Forcepoint Behavioral Analytics Upgrade Guide

Upgrade Guide | Forcepoint Behavioral Analytics | v3.3.2 | 21-Aug-2020

These instructions describe how to upgrade from v3.3.1 of Forcepoint Behavioral Analytics to v3.3.2 of Forcepoint Behavioral Analytics.

Preparation for upgrade

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 service ro-conv stop
```

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 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 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"
   ```

9. 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"
   ```

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 the 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 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.

13. Stop ro-content service on the cont server.

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

Offline Install

1. Remove ro-ansible package from the Jenkins host.

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

2. Backup 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 Behavioral Analytics 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-3.3.2-CentOS-7.bin
   or
   sudo bash /tmp/Forcepoint-UEBA-3.3.2-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 helps ensure the rpm updates are successful. It is best practice to run these commands as the centos user 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
```

2. Delete the 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 http://localhost:9500/v1/replication/
   rebuild/normalize
   -- check status --
   curl -XGET -k https://localhost:9500/v1/replication/
   rebuild/status
   ```

   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 we have not ran
   the entity cleanup then run this version)
   ```

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

5. Compute the analytics cache from mds.

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

Final upgrade step

1. Run the deploy-UEBA-Software job.

✓ **Note**

To install v3.3.2.1, follow the upgrade instructions here after completing the upgrade to v3.3.2.