VOSS Insights
DS9 for NetFlow Install Guide

Release 22.2

Oct 18, 2022

Legal Information

DOCUMENT ID: 20221018104203

Contents

1. What's New

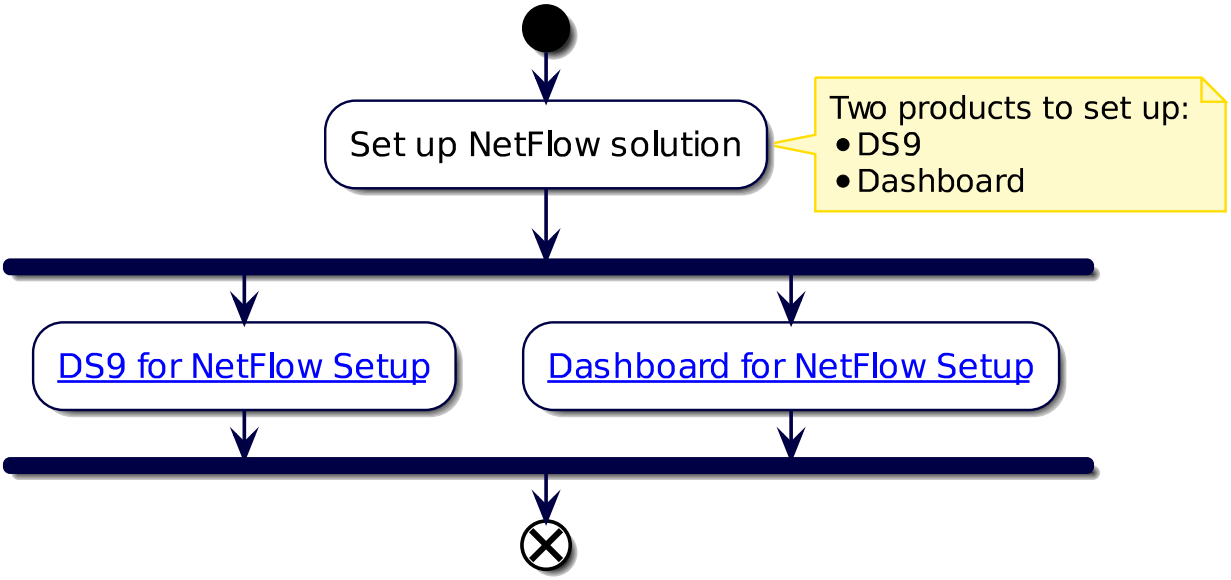
1.1. DS9 for NetFlow Install Guide: Release 22.2

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

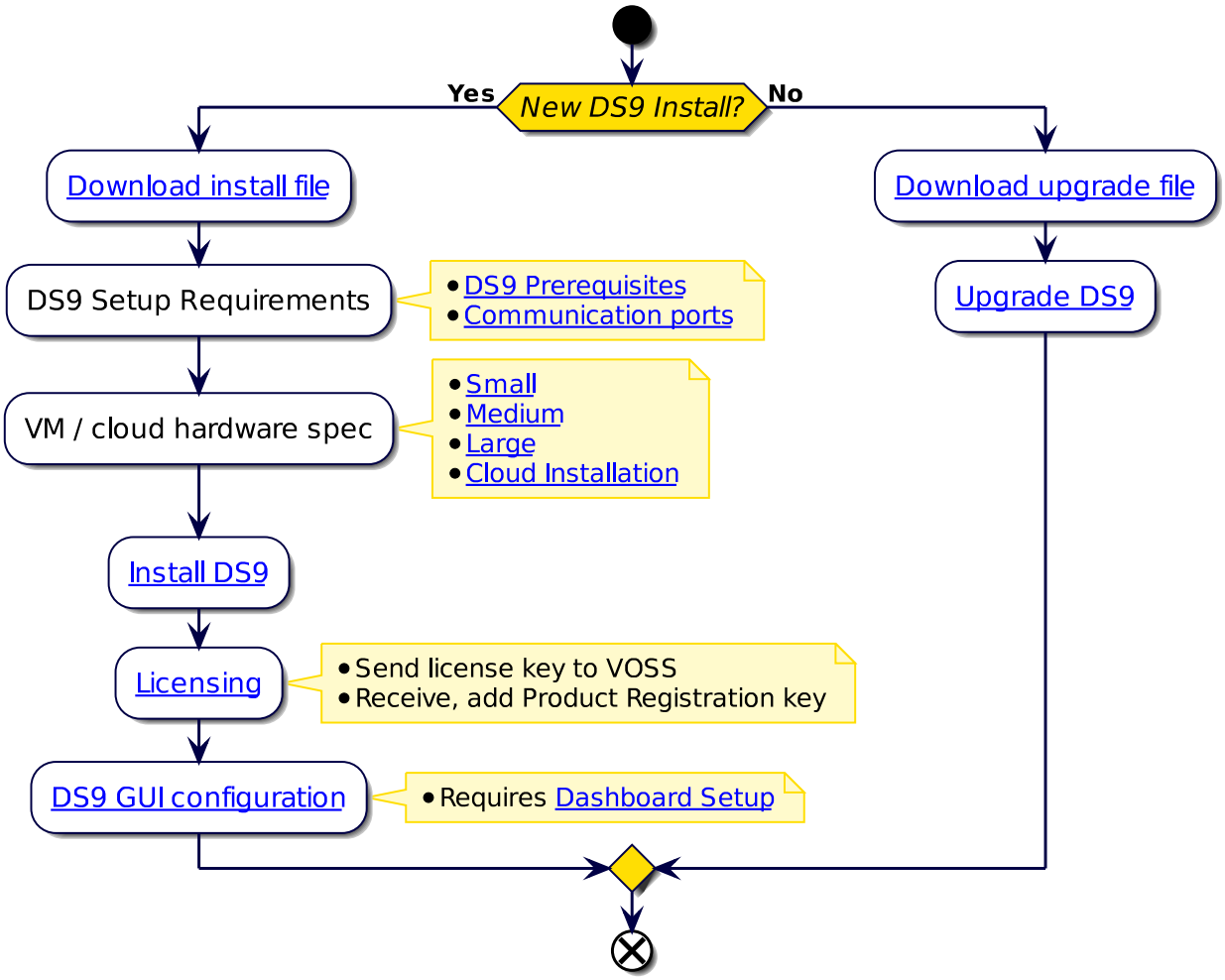
  Added note for SSHD Config that multi-line entries can be added if needed.

