VOSS Insights
Analytics Install Guide

Release 22.2

Oct 18, 2022

Legal Information

DOCUMENT ID: 20221018102824

Contents

1.   What's New

1.1.   Analytics Install Guide: Release 22.2

- EKB-13160: Add multi-line support to the SSHD config. See: *Deploy and VM Installation Steps*

  Added note for SSHD Config that multi-line entries can be added if needed.

- EKB-13823: Update Insights build process to generate SHA256 checksums for all published artifacts. See: *Dashboard Download*

  Added verification step using .sha256 checksum files.

2. Insights Analytics Quickstart

2.1. Insights Analytics Setup Overview

Set up Insights Analytics solution

Two products to set up:
- Dashboard
- Arbitrator

Additional:
- Windows Forwarder Install

Dashboard Setup

Arbitrator Setup

2.2. Dashboard Setup

```
                              ●
                              │
                              ▼
        Yes  ◄── New Dashboard Install? ──►  No
         │                                    │
         ▼                                    ▼
  ┌──────────────────┐              ┌──────────────────────┐
  │ Download install │              │ Download upgrade file│
  │       file       │              └──────────────────────┘
  └──────────────────┘                        │
         │                                     ▼
         ▼                              ┌──────────────────────┐
  ┌──────────────────────┐    • Port    │ Upgrade Dashboard    │
  │ Dashboard Setup      │    requirements└──────────────────────┘
  │ Requirements         │                        │
  └──────────────────────┘                        │
         │              • Sizing                   │
         ▼              • Cloud Installation        │
  ┌──────────────────────┐                         │
  │ VM / cloud hardware  │                         │
  │       spec           │                         │
  └──────────────────────┘                         │
         │                                          │
         ▼                                          │
  ┌──────────────────┐                             │
  │ Dashboard Install│                             │
  └──────────────────┘                             │
         │         • Send PRODUCT ID to VOSS        │
         ▼         • Receive, add PRODUCT KEY       │
  ┌──────────────┐                                  │
  │  Licensing   │                                  │
  └──────────────┘                                  │
         │                  ◆                       │
         └──────────────►   ◆   ◄──────────────────┘
                            │
                            ▼
                            ⊗
```
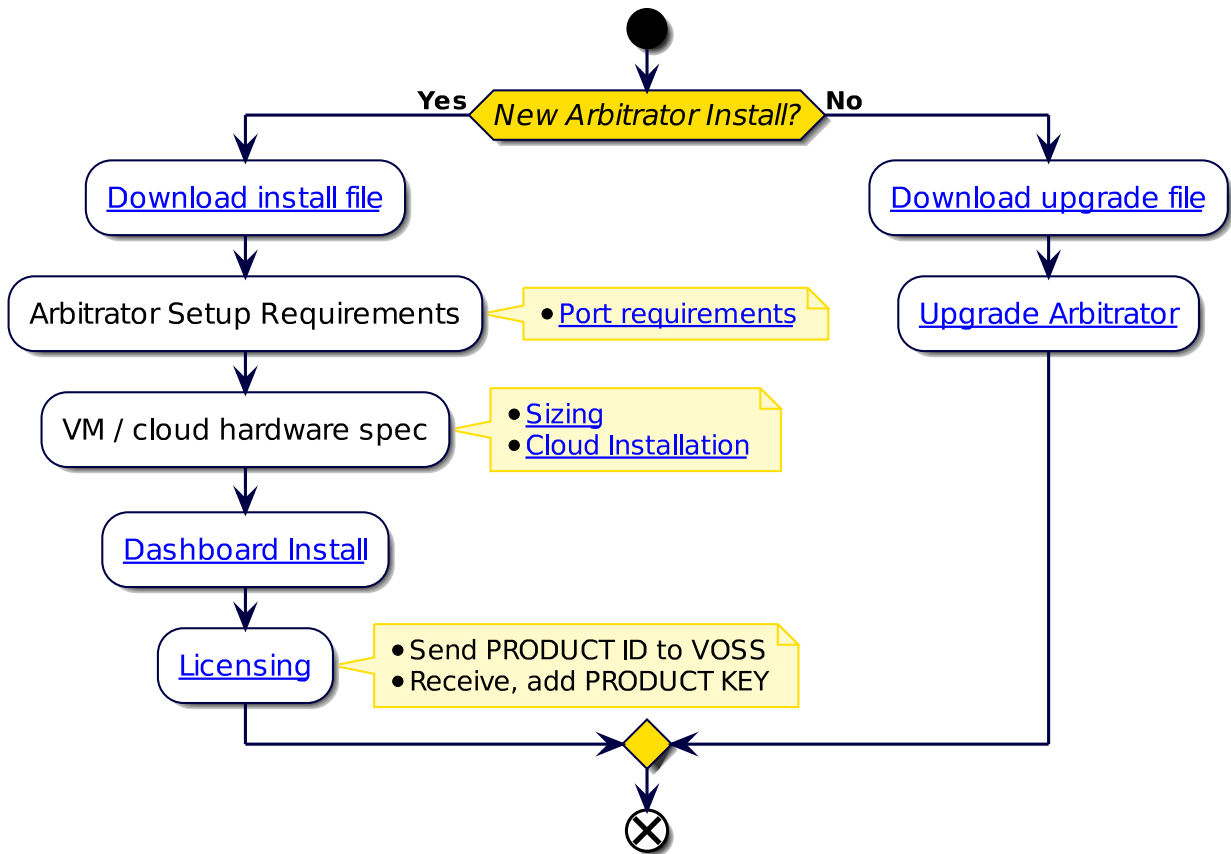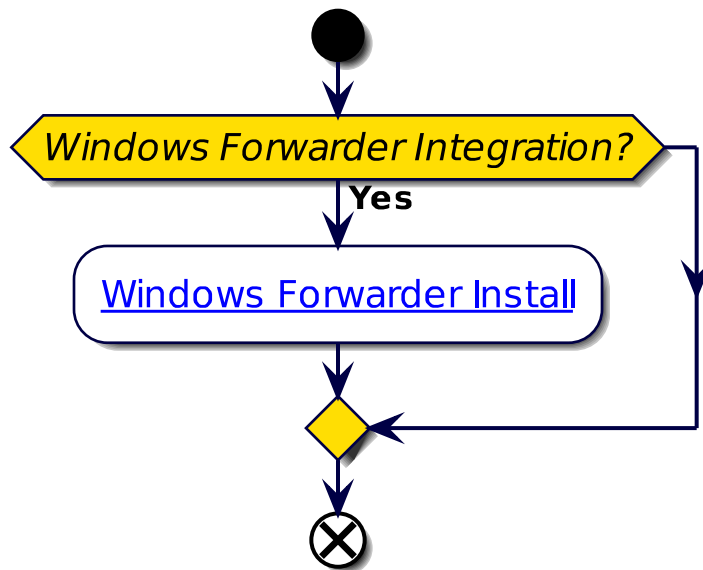
3

