Copyright

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

Copyright ©2020 Exabeam, Inc. All Rights Reserved.

Trademarks

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

Patents

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

Other Policies

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

1. What's New ............................................................................................................................. 5
   1.1. Exabeam Hardening For CSRF And CORS ................................................................. 5
   1.2. Get Notified When A Parser Is Disabled ................................................................. 5
   1.3. An Easier Way To Get New Content ......................................................................... 5
   1.4. Administrative Settings Get Dark Mode ................................................................... 6
2. Known Issues .......................................................................................................................... 7
3. Issues Fixed In Advanced Analytics I54.5 (General Availability) ........................................ 8
   3.1. Issues Fixed In Advanced Analytics I54.5.1 (First Customer Shipment) .............. 8
   3.2. Issues Fixed In Advanced Analytics I54.5.2 ........................................................... 9
1. What's New

1.1. Exabeam Hardening for CSRF and CORS

Security enhancements have been added to Advanced Analytics i53.6 and i54.5: If you have i52 or earlier, we recommend either manually completing the hardening steps given in Exabeam Operational Hardening or upgrade to Advanced Analytics i53.6 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. Get Notified When a Parser is Disabled

To protect your system from going down and ensure that it keeps processing data in real time, Advanced Analytics detects slow, inefficient parsers, then disables it. You should be informed about this important system information when it happens.

From Advanced Analytics i54, a system health alert notifies you when Advanced Analytics disables a parser. The alert describes which parsers are currently disabled, on which node, and recommended actions you can take.

You can still find a list of all disabled parsers in the System Health page, under the System Optimization tab.

Exabeam Documentation: System Health Alerts for Disabled Parsers

Exabeam Documentation: Disabled Parsers

1.3. An Easier Way to Get New Content

Wave goodbye to command line. You can upload and install new content directly in Advanced Analytics.

With Exabeam's new cloud service, you don't need to use Exabeam Content Installer or manually restart internal engines. In Advanced Analytics Content Update settings, you can retrieve the latest available content packages, both general Exabeam releases and custom fixes you request, from the cloud in real
time. Just hit install, and you’re done. You can even automatically check for new updated content and install them on a daily or weekly basis. If you have an environment that can't access the internet, you can't connect to the cloud to get the latest updates, but you can still find the latest content packages on the Exabeam Community and upload the ZIP files to Advanced Analytics.

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

Exabeam Documentation: Upload a Content Package

Exabeam Documentation: Manually Install a Content Package

Exabeam Documentation: Automatically Install Content Packages

1.4. Administrative Settings Get Dark Mode
We’re plugging the holes in your Dark Mode experience.

When Dark Mode was introduced in version i52, it was unavailable for most administrative tasks, including the Metrics and System Health pages, and most settings. Now, Dark Mode is available for these other pages, except the Metrics page. The Metrics page is still unavailable in Dark Mode.
2. Known Issues

INF-7229 You may receive a health alert stating that Calico issues were detected. This health alert triggers when Calico doesn’t properly remove old workload endpoints.

To solve this:

1. In /opt/exabeam/bin/plt/, edit clean_weps.py:
   - To the top of the file, add:
     ```python
     from time import script
     ```
   - Under def clean_weps, add a sleep function:
     ```python
     sleep(120)
     ```
     For example:
     ```python
def clean_weps():
    endpoints_1 = get_endpoints()
    weps_1 = get_weps()
    sleep(120)
    endpoints_2 = get_endpoints()
    weps_2 = get_weps()
```

2. Source the shell environment:
   ```bash
   source /opt/exabeam/bin/shell-environment.bash
   ```

3. Run clean_weps.py.
3. Issues Fixed in Advanced Analytics i54.5 (General Availability)

INF-7047  There was an error adding a worker node to clusters with three or more nodes, where at least one of the nodes is a Log Ingestion Messaging Engine (LIME) node and the cluster has a Hadoop Distributed File System (HDFS) High Availability (HA) setup; specifically, clusters with:

- One master node and two LIME nodes
- One master node, one LIME node, and one worker node
- One master node, one Case Manager node, one worker node, and one LIME node
- One master node, one LIME node, and you added two or more worker nodes, one at a time

The inventory files that list the nodes in the NameNode and JournalNode groups were incorrectly changed and moved to a different host. Now, if a cluster already has three or more nodes and an HDFS HA setup, the inventory file isn’t changed.

EXA-31543  In some environments, the Analytics Engine couldn’t begin processing because some connection threads to the MongoDB database expired while the Analytics Engine was initializing. The MongoDB database loaded models in parallel to maximize efficiency, but while doing this, surpassed the number of concurrent connection requests it could make to the Analytics Engine. Now, the MongoDB database limits the concurrent connections it uses to load models in parallel.

EXA-31692  Abnormal first access-type rules triggered incorrectly, when a user’s activity was normal. The corresponding model wasn’t trained correctly because a parameter in the model definition was miscalculated. The calculation for that parameter has been corrected and tuned.

EXA-31909  Under certain conditions, the anomaly factor wasn’t calculated and inflated risk scores because of other Data Science (DS) server issues. These issues have been resolved.

EXA-31302  Some pages, like Health Alerts settings, Account Lockouts watchlist, and some user Smart Timelines™, were slow or failed to load because parallel processes in Advanced Analytics Restful Web Services inefficiently queried the MongoDB database multiple times. We reduced or batched these queries to optimize the time they take to run.

EXA-31463  For some deployments, the MongoDB database ran out of disk space because it failed to automatically purge data when it reached 85 percent capacity or after the 180 day default retention period. The database failed to identify data it should purge because of a missing database index. Now, the database ensures that the index exists before purging.

EXA-31639  If a user executed a Windows account switch, the accounts they switched to didn’t appear next to their name in their profile because Advanced Analytics Restful Web Services fetched account information from the incorrect MongoDB database collection. Now, Advanced Analytics Restful Web Services fetches from the correct collection.

EXA-31945  A user’s account usernames didn’t appear next to their name in their profile because Advanced Analytics Restful Web Services fetched account information from the incorrect MongoDB database collection. Now, Advanced Analytics Restful Web Services fetches from the correct collection.

EXA-31834  When you navigated from Splunk to Advanced Analytics, the Home page couldn’t load because Advanced Analytics was fetching configurations it couldn’t access from Splunk. These configurations have been moved to a file that Advanced Analytics can access wherever it loads.

3.1. Issues Fixed in Advanced Analytics i54.5.1 (First Customer Shipment)

EXA-31656  In some environments, it was possible that Advanced Analytics didn’t display new data because of a deadlock that occurs when ingesting data.

A Log Ingestion and Messaging Engine (LIME) service, LogParser, failed to send internal Akka messages and notify other LIME services about its parsing progress or when it’s done parsing. This happened when LogParser closes over the Akka context method in threads outside the one running the actor. To solve this, LogParser behaviour was tuned so it doesn’t close over the Akka context method.
### 3.2. Issues Fixed in Advanced Analytics i54.5.2

| EXA-32163 | Some Advanced Analytics pages were vulnerable to cross-site scripting attacks, which used specially crafted event logs to execute scripts. This issue has been resolved. |