VOSS Insights
DS9 for Netflow Install Guide

Release 25.3

December 04, 2025

Legal Information

DOCUMENT ID: 20251204064447

Contents

1. What's New

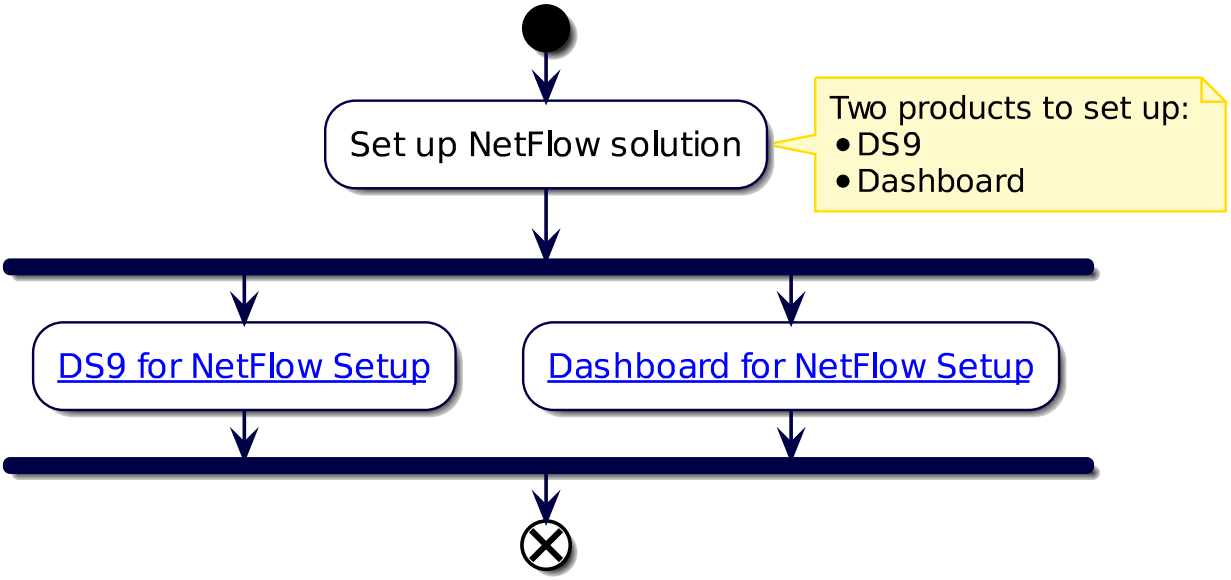
1.1. DS9 for Netflow Install Guide: Release 25.3

- VOSS-1563: Support across the product suite for alternative virtualization/hypervisor solution for on-prem deployments. See: *Supported virtualization and hypervisor platforms*

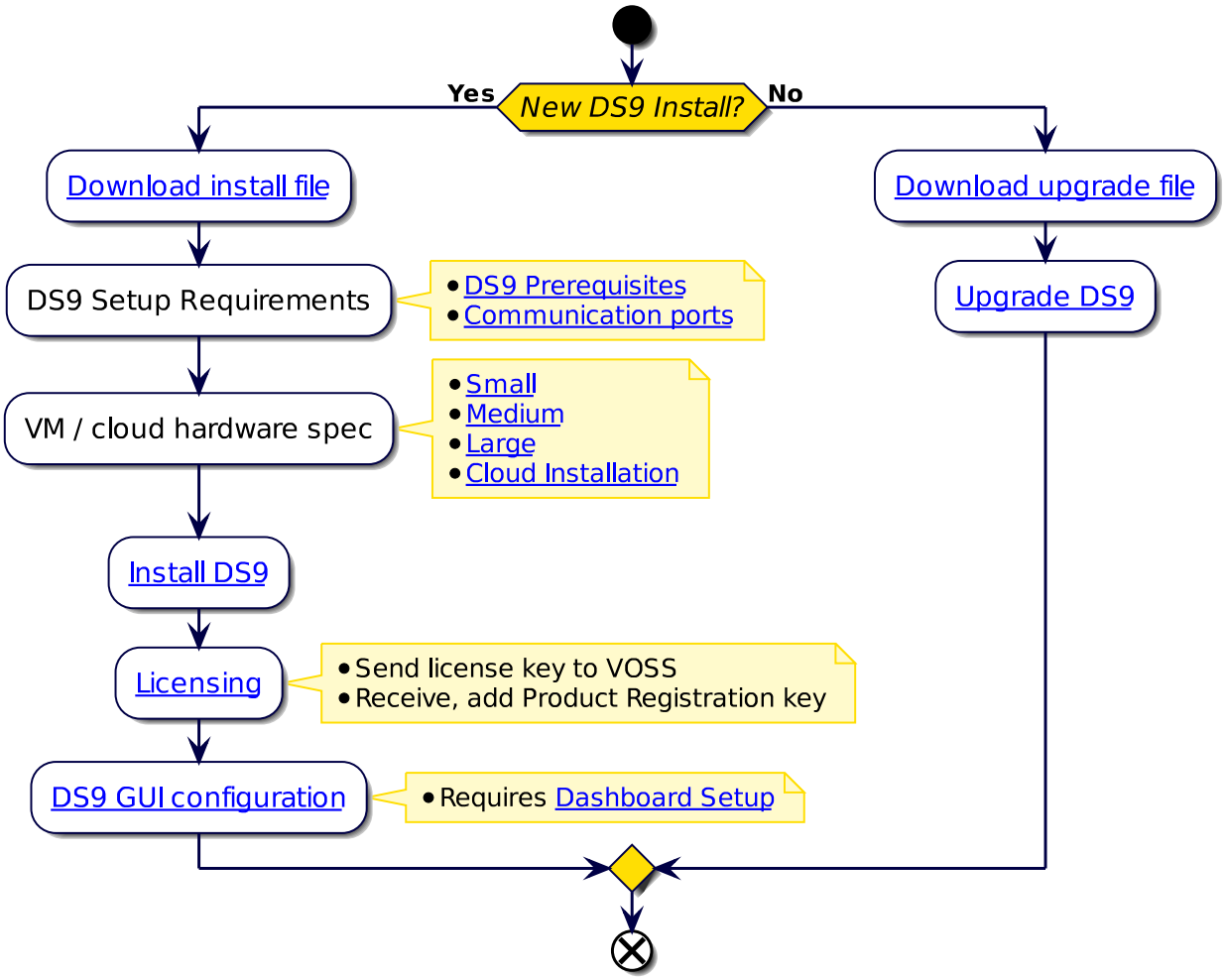
  Added details on the new virtual machine platform support in Automate: Hyper-V and Nutanix

