Forcepoint Behavioral Analytics Upgrade Guide

Upgrade Guide | Forcepoint Behavioral Analytics | v3.2 | 23-August-2019

These instructions describe how to upgrade from v3.1.2 or v3.1.3 of Forcepoint Behavioral Analytics to v3.2 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/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.

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

4. Wait for reveal.internal.event queue to drain.
5. Stop ro-qw service on qw server.

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

6. Stop ro-ui service on ui server.

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

7. Check for elasticsearch repository on mds1.

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

8. Create an elasticsearch snapshot from mds1 (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 mds1.

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

10. Verify green cluster health from mds1.

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

11. Clear the analytics cache from mds1.

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

12. Backup the postgresql databases on the postgresql server.

```
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
```

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

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

14. Remove files from the cont server.

```
sudo rm -rf /var/qtd/*
```

15. Update /etc/ansible/group_vars/all on jenkins server
    a. Add qtd_data_dir var.

```
# Mapped files location
qtd_data_dir: "/var/qtd"
```

Offline Install

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

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

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 /{directory of choice} (ensure there is space available)
sudo bash /{directory of choice}/Forcepoint-UEBA-3.2.0-CentOS-7.bin
or
sudo bash /{directory of choice}/Forcepoint-UEBA-3.2.0-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. Run sudo yum clean all on the following hosts.

```
api
qw
conv
rose
cont
ups
ui
nifi
```

Upgrade Specific Services

6. 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
```

7. Delete the analytics cache from mds1.

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

8. 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
```

9. Compute the analytics cache from mds1.

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

Event shorthand template changes

The default event shorthand templates have changed in this release. The old templates may not work anymore due to the changes in the underlying data model.

- If you have made no changes to the templates then run this command against on mds1 node:

```
curl -k -XPOST https://localhost:8080/reference/
event_shorthand/default/load?user_id=1\&overwrite=true
```

- If you have made changes to the templates then you will need to evaluate those templates for updates to the data model in addition to running this update.

The important change is that models can now have a `relationshipAttribute` instead of a `relationshipRole`.

Vault TLS settings

To correct the TLS settings in Vault run the following steps:

```
##On the Jenkins Host
sudo yum remove vault
sudo yum remove consul
Run remove certs ansible playbook (util-ueba-remove-crts)
Re-deploy the entire stack by running the job "Deploy-
UEBA-Stack" (This will ensure all of the settings are
correct to push the new vault settings out)
```

Final upgrade settings

Normally, you would run the Deploy-UEBA-Software job, but since Deploy-UEBA-Stack already has already been run, this is unnecessary.

1. After the success of Deploy-UEBA-Software job, run the timeslice alias job.

   ```
   util-ensure-daily-timeslice-aliases
   ```