Forcepoint Behavioral Analytics

3.4.0.2 UPGRADE GUIDE

Publish Date: January 09, 2023

F23-09-01-00

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. 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

Forcepoint Behavioral Analytics 3.4.0.2 Upgrade Guide 5
Automated Installation Instructions 5
Manual Installation Instructions 7
Installation Backout 18

Forcepoint Behavioral Analytics 3.4.0.2 Upgrade Guide

This Forcepoint Behavioral Analytics (FBA) Upgrade manual will guide technical FBA users through a complete upgrade from version 3.4.0 or 3.4.0.1 to the latest version 3.4.0.2 of the FBA system. This guide includes instructions for an automated upgrade and instructions for a manual upgrade that will result in a fully functional 3.4.0.2 system when complete.

Important
These changes must be performed within each Docker container on containerized installs.

AUTOMATED INSTALLATION INSTRUCTIONS

1. Download the hotfix file package from here:

   FBA 3.4.0 hotfix patch

2. Upload the Patch `.tar` file to the Jenkins host:

   ```
   scp -P 2222 fba-hotfix-3402.tar [Jenkins-server]:/tmp/
   ```

3. Log in to the Jenkins host and extract the patch files:

   ```
   ssh centos@[Jenkins-server] -p 2222
   sudo tar -xvf /tmp/fba-hotfix-3402.tar -C /data/html/
   ```

4. Run the Ansible® playbook:

   ```
   cd /data/html/3402upgrade/ansible
   ansible-playbook patch-Log4j-3402.yml -i /etc/ansible/hosts

   curl -k -u elastic:changeme -XPUT "https://<ES1-SERVER>:9200/_
   cluster/settings" -d'{"transient":
   {"cluster.routing.allocation.enable": "all"}}'
   ```

   Tip
   If authentication errors occur, ensure that the logged in user is the Centos™ user, If errors persist, disable host key checking:

```
vim /etc/ansible/ansible.cfg
HOST_KEY_CHECKING = False
```

5. Patch Minigator tool.

   Because the host location of the Minigator can be determined per individual installation, the steps can not be specific. A summary of the patch actions are as follows:

   Tip
   Patching the Minigator tool is only required if it has been deployed.

   a. Copy the Minigator `.rpm` file from the Jenkins host:

   ```
   /data/html/3402upgrade/ansible/files/rpm/minigator-1.98.1-1.el7.x86_64.rpm
   ```

   b. Remove the old Minigator `.jar` file.

   c. Install the new Minigator `.rpm` file:

   ```
   sudo rpm -Uvh minigator-1.98.1-1.el7.x86_64.rpm
   ```

   Important
   Any custom UI changes must be applied manually. Forcepoint will not persist those changes to the new version.

6. Remove backup files that were created during install to ensure that all files with the old versions of Log4j™ library code are removed. The following locations will have backup files:

   API server: `/usr/lib/java/ro-api/ro-api.jar.pre3402`

   Content server: `/usr/lib/java/ro-content/ro-content.jar.jar.pre3402`

   Conversion server: `/usr/lib/java/ro-conv/ro-conv.jar.jar.pre3402`

   Jenkins server: `/usr/lib/java/ro-schema/ro-schema.jar.jar.pre3402`

   Nifi server: `/usr/share/java/ro-ingest-utils/ro-ingest-utils.jar.jar.pre3402`

QW server: `/usr/lib/java/ro-qw/ro-qw.jar.jar.pre3402`

Rose server: `/usr/lib/java/ro-rose/ro-rose.jar.jar.pre3402`

MDS server: `/usr/lib/java/ro-mds/ro-mds.jar.jar.pre3402`

MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.jar.pre3402`

UI server: `/data/3402-backup-previous/ro-ui.backup.tar`

MANUAL INSTALLATION INSTRUCTIONS

1. Download the hotfix file package from here:

   FBA 3.4.0 hotfix patch

2. Upload the Patch `.tar` file to the Jenkins host:

   ```
   scp [-i ~/.ssh/my.pem] -P 2222 fba-hotfix-3402.tar [Jenkins-server]:/tmp/
   ```

   Log in to the Jenkins host and extract the patch files:

   ```
   ssh [-i ~/.ssh/my.pem] centos@[Jenkins-server] -p 2222
   sudo tar -xvf /tmp/fba-hotfix-3402.tar -C /data/html/
   ```

3. Copy the `.tar` ball from the Jenkins server to the ElasticService™, Monitoring and Kafka® instances:

   Tip
   The value in `[server]` should be replaced with the names of the ElasticSearch, Monitoring and Kafka instances.