2. NetFlow Quickstart

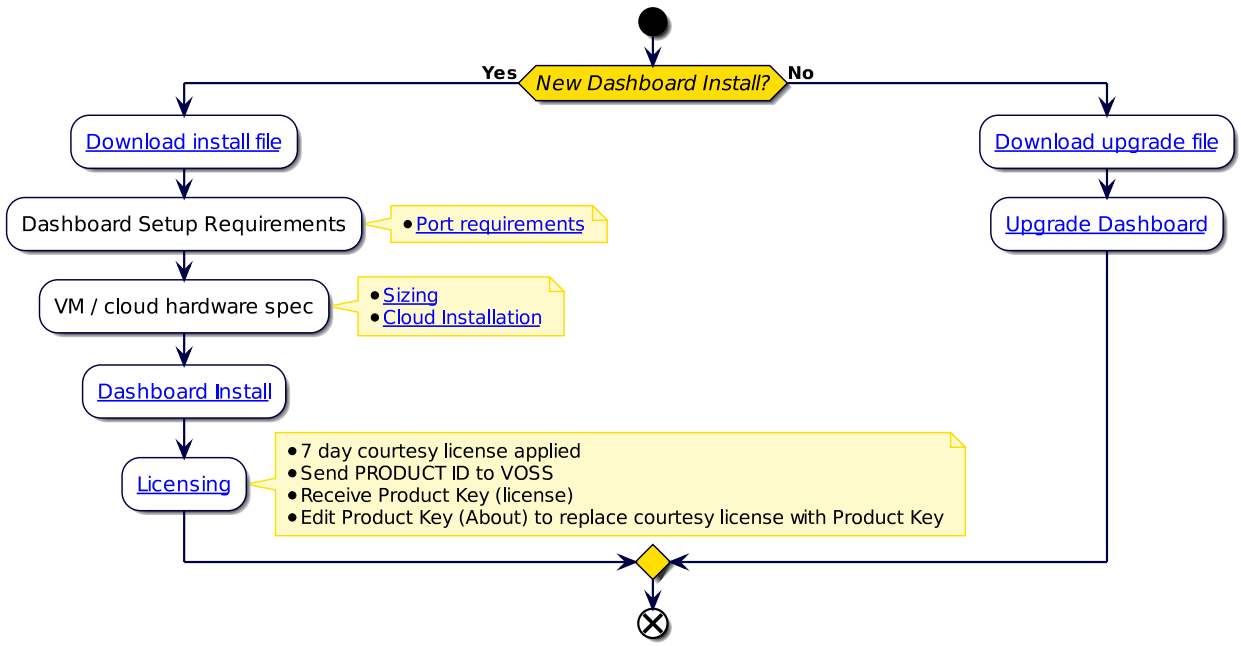
2.1. NetFlow Setup Overview



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 for Netflow: Infrastructure prep and installation parameters

3.1. Overview

This section describes the system requirements, network conditions, and required parameters for an Insights DS9 standalone installation.

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 Insights Dashboard reporting.

3.2. System requirements and network conditions

Before starting this deployment, ensure that the following infrastructure conditions and connectivity requirements are in place:

- Host machines will be located within the same sub-network
- All 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.

3.3. Parameters required for setup

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)

4. Prepare a production environment for Netflow

4.1. Overview

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

4.2. Environment setup

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

4.3. Required deployment details

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

5. DS-9 Netflow VM sizing specifications

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 Insights DS9 server and the Insights Dashboard server.

5.1. 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	

5.2. 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	

5.3. 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.

6. Netflow and DS9 monitoring system connectivity

6.1. 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

6.2. 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)

6.3. 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 repository access
Dashboard Server	DS9	TCP	8082	Unidirectional	Data repository access
Dashboard Server	DS9	TCP	443	Unidirectional	DS9 System Stats and management
DS9	Dashboard Server	TCP	443	Unidirectional	DS9 Dynamic Mapping Updates

6.4. 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

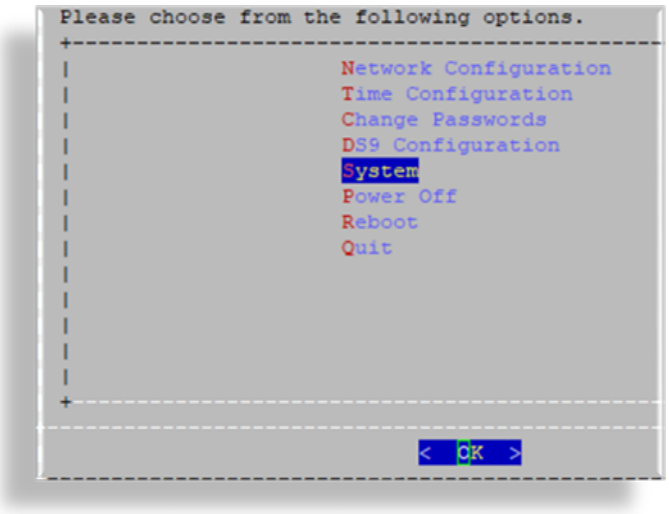
7. Download DS9

- 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:

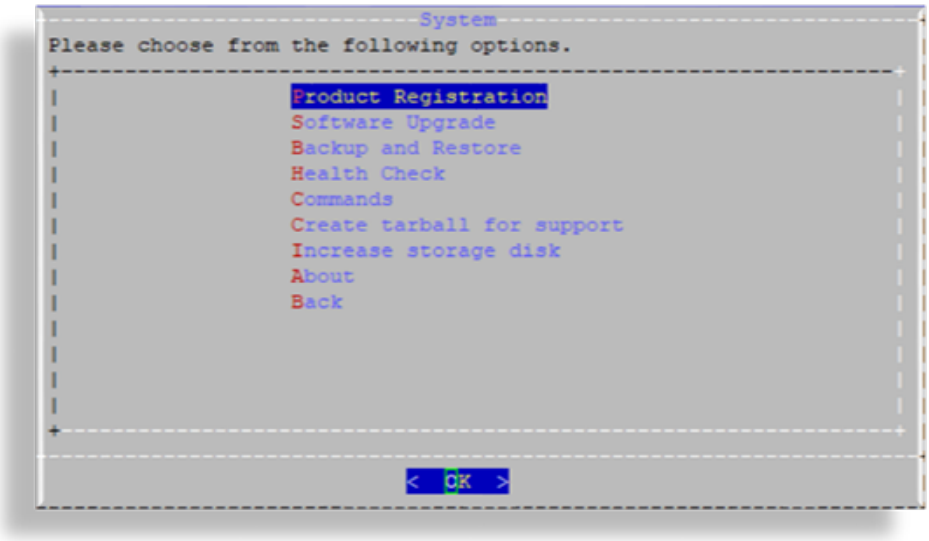
  Log in on the VOSS Customer Portal
  1. Go to **Downloads > VOSS Insights > Insights DS9 Hawaii > <release number> > Upgrade**.
  2. Download the `.lxsp` upgrade file

8. Insights DS9 for Netflow product registration

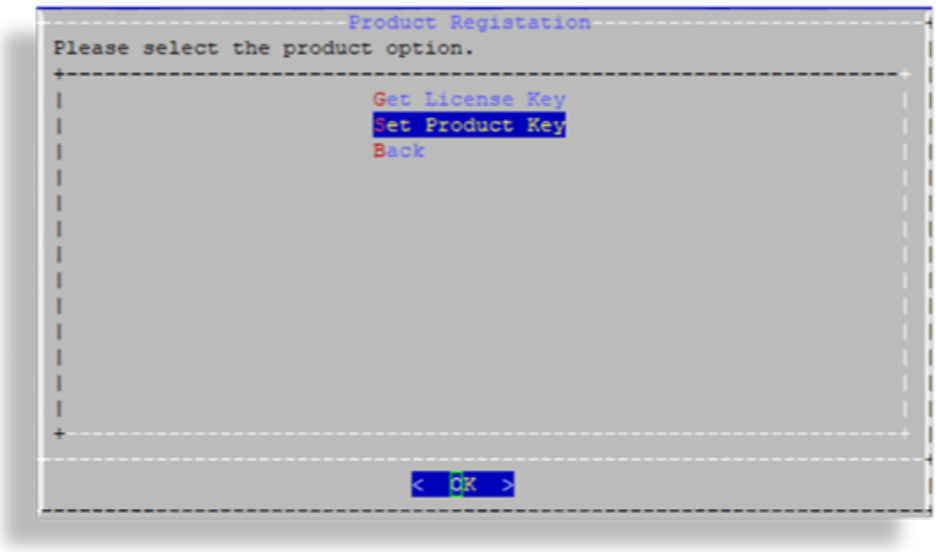
1. Connect to the DS9 server using an SSH client on port 22.
2. Log in using the admin credentials to access the **Administration** menu.
3. Select **System**.



