Forcepoint Behavioral Analyitcs

UPGRADE GUIDE FOR HOTFIXES (3.3.2.2 & 3.3.3.1)

Publish Date: February 17, 2022

F23-09-02-02172022

Legal Notice

Attributions

Upgrade Guide for Forcepoint Behavioral Analytics Hotfixes (3.3.2.2 & 3.3.3.1)

Prior to moving to step 2, the Log4j vulnerability mitigation steps need to be executed on the environment.

These instructions can be found here: Apache log4j2.x multiple vulnerabilities for Forcepoint Behavioral Analytics.

The primary change contained in these hotfix patches modifies the FBA top risk analytic calculation to rank calculations by score.

To apply the hotfix patches, complete the following steps:

1. Download the hotfix file consisting of the the `ro-mds` jar file from the support site:

   Forcepoint Behavioral Analytics 3.3.2.2 Hotfix

   Forcepoint Behavioral Analytics 3.3.3.1 Hotfix

   Note
   All steps below are on the `mds` and `mdslytics` hosts.

2. Copy and rename the file to the `mds` and `mdslytics` hosts via `scp` or other means. The file must be renamed to `ro-mds.jar`.

   ```
   #scp example
   scp reference-data-service-x.y.z-uberjar.jar user@mds-
   yourenvironment:/home/user/ro-mds.jar
   scp reference-data-service-x.y.z-uberjar.jar user@mdslytics-
   yourenvironment:/home/user/ro-mds.jar
   ```

   `x.y.z` refers to the downloaded file.

3. Stop the `ro-mds` service on both `mds` and `mdslytics` hosts.

   ```
   #example
   ssh -l user mds-yourenvironment
   sudo service ro-mds stop ssh -l user mdslytics-yourenvironment sudo service ro-
   mds stop
   ```

4. Rename the original `ro-mds.jar` files as a backup.

   ```
   #example
   Example: cd /usr/lib/java/ro-mds
   sudo mv ro-mds.jar ro-mds.original
   ```

5. Move the new jar file into place.

   ```
   #example
   sudo mv /home/user/ro-mds.jar /usr/lib/java/ro-mds/ro-mds.jar
   ```

6. Start the `ro-mds` service.

```
#example
sudo systemctl start ro-mds
```

7. Verify the fix is working as expected.

If a rollback is required, perform the following steps on the `mds` and the `mdslytics` hosts:

1. Stop the `ro-mds` service.
2. Rename the `ro-mds.jar` file to `ro-mds.<version>`.
3. Rename the `ro-mds.original` to `ro-mds.jar`.
4. Start the `ro-mds` service.
5. Verify that the system is running as expected.