Copyright

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

Copyright ©2020 Exabeam, Inc. All Rights Reserved.

Trademarks

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

Patents

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

Other Policies

For information regarding Exabeam’s treatment of personally identifiable information, please review Exabeam’s current privacy policy at www.exabeam.com/privacy.
Table of Contents
Introduction ......................................................................................................................................... 4
Document Structure ............................................................................................................................ 5
What to Expect From Exabeam Validated Architectures ................................................................. 5
Product Selection ............................................................................................................................... 6
  Understand Your Organizations Cyber and Business Risks ........................................................... 6
  Create Use Cases That Align with the Risks or Functionality of the Tools ..................................... 7
  Choose Which Exabeam Product(s) Address These Use Cases .................................................... 7
Product Architecture ....................................................................................................................... 10
  Data Lake Standalone .................................................................................................................... 10
  Data Lake Clustered for Data Replication ....................................................................................... 11
  Data Lake Integration with Advanced Analytics........................................................................... 12
  Advanced Analytics Disaster Recovery ........................................................................................... 14
  Entity Analytics ............................................................................................................................... 15
  Case Management and Incident Responder .................................................................................. 16
  Case Management/Incident Responder Disaster Recovery ......................................................... 17
  Exabeam Security Management Platform ...................................................................................... 18
  Exabeam Security Management Platform Disaster Recovery ....................................................... 19
Data Collection .................................................................................................................................. 20
  Design Principles and Best Practices ............................................................................................. 20
    Events Per Second or Ingestion Volume? ...................................................................................... 20
    Growth ......................................................................................................................................... 22
    Implementation Size .................................................................................................................... 22
    Deployment Location ................................................................................................................... 22
    Other Considerations .................................................................................................................. 23
Appendix ............................................................................................................................................ 24
  Network Ports ................................................................................................................................. 24

Figures
Figure 1: Simple Risk to Detection Mapping .................................................................................... 7
Figure 2: Standalone Data Lake Architecture .................................................................................... 10
Figure 3: Data Replication Cluster Model .......................................................................................... 11
Figure 4: Data Lake and Advanced Analytics Integration ................................................................. 12
Figure 5: Basic Advanced Analytics Architecture .............................................................................. 13
Figure 6: Advanced Analytics Disaster Recovery Architecture ....................................................... 15
Figure 7: Advanced Analytics, Case Management, and Incident Responder Architecture .............. 16
Figure 8: Advanced Analytics, Case Management, and Incident Responder Disaster Recovery Architecture .......................................................................................................................... 17
Figure 9: Full Exabeam Security Management Platform ................................................................. 18
Figure 10: Full Exabeam Security Management Platform with Data Replication and Disaster Recovery ................................................................. 19
Figure 11: Exabeam Collectors ......................................................................................................... 20

Tables
Table 1: Exabeam Validated Architectures Explanation .................................................................... 6
Table 2: Example Data Sources ........................................................................................................... 21
Table 3: Network Ports ....................................................................................................................... 24
Introduction

Exabeam Validated Architectures are supported reference architectures that have been deployed in many environments and are designed for stability and efficiency. As Exabeam has multiple products, the validated architectures are designed to allow simple deployment for either standalone products or as a complete platform.

The Exabeam product suite consists of the following:

**Data Lake** - Unlimited collection and secure data storage without volume-based pricing

**Advanced Analytics** - The world’s most-deployed UEBA security solution — modern threat detection using behavioral modeling and machine learning

**Entity Analytics** - Behavioral analytics for internet-connected devices to complete your UEBA solution

**Incident Responder (Inc. Case Management)** - Add automation and orchestration to your security operations center to make your cyber security incident response team more productive

**Cloud Collectors** - Reliably collect logs from over 40 cloud services into Exabeam Data Lake, Exabeam Advanced Analytics, and any other SIEM to enhance your cloud security

**Exabeam Collectors** - Lightweight processes that are installed on machines (i.e. workstations, servers) to capture operational data such as hardware events, security system events, application events, operating system metrics, network packets, health metrics, and more

Exabeam Validated Architectures offer many different product configuration options depending on what products the organization purchases. As each product has its own validated architecture, it may simply be a case of adding one or more together, along with an understanding of how they connect to share information and log data. Within some Exabeam products, scalability is taken into account by the addition of additional nodes dependent on events per second (EPS) or log ingestion volume (Gb/day or Tb/day).

