Forcepoint Behavioral Analytics

3.4.1 GENERAL AVAILABILITY TO 3.4.2 LIMITED AVAILABILITY UPGRADE GUIDE

Publish Date: March 28, 2022

F23-10-06-03282022

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

FBA 3.4.1 General Availability Version to 3.4.2 Limited Availability Version Upgrade Guide

OVERVIEW

This document provides details on the upgrade approach that the primary consumers of the limited availability version will execute. A high-level overview of the approach is that the customer will be setting up new instances of the Forcepoint Behavioral Analytics (FBA) 3.4.2 application and migrating data from the existing FBA 3.4.1 application environment. The information in this document provides the steps to backup and migrate data from the FBA 3.4.1 environment to the new FBA 3.4.2 environment.

SETUP FBA 3.4.2 LIMITED AVAILABILITY VERSION

Complete the installation steps in the *Forcepoint Behavioral Analytics 3.4.2 Limited Availability Installation Guide*.

Note
Transfer the configuration and flows for Postfix and Nifi from the v3.4.1 environment to the v3.4.2 environment as needed.

BACKUP DATA FROM THE FBA 3.4.1 ENVIRONMENT

Before the data can be migrated to the new FBA 3.4.2 system, the data from the 3.4.1 system must be backed up. This section will describe how to create a backup of the 3.4.1 FBA data stores.

Complete the following steps to stop the UI and ingest services, and create data store backups.

1. Export all Nifi Flows that need to be saved, using the Nifi UI.
2. Stop the `nifi` service on the **nifi** server.
3. Confirm that the `nifi` service has stopped.
4. Copy **nifi** data to the backup directory:

```
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/
```

5. Stop `ro-conv` service on all **conv** servers.

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

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

6. Wait for `reveal.internal.event` queue to drain.

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

7. Stop `ro-qw` service on all **qw** servers.

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

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

8. Stop `ro-ui` service on **ui** server.

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

9. Take note of 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.

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"
```

10. 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
```

11. 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"
```

12. When the snapshot completes, verify that it is complete by running the following command on **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'
```

The result of the query must include:

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

13. 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'
```

The result of the query must include:

```
green
```

14. Clear the analytics cache on the mds and mdslytics hosts by running the following command on the **mds host** and the **mdslytics host**.

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

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. 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;
```

18. Backup **PostgreSQL** databases by running the following command on the postgress server (update as needed to create backups where adequate space is available).

> **Note**
> Commands must be run from inside the existing FBA Docker container.

```
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
```

MIGRATE DATA INTO THE NEW FBA 3.4.2 SYSTEM

1. Stop the following services in the FBA 3.4.2 system. These services must be stopped in this order, using the Jenkins **stop** jobs:
   a. `data ingest` (api, conv, content, qw)
   b. `ui`
   c. `mds`
   d. `mdslytics`
   e. `rose`
   f. `ups`
   g. `oapi`
   h. Stop the `collectd` service on the postgres host

      ```
      systemctl stop collectd.service
      ```
2. Transfer the **FBA 3.4.1** Posgres database backups to the new Postgres host.
   a. Download the **FBA 3.4.1** Postgres database backups to a location that is accessible from the new **FBA 3.4.2** deployment.
   b. Upload the **FBA 3.4.1** Postgres database backups to the new **FBA 3.4.2** Postgres host.

      ```
      scp -i your/pemfile centos@postgres-stackname:/location/of/file/mds_database_
      backup_file.sql
      scp -i your/pemfile centos@postgres-stackname:/location/of/file/redowl_
      streaming_database_backup_file.sql
      scp -i your/pemfile centos@postgres-stackname:/location/of/file/the_ui_
      database_backup_file.sql
      scp -i your/pemfile centos@postgres-stackname:/location/of/file/rosedb_
      database_backup_file.sql
      ```
   c. Copy the files to the **Docker** container.

      ```
      docker cp mds_database_backup_file.sql container_id:/var/lib/pgsql
      docker cp redowl_streaming_database_backup_file.sql container_
      id:/var/lib/pgsql
      docker cp the_ui_database_backup_file.sql container_id:/var/lib/pgsql
      docker cp rosedb_database_backup_file.sql container_id:/var/lib/pgsql
      ```
3. Restore Postgres data dumps.
   a. Log into the **Postgres** host using `ssh`.
   b. Log into the **Docker** container.