2.3.   Arbitrator Setup

New Arbitrator Install?

Yes

No

Download install file

Download upgrade file

Arbitrator Setup Requirements

- Port requirements

Upgrade Arbitrator

VM / cloud hardware spec

- Sizing
- Cloud Installation

Dashboard Install

Licensing

- Send PRODUCT ID to VOSS
- Receive, add PRODUCT KEY

2.4.   Dashboard Integrations

```
        ●
        │
        ▼
 ◁ Windows Forwarder Integration? ▷
        │ Yes
        ▼
 ╭──────────────────────────╮
 │  Windows Forwarder Install  │
 ╰──────────────────────────╯
        │
        ▼
        ◆
        │
        ▼
        ⊗
```

2.5.   Analytics Solution Documentation

2.5.1.   Additional Reference Documentation

- Dashboard Release Notes
- Compatibility Matrix
- Dashboard Install Guide
- Dashboard and Arbitrator Maintenance and Upgrade Guide
- Dashboard Administration Guide
- Dashboard API Guide
- Platform Guide
- Arbitrator Release Notes
- Compatibility Matrix
- Arbitrator Install Guide
- Dashboard and Arbitrator Maintenance and Upgrade Guide
- Arbitrator Administration Guide
- Arbitrator API Guide
- Platform Guide
- VOSS Insights Windows Forwarder Install Guide

3. Download

3.1. Dashboard Download

- Dashboard OVA file:

  1. Log in on the VOSS Customer Portal

  2. Go to **Downloads > VOSS Insights > Insights Dashboard > <release number> > New Installation**.

  3. Download the `.ova` file

  4. Verify that the original `.sha256` checksums on the download site server match.

     – **system checksum media/<ova_file>**

     ```
     Checksum:   <SHA256>
     ```

- Dashboard upgrade file:

  a. Log in on the VOSS Customer Portal

     i. Go to **Downloads > VOSS Insights > Insights Dashboard > <release number> > Upgrade**.

     ii. Download the `.lxsp` upgrade file

     iii. Verify that the original `.sha256` checksums on the download site server match.

        – **system checksum media/<lxsp_file>**

        ```
        Checksum:   <SHA256>
        ```

  or

  b. Use the direct link - for automated download mechanisms:

     i. http://www.layerxtech.com/downloads/analytix/updates/layerX-reporter-sp66-sp22.1.1.lxsp

        To ensure continuity, the release updates will still be available from the LayerX download site, allowing customers to either download files manually, or via the automated download mechanisms from that location.

4. VMWare Specification and Requirements

4.1. Dashboard Reporting VM Sizing Specifications

Size	Cores (vCPU)	CPU Spec (Ghz)	Memory (Gb)	Storage (Gb)	Storage Spec	Network
Up to 5k users	8	2,8	16	500	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB
5k to 20k users recommended option	12	2,8	32	500	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB
20k to 40k users	16	2,8	128	500/1000	SSD preferred Thick Eager Zero 15k HDD 1500 IOPS	1GB

- The specs for 5k up to 20k users is the recommended option.

4.2. Cloud Installation

The VMWare specification and requirements for each product can be used as guidelines when preparing for cloud installations.

For example, for the example minimum sizes below, the VM specifications are best matched by the cloud VM types indicated:

- Google Cloud products

Product	Size	Cloud VM Specification
Arbitrator	< 5k users	n2-standard-8
Dashboard	< 10k users	n2-standard-8
Raptor	N/A	custom
DS-9	< 1,000 flows/sec	n2d-standard-16

• Amazon Web Services

Product	Size	Cloud VM Specification
Arbitrator	< 5k users	t2.2xlarge
Dashboard	< 10k users	t2.2xlarge
Raptor	N/A	t2.small
DS-9	< 1,000 flows/sec	m6g.4xlarge

• Microsoft Azure

Product	Size	Cloud VM Specification
Arbitrator	< 5k users	B8ms
Dashboard	< 10k users	B8ms
Raptor	N/A	B1ms
DS-9	< 1,000 flows/sec	D16 v5

5. Port Requirements

5.1. Arbitrator and Dashboard System Connectivity

This table includes connectivity requirements between Insights Arbitrator, Reporting Dashboard, as well as connectivity between these and the following: VOSS Automate, NTP, DNS and AD.

