Forcepoint Behavioral Analytics

FBA 3.5 UPGRADE GUIDE

Publish Date: December 20, 2023

F23-09-05-00

Legal Notice

Attributions

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. The company cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Document Conventions

The following typographic conventions are used in this guide:

Typography

Format	Description
Bold font	Used to identify Graphical User Interface (GUI) elements, buttons, fields, and list labels. Example: Type your IP address in the **ip address** field and click **OK**.
Italic font	Used to identify book titles or words that require emphasis. Example: Read the *User's Guide.*
Monospaced font	Used to identify names of commands, files, and directories. Example: Use the `ls -a` command to list all files.
Monospaced bold font	When inline, this is used to identify text that users need to type. Example: Type **`SYSTEMHIGH`** in the **Network** field.
Shaded monospaced font	Used to identify screen output. Example: A network device must exist; otherwise, the following warning message displays `Warning: device [DEVICE] is not a valid network device`
Shaded monospaced bold font	Used to identify text that users need to type. Example: Specify your network configuration. Type: **`$ sudo ip addr show`**

This guide makes use of the following elements:

Note
Contains important information, suggestions or references to material covered elsewhere in the guide.

Tip
Provides helpful suggestions or alternative methods to perform a task.

Warning
Alerts you to an activity that may cause permanent loss of data or product functionality. Failure to heed a warning could result in permanent consequences to your data or system.

Caution
Alerts you to anything that could result in a security breach or temporary loss of data or product functionality. You may also see a caution when a particular action may have an adverse impact that is not readily apparent.

Important
Highlights critical tasks, information or actions that may be damaging to your system or security.

CONTENTS

Forcepoint Behavioral Analytics 3.5 Upgrade Guide

This Forcepoint Behavioral Analytics (FBA) Upgrade manual will guide technical FBA users through a complete upgrade from version 3.4.2 to the latest version 3.5 of the FBA system. This guide includes instructions that will result in a fully functional 3.5 FBA system when complete.

UPGRADE PREPARATIONS

The UI and ingest services must be stopped, and backups of the data store must be done prior to upgrading the FBA system. This section provides the procedures required to stop the services and backup the data stores.

Note
Any command that starts with "ansible" must be run from the Jenkins server as the user that is configured for ssh and sudo across the environment.

1. Export the needed Nifi flows:
   a. Stop the input processor, ensure the queues drain, then stop Nifi:

      ```
      ansible nifi -m shell -a "sudo systemctl stop nifi" --become
      ```

   b. Confirm that Nifi is not running:

      ```
      ansible nifi -m shell -a "sudo systemctl status nifi" --become
      ```

   c. Move the Nifi directory to a backup location:

      ```
      ansible nifi -m shell -a "sudo mv /data/ro-nifi /data/nifi.bak" --become
      ```

2. Stop the api service on all api servers:

   ```
   ansible api -m shell -a "sudo systemctl stop ro-api" --become
   ```

3. Monitor the `reveal.internal.event` queue to ensure the queue drains:

   `http://rabbit-{var.stackname}.{domain}:15672/#/queues`

4. Optional: Check the size of the disk usage for each Elasticsearch node as a reference point and check the event counts in Elasticsearch for verification after the upgrade is completed:

```
#Check disk usage
curl -k -u elastic:changeme https://localhost:9200/_cat/allocation?v

#Check doc counts in ES
curl -ku elastic:changeme "https://localhost:9200/_cat/count?v"

#Stop the rest of the ingest services once all rabbit queues drain
ansible api -m shell -a "sudo systemctl stop ro-api" --become
ansible conversion -m shell -a "sudo systemctl stop ro-conv" --become
ansible qw -m shell -a "sudo systemctl stop ro-qw" --become
ansible content -m shell -a "sudo systemctl stop ro-content" --become
ansible ui -m shell -a "sudo systemctl stop ro-ui" --become
```

5. On es1, check that the Elasticsearch repository exists and confirm the location: either S3 or NFS:

```
curl -k -u elastic:changeme https://localhost:9200/_snapshot
```

6. Create an Elasticsearch snapshot from es1:

Note
Replace `$REPO` with the repository from previous step, *ex: default_s3_repository.*

```
REPO="default_s3_repository"
curl -XPUT -k -u elastic:changeme "https://localhost:9200/_
snapshot/$REPO/snapshot_$(date +%Y%m%d%H%M%S)?wait_for_completion=false"
```