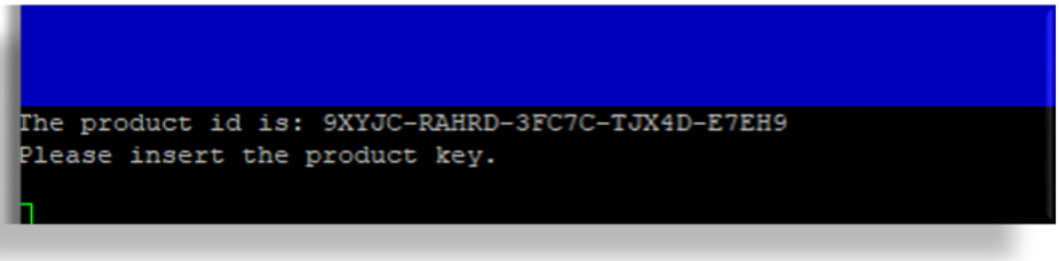
4. Select **Product Registration**.



5. Select **Set Product Key**.



6. Input the product key. Paste the product key into the interface, then press **Enter** to update the licensing expiration on the DS9 Netflow server.



7. Return to the **Product Registration** page, then select **Back** to navigate back to the **Administration** menu. Select **Quit** to exit and close the SSH session.

9. Deploy and VM installation

9.1. Deploy the installation on the VM

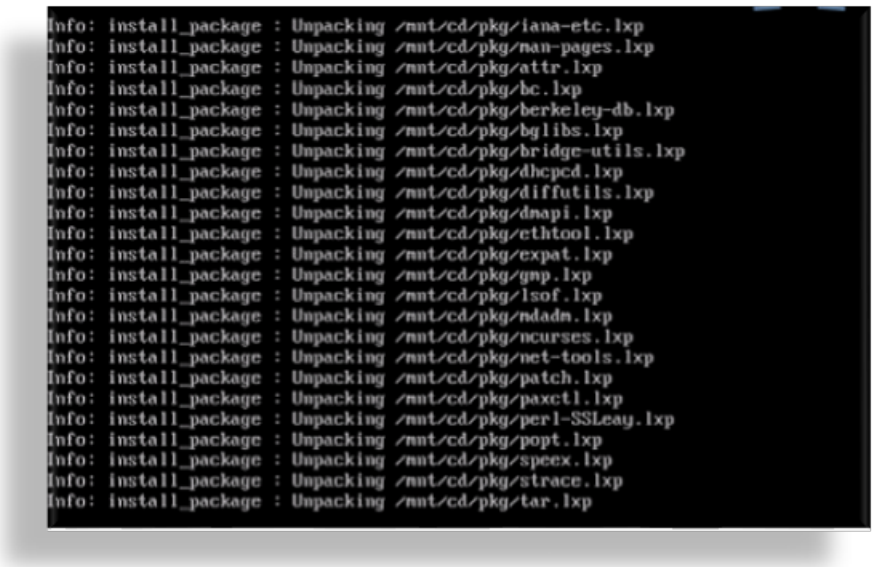
See: *Supported virtualization and hypervisor platforms*

Select virtualization platform:

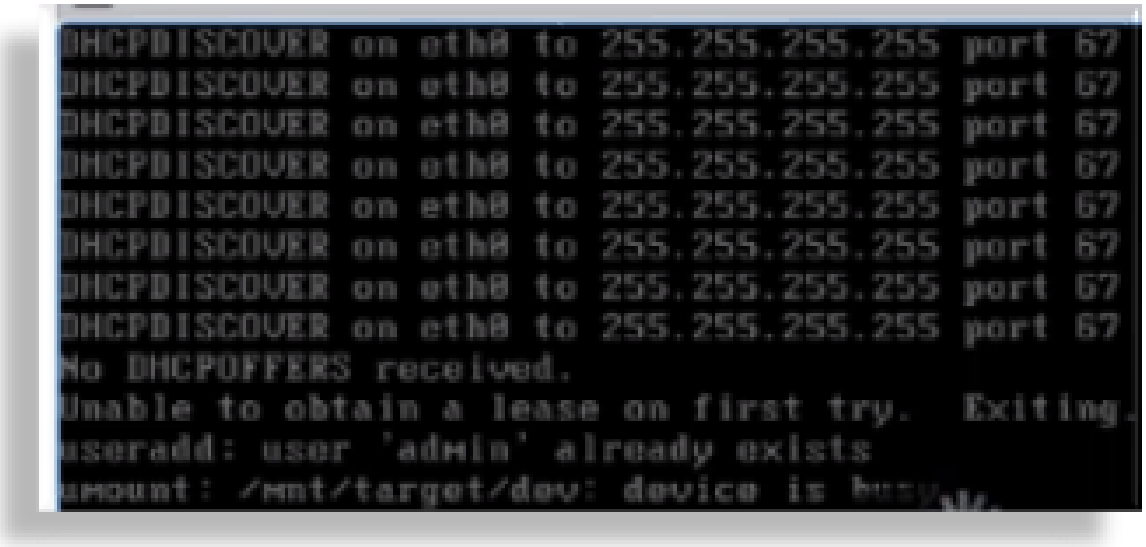
- *VMWare Esxi 8*
- *Hyper-V*
- *Nutanix*

9.2. Run the VM

1. Run the VM, and monitor installation of the packages (this may take some time).



   Once all packages are installed, the VM is automatically powered off, confirmed via the `auto-poweroff` message on the console.



2. The system reboots. Wait until you see the **About** console, which displays placeholder values for hostname, version, license, days licensed and remaining, and so on.

```
                    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:
```

9.3. Log in to the Administration console

Once the system reboots, you'll need to provide admin user credentials to log in.

1. On the **About** console, at **<hostname> login:**, fill out username `admin`.
2. For the password, use the last *10 characters* of the value at **License**, *excluding the dash*.

> **Important:** The **License** key value displays *only* on the **About** console. When you *ssh* in, it is not visible. For this reason, copy the admin password from the **About** console.
>
> For security purposes, it is recommended that you update this admin password prior to configuring the VMs networking address.

3. View the **Administration** menu, which displays once you're logged in.

9.4. Change the admin user password

This procedure updates the admin password that is set during the installation process, using the last 10 digits of your license key.

Note: The admin password will need to be updated for all Insights products you install. For security purposes, it is recommended that you update this admin password prior to configuring the VM networking address.

Once you update the password, it is strongly recommended that you make a written or digital copy of any system passwords and share the copies with trusted team members or store them in a secure location from where they may be retrieved if needed.

---

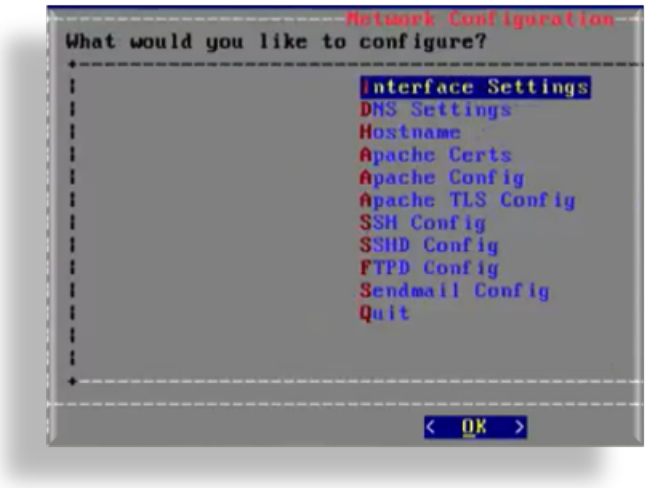
1. On the **Administration** menu, select **Change Passwords**.

