OZ = Scope=Organization, Feature=Zone

- **A/F**: For rules only
• A = Abnormal
• F = First

Z : Additional Information (Optional). For example,

• DC: Domain Controller models/rules
• CS: Critical Systems

4.6.5. REPROCESS RULES
When adding new or managing existing Exabeam rule on the Exabeam Rules page, you can choose to reload individual or all rules. You can choose to reload and apply rule changes from the current point in time, or and reprocess historic data. When applying and reprocessing rule changes to historic data, the reprocess is done in parallel with active, live processing. It does not impede or stop any real-time analysis.

You can view the status of pending, in-progress, completed, canceled, and failed jobs at any time by navigating to Settings > Admin Operations > Exabeam Engine > Reprocessing Jobs. For more information on reprocessing, please see the section Reprocess Jobs.

4.6.6. CREATE FACT BASED RULES USING THE SIMPLE EDITOR
The Simple Editor allows an administrator to create fact based rules. A fact based rule is one that does not rely on a model in order to trigger. See Exabeam Rules and the How Exabeam Models Work sections in this document for more information on the difference between fact based and model based rules.

Access the Simple Editor by navigating to Settings > Admin Operations > Exabeam Rules and clicking the + button.

After an administrator creates a rule, the rule is validated during the save operation.

Rule Category – Defines which category the rule falls under. For example, VPN Activity, Critical System Activity, etc.

Name – When the rule is triggered, this is the name displayed in the Advanced Analytics UI during the user session. We recommend using descriptive rule names to indicate the nature of the risky behavior; for example, Data Exfiltration by a Flight Risk User.

Description – The rule description provides additional details to help analysts investigate. Defining the why of the rule as well as the what helps analysts interpret the results of User Sessions more easily.

Events – Select the event types that the rule will depend on. For example, if your rule is evaluating user logins then the log types should reflect all the different login events that you want analyzed.

Risk Level – The risk level reflects the risk score that will be added to a User Session if the rule is triggered.

Rule Expression – This is the boolean expression that the rule engine uses to determine if a particular rule will trigger. This means that your rule will only trigger if all of the conditions described in the Rule Expression are met.
**Rule Dependency** – This is the only field in the Simple Editor that is optional. The Rule Dependency defines another rule (identified by the Rule ID) that your rule is dependent upon. When Rule A depends on Rule E, then Rule A will only trigger if Rule E is evaluated to true.

### 4.6.6.1. Example of Using the Simple Editor

We want to create a new fact-based rule: add 15 extra risk points to the sessions of users HR considers to be a flight risk. We have already added a context file titled ‘Flight Risk’ that contains the IDs of those users. We want our rule to trigger every time a User with the user label ‘Flight Risk’ starts a session.

We want the name and description of our rule to reflect its purpose.

**Name** – Flight Risks

**Description** – Users that HR considers to be flight risks.

We then want to select all of the events that this rule will analyze and how many points are added to a user session if this rule triggers.

**Event Types** – remote-access, remote-logon, local-logon, kerberos-logon, ntlm-logon, account-switch, app-logon, app-activity, privileged-object-access

**Risk Level** – Critical (15)

We then want to build a **Rule Expression** - this is the boolean expression that the rule engine uses to determine if a particular rule will trigger. This means that your rule will only trigger if all of the conditions described in the Rule Expression are met.

Our Field is **User** and the property of the user field that we want is **User Label**. In this case, a rule has to be triggered when the value of the user label is **Flight Risk**. Note that the label in the context lookup table for the Flight Risk users should match this value.

Click **Done with Expression** and we’ve created a rule expression for a rule that will trigger whenever the term Flight Risk is found in the user_label field.

Returning back to the **Create a Rule** page, we want our rule to trigger once per session and it does not depend on another rule triggering.

Click **Save & Reload All**. This saves the rule and reloads the rule file; rules need to be reloaded into the Exabeam Engine to have the changes be effective.

### 4.6.7. EDIT RULES USING THE ADVANCED EDITOR

The Advanced Editor is a JSON style editor and is what an administrator would use if they wanted to edit one of Exabeam’s existing rules, or edit a cloned rule. All of Exabeam's out-of-the-box rules can be edited only via the Advanced Editor.
NOTE
Be careful here, these settings are for very advanced users only. Changes you make here can have a significant impact on the Exabeam Analytics Engine. The Advanced Editor allows administrators and advanced analysts to make changes to Exabeam rules in a JSON style configuration format. This should be used by administrators that have the expertise to create or tweak a machine learning rule and understand the syntax language for expressing a rule. In case of questions, reach out to Exabeam Customer Success for guidance.

This editor shows the entire rule as it exists in the configuration file. The Rule ID is the only field that cannot be changed. See the Rule Naming Convention section in this document for more information about Exabeam’s naming convention. When an administrator makes any changes to a rule, the rule is validated during the save operation. If the rule has incorrect syntax, the administrator is prompted with the error and the details of the error. Once a rule is edited and saved using the Advanced Editor, the rule cannot be viewed via the Simple Editor.

4.6.7.1. Fields in the Advanced Editor

ClassifyIf
This expression is similar to the TrainIf field in the model template. It evaluates to true if classification needs to be performed for a given event. In other words, how many times this rule should trigger.

DependencyExpression
This field defines a Boolean expression of other rule IDs. When rule A depends on expression E, A will only trigger if its parameters satisfy the RuleExpression, and E is evaluated to true after the rule IDs are substituted with their rule evaluation result. When an administrator makes any changes to a rule, the rule is validated during the save operation. If the rule is not syntactically well formed, the administrator is prompted with the error and the details of the error.

Disabled
This field will read either True or False. Set to True to deactivate the rule and all associated modelling.

FactFeatureName
The name of a feature used for fact based rules. For model-based rules the FactFeatureName is defined in the associated model.

Model
The name of the model that this rule references. If this rule is fact-based, then the model name is FACT.

PercentileThreshold
This value indicates which observations are considered anomalous based on the histogram. For example, a value of 0.1 indicates a percentile threshold of 10%. This goes back to the histogram and means that for the purposes of this rule we only consider events that appear below the 10th percentile to be abnormal. Note that many rules distinguish between the first time an event occurs and when that event has happened before, but is still abnormal. These two occurrences often appear as two separate rules because we want to assign two different scores to them.
ReasonTemplate

This appears in the UI and is to facilitate cross-examination by users. The items between braces represent type and value for an element to be displayed. The type helps define what happens when the user clicks on the hyperlink in the UI.

Rule ID

Unique identifier for this rule. The name in our example is NKL-UH-F. Exabeam has a naming convention for both models and rules that is outlined in the section titled *Naming Convention*. When editing or cloning an existing rule you cannot change the Rule ID.

RuleDescription

This is used in the UI to describe the reason why a particular rule triggered.

RuleEventTypes

This collection defines what events we are considering in this rule. It can be the same events that the model considers, but does not have to be. Sometimes you may want to model on one parameter but trigger on another.

RuleExpression

This is the boolean expression that the rule engine uses to determine if a particular rule will trigger. Your rule will only trigger if all of the conditions described in the Rule Expression are met. You can use probability or number of observations (num_observations) to determine how many times this event has been seen before. When either is set to zero it is a way to see when something happens that has not happened before. The confidence_factor refers to a concept called convergence. In order for the rule to use the information gathered by the model, we must be confident in that information. A percentage is set in each Confidence in the model must be above a certain percentage for the information to be used by a rule. This percentage is set in each rule, though most use 80%. When there is enough reliable information for the confidence to be 80% or higher, this is called convergence. If convergence is not reached, the rule cannot be triggered for the event.

RuleName

Descriptive name for the rule. Used for documentation purposes.

RuleType

This appears in the UI and is to facilitate cross-examination by users. The items between braces represent type and value for an element to be displayed. The type helps define what happens when the user clicks on the hyperlink in the UI.

Score

This is the score that will be assigned to a session when this rule triggers. Higher scores mean a higher level of risk from the security perspective.

4.7. Exabeam Threat Intelligence Service

The Exabeam Threat Intelligence Service delivers a constant stream of up-to-date threat indicators to Advanced Analytics deployments.

The categories of indicators affected are the following:
• IP addresses associated with Ransomware or Malware attacks

• IP addresses associated with the TOR network

• Domain names associated with Ransomware, Phishing, or Malware attacks

Indicators are downloaded by the on premise products from Threat Intelligence Service on a daily basis.

![Figure 2. Exabeam Threat Intelligence Service Architecture](Image)

Advanced Analytics and Data Lake connect to Threat Intelligence Service through a cloud connector service that provides authentication and establishes a secure connection to Threat Intelligence Service. The cloud connector service then collects updated threat indicators from Threat Intelligence Service daily.

These indicators are then made available within Advanced Analytics to provide enhanced risk scoring based on curated threat intelligence.

This product does not require a separate license. It is bundled with Advanced Analytics deployments. Additional installation or configuration is not required.

If you would like to learn more, contact your technical account manager or watch product videos via the Exabeam Community.

**4.7.1. THREAT INTELLIGENCE SERVICE PREREQUISITES**

Before configuring Threat Intelligence Service, ensure your deployment meets the following prerequisites:

• At least 5 Mbps Internet connection

• Access to https://api.cloud.exabeam.com over HTTPS port 443
NOTE
Ensure dynamic access is enabled as the IP address may change. Also, for this reason, firewall rules for static IP and port addresses are not supported.

- DNS resolution for Internet hostnames (this will only be used to resolve to https://api.cloud.exabeam.com)

4.7.2. CONNECT TO THREAT INTELLIGENCE SERVICE THROUGH A PROXY
The communication between Threat Intelligence Service and Advanced Analytics occurs over a secure HTTPS connection.