   ```
   From Jenkins server, need to copy the tar ball to the ES, Monitoring and Kafka instances:
   scp [-i ~/.ssh/my.pem] -P 2222 /tmp/fba-hotfix-3402.tar [server]:/tmp/
   ```

```
ssh [-i ~/.ssh/my.pem] centos@[server] tar -xvf /tmp/fba-
hotfix-3402.tar -C /tmp/
```

4. Shut down the necessary services on each server environment associated with ElasticSearch and Monitoring to allow for the log4j updates to Elastic Search:

```
sudo systemctl status [server]_elasticsearch.service
sudo systemctl stop [server]_elasticsearch.service
sudo systemctl status [server]_elasticsearch.service

sudo rm /usr/share/elasticsearch/lib/log4j-*
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-api-
2.18.0.jar /usr/share/elasticsearch/lib/

sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-1.2-api-
2.18.0.jar /usr/share/elasticsearch/lib/

sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-core-
2.18.0.jar /usr/share/elasticsearch/lib/

sudo chown root:root /usr/share/elasticsearch/lib/log4j-*
sudo chmod 644 /usr/share/elasticsearch/lib/log4j-*
```

5. Shut down the necessary services on each server environment associated with Elastic Search and Monitoring to allow for the log4j updates to LogStash:

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

sudo rm /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-api/2.6.2/log4j-api-
2.6.2.jar
sudo rmdir /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-api/2.6.2
sudo mkdir /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-api/2.18.0
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-api-
2.18.0.jar /usr/share/logstash/logstash-
```

```
core/lib/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chown -R logstash:logstash /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chmod 755 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chmod 664 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-api/2.18.0/log4j-api-
2.18.0.jar

sudo rm /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.6.2/log4j-core-
2.6.2.jar
sudo rmdir /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.6.2
sudo mkdir /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.18.0
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-core-
2.18.0.jar /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.18.0/ sudo
chown -R logstash:logstash /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.18.0/
sudo chmod 755 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.18.0/
sudo chmod 664 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.18.0/log4j-
core-2.18.0.jar

sudo rm /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-slf4j-
impl/2.6.2/log4j-slf4j-impl-2.6.2.jar
sudo rmdir /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-slf4j-impl/2.6.2
sudo mkdir /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-slf4j-impl/2.18.0
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-slf4j-impl-
2.18.0.jar /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-slf4j-impl/2.18.0/
sudo chown -R logstash:logstash /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-slf4j-impl/2.18.0/
sudo chmod 755 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-slf4j-impl/2.18.0/
sudo chmod 664 /usr/share/logstash/logstash-
```

```
core/lib/org/apache/logging/log4j/log4j-slf4j-
impl/2.18.0/log4j-slf4j-impl-2.18.0.jar

sudo rm
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-log4j-3.1.3-java/vendor/jar-dependencies/runtime-
jars/log4j-1.2.17.jar
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-1.2-api-
2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-log4j-3.1.3-java/vendor/jar-dependencies/runtime-jars/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-api-
2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-log4j-3.1.3-java/vendor/jar-dependencies/runtime-jars/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-core-
2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-log4j-3.1.3-java/vendor/jar-dependencies/runtime-jars/
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-log4j-3.1.3-java/vendor/jar-dependencies/runtime-
jars/log4j-1.2-api-2.18.0.jar
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-log4j-3.1.3-java/vendor/jar-dependencies/runtime-
jars/log4j-api-2.18.0.jar
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-log4j-3.1.3-java/vendor/jar-dependencies/runtime-
jars/log4j-core-2.18.0.jar
sudo chmod 644
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-log4j-3.1.3-java/vendor/jar-dependencies/runtime-
jars/log4j-*

sudo rm
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
output-kafka-5.1.11/vendor/jar-dependencies/runtime-
jars/log4j-1.2.17.jar
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-1.2-api-
```