2. Select **Change Admin Password**.
3. Fill out a new password.
4. Save your changes.

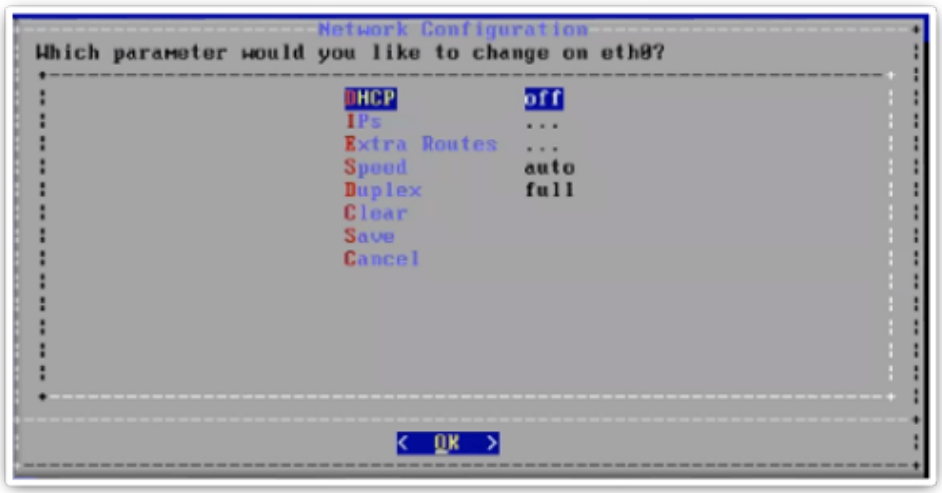
Important: It is strongly recommended that you make a written or digital copy of any system passwords and share the copies with trusted team members or store them in a secure location from where they may be retrieved if needed.

9.5. Configure network settings

1. On the **Administration** menu, select **Network Configuration**.

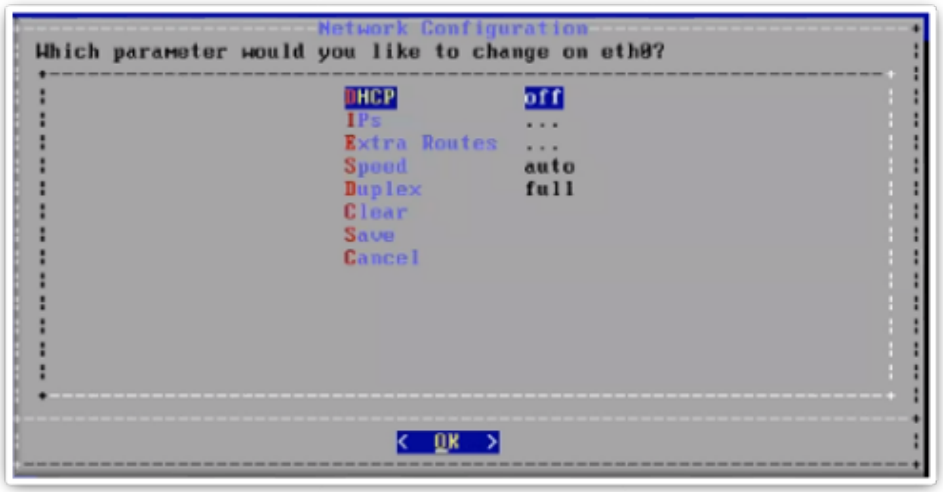


2. Configure interface settings:
    i. Select **Interface Settings**.
    ii. Select the relevant interface.

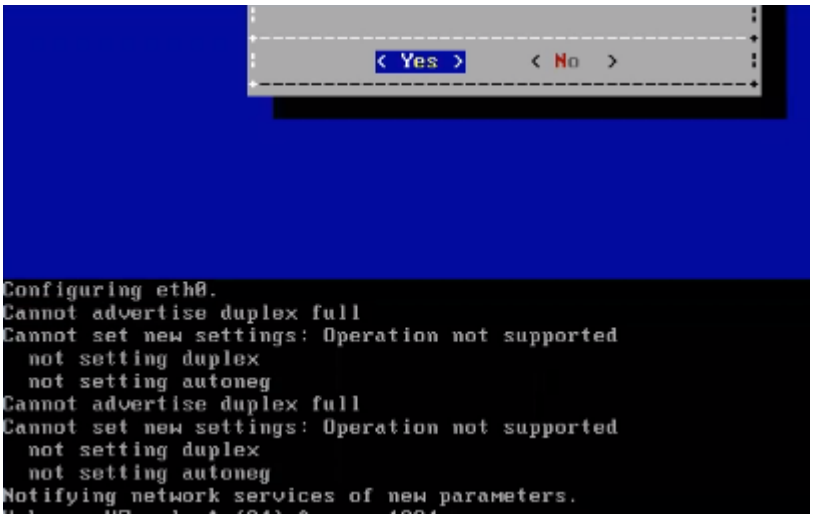


    iii. Select **IPs**. Set the IP address and netmask in the format `nn.nn.nn.nn/24`. Click **OK**.

    iv. Select **Extra Routes** to configure the default gateway.



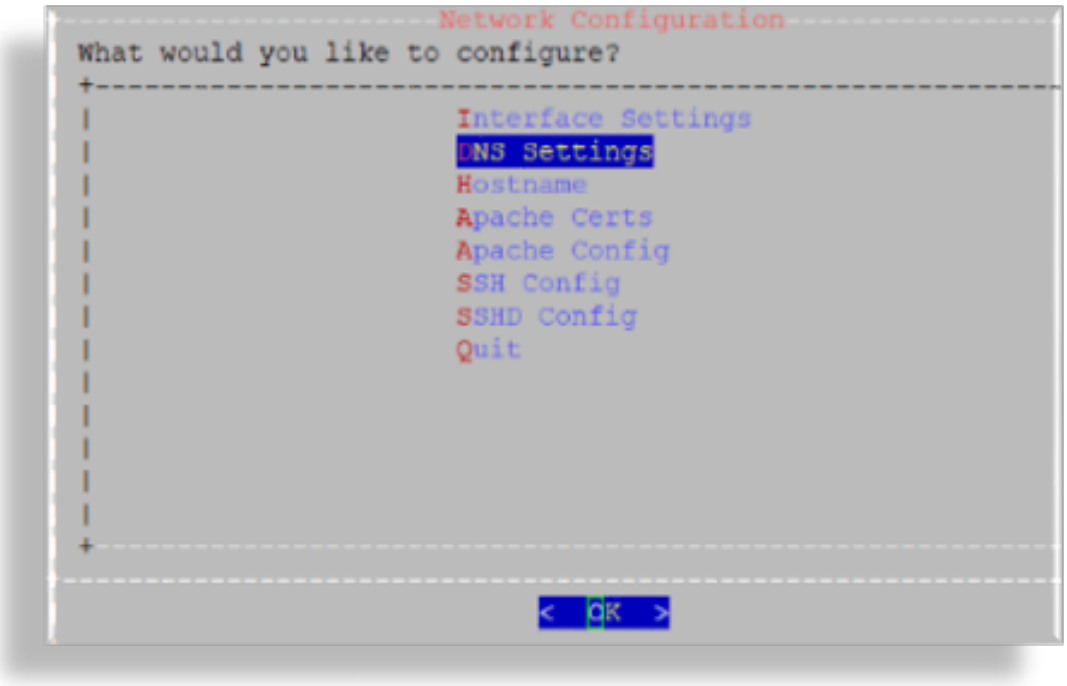
- Use the following format for the entry: *default <gateway IP address>*
- The word *default* is required. For additional route entries use the *<subnet> < gateway>* format. Similar to what would be done on a Linux system at the CLI.



