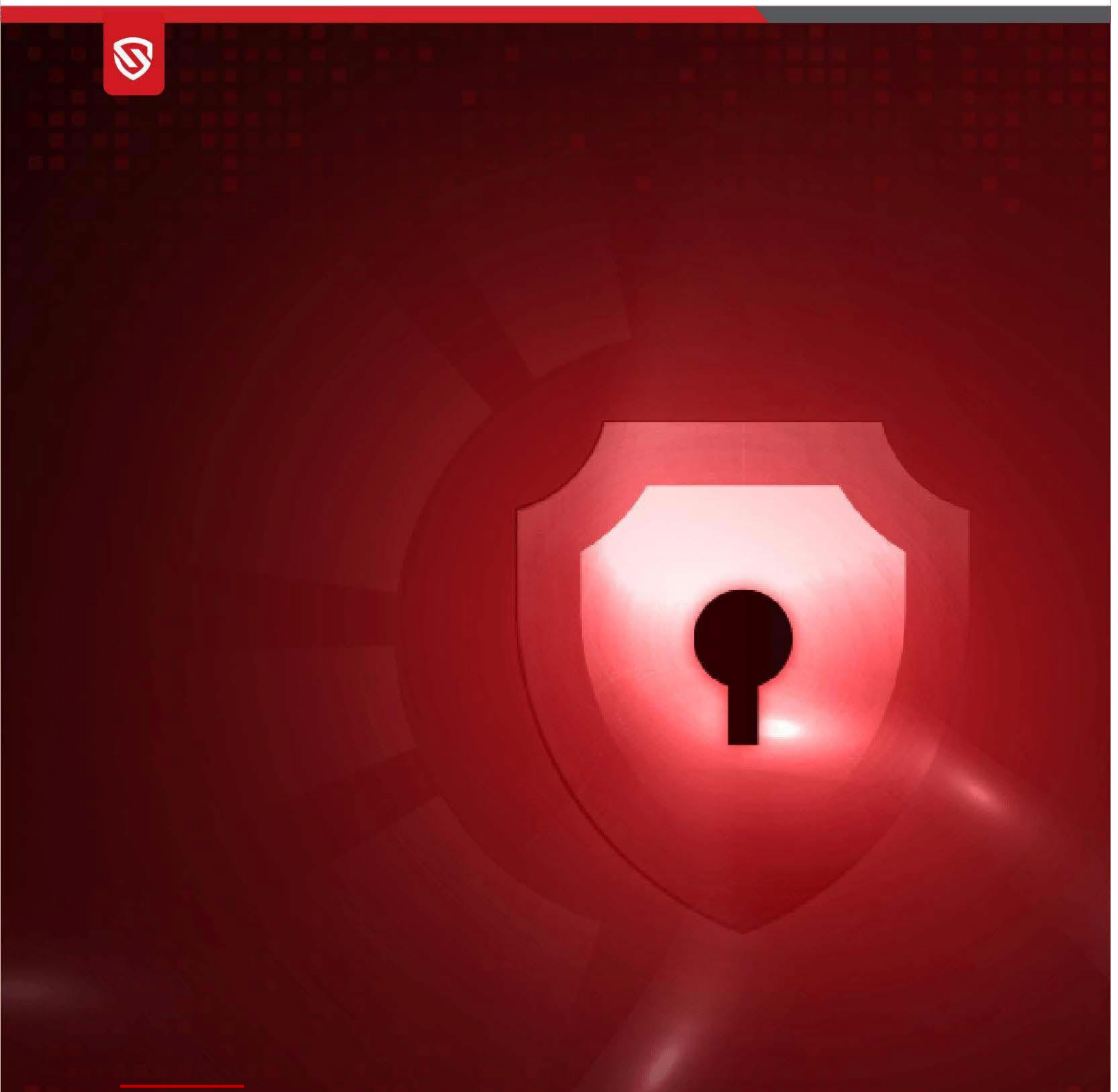
Seqrite

Endpoint Protection EDR



EDR Deployment Guide

EDR 2.1.0

www.seqrite.com

Copyright Information

Trademarks

License Terms

Installation and usage of Seqrite Endpoint Security is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit http://www.seqrite.com/eula and check the End-User License Agreement for your product.