If connections from your organization do not make use of a web proxy server, you may skip this section. Threat Intelligence Service is available automatically and does not require additional configuration.

If connections from your organization are required to go through a web proxy server to access the Internet, you will need to provide the configuration as shown below.

NOTE
Configuration is required for each of your Advanced Analytics Data Lake deployments.

WARNING
If your proxy performs SSL interception, it will replace the SSL certificate from the Exabeam Threat Intel Service (ETIS) with an unknown certificate during the SSL negotiation, which will cause the connection to ETIS to fail. If possible, please disable SSL Interception for the IP address of your Exabeam products. If this cannot be disabled, please contact Exabeam Customer Success for further assistance.

Before configuring Threat Intelligence Service, ensure your deployment meets the following prerequisites:

- At least 5 Mbps Internet connection
- Access to https://api.cloud.exabeam.com over HTTPS port 443

NOTE
Ensure dynamic access is enabled as the IP address may change. Also, for this reason, firewall rules for static IP and port addresses are not supported.

- DNS resolution for Internet hostnames (this will only be used to resolve to https://api.cloud.exabeam.com)

1. Establish a CLI session with the master node of your Exabeam deployment.
2. Open the custom file

   /opt/exabeam/config/common/cloud-connection-service/custom/application.conf
3. Add the following section to the custom file and configure the parameters `proxyHost`, `proxyPort`, `proxyUsername`, and `proxyPassword`.

```
# HTTP client proxy settings
proxyHost = "proxy-host"
proxyPort = 8080
proxyUsername = "user"
proxyPassword = "pass"
```

```
# HTTPS client proxy settings
proxyHost = "proxy-host"
proxyPort = 8080
proxyProtocol = "https"
```

**NOTE**

Be sure to choose the appropriate settings based on whether the proxy utilizes http or https. Additionally, always use quoted strings for `proxyHost`, `proxyProtocol`, `proxyUsername`, and `proxyPassword`.

4. Stop and then restart the cloud connector service in your product:
   a. `source /opt/exabeam/bin/shell-environment.bash`
   b. `cloud-connection-service-stop`
   c. `cloud-connection-service-start`

**NOTE**

**Important Note:** The username and password values are hashed in Data Lake i24 and later. After Cloud Connection Service (CCS) is restarted (step 4), the username and password are hashed using a 128 bit AES key, and these hashed values are stored in the local secrets store. In the config file, the username and password values are replaced by the hashed values.

If you want to subsequently change the values again, you can do so by replacing the hashed values by new plain text values and restart the CCS service.

As soon as the deployment can successfully connect to Threat Intelligence Service, threat intelligence feed data is pulled and saved as context tables and is also viewable on the Threat Intelligence Feeds settings page.

**4.7.3. VIEW AND MANAGE THREAT INTELLIGENCE FEEDS**

To view threat intelligence feeds, navigate to Settings > Cloud Config > Threat Intelligence Feeds.
The page displays details related to all threat intelligence feeds provided by the cloud-based Exabeam Threat Intelligence service, such as:

- The type of the feed (for example, domain list, IP list, etc.)
- The name of the feed (as given by the cloud-based service)
- A short description of the feed
- The status indicating the availability of the feeds in the cloud-based service
- The time of last update from the cloud service

NOTE
Data provided by the threat intelligence feeds can be accessed in Context tables (see section on Viewing Threat Intelligence Service Context Tables). The initial service feeds are associated with existing context tables by default. This means that as soon as your deployment is connected to the cloud-based Threat Intelligence Service service, your deployment will start collecting threat intelligence data.

If you want to collect data from some of the threads in other context tables, see the next section on Assigning a Threat Intelligence Feed to a New Context Table.

- Associated context tables
4.7.4. ASSIGN THREAT INTELLIGENCE FEED TO A NEW CONTEXT TABLE
Some of the feeds are pre-assigned to context tables. Click the arrow of a threat intelligence feed to expand and view additional details, including:

- ID
- Source URL
- Indicator in Context Tables
- Retrieved from Source
- Feed Indicator Sample
- Context Table(s)

Click the edit icon of a single threat intelligence feed to assign or unassign it to one or more context tables.

NOTE
You cannot unassign default context table mappings.

Click the view icon to view existing indicators in the context table.
Select multiple threat intelligence feeds to bulk assign or unassign them from context tables.

4.7.5. CREATE A NEW CONTEXT TABLE FROM A THREAT INTELLIGENCE FEED

To create a new context table from one or more threat intelligence feeds:

1. Navigate to Settings > Cloud Config > Threat Intelligence Feeds.
2. Edit a threat intelligence feed.
   a. To create a new context table from a single feed, click the edit icon of the single feed.
   b. To create a new context table from multiple feeds, select the feeds and then click Assign.
3. Click **Add Context Table**.

4. Configure the context table fields, including title, object type (users assets, miscellaneous), and type (key value or key only).

5. Click **ADD**.
4.7.6. VIEW THREAT INTELLIGENCE SERVICE CONTEXT TABLES
To view the current context tables provided by Threat Intelligence Service:

1. Log in to your instance of the UI.
3. Select one of the context tables listed above. For example, web_phishing (shown below).
4. On the context table details page, view the keys and values currently associated with the context table.
4.7.7. CHECK EXACLOUD CONNECTOR SERVICE HEALTH STATUS

To view the current status of the ExaCloud connector service:

1. Log in to your instance of the UI.
2. Click the top-right menu icon and select **System Health**.
3. Select the **Health Checks** tab.
4. Click **Run Checks**.
5. Expand the **Service Availability** section, and then review the **ExaCloud connection service availability** icon.
The service availability icon shows the current health of the Cloud connector service that is deployed on your Exabeam product.

- **Green** – The cloud connector service is healthy and running on your on-prem deployment.

**NOTE**
The green icon does not specifically indicate the cloud connector is connecting to the cloud and pulling Threat Intelligence Service data. It only indicates the cloud connector service is up and running.


### 4.8. 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.

#### 4.8.1. 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.

#### 4.8.2. 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"}.

**4.8.2.1. Metrics**
The example below shows the metrics data sent from the master node to the telemetry service in Exabeam Cloud:

```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, 0.4947], "name": "tm.plt.service_memory.mongodb-shard-host1"} ] }
```

**4.8.2.2. Events**
The example below shows the events data sent from the master node to the telemetry service in Exabeam Cloud:

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

**4.8.2.3. Environment**
The example below shows the environment data sent from the master node to the telemetry service in Exabeam Cloud:

```json
{ "environment": { "versions": { "uba": { "build": "4", "branch": "I46.2"}, "common": { "build": "7", "branch": "PLT-112.5"}, "exa_security": { "build": "33", "branch": "c180815.1"} }, "hosts": [ { "host": ".*.0.24", "roles": ["oar","cm"]}, { "host": ".*.0.72", "roles": ["uba_slave"]}, { "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 } }
```
4.8.3. 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.

NOTE
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.

<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>

### 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>
</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_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>
<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>

### 4.8.4. 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

#### 4.8.4.1. 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.

4.8.4.2. 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:

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

4. Restart CCS by running the following command:

   ```
   . /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.

4.8.4.3. 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:

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

2. Add a new line:

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

3. Restart CCS by running the following command:

   ```
   . /opt/exabeam/bin/shell-environment.bash
   cloud-connection-service-stop && cloud-connection-service-start
   ```
4.9. Disaster Recovery (Advanced Analytics, Case Manager, and Incident Responder)
Hardware and Virtual Deployments Only

In a disaster recovery scenario, Advanced Analytics content is replicated continuously from the active site to the passive site, including:

- **Logs/Events** – The active cluster fetches logs from SIEM and/or receiving the logs via Syslog. Once the logs are parsed, the events are replicated to the passive cluster.

- **Configuration** – Changes to configuration such as configuring new log feeds, parsers, LDAP server, roles and Exabeam users, models and rules are replicated from the active to the standby cluster. This includes files as well as the relevant database collections (for example, EDS configuration, users and roles are in database).

- **Context** – Contextual data such as users, assets, service accounts, peer groups, etc.

- **User Generated Data** – Comments, approved sessions, Watchlists, starred sessions, saved searches, and whitelists stored in the Mongo database.

**NOTE**
You can also configure your Advanced Analytics deployment to replicate only specific file types across clusters.

If you have Case Manager or a combined Case Manager and Incident Responder license, the disaster recovery system replicates:

- Incidents and incident details (entities, artifacts, comments, etc.)
- Custom incident filters and searches.
- Roles and permissions.
- Playbooks and actions (including history and saved results of previous actions)
- Configurations (for example, alert sources, alert feeds, notification settings, incident message and email settings), phases and tasks, integrated services (for example, parsers and alert rules).

4.9.1. DEPLOY DISASTER RECOVERY
Hardware and Virtual Deployments Only

**WARNING**
You can only perform this configuration with the assistance of Exabeam Customer Success Engineer.

The two-cluster scenario employs an Active-Passive Disaster Recovery architecture with asynchronous replication.

With this approach, you maintain an active and secondary set of Advanced Analytics (and additional Case Manager and Incident Responder) clusters in separate locations. In cases of a failure at the active site, you can fail over to the passive site.

At a high level, when Disaster Recovery is set up between two Advanced Analytics clusters, the active cluster is responsible for fetching the logs from SIEM or receiving the logs via Syslog. Once the logs have
been parsed into events, the events are replicated from the active cluster to the passive cluster every five minutes.

Optionally, the raw logs can be replicated from the active to the passive cluster. (This allows reprocessing of logs, if needed. However, replication will generate great bandwidth demands between nodes.) If the active cluster goes down, then the passive cluster becomes the active until such time as the downed site is recovered.

**4.9.1.1. Prerequisites**

- Open port TCP 10022 (bi-directional)
- IP addresses of both the primary and secondary clusters
- SSH key to access the primary cluster
- At least 200 megabits per second connection between primary and secondary clusters
The active and passive clusters must have the exact same number of nodes in the same formation. For example, if the second and third nodes on the primary cluster are worker nodes, the second and third nodes on the passive cluster must also be worker nodes. If the fifth node on the primary cluster is a Case Manager node, the fifth cluster on the passive cluster must also be a Case Manager node.

### 4.9.1.2. Deployment

This process requires you to setup disaster recovery first on the active cluster (primary node) and then on the passive cluster (secondary site).

**NOTE**

If you have already set up disaster recovery for Advanced Analytics and are adding disaster recovery for Incident Responder, please see *Adding Case Manager & Incident Responder Disaster Recovery to Existing Advanced Analytics Disaster Recovery*.

### Active Cluster Setup

On the active site, run the following:

```
screen -LS dr_setup
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

Select option: "Configure disaster recovery".