```
2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
output-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-api-
2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
output-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-core-
2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
output-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
output-kafka-5.1.11/vendor/jar-dependencies/runtime-
jars/log4j-1.2-api-2.18.0.jar
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
output-kafka-5.1.11/vendor/jar-dependencies/runtime-
jars/log4j-api-2.18.0.jar
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
output-kafka-5.1.11/vendor/jar-dependencies/runtime-
jars/log4j-core-2.18.0.jar
sudo chmod 644
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
output-kafka-5.1.11/vendor/jar-dependencies/runtime-
jars/log4j-*

sudo rm
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-beats-3.1.32-java/vendor/jar-
dependencies/org/apache/logging/log4j/log4j-api/2.6.2/log4j-
api-2.6.2.jar
sudo rmdir
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-beats-3.1.32-java/vendor/jar-
dependencies/org/apache/logging/log4j/log4j-api/2.6.2
sudo mkdir
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-beats-3.1.32-java/vendor/jar-
dependencies/org/apache/logging/log4j/log4j-api/2.18.0
sudo cp /tmp/apache-log4j-2.18.0-bin/log4j-api-2.18.0.jar
```

```
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-beats-3.1.32-java/vendor/jar-
dependencies/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chown -R logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-beats-3.1.32-java/vendor/jar-
dependencies/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chmod 755
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-beats-3.1.32-java/vendor/jar-
dependencies/org/apache/logging/log4j/log4j-api/2.18.0
sudo chmod 644
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-beats-3.1.32-java/vendor/jar-
dependencies/org/apache/logging/log4j/log4j-api/2.18.0/log4j-
api-2.18.0.jar

sudo rm
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/log4j-
slf4j-impl-2.8.2.jar
sudo cp /tmp/apache-log4j-2.18.0-bin/log4j-slf4j-impl-
2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/log4j-
slf4j-impl-2.18.0.jar
sudo chmod 664
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/log4j-
slf4j-impl-2.18.0.jar

sudo rm
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/log4j-
api-2.8.2.jar
sudo cp /tmp/apache-log4j-2.18.0-bin/log4j-api-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/
sudo chown logstash:logstash
```

```
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/log4j-
api-2.18.0.jar
sudo chmod 664
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-
input-kafka-5.1.11/vendor/jar-dependencies/runtime-jars/log4j-
api-2.18.0.jar

grep -Rl "log4j-api" /usr/share/logstash/* | xargs sudo sed -i
's/2\.6\.2/2\.18\.0/g'
```

6. Restart the associated services on ElasticSearch, Monitoring and UI for both sets of processes:

```
sudo systemctl status [server]_elasticsearch.service
sudo systemctl start [server]_elasticsearch.service
sudo systemctl status [server]_elasticsearch.service

sudo systemctl status logstash.service
sudo systemctl start logstash.service sudo systemctl status
logstash.service
```

7. Remove the log4j backup:

```
sudo rm -rf /tmp/3402upgrade
sudo rm /tmp/fba-hotfix-3402.tar
```

8. Stop the Kafka service:

```
sudo systemctl status kafka
sudo systemctl stop kafka
sudo systemctl status kafka
```

9. Update the Kafka instances to resolve the log4j issues on the environments:

```
sudo rm /usr/lib/kafka/libs/log4j-1.2.17.jar
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-1.2-api-
2.18.0.jar /usr/lib/kafka/libs/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-core-
2.18.0.jar /usr/lib/kafka/libs/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-api-
2.18.0.jar /usr/lib/kafka/libs/
```

```
sudo chown kafka:kafka /usr/lib/kafka/libs/log4j-1.2-api-
2.18.0.jar
sudo chown kafka:kafka /usr/lib/kafka/libs/log4j-core-
2.18.0.jar
sudo chown kafka:kafka /usr/lib/kafka/libs/log4j-api-
2.18.0.jar
sudo chmod 755 /usr/lib/kafka/libs/log4j-*

sudo rm /usr/lib/zookeeper/lib/log4j-1.2.16.jar
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-1.2-api-
2.18.0.jar /usr/lib/zookeeper/lib/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-core-
2.18.0.jar /usr/lib/zookeeper/lib/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-api-
2.18.0.jar /usr/lib/zookeeper/lib/

sudo chown zookeeper:zookeeper /usr/lib/zookeeper/lib/log4j-
1.2-api-2.18.0.jar sudo chown zookeeper:zookeeper
/usr/lib/zookeeper/lib/log4j-core-2.18.0.jar
sudo chown zookeeper:zookeeper /usr/lib/zookeeper/lib/log4j-
api-2.18.0.jar
sudo chmod 644 /usr/lib/zookeeper/lib/log4j-*

