Forcepoint Behavioral Analytics

3.4.1 GENERAL AVAILABILITY TO 3.4.2 GENERAL AVAILABILITY UPGRADE GUIDE

Publish Date: March 25, 2022

F23-10-05-03252022

Legal Notice

Attributions

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 3.4.1 to 3.4.2 Upgrade Guide

This Forcepoint Behavioral Analytics (FBA) Upgrade manual will guide technical FBA users through a complete upgrade from version 3.4.1 to the latest version 3.4.2 of the FBA system. This guide includes step-by-step instructions for upgrading FBA and will result in a fully functional 3.4.2 system when complete. The following three sections must be completed:

Preparation for Upgrade

1. Export all Nifi Flows that need to be saved, using the Nifi UI.
2. Stop **nifi** service on the nifi server.
   a. Validate **nifi** is stopped.
3. Copy **nifi** data to backup directory by doing the following:

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

4. Stop `ro-conv` service on conv servers:

   Tip
   There are typically at least 2 conv hosts in FBA 3.3.0 and above.

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

5. Wait for `reveal.internal.event` queue to drain:

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

6. Stop `ro-qw` service on qw servers:

   Tip
   There are typically at least 2 qw hosts in FBA 3.3.0 and above.

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

7. Stop `ro-ui` service on ui server:

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

8. Check the size of the disk usage for each Elasticsearch node as a reference point. Check the event counts in Elasticsearch for verification after the upgrade is complete.

Note
This step is optional.

```
#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"
```

9. On **es1**, verify that the Elasticsearch repository exists and whether it is located on **S3** or **NFS**:

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

10. Create elasticsearch snapshot from **es1**:

Note
Replace `$REPO` with the repository from step 9. 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"
```

11. Verify snapshot is complete from **es1**:

Note
Snapshots can take a considerable amount of time, depending on the index size.

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

Result of the query should include:

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

12. When the snapshot completes, verify the health of the Elasticsearch cluster by running the following command on **es1**.

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

Result of the query should include:

```
green
```

13. Clear analytics cache from **mds** and **mdslytics** hosts:

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

14. Gather stats from **ROSE** and **UI** databases in **Postgres** for comparison with the post-upgrade stats.

Note
This step is optional.

```
# 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;
```

15. 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 /data/mds_
database_backup_file.sql
pg_dump redowl_streaming --username postgres --create --clean --verbose --file
/data/redowl_streaming_database_backup_file.sql
pg_dump the_ui --username postgres --create --clean --verbose --file /data/the_
ui_database_backup_file.sql
pg_dump rosedb --username postgres --create --clean --verbose --file
/data/rosedb_database_backup_file.sql
```

16. Backup the **Jenkins** data (jobs, plugins, etc.) on the jenkins host:

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

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

17. Stop jenkins service on jenkins server.

```
sudo systemctl stop jenkins.service
```

FBA 3.4.2 Installation

The previous section prepared the hosts for the new installation of FBA 3.4.2. This section will follow the standard FBA 3.4.2 installation path.

1. Complete the install steps in the following sections of the *Forcepoint Behavioral Analytics Install Guide for Version 3.4.2*:
   a. Section: Download and run the FBA installer
   b. Section: Create and Configure the Hosts and Group/Vars/All Files
   c. Section: Generate and Push SSH Keys to all Hosts
   d. Section: Initialize Forcepoint Continuous Delivery Server
   e. Section: Deploy FBA from Jenkins
2. Validate that the entity replication function is working. Run the following command on the **Rose** host:

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

3. Compute analytics cache from the **mds**:

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

4. Restart the the services across the FBA stack by running the following command for each service:

```
sudo systemctl restart {service_name}
```

   a. `ro-mds` - located on the **mds** host
   b. `ro-mds` - located on the **mdslytics** host
   c. `ro-cont`
   d. `ro-conv`
   e. `ro-ui`
   f. `ro-qw`

Final Upgrade Steps

1. Verify the following:
   a. **FBA 3.4.2** UI users are working as expected.
   b. All data in **Elasticsearch** and **Postgres** appear as expected in the 3.4.2 system. Run the following commands:

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

#Check event counts in ES (same queries as above, preparation step 8)
#Check table counts in postgres (same queries as above, preparation step 14)
```

2. All health checks appear within a normal range in Grafana.