# Forcepoint Behavioral Analyitcs

## UPGRADE GUIDE FOR VERSION 3.3.3

Publish Date: May 25, 2021

Copyright © 2021

F23-09-01-05252021

## 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.<br><br>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.<br><br>Example: Read the *User's Guide.* |
| Monospaced font | Used to identify names of commands, files, and directories.<br><br>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.<br><br>Example: Type `SYSTEMHIGH` in the **Network** field. |
| Shaded monospaced font | Used to identify screen output.<br><br>Example: A network device must exist; otherwise, the following warning message displays<br><br>`Warning: device [DEVICE] is not a valid network device` |
| Shaded monospaced bold font | Used to identify text that users need to type.<br><br>Example: Specify your network configuration. Type:<br><br>`$ 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 3.3.2 to 3.3.3 Upgrade Guide

This Forcepoint Behavioral Analytics (FBA)Upgrade manual will guide technical FBA users through a complete upgrade from version 3.3.2 to the latest version 3.3.3 of the FBA system. This guide includes step-by-step instructions for upgrading FBA and will result in a fully functional 3.3.3 system when completed correctly.

## Preparation for Upgrade

1. Stop nifi service on the nifi server.

   a. Validate nifi is stopped.

2. Copy nifi data to backup directory by doing the following:

```
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 servers (there are generally at least 2 conv hosts in FBA 3.3):

```
sudo service ro-conv stop
```

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

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

5. Stop `ro-qw` service on qw servers (there are generally at least 2 qw hosts in FBA 3.3):

```
sudo service ro-qw stop
```

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

```
sudo service ro-ui stop
```

7. Check for elasticsearch repository on es1:

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

8. Create elasticsearch snapshot from es1 (replace `$REPO` w/ 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"
```

9. Verify 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"
```

10. Verify green cluster health from es1:

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

Result of the query should include:

```
green
```

11. Clear analytics cache from `MDS` and `MDSLYTICS` hosts:

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

12. Backup PostgreSQL databases on the Postgres server (update as needed to create backups where adequate space is available):

```
pg_dump the_ui --username postgres --create --clean --verbose --file the_ui_
database_backup_file.sql

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
```

> ☑ **Note**
>
> **IT IS STRONGLY RECOMMENDED** that if the entity cleanup was not run in the 3.3.0, 3.3.1, or 3.3.2 upgrades that it be completed now. This will help ensure the success of the upgrade and has shown to greatly improve performance after the upgrade. Please see *"Upgrade Addendum For The Forcepoint Behavioral Analytics 3.3.2 to 3.3.3 Upgrade Guide" on page 11*

13. 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>
```

14. Stop `ro-content` service on cont server:

```
sudo service ro-content stop
```

# Offline Install

1. Remove ro-ansible package from jenkins host:

```
sudo yum remove ro-ansible -y
```

2. Back up the following files:

```
sudo cp /etc/ansible/hosts /etc/ansible/hosts.bak

sudo cp /etc/ansible/ansible.cfg /etc/ansible/ansible.bak
```

3. Run Forcepoint UEBA binary:

```
#copy the bin file to the jenkins under /tmp or other directory with at least
10GB of free space

sudo bash /tmp/Forcepoint-UEBA-3.3.3-CentOS-7.bin

or

sudo bash /tmp/Forcepoint-UEBA-3.3.3-RHEL-7.bin
```

4. Remove new files and restore files from step 2:

```
sudo rm /etc/ansible/hosts

sudo rm /etc/ansible/ansible.cfg

sudo mv /etc/ansible/hosts.bak /etc/ansible/hosts

sudo mv /etc/ansible/ansible.bak /etc/ansible/ansible.cfg
```

5. From the Jenkins host run the below to grab all significant hosts and run `sudo yum clean all`. This will help ensure the rpm updates are successful. It is best practice to run these commands as the centos user and so the command is written from that perspective. You will need to change the path to the key for your instance.

```
IPLIST=`cat /etc/hosts | awk '{ print $1 }' | sort | uniq | grep -vwE "
(127.0.0.1|::1|^$)"`

for host in $IPLIST; do echo $host; ssh -i /{path to pem_file} $host 'sudo yum
clean all'; done
```

# Upgrade Specific Services

1. From the Jenkins host run the following playbooks in this order from `/usr/share/ro-ansible`:

```
ansible-playbook hostname.yml
```

```
ansible-playbook hosts_file.yml

ansible-playbook yum-mirror.yml

ansible-playbook ro-baseline.yml

ansible-playbook common.yml

ansible-playbook jenkins.yml

ansible-playbook redis.yml

ansible-playbook postgres.yml

ansible-playbook rabbit.yml

ansible-playbook ro-es.yml
```

✅ **Note**

This should be run directly as the `root` user. However, if the playbook fails due to being unable to communicate with the other hosts, you can run the command with the private key as any user with `sudo` permissions.

