# Forcepoint Behavioral Analytics

## HARDENING GUIDE

Publish Date: December 20, 2023



F23-08-00-00

## 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.<br>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.<br>Example: Read the *User's Guide.* |
| Monospaced font | Used to identify names of commands, files, and directories.<br>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.<br>Example: Type **`SYSTEMHIGH`** in the **Network** field. |
| Shaded monospaced font | Used to identify screen output.<br>Example: A network device must exist; otherwise, the following warning message displays<br>`Warning: device [DEVICE] is not a valid network device` |
| Shaded monospaced bold font | Used to identify text that users need to type.<br>Example: Specify your network configuration. Type:<br>**`$ 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 Hardening Guide

This guide is a generalized set of recommendations for installing Forcepoint Behavioral Analytics (FBA) in a customer's environment. There will be many customizations based on customer requirements, and this should not be viewed as an exhaustive list.

We highly recommend that Professional Services follow these guidelines when deploying FBA. The recommendations will greatly enhance the security of the application. If for any reason a customer cannot or will not implement FBA in the manner we describe below, they should be aware of the greater risk they are taking on. For example, exposing internal application endpoints to a corporate network increases the risk of malicious insiders exfiltrating data or conducting denial of service attacks.

## DOCKER LOGIN

If using the 3.4.1 Limited Availability release (with containerization), the Docker container must be logged into in order to make any changes to the FBA Services.

To login to the Docker container, perform the following:

1. Add -p 2222 to your typical SSH command such as:

```
ssh FBA_USER@service-HOSTNAME -p 2222
```

2. Log into the VM OS using your typical SSH command and then log into the container such as:

```
ssh FBA_USER@service-HOSTNAME
```

```
docker exec -it $(docker ps --format "{{.Names}}") bash
```

**Tip**
For further information on additional Docker related commands, refer to the Docker documentation.

## GENERAL RECOMMENDATIONS

We recommend that the entire system is installed onto a private virtual LAN and placed behind a firewall with rules that limit inbound and outbound traffic to trusted sources. See example rules listed below.

We also recommend that Professional Services install fail2ban on NiFi, Postfix, the Public API, and any other server in the system, and configure to trigger a firewall rule to block incoming connections from incoming IP traffic after several failed authentication attempts. See example configurations below.

If unable to place the entire system on a private virtual LAN, utilize Iptables to only accept inbound connections from expected sources. For example, the Public API can be configured to only accept inbound connections from Postfix, NiFi, and other specified IPs.

Credentials are updated from their defaults by Professional Services at time of installation. It is recommended that passwords be regularly changed and stored in a secure location.

## EXAMPLE FIREWALL SETTINGS

### Inbound Firewall Rules to FBA Environment

| | |
|---|---|
| **Source** | Remote Management Access for Administrators (Professional Services and internal admins) |
| **Destination (IP)** | VMWare ESXi Hypervisor host (Physical Server) |
| **Service Port** | TCP 22,443,902 |
| **Notes** | This is only if an appliance (server(s)) was provided for the FBA application stack. |

| | |
|---|---|
| **Source** | Remote Management Access for Administrators (Professional Services and internal admins) |
| **Destination (IP)** | All Forcepoint Analytics (FBA) Servers – SSH |
| **Service Port** | TCP 22 |
| **Notes** | |

| | |
|---|---|
| **Source** | DLP Server(s) – DDP functionality with DLP |
| **Destination (IP)** | Kafka server |
| **Service Port** | TCP 9092-9095 |
| **Notes** | This is only required for DDP functionality with DLP. This traffic is encrypted and authenticated using TLS, using DLP-inherited certs. |

| | |
|---|---|
| **Source** | Mail Server(s) – Journaling functionality |
| **Destination (IP)** | Postfix server |
| **Service Port** | TCP 25,587 |
| **Notes** | If email server uses static IP, customer can use IP to filter incoming traffic. If emails come from O365, or other dynamic IP address, that won't be an option. Email address and domain for the 'To' address should be allow-listed, and other domains can be rejected. |

