Forcepoint Behavioral Analytics Upgrade Guide

Upgrade Guide | Forcepoint Behavioral Analytics | v3.4 | 17-Feb-2021

These instructions describe how to upgrade from v3.3.2 of Forcepoint Behavioral Analytics to v3.4 of Forcepoint Behavioral Analytics.

Preparation for upgrade

This stage of the upgrade will stop the UI and ingest services and take the appropriate backups of our data stores.

1. Stop the nifi service on the nifi server.
   a. Validate nifi is stopped.
2. Copy nifi data to the backup directory.

```
sudo mkdir -p /data/ro-nifi/backup
sudo cp /data/ro-nifi/configuration_resources/flow.xml.gz /data/ro-nifi/backup/
sudo cp /data/ro-nifi/nifi/conf/authorizers.xml /data/ro-nifi/backup/
sudo cp -r /data/ro-nifi/database_repository/ /data/ro-nifi/backup/
sudo cp -r /data/ro-nifi/content_repository/ /data/ro-nifi/backup/
sudo cp -r /data/ro-nifi/flowfile_repository/ /data/ro-nifi/backup/
sudo cp -r /data/ro-nifi/provenance_repository/ /data/ro-nifi/backup/
```

3. Stop ro-conv service on conv server. There are generally at least 2 conv hosts in Forcepoint Behavioral Analytics 3.3.x.

```
sudo systemctl stop ro-conv.service
```

4. Wait for reveal.internal.event queue to drain.
   a. Check rabbit UI for status

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

5. Stop ro-qw service on qw server. There are generally at least 2 qw hosts in Forcepoint Behavioral Analytics 3.3.x.

   ```
   sudo systemctl stop ro-qw.service
   ```

6. Stop ro-ui service on ui server.

   ```
   sudo systemctl stop ro-ui.service
   ```

7. Optionally, 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"
   ```

8. Check for Elasticsearch repository on ES1 and confirm if it is located on S3 or NFS.

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

9. Create an Elasticsearch snapshot from ES1 (replace $REPO with the repository from the previous step. Example: 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"
   ```

10. Verify the snapshot is complete from ES1.

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

    Result of the query should include:

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

11. Verify the cluster health from ES1.

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

    Result of the query should include:

    ```
    green
    ```

12. Clear the analytics cache from MDS and MDSLYTICS hosts.

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

13. Optionally, 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;
```

14. Backup PostgreSQL databases on the Postgres server. Update as needed to create backups where adequate space is available.

```
pg_dump mds --username postgres --create --clean --
verbose --file mds_database_backup_file.sql

pg_dump redowl_streaming --username postgres --create --
clean --verbose --file
redowl_streaming_database_backup_file.sql

pg_dump the_ui --username postgres --create --clean --
verbose --file the_ui_database_backup_file.sql

pg_dump rosedb --username postgres --create --clean --
verbose --file rosedb_database_backup_file.sql
```

Note

It is strongly recommended if the entity cleanup was not run in the v3.3.0 or v3.3.1 upgrades, that it is completed now. This will help ensure the success of the upgrade and has shown to greatly improve performance after the upgrade.

Please see the Addendum of Forcepoint Behavioral Analytics 3.2.0 to 3.3.0 Upgrade Guide - Entities Cleanup.

Host clean up and preparation

At this stage in the upgrade process, it is strongly recommended that the data volumes, NFS mounts, and any other mounted partitions be unmounted from the hosts (to be mounted again in a new directory structure) and the latest minimal version of RHEL or CENTOS 7.9 be re-installed across the hosts. This is the optimal route to ensure all RPMs installed by Forcepoint for earlier versions are removed. Because this is not always an option given resource and timing constraints, the below directions take a conservative approach to cleaning up the hosts and preparing them for the new installation.

Now that the UI and ingest services have been stopped and the necessary backups have been performed to ensure we will not lose data, the hosts will be prepared for the new containers. This will prepare the hosts for running a containerized version of Forcepoint Behavioral Analytics using Docker with the rootless kit. While the

following can be done manually as well, a modifiable script has been provided to ease in the cleanup and preparation of the hosts (upgrade_cleanup.sh).

Going forward the following terms are used:

- $FBA_USER: used in place of the provisioned user created for installation and runtime of the Forcepoint Behavioral Analytics software.
- $FBA_DIR: the directory that is running the installer. It must be owned by the $FBA_USER.

1. Make the necessary modifications to the upgrade_cleanup.sh script.

   Update the following variables:

   a. $FBA_USER
      - Provisioned user created for installation and runtime of the Forcepoint Behavioral Analytics software.

   b. $FBA_GROUP
      - The group name of the provisioned FBA_USER, most likely the same as the FBA_USER name above.

   c. $FBA_DIR
      - Base install directory.
      - It is preferable that this be mounted on a separate partition from the root OS.

2. Run the script from the $FBA_DIR:

   ```
   bash upgrade_cleanup.sh
   ```

   Monitor the output of the script for completed steps and errors.

3. Ensure the state of the hosts post-cleanup script

   a. All services provisioned from prior Forcepoint Behavioral Analytics installations should be stopped across the hosts.

   b. Volumes mounted on the root directory should be unmounted from hosts:
      - /data
      - /data/nfs
      - /var/log

   c. Volumes should be re-mounted under the $FBA_DIR:
      - $FBA_DIR/data
      - $FBA_DIR/data/nfs
      - $FBA_DIR/var/log

Forcepoint Behavioral Analytics 3.4 installation

Now that the hosts are ready for the new install the steps will primarily follow the standard installation path in the Forcepoint Behavioral Analytics Installation Guide.

1. Follow the installation guide steps

a. Starting from "I. Download the Forcepoint Behavioral Analytics installer media"

b. Ending at "VI. Deploy Forecepoint Behavioral Analytics from Jenkins"Delete the analytics cache from ES1.

2. If the "Junk" entity cleanup has been cared for then on the Rose host run:

```
curl -XPOST -k http://localhost:9500/v1/replication/
rebuild/normalize

-- check status --

curl -XGET -k https://localhost:9500/v1/replication/
rebuild/status
```

3. If the "Junk" entity cleanup from 3.3.x has never been completed, run:

```
curl -XPOST -k http://localhost:9500/v1/replication/
rebuild/normalize?onlyMonitored=true

-- check status --

curl -XGET -k https://localhost:9500/v1/replication/
rebuild/status
```

4. Compute the analytics cache from mds.

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

5. At this point, it is best practice to restart the following services across the stack (sudo systemctl restart {service_name}:

a. ro-mds (both mds and mdslytics hosts)

b. ro-cont

c. ro-conv

d. ro-ui

e. ro-qw

Final upgrade step

1. Verify the following:
2. UI users are working as expected.
3. All data in Elasticsearch and Postgress appear as expected.

   Check disk usage

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

   Check event counts in ES (same queries as above)

   Check table counts in postgres (same queries as above)
4. All health checks appear within a normal range in Grafana.