

Configure Incident Responder

Exabeam Security Management Platform - Version SMP 2020.3 (IR i54)

Publication date February 18, 2021

Exabeam

1051 E. Hillsdale Blvd., 4th Floor
Foster City, CA 94404

650.209.8599

Have feedback on this guide? We'd love to hear from you!

Email us at docs@exabeam.com

Disclaimer: Please ensure you are viewing the most up-to-date version of this guide by visiting the [Exabeam Documentation Portal](#).

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 ©2021 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. Test Your Service	4
2. Configure A Service	5
3. Edit A Service You Configured	6
4. Disable A Service	7
5. Upload A Custom Service	8
6. Delete A Custom Service	9
7. Add Case Manager And Incident Responder To Advanced Analytics Disaster Recovery	10
7.1. 1. Stop The Replicator	10
7.2. 2. Upgrade The Passive And Active Advanced Analytics Clusters	10
7.3. 3. Add Case Manager To Advanced Analytics	11
7.4. 4. Configure Disaster Recovery On The Advanced Analytics And Case Manager Passive Clusters	12
7.5. 5. Start The Replicator	13

1. Test Your Service



Ensure the service you [configured](#) or [uploaded](#) is working correctly. You create a new test incident, run the service in the workbench, then view the results.

If you have a SaaS deployment, please contact your Technical Account Manager.

1. Ensure that you [configured](#) the service you're testing and you can access the command line interface (CLI).
2. Manually [create](#) a test incident. The information you enter doesn't need to be accurate.
3. Manually [run](#) an action supported by the service you're testing, and ensure you enter the input values you wish to check, like IP addresses, domain, and URLs.
If the action runs successfully, it appears in the workbench **ACTIONS** tab with a  check mark, and you see its output in the workbench.
4. (Optional) To debug the results, log into the CLI and view the results in `/opt/exabeam/data/logs/soar/python-action-engine/pythonActionEngine.log`



2. Configure a Service

Integrate a [service](#) with Incident Responder to gather the data needed to run [actions](#) and [playbooks](#). This service is usually one your organization already uses.

1. In the navigation bar, click the menu , select **Settings**, then navigate to **Automation > Services**.
2. Select a service:
 - To configure a specific service, hover over a tile, then click **CONFIGURE**. Use the search by vendor or filter by action to find a service.
 - To manually provide the relevant information for a service, click **Configure a new service** .
3. Enter the information. They may vary based on service.
 - **Service** – Select the service you wish to integrate.
 - **Service name** – Give the service a unique name.
 - **(Optional) Description** – Describe the service.
 - **(Optional) Owner** – Enter the email address of a person or group in your organization who's responsible for the service.
4. To validate the source, select **TEST CONNECTIVITY**.
5. Select **CREATE SERVICE**.



3. Edit a Service You Configured

Change how you configured a service.

1. In the navigation bar, click the menu , select **Settings**, then navigate to **Automation > Services**.
2. Select the **Configured** tab.
3. Hover over a service, then click **Edit Configuration**  .
4. Change the fields.
5. To validate the configuration, select **TEST CONNECTIVITY**.
6. Select **SAVE**.

4. Disable a Service

Disable a service you previously [configured](#). Once you disable a service, you can't use it in an [action](#) or [playbook](#).

1. Remove the service from any playbooks. If you disable a service that's used in a playbook, that playbook may run incorrectly.
2. In the navigation bar, click the menu , select **Settings**, then navigate to **Automation > Services**.
3. Select the **Configured** tab.
4. Hover over a service, then select **Delete Configuration** .
If you disable a service and it is still part of a playbook, you are warned that the "playbook contains errors" when you run the playbook.



5. Upload a Custom Service

If you created your own service, upload the ZIP file to Incident Responder .

You can create and upload two types of custom services: one you develop from scratch, and one that customizes an existing third-party service. If you upload a custom service that customizes an existing third-party service, all related actions and playbooks will start using this custom service.

If you create your own service from scratch, without using [Exabeam Action Editor](#), ensure your [ZIP file](#) includes certain components. If you introduce any Python dependencies, you must include any Python modules as Python wheels and a `requirements.txt` file containing these wheels. Place the `requirements.txt` file under the `python_dep` directory.

You can't upload the same custom service more than once. To edit a custom service, delete the service, then upload it again.



1. In the navigation bar, click the menu , select **Settings**, then navigate to **Automation > Services**.
2. Click **Upload service package** .
3. Click **UPLOAD PACKAGE**, then upload a ZIP file, no more more than 10MB. If the custom service changes or removes existing actions, playbooks that use these actions may not run as expected.
4. Click **SUBMIT**. The service is added to the list with a **Custom** label.

6. Delete a Custom Service

Delete a custom service you previously [uploaded](#).

You can create and upload two types of custom services: one that you've developed from scratch, and one that customizes an out-of-the-box service. If you delete a custom service that customizes an out-of-the-box service, all related actions and playbooks will return to using the out-of-the-box service.

You can only delete a custom service. You can't delete an out-of-the-box service, but you can [disable](#) ones you configured.

1. Ensure that you're not using the custom service in any playbooks. If you delete a service that's used in a playbook, that playbook may run incorrectly.
2. In the navigation bar, click the menu , select **Settings**, then navigate to **Automation > Services**.
3. Hover over the service, then select the trash .
4. Click **DELETE**.

Readd Case Manager and Incident Responder to Advanced Analytics Disaster

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.

7.1. 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:

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

4. On the active cluster, stop the replicator:

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

7.2. 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.

- 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).

- Change the permission of the file:

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

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

- To avoid accidentally terminating your session, initiate a screen session.

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

- 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.

- 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
```

7.3.3. Add Case Manager to Advanced Analytics

- SSH to the primary Advanced Analytics machine.

- Start a new screen session:

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

- When asked to make a selection, choose **Add product to the cluster**.

- 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
Choices: ['1', '2', '3', '4', '5', '6', '7', '8', '9', '10', '11', '12',
'13', '14', '15', '16']: default (1): 4
```

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.

7.4. 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"
    FilePattern = [ ".evt.gz" ]
  }
  Enabled = true
}
```

8. Start the replicator:

```
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**.

7.5. 5. Start the Replicator

On the active cluster, start the replicator:

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