Note
The snapshot creation can take considerable time depending on the size of the indexes, confirm it is complete by running the following on es1:

```
curl -k -u elastic:changeme https://localhost:9200/_snapshot/$REPO/_all | jq
-r '.snapshots'
```

Query results must include:

```
snapshots["state"] = "SUCCESS"
```

7. Verify the health of the Elasticsearch cluster from es1:

```
curl -k -u elastic:changeme https://localhost:9200/_cluster/health | jq -r
'.status'
```

Query results must include:

```
green
```

8. Clear the analytics cache from both the MDS and MDSLYTICS hosts:

```
curl -XPOST -k https://localhost:8080/reference/analytics/clear_cache -f
```

9. Optional: Gather stats from ROSE and UI databases in Postgres for comparison with the post-upgrade stats:

```
# Query both ROSE and UI databases
select table_name as table, (xpath('/row/cnt/text()', xml_count))[1]::text::int
as count
from (
  select table_name, table_schema, query_to_xml(format('select count(*) as cnt
from %I.%I', table_schema, table_name), false, true, '') as xml_count
  from information_schema.tables
  where table_schema = 'public'
) t;
```

10. Back up PostgreSQL databases on the Postgres server:

```
ansible postgres -m shell -a "sudo pg_dump mds --username
postgres --create --clean --verbose --file /data/mds_database_backup_file.sql" --
become
```

```
ansible postgres -m shell -a "sudo pg_dump redowl_streaming --username postgres -
-create --clean --verbose --file /data/redowl_streaming_database_backup_file.sql"
--become
```

```
ansible postgres -m shell -a "sudo pg_dump the_ui --username postgres --create --
clean --verbose --file /data/the_ui_database_backup_file.sql" --become
```

```
ansible postgres -m shell -a "sudo pg_dump rosedb --username postgres --create --
clean --verbose --file /data/rosedb_database_backup_file.sql" --become
```

```
ansible postgres -m shell -a "sudo chown postgres:postgres /data/*.sql" --become
```

11. Back up the Jenkins data (jobs, plugins) on the jenkins host:

```
#Stop Jenkins service
sudo systemctl stop jenkins

# copy the entire data directory
sudo cp -R /var/lib/jenkins /data/upgrade/jenkins-backup

# ensure the backup has the correct permissions
sudo chown -R jenkins:jenkins /data/upgrade/jenkins-backup
```

UPGRADE PROCEDURES

1. Complete the steps in the *FBA 3.5 Installation Guide*: "Download and Run the FBA Installer."
2. Complete the steps in the *FBA 3.5 Installation Guide*: "Create and Configure the Hosts and Group/Vars/All Files."
3. Complete the steps in the *FBA 3.5 Installation Guide*: "Generate and Push SSH Keys to all Hosts."
4. Complete the steps in the *FBA 3.5 Installation Guide*: "Initialize Forcepoint Continuous Delivery Server."
5. Prepare for installation:

   Note
   Adjust dir as necessary.

   ```
   sudo mkdir -p /data/upgrade
   sudo chown -R $USER. /data/upgrade
   cd /data/upgrade
   ```

   Move and backup `grafana.db` file:

   Note
   This is not compatible with newer versions of Grafana unless the 3.4.2.3 patch was applied.

   ```
   ansible monitoring -m shell -a "sudo mv /var/lib/grafana/grafana.db ~/" --become
   ```

   Backup ansible config files:

   ```
   sudo cp -p /etc/ansible/hosts ./hosts.bak
   sudo cp -p /etc/ansible/ansible.cfg ./ansible.cfg.bak
   sudo cp -p /etc/ansible/group_vars/all ./all.bak
   ```

   Run the installer bin:

   ```
   sudo bash Forcepoint-UEBA-3.5-CentOS-7.bin
   ```

   Backup plugins tar:

   ```
   cp /tmp/plugins.tar.gz .
   ```

   Restore ansible config files:

   ```
   sudo cp -p ./hosts.bak /etc/ansible/hosts
   sudo cp -p ./ansible.cfg.bak /etc/ansible/ansible.cfg
   sudo cp -p ./all.bak /etc/ansible/group_vars/all
   ```