Select the option: "This cluster is source cluster (usually the primary)"

Please select the type of cluster:

1. This cluster is source cluster (usually the primary)
2. This cluster is destination cluster (usually the dr node)
3. This cluster is for file replication (configuration change needed)

Please wait for the cluster setup to successfully complete before proceeding to the next section.

### Passive Cluster Setup

Copy onto the passive cluster master the SSH key that allows access to the active cluster. (Skip this step if you have a pre-existing key that allows you to SSH from passive to the active cluster.)

On the passive site (standby master), run the following:

```
screen -LS dr_setup
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

Select option: "Configure disaster recovery".

Select the option: "This cluster is destination cluster (usually the dr node)"

Please select the type of cluster:

1. This cluster is source cluster (usually the primary)
2. This cluster is destination cluster (usually the dr node)
3. This cluster is for file replication (configuration change needed)

Input the IP address of the active cluster.
What is the IP of the source cluster?

Select the option "SSH key".

The source cluster's SSH key will replace the one for this cluster. How do you want to pull the source cluster SSH key?
1) password
2) SSH key

Input the private key file path.

What is the path to the private key file?

The passive cluster will connect to the active cluster with the private key provided. If there is no SSH key at the passive cluster, select Option 1 and follow the prompts. You will be asked for user credentials (with sufficient privileges) to either access the active cluster master to retrieve the SSH key or generate a new key.

4.9.2. FAILOVER TO PASSIVE CLUSTER
Hardware and Virtual Deployments Only
This section includes instructions on how to failover to the passive site when the previously active site goes down. It also covers how to failback when you are ready to bring the restored site back online.

Exabeam’s recommended policy for failback is to demote the failed cluster as the new passive cluster going forward. For example, Cluster A is the active cluster and Cluster B is the passive. Cluster A fails and Cluster B becomes active. When Cluster A is ready to come back online, it rejoins as a passive cluster until complete data synchronization and is then promoted to an active cluster again.

4.9.2.1. Make Passive Cluster (Secondary Site) Become Active
Log on to the passive cluster and ensure docker is running:

sos; docker ps

Stop the replicator:

replicator-socks-stop; replicator-stop

After stopping the replicator, run the deployment script:

screen -LS dr_failover
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh

Select "Promote Disaster Recovery Cluster to be Primary." This step promotes the passive cluster to be the active.

After the passive cluster is promoted to active, stop docker:

sos; everything-stop

Start docker again:

docker-start
Run the following command to start all services:

`everything-start`

If using a Syslog server, please switch the Syslog server to push logs to the new active cluster environment (secondary site).

If you have deployed Helpdesk Communications, restart two-way email service in the UI.

Start Log Ingestion and Analytics Engine from the Exabeam Engine page.

### 4.9.2.2. Make Failed Active Cluster (Primary Site) Become Passive After Recovery

⚠️ **WARNING**

Do not immediately promote the restored cluster back to active status after recovery. It must be demoted in order to synchronize data lost during its outage.

1. Log on to the existing active and ensure docker is running.

```
sos; docker ps
```

2. Run the deployment script:

```
screen -LS dr_failover
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

3. Select option "Configure Disaster Recovery."

4. Select the option: "This cluster is destination cluster (usually the dr node)"

```
Please select the type of cluster:
1) This cluster is source cluster (usually the primary)
2) This cluster is destination cluster (usually the dr node)
3) This cluster is for file replication (configuration change needed)
```

5. Input the IP address of the source cluster.

```
What is the IP of the source cluster?
```

6. Select the option "SSH key".

```
The source cluster's SSH key will replace the one for this cluster. How do you want to pull the source cluster SSH key?
1) password
2) SSH key
```

7. Input the private key file path.

```
What is the path to the private key file?
```
8. Run the following command to stop all services:
   
   sos; everything-stop

9. After the recovered cluster is demoted, start docker again:
   
   docker-start

10. Run the following command to start all services:
    
    everything-start

4.9.2.3. Failback to Passive Site (Original Primary) Cluster

Demote Active Cluster (Secondary Site) Back to Passive After Synchronization

1. Log on to the current active cluster and ensure docker is running:
   
   sos; docker ps

2. Stop the replicator:
   
   replicator-socks-stop; replicator-stop

3. After stopping the replicator, run the deployment script:
   
   screen -LS dr_failback
   /opt/exabeam_installer/init/exabeam-multinode-deployment.sh

4. Select option "Configure Disaster Recovery."

5. Set the cluster as Disaster Recovery (Non Primary) to demote the active (former standby) cluster back to standby.
   After the active (former passive) cluster is demoted to passive, stop docker:
   
   sos; everything-stop

6. After everything is done, start docker again:
   
   docker-start

7. Run the following command to start all services:
   
   everything-start

Promote Restored Cluster (Original Primary) to Active

1. Log on to the restored cluster master and ensure docker is running:
Configure Advanced Analytics

2. Run the deployment script:

```
sos; docker ps
```

3. Select "Promote Disaster Recovery Cluster to be Primary." This step promotes the recovered cluster to back to active status.

4. Run the following command to stop all services:

```
sos; everything-stop
```

5. After the restored cluster is promoted, start docker again:

```
docker-start
```

6. Run the following command to start all services:

```
sos; everything-start
```

7. If you have deployed Incident Responder, restart incident feed log ingestion in the UI.

8. Navigate to Settings > Case Manager > Incident Ingestion > Incident Feeds.

9. Click Restart Log Ingestion Engine.

10. If you have deployed Helpdesk Communications, restart two-way email service in the UI.

11. Navigate to Settings > Case Manager > Incident Ingestion > 2-Way Email.

12. Click the pencil/edit icon associated with the applicable email configuration.

13. Click Restart.

14. If using a Syslog server, please switch the Syslog server to push logs to the active cluster (primary site). Start Log Ingestion and Analytics Engine from the Exabeam Engine page.

4.9.3. REPLICATE SPECIFIC FILES ACROSS CLUSTERS

Hardware and Virtual Deployments Only

⚠️ WARNING
You can only perform this configuration with the assistance of Exabeam Customer Success Engineer.

File replication across clusters leverages Advanced Analytics and Incident Responder disaster recovery functionality, which replicates entire cluster configurations, context, user generated data, logs/events, and HDFS files (for Incident Responder).

NOTE
Advanced Analytics HDFS files are copied from oldest to newest. Incident Responder HDFS files are copied from newest to oldest.
In certain customer scenarios, clusters are situated in remote areas with considerable bandwidth restraints. In these rare scenarios, you can configure Advanced Analytics and/or Incident Responder to only replicate and fetch specific files. For example, you can configure your deployment to replicate only compressed event files across clusters.

### 4.9.3.1. Primary Site – Source Cluster Setup

On the primary site, run the following:

```
screen -LS dr_setup
/opt/exabeam_installer/init/exabeam-multinode-deployment.sh
```

Select option: "Configure disaster recovery".
Select the option: "This cluster is source cluster (usually the primary)"

Please select the type of cluster:
1) This cluster is source cluster (usually the primary)
2) This cluster is destination cluster (usually the dr node)
3) This cluster is for file replication (configuration change needed)

Wait for the deployment to successfully finish.

4.9.3.2. Secondary Site – Destination Cluster Setup

1. On the secondary site, run the following:

   screen -LS dr_setup
   /opt/exabeam_installer/init/exabeam-multinode-deployment.sh

2. Select option: "Configure disaster recovery".
3. Select the option: "This cluster is for file replication (configuration change needed)"

   Please select the type of cluster:
   1) This cluster is source cluster (usually the primary)
   2) This cluster is destination cluster (usually the dr node)
   3) This cluster is for file replication (configuration change needed)

4. Input the IP address of the source cluster.

   What is the IP of the source cluster?

5. Select the option "SSH key".

   The source cluster's SSH key will replace the one for this cluster. How do you want to pull the source cluster SSH key?
   1) password
   2) SSH key

6. Input the private key path.

   What is the path to the private key file?

7. Wait for the deployment to successfully finish.

8. Replication of the primary cluster automatically begins, but all replication items are disabled. You must manually enable the replication items.

9. On the secondary site, access the custom configuration file /opt/exabeam/config/custom/custom_replicator_disable.conf, and then enable replication items.

10. For example, if you wish to only fetch compressed event files, then set the Enabled field for the [".evt.gz"] file type to true (shown below).

    ```
    {
        EndPointType = HDFS
    }
    ```
Configure Advanced Analytics

```
Include {
    Dir = "/opt/exabeam/data/input"
    FilePattern = [".evt.gz"]
}
Enabled = true
```

11. Start the replicator.

```
sos; replicator-socks-start; replicator-start
```

12. Once the replicator is started, log on to the standby cluster GUI. Navigate to **Context Setup** and click the **Generate Context** button. This gathers context from the active cluster to synchronize the standby cluster.

