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 Data Lake Release Notes - Version SMP 2020.3 (I35)
Published Dec 11, 2020

1. What's New ............................................................................................................................. 4
   1.1. Exabeam Hardening For CSRF And CORS ................................................................. 4
   1.2. Search Interface Refresh With Filtered Searches And Export Options ...................... 4
   1.3. Audit Log Management ................................................................................................. 6
   1.4. Parser Management UI ............................................................................................... 6
   1.5. Data Input From External Kafka Source ...................................................................... 6
   1.6. Support For Generic SAML SSO .................................................................................. 6
   1.7. Platform Deployment Efficiency Improvement ............................................................ 6
   1.8. Exabeam Advanced Analytics As Site Collector Destination ....................................... 6
   1.9. CentOS 8 And RedHat 8 Support For Data Lake Collector Agents .............................. 6
2. Fixed Issues In Data Lake SMP 2020.3 DL-I35 GA ................................................................. 7
   2.1. Issues Fixed In Data Lake SMP 2020.3 DL-I35.6 Patch Release ................................. 7
3. Known Issues In Data Lake SMP 2020.3 DL-I35 GA ............................................................. 8
1. What's New

The SMP 2020.3 release of Data Lake arrives with some very powerful and handy use cases for the Security Analyst in addition to other system stability and maintainability improvements.

Data Lake I35 features include:

- Filtered searches to narrow large data pools before you query and enhancements and layout improvements to visually organize, highlight, and share query results
- User activity logging within Data Lake
- Parse management
- Support for SAML 2.0 SSO
- Performance improvement in node deployment
- Support for Exabeam Advanced Analytics as a log destination
- Support for CentOS 8 and RedHat 8 collector agents

1.1. Exabeam Hardening for CSRF and CORS

Security enhancements have been added to Data Lake i34.6 and i35. If you have i33 or earlier, we recommend either manually completing the hardening steps given in Exabeam Operational Hardening or upgrade to Data Lake i34.6 or later.

The Exabeam Security Management Platform (SMP) has additional security configurations that can be enabled for stricter controls and data protection. Exabeam has enabled protections to specific releases against Cross-Site Request Forgery (CSRF) and Cross-Origin Resource Sharing (CORS) by default.

This improves the default security of the environment for all Exabeam services. These protections may affect API calls to the Exabeam SMP. Please follow instructions given in Exabeam Operational Hardening if you have affected scripts.

For Exabeam SaaS deployments that use Exabeam Advanced Analytics as your Exabeam Cloud Connector identity provider (IdP), Exabeam will automatically update your Cloud Connector to v.2.5.86 or later to ensure compatibility with the security configuration.

No manual configuration is needed for deployments with the following versions or later:

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

For more information, please see Exabeam Operational Hardening.

1.2. Search Interface Refresh with Filtered Searches and Export Options

Exabeam has refreshed its Search interface to improve your query experience.
In addition to using time constraints to narrow the amount of data to search, you can apply filters using context tables to optimize your queries. Filtered searches are now available in all Data Lake features for running custom queries, offering the ability to search against IOCs list and enable reporting granularity. Click **Context table** under the **Search** field to create filters.

When you have pinpointed logs of interest, you can now readily export individual raw logs to distribute among team analysts. Each log in raw and enhanced view offers exports of log text, hyperlink, or as a separate web browser tab.

In Data Lake I35, you will find:

- Structured view
- Category specific fields first
- Raw messages always visible
- More clear fonts and colors
- Metadata and less important fields placed at the end
1.3. Audit Log Management
Exabeam user audit logs can now be stored and searched within Data Lake. User actions like searches, operating system level activities, and dashboard creation, are tracked. Audit event logs can be handled like typical Data Lake logs so you can create log trails after every:

- search
- visualizations
- dashboards
- report executed

For more information, see Audit Log Management in Data Lake in the Data Lake Administration Guide.

1.4. Parser Management UI
In Data Lake i35, you can select the parsing policy that determines whether the system prioritizes accurate parsing of all ingested raw logs, events per second throughput, or a balance of both. Learn more about parser policies. For more information, see Parser Management in the Parser Troubleshooting Guide.

1.5. Data Input from External Kafka Source
Data Lake can now ingest event logs from your own Kafka sources outside. Data is sent from the external Kafka source directly to the Exabeam Site Collector. For more information, see Exabeam Site Collector Guide.

1.6. Support for Generic SAML SSO
Exabeam has enabled a generic authentication option to support SAML 2.0 SSO. You can use your preferred single sign-on (SSO) tool of choice. API information is available in the Exabeam Community. For more information, see Configuring Single Sign-on and Multifactor Authentication in the Data Lake Administration Guide.

1.7. Platform Deployment Efficiency Improvement
With improvements the Exabeam Data Services and other system components, expect faster node deployments.

1.8. Exabeam Advanced Analytics as Site Collector Destination
Exabeam Site Collector can now be configured to forward logs to Exabeam Advanced Analytics destinations deployed on appliances and cloud platforms. For more information about Site Collector, please see Exabeam Site Collector.

1.9. CentOS 8 and RedHat 8 Support for Data Lake Collector Agents
Data Lake log ingestion options now include Exabeam log collector agents that run on CentOS 8 and Redhat 8.
2. Fixed Issues in Data Lake SMP 2020.3 DL-i35 GA

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PLT-10854</td>
<td>When upgrading, the site collector files are not included and may cause the upgrade to fail.</td>
</tr>
<tr>
<td>LMS-13589</td>
<td>The expand view icon for event logs appears on top of the event date and time.</td>
</tr>
<tr>
<td>LMS-13276</td>
<td>PDF export fails when fields are missing for a given report.</td>
</tr>
</tbody>
</table>

2.1. Issues Fixed in Data Lake SMP 2020.3 DL-i35.6 Patch Release

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLA-3137</td>
<td>Some customers may experience Data Lake’s Visualization dashboard not presenting correct results if searches are amended without being saved.</td>
</tr>
<tr>
<td>DLA-3066</td>
<td>Data Lake export was limited to 10,000 records per single formatted output. Now customers can export up to 1,000,000 records.</td>
</tr>
</tbody>
</table>
3. Known Issues in Data Lake SMP 2020.3 DL-i35 GA

DLA-3148  Exabeam Data Lake collector beats upgrades follow strict compatibility. If you’re upgrading your agent collectors (beats), navigate to Settings > Collector Management > Upgrade > Choose a New Version menu and then select beats version 2.0.4 only.

Site collector upgrading is not supported. The site collector Data Forwarder cannot be upgraded to any version.