2. NetFlow Quickstart

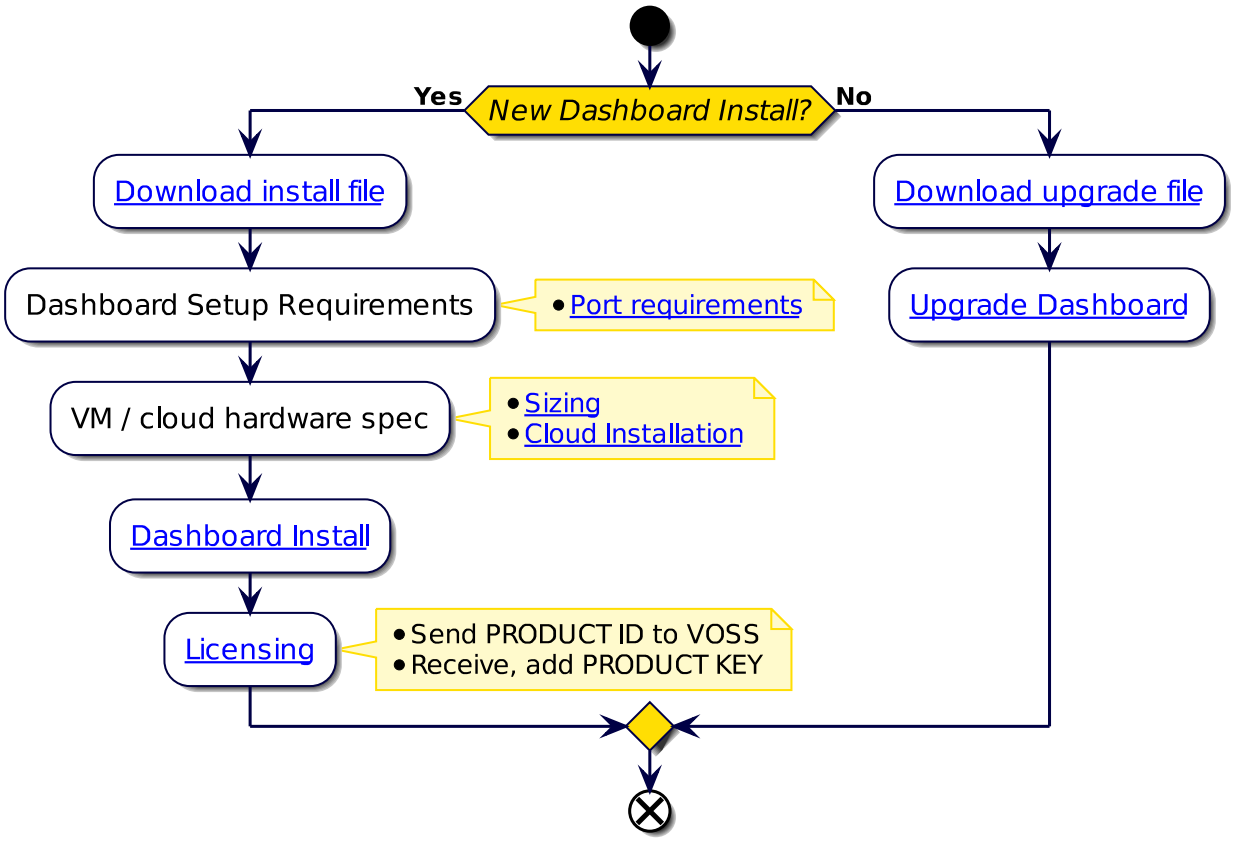
2.1. NetFlow Setup Overview



2.1.1. DS9 for NetFlow Setup



2.1.2. Dashboard for NetFlow Setup



2.2. NetFlow Solution Documentation

2.2.1. 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

3. DS9 Download

- DS9 OVA file:
  1. Log in on the VOSS Customer Portal
  2. Go to **Downloads > VOSS Insights > Insights DS9 Hawaii > <release number> > New Installation**.
  3. Download the `.ova` file
- DS9 upgrade file:
  a. Log in on the VOSS Customer Portal
     i. Go to **Downloads > VOSS Insights > Insights DS9 Hawaii > <release number> > Upgrade**.
     ii. Download the `.lxsp` upgrade file

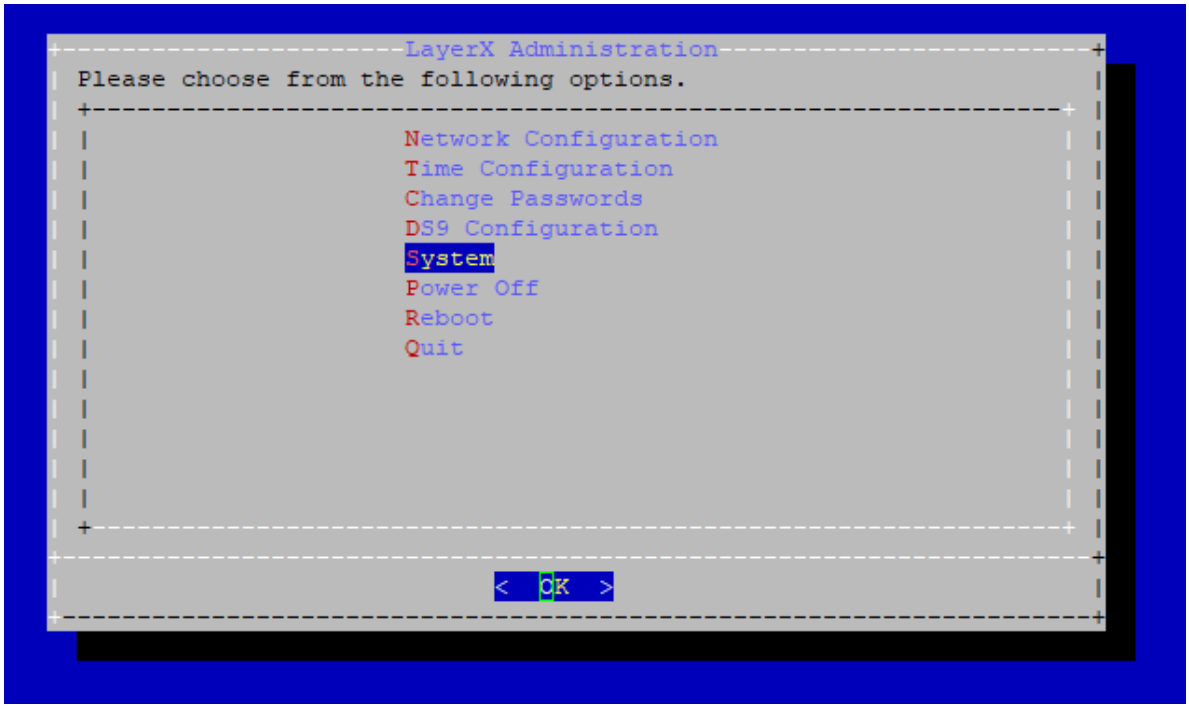
  or

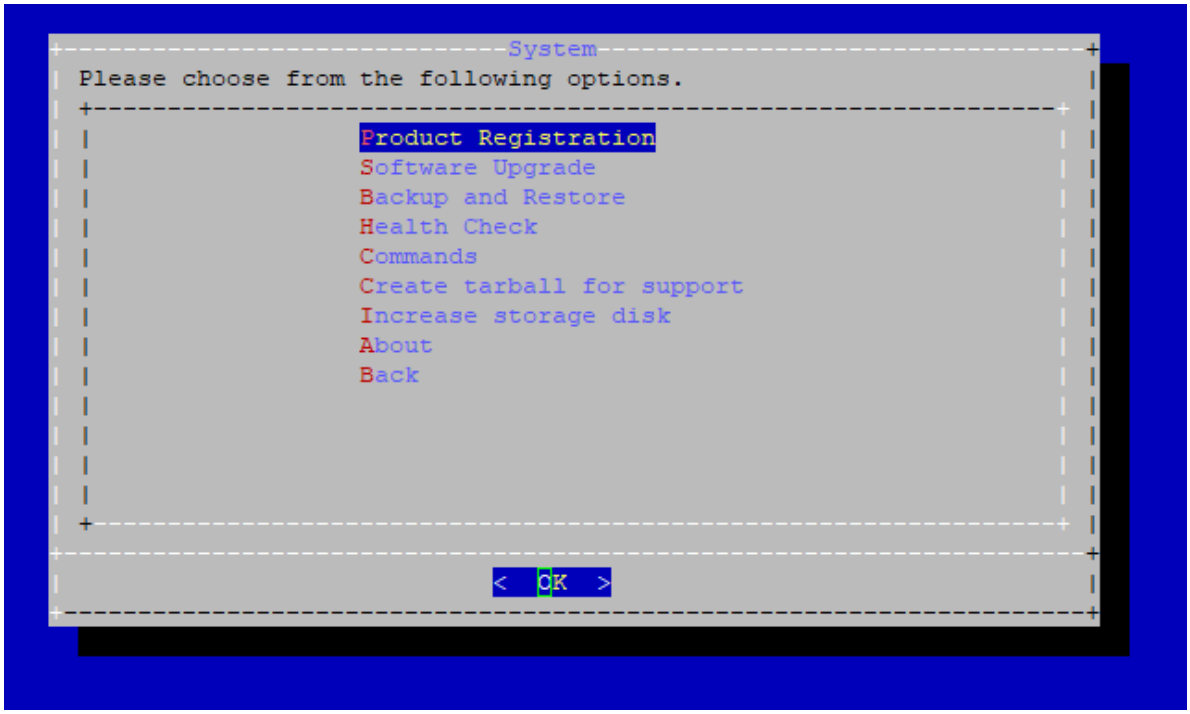
  b. Use the direct link - for automated download mechanisms:
     i. http://www.layerxtech.com/downloads/ds9/updates/layerX-lxtds9-hawaii-sp1-sp22.1.lxsp

