Forcepoint Behavioral Analytics Installation Manual

Installation Manual | Forcepoint Behavioral Analytics | v3.4 | 17-Feb-2021

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.

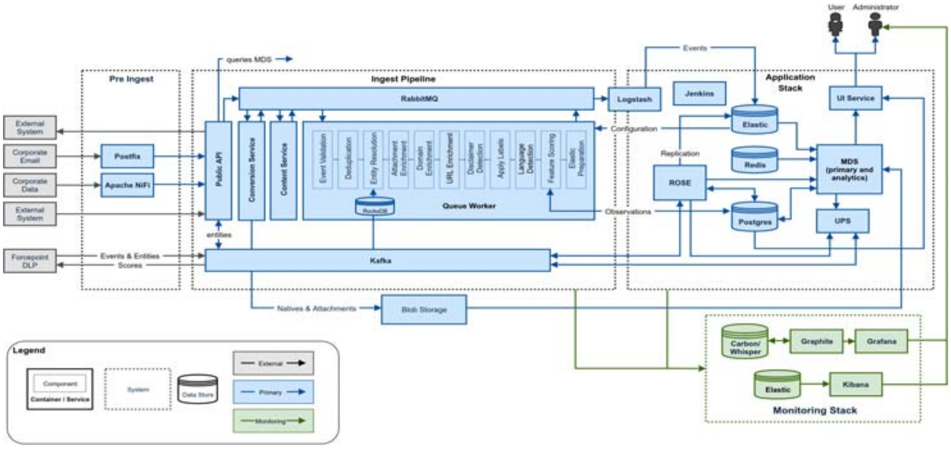
To conclude this document, we include step-by-step instructions for using Ansible to initialize the Jenkins CI/CD server to install each required software component.

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

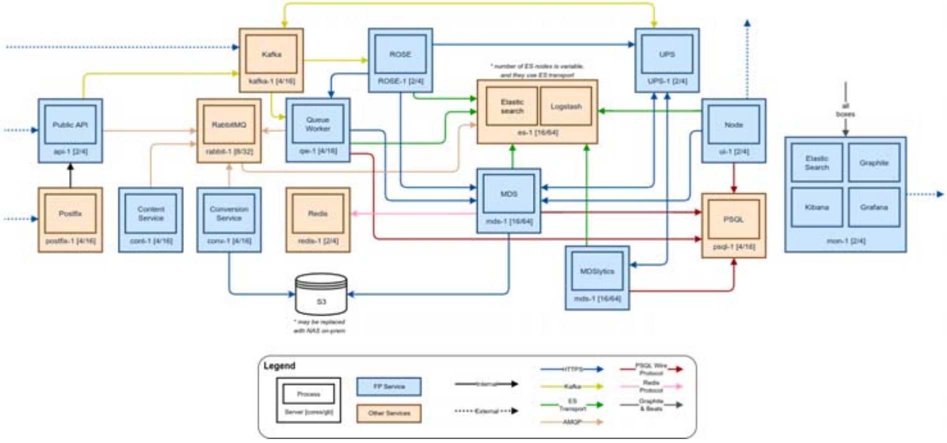
Go to the Downloads page and navigate to Forcepoint Behavioral Analytics to find the downloads for Forcepoint Behavioral Analytics.

Platform Overview

Component Architecture



Physical Architecture



Installation Components Overview

Host OS

Forcepoint requires a RedHat 7.9 host-based Operating System for the Forcepoint Behavioral Analytics platform to be installed. A minimum kernel version of 3.10.0-1127, as well as CentOS 7.9 or RHEL 7.9, are required. The minimal versions of either CentOS or RHEL should be used. Please note, other heavier install should not be used as there might be RPMs that cause conflicts with required RPMs and versions of those RPMs. Centos and RHEL versions 7.8 and below are no longer supported and are blocked through the install process.

Docker Containers

New in Forcepoint Behavioral Analytics 3.4.0 is the addition of Docker to house the services and applications. Docker runs as a non-root user (rootless) to allow the Forcepoint Behavioral Analytics product to be installed under a custom user and within custom directories while ensuring the least privileges model for installation and runtime. Rootless Docker version 19.03.9 is included in the installation media and installed through the provided install scripts. All ports mentioned below are being mapped from the Host OS to the container. Each host OS contains a single container running a minimal CentOS 7.9 container image.