Contents

Overview

The Endpoint Detection and Response (EDR) is a platform deployed on an organization's own infrastructure rather than on a cloud-based environment. It is a system designed to protect the endpoints from potential cyber threats. EDR helps detect and respond to the threats that may evade the traditional antivirus and other security solutions deployed at the endpoint.

Audience

This guide is helpful for Seqrite Administrators and SOC Managers using EPP 8.4 and above with EDR edition.

System requirements for EDR

- Operating System: **Ubuntu** 24.04 LTS server edition
- Kernel version consistency**:** The kernel version must be identical on both the master and worker systems
- VM requirements:
    - Master (1 VM) - 4 vCPU / 8GB RAM / 250GB Disk
    - Worker (1 VM) - 12 vCPU / 32 GB RAM / 1TB Disk

  NOTE:
    - 100 GB of free disk space on /var (both on Master & Worker nodes)
    - 30 GB of free disk space on /home on Master node
- As a part of best practice, all VMs must have a clean OS snapshot.
- High Availability: No

Important: For best performance, use modern server hardware (CPU, RAM, and disk) in addition to meeting the recommended specifications below. Legacy or end-of-life hardware may not deliver expected performance even if capacity requirements are met.

System requirements for EDR with required Endpoints

EDR	Master node			Worker node(s)		
Operating Sys	**Ubuntu 24.04 LTS**			**Ubuntu 24.04 LTS**		
Endpoints	**CPU**	**Memory**	**Disk (SSD)**	**CPU**	**Memory**	**Disk (SSD)**
Below 100	4 Core 2.60GHz or above	8 GB	250 GB	12 Core 2.60GHz or above	32 GB	1 TB
100-1000	4 Core 2.60GHz or above	8 GB	250 GB	16 Core 2.60GHz or above	48 GB	2.5 TB
1000 - 2000	4 Core 2.60GHz or above	8 GB	250 GB	20 Core 2.60GHz or above	52 GB	4 TB
2000-3000	4 Core 2.60GHz or above	8 GB	250 GB	24 Core 2.60GHz or above	60 GB	6 TB
3000-4000	4 Core 2.60GHz or above	8 GB	250 GB	28 Core 2.60GHz or above	68 GB	8 TB
4000-5000	4 Core 2.60GHz or above	8 GB	250 GB	32 Core 2.60GHz or above	76 GB	10 TB
5000- 10000	4 Core 2.60GHz or above	8 GB	250 GB	48 Core 2.60GHz or above	84 GB	20 TB

Network Requirements

The following ports should be allowed/whitelisted in the Network firewall.

Purpose	Protocol	EDR 2.0.0	EDR 2.1.0	Traffic Direction
Communication Between EDR Servers	TCP	6443, 2379:2380, 10250, 10256, 10257, 10259, 179, 22, 30000-32767, 80, 443, 53, 5000, 2381, 35677, 34351, 9099, 10248, 10249, 9100	6443, 2379:2380, 10250, 10256, 10257, 10259, 179, 22, 30000-32767, 443, 53, 5000, 2381, 35677, 34351, 9099, 10248, 10249, 9100	Bi-directional
EPP Server to communicate with EDR	TCP	8080, 443	443	
Endpoint to server Communication	TCP	8184, 31204, 80, 443	8184, 31204, 443	
EDR Server to UM	TCP	18081, 8080	18081	

System requirements for EDR Update Manager

CPU	Memory	Disk	Supported Platforms
2 Core	4 GB	50 GB	Linux Mint 19.2 Linux Mint 20 64bit Ubuntu 22 openSUSE 42.3 64bit openSUSE 15.2 64bit Ubuntu 20.04 64bit Red Hat Enterprise Linux 9.1 BOSS 6 32bit BOSS 8 64bit Rocky Linux

Supported platforms for EDR Clients

Windows (64 bit)	Linux (64 bit)	Mac OS
Windows 8	Ubuntu 16.04,17.04,19.04,20,22.04, 23.04, 24.04 (Kernel version 6.11.x or higher), 26.04	macOS 10.15 Catalina
Windows 8.1	RHEL 7.5, 7.8, 8.1, 8.2, 8.6, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 10.1	macOS 11 Big Sur
Windows 10	Fedora 30, 32, 37, 38, 39, 40, 42	macOS 12 Monterey
Windows 11	Debian 10, 11, 12, 13	macOS 13 Ventura
Windows Server 2012	Linux Mint 19.3,20,21.3	macOS 14 Sonoma
Windows Server 2016	CentOS 8, 8.2, 9	macOS 15 Sequoia
Windows Server 2019	Rocky Linux 8.4, 8.10, 9.3, 9.5, 9.6, 10, 10.1	macOS 26 Tahoe
Windows Server 2022	openSUSE 15.1, 15.2, 42.3	
Windows Server 2025	SUSE Linux 12 SP4	
	SUSE Enterprise Desktop 15	
	BOSS 8, 9, 10	
	Oracle Linux 7.9, 8.8, 8.10, 9.6, 10.1	
	AlmaLinux 9.6, 10	

