Forcepoint Behavioral Analytics

3.4.1 LIMITED AVAILABILITY VERSION UPGRADE GUIDE (ROOTLESS - UEBA 3.3.3 TO 3.4.1)

Publish Date: November 02, 2021

F23-10-03-11022021

Legal Notice

Although every precaution has been taken in the preparation of this document, the authors and the company assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

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.

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or completeness is implied. The provided information is on an "as is" basis. The authors and the company shall have neither liability nor responsibility for any loss or damages arising from the information contained in this document. Printed in the United States of America.

This document contains proprietary information and is furnished for evaluation purposes only, and, except with written permission of the vendor, such information shall not be published, or disclosed to others, or used for any other purpose, or duplicated in whole or in part.

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

List of Tables

Forcepoint Behavioral Analytics 3.3.3 to 3.4.1 Rootless Upgrade Guide

This Forcepoint Behavioral Analytics (FBA) Upgrade manual will guide technical FBA users through a complete upgrade from version 3.3.3 to the Limited Availability rootless version 3.4.1 of the FBA system. This guide includes step-by-step instructions for upgrading FBA and will result in a fully functional 3.4.1 system when completed correctly.

PREPARATION FOR UPGRADE

To begin the upgrade process, the User Interface and Ingest Services must be stopped, and backups of the data stores must be made.

1. Stop `nifi` service on the `nifi` server.
   a.
   ```
   systemctl stop nifi.service
   ```
   b. Verify that the `nifi` service is no longer running.
2. Move `nifi` data and configurations to a 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/
   sudo mv /data/ro-nifi/backup /data/backup/
   ```
3. Stop `ro-conv` service on all conv servers (there are generally at least 2 conv hosts in FBA 3.3):
   ```
   sudo systemctl stop ro-conv.service
   ```
4. Wait for `reveal.internal.event` queue to drain. Queue activity can be monitored here:
   `http://rabbit-{var.stackname}.{domain}:15672/#/queues`
5. Stop `ro-qw` service on all qw servers (there are generally at least 2 qw hosts in FBA 3.3):
   ```
   sudo systemctl stop ro-qw.service
   ```
6. Stop `ro-ui` service on ui server:

   Stop `ro-ui` service:
   ```
   sudo systemctl stop ro-ui.service
   ```
   Stop `nginx.service` Service:

```
sudo systemctl stop nginx.service
```

Stop `logstash` service:

```
sudo systemctl stop logstash.service
```

Tip

The `logstash`service resides on each elasticsearch node and must be stopped on each node.

7. Stop `logstash` service on `elasticsearch` servers:

```
sudo systemctl stop logstash.service
```

8. (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:

Tip

This step must be run by logging directly into the elasticsearch node.

```
#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` check that the `Elasticsearch` repository exists and is located on `S3` or `NFS`:

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

10. Create `Elasticsearch` snapshot from es1 (replace `$REPO` with 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"
```

11. As the snapshot can take considerable time depending on the size of the indexes, wait until complete and verify complete by running the following on `es1`:

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

The result of the query should include:

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

12. Once the snapshot has completed successfully then verify the health of the `Elasticsearch` cluster from `es1`:

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

The result of the query should include:

```
green
```

13. (Optional) Clear the analytics cache from both the `MDS` and `MDSLYTICS` hosts:

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

Tip

STRONGLY RECOMMENDED: Run the junk entity cleanup process. This will help ensure the success of the upgrade and has shown to greatly improve performance post-upgrade. Refer to the Upgrade Addendum for FBA 3.4.1, "Junk Entities Cleanup" for more information.

14. (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;
```

15. Backup `PostgreSQL` databases on the `Postgres` server by logging in as root and performing the following commands (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
```

Note

The location of the output will need to be the same as the mounted data directory for `postgres`; if this location is not in the default /data directory, the output will need to be adjusted accordingly.

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