sudo rm /usr/lib/zookeeper/contrib/rest/lib/log4j-1.2.15.jar
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-1.2-api-
2.18.0.jar /usr/lib/zookeeper/contrib/rest/lib/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-api-
2.18.0.jar /usr/lib/zookeeper/contrib/rest/lib/
sudo cp /tmp/3402upgrade/ansible/files/jar/log4j-core-
2.18.0.jar /usr/lib/zookeeper/contrib/rest/lib/

sudo chown zookeeper:zookeeper
/usr/lib/zookeeper/contrib/rest/lib/log4j-1.2-api-2.18.0.jar
sudo chown zookeeper:zookeeper
/usr/lib/zookeeper/contrib/rest/lib/log4j-api-2.18.0.jar
sudo chown zookeeper:zookeeper
/usr/lib/zookeeper/contrib/rest/lib/log4j-core-2.18.0.jar
sudo chmod 644 /usr/lib/zookeeper/contrib/rest/lib/log4j-*
```

10. Restart the Kafka services:

```
sudo systemctl status kafka
sudo systemctl start kafka
sudo systemctl status kafka
```

11. Remove backup files:

```
sudo rm -rf /tmp/3402upgrade
sudo rm /tmp/fba-hotfix-3402.tar
```

12. Apply new versions of the FBA service `.jar` files to the following hosts:

    API server: `/usr/lib/java/ro-api/ro-api.jar`

    Content server: `/usr/lib/java/ro-content/ro-content.jar`

    Conversion server: `/usr/lib/java/ro-conv/ro-conv.jar`

    Jenkins server: `/usr/lib/java/ro-schema/ro-schema.jar`

    Nifi server: `/usr/share/java/ro-ingest-utils/ro-ingest-utils.jar`

    QW server: `/usr/lib/java/ro-qw/ro-qw.jar`

    Rose server: `/usr/lib/java/ro-rose/ro-rose.jar`

    MDS server: `/usr/lib/java/ro-mds/ro-mds.jar`

    MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar`

13. Copy the service `.jar` files to the appropriate host in the FBA environment:

```
from the Jenkins host
scp -P 2222 /data/html/3402upgrade/ansible/files/jar/<FBA
SERVICE>.jar.3402 /tmp/<FBA SERVICE>.jar.3402

ssh centos@<FBA SERVICE>-yourenvironment
sudo systemctl stop <FBA SERVICE>
sudo systemctl status <FBA SERVICE> cd /usr/lib/java/<FBA
SERVICE FOLDER>
sudo mv /usr/lib/java/<FBA SERVICE FOLDER>/<FBA SERVICE>.jar
/usr/lib/java/<FBA SERVICE FOLDER>/<FBA SERVICE>.jar.pre3402
sudo mv /tmp/<FBA SERVICE>.jar.3402 /usr/lib/java/<FBA SERVICE
```

```
FOLDER>/<FBA SERVICE>.jar.3402
sudo cp -p /usr/lib/java/<FBA SERVICE FOLDER>/<FBA
SERVICE>.jar.3402 /usr/lib/java/<FBA SERVICE FOLDER>/<FBA
SERVICE>.jar
sudo systemctl start <FBA SERVICE>
sudo systemctl status <FBA SERVICE>

Repeat these steps for each of the <FBA SERVICES> listed in
Step 13
```

14. Remove old version of the `.jar` file from each environment:

Tip
Make sure all environments have been updated and tested before removing the old `.jar` files.

```
#example
sudo rm /usr/lib/java/<FBA SERVICE FOLDER>/<FBA
SERVICE>.jar.pre3402
```

15. Update UI node with the new version:

```
from the Jenkins host:
scp -P 2222 <FBA UI SERVICE>
/data/html/3402upgrade/ansible/files/rpm/ro-ui-1.98.2-
0.6.20220914git7e48eb7f95.el7.x86_64.rpm /tmp/ro-ui-1.98.2-
0.6.20220914git7e48eb7f95.el7.x86_64.rpm

ssh centos@<FBA UI SERVICE>-yourenvironment
sudo systemctl stop ro-ui
sudo systemctl status ro-ui

#backup the /usr/lib/node_modules/ro-ui folder and contents:
sudo tar -cvfz /data/3402-backup-previous/ro-ui.backup.tar
/usr/lib/node_modules/ro-ui/

sudo mv /etc/ro-ui/version.yml /etc/ro-ui/version.yml.previous

#install the new UI via the following command:
sudo rpm -Uvh /tmp/ro-ui-1.98.2-
0.6.20220914git7e48eb7f95.el7.x86_64.rpm
```

```
apply any custom UI changes that are required.