Getting Started

Prerequisites

- EPP Server installed *(Refer this link for more details on Installing EPP Server.)*
- EPP server with EDR license activated.
- Refer this link for details on Update Manager Guide. Update Manager must be installed to download updates from update manager.
- User privileges**:** Sudo access is required
- For FQDN-based installations, ensure that the FQDN entries for the EPP server, EDR master, and EDR worker machines are added to the **/etc/hosts** file in lowercase on both the EDR master and worker machines.
- Network connectivity**:** Intranet connectivity must be established between the EPP, EDR master, and worker nodes and for EPP 8.5.1 inbound rule should be added in firewall
- Gateway and DNS should be configured in EDR master and worker systems

Deployment Overview

The deployment process is designed to be simple and guided. It includes the following steps:

1. Download the installation script.
2. Run the installation script.
3. Provide required inputs through the CLI prompt (for example, master node IP, worker node details, passwords).
4. The installation script will automatically configure and deploy all necessary components based on the provided inputs.

Note: The installation script may take approximately one hour to complete execution, depending on system performance and network conditions.

Installation Steps

The following steps will guide you through the installation process to set up the Seqrite EDR platform on your environment.

1. Log in to the EDR Master machine with user having sudo privileges.
2. Download the Seqrite EDR installation script using below commands.

   For **EPP Server version 8.5/8.5.1** (Windows), use the EDR version 2.0.0:

   wget https://download.quickheal.com/builds/seqrite/ope/en/openext/Seqrite_EDR_Installer_2_0_0.sh

   For **EPP Server versions 8.4** (Linux) and earlier, use the EDR version 2.1.0:

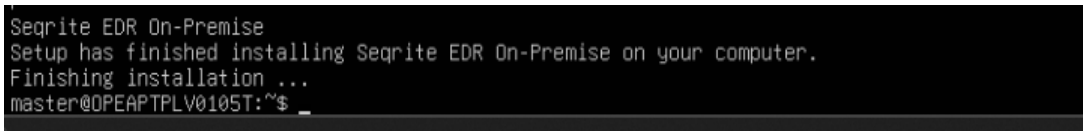
   wget https://download.quickheal.com/builds/seqrite/ope/en/openext/Seqrite_EDR_Installer_2_1_0.sh
3. Run the following command to make the script executable:

   chmod +x Seqrite_EDR_Installer_2_0_0.sh
4. Run the following command to start the installation.
   sudo ./Seqrite_EDR_Installer_2_0_0.sh -c
5. When prompted, provide the required details:
   - **EPP HA Enabled (Yes/No):** Enter **Yes** if the EPP server is deployed in a High Availability (HA) setup. Otherwise, enter **No**.
   - **Is AGR Installed? (Yes/No):** Enter **Yes** if AGR is configured. Otherwise, enter **No**.
   - Enter the **IP address** or **FQDN** of the EPP server, EDR Master and EDR Worker, as per your installation choice.
     - Example (IP Address): 192.168.x.x
     - Example (FQDN): master.ope.com
   - For FQDN-based deployment, when prompted, enter the directory path containing the FQDN certificate (.crt) and private key (.key) files.

```
[redacted] sudo ./Seqrite_EDR_Installer_2_0_0.sh -c
[sudo] password for qhuser:
Unpacking JRE ...
Starting Installer ...
Seqrite EDR On-Premise: Server Details

EPP FQDN or IP address []: 172.XX.XX.XX
License Key []: 815F727B3015B6E203A7
EPP HA Enabled (Yes/No) [No]: No

Is AGR Installed? (Yes/No) [No]: No

EDR Master Node FQDN or IP address []: 172.XX.XX.XX
EDR Master Node username (with sudo privileges) []: qhuser
EDR Master Node Password: RootPassword:


EDR Worker Node FQDN or IP address []: 172.XX.XX.XX
EDR Worker Node username (with sudo privileges) []: qhuser
EDR Worker Node Password:
```

6. Once the installation is completed, you get this message:

Setup has finished installing Seqrite EDR On-Premise on your computer.