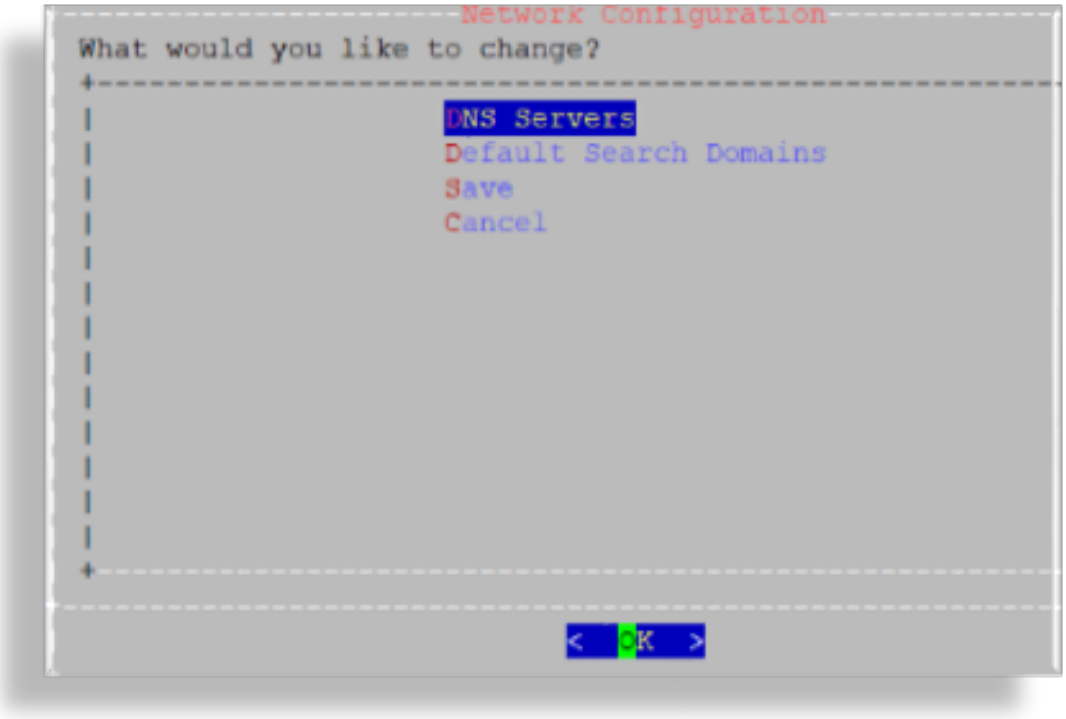
v. Save your changes.

3. Configure DNS settings:

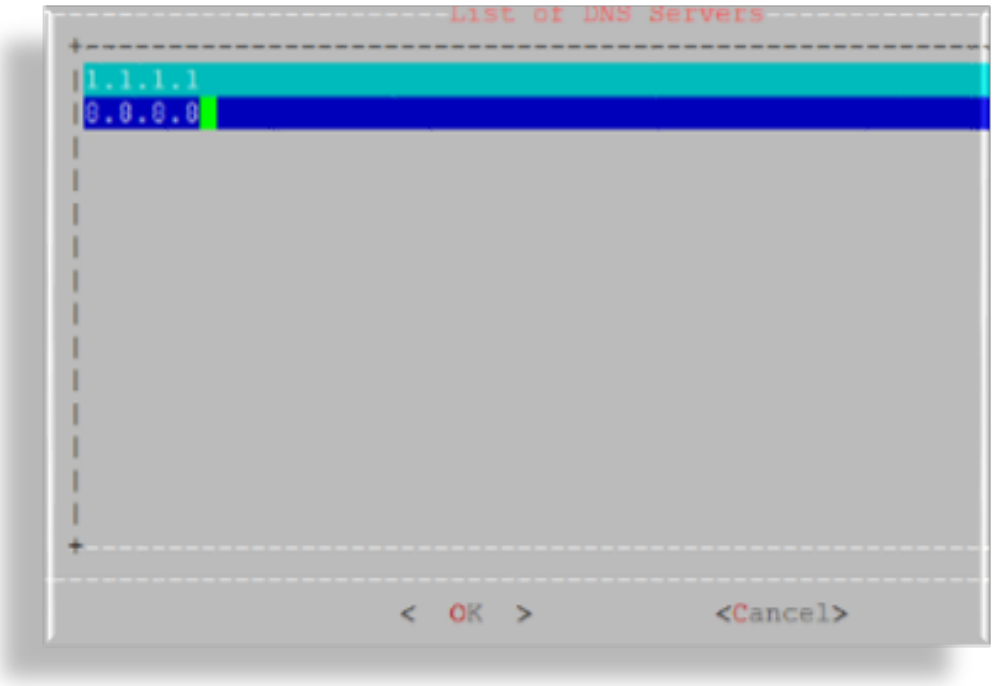
i. Select **DNS Settings**



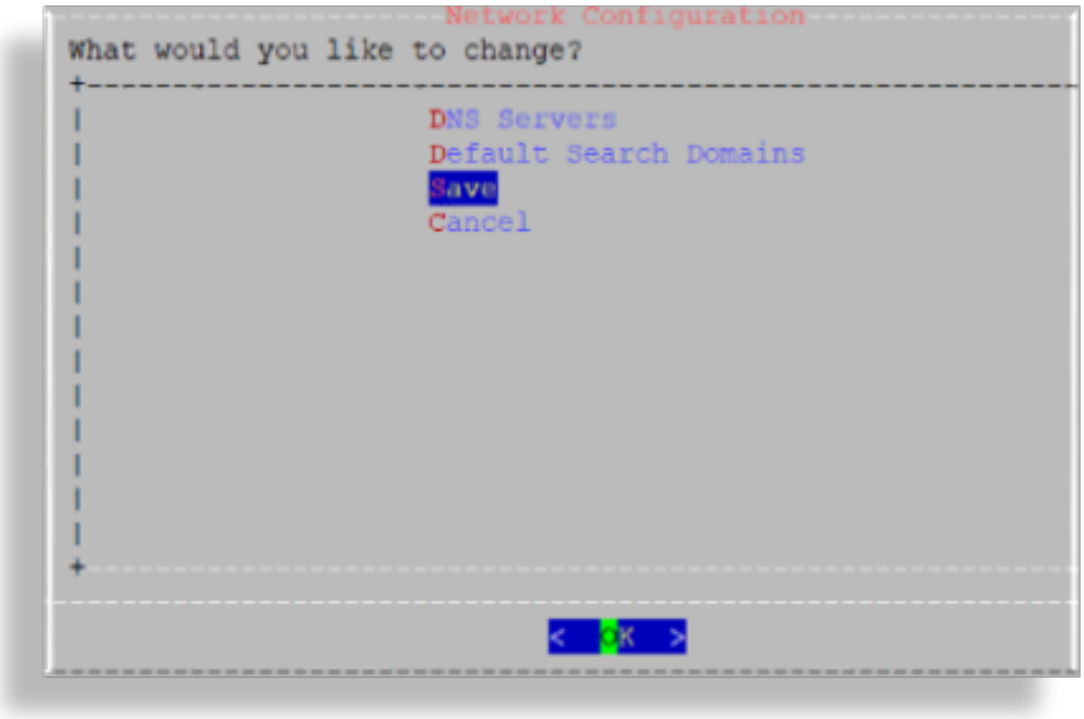
ii. Select **DNS Servers**.



iii. Add the IP address for each DNS server, one per line, then click **OK**.