Source	Destination	Port / protocol	Notes
Arbitrator Server / Dashboard Server	Arbitrator Server / Dashboard Server	5432, 5433, 5000, 60514, 64514, 64515, 65515, 65516, 64005, 64004, 62009, 62010 (all TCP)	Note: Intra-system communication and queries – Bi-directional
Arbitrator Server	Arbitrator Server	62002, 62003, 62004, 62005, 62006, 11501,30501, 30503, 40501, 40503 (all TCP)	Note: VOSS Fabric TLS tunnel Connection Ports – Bi-directional between Customer systems and NOC systems for event forwarding
Arbitrator Server / Dashboard Server	Network Resources (NTP, DNS)	53, 123 UDP	Time and DNS
Client PC – GUI Interface and CLI Management Access	Arbitrator Server / Dashboard Server	443, 8443, 22, 80 TCP	User Interface Access
VOSS Automate	Dashboard Server	27020	Database access
Arbitrator Server / Dashboard Server	AD	389 636 TCP UDP	Authentication

5.2. Cisco UC Monitoring System Connectivity

Source	Destination	Port / protocol	Notes
Monitored Cisco UC system	Correlation Server / Dashboard Server	514 tcp/udp, 22 tcp, 162 udp	Cisco syslog, snmp trap, CDR/CMR file transfer
Correlation Server	Monitored Cisco UC system	443 tcp, 8443 tcp, 22 tcp, 21 tcp, 161 udp	Correlation server AXL query, ssh and snmp query

5.3. MS Teams System Connectivity

Source	Destination	Port / protocol	Notes
MS Teams - Cloud Agent	Cloud Arbitrator	5432 tcp 443 tcp	Collects data from the MS Teams Tenant to the arbitrator
Cloud Arbitrator	Dashboard Server	5432 tcp	Pushes data to the dashboard to display dashboard data
Client PC – GUI Interface and CLI Management Access	Correlation Server / Dashboard Server	443, 8443, 22, 80 TCP	User Interface Access

5.4. NetFlow and DS9 Monitoring System Connectivity

5.4.1. Communication ports between NetFlow Source and DS9

Source	Destination	Protocol	Port	Direction	Description
NetFlow Source	DS9	UDP	4739	Unidirectional	IPFIX (Optional)
NetFlow Source	DS9	UDP	2055	Unidirectional	NetFlow v9 (Optional)
NetFlow Source	DS9	UDP	9996	Unidirectional	NetFlow v5 (Optional)
NetFlow Source	DS9	UDP	6343	Unidirectional	Sflow v5 (Optional)
DS9	NetFlow Source	UDP	161	Unidirectional	SNMP queries

5.4.2. Communication ports between Dashboard Server Users and Dashboard Server

Source	Destination	Protocol	Port	Direction	Description
Dashboard users	**Dashboard** Server	TCP	443	Unidirectional	HTTPS (GUI access)

5.4.3. Communication ports between the DS9 Server and Dashboard Server

Unless the DS9 and Dashboard Servers are located in the same subnet, system administrators need to ensure the following network ports are open between these two components.

Source	Destination	Protocol	Port	Direction	Description
Dashboard Server	DS9	TCP	5432	Unidirectional	Data respository access
Dashboard Server	DS9	TCP	8082	Unidirectional	Data respository access
Dashboard Server	DS9	TCP	443	Unidirectional	DS9 System Stats and management
DS9	Dashboard Server	UDP	514	Unidirectional	DS9 System Logs

5.4.4. Communication ports that are required for remote management purposes

Source	Destination	Protocol	Port	Direction	Description
Admin users	DS9	TCP	22	Unidirectional	SSH (remote CLI access) and file transfer
Admin users	**Dashboard** Server	TCP	22	Unidirectional	SSH (remote CLI access) and file transfer
Admin users	**Dashboard** Server	TCP	443	Unidirectional	WEB access

5.5. VOSS Automate Port Usage

VOSS Automate port usage for each node type:

Protocol	Ports	WebProxy node	Application node	Database node
ssh / sFTP	TCP 22	X	X	X
http	TCP 80	X	X	
https	TCP 443, 8443	X	X	
snmp	TCP/UDP 161, 162	X	X	X
mongodb	TCP 27017, 27030		X	
mongodb	TCP 27019, 27020			X
LDAP	TCP/UDP 389 (636 TLS/SSL)		X	
NTP	UDP 123		X	
SMTP	TCP25		X	X

5.6. Skype for Business Monitoring System Connectivity

Source	Destination	Port / protocol	Notes
VOSS Forwarder installed on Windows Machine	Customer SfB Monitoring Server (SQL)	1433	Collection of CDR/QoS Data. SfB monitoring server is typically deployed on the SfB Front-End Server (Option 1)
VOSS Forwarder installed on Windows Machine	Separate Customer SfB Reporting Server - QoE DB (SQL)	1433	Collection of CDR/QoS Data from the Reporting (QoE) Server that is a replication of the SfB Monitoring Server (Option 2)
VOSS Forwarder installed on Windows Machine	Arbitrator Correlation	62009-62010, 514	Management and Syslog Traffic
VOSS Forwarder installed on Windows Machine	Dashboard / Reporting	62009-62010, 5432-5433, 80, 443, 514, 1194	Management and Syslog Traffic
SfB Monitoring Server	Dashboard / Reporting	1433	SQL Transactional Data Replication
SfB Monitoring Server	Arbitrator Correlation	80, 443	SDN Traffic
SfB Monitoring Server	Dashboard / Reporting	80, 443	SDN Traffic