Clean up Yum:

```
ansible-playbook /usr/share/ro-ansible/yum-mirror.yml
sudo systemctl restart nginx
ansible vms -m shell -a "sudo yum history sync" --become
ansible vms -m shell -a "sudo yum clean all" --become
```

Clear out old Jenkins plugins:

Note
This is not compatible with newer versions of Jenkins.

```
ansible jenkins -m shell -a "sudo systemctl stop jenkins" --become
ansible jenkins -m shell -a "sudo yum remove jenkins -y" --become
ansible jenkins -m shell -a "sudo rm -rf /var/lib/jenkins/plugins/*" --become
```

Deploy Jenkins:

```
ansible-playbook /usr/share/ro-ansible/jenkins-init.yml

#Logon to jenkins at http://jenkins-whatever:8080
# It will ask about plugins just click the X in the upper right
# It will bring up another window click start using jenkins button

#After stack deploy is complete (this will enable TLS for Jenkins and change port
to 8443)
ansible-playbook /usr/share/ro-ansible/jenkins.yml
```

6. Restart services:

```
ansible api -m shell -a "sudo systemctl restart ro-api" --become
ansible conversion -m shell -a "sudo systemctl restart ro-conv" --become
ansible qw -m shell -a "sudo systemctl restart ro-qw" --become
ansible content -m shell -a "sudo systemctl restart ro-content" --become
ansible mds -m shell -a "sudo systemctl restart ro-mds" --become
ansible mdslytics -m shell -a "sudo systemctl restart ro-mds" --become
ansible ui -m shell -a "sudo systemctl restart ro-ui" --become
```

KAFKA DEPLOY ISSUES

Run the following commands if the Kafka deployment fails.

Warning
Running these commands before all of the queues have drained will result in data loss. The status of the queues can be monitored here:
`http://rabbit-{var.stackname}.{domain}:15672/#/queues`

```
#delete streams topics optional, if having issues with partitions on deploy-kafka job
ansible kafka -m shell -a "sudo sed -i '/^delete.topic.enable/s/=False/=True/'
/etc/kafka/conf/server.properties" --become

ansible kafka -m shell -a "sudo systemctl restart kafka" --become

sleep 30

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic 'dlp.*'" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic CHANGED_ALIASES" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic CONSUMER_ERRORS" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic DLP_INCIDENTS_IN_MOTION" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic END_POINT_DATA" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic ENTITY_RISK_LEVEL" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic EXPORT_ENTITY_RISK_LEVEL" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic NEW_ENTITIES" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic PUBLIC_ENTITIES" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
topic RAW_ALIAS_ER" --become

ansible kafka -m shell -a "sudo kafka-topics.sh --zookeeper localhost:2181 --delete --
```

```
topic UPDATED_ENTITIES" --become

ansible qw -m shell -a "sudo rm -rf /data/ro-qw/state/*" --become

ansible api -m shell -a "sudo rm -rf /tmp/kafka-streams" --become
```

FINAL UPGRADE STEPS

1. Confirm the following:
   a. UI users are working as expected.
   b. All data in Elasticsearch and Postgres appears as expected:

```
#Check disk usage on es1:
curl -k -u elastic:changeme https://localhost:9200/_cat/allocation?v
```

   c. Confirm that the event counts in ES are correct:

```
curl -ku elastic:changeme "https://localhost:9200/_cat/count?v"
```

   d. Confirm that the table counts in postgres are correct:

```
# Query both ROSE and UI databases
select table_name as table, (xpath('/row/cnt/text()', xml_count))
[1]::text::int as count
from (
  select table_name, table_schema, query_to_xml(format('select count(*) as
cnt from %I.%I', table_schema, table_name), false, true, '') as xml_count
  from information_schema.tables
  where table_schema = 'public'
) t;
```

   e. Confirm that all health checks appear within a normal range in Grafana.
   f. Validate that the entity replication function is working by running the following commands on the Rose host:

```
curl -XPOST -k http://localhost:9500/v1/replication/rebuild/normalize
#-- check status --
curl -XGET -k https://localhost:9500/v1/replication/rebuild/status
```

   g. Compute the analytics cache from MDS:

```
curl -XPOST -k https://localhost:8080/reference/analytics/compute_dashboard |
jq .
```

2. Apply available hotfixes.