This whitepaper will provide an overview of validated architectures and will provide the information you need to enable their successful selection and deployment, design principles, best practice guidelines, and general information.
Exabeam Validated Architectures consist of four main focus areas:

1. Product selection
2. Standalone or multi-product architecture
3. Data collection components
4. Design principles and best practices

Product selection aligns an organization’s identified risks and use cases and determines which Exabeam products are required.

Standalone and multi-product covers the architecture recommended for Exabeam products, including intercomponent connectivity, clustering, and resiliency.

Data collection components cover the various methods for collecting data such as Syslog, Beats Collectors, and Exabeam Cloud Connectors.

Design principles and best practices apply to architecture as a whole and help you make informed decisions for your deployment.

What to Expect From Exabeam Validated Architectures

Please note the Exabeam Validated Architectures do not include deployment sizing or deployment technologies (physical vs virtual vs cloud) for the following reasons:

Deployment sizing requires a discovery session to understand use cases and organizational requirements around threat detection, compliance, and auditing, which all tend to be very customer specific and, other than number of nodes/appliances required, has no bearing on the actual deployment architecture itself. Once the data source EPS or volume has been identified, your Exabeam account team will be able to provide you with an indication of sizing. We touch on risks and use cases below in relation to product selection. However, the best practice and guidelines section will detail the level of information required for successful discovery.

Deployment technologies, such as physical appliance, virtual appliances, or cloud deployment, are purely implementation choices and as above have no bearing on the actual architecture.
What to Expect From Exabeam Validated Architectures

Exabeam Validated Architectures provide

<table>
<thead>
<tr>
<th>Not included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clustered and non-clustered deployment options</td>
</tr>
<tr>
<td>Diagrams of reference architecture</td>
</tr>
<tr>
<td>Guidelines to help make the right choice for you</td>
</tr>
<tr>
<td>Best practices for building your Exabeam deployment</td>
</tr>
</tbody>
</table>

Table 1: Exabeam Validated Architectures Explanation

Product Selection

The first steps in product selection and defining the architecture for your Exabeam solution are as follows:

1. Understand your organization’s cyber and business risks
2. Create use cases that align with the risks or functionality of the tools
3. Choose which Exabeam product(s) address these use cases

Understand Your Organization’s Cyber and Business Risks

For an organization that is looking to replace existing SIEM capabilities with an Exabeam solution, there is a good chance that you will have already performed a cyber and business risk assessment and determined how the current SIEM solution helps address the monitoring and mitigation of those risks. If you are embarking on a new security program and looking at Exabeam as your first security monitoring and incident response platform, a risk identification and mapping exercise must be conducted. This would include identification of risks to the business from both external and internal threats ranging from phishing attacks to insider threats. These risks should be mapped to the controls that are in place to help prevent the attack, followed by a further assessment of how these controls can provide suitable logs to the SIEM solution to aid detection and mitigation.

Exabeam products such as Advanced Analytics perform SIEM capabilities using a much more reliable method such as behavior analysis. Even if you have performed a previous risk assessment for you current SIEM, Exabeam recommends you revisit this to ensure any newly identified threats or previously undetectable threats are identified in line with the enhanced capability of Advanced Analytics.
Creating Use Cases That Align with the Risks or Functionality of the Tools

Traditionally SIEM tools were developed to meet demanding compliance requirements and centralized logging. Commonly, all information security and operational data sources were added to the SIEM to meet the compliance and subsequent data retention needs.

The fundamental problem with this approach was that the SIEM was very hard to use. A security analyst, whilst having all logs centrally, was inundated with noise and it became almost impossible to separate the events of interest, the signal, from the noise. This quickly led to event fatigue and analyst burnout and provided very little security value to an organization.

The modern SIEM has evolved and some have the ability to ingest logs from everything to meet compliance whilst being able to present a subset of those logs to the security or operations analyst. However, unless you have a pressing requirement to log everything, the recommended approach is to use a ‘top-down, use case-driven approach,’ mapping a risk to a use case, identifying the required log source(s), and then sending those logs to the SIEM or Advanced Analytics depending on your existing or proposed technologies as per the diagram below.