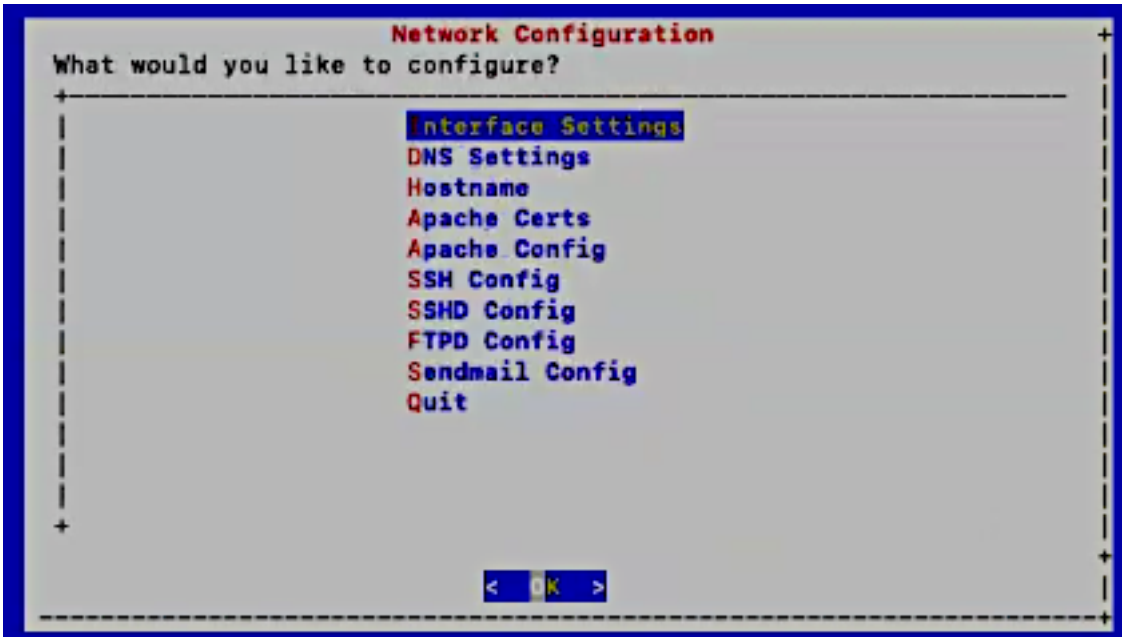


iv. Click **Save**.



4. Configure the hostname:
    i. Select **Hostname**.
    ii. Save to trigger the update.

    The console displays a message, *Updating hosts*. This setup may take a few minutes.



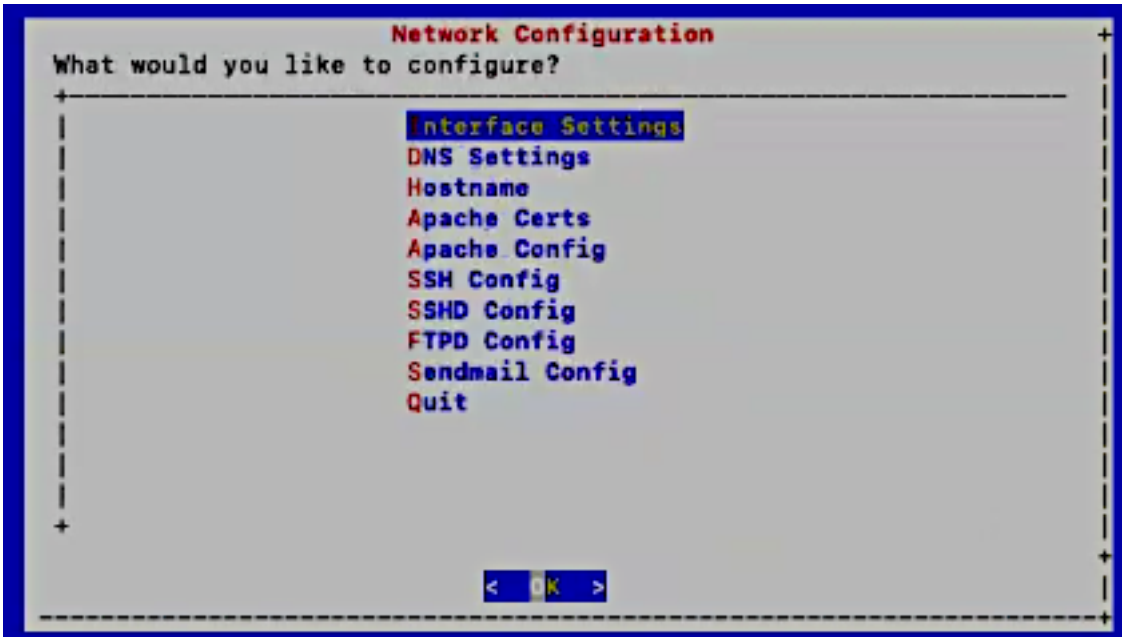
5. Update SSL ciphers.

    i. Select **Apache Config**.

```
SSLCipherSuite HIGH: !MEDIUM: !ADH: !LOW
```

Note:

- `SSLCipherSuite` defaults to `HIGH` encryption.
- For `SSLProtocol`, only TLSv1.2 is supported.
- OpenLDAP defaults to `HIGH` encryption.
- OpenSSH does not support weak ciphers.
- On system upgrade, if the contents of this configuration are no longer valid, then the contents will be will be reset to an empty state.



6. Configure SSH settings:
   i. Select **SSH Config**.

   Custom entries can be added, if required. The following entries have been added:

```
kexalgorithms
diffie-hellman-group14-sha1
diffie-hellman-group-exchange-sha1
hostkeyalgorithms
ssh-rsa
```

   Note: On system upgrade, if the contents of this configuration are no longer valid, the contents will be reset to an empty state.

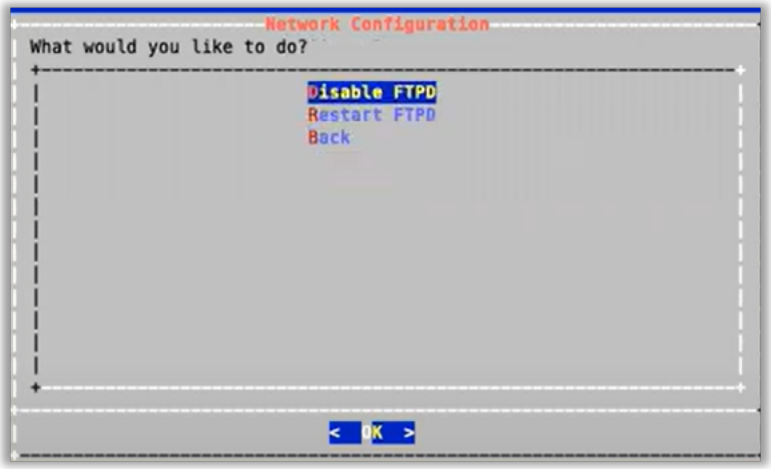
7. Configure SSHD:
   i. Select **SSHD Config**.