sudo systemctl start ro-ui
sudo systemctl status ro-ui
```

16. Patch Minigator tool.

    Because the host location of the Minigator can be determined per individual installation, the steps can not be specific. A summary of the patch actions are as follows:

    Tip
    Patching the Minigator tool is only required if it has been deployed.

    a. Copy the minigator `.rpm` file from the Jenkins host:

    ```
    /data/html/3402upgrade/ansible/files/rpm/minigator-1.98.1-1.el7.x86_64.rpm
    ```

    b. Remove the old minigator `.jar` file.

    c. Install the new minigator `.rpm` file:

    ```
    sudo rpm -Uvh minigator-1.98.1-1.el7.x86_64.rpm
    ```

    Important
    Any custom UI changes must be applied manually. Forcepoint will not persist those changes to the new version.

17. Remove backup files that were created during install to ensure that all files with the old versions of Log4j library code are removed. The following locations will have backup files:

    API server: `/usr/lib/java/ro-api/ro-api.jar.pre3402`

    Content server: `/usr/lib/java/ro-content/ro-content.jar.jar.pre3402`

    Conversion server: `/usr/lib/java/ro-conv/ro-conv.jar.jar.pre3402`

    Jenkins server: `/usr/lib/java/ro-schema/ro-schema.jar.jar.pre3402`

    Nifi server: `/usr/share/java/ro-ingest-utils/ro-ingest-utils.jar.jar.pre3402`

    QW server: `/usr/lib/java/ro-qw/ro-qw.jar.jar.pre3402`

    Rose server: `/usr/lib/java/ro-rose/ro-rose.jar.jar.pre3402`

    MDS server: `/usr/lib/java/ro-mds/ro-mds.jar.jar.pre3402`

    MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.jar.pre3402`

UI server: `/data/3402-backup-previous/ro-ui.backup.tar`

INSTALLATION BACKOUT

1. Replace patched version of the FBA service `.jar` file with the original `.jar` file in each environment:

```
sudo systemctl stop <FBA SERVICE>
cd /usr/lib/java/<FBA SERVICE FOLDER>
sudo rm /usr/lib/java/<FBA SERVICE FOLDER>/<FBA SERVICE>.jar
sudo mv /usr/lib/java/<FBA SERVICE FOLDER>/<FBA
SERVICE>.pre3402 /usr/lib/java/<FBA SERVICE FOLDER>/<FBA
SERVICE>.jar
sudo systemctl start <FBA SERVICE>
```

The hosts and location of the `.jar` files are as follows:

Pre-Patch Versions

API server: `/usr/lib/java/ro-api/ro-api.jar.pre3402`

Content server: `/usr/lib/java/ro-content/ro-content.jar.pre3402`

Conversion server: `/usr/lib/java/ro-conv/ro-conv.jar.pre3402`

Jenkins server: `/usr/lib/java/ro-schema/ro-schema.jar.pre3402`

Nifi server: `/usr/share/java/ro-ingest-utils/ro-ingest-utils.jar.pre3402`

QW server: `/usr/lib/java/ro-qw/ro-qw.jar.pre3402`

Rose server: `/usr/lib/java/ro-rose/ro-rose.jar.pre3402`

MDS server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3402`

MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3402`

Destination

API server: `/usr/lib/java/ro-api/ro-api.jar`

Content server: `/usr/lib/java/ro-content/ro-content.jar`

Conversion server: `/usr/lib/java/ro-conv/ro-conv.jar`

Jenkins server: `/usr/lib/java/ro-schema/ro-schema.jar`

Nifi server: `/usr/share/java/ro-ingest-utils/ro-ingest-utils.jar`

QW server: `/usr/lib/java/ro-qw/ro-qw.jar`

Rose server: `/usr/lib/java/ro-rose/ro-rose.jar`

MDS server: `/usr/lib/java/ro-mds/ro-mds.jar`

MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar`

2. Back out UI changes.

   Tip
   After backing out the UI changes, performing one of the following options is suggested:

   Option 1:

   - Redeploy the UI via Jenkins job.
   - Apply any UI patch that ay have been introduced.

   Option 2:

   - Extract the backup the patch installer created:

     ```
     sudo tar -xvf /data/3402-backup-previous/ro-ui.backup.tar -C /usr/lib/node_modules/ro-ui/
     ```

3. Other Servers:

   ```
   # Re-deploy via Jenkins job. build deploy elastic build deploy logstash build deploy monitoring build deploy kafka
   ```