| | |
|---|---|
| **Source** | Management Access for Administrators (Professional Services and internal admins) |
| **Destination (IP)** | Rabbit Server – rabbitmq server |
| **Service Port** | TCP 15672 |
| **Notes** | http://rabbit-ip-address:15672/ |

| | |
|---|---|
| **Source** | Management Access for Administrators (Professional Services and internal admins) |
| **Destination (IP)** | Monitoring Server – monitoring server |
| **Service Port** | TCP 443,5601 |
| **Notes** | https://monitoring-ip-address/<br>https://monitoring-ip-address:5601/ |

| | |
|---|---|
| **Source** | Remote Management Access for Administrators (Professional Services and internal admins) |
| **Destination (IP)** | UI Server – FBA UI server |
| **Service Port** | TCP 443 |
| **Notes** | https://ui-ip-address/ |

| | |
|---|---|
| **Source** | Remote Management Access for Administrators (Professional Services and internal admins) |
| **Destination (IP)** | NIFI Server – nifi server |
| **Service Port** | TCP 443,8080 |
| **Notes** | https://nifi-ip-address/nifi/<br>http://nifi-ip-address:8080/nifi/ |

| | |
|---|---|
| **Source** | Management Access for Administrators (Professional Services and internal admins) |
| **Destination (IP)** | New Jenkins Server – Jenkins server |
| **Service Port** | TCP 8080,8443 |
| **Notes** | http://jenkins-ip-address:8080/<br>https://jenkins-ip-address:8443/ |

| | |
|---|---|
| **Source** | Load Balancer – MDS load balancing against ES nodes |
| **Destination (IP)** | ES servers |
| **Service Port** | TCP 8080 |
| **Notes** | |

### Additional Inbound Firewall Rules to FBA Environment

**Note**

These additional rules will be for data ingest into the application. These are not an exhaustive list and will be specific to the data sources they come from.

| | |
|---|---|
| **Source** | Customer specific data sources (for example: Splunk, Syslog.) |
| **Destination (IP)** | Public API and Nifi services |
| **Service Port** | TBD based off of specific use cases and data sources. |
| **Notes** | |

### Outbound Firewall Rules from FBA Environment

| | |
|---|---|
| **Source** | UI Server – UI load balancing against MDS nodes |
| **Destination (IP)** | Load Balancer |
| **Service Port** | TCP 8080 |
| **Notes** | |

| | |
|---|---|
| **Source** | All Forcepoint Analytics (FBA) Servers |
| **Destination (IP)** | External package repositories and NTP. No Certificates, and No Authentication |
| **Service Port** | UDP 123, TCP 443 |
| **Notes** | |

| | |
|---|---|
| **Source** | FBA Kafka server – DDP functionality with DLP |
| **Destination (IP)** | DLP server(s) |
| **Service Port** | TCP 17433 |
| **Notes** | This is only required for DDP functionality with DLP. This traffic is encrypted and authenticated using TLS, using DLP-inherited certs. |

| | |
|---|---|
| **Source** | Nifi Server |
| **Destination (IP)** | UAM System Oracle Database |
| **Service Port** | TCP 1521 |
| **Notes** | This is only required for FBA to collect endpoint data through the UAM System. |

### Fail2Ban Example Configuration

fail2ban for CentOS and Red Hat will be made available in the 3.3.2 release, included in the EPEL rpm repository. This is not installed by default, but we strongly recommend that Professional Services configure this during installation. Example configurations are given below.

The configuration of fail2ban is typically stored in `/etc/fail2ban` and includes canned recipes for many software packages, including the ones we care about, `nginx-http-auth.conf` and `postfix.conf`.