     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.

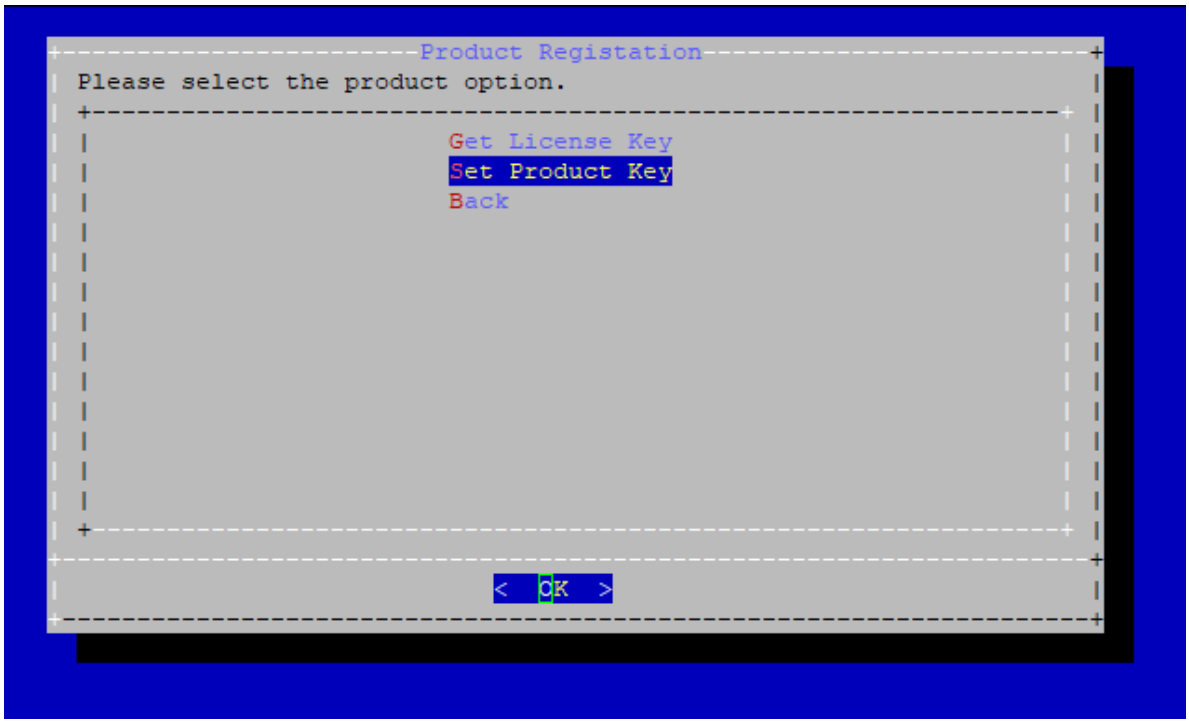
4. VOSS Insights DS9 for NetFlow Product Registration

1. Connect to the DS9 server using an SSH client on port 22 and login using the `admin` credentials to access the **Administration** menu.
2. Select the **System > Product Registration** menu.





3. Select the **Set Product Key** option to input the Product Key.



4. Paste the Product Key into the interface and hit <Enter> to update the licensing expiration on the DS9 Netflow server.
5. Once returned back to the **Product Registration** menu, select **Back** to navigate back to the **Administration** menu then select **Quit** to exit the interface and close the SSH session.

5. VOSS Insights DS9 for NetFlow Base Environment Installation

5.1. VOSS Insights DS9 Standalone Installation

VOSS Insights DS9 is a standalone single server to collect, process and store NetFlow-v5/v9/v10 and SNMP data. Visualization of the data will be handled via the VOSS Insights Dashboard reporting.

5.1.1. Assumptions

- Host machines will be located within the same sub-network
- All the required TCP/UDP ports are open between DS9, Dashboard and NetFlow sources.
  - TCP: 5432 - 8082
  - UDP Depending on desired vflow: 2055 - 9996 - 4739 There is no redundancy requirement for any of the components
- Internet access is available to the DS9 system during installation.

  After the installation, no internet access is necessary.
- Customer premises equipment is sending NetFlow data to Collector successfully Collector can access customer premises equipment via SNMP v1/2/3 successfully

5.1.2. Installation

Items that will be needed during configuration:

1. Hostname
2. Dashboard Reporter IP
3. For each NetFlow device added:
   - IP of device interface sending NetFlow to the DS9
   - NetFlow version
   - SNMP version
     - v1 or v2c - community string

  - v3 - user name, user password, and encryption key
- NAT IP address (often same as IP)

6. Preparing a Production Environment for VOSS NetFlow Solution

6.1. Abstract

This guide is an overview of all the action items that need to be completed by system administrators before implementation of a successful deployment.

6.2. Checklist

The following action items need to be completed by system administrators before the implementation starts:

ID	Action	Description	Criticality
1	Hardware specifications	The hardware/VM specifications have to meet the requirements defined by VOSS	Critical
2	Software specifications	VOSS Dashboard server is delivered as an OVA which includes an operating system. If this is a VM deployment, the following should be available in customer's VM datastore: • Latest OVAs. (Available at VOSS Customer Portal. Log in and select DOWNLOADS.)	Critical
3	Firewall rules	All the required traffic rules are applied to customer environment based on the firewall matrix provided by VOSS deployment Team.	Critical
4	Internet access	Internet access is enabled for the DS9 during implementation. Once the implementation is over, internet access is no longer required.	Critical
5	Round trip times (RTT)	RTT time between the DS9 and Dashboard Server is not more than 100msec.	Critical
6	NetFlow configuration	NetFlow sources are configured to send their NetFlow data to VOSS DS9 Servers based on the suggested settings by VOSS	Critical
7	SNMP configuration	NetFlow sources are configured with SNMP v1 or 2c or v3.	Critical
8	NetFlow and SNMP details	Following information is provided to VOSS deployment team: • Device IP & Hostname and NetFlow version for the NetFlow source(s) • SNMP details for NetFlow source(s)	Critical
9	Remote access	Some method of remote access is enabled for VOSS deployment team.	Critical
10	Integration to customer environment	Both DS9 and Dashboard Servers have access to customers data infrastructure for the following services: NTP, SMTP, DNS.	Critical
11	Authentication via existing customer resources	Dashboard Servers have access to customers' existing Active Directory/Identity servers to authenticate users via LDAP or SAMLv2.	Optional