```
# copy the entire data directory
```

```
sudo cp -R /var/lib/jenkins <path>/<to>/<backup>

# ensure the backup has the correct permissions
sudo chown -R jenkins:jenkins <path>/<to>/<backup>
```

17. Stop the Jenkins service on the jenkins host:

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

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. Since this is not always an option given resource and timing constraints, the below directions take a conservative "best efforts" 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 made to ensure that there will be no data loss, host preparation for new containers will be done. This will prepare the hosts for running a containerized version of FBA using Docker. While the below 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`).

Table 1.1. Definition of Terms Used

Term	Use/Definitions	Example Value	Additional Information
FBA_USER	User can be chosen by client prior to upgrade and installation	centos	The `$FBA_USER` is required to have sudo permissions enabled across all hosts in the deployment. In addition, some commands run from the host will require sudo permissions to run correct (i.e. all docker commands run from the host as the `$FBA_USER` will use `sudo`).
FBA_GROUP	the group of the FBA_USER	centos	
FBA_DIR	The directory where the FBA software will be installed	`/home/centos`	Must be owned by the `$FBA_USER` Preferable that this be mounted on a separate partition from the root OS.

1. Make the necessary modifications to the `upgrade_cleanup.sh` script.
    a. Update the following variables:
        i. `$FBA_USER`
        ii. `$FBA_GROUP`
        iii. `$FBA_DIR`
2. Run the script from the `$FBA_DIR` (as root user or as the `FBA_USER` with `sudo`).

```
bash upgrade_cleanup.sh
```

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

3. Ensure the state of the hosts post-cleanup script.
   a. All services provisioned from prior FBA installs should be stopped across the hosts.
   b. Volumes mounted on the root directory should be unmounted from hosts:
      i. `/data`
      ii. `/data/nfs`
      iii. `/var/log`
   c. Volumes should be re-mounted under the `$FBA_DIR`:
      i. `/$FBA_DIR/data`
      ii. `/$FBA_DIR/data/nfs`
      iii. `/$FBA_DIR/var/log`

FBA 3.4.1 INSTALL

After completing the steps above, the host is ready for the new install. The installation steps below will follow the standard installation path.

1. Complete installation steps X through X. Refer to the *Forcepoint Behavioral Analytics Install Guide 3.4.1*
2. Confirm the status of the "Junk" entity cleanup script.
   a. If the "Junk" entity cleanup script has been run, then run the following 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
```

   b. If the "Junk" entity cleanup script has never been run, then run the following 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 the analytics cache from Master Data Service (MDS):

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

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

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

   a. `ro-mds` (both `mds` and `mdslytics` hosts)
   b. `ro-cont`

c. `ro-cont`

d. `ro-ui`

e. `ro-qw`

FINAL UPGRADE STEPS

1. Verify the following:

   a. UI users are working as expected.

   b. 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)
   ```

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

Upgrade Addendum for Forcepoint Behavioral Analytics 3.4.1.

To ensure the success of the upgrade, the following steps should be performed after Step 13 of the Upgrade Guide.

Taking this step will allow for more space to be allotted to Postgres to support the upgrade. The Platform Ops group should be involved in this step to help determine that the proper parameters are being met.

All steps below will be performed in `rosedb` database.

1. The total number of monitored entities and the total number of junk entities that exist n the pre-upgraded solution must be determined. Do this by running the following `sql` scripts:

```
 Total # of monitored entities:
SELECT count(*) FROM entity WHERE id IN ( SELECT entity_id FROM entityattribute
WHERE key = 'Monitored Entity');

Total # of "junk" entities:
SELECT count(*) FROM entity WHERE id NOT IN ( SELECT entity_id FROM
entityattribute WHERE key = 'Monitored Entity');
```

2. Based on the results of the previous `sql` scripts, it must be determined whether or not to delete junk entities.The following commands must be used to delete the junk entities:

   Note

   The removal of the "junk" entities is highly recommended (and required for environments with high number of overall entities with majority being "non-monitored"). After a 3.3x upgrade the mechanism which creates "junk" entities will not be present in the code base and will not occur post a 3.3.x upgrade. This in return will introduce an additional performance gain to the system going forward.

3. Replication slots in Postgres must be dropped. To drop replication slots, perform the following steps:

   a. Loop up the slots that are setup in the Postgres database using the following `sql`:

   ```
   SELECT slot_name, slot_type, active FROM pg_replication_slots;
   ```

   b. For each existing replication slot, execute the following command:

   ```
   SELECT pg_drop_replication_slot('slot_name');
   ```

4. Remove junk entities from the `normalizedalias_entity` table to avoid any foreign key constraint violations by performing the following `sql`:

```
DELETE FROM normalizedalias_entity WHERE entity_id NOT IN ( SELECT entity_id FROM
entityattribute WHERE key = 'Monitored Entity');
```

5. Remove junk entities from the primary table by performing he following `sql`:

```
DELETE FROM entity WHERE id NOT IN ( SELECT entity_id FROM entityattribute WHERE
key = 'Monitored Entity');
```

6. Proceed with the upgrade of the solutions.
7. After the upgrade, it is recommended to run a re-sync of the entity data collection.