   Note:

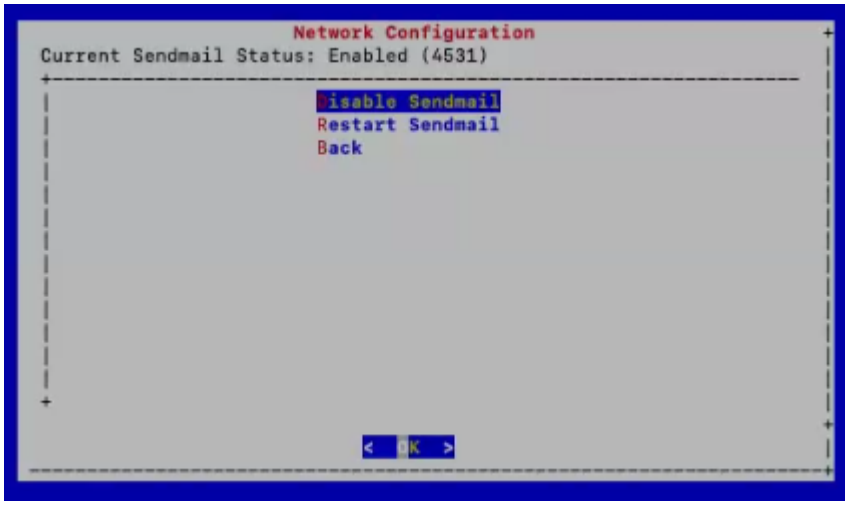
   - Multi-line entries can be added, if required. For example, for CUCM v11.5 support, see: *Configure multi-line CUCM cipher support*.
   - This step is relevant *only* to an Insights Assurance solution and its integration with Cisco UC systems. This step is *not* relevant to the DS9 and Insights NetFlow solution.
   - On system upgrade, if the contents of this configuration are no longer valid, then the contents will be will be reset to an empty state.

8. Enable/disable FTPD or restart the FTPD daemon:
   1. Select **FTPD Config**.

Important: On new installs, the FTPD daemon is disabled by default. It is strongly recommended that the FTPD daemon remains disabled, unless there is a good reason you need to use it. It has been seen that enabling the FTPD daemon may introduce a system vulnerability. FTPD is typically *only* required in rare situations, where FTP is the only way to transfer files to the server. Instead of using FTPD, it is recommended that you use the drop account with SCP or SFTP. The drop account username is “drop”. You can set the password via the **Administration** menu.



9. Enable/disable Sendmail or restart Sendmail on port 25:



   i. Select **Sendmail Config**. The current status of the service displays on the menu.

   ii. Choose to enable, disable, or restart the service as required.

10. Base system installation is now complete. Select **Quit** to exit the **Administration** menu on the console.

Next steps

- *Create GUI admin password for Arbitrator and Dashboard*

9.6. Create GUI admin password for Arbitrator and Dashboard

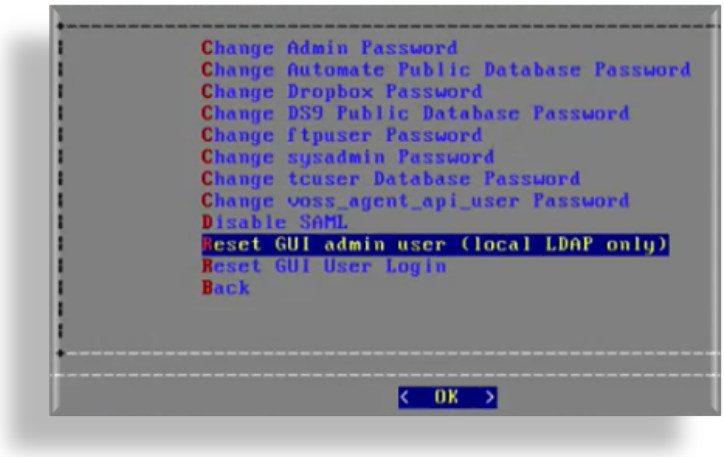
This procedure creates the GUI admin password, which is the password you will need to log in to Arbitrator or Dashboard via the browser.

The default credentials will not allow browser access, so the GUI admin password must be set up for the Arbitrator and Dashboard systems. The procedure is the same for both Arbitrator and Dashboard.

Important: It is strongly recommended that you make a written or digital copy of any system passwords and share the copies with trusted team members or store them in a secure location from where they may be retrieved if needed.

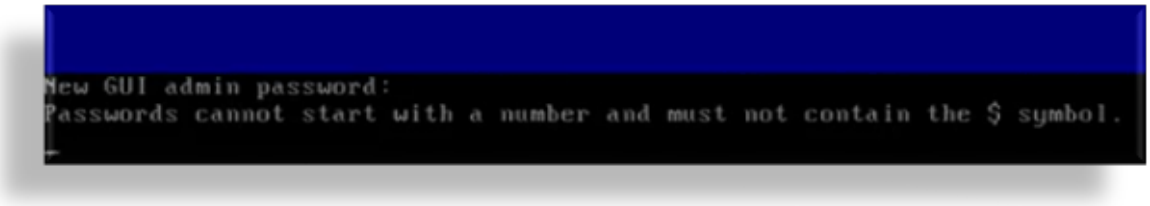
The steps to create the GUI admin password for Arbitrator and Dashboard are the same.

1. Log in via the CLI, then from the **Administration** menu, select **Change Passwords**.
2. Select **Reset GUI admin user (local LDAP only)**.



3. Fill out a new GUI admin password.

   The GUI admin password cannot start with a number and must not contain the dollar ($) symbol.



4. Log in to the Arbitrator / Dashboard via the browser, using the GUI admin user password created in this procedure.

Next steps

- *Product registration and system configuration*

9.7. Product registration and system configuration

Once you've installed and configured initial settings via the Administration console, you can continue with product registration, and with the configuration of your system through the GUI:

- 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.

9.8. Configure 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.

You can copy the keys into the screen in a comma separated list (without spaces).