6.   Deploy and Networking Setup

6.1.   Deploy and VM Installation Steps

1. Download the OVA for your system to a directory accessible by the VM client.

2. Deploy the OVA:

   Select the downloaded OVA file and choose a VM name.
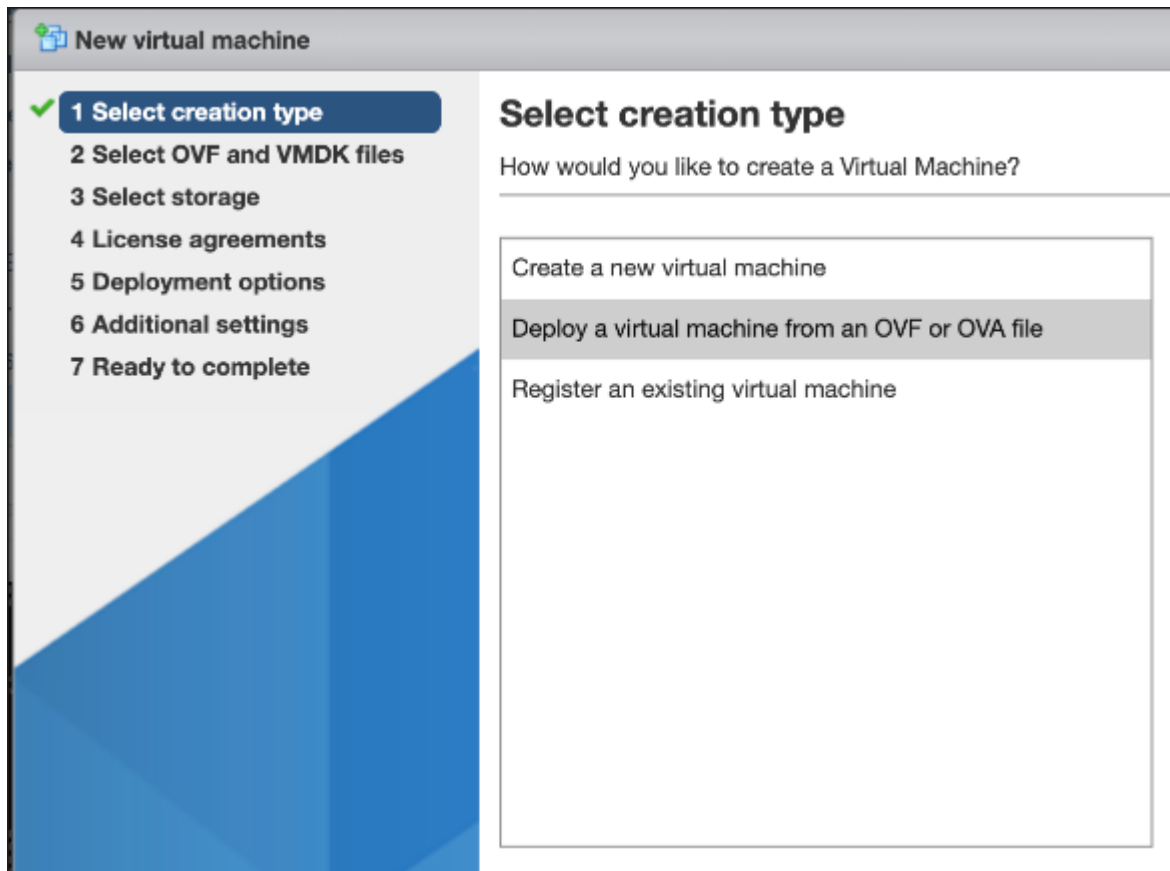
3. Select *storage* according to the recommended hardware specifications for the required configuration. See the *VMWare Specification and Requirements* for your system.

4. Select *network* mappings according to the recommended hardware specifications for the required configuration. See the *VMWare Specification and Requirements* for your system.

5. When you run the VM, you will see `.lxp` packages being installed. This takes a while.

6. After all the packages are installed, the VM is automatically powered off.

You will see the `auto-poweroff` message on the console.

7. After the system boots, wait at the `login:` prompt until a banner with an `About` console display shows displaying values for the placeholders below:

```
                  About
================================================
      Hostname:   <hostname>
       Version:   <version>
         Theme:   <theme>
        Flavor:
       License:   NNNNN-NNNNN-NNNNN-NNNNN-NNNNN
 Days Licensed:   nnnnn
Days Remaining:   nnnnn
   Product Key:
       Website:   <website>
        Kernel:   Linux n.nn.nn-lxt-3 x86_64 GNU/Linux

<hostname> login:
```

8. At the `login:` prompt, log in as `admin` with password as the last 10 characters of the `License:` value, *excluding the dash*.

Note: Since the Licence key value is only displayed here. When you ssh in it will not be seen. Be sure to copy out your admin password from this console.

Changing the admin password is possible via the **Change Passwords** menu option.

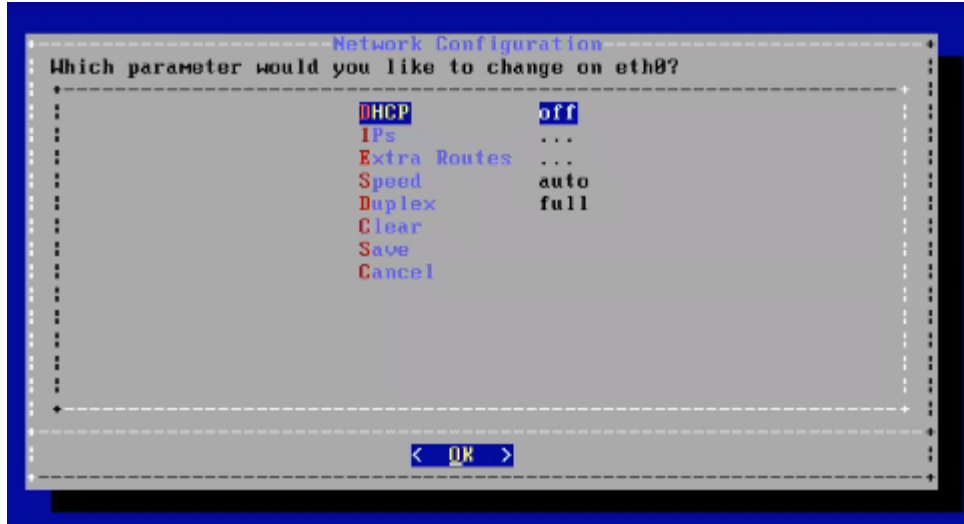9. After login, the **Administration** menu shows, as in the example below for DS9:
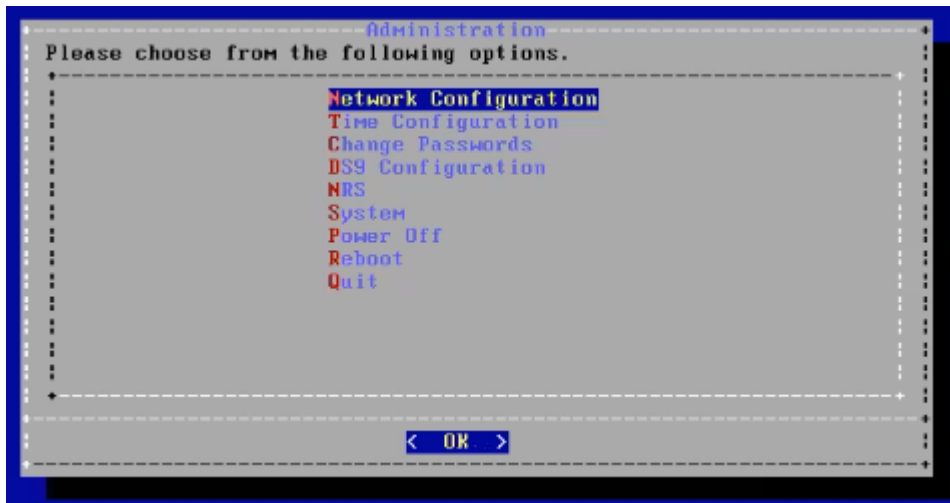
10. Under **Network Configuration**, provide ip/netmask, default gateway and hostname.