      ```
      docker exec -it container_id bash
      ```
   c. Start the **Postgres CLI**.

```
psql -U postgres
```

d. Drop the existing databases in the **FBA 3.4.2** environment.

```
# In psql
DROP DATABASE mds;
DROP DATABASE rosedb;
DROP DATABASE the_ui;
DROP DATABASE redowl_streaming;
```

i. If there are problems dropping the **rosedb** run the following command:

```
SELECT pg_drop_replication_slot('rose_slot');
```

e. Recreate the databases and role.

```
CREATE DATABASE mds;
CREATE DATABASE rosedb;
CREATE DATABASE the_ui;
CREATE DATABASE redowl_streaming;
```

i. Exit the Postgres **CLI**.

f. Restore the **FBA 3.4.1** database backups.

i. Change directory to the location where the backup files are located.

Example: `cd /var/lib/pgsql`

ii. Restore the database backups.

```
psql -U postgres mds < mds_database_backup_file.sql
psql -U postgres redowl_streaming < redowl_streaming_database_backup_
file.sql
psql -U postgres the_ui < the_ui_database_backup_file.sql
psql -U postgres rosedb < rosedb_database_backup_file.sql
```

4. Restore the Elastic Search data backups.

```
# Register snapshot location in the new v3.4.2 environment

# If s3 bucket snapshot location (update as necessary) curl -XPUT -k -u
elastic:changeme "https://localhost:9200/_snapshot/default_s3_repository?pretty"
-d ' {"type":"s3","settings:{"bucket":"BUCKET_NAME","region":"us-east-1"}}'

# If file system snapshot location (update as necessary) curl -XPUT -k -u
elastic:changeme "https://localhost:9200/_snapshot/default_fs" -d '{ "type":
"fs", "settings": { "location": "/usr/share/elasticsearch/es_backup_folder" } }'

# NOTE: For the following commands use "default_fs" instead of "default_s3_
```

```
repository" if using a filesystem to store the backup files

# If in doubt, the correct option can be found with `curl -k -u elastic:changeme
https://localhost:9200/_snapshot`

# Verify that the snapshot repository is set up correctly in the new v3.4.2
environment
1. curl -X GET -k -u elastic:changeme "https://localhost:9200/_snapshot/default_
s3_repository?pretty"
2. curl -X GET -k -u elastic:changeme "https://localhost:9200/_snapshot/default_
s3_repository/_all?pretty"

# Close all indices so there is no collision with the restore
3. curl -XPOST -u elastic:changeme "https://localhost:9200/_all/_close?pretty"

# Restore the indices
# Note: The "snapshot_name" can be found using command 2 found above
4. curl -X POST -u elastic:changeme "https://localhost:9200/_snapshot/default_s3_
repository/${snapshot_name}/_restore?pretty"
```

5. Restart the following services in the **FBA 3.4.2** system. These services must be started in this order, using the Jenkins **start** jobs:
   a. Start the `collectd` service on the postgres host
      `systemctl start collectd.service`
   b. `oapi`
   c. `ups`
   d. `rose`
   e. `mdslytics`
   f. `mds`
   g. `ui`
   h. `data ingest` (api, conf, content, qw)
6. Re-run the jenkins `deploy-ueba-ui` job.
7. Verify that all FBA 3.4.2 services are running.

Note
Data counts, such as event, entities, and users can be compared between the 3.4.1 and 3.4.2 environments to validate the data migration.

ADDITIONAL FUNCTIONALITY VALIDATION

1. Validate that the entity replication function is working by running the following command on the **Rose** service host:

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

2. Compute analytics cache from **mds**.

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

3. Restart the following services across the stack:

   Example: `sudo systemctl restart {service_name}`

   a. `ro-mds` on the **mds host**

   b. `ro-mds` on the **mdslytics host**

   c. `ro-cont`

   d. `ro-cont`

   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 the 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 7)
curl -ku elastic:changeme "https://localhost:9200/_cat/count?v"

#Check table counts in postgres (same queries as above, preparation step13)
select table_name as table, (xpath('/row/cnt/text()', xml_count))
[1]::text::intas 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;
```

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