A `nginx-http-auth.conf` configuration looks like this:

```
# fail2ban filter configuration for nginx
[Definition]
failregex = ^ \[error\] \d+#\d+: \*\d+ user "\S+":? (password mismatch|was not found
in ".*"),
client: <HOST>, server: \S*, request: "\S+ \S+
HTTP/\d+\.\d+", host: "\S+"(, referrer: "\S+")?\s*$ ignoreregex =
# DEV NOTES:

# Based on samples in https://github.com/fail2ban/fail2ban/pull/43/files
# Extensive search of all nginx auth failures not done yet. #
# Author: Daniel Black
```

And will catch any failed HTTP basic auth login failures.

A configuration for postfix looks like this:

```
# Fail2Ban filter for selected Postfix SMTP rejections
# #
[INCLUDES]
# Read common prefixes. If any customizations available -- read them from #
common.local
before = common.conf [Definition]
_daemon = postfix/(submission/)?smtp(d|s)
failregex = ^%(  prefix_line)sNOQUEUE: reject: RCPT from \S+\[<HOST>\]: 554 5\.7\.1
.*$
^%(  prefix_line)sNOQUEUE: reject: RCPT from \S+\[<HOST>\]: 450 4\.7\.1 Client host
rejected:
cannot find your hostname, (\[\S*\]); from=<\S*> to=<\S+> proto=ESMTP helo=<\S*>$
^%(  prefix_line)sNOQUEUE: reject: RCPT from \S+\[<HOST>\]: 450 4\.7\.1 : Helo command
rejected:
Host not found; from=<> to=<> proto=ESMTP helo= *$
^%(  prefix_line)sNOQUEUE: reject: VRFY from \S+\[<HOST>\]: 550 5\.1\.1 .*$
^%(  prefix_line)simproper command pipelining after \S+ from [^[]*\ [<HOST>\]:?$
ignoreregex = [Init]
journalmatch = _SYSTEMD_UNIT=postfix.service
# Author: Cyril Jaquier
```

We would want to modify this to include matching on the condition where mail is being directed to an address that is not the configured reception address.

**Note**

These filters have to be enabled by a suitable file in the `jail.d` directory. *For example*: for postfix:

```
[postfix]
enabled = true
```

A corresponding file for nginx will need to be added to the nifi host.

These configurations detect repeated failures (3 failures within 10 minutes, by default) and institute automatic firewall rules to prevent exploitative traffic. By default, fail2ban times out these blocks after a period of time (typically 30 minutes), but in our use case where we expect only known authorized data to be inbound via postfix and/or nifi, we could set them to begin blocking immediately (no grace period) and to retain the block for a longer period of time (even multiple days if needed).

## DISABLING TLSV1.0/1.1 ACROSS FBA PRODUCT

### Eligible Versions of FBA Product

Although this was tested on FBA v3.3.3, these changes should be identical for the FBA product from v3.1.x and onward. Although they may also work on earlier versions, those are not currently supported by this documentation and may yield unexpected results.

### Affected Services

Below is a list of services that will need to be adjusted to remove the deprecated versions of TLS.

- elasticsearch
- kibana
- Kafka
- RabbitMQ
- postgres
- vault

A certain level of TLS will be need to be enforced (either explicitly or via the ciphers that are listed) . The steps to do this are listed below for each of the affected services. These steps will need to be performed on each host and monitoring host.

**Elasticsearch**

On the monitoring host and all elasticsearch hosts, perform the following steps:

1. Navigate to the ealsticsearch configuration file.
   a. This file is typically located here: `/etc/elasticsearch/<host>-<stack-name>/elasticsearch.yml`
   b. Insert the following code into the config file:

```
xpack.ssl.supported_protocols: TLSv1.2
```

2. Restart the elasticsearch service:

```
sudo systemctl restart <host>-<stack-name>_elasticsearch.service
```

**Tip**
For more information on the Elasaticsearch service, please refer to the Elasticsearch documentation.

### Kibana

On the monitoring host and all elasticsearch hosts, perform the following steps:

1. Navigate to the kibana configuration file.
   a. This is typically located here: `/etc/kibana/kibana.yml`
   b. Insert the following code into the config file:

```
server.ssl.supportedProtocols: ["TLSv1.2"]
```