    a. Under **Interface Settings**, select the interface to configure.

       Select **IPs** and set the IP Address and netmask in the format `nn.nn.nn.nn/24` and save.
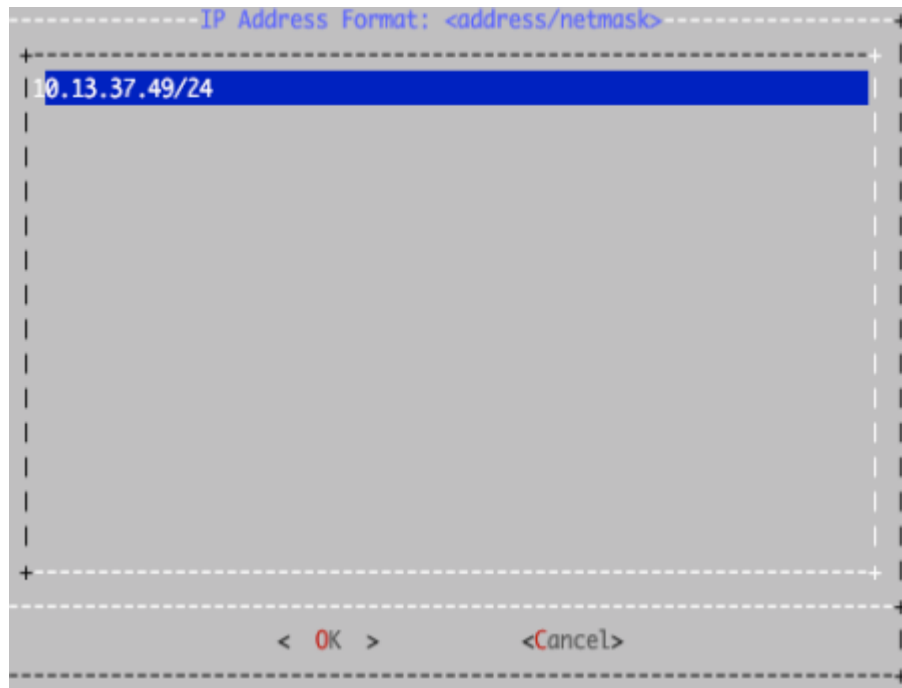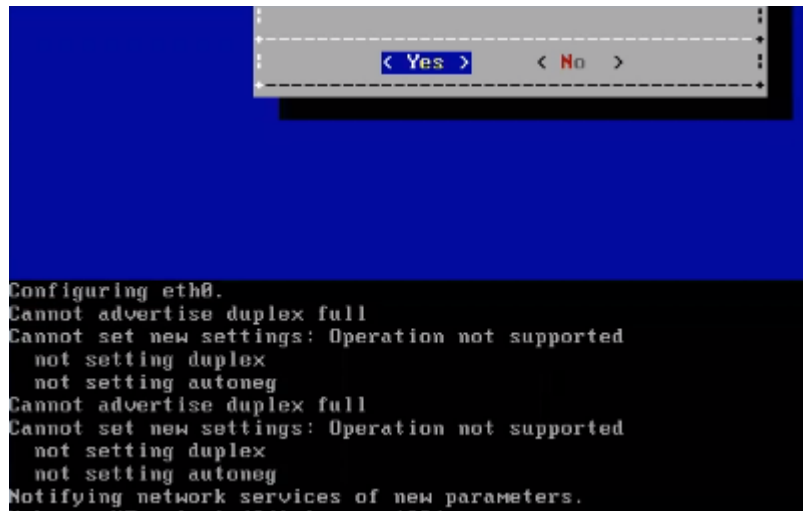

       Modify the parameters for the selected interface:

Set up the default gateway under the **Extra Routes** menu.

Be sure to use the format *default <gateway IP address>* for the entry. The word *default* is required. For additional route entries use the *<subnet> < gateway>* format. Similar to what would be done on a Linux system at the CLI.

b. Set hostname

The console will show the `Updating hosts:` message. Note that this setup takes a few minutes.

c. For **SSHD Config**, multi-line entries can be added if needed - for example for CUCM v11.5 support. See: *Multi-line CUCM Cipher support*.

Note: This step is not relevant to the DS9 and Insights NetFlow solution. This step is relevant only to an Insights Assurance solution and its integration with Cisco UC systems.

---

11. Base system installation is now complete. Select **Quit** to exit the **Administration** menu on the console and continue with product registration and with the configuration of your system through the GUI:

    • Insights Dashboard

      See the VOSS Automate Database Setup section in the VOSS Insights Install Guide.

    • Insights Arbitrator (relevant only to an Insights Assurance solution and its integration with Cisco UC systems)

      See the Install Arbitrator System section in the VOSS Insights Install Guide.

    • Insights DS9

Note: Prior to opening the DS9 GUI, reboot the system.

See the DS9 Product Registration and Configuration on the Dashboard section in the VOSS Insights DS9 for NetFlow Install Guide.