Security

Please see the accompanying Hardening Guide for best security practices. 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
SSH	All	2222	All containers use 2222 for SSH
Redis	redis	6379	UI
Graphite	mon	2003	All
Grafana	mon	443	Administrator Workstation
Jenkins	jenkins	8080/8443/80	All, Administrator Workstation, YUM Repo
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

Service	Host	Port	Consumers
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 (internal port)
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
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 shell script and Ansible based and requires Ansible version 2.5.8.0. No action is required as the installer has prerequisites packaged. External access to ports 8080 and 8443 on the Jenkins host is critical during installation as great care has been given to automate the installation process through Jenkins jobs. While it is technically possible to bypass the Jenkins jobs and run the install solely via Ansible playbooks, this is not recommended as permissions and least privilege are put at risk. Please contact Forcepoint Support for further information.

Installation Facilitators

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.

Makeself

The Forcepoint Behavioral Analytics installation media is packaged using self-extractable archives through an open-source solution named makeself (makeself.io). This allows for the Forcepoint Behavioral Analytics installation bundle to run and be pre-installed on a primary host (Jenkins) and extract the required packages into the proper directories under the provisioned user with limited privileges. During this phase of the install process, the required Docker binaries and required scripts are installed and run.

The following steps are completed by makeself:

1. Extracts files.
2. Verifies integrity using sha256.
3. Executes install scripts.
    a. Install required host-level RPMs.
    b. Verify required directories are created.
    c. Verify docker can be installed on each host.
    d. Install docker on each host.
    e. Run docker on each host.
    f. Setup yum repo and RPMs on mounted volume inside the container.
    g. Install RPMs needed to run the install inside the Jenkins container.

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
```

Installation Procedures

Prerequisites

- 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)
- The minimum kernel version is 3.10.0-1127.
- Disabling swap on all hosts is highly recommended, and at a minimum, this needs to be done on the ElasticSearch hosts.
    - 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.
- $FBA_USER is used below in place of the provisioned user created for installation and runtime of the Forcepoint Behavioral Analytics software.
- $FBA_DIR is the directory we are running the installer from and must be owned by the $FBA_USER. The install process requires this directory to have 12GB of free space.

  File paths we require are as follows:

    - $FBA_DIR
        - Base install directory
        - It is preferable that this be mounted on a separate partition from the root OS
    - $FBA_DIR/data
        - Data volumes should be mounted here.
        - It is preferable that this be mounted on a separate partition from the root OS and the $FBA_DIR

  Optional file paths:

    - $FBA_DIR/data/nfs
        - For use when not using S3 for LOB storage.
        - Required to be mounted to the host under this directory for use within the container.
        - The NFS server must be configured with exports set to include 'all_squash' and the anonuid and anongid set to the $FBA_USER's uid and gid.
    - $FBA_DIR/var/log
        - It is preferable that this be mounted on a separate partition from the root OS and the $FBA_DIR
- Our install and configuration is Ansible based
    - Hosts file must be accurate. Note that the template is included.

        - Replaces the use of the /etc/hosts file
    - The ansible-all file must be accurate and tailored to any site-specific overrides if necessary. Note that the template is included.
        - Copied to the /etc/ansible/group_vars/all file inside the container
    - The ansible-hosts file must be accurate and include all hosts in their appropriate groups. Note that the template is included.
        - Copied to the /etc/ansible/hosts file inside the container
    - 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 7.9 or RHEL 7.9 host.
- Escalated privileges are required for installation.
    - 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.
    - Full allow-list in the appendix below.
- The Jenkins host will be where you perform all subsequent actions.
- The Jenkins server is initialized and after, the Forcepoint Behavioral Analytics platform is deployed via the Continuous Delivery server.

Getting Started

I. Download the Forcepoint Behavioral Analytics installer media

1. Retrieve Forcepoint Behavioral Analytics installer from the support site.

    Go to https:// support.forcepoint.com

2. Untar the installer tarball under the $FBA_DIR.

    ```
    tar xf FBA-340.tar.gz
    ```

II. Create and Configure Client's Inventory Directory

To accommodate for custom directory installations, we will refer to the source custom directory in the following steps as $FBA_DIR. This directory is the basis for all directories volume mounted within the container. The ideal location for this directory is the home directory of the provisioned user. For example /home/$FBA_USER = $FBA_DIR. The $FBA_DIR must be owned by the $FBA_USER. The $FBA_DIR is mapped to/when mounted inside the containers.

There are three system configuration files that must be created with care on the Jenkins host in order for the install and runtime processes to work successfully. Templates for these files are included in the installer tarball.

- $FBA_DIR/hosts

  - Use: Operating system file that translates hostnames or domain names to IP addresses.
  - Template Name: hosts
- $FBA_DIR/ansible-hosts
  - Use: Config file used by Ansible for a list of hosts and groupings of hosts being managed.
  - Template Name: ansible-hosts
- $FBA_DIR/ansible-all
  - Use: The top-level setting of variables used in the Ansible playbooks.
  - Template Name: ansible-all

It is highly recommended to use the example files provided as the starting point for these three files, and the instructions below reference how to do so.

1. Configure $FBA_DIR/hosts

   Using the command in the example below will update the example file with the updated hostnames. The IP addresses will need to be filled out. The example file is based on a minimal deployment and will need to be adjusted for the actual hosts in your deployment. For example, if there are additional ES nodes they will need to be added manually.

   ```
   sed -i 's/xxxxx/change_me/g' hosts