2. Restart the Kibana service:

```
sudo systemctl restart kibana.service
```

**Tip**
For more information on the Kibana service, please refer to the Kibana documentation.

### Kafka

1. On the Kafka host, navigate to the Kafka server configuration file.
   a. This is typically located here: `/etc/kafka/conf/server.properties`
   b. Insert the following code into the config file:

```
ssl.enabled.protocols=TLSv1.2
```

2. Restart the Kafka service:

```
sudo systemctl restart kafka.service
```

**Tip**
For more information on the Kafka service, refer to the Kafka documentation.

### RabbitMQ

1. On the RabbitMQ host, navigate to the RabbitMQ configuration file.
   a. This is typically located here: `/etc/rabbitmq/rabbitmq.config`
   b. Replace the following code into the config file:

```
# Original{ssl, [{versions, ['tlsv1.2', 'tlsv1.1']}]}
# new code
{ssl, [{versions, ['tlsv1.2']}]}
```

2. Restart the RabbitMQ service:

```
sudo systemctl restart rabbitmq-server.service
```

**Tip**
For more information on the RabbitMQ service, please refer to the RabbitMQ documentation.

### Postgres

1. On the postgres host, navigate to the postgres configuration file.
   a. This is typically located here: `/data/ro-postgres/postgresql.conf`
   b. Add the following code into the config file:

```
ssl_prefer_server_ciphers = true ssl_ciphers = 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:DHE-RSA-AES128-SHA256:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK'
```

2. Restart the postgres service:

```
sudo systemctl restart postgresql-9.6.service
```

**Tip**
For more information on the postgres service, please refer to the postgress documentation.

### Vault

1. On the Jenkins host, navigate to the `vault.hcl` configuration file.
   a. In a default deployment, this is located here: `/etc/vault/vault.hcl`
   b. Edit the `vault.hcl` configuration file and add the following code inside of the listener "tcp" stanzas:

```
1 listener "tcp" {tls_min_version = "tls12"
2 tls_cipher_suites = "TLS_RSA_WITH_AES_128AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_
  AES_128_GCM_SHA256"tls_prefer_server_cipher_ s
3 }
4
```

**Important**
This change has already been implemented into the default deployment of FBA; this adjustment is only needed in FBA v3.1.3 and earlier.

## ELASTICSEARCH ENCRYPTION FOR FBA 3.3.2+

For versions of FBA that are older than 3.3.2, the elasticsearch notes do not have any encryption at rest (TLS/SSL is deployed for encryption in transit). As a part of the FBA hardening efforts, encryption has been implemented for data at rest in the elasaticsearch node. This can be applied to FBA version 3.3.2 and above.

The elastic recommended solution is to use the `dm-crypt` tool for Linux based systems. This tool was chosen by the elastic team for the following reasons:

- It is widely used across the industry, showing that it has a lot of support and a robust feature set.
- It has the same algorithms used by FileVault on Mac systems, hardware based implementations, and other commercial products.
- The Package is open source and free.
- It supports many different standardized encryption formats, algorithms and features.
- It can be used to encrypt entire disks, or smaller volumes which are mounted individually. This allows one to encrypt individual indices with different keys for example (although it adds logistical complexity).
- It comes with a number of tools to manage keys, user roles and authentication, revoke access, etc.
- It provides the same semantics as a file system since it operates on the block layer (e.g. under the FS); this means that guarantees like transactional journaling provided by ext, zfs, etc. are kept. This is in contrast to FUSE options, which often re-implement "filesystem-like operations". Since these live above the FS, they can be buggy and introduce corruption into one's data which are not protected by the FS guarantees.

Beyond that, the elastic team also recommends the `encryptFS` tool or a commercial offering. Because of the reasons listed above and the fact that `dm-crypt` is the first recommended solution, the ES node hardening will be using this tool.

### Implementation

#### Prerequisites

In order to encrypt the data at rest, the following packages must be installed and available:

- `cryptsetup-luks`
- parted (if the data will be stored or encrypted on a drive partition rather than the entire drive).