6.1.1. Multi-line CUCM Cipher support

This section provides details for the use of the **SSHD Config** menu option.

Note: This section is not relevant to the DS9 and Insights NetFlow solution. This solution is relevant only to an Insights Assurance solution and its integration with Cisco UC systems.

For CUCM v11.5 support:

```
kexalgorithms diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,diffie-hellman-
↪group-exchange-sha1
ciphers aes128-cbc,3des-cbc,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,
↪aes256-gcm@openssh.com
macs hmac-md5,hmac-sha1,hmac-sha2-256,hmac-sha1-96,hmac-md5-96
hostkeyalgorithms ssh-rsa,ssh-dss
```

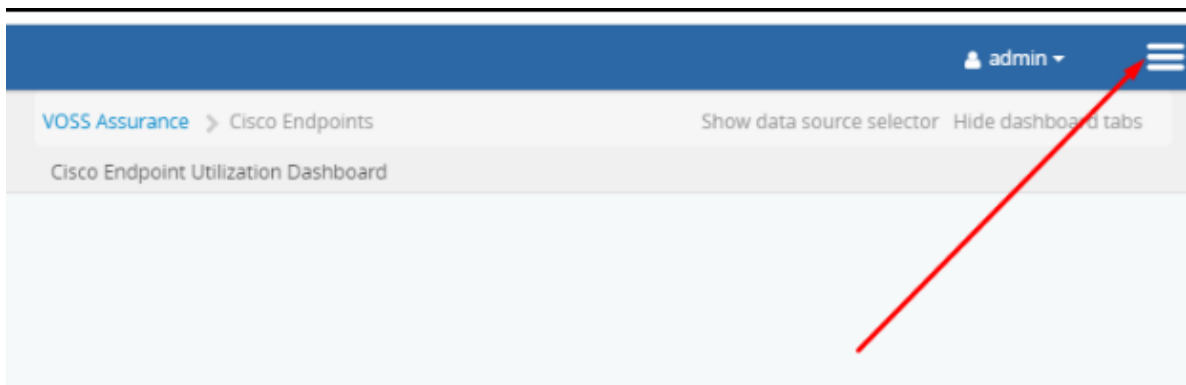# 7. VOSS Automate Database and System Setup

7.1. VOSS Automate Database Setup
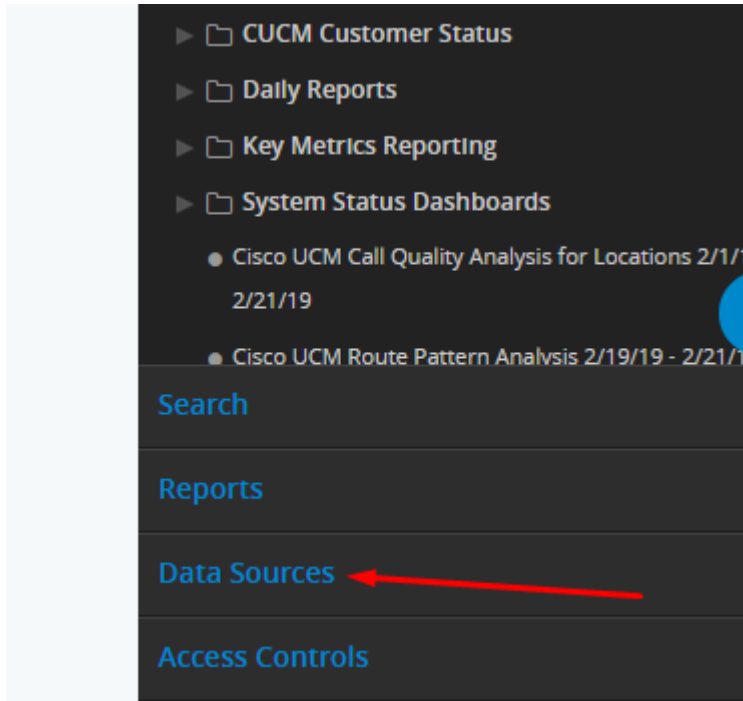
1. Add a Database user - this is a Read only user

2. Take note of the username and password you just configured
3. Log in to the GUI on the Dashboard Server username admin — password admin
4. Click the toolbar Hamburger Menu icon adjacent to the admin menu.

