Forcepoint Behavioral Analytics Installation Manual

Installation Manual | Forcepoint Behavioral Analytics | v3.3.2 | 21-Aug-2020

Installation Overview

This Forcepoint Behavioral Analytics Installation manual guides technical Forcepoint Behavioral Analytics users through a complete installation of a Forcepoint Behavioral Analytics deployment. This guide includes step-by-step instructions for installing Forcepoint Behavioral Analytics via Ansible and Jenkins. This document covers system architecture, required software installation tools, and finally a step-by-step guide for a complete install.

The System Architecture section shows how data moves throughout software components, as well as how 3rd party software is used for key front- and back-end functionalities.

The Installation Components section elaborates on important pre-installation topics. In preparation for the initial installation setup, we discuss high-level topics regarding Jenkins and Ansible - the tools Forcepoint Behavioral Analytics utilizes to facilitate installation commands. Additionally, we strongly recommend following the Forcepoint Behavioral Analytics Hardening Guide (available through Professional Services) to ensure the system is set up with security best practices.

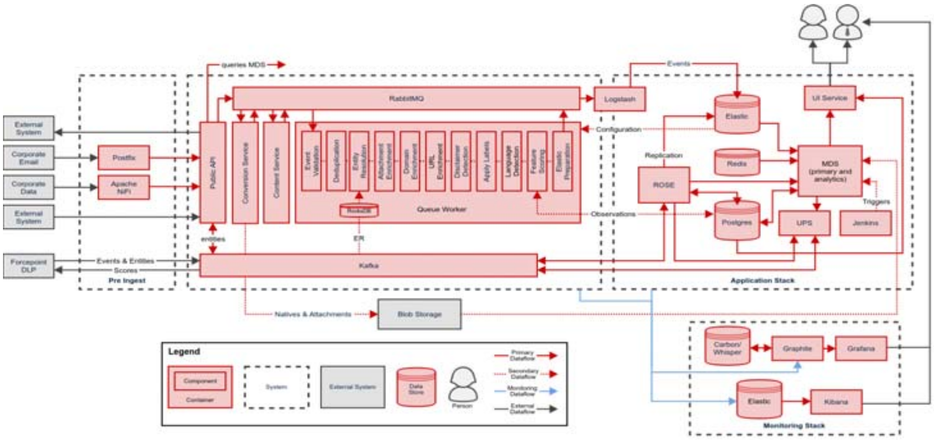
Although Jenkins is pre-configured at the time of install, we include Jenkins Setup information and important access and directory location information for a holistic understanding of this key installation facilitator.

To conclude this document, we include step-by-step instructions for using Ansible to initialize the Jenkins CI/CD server to install each required software component.

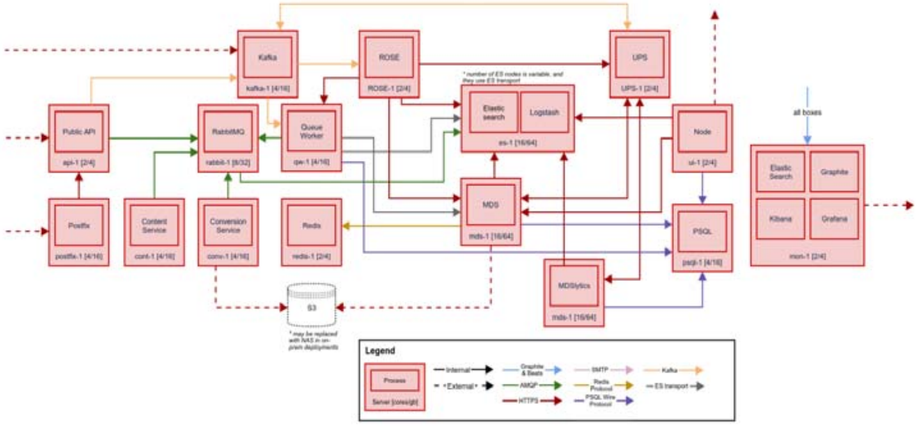
An addendum is included for additional components which can optionally be installed.

