Configure Incident Responder

Publication date October 30, 2020
# Table of Contents

1. Add A Service ........................................................................................................................... 3
2. Edit A Service ........................................................................................................................... 4
3. Delete A Service ....................................................................................................................... 5
4. Upload A Custom Service ......................................................................................................... 6
5. Delete A Custom Service .......................................................................................................... 7
6. Add Case Manager And Incident Responder To Advanced Analytics Disaster Recovery ........... 8
   6.1. 1. Stop The Replicator ................................................................................................... 8
   6.2. 2. Upgrade The Passive And Active Advanced Analytics Clusters .............................. 8
   6.3. 3. Add Case Manager To Advanced Analytics .............................................................. 9
   6.4. 4. Configure Disaster Recovery On The Advanced Analytics And Case Manager Passive Clusters ................................................................. 10
   6.5. 5. Start The Replicator ............................................................................................... 11
1. Add a Service
Integrate a service with Incident Responder to gather the data needed to run actions and playbooks.

1. Click the Menu, select Settings, then navigate to Automation > Services.
2. Select a service:
   - To provide information based on a specific service, hover over a tile, then click ADD. Use the search by vendor or filter by action to find a service.
   - To manually provide the relevant information, click the add button.
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 charge of the service.
4. To validate the source, select TEST CONNECTIVITY.
5. Select CREATE SERVICE.
2. Edit a Service

If you've integrated a service with Incident Responder, change how you've configured it.

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 select the pencil  
4. Change the fields.
5. To validate the configuration, select TEST CONNECTIVITY.
6. Select SAVE.
3. Delete a Service

Once you delete a service, you can't use it in an action or playbook. If you delete a service and it is still part of a playbook, you are warned that the "playbook contains errors" when you run the playbook.

1. Remove the service from any playbooks.
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 the trash 🗑️.
4. 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 out-of-the-box service. If you upload a service that customizes an out-of-the-box service, all related actions and playbooks will start using this custom service instead of the out-of-the-box service.

If you create your own service on your own, 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 the upload button.
3. Click UPLOAD PACKAGE, then upload a ZIP file, no 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.
5. Delete a Custom Service

If you uploaded a custom service, you can delete it.

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.

1. In the navigation bar, click the Menu ☰, select Settings, then navigate to Automation > Services.
2. Hover over the service, then select the trash 🗑.
3. Click DELETE. If you delete a service that is used in a playbook, that playbook may not run as expected.
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.

### 6.1. 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:
   ```bash
   . /opt/exabeam/bin/shell-environment.bash
   ```
4. On the active cluster, stop the replicator:
   ```bash
   sos; replicator-socks-stop; replicator-stop
   ```

### 6.2. 2. Upgrade the Passive and Active Advanced Analytics Clusters

⚠️ 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.

```yaml
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:
      ```bash
      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
```

6.3. 3. Add Case Manager to Advanced Analytics

1. SSH to the primary Advanced Analytics machine.

2. Start a new screen session:

```
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] 0
How much memory in GB for each elasticsearch instance? [16] 16
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.

6.4. 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:

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

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.

**6.5. Start the Replicator**

On the active cluster, start the replicator:
Add Case Manager and Incident Responder to Advanced Analytics Disaster Recovery

replicator-socks-start; replicator-start