Bottomline

CFRM Record and Replay Trial

For Datadog

December 05th, 2022

Legal Statement

Bottomline Technologies Cyber Fraud and Risk Management

Information in this document is subject to change without notice and does not represent a commitment on the part of Bottomline Technologies. Bottomline Technologies makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability or fitness for particular purpose.

Bottomline Technologies

Corporate Headquarters

325 Corporate Drive

Portsmouth, NH 03801 USA

Europe, Middle East, Africa

1600 Arlington Business Park

Theale, Reading, Berkshire RG7 4SA UK

APAC Headquarters

Level 3, 69-71 Edward Street

Pyrmont, Sydney NSW 2009, AU

60 Robinson Road

#15-01 BEA Building

Singapore 068892

Table of Content

Europe, Middle East, Africa
1600 Arlington Business Park,
Theale, Reading, Berkshire RG7 4SA
United Kingdom
www.bottomline.com

I. Pre-requisites

Datadog Agent:

1. Run from shell: `DD_API_KEY=1234 DD_SITE="datadoghq.com" bash -c "$(curl -L https://s3.amazonaws.com/dd-agent/scripts/install_script_agent7.sh)`
2. Edit: /etc/datadog-agent/datadog.yaml
    a. logs_enabled: true
3. Create directory: /etc/datadog-agent/conf.d/Bottomline.d
4. Create file named conf.yaml with contents below with your details for path, service, and source:

```
logs:

 - type: file

   path: "/myDrive/logs/myapp*.log"

   service: "mainframe"

   source: "bottomline"
```

5. Restart agent by running the following from shell:
    a. systemctl stop datadog-agent
    b. systemctl start datadog-agent

Create a Database:

Supported DBs: Postgres or Oracle – See CFRM Product Overview Guide for production supported databases and versions.

1. Note the connection details: name, location, port, username, password

II. Bottomline Installation

Install Enterprise Manager:

EM is used to manage configurations from a Windows Desktop.

1. Click CFRM-version.exe located in the Enterprise Manager for Windows folder
    a. Click Next to start install
    b. Select install folder and click Next
    c. Unselect Server, leaving only Enterprise Manager (not Web-Start) and Click Next
    d. Click through agree and next buttons to complete

Europe, Middle East, Africa
1600 Arlington Business Park,
Theale, Reading, Berkshire RG7 4SA
United Kingdom
www.bottomline.com

Install CFRM Record and Replay Trial:

Option 1 - Container Based:

1. Run from shell in/myDrive: tar -zxvf archive-bottomline-trial.tar.gz ./
2. Copy your license file as license.xml file to the /myDrive/Server/license folder
3.
```
docker run -d --name rr-trial /
 -v /myDrive/Server/license:/opt/cfrm/Server/license /
 -v /myDrive/Server/servers/testcfrmsvc:/opt/cfrm/Server/servers/cfrmsvc /
 -v /myDrive/Queues:/Queues /
 -v /myDrive/logs:/var/myapp/logs /
 -p 2345:2345 /
 -p 8023:8023 /
 nbk96f1/cfrm:latest
```

Notes:

- cfrmsvc mapping: makes service changes persistent outside container. Files from archive contain the trial implementation and sample of screen mappings
- logs mapping: are where the JSON user events will be written on the server for the datadog agent
- queues mapping: an example on how to make the queues outside the container (not used). It is also possible to use a message queue service as recommended for production.
- Port 2345 mapping: this is the port Enterprise Manager will use to configure and administrate Record and Replay
- Port 8023 mapping: this is the web viewer port for Replay via http or https

Option 2 - Linux install files:

1. Install Pre-requisites: OpenJDK
    a. Note: Libpcap is not needed unless capturing network traffic from a network card. Please refer to Record and Replay Configuration guide for this if needed.
2. Copy install.sh and CFRM-<version>-<build>.tar.gz to the linux server install director
3. Run from shell: chmod -R 777 .*
4. Run from shell: ./install.sh
5. Complete the install by following the prompts, select No to starting the container now.
6. Copy the contents of the archive-bottomline-trial.gz to the appropriate directories in the install folders.
7. Run from shell in the install directory: ./smCLI.sh start all

Note: See Record and Replay Configuration Guide for additional install and configuration options if needed.