Go to the Downloads page and navigate to Forcepoint Behavioral Analytics to find the downloads for Forcepoint Behavioral Analytics.

Component Architecture



Physical Architecture



Installation Components

Host OS

Forcepoint requires a RedHat 7 host-based Operating System for the Forcepoint Behavioral Analytics platform to be installed. CentOS 7 (minimal) is the recommended OS to be used. Please note, other heavier install media can be used, but not necessary or recommended. At the time of publication, the latest version is CentOS 7.8. CentOS 6 is not supported, as it has known incompatibilities with our installation process and may introduce bugs into the Forcepoint Behavioral Analytics product due to OS differences.

Security

Forcepoint recommends using commonly accepted network security practices to restrict access to the Forcepoint Behavioral Analytics infrastructure. For instance, creating rules in IPTables, or implementing a network firewall that only allows the access defined in the ports list below.

Port List

Service	Host	Port	Consumers
Redis	redis	6379	UI
Graphite	mon	2003	All
Grafana	mon	443	Administrator Workstation
Jenkins	jenkins	8080/8443	All, Administrator Workstation
Vault	jenkins	8200/8201/8300/8301	All, Administrator Workstation
Kafka	kafka	9092-9095	API, Rose
Kafka Manager	kafka	9000	Administrator Workstation
Postgres	postgres	5432	Conversion, Rose, Master Data Service, Queue Worker, UI
RO-API	api	9000	External Data Sources, RabbitMQ
RO-API	api	9001	Administrator Workstation
RO-Conv	conv	9080	RabbitMQ
RO-Conv	conv	9081	Administrator Workstation
RO-Cont	cont	9700	RabbitMQ, ES
RabbitMQ	rabbit	4369	RabbitMQ
RabbitMQ	rabbit	15672	Administrator Workstation
ro-qw	qw	9090	RabbitMQ
ro-qw	qw	9091	Administrator Workstation
redis	redis	6379	UI
UI	ui	80/443	Users

Service	Host	Port	Consumers
Elasticsearch	es	9200	UI, Jenkins, ES, MDS, API, Conv, QW
Elasticsearch	es	9201	Administrator Workstation
Elasticsearch	es	9300-9400	Elasticsearch
ro-mds	mds, mdslytics	8080	UI, Jenkins, MDS
ro-mds	mds, mdslytics	8081	Administrator Workstation
ro-rose	rose	9500	API, Postgresql, Nifi, QW, UPS
ro-rose	rose	9501	Administrator Workstation
ro-ups	ups	9600	MDS
ro-ups	ups	9601	Administrator Workstation
OpenVPN	vpn	1194	External Clients

Installation Requirements

The Forcepoint Behavioral Analytics installation is Ansible based and requires Ansible version 2.5.8.0. No action is required as the installer has prerequisites packaged. Our current internal version is stable/3.7 in the Ansible git repository. The most recent stable version of this must be available to properly deploy the Forcepoint Behavioral Analytics platform. This Ansible code is distributed via the offline-installer. Please contact Forcepoint Support for further information.

Installation Facilitators

Ansible

Ansible is an IT automation tool that can configure systems, deploy software, and orchestrate more advanced IT tasks such as continuous deployments or zero downtime rolling updates. Ansible playbooks are used to incrementally install the separate components of a Forcepoint Behavioral Analytics instance.

File Format: YAML

- Ansible uses YAML because it is easier for humans to read and write than other common data formats, like XML or JSON. Further, there are libraries available in most programming languages for working with YAML.

Playbooks

- Playbooks are the basis for really simple configuration management and multimachine deployment system that is well suited to deploy complex applications.
- Playbooks can declare configurations, and they can also orchestrate steps of any manual ordered process, even as different steps must bounce back and forth between sets of machines in particular orders. They can launch tasks synchronously or asynchronously.
- Individual "Tasks" Make Up a role or playbook. A "Playbook" is comprised of tasks and roles.

```
- hosts: webservers
  remote_user: root



  tasks:
  - name: ensure apache is at the latest version
    yum: name=httpd state=latest
  - name: write the apache config file
    template: src=/srv/httpd.j2 dest=/etc/httpd.conf



- hosts: databases
  remote_user: root



  tasks:
  - name: ensure postgresql is at the latest version
    yum: name=postgresql state=latest
  - name: ensure that postgresql is started
    service: name=postgresql state=started
```

Jenkins

Jenkins is an open-source automation server that helps to automate the non-human part of continuous delivery. This is the primary way in which Forcepoint installs the Forcepoint Behavioral Analytics software.