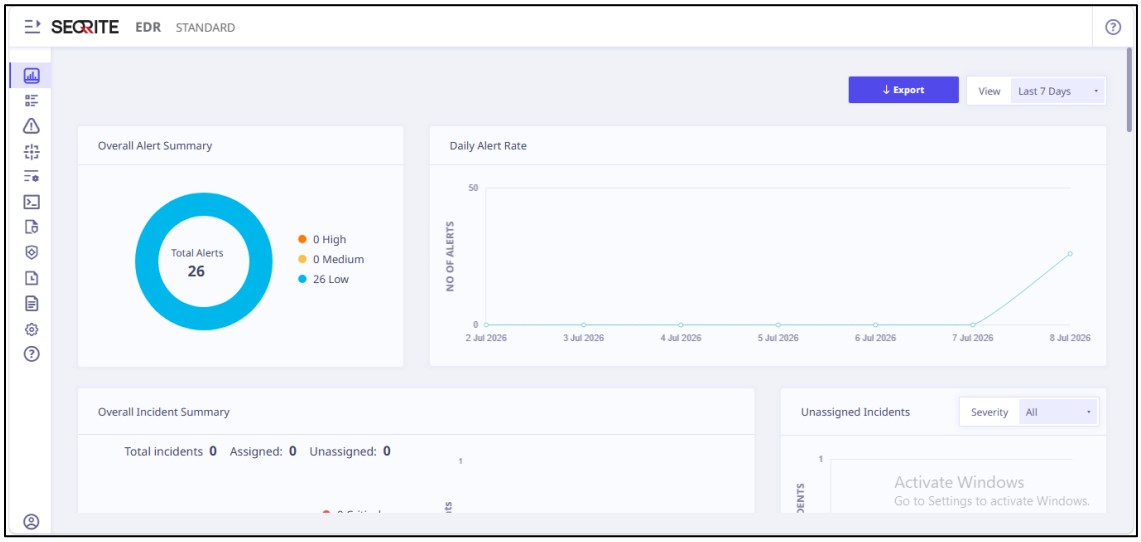
Installation Verification

After the installation is completed, verify that the deployment is successful by performing the following steps:

1. Run the following command to ensure all pods are in a running state:
   kubectl get pods -A -

```
master@master:~$ kubectl get pods -A
NAMESPACE       NAME                                                READY   STATUS
clickhouse      clickhouse-shard0-0                                 1/1     Running
clickhouse      clickhouse-zookeeper-0                              1/1     Running
elasticsearch   elasticsearch-coordinating-0                        1/1     Running
elasticsearch   elasticsearch-data-0                                1/1     Running
elasticsearch   elasticsearch-ingest-0                              1/1     Running
elasticsearch   elasticsearch-master-0                              1/1     Running
kafka           kafka-client                                        1/1     Running
kafka           kafka-controller-0                                  1/1     Running
kafka           kafka-controller-1                                  1/1     Running
kafka           kafka-controller-2                                  1/1     Running
kube-system     calico-kube-controllers-5b5744dbc9-qcjtk            1/1     Running
kube-system     calico-node-f5tms                                   1/1     Running
kube-system     calico-node-jndt4                                   1/1     Running
kube-system     coredns-86648c6f69-qh8fp                            1/1     Running
kube-system     coredns-86648c6f69-zjqxm                            1/1     Running
kube-system     etcd-master                                         1/1     Running
kube-system     kube-apiserver-master                               1/1     Running
kube-system     kube-controller-manager-master                      1/1     Running
kube-system     kube-proxy-4dh5z                                    1/1     Running
kube-system     kube-proxy-f4g6w                                    1/1     Running
kube-system     kube-scheduler-master                               1/1     Running
livequery       create-tenant-user-zb8nm                            0/1     Completed
livequery       livequery-backend-cb94df85-79smx                    1/1     Running
livequery       livequery-redis-6449997996-khwht                    1/1     Running
livequery       osctrl-admin-566968b4bb-v8rm5                       1/1     Running
livequery       osctrl-api-74f5ccccb-77m9z                          1/1     Running
livequery       osctrl-nginx-5f84c7cf77-s7gf5                       1/1     Running
livequery       osctrl-tls-5dc89c8f7-rn7jp                          1/1     Running
livequery       postgres-8586b65c78-72956                           1/1     Running
logging         loki-loki-distributed-distributor-6f45db8c89-h2jl4  1/1     Running
logging         loki-loki-distributed-gateway-7788d4bb76-f7h5b      1/1     Running
logging         loki-loki-distributed-ingester-0                    1/1     Running
logging         loki-loki-distributed-querier-0                     1/1     Running
logging         loki-loki-distributed-query-frontend-55695fd55-wlrjk 1/1     Running
```