### 4.9.4. ADD CASE MANAGER AND INCIDENT RESPONDER TO ADVANCED ANALYTICS DISASTER RECOVERY

#### Hardware and Virtual Deployments Only

If you are upgrading from Advanced Analytics SMP 2019.1 (i48) or lower and have configured disaster recovery for Advanced Analytics, add Case Manager and Incident Responder to the existing Advanced Analytics disaster recovery.

⚠️ **WARNING**

Configure this only with an Exabeam Customer Success Engineer.

#### 4.9.4.1. Stop the Replicator

1. Ensure that the Advanced Analytics replication is current.
2. To ensure that the passive site matches the active site, compare the files in HDFS, the local file system, and MongoDB.
3. Source the shell environment:

   ```bash
   . /opt/exabeam/bin/shell-environment.bash
   ```
4. On the active cluster, stop the replicator:

   ```bash
   sos; replicator-socks-stop; replicator-stop
   ```

#### 4.9.4.2. Upgrade the Passive and Active Advanced Analytics Clusters

⚠️ **NOTE**

Both the primary and secondary clusters must be on the same release version at all times.
**WARNING**

If you have an existing custom UI port, please set the `web_common_external_port` variable in `/opt/exabeam_installer/group_vars/all.yml`. Otherwise, you may lose access at the custom UI port after the clusters upgrade.

```
web_common_external_port: <UI_port_number>
```

1. **(Optional)** Disable Exabeam Cloud Telemetry Service.
2. If you use the SkyFormation cloud connector service, stop the service.
   a. For SkyFormation v.2.1.18 and higher, run:
      ```
sudo systemctl stop sk4compose
```
   b. For SkyFormation v.2.1.17 and lower, run:
      ```
sudo systemctl stop sk4tomcat
sudo systemctl stop sk4postgres
```

**NOTE**

After you've finished upgrading the clusters, the SkyFormation service automatically starts. 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. From Exabeam Community, download the `Exabeam_[product]_[build_version].sxb` file of the version you're upgrading to. Place it anywhere on the master node, except `/opt/exabeam_installer`, using Secure File Transfer Protocol (SFTP).
4. Change the permission of the file:
   ```
   chmod +x Exabeam_[product]_[build_version].sxb
   ```
5. Start a new terminal session using your `exabeam` credentials (do not run as ROOT).
6. To avoid accidentally terminating your session, initiate a screen session.
   ```
   screen -LS [yourname]_[todaysdate]
   ```
7. Execute the command (where `yy` is the iteration number and `zz` is the build number):
   ```
   ./Exabeam_[product]_[build_version].sxb upgrade
   ```
   The system auto-detects your existing version. If it can't, you are prompted to enter the existing version you are upgrading from.
8. When the upgrade finishes, decide whether to start the Analytics Engine and Log Ingestion Message Extraction engine:
Upgrade completed. Do you want to start exabeam-analytics now? [y/n] y
Upgrade completed. Do you want to start lime now? [y/n] y

4.9.4.3. 3. Add Case Manager to Advanced Analytics

1. SSH to the primary Advanced Analytics machine.
2. Start a new screen session:
   
   ```bash
   screen -LS new_screen
   /opt/exabeam_installer/init/exabeam-multinode-deployment.sh
   ```
3. When asked to make a selection, choose **Add product to the cluster**.
4. From these actions, choose option 4.
   1) Upgrade from existing version
   2) Deploy cluster
   3) Run precheck
   4) Add product to the cluster
   5) Add new nodes to the cluster
   6) Nuke existing services
   7) Nuke existing services and deploy
   8) Balance hadoop (run if adding nodes failed the first time)
   9) Roll back to previously backed up version
   10) Generate inventory file on disk
   11) Configure disaster recovery
   12) Promote Disaster Recovery Cluster to be Primary
   13) Install pre-approved CentOS package updates
   14) Change network settings
   15) Generate certificate signing requests
   16) Exit
   

5. Indicate how the node should be configured:

   Which product(s) do you wish to add? ['ml', 'dl', 'cm']: cm
   How many nodes do you wish to add? (minimum: 0): 1
   What is the IP address of node 1 (localhost/127.0.0.1 not allowed)? 10.10.2.40
   What are the roles of node 1? ['cm', 'uba_slave']: cm

6. To configure Elasticsearch, Kafka, DNS servers, and disaster recovery, it's best that you use these values:

   How many elasticsearch instances per host? [2] 1
   What's the replication factor for elasticsearch? 0 means no replication. [0]
   How much memory in GB for each elasticsearch instance? [16] 16
   How much memory in GB for each kafka instance? [5]
Would you like to add any DNS servers? [y/n]  n
Do you want to setup disaster recovery? [y/n]  n

7. Once the installation script successfully completes, restart the Analytics Engine.

4.9.4.4. Configure Disaster Recovery on the Advanced Analytics and Case Manager Passive Clusters

1. On the secondary site, run:

   screen -LS dr_setup
   /opt/exabeam_installer/init/exabeam-multinode-deployment.sh

2. Select option: Configure disaster recovery.

3. Select the third option: This cluster is for file replication (configuration change needed)

   Please select the type of cluster:
   1) This cluster is source cluster (usually the primary)
   2) This cluster is destination cluster (usually the dr node)
   3) This cluster is for file replication (configuration change needed)

4. Enter the IP address of the source cluster.

   What is the IP of the source cluster?

5. Select option: SSH key.

   The source cluster's SSH key will replace the one for this cluster. How do you want to pull the source cluster SSH key?
   1) password
   2) SSH key

6. Enter the private key path.

   What is the path to the private key file?

   The deployment may take some time to finish.

7. The primary cluster begins to replicate automatically, but all replication items are disabled. You must manually enable the replication items.

   On the secondary site, access the custom configuration file /opt/exabeam/config/custom/custom_replicator_disable.conf, then enable replication items.

   For example, if you wish to only fetch compressed event files, then set the Enabled field for the [.evt.gz] file type to true:

   ```
   {
   EndPointType = HDFS
   Include {
   Dir = "/opt/exabeam/data/input"
   ```
8. Start the replicator:

```bash
sos; replicator-start
```

9. Log on to the standby cluster GUI.

10. To gather context from the active cluster to synchronize the standby cluster, navigate to **LDAP Import > Generate Context**, then click **Generate Context**.

### 4.9.4.5. 5. Start the Replicator

On the active cluster, start the replicator:

```bash
replicator-socks-start; replicator-start
```

### 4.10. Enable Settings to Detect Email Sent to Personal Accounts

**Hardware and Virtual Deployments Only**

To start monitoring when someone sends company email to a personal email account, enable it in the **algorithms.conf** custom configuration file.

Don’t change the other parameters in the custom configuration file; they affect the machine learning algorithm behind this capability. If you have questions about these parameters, contact Exabeam Customer Success.

1. Source the shell environment:

```bash
./opt/exabeam/bin/shell-environment.bash
```

2. Navigate to `/opt/exabeam/ds-server/config/custom/algorithms.conf`.

3. In the `algorithms.conf` file under `personal-email-identification`, change the value of `Enabled` to `true`:

```bash
personal-email-identification {
    Enabled = true
}
```

4. Add your company domain as a string to `CompanyDomain`:

```bash
personal-email-identification {
    Enabled = true
    Parameters = {
        CompanyDomain = "company.com"
    }
}
```

To add multiple company domains, insert them in a list:
5. Save the `algorithms.conf` file.
6. Restart the DS server:

```
ds-server-stop
ds-server-start
```

### 4.11. Manage Security Content in Advanced Analytics

Install, get updates on, uninstall, and upload content packages in Advanced Analytics settings.

Manage all your content packages directly in Advanced Analytics settings, under **Admin Operations > Additional Settings > Content Updates**. Instead of using **Content Installer**, which requires you to use the command line and manually restart internal engines, you retrieve the latest available content packages from the cloud in real time, including both general Exabeam releases and custom fixes you request.

In these settings, a content package that includes custom fixes you requested is called a *custom package*. A content package from a general Exabeam release is called a *default package*. It's important that you update your content with each release because the release may contain new rules and models, support new log sources and vendors, and remove noisy rules or faulty models, and other additions and fixes that keep your system running smoothly.

If you have an environment that can access the internet, you can pull the latest content packages *manually* or *automatically*, select a specific content packages to *install*, or even *schedule* content packages to automatically install on a daily or weekly basis, all from the cloud.

If you have an environment that can't access the internet, you can't connect to the cloud. You must view and download the latest content packages from the Exabeam Community, then *upload* them.

You can only install and upload content packages that contain event builders or parsers.

#### 4.11.1. Manually Install a Content Package

Install a new content package directly from Advanced Analytics settings onto your system.

Select a content package to install from a list of the latest, available content packages. If your environment can't access the internet, you can't install content packages from the cloud. Instead, download the content package from the Exabeam Community or your case ticket, then manually *upload* it.

A content package from a general Exabeam release is called a *default package*. It's important that you update your content with each release because the release may contain new rules and models, support new log sources and vendors, and remove noisy rules or faulty models, and other additions and fixes
that keep your system running smoothly. You can upload multiple default content packages, but only install one default package at a time.

A content package that includes custom fixes you requested is called a custom package. You can upload and install any number of custom packages.

You can only install custom content packages that contain event builders or parsers.

1. In the navigation bar, click the Menu, select Settings, then navigate to Admin Operations > Additional Settings.
2. Under Admin Operations, select Content Updates.
3. To install a default content package, click the DEFAULT PACKAGES tab. To install a custom content package, click the CUSTOM PACKAGES tab.
4. Click INSTALL.
   - If the package is a default content package and a newer version of one you previously installed, this newer version replaces the older version. You can no longer view or install the older version.
   - If the package is a custom content package and a newer version of one you already installed, ensure that you uninstall the older version.