Installation Procedures

Things to consider

- Infrastructure must be provisioned beforehand. This includes the following:
  - All hosts as needed for the size of the deployment

        - Every major component in the Forcepoint Behavioral Analytics tech stack runs on its own host
    - Appropriate networking considerations
    - Local disk storage
    - NFS shared storage or S3 (dependent on on-prem vs AWS deployment type)
- Disabling swap on all hosts is highly recommended, and at a minimum, this needs to be done on the ElasticSearch
    - This can be done by simply running 'swapoff -a' on all nodes and then removing any mount points for swap in '/etc/fstab'
- If installing under VMware install the package open-vm-tools for better VM support
- Python version 2.7 is required on all hosts. Version 2.7.5 is included in the latest version of the installer at the time of publication
- All hosts must have SSH enabled and reachable from the provisioning Ansible host (Jenkins) via /etc/hosts or DNS
- Our install and configuration is Ansible based
    - /etc/ansible/hosts file must be accurate
    - /etc/ansible/group_vars/all must be accurate and tailored to any site-specific overrides if necessary
    - Host machine running ansible playbooks must have ssh access to all hosts in the /etc/ansible/hosts inventory file
- All commands are assumed to be run on a fully updated CentOS 7 or RHEL 7 host
- Escalated privileges are required for installation and runtime
    - Installation should be done using the sudo user and not the root user
    - Depending on security policies, for ease, the sudoers file should be updated to allow for passwordless sudo usage
- The Jenkins host will be where you perform all actions from here on
- The Jenkins server is initialized and after, the Forcepoint Behavioral Analytics platform is deployed via the Continuous Delivery server

Installing miscellaneous tools

Wget is a useful tool not included in the minimal install that can be used to download the installer file.

To install:

```
sudo yum install wget
```

I. Download the Forcepoint Behavioral Analytics installer

1. Retrieve Forcepoint Behavioral Analytics installer from support.

    Go to [https:// support.forcepoint.com](https://support.forcepoint.com)

2. Set Forcepoint Behavioral Analytics installer to be executable.

```
sudo chmod +x Forcepoint-UEBA-3.3.x-CentOS-7.bin
```

3. Extract Forcepoint Behavioral Analytics installer.

```
sudo bash Forcepoint-UEBA-3.3.x-CentOS-7.bin
```

II. Create and Configure Client's Inventory Directory

There are three system config files that must be created with care in order for the install and runtime processes to work successfully:

- /etc/ansible/hosts

  Use: Config file used by Ansible for a list of hosts and groupings of hosts being managed.

- /etc/hosts

  Use: Operating system file that translates hostnames or domain names to IP addresses.

- /etc/ansible/group_vars/all

  Use: The top-level setting of variables used in the Ansible playbooks.

  Example Versions:

  all.aws.example for AWS installations

  all.on-prem.example for On-Prem installations

Example files for each of these files are available under:

```
/usr/share/ro-ansible/sysconfdir/
```

It is highly recommended to use the example files provided as the starting point for these three files.

1. Prep for file creation

   Create the necessary file path by running the below command:

   ```
   mkdir -p /etc/ansible/group_vars
   ```

2. Create and configure /etc/ansible/hosts

   Below is a command to grab the template '/etc/ansible/hosts' file, do a search and replace command using sed, and copy the updated file to the correct location. The find and replace command (sed) will change 'xxxxx' to the text that is in the 'change_me' field. Make sure to change 'change_me' in the example below before running the command. It will be visible to users, so we recommend an abbreviation of the customer's name or something else that will be intuitive. The example file is based on a minimal deployment and will need to be adjusted for the actual hosts in your deployment. An example being: if there are additional ES nodes they will need to be added manually.