![Figure 1: Simple Risk to Detection Mapping](image)

Choose Which Exabeam Product(s) Address These Use Cases

**Data Lake** – The first step of collecting logs centrally starts with the Log Manager component of a SIEM such as Exabeam Data Lake, which uses industry-standard methods of log collection e.g. Syslog, Exabeam Collectors, and Exabeam Cloud Connectors. Logs are sent to Data Lake, where they are normalized, aggregated, and data enriched. Data Lake presents a single glass-pane view of gathered logs, allowing searching, correlation, dashboards, and reporting. Data Lake is based on Elastic architecture and utilizes technologies such as Hadoop, Kafka, and Mongo. The Exabeam implementation of Elastic has been heavily customized to provide an information security focus and includes useful features such as security-centric correlation rules and centralized collector management.
Product Selection

As Exabeam Data Lake is not priced on log volume ingestion, it allows customers to add all data sources required to satisfy use cases.

Although an organization is no longer constrained by log volume costs, which previously may have restricted which sources to add, as per the previous section, data sources should only be added where required to meet a use case. Throwing every data source at a SIEM is counterproductive.

Data Lake consists of one or more physical or virtual appliances known as nodes. Multiple nodes are known as a cluster and a cluster must consist of the same type of nodes, i.e. you cannot mix virtual and physical in the same cluster. Where three or more nodes are provisioned, data is stored in indexes and indexes are split into shards. Data is stored twice, in two different shards, and the shards are arranged so that data is distributed around the Data Lake clusters with copies of the same data always being stored on different nodes within the cluster. In that way, a node can lose a disk, or a cluster can lose an entire node and no data loss will take place.

**Advanced Analytics** – Although Data Lake has correlation rule capabilities to detect ‘known knowns,’ like any legacy SIEM to enable detection of more complex threats such as credential theft, compromised users, insider threat, and lateral movement, behavior analytics is a critical technology to help detect and protect an organization from these threats. Exabeam Advanced Analytics platform receives logs forwarded from Data Lake or another vendor SIEM. As a side note, Advanced Analytics only requires a subset of logs typically gathered at the log manager component. These are also aligned with the use cases required.

Similar to Data Lake, Advanced Analytics can consist of one or more nodes, including a master node and worker nodes. The number of nodes required is dependent on events per second and retention. For larger implementations, dedicated log ingestion (LIME) nodes can be added.

**Entity Analytics** – Threats move laterally through a network, leveraging users and machines in their search for high-value data. Connected assets like medical equipment, machinery, and power grid infrastructure are an easy target. Assets require the same monitoring as humans. Entity Analytics establishes baseline behavior using communication patterns, ports and protocols, and operating activity — automatically identifying irregular activities indicative of a security incident.
**Incident Responder/Case Management** – Detecting known bad behavior or anomalous behavior is only part of the overall detection and response function. The ability to automate responses with SOAR (security orchestration and response) can save an analyst critical time in investigating and triaging an incident. For example, investigating a phishing or ransomware email would traditionally take around an hour whilst the analyst gathers any artifacts and performs individual investigation such as IP reputation lookup, analysis of attached files, etc. With Exabeam Incident Responder, an alert triggered from Advanced Analytics for a suspected phishing email can invoke a playbook with a set of actions that can concurrently run and then perform an action depending on the results such as deleting the email from a user’s Office365 mailbox. These playbooks can reduce triage time to minutes, saving valuable investigation time and more importantly risk exposure to the user.

**Cloud Connectors** – Cloud Connectors – Exabeam Cloud Connectors allow logs to be gathered from over 40 different cloud services. A stand-alone cloud connector server is required to collect the logs and then forward to Data Lake (or Advanced Analytics) and can be provisioned as a VM or installed on a standalone Exabeam physical appliance.

**Exabeam Collectors** – These are lightweight processes that are installed on machines (i.e. workstations, servers) to capture operational data such as hardware events, security system events, application events, operating system metrics, network packets, health metrics, etc. The connectors read from one or more event logs, Gzipped logs, and filters the events based on user-configured criteria. The connectors watch the event logs and send any new events in real time. The read position is persisted in order to allow the connectors to resume after restarts. Collectors are uniquely managed centrally from within Data Lake.
Product Architecture

The following section details some of the options for Exabeam products and covers the following:

- Standalone
- Clustered for data replication or disaster recovery
- Integration with other Exabeam products

Data Lake Standalone

Exabeam Data Lake can be used as a standalone traditional log management and SIEM platform. Data Lake uses a heavily customized version of Elastic and accepts device logs such as Syslog or Exabeam collectors. For further event enrichment, Exabeam recommends that Data Lake is configured to pull Active Directory information.