2. Open a web browser and log in to the EPP console using your credentials. After successful authentication, click **Advanced Protection** > **EDR** from the left panel to be automatically redirected to the **EDR** dashboard.



Configure EDR Updates

Updates can be downloaded from either the default **CDN URL**, **Update Manager**, or a **local path**.

To enable automatic updates download, follow these steps:

1. Open the **updater.ini** file located at: **/var/qh/ope-data-fresh/deploy/data/updater/updater.ini.**

2. Set these parameters to true:
   UseNewCopy=true

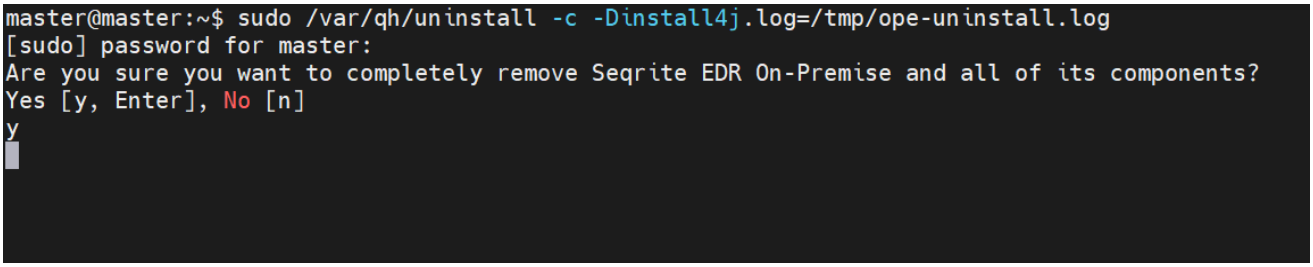
3. Configure the update source:
   a. By default, CDN URL is configured as given below. To download updates from the default CDN URL, retain the default values.
      NewCopyPath =
      https://dlupdate.quickheal.com/builds/seqrite/ope/en/openext/updates/EDR/prdUpdate
      NewCopyChecksumJson =
      https://dlupdate.quickheal.com/builds/seqrite/ope/en/openext/updates/EDR/prdUpdate
   b. To download updates from the Update Manager, modify the URL with the update manager URL as mentioned below:
      NewCopyPath= http://<UpdateManager_IP>:18081/EDR/prdUpdate
      NewCopyChecksumJson= http://<UpdateManager_IP>: 18081/EDR/prdUpdate/checksum.json
   c. If you have updates copied at the predefined location e.g.: /home/qhuser/seqrite-updates, then update the path as below:
      NewCopyPath = /home/qhuser/seqrite-updates
      NewCopyChecksumJson = /home/qhuser/seqrite-updates/checksum.json

4. Save the file and your updates are configured

Uninstalling EDR

To uninstall the EDR server, use the command below and provide the appropriate inputs when prompted.
`sudo /var/qh/uninstall -c -Dinstall4j.log=/tmp/ope-uninstall.log`

Note: Execute the above command from any location except **/var/qh**.



Troubleshooting

If you encounter issues during installation, follow these steps:

1. **Verify the operating system version**
   Ensure that the system is running **Ubuntu 24.04 LTS**. Other versions are not supported.
2. **Validate system resources**
   Make sure that there are adequate **disk space** and **available memory** to support the installation process.
3. **If the installation fails,**
   Check the log file at **/var/qh/ope-data-fresh/app.log** for detailed error messages.
4. If any of the services fail, then use the command below to check the service logs:
   - `kubectl get pods -A` – (to get the list of all the services)
   - `kubectl –n <NAMESPACE> logs –f <NAME>` - (to check the logs of a specific service)
     For example, `kubectl -n service logs -f ope-ui-cb7b5d8f-b6ffs`