#### Preparation

Before the disk encryption can be enabled and deployed, the following preparations need to be made:

1. Back up an elasticsearch data.

   **Warning**
   The encryption process will wipe any data that is on the drive, a backup **must** be made. If a drive is being added for encryption, and then migrating (rather than encrypting an existing partion/drive), a backup may not be required, but is still recommended.

2. Ensure the new drive or partition is available and not mounted.
3. Ensure that you have `root` access or `sudo` permissions.

### Implementation steps:

1. Using the cryptsetup package, format the hard drive using `LUKS`.
   a. `cryptsetup -y -v luks` Format: `/PATH/TO/STORAGE`
      i. Type 'YES' and put in your password to encrypt the storage.

      **Note**

      This password cannot be retrieved once set, ensure that it is securely stored it in a location for future retrieval.

2. Create a target to open the encrypted volume.
   a. `cryptsetup -v luks` Open `/PATH/TO/STORAGE BACKUPNAME`
   b. Run the `lsblk` command to confirm the storage is open; it will have your BACKUPNAME and a type of "crypt".
3. Format the filesystem on the encrypted volume:

```
mkfs.xfs /dev/mapper/BACKUPNAME
```

4. Create a mounting directory:

```
mkdir -p /PATH/TO/MOUNT/DIRECTORY
```

5. Mount the encrypted voume to the mounting directory:

```
mount -v /dev/mapper/BACKUPNAME /PATH/TO/MOUNT/DIRECTORY
```

### Encrypted Drive Automounting

It is not recommended to set up the automounting of the encrypted volume or partition. Having this set up removes some of the security of having the data encrypted in the first place, therefore it is recommended to have a step that requires a person to be available to enter the password.

### Example Procedure

The guide below will follow the process of encrypting the storage being used for Elastic search. This example process is being done on an AWS t2.micro instance with CentOS 7 and an additional EBS volume that is attached but not mounted.

**Prerequisites**

Ensure that the packages are installed (Figure 1).

```
[root@ip-172-31-89-12 ~]# yum list installed | grep 'cryptsetup\|parted'
cryptsetup.x86_64                       2.0.3-6.el7                @base
cryptsetup-libs.x86_64                  2.0.3-6.el7                @base
parted.x86_64                           3.1-32.el7                 @base
[root@ip-172-31-89-12 ~]#
```

Figure 1. Packages Installed

**Preparation**

1. Backup elasticsearch data.

   **Note**

   Details on this process will not be outlined as each customer deployment may have different specifications/requirements for this process.

2. Ensure new drive or partition is available and not mounted (Figure 2).

   **Note**

   In this example, a separate EBS volume (xvdb volume) will be attached and the entire disk will be encrypted, however, this step can also be performed on a partition.

3. `root`or `sudo`permissions are reqauired.

