

Forcepoint Behavioral Analytics

UPGRADE GUIDE FOR HOTFIXES (3.3.2.2 & 3.3.3.1)

THESE ITEMS ARE CONTROLLED BY THE U.S. GOVERNMENT AND AUTHORIZED FOR EXPORT ONLY TO THE COUNTRY OF ULTIMATE DESTINATION FOR USE BY THE ULTIMATE CONSIGNEE OR END-USER(S). THEY MAY NOT BE RESOLD, TRANSFERRED, OR OTHERWISE DISPOSED OF, TO ANY OTHER COUNTRY OR TO ANY PERSON OTHER THAN THE AUTHORIZED ULTIMATE CONSIGNEE OR END-USER(S), EITHER IN THEIR ORIGINAL FORM OR AFTER BEING INCORPORATED INTO OTHER ITEMS, WITHOUT FIRST OBTAINING APPROVAL FROM THE U.S. GOVERNMENT OR AS OTHERWISE AUTHORIZED BY U.S. LAW AND REGULATIONS.

PROPRIETARY

Publish Date: February 17, 2022

Copyright © 2022

F23-09-02-02172022

Legal Notice

No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the company. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this document, the authors and the company assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. The company cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or completeness is implied. The provided information is on an "as is" basis. The authors and the company shall have neither liability nor responsibility for any loss or damages arising from the information contained in this document. Printed in the United States of America.

This document contains proprietary information and is furnished for evaluation purposes only, and, except with written permission of the vendor, such information shall not be published, or disclosed to others, or used for any other purpose, or duplicated in whole or in part.

Attributions

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. The company cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

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.