   ```
   sudo sh -c "cd /usr/share/ro-ansible/sysconfdir/; sed -e
   's/xxxxx/change_me/g' etc_ansible_hosts.example > /etc/
   ansible/hosts"
   ```

   ```
   Example excerpt: /etc/ansible/hosts
   ```

```
###########################################
[api]
api-xxxxx
[ca]
ro-root-ca ansible_host=jenkins-xxxxx
[content]
cont-xxxxx
[conversion]
conv1-xxxxx
conv2-xxxxx
[curator]
curator-xxxxx ansible_host=jenkins-xxxxx
[es]
es1-xxxxx
es2-xxxxx
es3-xxxxx
###########################################
```

3. Create and configure /etc/hosts

   Setup /etc/hosts, static table lookup for hostnames. Using the command in the example below will place the example file in '/etc/hosts' with the updated hostnames. The IP addresses will need to be filled out still. The example file is based on a minimal deployment and will need to be adjusted for the actual hosts in your deployment. An example being: if there are additional ES nodes they will need to be added manually.

   ```
   sudo sh -c "cd /usr/share/ro-ansible/sysconfdir/; sed -e
   's/xxxxx/change_me/g' etc_hosts.example > /etc/ansible/
   group_vars/all"
   ```

   ```
   Example exert: /etc/hosts
   ###########################################
   127.0.0.1 localhost localhost.localdomain localhost4
   localhost4.localdomain4
   ::1 localhost localhost.localdomain localhost6
   localhost6.localdomain6
   10.55.10.110 api-xxxxx
   10.55.10.106 conversion-xxxxx
   10.55.10.105 jenkins-xxxxx
   10.55.10.120 kafka-xxxxx
   10.55.10.122 es1-xxxxx
   10.55.10.124 es2-xxxxx
   10.55.10.136 es3-xxxxx
   ```

```
10.55.10.137 mds-xxxxx
10.55.10.138 mdslytics-xxxxx
###########################################
```

4. Create and configure /etc/ansibel/group_vars/all

   There are two example files provided for the '/etc/group_vars/all' file, one for an AWS install and another for an On-Prem install. Choose the version based on your install location. This file is extremely important and many errors in the install process are commonly due to missing variables or typos in this file. All of the 'x' in this file will need to be manually modified as they are specific to the environment being created.

```
# AWS Install Version
sudo cp /usr/share/ro-ansible/sysconfdir/group_vars/
all.aws.example /etc/ansible/group_vars/all


# On-Prem Install Version
sudo cp /usr/share/ro-ansible/sysconfdir/group_vars/
all.on-prem.example /etc/ansible/group_vars/all


Example exert: /etc/ansible/group_vars/all
###########################################
##offline install
yum_repo_epel_enabled: "{{ epel_repo_enable }}"
yum_repo_sslverify: "0"
ueba_offline_install: true


##environment name (domain)
ro_env: xxxxx
domain: "{{ domain_name }}"
tld: internal
domain_name: "ro.{{ tld }}"
###########################################
```

III. Generate and Push SSH Keys to all Hosts

1. Generating an SSH key pair

   It is recommended to use passwordless ssh key authentication. To create the keys run the example below as the privileged (sudo) user:

```
ssh-keygen -t ed25519
```

2. Copy SSH public key to all hosts defined in /etc/hosts

A script has been provided under '/usr/share/ro-ansible/sysconfdir/scripts/SSH_key_copy.sh` to allow the key generated above to be copied to all hosts in '/etc/hosts'. The script assumes there is a common password used for all of the hosts.

To run the script:

```
#1 Ensure permissions are set so that the script is
executable
sudo chmod +x /usr/share/ro-ansible/sysconfdir/scripts/
SSH_key_copy.sh


#2 Ensure sshpass is installed on the system which
sshpass


#2a If not installed
sudo yum install sshpass


#3 Run the script and enter the password when prompted
bash /usr/share/ro-ansible/sysconfdir/scripts/
SSH_key_copy.sh
```

IV. Initialize Forcepoint Continuous Delivery Server

Based on the client-dictated ssh authentication method, adjust the following commands as necessary (remembering to include the private key or credentials, according to the previous section).