6.3. Requirements

The following list of items needs to be provided to VOSS before the deployment:

ID	Action	Description	Criticality
1	IP Addresses for VOSS components	IP addresses & Subnetmasks & Default IP Gateway settings for all the VOSS Host Machines (DS9, Dashboard Servers).	Critical
2	IP Addresses for Data services	IP addresses for the following services: DNS, NTP, SMTP, LDAP/SAMLv2.	Critical
3	Remote access details	VPN access details for VOSS Team to access the DS9 and Dashboard remotely.	Critical
4	Primary and Secondary contact details	Primary and secondary contact details for technical and project management related items.	Critical
5	Email authentication for scheduled reports	SMTP authentication details for smart host servers.	Optional
6	SNMP community strings, versions and other details	SNMP community strings and protocol versions need to be provided to VOSS for successful SNMP queries.	Critical
7	List of NetFlow Sources	Provide VOSS a list of NetFlow sources (routers, switches) with the following details: IP addresses, Make/Model, Software Version, NetFlow version.	Critical
8	List of IP addresses and Hostnames	A CSV or Excel file that maps certain IP addresses to internal hostnames can help VOSS Team to improve the data visualization experience by mapping IP address fields to hostnames.	Optional

7. DS-9 NetFlow VM Sizing Specifications

VOSS Insights DS9 for NetFlow sizing specifications are divided into small, medium and large solutions based on tiers related to the number of flows that need to be supported.

Each solution below includes the VM specifications for both the VOSS Insights DS9 server and the VOSS Insights Dashboard server.

7.1. Small NetFlow Solution

The three small tiers in Flows per Second:

- 1,000
- 5,000
- 10,000

Dashboard Server VM			**DS9 NetFlow Collector VM**	
Cores	12		Cores	16
Memory GB	32		Memory	64
Disc Storage GB	500		Disc 1 OS in GB	250
SSD provisioned as Thick Eager Zero			Disc 2 Storage in GB	500
			All Discs must be SSDs and Provisioned as Thick Eager Zero	

7.2. Medium NetFlow Solution

Two medium tiers in Flows per Second:

- > 10,000 but <= 25,000
- > 25,000 but <= 50,000

Dashboard Server VM			**DS9 NetFlow Collector Bare Metal Server (Dell R740 or Equivalent)**	
Cores	16		Cores	16
			CPU Needs to be Intel Gold or better.	
Memory GB	64		Memory	196
Disc Storage GB	500		Disc 1 OS in GB	250
SSD provisioned as Thick Eager Zero			Disc 2 Storage in TB	1,5
			Read Intensive SSDs required	
			Dual Intel 10GB NIC	1
			Intel Quad 1GB NIC	1
			iDRAC Enterprise or Equivalent	
			Dual Power Supplies	

7.3. Large NetFlow Solution

Two large tiers in Flows per Second:

- > 50,000 but <= 100,000
- > 100,000 but <= 200,000

Note: The DS9 Collector requires a minimum of 2 Bare Metal Servers to collect this volume in one location.

Dashboard Server VM			**DS9 NetFlow Collector Bare Metal Server 1 (Dell R740 or Equivalent)**	
Cores	16		Cores CPU Needs to be Intel Gold or better.	16
Memory GB	64		Memory	196
Disc Storage GB	500		Disc 1 OS in GB	250
SSD provisioned as Thick Eager Zero			Disc 2 Storage in TB	3
			Read Intensive SSDs required	
			Dual Intel 10GB NIC	1
			Intel Quad 1GB NIC	1
			iDRAC Enterprise or Equivalent Dual Power Supplies	
			Dual Power Supplies	

		Bare Metal Server 2 (Dell R740 or Equivalent)	
		Cores CPU Needs to be Intel Gold or better.	16
		Memory	196
		Disc 1 Storage in TB	3
		Disc 2 Storage in TB	3
		Disc 3 Storage in TB	3
		Read Intensive SSDs required	
		Dual Intel 10GB NIC	1
		Intel Quad 1GB NIC	1
		iDRAC Enterprise or Equivalent Dual Power Supplies	
		Dual Power Supplies	

Note:

- Larger than 200K flows per second requires special pricing and configuration.
- Distributed DS9 collection is available. This may reduce the compute required at each collection location.

8. NetFlow and DS9 Monitoring System Connectivity

8.1. 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

8.2. 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)

8.3. 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

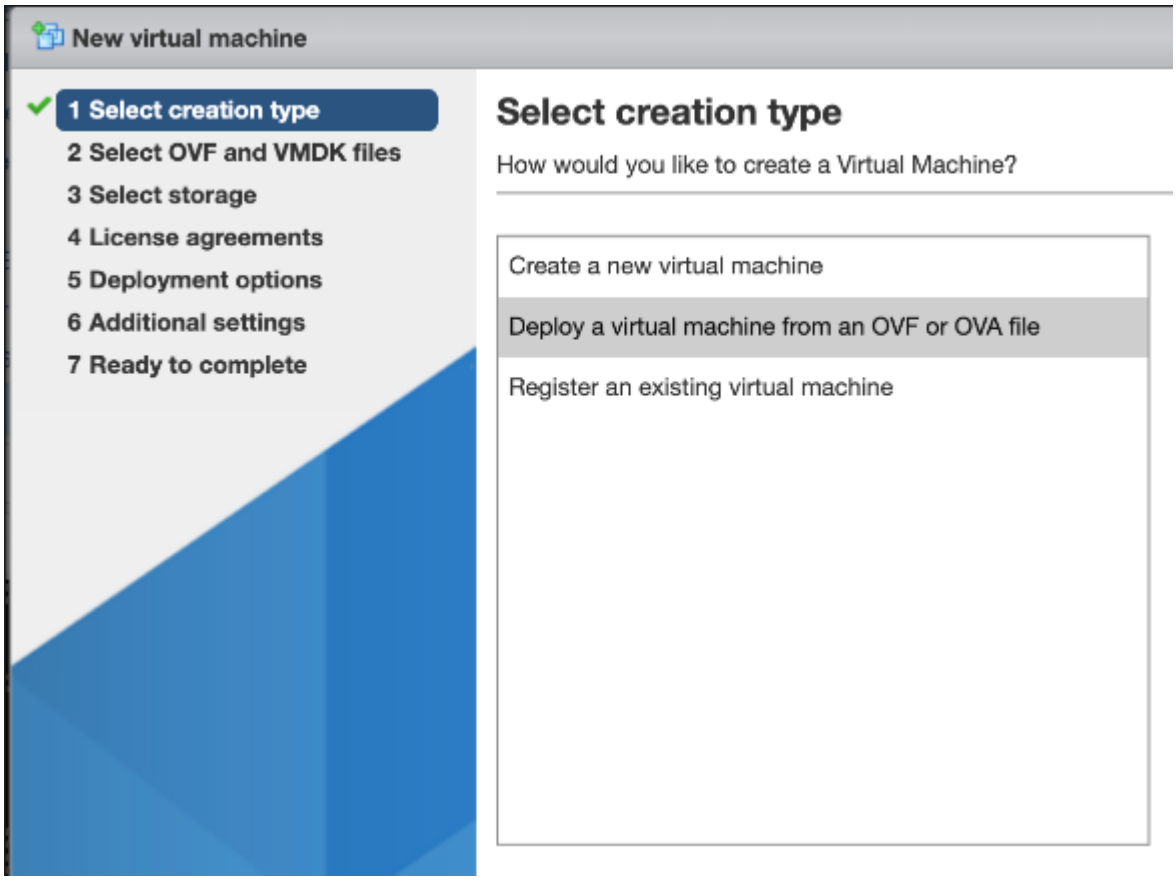
8.4. Communication ports that are required for remote management purposes