   Example excerpt: 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
   ###########################################
   ```

2. Create and configure $FBA_DIR/ansible-hosts

   Below is a command to grab the template '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. Change 'change_me' in the example below before running the command. This field will be visible to users. The example file is based on a minimal deployment and will need to be adjusted for the actual hosts in your deployment. For example, 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"

sed -i 's/xxxxx/change_me/g' ansible-hosts

Example excerpt: 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 $FBA_DIR/ansible-all

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

```
# AWS Install Version
cp ansible-all.aws.example ansible-all

# On-Prem Install Version
cp ansible-all.on-prem.example ansible-all

Example exert: ansible-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 $FBA_USER:

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

2. Copy SSH public key to all hosts defined in the 'hosts' file.

   A script has been provided under 'scripts/SSH_key_copy.sh` to allow the key generated above to be copied to all hosts in the 'hosts' file. 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
   chmod +x 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 SSH_key_copy.sh
   ```

IV. Run the Forcepoint Behavioral Analytics installer

1. Set the Forcepoint Behavioral Analytics installer to be executable.

   ```
   chmod +x Forcepoint-UEBA-3.4.0.bin
   ```

2. Extract the Forcepoint Behavioral Analytics installer.

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

3. The installer will first run the pre-install scripts which will prep the Jenkins host to run parallel and install Docker rootless kit across the hosts.
   - Monitor the logs from the pre-install script for updates on status and to ensure there are no errors
4. Once the pre-install completes successfully, you will be prompted to run the following:

```
docker exec jenkins-{stack-name}-docker su - centos -c
'ansible-playbook /usr/share/ro-ansible/jenkins-init.yml'
```

> ⚠ **Warning**
>
> Make sure to run source ~/.bashrc before running the Jenkins-init playbook command.

5. After the Jenkins-init playbook completes, the Jenkins UI will be up and running.

V. NFS steps for on-premises installations

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

1. Update 'hosts' on the Jenkins host to include the NFS server

   Example:

```
10.55.10.105 nfs-xxxxx
```

2. Update '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
```

3. Deploy the NFS server and client

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

VI. 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.,

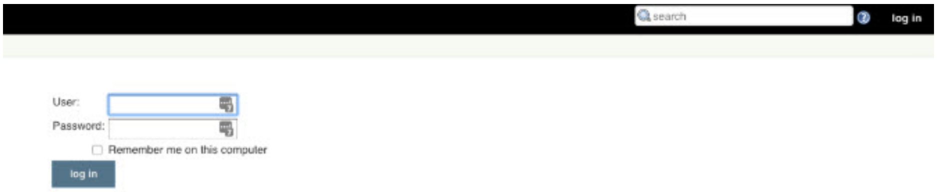
      - http://jenkins-customer.domain.com:8080

      - 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


search

log in

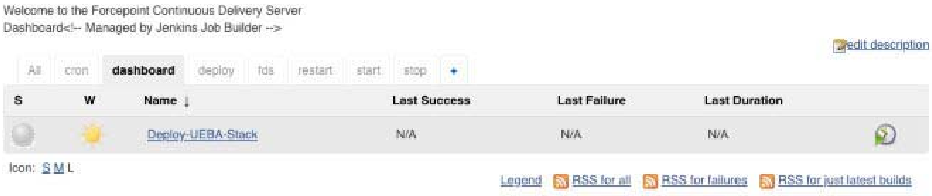
User:

Password:

□ Remember me on this computer

log in

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 -->

edit description

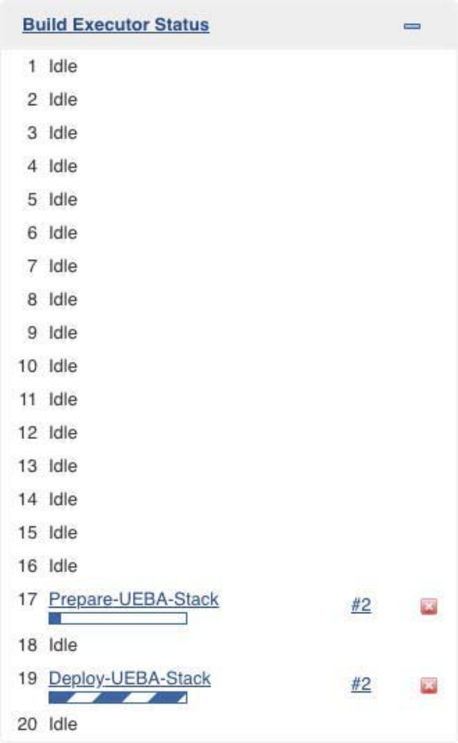
All | cron | dashboard | deploy | fds | restart | start | stop | +

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

Icon: S M L

Legend | RSS for all | RSS for failures | RSS for just latest builds

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		

VII. Create Default UI Admin User

1. Create the first admin user for the UI.

   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'

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 container from the command line.

```
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

Allow-List Sudo Commands - Enhanced Privileges Allow list

The installation process for the dockerized Forcepoint Behavioral Analytics 3.4.0 release requires a small subset of commands that can be run with sudo during the installation.

Variable	Use/Definiteion	Example Value
FBA_USER	The username of the user FBA will be running as.	centos
FBA_UID	The userid number of the FBA_USER.	1000
FBA_GROUP	The group of the FBA_USER.	centos
FBA_DIR	The directory where the FBA software will be installed.	/home/centos

Several commands are required to be run with sudo on all hosts in the installation. Some of the commands are only required on specific hosts.

Command	Purpose	Hosts	Notes
chown ${FBA_USER}:${FBA_GROUP} ${FBA_DIR}	Ensure ownership of the FBA_DIR is correct.	all	not needed if the ownership and group of the directory are already correct
cp ${FBA_DIR}/hosts /etc/hosts	Include list of fba hosts in /etc/hosts.	all	not needed if DNS is correctly set up and working on the host
loginctl enable-linger ${FBA_USER}	Allow the rootless docker to continue running after the FBA_USER logs out.	all	
mkdir -p ${FBA_DIR}	Ensure that the FBA_DIR is present.	all	not needed if the directory is already present

Command	Purpose	Hosts	Notes
rpm -Uvh ${FBA_DIR}/ slirp4netns-0.4.3-4.el7_8.x86_64.rpm rpm -Uvh ${FBA_DIR}/ yum-plugin-versionlock-1.1.31-54.el7_8.noarch.rpm	Install required system-level software.	all	slirp4netns improves network performance of port forwards in docker. yum-plugin-versionlock is used to ensure that slirp4netns is not updated during normal system upgrades so we can make sure the version installed has been tested with our environment
yum versionlock slirp4netns*	Version lock the slirp4netns rpm.	all	note that this is not a wildcard, but rather a literal "*" character
sed -i '/Service/a LimitMEMLOCK=infinity:infinity' /usr/lib/ systemd/system/ docker_${FBA_USER}.service	Modify the rootless docker unit file in place to set the MEMLOCK limit to unlimited during docker startup.	es, jenkins, mds, mon, nifi, postfix, postgres, rabbit, redis, rose, ui, and ups	
setcap cap_net_bind_service=ep ${FBA_DIR}/ bin/rootlesskit >/ dev/null	Allow the rootless docker executable to bind IP ports < 1024.	all	

Command	Purpose	Hosts	Notes
sysctl --system >/dev/null sysctl -w vm.max_map_count=262144 sysctl vm.overcommit_memory=1	Update sysctl parameters as required during the installation.	all	vm.max_map_count is required on some systems that use mmap on a large number of files (specifically for elastic search nodes and the monitoring node that also runs elastic).
systemctl daemon-reload systemctl enable docker_${FBA_USER}.service systemctl restart docker_${FBA_USER} systemctl start docker_${FBA_USER}.service	Start, restart, enable the rootless docker systemd unit.	all	vm.overcommit_memory is used on some systems that allocate a large amount of virtual memory even if it is not going to be used (specifically for rabbit and redis hosts).

Several system files need to be written to during the installation process. We do this using the tee -a filename commands:

File	Use	Hosts	Text written to the file
/etc/rc.local	Transparent_hugepages must be disabled at system boot time.	postgres, redis	echo never | sudo tee /sys/kernel/mm/transparent_hugepage/enable
/etc/subgid	Initialize the gid mapping utilized by the rootless docker system.	all	${FBA_GROUP}:100000:65536
/etc/subuid	Initialize the uid mapping utilized by the rootless docker system.	all	${FBA_USER}:100000:65536
/etc/sysctl.d/01-max_user_namespaces.conf	Update the max user namespaces at system boot time, required by rootless docker.	all	user.max_user_namespaces=28633

File	Use	Hosts	Text written to the file
/etc/sysctl.d/01-overcommit-memory.conf	Update the overcommit memory setting as described above at system boot time.	all	vm.overcommit_memory=1
/usr/lib/systemd/system/docker_${FBA_USER}.service	The rootless docker systemd unit file.	all	see the template below
/etc/sysctl.conf	Update the max_map_count vm setting for mmapped files as described above.	all	vm.max_map_count =262144
/sys/kernel/mm/transparent_hugepage/enabled	Modify the transparent hugepage setting on the system as described above (in the section on the /etc/rc.local file), it is done here during the installation process so a reboot is not required.	postgres, redis	never

This is the template for the rootless docker systemd unit file:

```
[Unit]
Description=Run dockerd rootless as user ${FBA_USER}
DefaultDependencies=no
After=network.target

[Service]
LimitNOFILE=65536:65536
Type=simple
User=${FBA_USER}
Group=${FBA_GROUP}
Environment="PATH=${FBA_DIR}/bin:/bin:/usr/bin:/sbin:/usr/
sbin"
Environment="DOCKER_HOST=unix:///run/user/${FBA_UID}/
docker.sock"
Environment="XDG_RUNTIME_DIR=/run/user/${FBA_UID}"
ExecStart=${FBA_DIR}/bin/dockerd-rootless.sh --experimental
--storage-driver vfs
TimeoutStartSec=0
```

```
[Install]
WantedBy=default.target
```

In addition to the above, the Jenkins host requires the following software packages to be installed. Our installation process performs this installation with an rpm -Uvh --force command. The rpms listed here are included in our offline_installer bundle.

```
bzip2-1.0.6-13.el7.x86_64.rpm
groff-base-1.22.2-8.el7.x86_64.rpm
perl-5.16.3-297.el7.x86_64.rpm
perl-Carp-1.26-244.el7.noarch.rpm
perl-Encode-2.51-7.el7.x86_64.rpm
perl-Exporter-5.68-3.el7.noarch.rpm
perl-File-Path-2.09-2.el7.noarch.rpm
perl-File-Temp-0.23.01-3.el7.noarch.rpm
perl-Filter-1.49-3.el7.x86_64.rpm
perl-Getopt-Long-2.40-3.el7.noarch.rpm
perl-HTTP-Tiny-0.033-3.el7.noarch.rpm
perl-PathTools-3.40-5.el7.x86_64.rpm
perl-Pod-Escapes-1.04-297.el7.noarch.rpm
perl-Pod-Perldoc-3.20-4.el7.noarch.rpm
perl-Pod-Simple-3.28-4.el7.noarch.rpm
perl-Pod-Usage-1.63-3.el7.noarch.rpm
perl-Scalar-List-Utils-1.27-248.el7.x86_64.rpm
perl-Socket-2.010-5.el7.x86_64.rpm
perl-Storable-2.45-3.el7.x86_64.rpm
perl-Text-ParseWords-3.29-4.el7.noarch.rpm
perl-Time-HiRes-1.9725-3.el7.x86_64.rpm
perl-Time-Local-1.2300-2.el7.noarch.rpm
perl-constant-1.27-2.el7.noarch.rpm
perl-libs-5.16.3-297.el7.x86_64.rpm
perl-macros-5.16.3-297.el7.x86_64.rpm
perl-parent-0.225-244.el7.noarch.rpm
perl-podlators-2.5.1-3.el7.noarch.rpm
perl-threads-1.87-4.el7.x86_64.rpm
perl-threads-shared-1.43-6.el7.x86_64.rpm
wget-1.14-18.el7_6.1.x86_64.rpm
parallel-20160222-1.el7.noarch.rpm
```

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.