4.11.2. AUTOMATICALLY INSTALL CONTENT PACKAGES
Schedule Advanced Analytics to automatically check for and install new content packages on a daily or weekly basis.

If you have an environment that can't access the internet, you can't install content packages from the cloud. Instead, download a content package from the Exabeam Community or your case note, then manually upload it.

Only content packages that contain event builders or parsers are available.

1. In the navigation bar, click the Menu, select Settings, then navigate to Admin Operations > Additional Settings.
2. Under Admin Operations, select Content Updates.
3. Click Install Schedule, then toggle Auto Install on.
4. After Install package, select the day of the week when Advanced Analytics downloads new content.
5. After at, select the time when Advanced Analytics downloads new content.
6. Click SAVE. If newer versions of custom content packages were installed, ensure that you uninstall the older version.

4.11.3. MANUALLY CHECK FOR NEW CONTENT PACKAGES
Manually fetch the latest available content packages. You can also set Advanced Analytics to automatically check for new packages every 30 minutes.
If you have an environment that can't access the internet, you can't connect to the cloud to view the latest, available content packages. Instead, check the Exabeam Community for the latest content packages. If you manually refresh the list, Advanced Analytics says you have no new packages.

Only content packages that contain event builders or parsers are available.

1. In the navigation bar, click the Menu , select Settings, then navigate to Admin Operations > Additional Settings.
2. Under Admin Operations, select Content Updates.
3. Click the refresh button. Advanced Analytics checks for new default and custom content packages and updates both lists.

4.11.4. AUTOMATICALLY CHECK FOR NEW CONTENT PACKAGES
Set Advanced Analytics to automatically check for new content packages and fetch them every 30 minutes.

This setting automatically checks for new content packages but doesn't install them. To automatically install them, you must schedule it separately.

If you have an environment that can't access the internet, you can't connect to the cloud to view the latest, available content packages. Instead, check the Exabeam Community for the latest content packages.

Only content packages that contain event builders or parsers are available.

1. In the navigation bar, click the Menu , select Settings, then navigate to Admin Operations > Additional Settings.
2. Under Admin Operations, select Content Updates.
3. Click Last Update Checked, toggle Auto Updates on, then click SAVE. Advanced Analytics checks for new content packages every 30 minutes and updates the list.

4.11.5. UPLOAD A CONTENT PACKAGE
If you have an environment that can't access the internet, download new content from the Exabeam Community or your case ticket, then upload it directly in Advanced Analytics settings.

If you can access the internet in your environment, you see a list of the latest available content packages in the cloud. Directly install a content package from this list instead of uploading packages to Advanced Analytics.

A content package from a general Exabeam release is called a default package. It's important that you update your content with each release because the release may contain new rules and models, support new log sources and vendors, and remove noisy rules or faulty models, and other additions and fixes that keep your system running smoothly. You can upload multiple default content packages, but only install one default package at a time.
A content package that includes custom fixes you requested is called a *custom package*. You can upload and install any number of custom packages.

You can only upload content packages that contain event builders or parsers.

1. Ensure that you download the content package from the Exabeam Community or your case ticket.

2. In the navigation bar, click the Menu, select **Settings**, then navigate to **Admin Operations > Additional Settings**.

3. Under **Admin Operations**, select **Content Updates**.

4. To upload a content package from a general Exabeam content release, click **DEFAULT PACKAGES**. To upload a content package you requested, click **CUSTOM PACKAGES**.

5. Click the upload button.

6. Click **UPLOAD THE PACKAGE**, then select a ZIP file to upload, up to 100 MB.

7. Click **SAVE**. Your content package is uploaded.

8. Locate your content package, then click **INSTALL**. Your content package is installed. If the package is a custom content package and a newer version of one you already installed, ensure that you **uninstall** the older version.

### 4.11.6. UNINSTALL A CUSTOM CONTENT PACKAGE

Uninstall a custom content package if there's an issue with the package or to remove an older version of a package once you upload a newer version.

A content package from a general Exabeam release is called a *default package*. A content package that includes custom fixes you requested is called a *custom package*. You can only uninstall a custom content package, not a default content package. To remove a default content package, you must **install** another default content package.

1. In the navigation bar, click the Menu, select **Settings**, then navigate to **Admin Operations > Additional Settings**.

2. Under **Admin Operations**, select **Content Updates**.

3. Click the **CUSTOM PACKAGES** tab, then next to the content package, click **UNINSTALL**.

### 4.12. 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.

### 4.12.1. 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:

   ```
csrf.enabled=true
csrf.cookie.secure=true
csrf.cookie.name="CSRF_TOKEN"
```
b. Restart `web-common` to enable CSRF 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.

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:

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

   b. Restart services.

   ```
   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.

4.12.2. 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 in the CONF file to match your Exabeam service domain:

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

   Here's an example with 2 service origins:

   ```text
   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.

---

### 4.12.2.1. 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):

```bash
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:

```bash
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.
5. Health Status Page

The Health Status page is an on-demand assessment of the Exabeam pipeline. It is broken down into three categories:

**General Health** - General health tests that all of the back-end services are running - database storage, log feeds, snapshots, CPU, and memory.

**Connectivity** - Checks that Exabeam is able to connect to external systems, such as LDAP and SIEM.

**Log Feeds** - This section reports on the health of the DC, VPN, Security Alerts, Windows Servers, and session management logs.

In all of the above areas, GREEN indicates the status is good, YELLOW for a warning, and RED if the system is critical.

Located on the homepage are the Proactive Health Checks that will alert administrations when:

- Any of the core Exabeam services are not running
- There is insufficient disk storage space
- Exabeam has not been fetching logs from the SIEM for a configurable amount of time

5.1. Proactive and On-Demand Health Checks

Advanced Analytics provides visibility on the backend data pipeline via **Health Checks**. Health checks can be either proactive or on-demand.

Proactive health checks run automatically and periodically in the background. When a proactive check is triggered, a notification message is displayed.

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.

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.
- **Log Feeds** – Session counts, alerts, and metrics.
- **System Health Information** – Core data and operations processor metrics.
- **Service Availability** (Incident Processors and Repositories) - IR, Hadoop, and Kafka performance metrics.
- **Elasticsearch Storage** (Incident Responder) – Elasticsearch capacity and performance metrics.
All proactive and on-demand health checks are listed on the Health Checks page. Proactive health checks are visible by any Advanced Analytics user in your organization.

**NOTE**
Only users with administrator permission can reach the page.

![Figure 3. System Health - Advanced Analytics Health Checks menu](image)

### 5.1.1. CONFIGURE ALERTS FOR WORKER NODE LAG

When processing current or historical logs, an alert will be triggered when the worker node is falling behind the master node. How far behind can be configured in `/opt/config/exabeam/tequila/custom/health.conf`. The parameters are defined below:

- **RTModeTimeLagHours** - During real-time processing the default setting is 6 hours.
- **HistoricalModeTimeLagHours** - During historical processing the default setting is 48 hours.
- **syslogIngestionDelayHour** - If processing syslogs, the default setting is 2 hours.

```json
slaveMasterLagCheck {
    printFormats = {
        json = "{ \"lagTimeHours\": \"$lagTimeHours\", \"masterRunDate\": \"$masterRunDate\", \"slaveRunDate\": \"$slaveRunDate\", \"isRealTimeMode\": \"$isRealTimeMode\"}"}
}```
Worker nodes processing lagging by more than $lagTimeHours hours. Is in real time: $isRealTimeMode 

RTModeTimeLagHours = 6

HistoricalModeTimeLagHours = 48

limeCheck {
    syslogIngestionDelayHour = 1
}

5.2. System Health Checks

**Martini Service Check:** Martini is the name Exabeam has given to its Analytics Engine. In a multi-node environment, Martini will be the Master node.

**Tequila Service Check:** Tequila is the name Exabeam has given to its User Interface layer.

**Lime Service Check:** LIME (Log Ingestion and Message Extraction) is the service within Exabeam that ingests logs from an organization’s SIEM, parses and then stores them in HDFS. The main service mode parses message files and creates one message file per log file. This mode is used to create message files that will be consumed by the main node.

**Mongo Service Check:** MongoDB is Exabeam's chosen persistence database. A distributed MongoDB system contains three elements: shards, routers, and configuration servers (configsvr). The shards are where the data is stored; the routers are the piece that distributes and collect the data from the different shards; and the configuration servers which tracks where the various pieces of data are stored in the shards.

**Zookeeper Service Check:** Zookeeper is a centralized service for maintaining configuration information, naming, providing distributed synchronization, and providing group services. In a distributed multi-node environment, we need the ability to make a value change inside one process on a machine and have that change be seen by a different process on a different machine. Zookeeper provides this service.

**Hadoop Service Check:** Master - Hadoop is Exabeam’s distributed file system, where the raw logs and parsed events are stored. These files are available to all nodes.

**Ganglia Service Check:** Ganglia is a distributed monitoring system for computing systems. It allows us to view live or historical statistics for all the machines that are being monitored.

**License Checks:** The status of your Exabeam license will be reported in this section. This is where you will find the expiration date for your current license.
5.3. Alerts for Storage Use

Available on the System Health page, the Storage Usage tab provides details regarding the current data retention settings for your Advanced Analytics deployment. Advanced Analytics sends notifications when available storage capacity dwindles to a critical level. Admins have the option to enable and configure automatic data retention and data purging for both HDFS and MongoDB usage.

5.3.1. DEFAULT DATA RETENTION SETTINGS

The table below lists default retention periods for data elements in your Advanced Analytics deployment:

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
<th>Default Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logs</td>
<td>Original logs</td>
<td>90 days</td>
</tr>
<tr>
<td>Events on Disk</td>
<td>Parsed events on disk</td>
<td>180 days</td>
</tr>
<tr>
<td>Events in Database</td>
<td>Parsed events in the database</td>
<td>180 days</td>
</tr>
<tr>
<td>Triggered Rules and Sessions in Database</td>
<td>Container and triggered rule collections in the database</td>
<td>365 days</td>
</tr>
</tbody>
</table>

5.4. System Health Alerts for Disabled Parsers

Get notified when Advanced Analytics disables a parser.

To protect your system from going down and ensure that it continues to process data in real time, Advanced Analytics detects when a parser is taking an abnormally long time to parse a log, then disables it.

When Advanced Analytics disables a parser, you receive a health alert that describes which parser was disabled, on which node, and recommended actions you could take. When Advanced Analytics disables additional parsers, it resolves the existing health alert and sends a new alert that lists all disabled parsers.

Advanced Analytics also resolves an existing health alert any time you restart the Log Ingestion and Messaging Engine (LIME) and re-enable a disabled parser. For example, if you change the threshold for when parsers get disabled, you must restart LIME, which re-enables any disabled parsers and prompts Advanced Analytics to resolve any existing health alerts. If a re-enabled parser continues to perform poorly, Advanced Analytics disables it again and sends another health alert about that parser.

5.5. View Storage Usage and Retention Settings

By default, Advanced Analytics implements data retention settings for logs and messages. This allows the system to automatically delete old data, which reduces chances of performance issues due to low repository space.

Available on the System Health page, the Storage Usage tab provides details regarding the current data retention settings for your Advanced Analytics deployment, including:

- **HDFS Data Retention** – Number of days the data has been stored, the number of days remaining before it is automatically deleted, and a toggle to enable/disable auto-deletion of old data.
If enabling or disabling **Auto-delete Old Data**, you must also restart the Log Ingestion Engine before the change goes into effect. For more information on restarting the Log Ingestion Engine, please refer to the Restart the Analytics Engine section.

A warning message appears if the average rate of HDFS usage exceeds the intended retention period.

- **HDFS Usage** – Total HDFS usage, including specific breakdowns for logs, events on disk, and events in database.

- **MongoDB Retention** – A dialog to set retention settings and a toggle to enable/disable disk-based deletion of old data.
  
  You can edit the MongoDB data retention settings by clicking the pencil icon.
  
  The capacity used percentage threshold is set to 85% by default, with a maximum value of 90%. It helps to prevent MongoDB from reaching capacity before hitting the default retention period threshold. As soon as MongoDB meets the percentage on any node, the system will start purging events until it is back below the capacity used threshold.
  
  In addition to the capacity used percentage, Advanced Analytics keeps 180 days of event data in MongoDB and 365 days of triggered rules and containers data by default.

  **NOTE**
  
  The **Days for Triggered Rules & Sessions** value cannot by less than the **Days for Events** value.

- **MongoDB Usage** – Total MongoDB usage.

5.6. Set Up System Optimization

This tab is a single aggregated page for auditing and viewing disabled data types (including models, event types, and parsers) and system load redistribution.

**5.6.1. DISABLED MODELS**

When a model takes up too much memory, it is disabled. If you enable these models, the system may suffer performance issues.

  **NOTE**
  
  Exabeam disables models as a last resort to ensure system performance. We have other defensive measures to prevent models from using all of the system's memory. These measures include enabling model aging and limiting the model bin size count. If these safeguards cannot prevent a model from consuming too much memory, the system prevents itself from shutting down as it runs out of memory.

**5.6.1.1. Configure Model Maximum Bin Limit**

Models are disabled once they reach their maximum bin limit. You can either set a global configuration for the maximum number of bins or an individual configuration for each model name.

This is done by setting a max number of bins, MaxNumberOfBins in exabeam_default.conf or the model definition, for categorical models. The new limit is 10 million bins, although some models,
such as ones where the feature is "Country" have a lower limit. We have put many guardrails in place to make sure models do not consume excessive memory and impact overall system health and performance. These include setting a maximum limit on bins, enabling aging for models, and verifying data which goes into models to make sure it is valid. If a model is still consuming excessive amounts of memory then we will proceed to disable that model.

To globally configure the maximum bin limit, navigate to the **Modeling** section located in the `exabeam_default.conf` file at `/opt/exabeam/config/default/exabeam_default.conf`.

All changes should be made to `/opt/exabeam/config/custom/custom_exabeam_config.conf`:

```plaintext
Modeling {
  ...
  # To save space we limit the number of bins saved for a histogram. This defaults to 100 if not present
  # This parameter is only for internal research
  MaxSizeOfReducedModel = 100
  MaxPointsToCluster = 250
  ReclusteringPeriod = 24 hours
  MaxNumberOfBins = 1000000
}
```

Additionally, it is possible to define a specific bin limit on a per model basis via the model definition section in the `models.conf` file at `/opt/exabeam/config/custom/models.conf`. Here is an example model, where `MaxNumberOfBins` is set to 5,000,000:

```plaintext
WTC-OH {
  ModelTemplate = "Hosts on which scheduled tasks are created"
  Description = "Models the hosts on which scheduled tasks are created"
  Category = "Asset Activity Monitoring"
  IconName = ""
  ScopeType = "ORG"
  Scope = "org"
  Feature = "dest_host"
  FeatureName = "host"
  FeatureType = "asset"
  TrainIf = """"count(dest_host,'task-created')=1"
  ModelType = "CATEGORICAL"
  BinWidth = "5"
  MaxNumberOfBins = "5000000"
  AgingWindow = ""
  CutOff = "10"
  Alpha = "2"
  ConvergenceFilter = "confidence_factor>=0.8"
  HistogramEventTypes = [
    "task-created"
  ]
  Disabled = "FALSE"
}
```
5.6.2. DISABLED PARSERS

To protect the system from going down and ensure that it keeps processing data in real time, Advanced Analytics automatically identifies poor parser performance and disables such parsers.

We determine the average parse time per event for each parser every five minutes. We compare that to a configurable threshold variable in `lime.conf`, `ParserDisableThresholdInMills`. Then we divide each by the total time taken by all parsers in the same five minute period and compare the values to a configurable threshold variable in `lime.conf`, `ParserDisableTimePercentage`. If the parsers average parse time exceeds the threshold and it exceeds the second threshold of being over a certain percentage of the overall parse time by all parsers then it becomes a candidate for disabling. We perform the same check during a second five minute period and if the same holds true then we proceed to disable the parser.

A slow parser is placed in a cache during the first parsing time period, and is then disabled during the second period if its average parsing time continues to meet the following conditions:

- It is above the parsing time threshold, which is set at 7 ms by default. The parsing time threshold, `ParserDisableThresholdInMills`, is configurable.
- It makes up 50% or more of the total parsing time of all parsers. The parsing time percentage, `ParserDisableTimePercentage`, is configurable.

When a parser meets these conditions on a Log Ingestion and Messaging Engine (LIME) node, it is disabled only on that node. If you have multiple LIME nodes, it is not automatically disabled on all nodes unless it meets these conditions on every node.

When Advanced Analytics disables a parser on any node, you receive a system health alert.

Disabled parsers are also displayed on the System Optimization tab of the System Health page. You can see a list of all parsers that have been disabled.

![Figure 4. System Health - System Optimization menu](image)

The Disabled Parsers table is sorted alphabetically by parser name.

The table includes columns with the following categories:
• **Parser Name** – The name of the disabled parser.

• **Average Log Line Parse Time** – Average time taken by the parser to parse each event.

• **Disabled Time** – Date and time when the parser was disabled.

You can also view disabled parsers in `disabled_parsers_db.current_collection`. Here is a sample disabled parser collection:

```
{
  "_id" : ObjectId("5cf5bb9e094b83c6f7f89b86"),
  "_id" : ObjectId("5cf5bb9e094b83c6f7f89b86"),
  "parser_name" : "raw-4625",
  "average_parsing_time" : 9.774774774774775,
  "time" : NumberLong(1559608222854)
}
```

### 5.6.2.1. Configure Thresholds for Disabling Parsers

Hardware and Virtual Deployments Only

The parsing time period, `OutputParsingTimePeriodInMinutes`, is configurable.

Navigate to the LogParser section located in the `lime_default.conf` file at `/opt/exabeam/config/default/lime_default.conf`.

All changes should be made to `/opt/exabeam/config/custom/custom_lime_config.conf`:

```yaml
LogParser{
  #Output parsing performance in debug mode, be cautious this might affect
  #performance in parsing
  OutputParsingTime = true
  OutputParsingTimePeriodInMinutes = 5
  AllowDisableParser = true // If this is enabled, output parsing time will
  // be enabled by default.
  ParserDisableThresholdInMills = 7 //If average parsing time pass this
  threshold, we will disable that parser
  ParserDisableTimePercentage = 0.5
}
```

Acceptable values for `ParserDisableThresholdInMills` includes any integer value. `ParserDisablePercentage` can be a percentage decimal value between 0.1 to 0.9.

**NOTE**

Setting a higher parsing time percentage would identify more severe parsers.

### 5.6.3. DISABLED EVENT TYPES

When a high volume user or asset amasses a large number of events of a certain event type, and that event type contributes to a large portion of the overall event count for that user (typically 10M+ events in a session) the event type is automatically disabled and listed here.
NOTE

You are also shown an indicator when Advanced Analytics determines that the event type is problematic and disables it for the entity. The affected User/Asset Risk Trend and Timeline accounts for the disabled event type by displaying statistics only for the remaining events.

Disabled event types are displayed on the **System Optimization** tab of the **System Health** page. You can see a list of all event types that have been disabled, along with the users and assets for which they have been disabled for.

![Figure 5. System Health - System Optimization menu](image)

The **Disabled Event Type by Users and Assets** table is sorted first alphabetically by event type, then sorted by latest update timestamp.

The table includes columns with the following categories:

- **Event Type** – The disabled event type.
- **Count** – Last recorded total number of events for this entity.
- **Last Log Received** – Date and time of the event that triggered the disabling of this event type for the specified entity.
- **Disabled Time** – Date and time for when the event type was disabled for this entity.

You can also view disabled event types for an entity in `metadata_db`. Here is a sample disabled event types collection:

```javascript
> db.event_db.event_count_stats_collection db.event_disabled_collection
mongos> db.event_disabled_collection.findOne()
{
   "_id" : ObjectId("5ce346016885455be1648a0f"),
   "entity" : "exa_kghko5dn",
   "last_count" : NumberLong(53),
   "disabled_time" : NumberLong("1558399201751"),
   "last_event_time" : NumberLong("1503032400000"),
   "is_entity_disabled" : true,
   "sequence_type" : "session",
}```
"disabled_event_types" : [
  "Dlp-email-alert-in",
  "Batch-logon",
  "Remote-access",
  "Service-logon",
  "Kerberos-logon",
  "Local-logon",
  "Remote-logon"
]
}

5.6.3.1. Configure Thresholds for Disabling Event Types
Hardware and Virtual Deployments Only

When an entity's session has 10 million or more events in a session and an event type contributes to
70% or more of the events in that session, then that event type is disabled. If no single event type
accounts for over 70% of the total event count in that session, then that entity is disabled. These
thresholds, EventCountThreshold and EventDisablePercentage are configurable.

To configure the thresholds, navigate to the **Container** section located in the
exabeam_default.conf file at /opt/exabeam/config/default/exabeam_default.conf.

All changes should be made to /opt/exabeam/config/custom/
custom_exabeam_config.conf:

Container {
  ...
  EventCountThreshold = 10000000 // Martini will record the user as top user
  // once a session or a sequence has more than
  // 10 million events
  TopNumberOfEntities = 10 // reporting top 10 users and assets
  EventDisablePercentage = 0.7 // a single event type that accounts for 70%
  of all event types for a disabled user
  EventCountCheckPeriod = 60 minutes
}

Acceptable values for EventCountThreshold are 10,000,000 to 20,000,000 for a typical
environment. EventDisablePercentage can be a percentage decimal value between 0.1 to 0.9.

5.6.4. MANUALLY REDISTRIBUTE SYSTEM LOAD
Hardware and Virtual Deployments Only

You can opt to manually configure the system load redistribution by creating a manual config section in
custom_exabeam_config.conf.

To configure manual redistribution:

1. Run the following query to get the current distribution in your database:

```
mongo metadata_db --eval
'db.event_category_partitioning_collection.findOne()'
```
2. Taking the returned object, create a manual config section in `/opt/exabeam/config/custom/custom_exabeam_config.conf`.

3. Edit the configuration to include all the hosts and event categories you want.

4. Choose which categories should be shared by certain hosts by using `true` or `false` parameter values after “Shared =”.
   For example, the below section shows that host 2 and 3 both share the web event category. All other categories, which are marked as `Shared = “false”`, are owned solely by one host.

```plaintext
Partitioner {
    Partitions {
        exabeam-analytics-slave-host3 = [
            { EventCategory = "database", Shared = "false" },
            { EventCategory = "other", Shared = "false" },
            { EventCategory = "web", Shared = "true" },
            { EventCategory = "authentication", Shared = "false" },
            { EventCategory = "file", Shared = "false" }
        ]
        exabeam-analytics-slave-host2 = [
            { EventCategory = "network", Shared = "false" },
            { EventCategory = "app-events", Shared = "false" },
            { EventCategory = "endpoint", Shared = "false" },
            { EventCategory = "alerts", Shared = "false" }
        ]
    }
}
```
5.6.5. AUTOMATICALLY REDISTRIBUTE SYSTEM LOAD

Exabeam can automatically identify overloaded worker nodes, and then take corrective action by evenly redistributing the load across the cluster.

This redistribution is done by measuring and comparing job completion time. If one node finishes slower by 50% or more compared to the rest of the nodes, then a redistribution of load is needed. The load is then scheduled to be rebalanced by event categories.

You can enable automatic system load redistribution on the **System Optimization** tab of the **System Health** page. This option is enabled by default. Doing so allows the system to check the load distribution once a day.

**NOTE**

It is not recommended that you disable the system rebalancing option as it will result in uneven load distribution and adverse performance impacts to the system. However, if you choose to do so, you can configure manual redistribution to avoid such impacts.

You must restart the Exabeam Analytics Engine for any changes to **System Rebalancing** to take effect.

The **System Load Redistribution** tab shows an indicator when a redistribution of load is needed, is taking place, or has completed. The rebalancing process can take up to two hours. During this time you may experience slower processing and some data may not be available. However, the system resumes normal operations once redistribution is complete.

5.7. Automatic Shutdown

If the disk usage on an appliance reaches 98%, then the Analytics Engine and log fetching will shut down automatically. Only when log space has been cleared and usage is below 98% will it be possible to restart.

Users can restart either from the **CLI** or the **Settings** page.
6. Generate Technical Support Information

This chapter describes how to generate the information that Exabeam Technical Support needs to understand a problem in a customer's system. You can contact Exabeam Customer Success by opening a case via Community.Exabeam.com.

Navigate to the Generate Support File UI.

Click the check box to select the product to extract information from, then select Generate Support.

Support logs will download automatically. You can now create a support ticket on Exabeam Community and attach your files there.
7. View Version Information

View the Advanced Analytics release version of your deployment, as well as build numbers that constitute the release version (Advanced Analytics product, Incident Responder product, Data Lake product, Exabeam platform common services, and Security content).

Click the **collapsed menu** icon at the top-right corner of any page in the UI.
8. Syslog Notifications Key-Value Pair Definitions

The Incident Notifications sent via Syslog to your SIEM use the following parameters in their key-value pairs. The pairs are separated by a space (for example, reasons_count="3" score="135").

The following tables define each extension field key in Syslog messages by Event Type for Advanced Analytics v.i48 and later.

**Event Type: System Health**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Key Value</th>
<th>Description</th>
<th>Syslog Key Value Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Service of the system health</td>
<td>The service of the system health.</td>
<td>service=&quot;Analytics Log Ingestion&quot;</td>
</tr>
<tr>
<td>status</td>
<td>Status of the system health</td>
<td>The status of the system health, either &quot;running&quot; or &quot;stopped&quot;.</td>
<td>status=&quot;stopped&quot;</td>
</tr>
</tbody>
</table>

**Event Type: Notable Sessions / Anomalies**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Key Value</th>
<th>Description</th>
<th>Syslog Key Value Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Session, sequence, or asset sequence ID</td>
<td>The ID of the session, sequence, or asset sequence ID. Also the triggered rule containerId of a session or sequence.</td>
<td>id=&quot;npage-201905151524&quot;</td>
</tr>
<tr>
<td>url</td>
<td>URL to the session, sequence, or asset sequence</td>
<td>The URL to the session, sequence, or asset sequence in the timeline.</td>
<td>url=&quot;https://&lt;ExabeamAA&gt;:8484/uba/#user/admin/timeline/admin-201906241700&quot;</td>
</tr>
<tr>
<td>entity_value</td>
<td>Asset sequence entity value</td>
<td>The asset sequence entity value.</td>
<td>entity_value=&quot;dev_kr&quot;</td>
</tr>
<tr>
<td>score</td>
<td>Session, sequence, or asset sequence risk score</td>
<td>The session, sequence, or asset sequence risk score. Also the triggered rule risk score.</td>
<td>score=&quot;316&quot;</td>
</tr>
<tr>
<td>sequence_type</td>
<td>Type of sequence</td>
<td>The type of sequence or asset sequence entity name.</td>
<td>sequence_type=&quot;lockout&quot;</td>
</tr>
<tr>
<td>start_time</td>
<td>loginTime in UTC format</td>
<td>The loginTime for the session or sequence. Also the day for the asset sequence.</td>
<td>start_time=&quot;2019-05-25T08:05:24-07:00&quot;</td>
</tr>
<tr>
<td>end_time</td>
<td>logoutTime in UTC format</td>
<td>The logoutTime for the session or sequence. Also the start_time + 24 hours for the asset sequence.</td>
<td>end_time=&quot;2019-05-25T18:26:24-07:00&quot;</td>
</tr>
<tr>
<td>status</td>
<td>Status of the session or sequence</td>
<td>The status of the session or sequence, either &quot;open&quot; or &quot;closed&quot;. It is closed if logoutTime is != 0, otherwise it is open.</td>
<td>status=&quot;closed&quot;</td>
</tr>
<tr>
<td>user</td>
<td>Session or sequence username</td>
<td>The session or sequence user. Also the triggered rule username.</td>
<td>user=&quot;admin&quot;</td>
</tr>
</tbody>
</table>
### Syslog Notifications Key-Value Pair Definitions