Figure 2: Standalone Data Lake Architecture

Where an organization has a large infrastructure or multiple site locations, Data Lake can be implemented in a cross-cluster search model where up to seven clusters can be searched from a single ‘master’ cluster accessed by the security operations team. Discuss this option with your Exabeam account team.
Data Lake Clustered for Data Replication

For customers who want a level of data resiliency, Data Lake can forward all events (both raw and parsed) to a second Data Lake cluster that can then be included in an organization’s disaster recovery program.

Figure 3: Data Replication Cluster Model
Data Lake Integration with Advanced Analytics

The integration with Exabeam Advanced Analytics is straightforward and, as a basic requirement, Data Lake simply forwards logs to Advanced Analytics using Syslog.

It should be noted that not every log source sent to Data Lake is required for Advanced Analytics. Logs should be forwarded in line with the Advanced Analytics use cases.

Figure 4: Data Lake and Advanced Analytics Integration
**Advanced Analytics**

Exabeam Advanced Analytics can be used with an existing SIEM implementation, with Exabeam Data Lake, or can ingest logs direct via Syslog, API, or Cloud Connectors. Logs gathered via Exabeam collectors must first go to Data Lake before forwarding to Advanced Analytics. Advanced Analytics may consist of one or more nodes depending on log volume received and also has the option of disaster recovery. Raw logs are normally stored on the upstream log management solution, but variable retention can be scoped for the Advanced Analytics platform if desired. Depending on size and configuration, an Advanced Analytics cluster could consist of master nodes, worker nodes (processing or storage), dedicated LIME nodes, and nodes for Entity Analytics, Case Management, and Incident Responder. (These will be discussed later).

![Figure 5: Basic Advanced Analytics Architecture](image-url)
Advanced Analytics Disaster Recovery

For customers who require a level of resiliency with their Advanced Analytics solution, Exabeam has a disaster recovery option.

In a disaster recovery scenario, Advanced Analytics content is replicated continuously (the default is every hour) from the primary to the secondary site, including:

- Logs/events – The active cluster fetches logs from SIEM and/or receives the logs via Syslog. Once the logs are parsed, the events are replicated to the standby 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 (e.g. EDS configuration, users, and roles are in the database).
- Context – Contextual data, such as users, assets, service accounts and peer groups.
- User Generated Data – Comments, approved sessions, watchlists, starred sessions, saved searches, and whitelists stored in the Mongo database.

The two-cluster scenario employs an active-passive disaster recovery architecture with asynchronous replication. With this approach, you maintain a primary and secondary set of Advanced Analytics clusters in separate locations. In cases of a failure at the primary site, you can failover to the secondary site.

The active and standby clusters should have identical configurations in terms of number of nodes.

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 standby cluster every five minutes. This is initiated as a pull on the secondary, fetching the logs from the active cluster.

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

Entity Analytics is an add-on feature to Advanced Analytics and only requires an additional node (or nodes), depending on the number of events or log volume as with Advanced Analytics. Architecture remains the same as Advanced Analytics.
Case Management and Incident Responder
Similar to the Entity Analytics, Case Management and Incident Responder are additional nodes that are added to the Advanced Analytics architecture at the time of sizing. The integration of the products on the same platform allows for a single console view so an analyst can see notable users or notable entities and then be able to create cases and perform triage and automation from one console.

Figure 7: Advanced Analytics, Case Management, and Incident Responder Architecture
Case Management/Incident Responder Disaster Recovery
Case Management or a combined Case Management and Incident Responder replicates the following across the disaster recovery system:

- 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)

Figure 8: Advanced Analytics, Case Management, and Incident Responder Disaster Recovery Architecture
Exabeam Security Management Platform
The full stack of Exabeam products is collectively known as the Security Management Platform to provide a full end-to-end SIEM and SOAR platform.

Figure 9: Full Exabeam Security Management Platform
Exabeam Security Management Platform Disaster Recovery

The data replication and disaster recovery features mentioned above are also available across the entire platform when deployed together.

Figure 10: Full Exabeam Security Management Platform with Data Replication and Disaster Recovery
Data Collection
Data Lake is able to consume logs from multiple sources using various methods such as Syslog, API, Cloud Connectors, and Exabeam Collectors.

- Syslog – Data Lake supports forwarding from devices using the RFC3164 and RFC5424 standards
- API – Data Lake supports pulling from external sources
- Cloud Connectors – Exabeam Cloud Connectors allow logs to be gathered from over 40 different cloud services. A stand-alone cloud connector server is required to collect the logs and then forward to Data Lake (or Advanced Analytics) and can be provisioned as a VM or installed on a standalone Exabeam physical appliance
- Exabeam Collectors are able to collect Windows events, log files, and database events and are uniquely managed centrally from within Data Lake

Design Principles and Best Practices
In this section we will discuss some of the design principles, from deployment location considerations to Exabeam Best Practice guidance on topics such as data source selection, growth factors, etc.