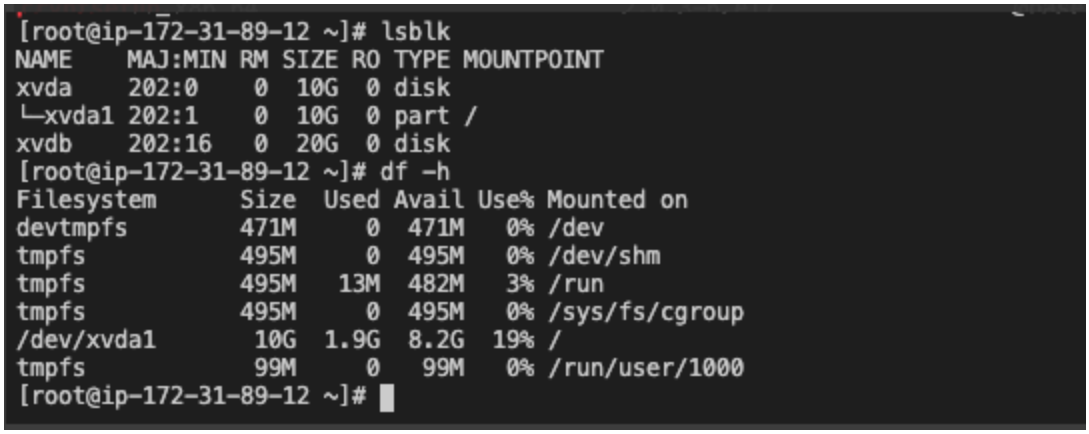


Figure 2. Partition Confirmation

**Example Steps**

1. Using the cryptsetup package, format the hard drive using `LUKS`.
   a. `cryptsetup -y -v luks` Format `/PATH/TO/STORAGE`

      Type 'YES' and put in the password to encrypt the storage.

      **Note**

      This password cannot be retrieved once set, ensure that it is securely stored it in a location for future retrieval.

      ```
      [root@ip-172-31-89-12 ~]# cryptsetup -y -v luksFormat /dev/xvdb

      WARNING!
      ========
      This will overwrite data on /dev/xvdb irrevocably.

      Are you sure? (Type uppercase yes): YES
      Enter passphrase for /dev/xvdb:
      Verify passphrase:
      Command successful.
      [root@ip-172-31-89-12 ~]#
      ```

2. Create a target to open the encrypted volume
   a. `cryptsetup -v luks` Open `/PATH/TO/STORAGE BACKUPNAME`
   b. Run the `lsblk`command to confirm that the storage is open; it will contain the backup name chosen and a type of "crypt".

## ENABLE SSL ON RABBITMQ MANAGEMENT UI

To Enable SSL on RabbitMQ using port 15672, perform the following steps:

1. Edit the `rabbitmq.config.j2` file on Jenkins:

```
/usr/share/ro-ansible/roles/rabbit/templates/rabbitmq.config.j2
```

2. Open the `rabbitmq.config` file:

```
vi /etc/rabbitmq/rabbitmq.config.j2
```

3. Locate the `rabbitmq_management` section in the `rabbitmq.config.j2` file:

```
{rabbitmq_management, [
        {load_definitions, "{{ rabbitmq_conf_dir }}/rabbitmq_definitions.json"}
  ]}
].
```

4. Replace the text in the `rabbitmq_management` section with the following code block:

```
{rabbitmq_management, [
        {load_definitions, "{{ rabbitmq_conf_dir }}/rabbitmq_definitions.json"}
        {listener, [{port, 15672},
                {ssl, true},
                {ssl_opts, [
                        {cacertfile, "{{ rabbit_ssl_certificate_authority }}" },
                        {certfile,   "{{ rabbit_ssl_certificate }}" },
                        {keyfile,    "{{ rabbit_ssl_key }}" }]}
                ]}
        ]}
   ]}
].
```

5. Save the updated `rabbitmq.config.j2` file.
6. Edit the `rabbitmq.config` file:

```
/usr/share/ro-ansible/roles/rabbit/templates/rabbitmq.config
```

7. Open the `rabbitmq.config` file:

```
vi /etc/rabbitmq/rabbitmq.config
```

8. Locate the `rabbitmq_management` section in the `rabbitmq_config` file:

```
{rabbitmq_management, [

        {load_definitions, "/etc/rabbitmq/rabbitmq_definitions.json"}

]}
```

9. Replace the text in the `rabbitmq_management` section with the following code block:

```
{rabbitmq_management, [

        {load_definitions, "/etc/rabbitmq/rabbitmq_definitions.json"},

        {listener, [{port, 15672},

                    {ssl, true},

                    {ssl_opts, [

                          {cacertfile, "/etc/pki/tls/certs/ueba-ca-bundle.crt"},

                          {certfile, "/etc/pki/tls/certs/rabbit-ueba.crt"},

                          {keyfile, "/etc/pki/tls/private/rabbit-ueba.key"}

                     ]}

        ]}

   ]}
```

10. Save the updated `rabbitmq_config` file.
11. Restart the RabbitMQ service:

```
systemctl restart rabbitmq-server.service
```