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Key Value</th>
<th>Description</th>
<th>Syslog Key</th>
<th>Value Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>src_host</td>
<td>Session or sequence loginHost</td>
<td>The session or sequence loginHost. Also the triggered rule src host. (optional)</td>
<td>src_host</td>
<td>&quot;dc_464&quot;</td>
</tr>
<tr>
<td>src_ip</td>
<td>Session src_ip</td>
<td>The session src_ip. Also the triggered rule src_ip. (optional)</td>
<td>src_ip</td>
<td>&quot;10.55.0.123&quot;</td>
</tr>
<tr>
<td>accounts</td>
<td>Session or sequence accounts</td>
<td>The session or sequence accounts.</td>
<td>accounts</td>
<td>&quot;achan, tmiles, dgreen, mbridges&quot;</td>
</tr>
<tr>
<td>labels</td>
<td>Session or sequence labels</td>
<td>The session or sequence labels.</td>
<td>labels</td>
<td>&quot;TIME&quot;</td>
</tr>
<tr>
<td>assets_count</td>
<td>Session or sequence assets count</td>
<td>The total number of assets recorded for the session or sequence.</td>
<td>assets_count</td>
<td>&quot;23&quot;</td>
</tr>
<tr>
<td>assets</td>
<td>Session or sequence assets</td>
<td>The names of all unique assets for the session or sequence.</td>
<td>assets</td>
<td>&quot;srv_123_dev, 10.23.123.56, tks_en_0b_jt&quot;</td>
</tr>
<tr>
<td>zones</td>
<td>Session zones</td>
<td>The session zones. Also the asset sequence zones. (optional)</td>
<td>zones</td>
<td>&quot;atlanta office&quot;</td>
</tr>
<tr>
<td>reasons</td>
<td>All unique rule definition</td>
<td>The total number of reasons recorded for the session or sequence.</td>
<td>reasons</td>
<td>&quot;8&quot;</td>
</tr>
<tr>
<td>reasons_count</td>
<td>Session or sequence reasons count</td>
<td>By default, only takes the top three by triggered rule risk score. Configurable through exabeam_custom_config ScoreManager.IncidentReasonsLimit.</td>
<td>reasons_count</td>
<td>&quot;779&quot;</td>
</tr>
<tr>
<td>events_count</td>
<td>Session or sequence events count</td>
<td>The total number of events recorded for the session or sequence.</td>
<td>events_count</td>
<td>&quot;77&quot;</td>
</tr>
<tr>
<td>alerts_count</td>
<td>Session or sequence alerts count</td>
<td>The total number of security events recorded for the session or sequence.</td>
<td>alerts_count</td>
<td>&quot;77&quot;</td>
</tr>
<tr>
<td>asset_labels</td>
<td>Labels for the asset</td>
<td>The labels for the asset.</td>
<td>asset_labels</td>
<td>&quot;SOURCE HOST&quot;</td>
</tr>
<tr>
<td>asset_locations</td>
<td>Locations for the asset</td>
<td>The locations for the asset.</td>
<td>asset_locations</td>
<td>&quot;los angeles office&quot;</td>
</tr>
<tr>
<td>top_users</td>
<td>Top users for the asset</td>
<td>The top users for the asset.</td>
<td>top_users</td>
<td>&quot;adonald&quot;</td>
</tr>
<tr>
<td>host_name</td>
<td>Hostnames for the asset</td>
<td>The hostnames for the asset.</td>
<td>host_name</td>
<td>&quot;adonald-win7&quot;</td>
</tr>
<tr>
<td>ip_address</td>
<td>IP addresses for the asset</td>
<td>The IP addresses for the asset.</td>
<td>ip_address</td>
<td>&quot;10.0.0.3&quot;</td>
</tr>
<tr>
<td>dest_host</td>
<td>dest_host of the triggered rule</td>
<td>The dest_host of the triggered rule.</td>
<td>dest_host</td>
<td>&quot;lt-adonald-123&quot;</td>
</tr>
<tr>
<td>dest_ip</td>
<td>dest_ip of the triggered rule</td>
<td>The dest_ip of the triggered rule.</td>
<td>dest_ip</td>
<td>&quot;10.23.121.87&quot;</td>
</tr>
<tr>
<td>event_time</td>
<td>Time of the event</td>
<td>The time of the event.</td>
<td>event_time</td>
<td>&quot;8:26:00&quot;</td>
</tr>
<tr>
<td>event_type</td>
<td>Type of the event</td>
<td>The type of the event.</td>
<td>event_type</td>
<td>&quot;remote-access&quot;</td>
</tr>
<tr>
<td>host</td>
<td>Host for the triggered rule</td>
<td>The host for the triggered rule.</td>
<td>host</td>
<td>&quot;atl-file-01&quot;</td>
</tr>
</tbody>
</table>
Syslog Notifications Key-Value Pair Definitions

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Key Value</th>
<th>Description</th>
<th>Syslog Key Value Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain (optional)</td>
<td>Domain for the triggered rule</td>
<td>The domain for the triggered rule.</td>
<td>domain=&quot;kt_cloud&quot;</td>
</tr>
<tr>
<td>raw (optional)</td>
<td>Raw &quot;payload&quot;</td>
<td>The raw &quot;payload&quot; for the triggered rule or event.</td>
<td>raw=&quot;http: //exampleurl&quot;</td>
</tr>
<tr>
<td>rule_id</td>
<td>Rule definition ID</td>
<td>The rule definition ID for the triggered rule.</td>
<td>rule_id=&quot;WL-HG-F&quot;</td>
</tr>
<tr>
<td>rule_name</td>
<td>Rule definition name</td>
<td>The rule definition name for the triggered rule.</td>
<td>rule_name=&quot;Account switch by new user&quot;</td>
</tr>
<tr>
<td>rule_description</td>
<td>Rule definition description</td>
<td>The rule definition description for the triggered rule.</td>
<td>rule_description=&quot;User for which we have insufficient data logged onto a Domain Controller&quot;</td>
</tr>
</tbody>
</table>

**Event Type: Advanced Analytics/Case Manager/OAR Audit**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Key Value</th>
<th>Description</th>
<th>Syslog Key Value Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>Time in Unix timestamp</td>
<td>When the event took place.</td>
<td>time=&quot;1559076154132&quot;</td>
</tr>
<tr>
<td>user</td>
<td>Admin or user’s username</td>
<td>The user performing the activity in Exabeam.</td>
<td>user=&quot;admin&quot;</td>
</tr>
<tr>
<td>host</td>
<td>Hostname, and if not available, IP address</td>
<td>The machine logging the event.</td>
<td>host=&quot;10.0.0.4&quot;</td>
</tr>
<tr>
<td>src_ip</td>
<td>Client IP address</td>
<td>The IP from which the user connected to Exabeam.</td>
<td>src_ip=&quot;10.0.0.6&quot;</td>
</tr>
<tr>
<td>event_type</td>
<td>Event type</td>
<td>The event type, such as &quot;app-activity&quot;, &quot;remote-logon&quot;, and &quot;logout&quot;.</td>
<td>event_type=&quot;failed-app-login&quot;</td>
</tr>
<tr>
<td>app</td>
<td>Name of the application</td>
<td>The name of the application that logs the event, such as &quot;Exabeam Advanced Analytics&quot;. If it is not possible to get the app type then &quot;Exabeam&quot; is used.</td>
<td>app=&quot;Exabeam&quot;</td>
</tr>
<tr>
<td>event_subtype</td>
<td>Exabeam Audit Event</td>
<td>The Exabeam Audit Event identifier.</td>
<td>event_subtype=&quot;Exabeam Audit Event&quot;</td>
</tr>
<tr>
<td>activity</td>
<td>Activity type</td>
<td>The activity type, such as &quot;User added&quot;, &quot;Role updated&quot;, and &quot;LDAP server removed&quot;.</td>
<td>activity=&quot;Failed log in&quot;</td>
</tr>
<tr>
<td>additional_info</td>
<td>Activity details</td>
<td>The activity details, such as those pertaining to user, role, and LDAP updates.</td>
<td>additional_info=&quot;User 'admin' failed to login&quot;</td>
</tr>
</tbody>
</table>

**Event Type: Job Status**

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Key Value</th>
<th>Description</th>
<th>Syslog Key Value Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>job_status</td>
<td>Job status</td>
<td>The job status, either &quot;Started&quot;, &quot;Failed&quot;, or &quot;Completed&quot;.</td>
<td>job_status=&quot;Started&quot;</td>
</tr>
</tbody>
</table>
### Syslog Notifications Key-Value Pair Definitions

<table>
<thead>
<tr>
<th>Key Name</th>
<th>Key Value</th>
<th>Description</th>
<th>Syslog Key Value Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>job_details</td>
<td>Job details</td>
<td>The job details, which includes modified rules and reprocess times.</td>
<td>job_details=&quot;Modified rules: rule AM-OG-A has new score 40.0, rule AM-GOU-A has new score 40.0, rule AM-GA-AC-A has new score 40.0. Reprocess starts from May 5 2014, 7:00AM (UTC), ends on May 7 2018, 6:59AM (UTC).&quot;</td>
</tr>
<tr>
<td>job_id</td>
<td>Job ID</td>
<td>The job ID string.</td>
<td>job_id=&quot;5c1ace5c123 b3801207481f&quot;</td>
</tr>
<tr>
<td>created_by</td>
<td>Admin or user's username</td>
<td>The user who created the job in Exabeam.</td>
<td>created_by=&quot;admin&quot;</td>
</tr>
<tr>
<td>timestamp</td>
<td>Timestamp in UTC format</td>
<td>When the event took place.</td>
<td>timestamp=&quot;December 19 2018, 11:05PM (UTC)&quot;</td>
</tr>
<tr>
<td>start_time (optional)</td>
<td>Timestamp in UTC format</td>
<td>When the event started.</td>
<td>start_time=&quot;March 12 2019, 10:05PM (UTC)&quot;</td>
</tr>
<tr>
<td>end_time (optional)</td>
<td>Timestamp in UTC format</td>
<td>When the event ended.</td>
<td>end_time=&quot;March 13 2018, 12:05AM (UTC)&quot;</td>
</tr>
</tbody>
</table>