EVENTS PER SECOND OR INGESTION VOLUME?
Once you have identified which Exabeam products match your use cases and requirements, and you have identified which data sources you want to log, the next step is to understand the principles behind the correct sizing of your Exabeam solution.
Other SIEM vendors will happily take a figure of 500GB per day log volume because their solutions: a) don’t perform any analytics or machine learning or b) charge on log ingestion volume (and happily encourage you to log everything). Exabeam Advanced Analytics is a far more powerful security solution and must take into consideration different event types and event sizes. This enables both an organization and Exabeam to ensure a correctly-sized implementation is made to match expectations and desired outcomes.

By choosing events per second (EPS) and a list of data sources as our sizing preference, it allows a much more accurate sizing and takes into consideration important factors such as high-volume feeds (HVFs), event byte sizes, and what is classified as session data or sequence data. These are all important factors to consider as each may be processed differently within the platform, higher volumes of one over the other may require additional worker nodes, etc.

By their very nature, events create volume, and the larger the individual event, the greater the volume. If we look at some generic examples, it’s easy to see how this can lead us to wildly differing and inaccurate sizing:

- 3000 EPS @ average event size of 800b = 212GB/Day
- 3000 EPS @ average event size of 1500b = 398GB/Day

The above figures would assume that 80 percent of the events are HVFs. This also results in a difference in the number of appliances required. By being generic we could either be undersized or oversized.

Instead, we take a selection of typical log sources and break them down to be more granular as per the table below:

<table>
<thead>
<tr>
<th>Data Source</th>
<th>EPS</th>
<th>Event Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkpoint</td>
<td>600</td>
<td>230</td>
</tr>
<tr>
<td>Cisco ACS</td>
<td>100</td>
<td>880</td>
</tr>
<tr>
<td>Database</td>
<td>200</td>
<td>1050</td>
</tr>
<tr>
<td>DNS</td>
<td>100</td>
<td>400</td>
</tr>
<tr>
<td>Proxy</td>
<td>150</td>
<td>1100</td>
</tr>
<tr>
<td>VPN</td>
<td>150</td>
<td>300</td>
</tr>
<tr>
<td>MS Exchange</td>
<td>300</td>
<td>350</td>
</tr>
<tr>
<td>MS Office 365</td>
<td>200</td>
<td>1270</td>
</tr>
<tr>
<td>Symantec SEP</td>
<td>100</td>
<td>310</td>
</tr>
<tr>
<td>UNIX</td>
<td>100</td>
<td>400</td>
</tr>
<tr>
<td>Windows General</td>
<td>1000</td>
<td>1800</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>3000</td>
<td>972 Average</td>
</tr>
</tbody>
</table>

*Table 2: Example Data Sources*
So now with the same 3000 EPS, we have 258GB/Day, an average event byte size of 972, and only 38 percent of those sources are considered as HVFs. We can now more accurately size the Exabeam solution.

Exabeam encourages customers to perform a discovery workshop to identify the data source types, vendor, model, and how many EPS are generated. Whilst there will be occasions where gaining this information may be difficult, such as a green field security deployment, Exabeam will be more than happy to take part in these discovery workshops where our skilled and knowledgeable team will assist.

**GROWTH**

One area commonly overlooked when sizing a solution is future growth of the organization. Growth factors to take into consideration which affect sizing are:

- Tech refresh, e.g. firewall replacement with next gen–firewalls = more and bigger events
- Organization expansion (year-on-year growth)
- Acquisitions of other business
- Mergers with other organizations
- Consolidation of physical locations

All of the above can result in an increase of log volumes affecting EPS and storage capacities for log retention. If your organization is facing year-on-year growth, don’t forget to calculate using a compound formula!

**IMPLEMENTATION SIZE**

At Exabeam, a deployment is categorized in one of two sizes for either Data Lake, Advanced Analytics, or Security Management Platform:

- Small = 1 – 19 appliances
- Large = 20+ appliances

**DEPLOYMENT LOCATION**

Where Exabeam products consist of several nodes (clusters), these must be deployed in the same physical rack or subnet, depending on whether physical or virtual.