Example (do not run this at this time) ansible command with ssh key:

```
ansible-playbook ro-baseline.yml -u centos --private-key=~/
.ssh/client.pem
```

Example (do not run this at this time) ansible command with ssh username and password:

```
ansible-playbook ro-baseline.yml -u centos -k
```

1. Deploy Jenkins host (Before running playbook, all hosts must have SSH enabled and reachable from the provisioning ansible host via /etc/hosts or DNS).

   ```
   ansible-playbook /usr/share/ro-ansible/jenkins-init.yml
   ```

2. If deploying on-prem then deploy NFS server and client for shared storage.

   a. Update '/etc/hosts' to include the NFS server

      example:

      ```
      10.55.10.105 nfs-xxxxx
      ```

   b. Update '/etc/ansible/hosts' to include the NFS server. Note that the NFS server can be implemented on any of the hosts in the stack, but it is recommended to either be on the Postgres or Jenkins hosts.

      example:

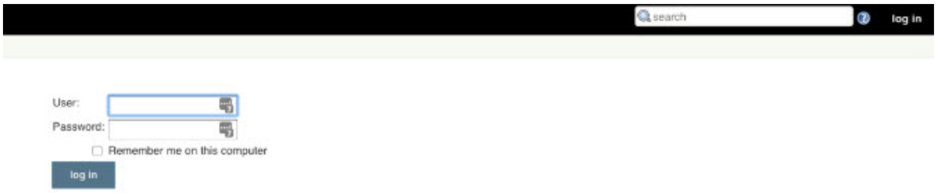
```
[nfs]
nfs-xxxxx ansible_host=postgres-xxxxx
```

c. Deploy the NFS server and client

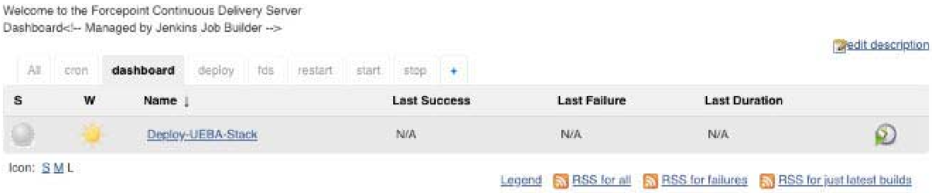
```
ansible-playbook /usr/share/ro-ansible/nfs-server.yml
ansible-playbook /usr/share/ro-ansible/nfs-client.yml
```

V. Deploy Forcepoint Behavioral Analytics from Jenkins

1. Navigate to the Jenkins web-based service in a browser
   a. The hostname can be reached by hostname, FQDN, or IP.
      e.g.
      - http://jenkins-customer.domain.com:8080
      - http://jenkins-customer:8080
      - http://10.0.0.100:8080
2. Login to Forcepoint Continuous Delivery Server - Jenkins
   a. Default credentials are:
      Username: forcepoint
      Password: forcepoint



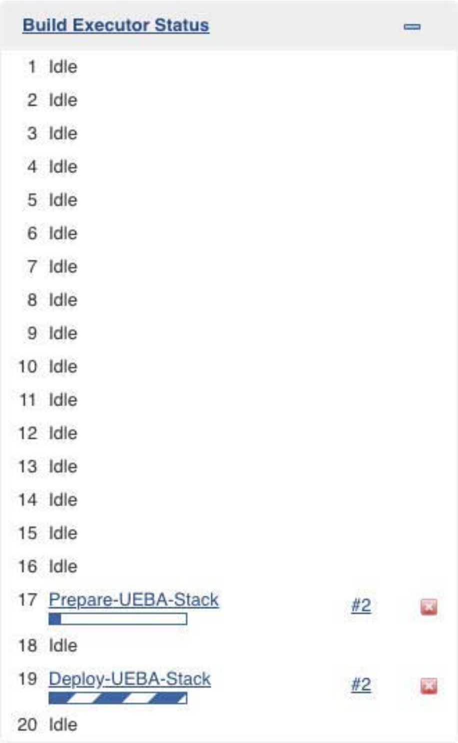
3. Deploy the Forcepoint Behavioral Analytics Stack from Forcepoint Continuous Delivery Server.