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

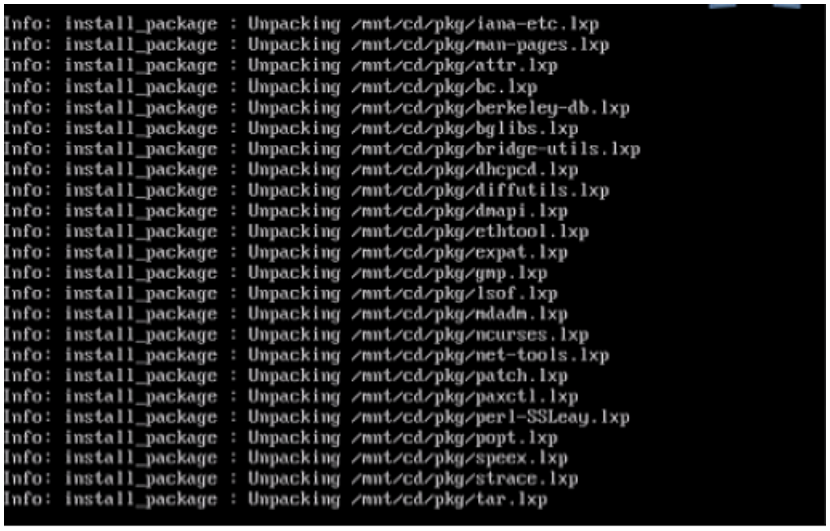
9. Deploy and VM Installation Steps

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

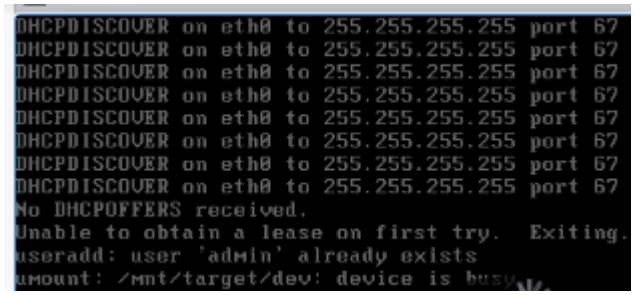
   Select the downloaded OVA file and choose a VM name.



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:

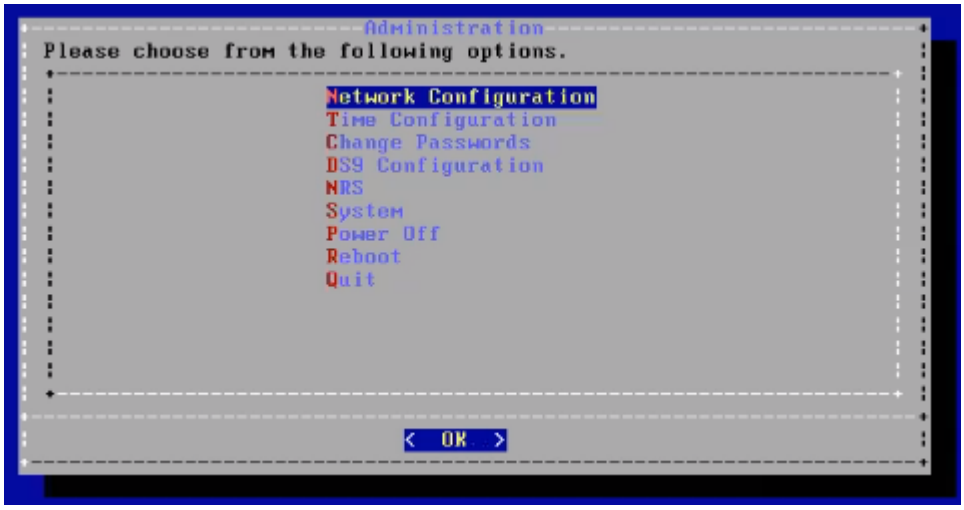
```
                    About
================================================
      Hostname:  <hostname>
       Version:  <version>
         Theme:  <theme>
        Flavor:
       License:  NNNNN-NNNNN-NNNNN-NNNNN-NNNNN
 Days Licensed:  nnnnn
Days Remaining:  nnnnn
   Product Key:
       Website:  <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.

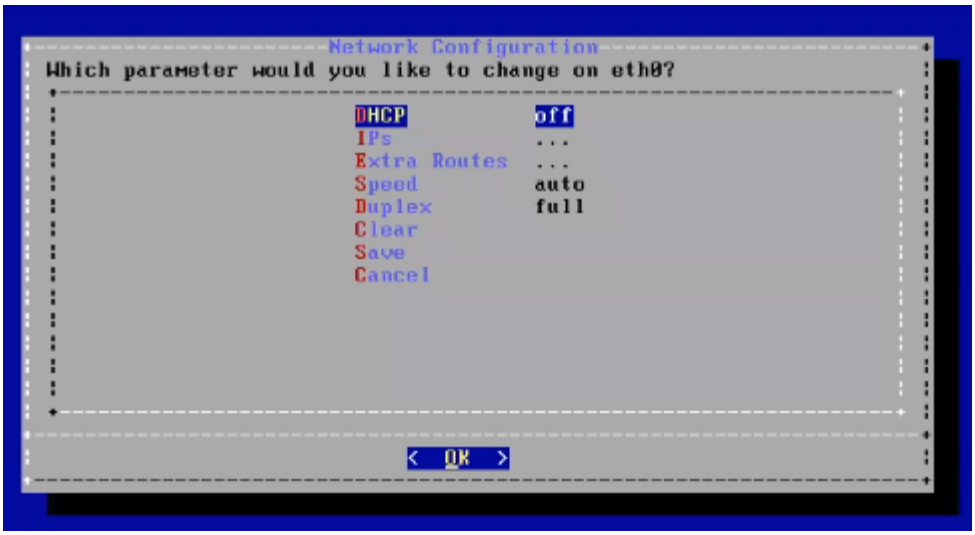
9. After login, the **Administration** menu shows, as in the example below for DS9:



10. Under **Network Configuration**, provide ip/netmask, default gateway and hostname.
    a. Under **Interface Settings**, select the interface to configure.

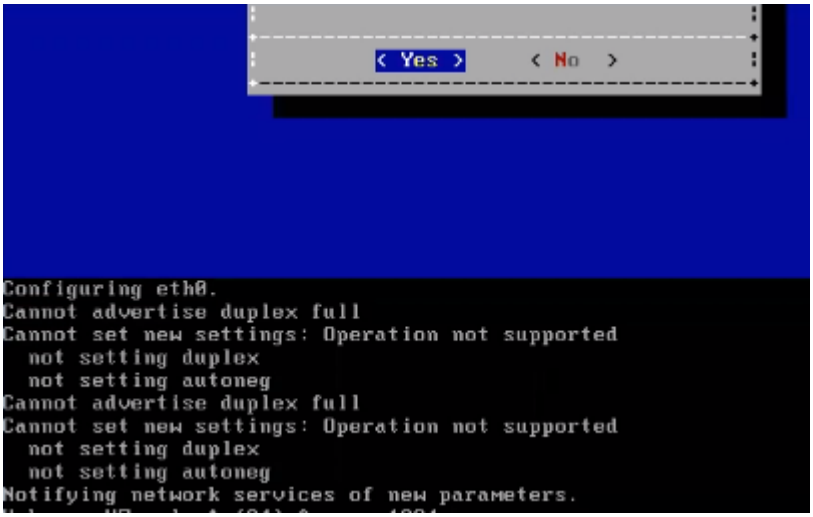
    Select **IPs** and set the IP Address and netmask in the format `nn.nn.nn.nn/24` and save.

    Modify the parameters for the selected interface:

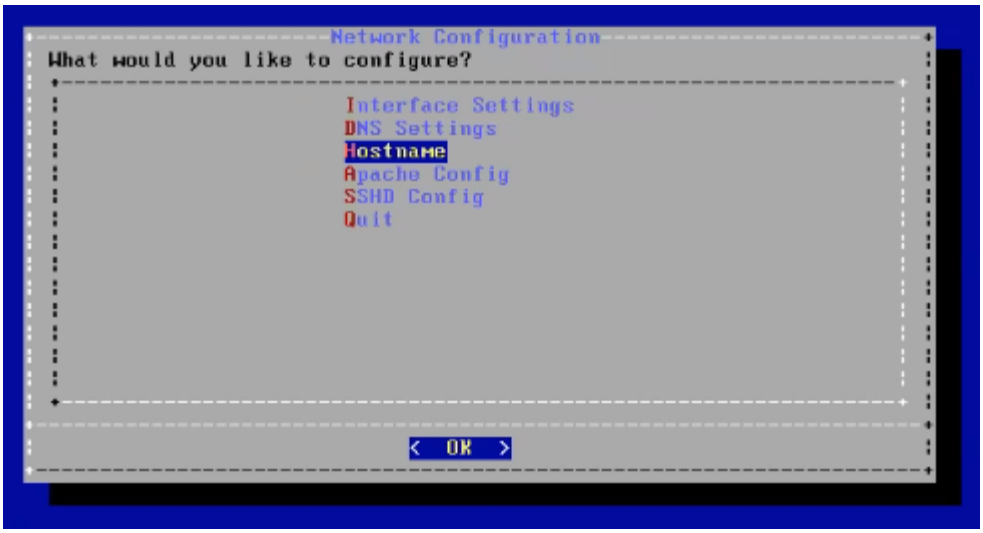


Set up the default gateway under the **Extra Routes** menu.

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.

9.1. 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.

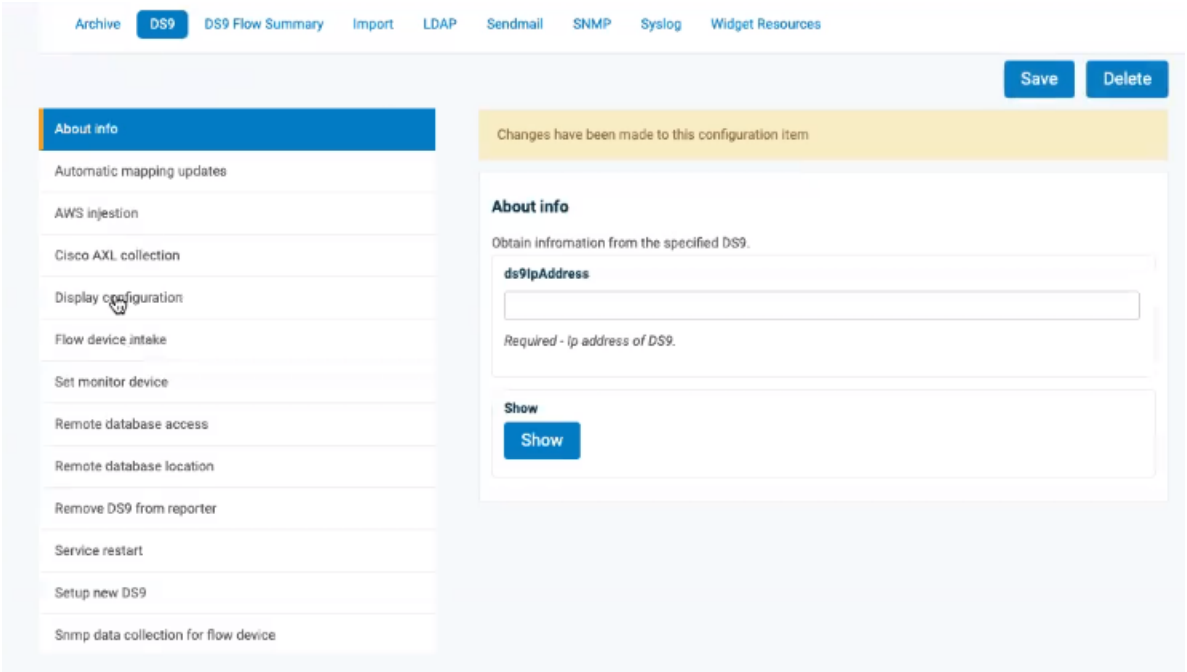
For CUCM v11.5 support:

```
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
```

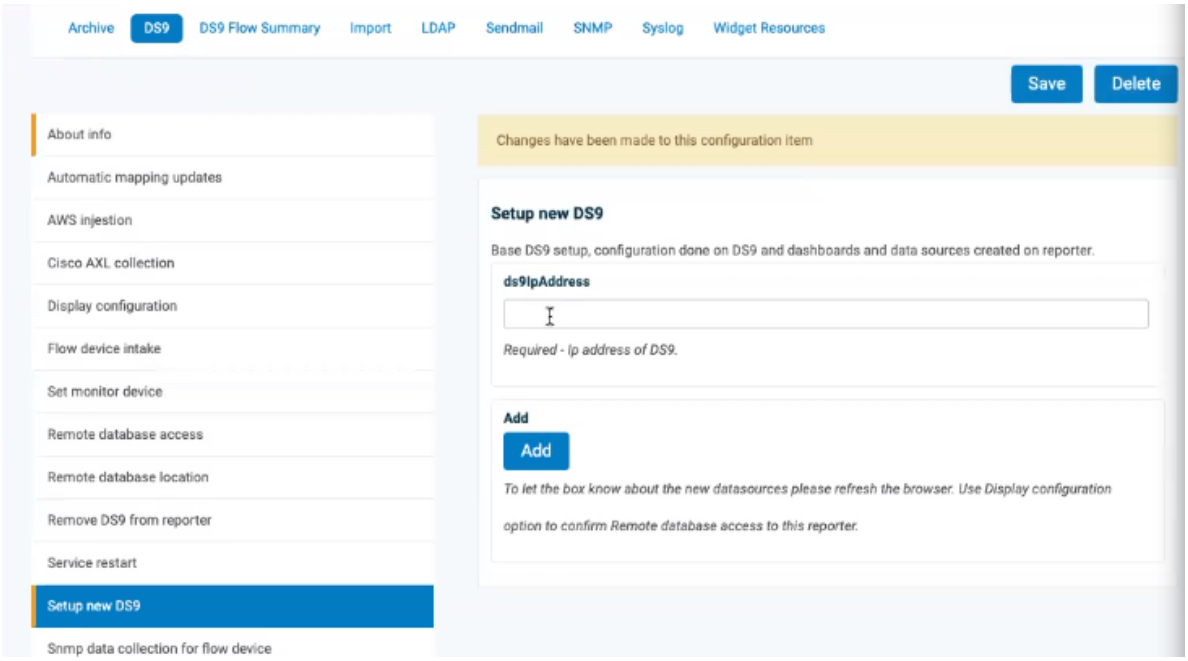
10. DS9 Configuration on the Dashboard

To complete the configuration between the Insights Dashboard Reporter and DS9, flow devices and SNMP configuration can be carried out:

1. Log in on the Dashboard GUI as admin, then go to **admin > Configuration**. On the **Configuration Settings** page, select the **DS9** tab.



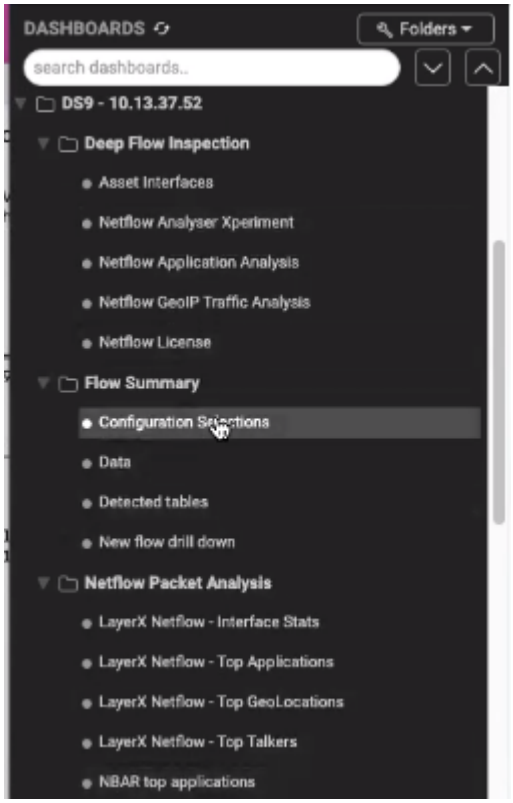
2. Choose **Setup new DS9**, add the **ds9IpAddress**, then click **Add**. Repeat this step according to the number of DS9 systems to be utilized in the environment.



3. Refresh the Dashboard browser page and from the menu, select **Data Sources**.

   The new entries for the IP address are listed as `DS9 SNMP...`, `DS9 SUMMARY...` `DS9 TOPN...` entries.

4. Under the **DASHBOARDS** menu, the new **DS9 - <IP>** dashboard menu shows, for example:

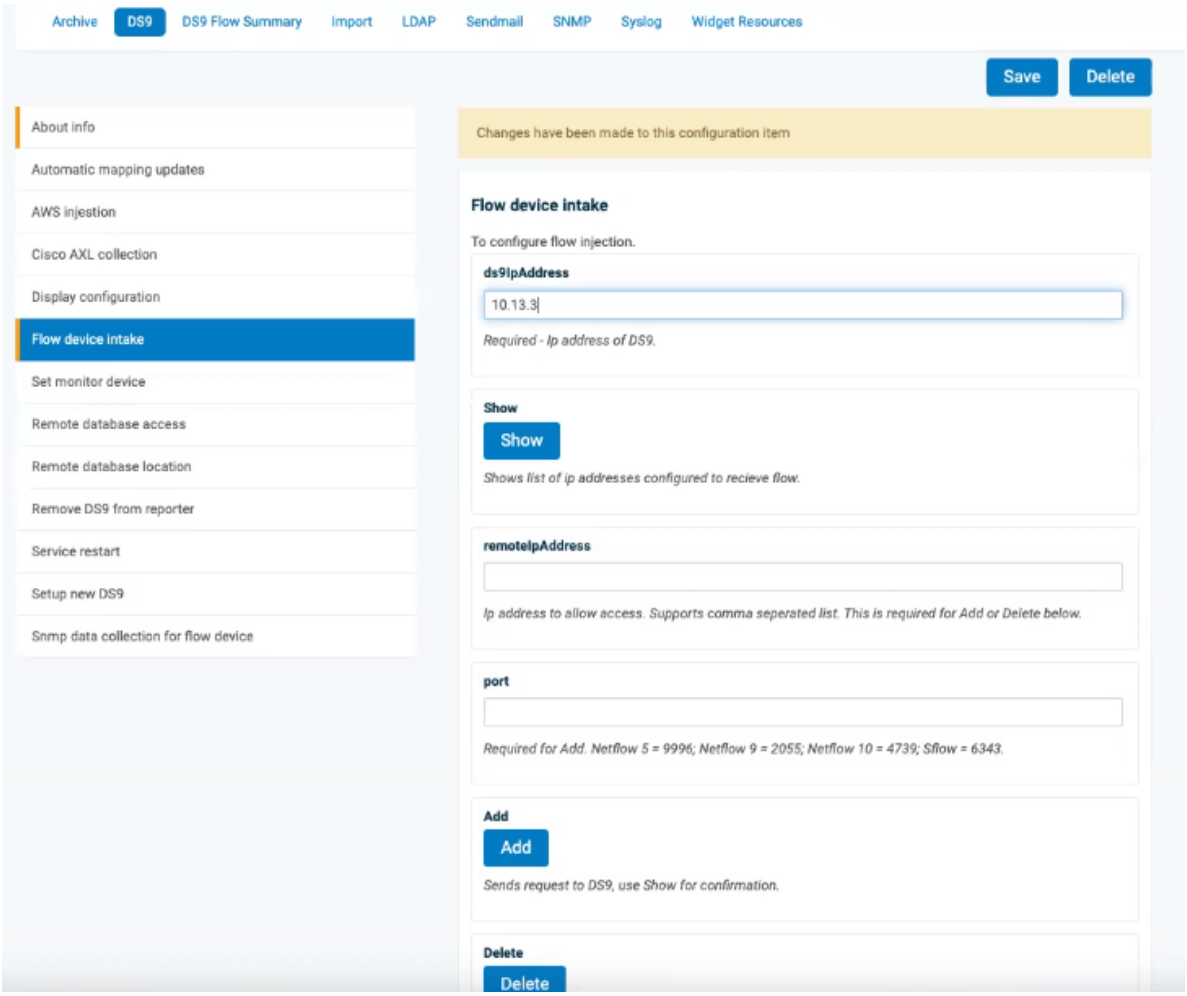


   Note at this stage the sub-menus are still empty.

5. Set up the DS9 to receive netflow from the source devices sending to the DS9. Go to **admin >**

Configuration and on the **Configuration Settings** page, select the **DS9** tab.

6. Choose **Flow device intake** and for each remote netflow device that the DS9 server will receive flow data, set up **ds9IpAddress**, **remoteIpaddress** and **port** and click **Add**.