5. Click **Data Sources**.

6. Click **New Data Source**.
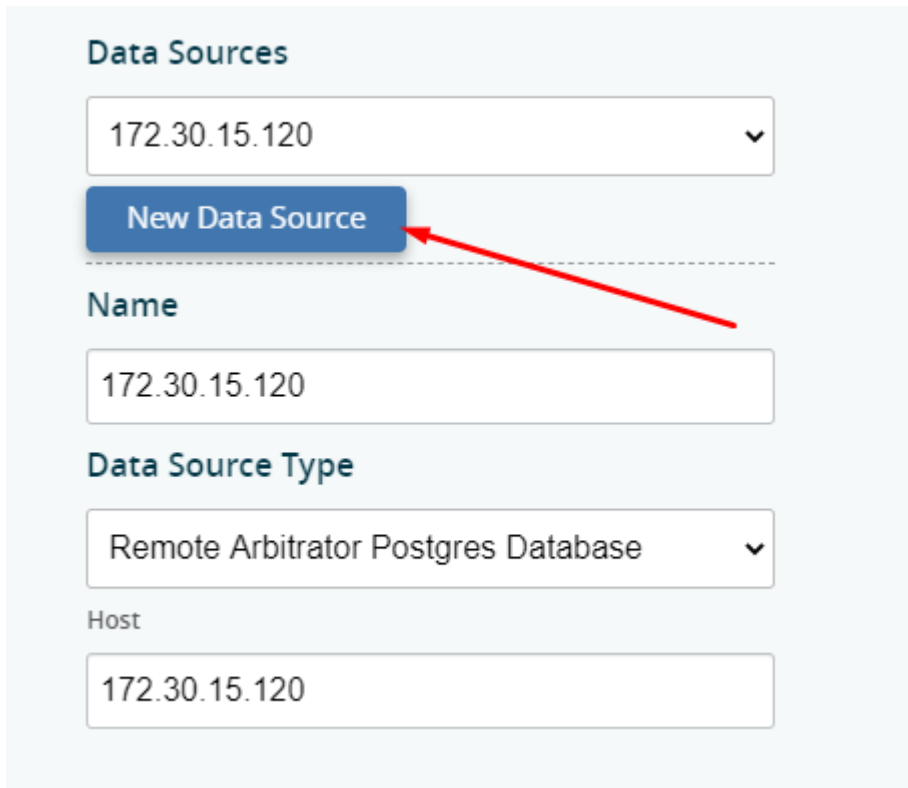
7. Choose **Voss Mongo Database**.

Data Source Type

Voss Mongo Database

Ip

localhost

Port

27020

Db

VOSS

Username

admin

AuthSource

admin

Password

••••••••••••

Ssl

true

Alias

Cancel   Save

8. Fill out the form presented:

- At **Name**, fill out a name for the data source.

- At **Data Source Type**, choose the data source type.

- At **IP**, set the IP address of VOSS Automate UN1/primary database node.

- Fill out values for **Port** and **DB**.

- At **Username**, fill out the username you set on VOSS Automate.

- At **AuthSource**, change the AuthSource from admin to VOSS.

- Fill out the password set up in VOSS Automate.

- Set SSL to True.

9. Repeat the steps above to add the Arbitrator as a Data Source:

- Fill out a name for the data source.

- Select the data source type (Remote Arbitrator Postgre Database), and fill in the rest of the fields.
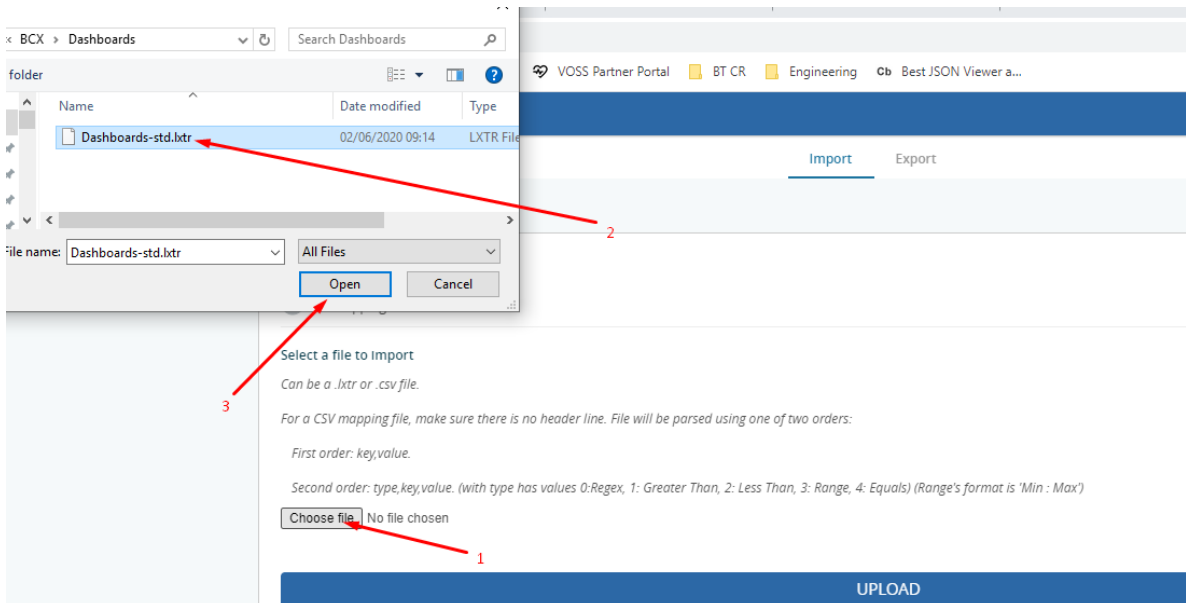
- At **Host** set the IP address of the Arbitrator.

- Fill out the port.
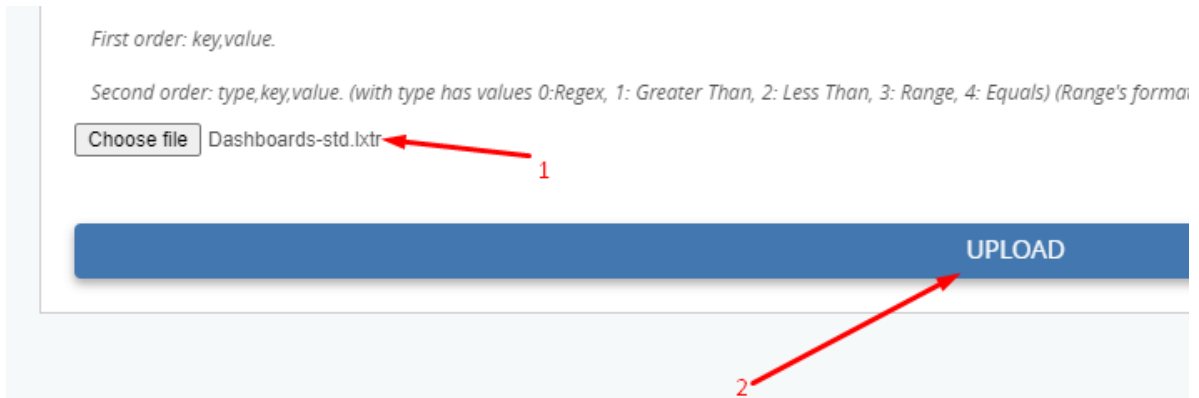
7.2. Install Dashboard System