Welcome to the Forcepoint Continuous Delivery Server Dashboard<!-- Managed by Jenkins Job Builder -->

S	W	Name ↓	Last Success	Last Failure	Last Duration
○	☀	Deploy-UEBA-Stack	N/A	N/A	N/A

4. Check the deployment status from Forcepoint Continuous Delivery Server(optional).

a. The status and currently running deployment jobs can be found in the BuildExecutor Status window.



Build Executor Status

1	Idle	
2	Idle	
3	Idle	
4	Idle	
5	Idle	
6	Idle	
7	Idle	
8	Idle	
9	Idle	
10	Idle	
11	Idle	
12	Idle	
13	Idle	
14	Idle	
15	Idle	
16	Idle	
17	Prepare-UEBA-Stack	#2
18	Idle	
19	Deploy-UEBA-Stack	#2
20	Idle	

VI. Create Default UI Admin User

1. Create the first admin user for the UI.

   a. By default, Forcepoint Behavioral Analytics does not ship with an initial user configured.

   b. You must manually create this user to successfully log into the UI.

   c. These commands must be executed on the postgres host from the command line.

   d. This will create the following default user:

      Username: redowl@redowl.com

      Password: redowl

Note

Do not copy and paste the text below directly.

The line-wrapping does not allow the commands to be executed correctly.

Copy instead from Jenkins host under '/usr/share/ro-ansible/sysconfdir/scripts/psql_admin_setup.sh'

```
psql -U redowlpostgres -d the_ui -c "INSERT INTO USERS
(email, encrypted_password, name, created_at,
updated_at, password_updated_at) VALUES
('redowl@redowl.com','\$2a\$06\$mMhM9IWYk1J3Q15tGgP5rO
ryw7Mo1m3JL0eydVOtJ20gmm4twDKMW','Red Owl',
CURRENT_DATE, CURRENT_DATE, CURRENT_DATE);"
```

```
psql -U redowlpostgres -d the_ui -c "INSERT INTO
roles_users (role_id, user_id) (SELECT r.id, u.id FROM
roles r INNER JOIN users u ON (u.email LIKE
'redowl@redowl.com') WHERE r.id != 13);"
```

```
psql -U redowlpostgres -d the_ui -c "INSERT INTO
groups_users (group_id, user_id) values (1,1);"
```

Appendix

Notes on OpenVPN

This process is currently operations intensive due to the evolving customer deployment models. These operations should only be performed by Professional Services.

Things to consider

- The VPN host must be provisioned beforehand.
- The VPN host must have SSH enabled and reachable from the provisioning ansible host.
- The install and configuration are Ansible based.
  - /etc/ansible/hosts file must be accurate.
  - /etc/ansible/group_vars/all must be accurate and tailored to any site-specific overrides necessary.
  - Host machine running ansible playbooks must have ssh access to all hosts in the /etc/ansible/hosts inventory file.

Deploying the OpenVPN

1. Baseline Forcepoint Behavioral Analytics VPN host.

   ```
   ansible-playbook ro-baseline.yml --limit openvpn
   ```

2. Ensure SSH Key is Copied to Forcepoint Behavioral Analytics VPN host.

   ```
   cp user.pem ~/.ssh/user.pem
   chmod 600 ~/.ssh/user.pem
   ```

3. Retrieve Forcepoint Behavioral Analytics VPN host Public IP.

```
curl ipecho.net/plain
```

4. Install common Forcepoint Behavioral Analytics packages.
   a. Option 1 - Run everything:

      ```
      ansible-playbook ro-common.yml --limit openvpn
      ```

   b. Option 2 - Run select playbooks, based on customer needs:
      - ○ Always run (do NOT confuse this with ro-common.yml):

        ```
        ansible-playbook common.yml
        ```

      - ○ Optionally run:

        ```
        ansible-playbook selinux.yml --limit openvpn
        ansible-playbook ntp.yml --limit openvpn
        ansible-playbook hostname.yml --limit openvpn
        ansible-playbook ro-ssh.yml --limit openvpn
        ansible-playbook hosts_file.yml --limit openvpn
        ```

5. Deploy OpenVPN Service.

   ```
   ansible-playbook openvpn.yml
   ```

6. Start OpenVPN Service.
   a. Run from Forcepoint Behavioral Analytics VPN host:

      ```
      sudo systemctl restart openvpn@server.service
      ```

7. Create OpenVPN Users

Note
✓ Substitute {{user}} with correct username.

   a. Run from Forcepoint Behavioral Analytics VPN host:

      ```
      sudo /etc/openvpn/addvpnuser.sh fp-ueba-ops-{{user}}
      sudo su - {{user}}
      passwd - enter password twice when prompted
      cp /etc/openvpn/keys/{{user}}-vpn-*.tar.gz /home/{{user}}
      ```

   b. Copy /home/{{user}}-vpn-*.tar.gz to remote machine for Professional Services Engineer use.

8. Configure 2FA - Google Authenticator.

Note
✓ Substitute {{user}} with correct username.

   a. Run from Forcepoint Behavioral Analytics VPN host logged in as newly created user:

      ```
      google-authenticator
      ```

      - ○ Correct question answers are: YYYNY

- ○ Copy the barcode and/or the url to add to the authenticator app.

9. Test Forcepoint Behavioral Analytics VPN connection.

> ✓ **Note**
> Substitute {{user}} with correct username.

a. Run from Professional Services OSX host:

```
tar {{user}}-vpn-*.tar.gz -C {{user}}-vpn.tblk
```

b. Drag and drop {{user}}-vpn.tlbk into tunnelblick configuration windows.

c. Connect using username,password+googleauth.

Troubleshooting OpenVPN

- If authentication fails, ensure the password is set correctly. Reset password as necessary.
- Google-authenticator may need to be rerun.
- If name lookups are failing there is a bug in the tunnelblik software to where the client does not push the AWS DNS server and search domains to the local machine.
  - In this case, go to your primary network interface and manually add the route53 address x.x.x.2 for the DNS server and appropriate search domain.

Deployment - AWS Encryption Options for Native and Attachment Storage

Forcepoint Behavioral Analytics supports various means of encryption options in AWS S3 for Native and Attachment storage in the Conversion Service. The default used is SSE-S3. Alternatively, SSE-C or SS3-KMS can be enabled. No UI configuration changes are necessary to enable either SSE-C or SSE-KMS, but the AWS IAM credentials used by the UI must be on the KMS key policy.

To enable one of the alternative AWS encryption options, alterations must be made to:

```
/usr/share/ro-ansible/roles/ro-conv/defaults/main.yml
```

Default Values:

```
# encryption for S3 storage; supported types are (sse-s3,
sse-c, ss3-kms)
natives_encryption_type: sse-s3
attachments_encryption_type: sse-s3
# required if sse-c is enabled
natives_sse_c_key_file: ""
attachments_sse_c_key_file: ""
# required if sse-kms is enabled
```

```
natives_sse_kms_key_arn: ""
attachments_sse_kms_key_arn: ""
```

To enable sse-c:

```
# encryption for S3 storage; supported types are (sse-s3,
sse-c, ss3-kms)
natives_encryption_type: sse-c
attachments_encryption_type: sse-c
# required if sse-c is enabled
natives_sse_c_key_file: "/path/to/my.key"
attachments_sse_c_key_file: "/path/to/my.key"
# required if sse-kms is enabled
natives_sse_kms_key_arn: ""
attachments_sse_kms_key_arn: ""
```

To enable ss3-kms:

```
# encryption for S3 storage; supported types are (sse-s3,
sse-c, ss3-kms)
natives_encryption_type: ss3-kms
attachments_encryption_type: ss3-kms
# required if sse-c is enabled
natives_sse_c_key_file: ""
attachments_sse_c_key_file: ""
# required if sse-kms is enabled
natives_sse_kms_key_arn:
"arn:aws:kms:<region>:<account>:key/<key>"
attachments_sse_kms_key_arn:
"arn:aws:kms:<region>:<account>:key/<key>"
```