7. NetFlow source device interface utilization statistics that are gathered using SNMP data collection is also required. Choose the **Snmp data collection for flow device** menu, enter data into the fields according to your SNMP version configuration preferences, then click **Add**.

   Repeat this step for each of the flow sources set up to send flow to the DS9.

   Specify the same IP address of the NetFlow source to be queried in the **deviceIpAddress** field and the **snmpIpAddr** field if NAT is not being used to connect to the NetFlow source device from the DS9 system.

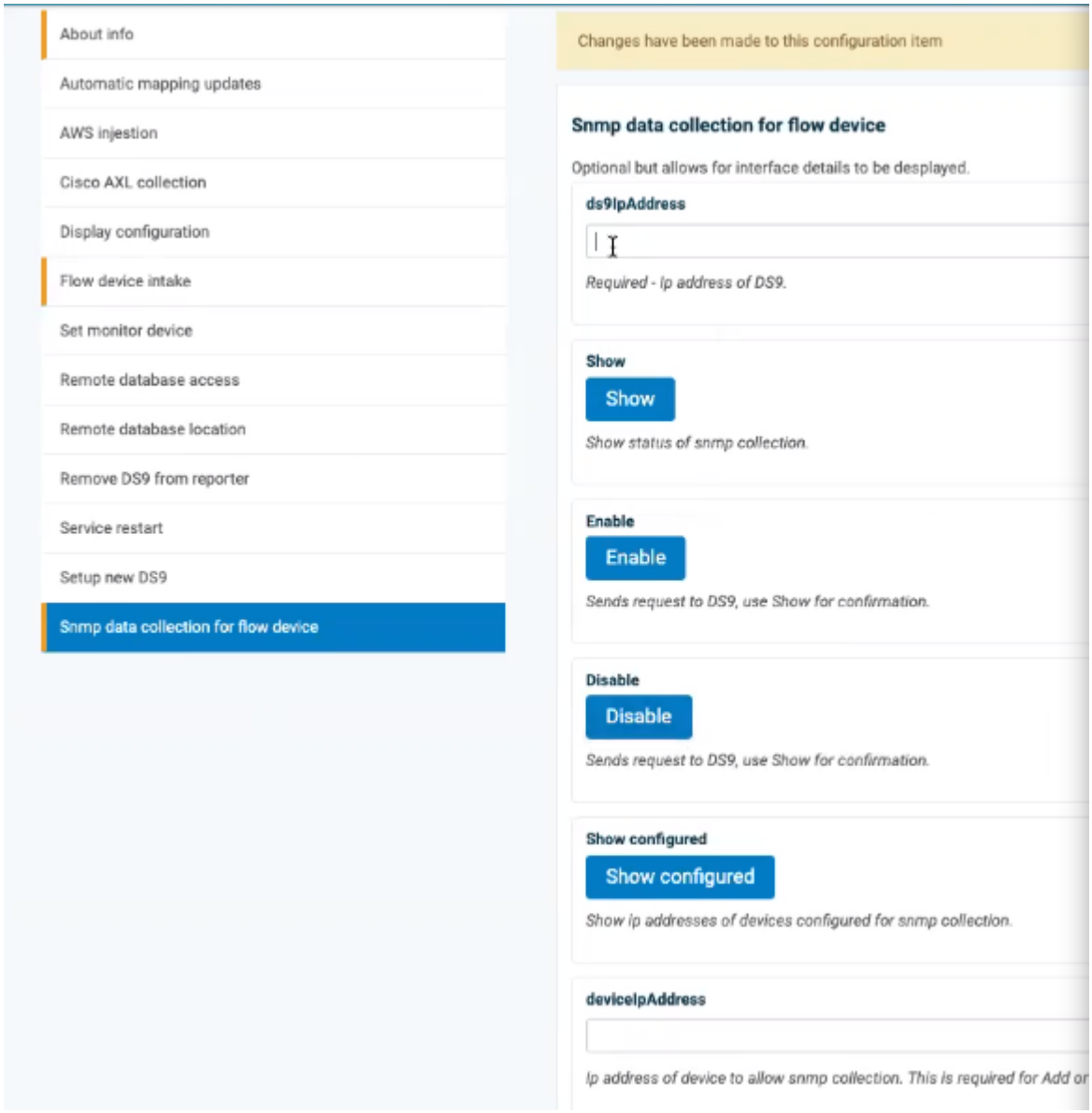
   If NAT is used to connect to the NetFlow source device, specify the NAT IP address of the NetFlow source device in the **snmpIpAddr** field to use as the Ip address to connect to the system for the SNMP query.

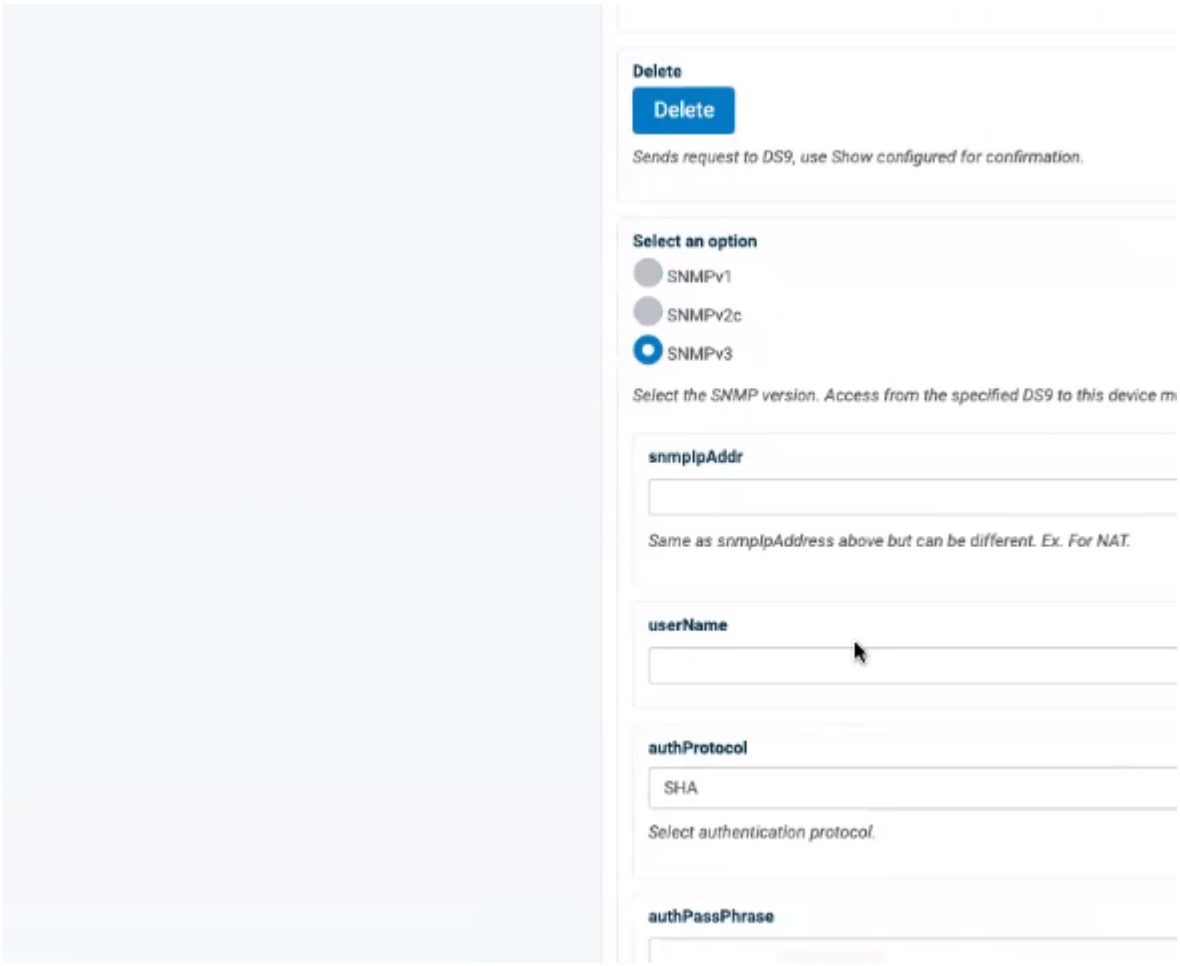
   Input the real IP address of the system into the **deviceIpAddress** field and then input the SNMP authentication parameters.

   Click the **Add** button when complete.

   Repeat for each NetFlow source device to be queried. The authentication parameters will cache in the browser so only changing the **deviceIpAddress** and **snmpIpAddr** fields is usually required for a new

entry.





Index

F