Example: `ansible-playbook --private-key=${path_to_key_file} <playbook-yaml>.yml`

➡️ **Tip**

If you have trouble creating the yum cache in the `common.yml` playbook, try restarting the **nginx** service on the jenkins host and rerunning the playbook.

➡️ **Tip**

If there are issues with the `jenkins.yml` playbook, instead run the `jenkins-init.yml` playbook. This will follow the same process as a fresh installation and will upgrade all of the remaining components. In this instance, any custom jenkins jobs will be overwritten and will require manually restoring them after the installation is complete.

If you ultimately go this route, you will first need to completely remove the existing version of jenkins in order to ensure the new version is able to install correctly. To do this, follow the below steps:

```
### PLEASE MAKE SURE YOU HAVE BACKED UP YOUR JENKINS DATA BEFORE
FOLLOWING THESE STEPS

### IF YOU DO NOT, ALL CUSTOM JOBS/PLUGINS/ETC. WILL BE LOST

# Stop the jenkins service

sudo systemctl stop jenkins

# Uninstall the jenkins service

sudo yum -y erase jenkins
```

```
# run the new jenkins job and re-install the updated version of jenkins
ansible-playbook jenkins-init.yml
```

2. Delete analytics cache from es1:

```
curl -k -u elastic:changeme -XDELETE 'https://localhost:9200/analytics_cache'
```

3. From the Jenkins host run the following playbooks in this order from /usr/share/ro-ansible:

```
ansible-playbook kafka.yml

ansible-playbook ro-mon-es.yml

(If the last task fails re run playbook TASK [ro-mon-es : Create a disabled role
mapping to initialize security index (with auth)])

ansible-playbook ro-schema.yml

ansible-playbook ro-ui.yml

ansible-playbook minigator.yml

ansible-playbook ro-monitoring.yml

ansible-playbook ro-kibana.yml

ansible-playbook ro-mds.yml

ansible-playbook ro-api.yml

ansible-playbook ro-qw.yml

ansible-playbook ro-conv.yml

ansible-playbook ro-logstash.yml

ansible-playbook ro-rose.yml

ansible-playbook ro-content.yml

ansible-playbook ro-ups.yml

ansible-playbook ro-ui.yml

ansible-playbook ro-nifi.yml
```

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

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

-- check status --

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

   a. If the Junk entity cleanup has **not** been cared for then run:

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

```
the entity cleanup has not been run, then run this version)
-- check status --
curl -XGET -k https://localhost:9500/v1/replication/rebuild/status
```

5. Compute analytics cache from mds:

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

# Final Upgrade Steps

1. Run the `Deploy-UEBA-Software` job.

2. Monitor the Jenkins jobs to confirm that the upgrade was successful and complete.

3. After the FBA instance stack is up and running, all calls to the Nifi API need to be modified to contain an Access Token in the header. Please follow the steps in the Config Manual (section: Nifi API Integration Requirements) to modify existing calls as needed.

# Upgrade Addendum For The Forcepoint Behavioral Analytics 3.3.2 to 3.3.3 Upgrade Guide

## JUNK ENTITIES CLEANUP (POSTGRES DB BACKUP)

To ensure the success of the upgrade the following steps should be considered post **Preparation for Upgrade**(step 12 and before beginning step 13).

Recommendation to be added to allow for more space being allotted to Postgres to support the upgrade but this recommendation needs to be determined with the help of the Platform Ops group.

## THE FOLLOWING STEPS ARE TO BE PERFORMED IN THE ROSEDB DATABASE

1. Determine the total number of monitored entities and the total number of junk entities that exist in the pre-upgraded solution with the following sql:

   **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. If junk entities are going to be removed, perform the following steps (if the will not be removed, skip to Step 3):

   > **➔ Tip**
   >
   > The removal of the junk entities is strongly recommended. 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.

   > **✓ Note**
   >
   > Ensure that any junk entities in the table `normalizedalias_entity` are removed to prevent a foreign key constraint violation.

   > **➔ Tip**
   >
   > Step 2 is only necessary for pre-3.3.x environments.

> **Delete foreign key table entry:**

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

> **Remove junk entites from the primary table:**

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

3. If junk entities are not going to be removed, replication slots in Postgres will need to be dropped. To do this use the following commands:

> **Lookup the slots that are setup in Postgres database using the following sql:**

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

> **For each existing replication slot, execute the following command:**

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

4. Proceed with the solution upgrade.

> **Tip**
>
> After the upgrade is complete, it is recommended to rerun a re-sync of the entity data collection.