Setup CFRM Record and Replay Trial:

1. Open Enterprise Manager
2. Right Click in Services box and select Add Server

Europe, Middle East, Africa
1600 Arlington Business Park,
Theale, Reading, Berkshire RG7 4SA
United Kingdom
www.bottomline.com

    a. Enter address of docker container or server where installed and 2345 for port and click OK
3. Right click BacklogWriter and select Open
4. Click Modify next to Database Connection
5. Select Database type on General Tab
6. Click Database Properties tab and enter connection Information, click OK
7. Click Synchronize Schema and then click OK to save
8. Right click on BacklogWriter and click Start Service
9. Right click on Viewer and click Start Service
10. Select the Implementation Tab
11. Navigate to Common/replay/replay_url Rick Click and select Open
12. Update the IP/Port (default port is 8023) in the URL string for your CFRM container details and select OK
13. Right Click on dc_3270 and select Deploy Entity and click Next
14. Select Yes to restart the Data Channel after deploying and click Finish

Note: you can change the logger for where the JSON files are written if needed by modifying the EventsToExternalSystem configuration entity in Enterprise Manager by right clicking on the service under the Administration tab and selecting Show Configuration Entities which will allow you to modify this object.

Load sample recordings from Enterprise Manager:

- Method 1: Provided sample recordings mainframe traffic
    1. From the administration tab, Right Click dc_3270 and select Load Recordings
    2. Select the folder where the recordings were downloaded from the Sample Recording Files folder and select Finish
- Method 2: Your PCAP from a tcpdump of user sessions from your mainframe
    1. From the administration tab, Right Click sensor_3270 and select Open
    2. Select the Capture Device tab
    3. Select CaptureDevice_PCAP and click Modify
    4. Select the Device Properties tab
    5. Update the Path field with the file name and location of your PCAP file and select OK
    6. Right Click the sensor_3270 and select Start Service
    7. Right Click the sensor_3270 and select Stop Service

Validate Recordings Processed Successfully:

In addition to seeing the user events in the log, you can check that the recordings processed successfully and replay these from Enterprise Manager by following the instructions below.

1. Select the Investigation tab
2. Right Click on Reports and select New -> Event Viewer Report
3. Click Finish
4. Update the “In the last” field to last 20 Years and click Execute Query
5. Right Click any recording to Replay

Europe, Middle East, Africa
1600 Arlington Business Park,
Theale, Reading, Berkshire RG7 4SA
United Kingdom
www.bottomline.com

Integration with Existing Bottomline Record and Replay:

Integration between Datadog and Bottomline leverages the Datadog agent custom log feature which can be setup using the instruction in the pre-requisite section of this guide for setting up the Datadog agent. For the JSON message creation in the logs from Record and Replay we have provided an IER file in the Integrations folder to import in the Implementation tab of Enterprise Manager: “Repository_3270_JSON_UserEvent_<version>.ier.zip”.

1. In the Implementation tab of Enterprise Manager Right Click on the repository and select Import
2. Select the provided IER file and follow the prompts to import
3. Update the replay URL: Right Click on Common/replay/replay_url and select Open
4. Update the IP/Port (default port is 8023) in the URL string for your CFRM container details and select OK
5. The dc_3270/events folder contains sample events that can be used to generate the JSON messages or can be copied into your Data Channel to create these messages for sending to Datadog.

Note: you can change the logger for where the JSON files are written if needed by modifying the EventsToExternalSystem configuration entity in Enterprise Manager by right clicking on the service under the Administration tab and selecting Show Configuration Entities which will allow you to modify this object.

Europe, Middle East, Africa
1600 Arlington Business Park,
Theale, Reading, Berkshire RG7 4SA
United Kingdom
www.bottomline.com