Deployment - Manually Run Ansible Playbooks

Prepare Forcepoint Behavioral Analytics Stack

1. Forcepoint Behavioral Analytics hostnames.

   ```
   ansible-playbook hostname.yml
   ansible-playbook hosts_file.yml
   ```

2. Forcepoint Behavioral Analytics baseline.

   ```
   ansible-playbook ro-baseline.yml
   ```

3. Install common Forcepoint Behavioral Analytics packages.

   a. Option 1 - Run everything:

   ```
   ansible-playbook ro-common.yml
   ```

b. Option 2 - Run select playbooks, based on customer needs:

   ○ Always run (do NOT confuse this with ro-common.yml):

     ```
     ansible-playbook common.yml
     ```

   ○ Optionally run:

     ```
     ansible-playbook selinux.yml
     ansible-playbook ntp.yml
     ansible-playbook ansible-openssh.yml
     ```

4. Deploy Forcepoint Behavioral Analytics secrets:.

   ```
   ansible-playbook vault.yml
   ```

5. To deploy Forcepoint Behavioral Analytics Middleware, deploy Jenkins host.

   ```
   ansible-playbook jenkins.yml
   ```

6. Deploy Redis.

   ```
   ansible-playbook redis.yml
   ```

7. Deploy Postgresql.

   ```
   ansible-playbook postgres.yml
   ```

8. Deploy RabbitMQ.

   ```
   ansible-playbook rabbit.yml
   ```

9. Deploy Kafka.

   ```
   ansible-playbook kafka.yml
   ```

10. Deploy ElasticSearch.

    ```
    ansible-playbook ro-es.yml
    ```

11. Deploy Monitoring ElasticSearch.

    ```
    ansible-playbook ro-mon-es.yml
    ```

12. Initialize Forcepoint Behavioral Analytics Schema.

    ```
    ansible-playbook ro-schema.yml
    ```

13. Deploy Forcepoint Behavioral Analytics Monitoring Software.

    ```
    ansible-playbook ro-monitoring.yml
    ```

14. Deploy Forcepoint Behavioral Analytics Master Data Service.

    ```
    ansible-playbook ro-mds.yml
    ```

15. Deploy Forcepoint Behavioral Analytics Master Data Service analytics node

    ```
    ansible-playbook ro-mdslytics.yml
    ```

16. Deploy Forcepoint Behavioral Analytics API Service.

    ```
    ansible-playbook ro-api.yml
    ```

17. Deploy Forcepoint Behavioral Analytics Queue Worker Service.

    ```
    ansible-playbook ro-qw.yml
    ```

18. Deploy Forcepoint Behavioral Analytics Conversion Service.

    ```
    ansible-playbook ro-conv.yml
    ```

19. Deploy Forcepoint Behavioral Analytics Content Service.

```
ansible-playbook ro-cont.yml
```

20. Deploy Forcepoint Behavioral Analytics UPS Service.

    ```
    ansible-playbook ro-ups.yml
    ```

21. Deploy Rose Service.

    ```
    ansible-playbook ro-rose.yml
    ```

22. Deploy Apache Nifi Service.

    ```
    ansible-playbook ro-nifi.yml
    ```

23. Deploy Forcepoint UI Service.

    ```
    ansible-playbook ro-ui.yml
    ```

24. Deploy Lostash.

    ```
    ansible-playbook ro-logstash.yml
    ```

25. Deploy Kibana.

    ```
    ansible-playbook ro-kibana.yml
    ```

26. Deploy Forcepoint Integration Service (optional).

    ```
    ansible-playbook ro-api.yml
    ```

27. Deploy Security Features (optional).

    ```
     ansible-playbook ro-jobs.yml -i /etc/ansible/hosts -t
    tls-version -f 5 -e set_tls_version=true -v
    ```

Deploying the Curator

The deploy-ueba-curator job was removed from the deploy stack process as it requires Jenkins to restart at the end of the job. This causes the deploy process to appear as though it failed. Manually run the deploy-ueba-curator job after the install process is complete.