For deployments that include data replication or disaster recovery functionality, whilst deploying clusters in different locations is supported, the bandwidth between the two locations must be able to support the replication between the two clusters.

When Data Lake is deployed in a cluster, a load balancer is a mandatory requirement to ensure that Syslog events are evenly distributed across nodes for ingestion. Logs collected by Exabeam Collectors are load-balanced within the collectors and written directly to the Data Lake Kafka bus and are not sent via external load balancers.
Product Architecture

Where Exabeam Cloud Connectors are required as part of the design, a dedicated server must be provisioned using either a VM or a physical Exabeam appliance. For performance reasons, this cannot co-exist with another shared VM or appliance.

OTHER CONSIDERATIONS
An Active Directory connection is a key requirement for Advanced Analytics and Data Lake as it provides rich context used in event enrichment and peer grouping. It also presents useful information in the dashboards to enable analysts to make quicker assumptions and therefore minimize triage time. As the information is updated every 24 hours, an active connection from the product to Active Directory should be maintained and requires a read-only account with Bind DN authenticated connection. Using anonymous bind may result in incomplete directory information such as missing groups etc.
## Appendix

### 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>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Network</td>
<td>Exabeam DL/AA/CM/IR</td>
<td>22/TCP</td>
<td>SSH</td>
<td>CLI administration</td>
</tr>
<tr>
<td>User Network</td>
<td>Exabeam DL/AA/CM/IR</td>
<td>8484/TCP</td>
<td>HTTPS</td>
<td>UI administration and general usage of Exabeam</td>
</tr>
<tr>
<td>Log Sources</td>
<td>Exabeam DL/AA</td>
<td>514/TCP/UDP</td>
<td>Syslog</td>
<td>Direct log collection</td>
</tr>
<tr>
<td>Exabeam Collectors</td>
<td>Exabeam DL</td>
<td>8484/TCP, 9092/TCP &amp; 9093/TCP</td>
<td>HTTPS</td>
<td>Local log collection from file, Windows events or DBs</td>
</tr>
<tr>
<td>Exabeam DL/AA/CM/IR</td>
<td>DNS Servers</td>
<td>53/UDP</td>
<td>DNS</td>
<td>Name resolution</td>
</tr>
<tr>
<td>Exabeam DL/AA/CM/IR</td>
<td>AD or LDAP Servers</td>
<td>389/TCP or 636/TCP</td>
<td>LDAP &amp; LDAPS</td>
<td>Collecting context</td>
</tr>
<tr>
<td>Exabeam DL/AA/CM/IR</td>
<td>NTP Servers</td>
<td>123/UDP</td>
<td>NTP</td>
<td>Time</td>
</tr>
<tr>
<td>Exabeam DL/AA/CM/IR</td>
<td>SMTP Server</td>
<td>25/TCP</td>
<td>SMTP</td>
<td>Notifications</td>
</tr>
<tr>
<td>Exabeam AA/CM/IR</td>
<td>Exabeam DL</td>
<td>514/TCP/UDP</td>
<td>Syslog</td>
<td>Forward logs from Data Lake to Advanced Analytics</td>
</tr>
<tr>
<td>Exabeam DL</td>
<td>Exabeam AA</td>
<td>514/TCP</td>
<td>Syslog</td>
<td>Forwards logs</td>
</tr>
<tr>
<td>Exabeam IR</td>
<td>Internal Email Server</td>
<td>143/TCP or 993/TCP</td>
<td>IMAP &amp; IMAPS</td>
<td>Email</td>
</tr>
<tr>
<td>Exabeam IR</td>
<td>Internal Email Server</td>
<td>995/TCP</td>
<td>POP</td>
<td>Email</td>
</tr>
<tr>
<td>Exabeam IR</td>
<td>Internet</td>
<td>43/TCP</td>
<td>HTTP</td>
<td>Whois</td>
</tr>
<tr>
<td>Exabeam AA/DL</td>
<td>Cloud Services</td>
<td>443/TCP</td>
<td>HTTPS</td>
<td>Connection via Cloud Connectors for “Cloud” logs</td>
</tr>
<tr>
<td>Exabeam AA/DL</td>
<td>Exabeam SIP</td>
<td>443/TCP</td>
<td>HTTPS</td>
<td>Connection for Exabeam TIP feeds</td>
</tr>
</tbody>
</table>

*Table 3: Network Ports*

### Legend

- AA – Advanced Analytics
- DL – Data Lake
- IR – Incident Responder
- CM – Case Manager