1. Access the Dashboard Server: `admin/admin`

2. In the top banner bar click on admin, then click on **Import/Export Wizard**.
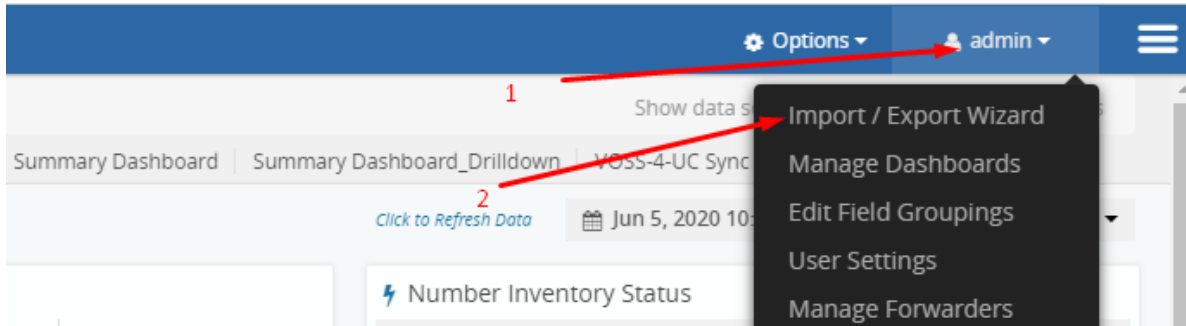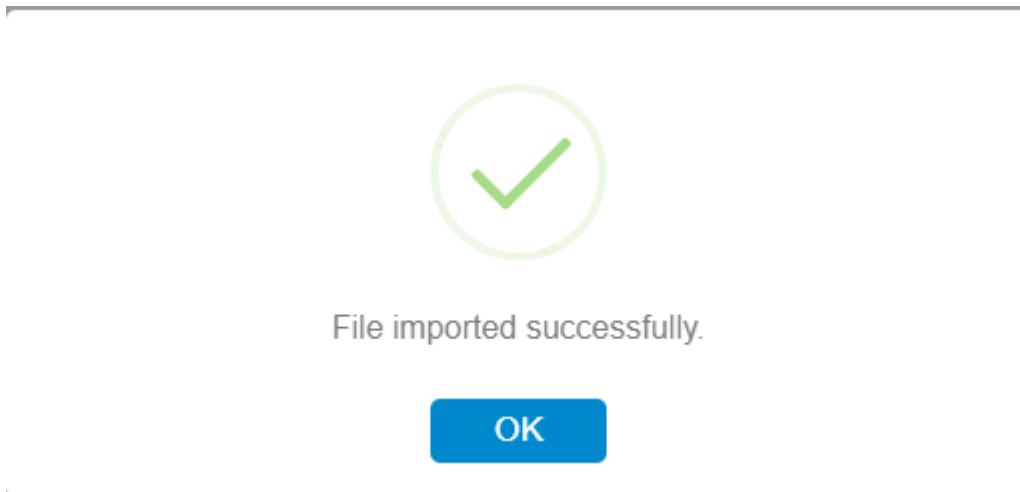

3. Click on **Choose file**, then navigate to the file you wish to import (dashboard files have the `.lxtr` file extension) then click **OK**.
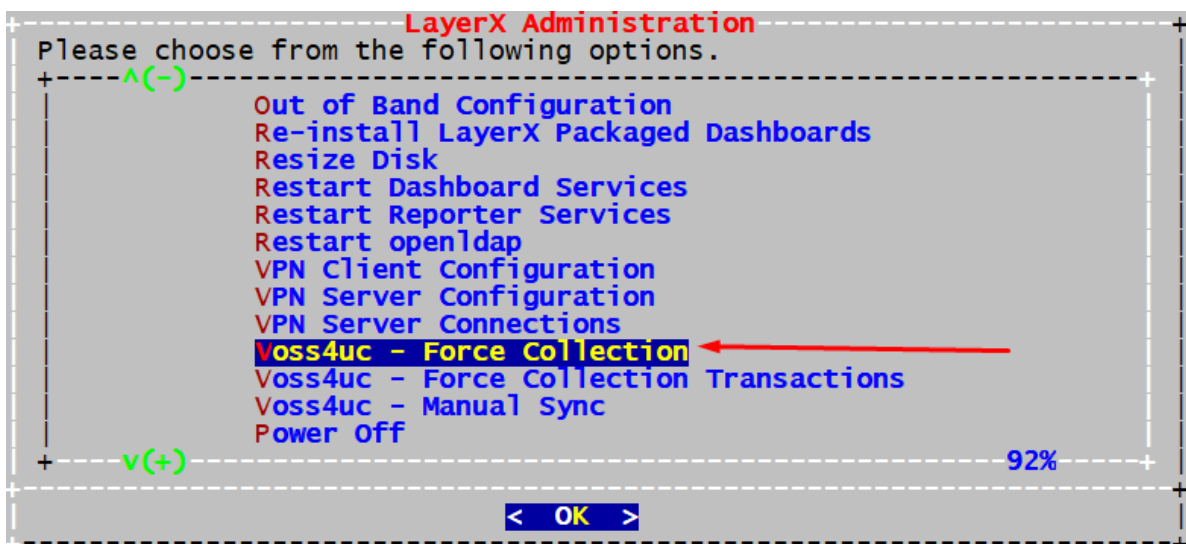

4. Ensure your file is visible adjacent to **Choose file**, then click **Upload**.

5. Your file will then upload, and you will see the below — click **OK**.

6. Log in to the Dashboard CLI as `admin/admin`.

7. Navigate down to **Voss - Force Collection** and click **OK**. This will then sync VOSS Automate data into the dashboard.

8. Certificates

8.1.   Add Certificates

1. SCP the new `server.crt` and `server.key` files to the `etc/apache2/` directory on the system, overwriting the old certificate files.

   Recommended: back up the current certificate files prior to overwriting them.

2. SSH to the system as `root` and restart the apache service using the **sv restart apache** command.

3. Clear browser cache.

4. Apache will now use the new signed certificate.

Index

F

Flowchart
    Insights Analytics Setup Overview, 2
    Insights Arbitrator for Analytics Setup,
        4
    Insights Dashboard for Analytics Setup,
        3
    Insights Dashboard Integrations for
        Analytics Setup, 5