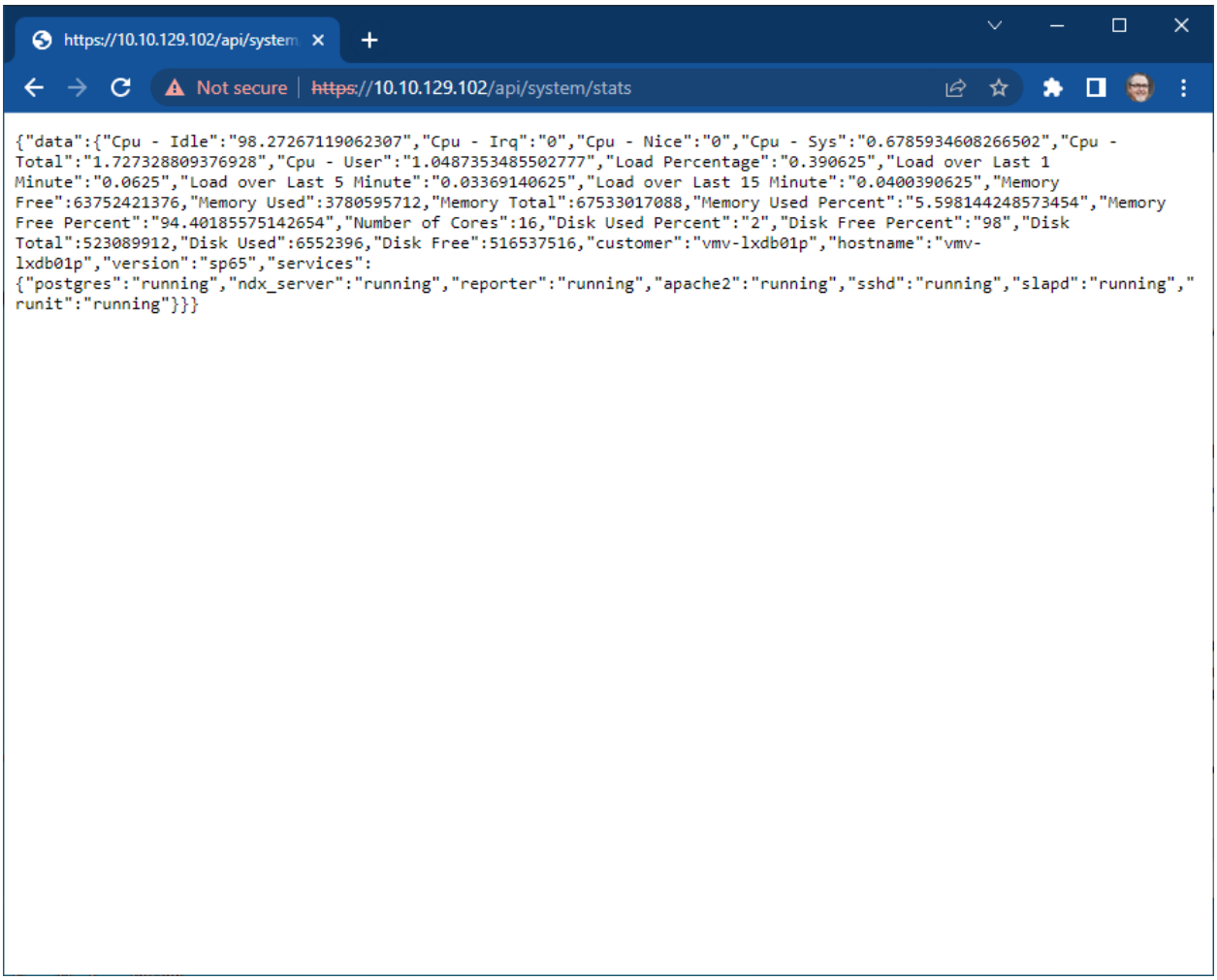
For CUCM v11.5 support:

```
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. Dashboard server system status API check

In a browser, navigate to the Dashboard System Status API, using a URL with the following format:

https://<IP address>/api/system/stats



API output text displays system utilization statistics (CPU, RAM, Disk) and process status. All service status results should display as “running” for proper system operation.

API text output:

```
{"data":
```

(continues on next page)

(continued from previous page)


```
{"Cpu - Idle":"98.27267119062307",
 "Cpu - Irq":"0",
 "Cpu - Nice":"0",
 "Cpu - Sys":"0.6785934608266502",
 "Cpu - Total":"1.727328809376928",
 "Cpu - User":"1.0487353485502777",
 "Load Percentage":"0.390625",
 "Load over Last 1 Minute":"0.0625",
 "Load over Last 5 Minute":"0.03369140625",
 "Load over Last 15 Minute":"0.0400390625",
 "Memory Free":63752421376,
 "Memory Used":3780595712,
 "Memory Total":67533017088,
 "Memory Used Percent":"5.598144248573454",
 "Memory Free Percent":"94.40185575142654",
 "Number of Cores":16,
 "Disk Used Percent":"2",
 "Disk Free Percent":"98",
 "Disk Total":523089912,
 "Disk Used":6552396,
 "Disk Free":516537516,
 "customer":"vmv-lxdb01p",
 "hostname":"vmv-lxdb01p",
 "version":"sp65",
 "services":{"postgres":"running",
             "ndx_server":"running",
             "reporter":"running",
             "apache2":"running",
             "sshd":"running",
             "slapd":"running",
             "runit":"running"}}}
```

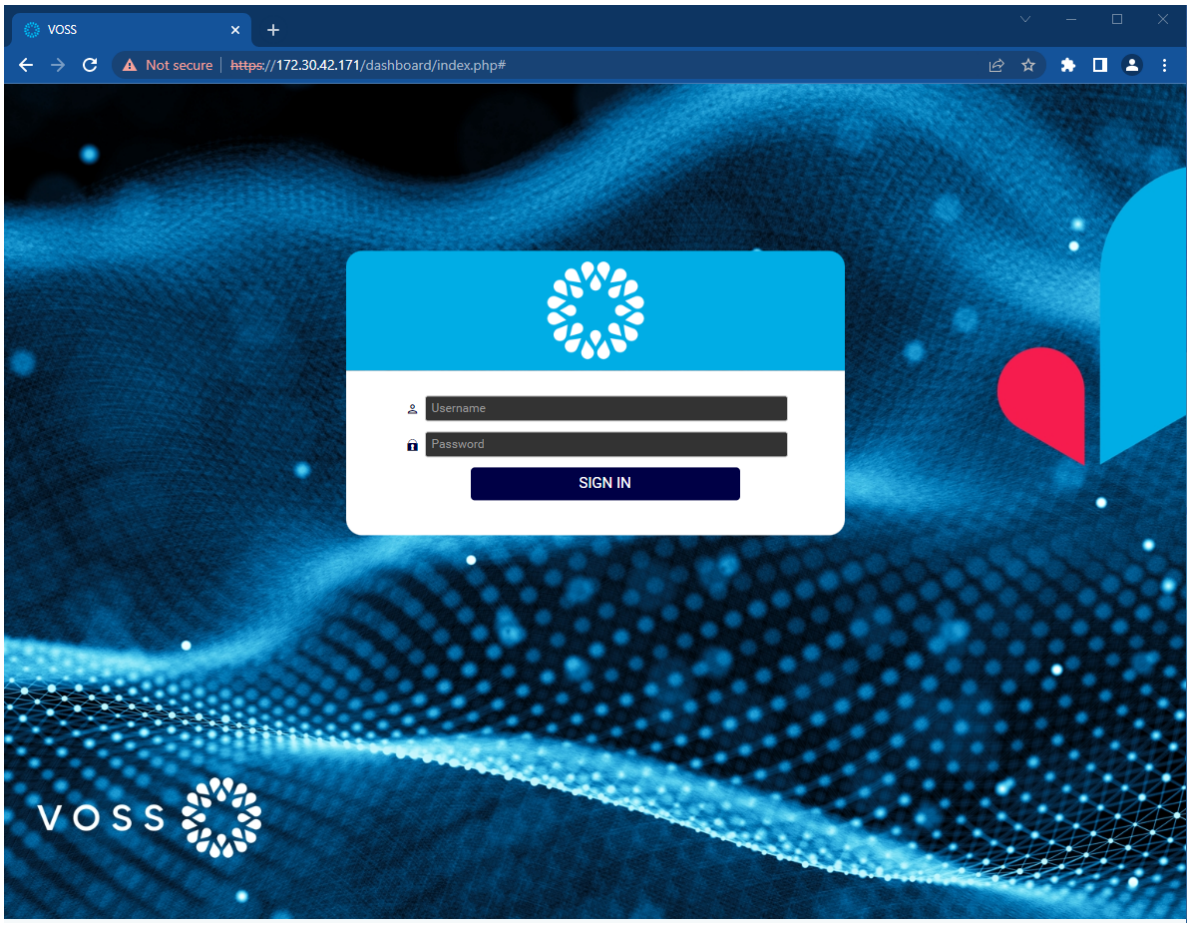
11. Dashboard server GUI login, interface validation check

1. In a browser, navigate to the Dashboard GUI, using a URL with the following format:

   https://<IP address>

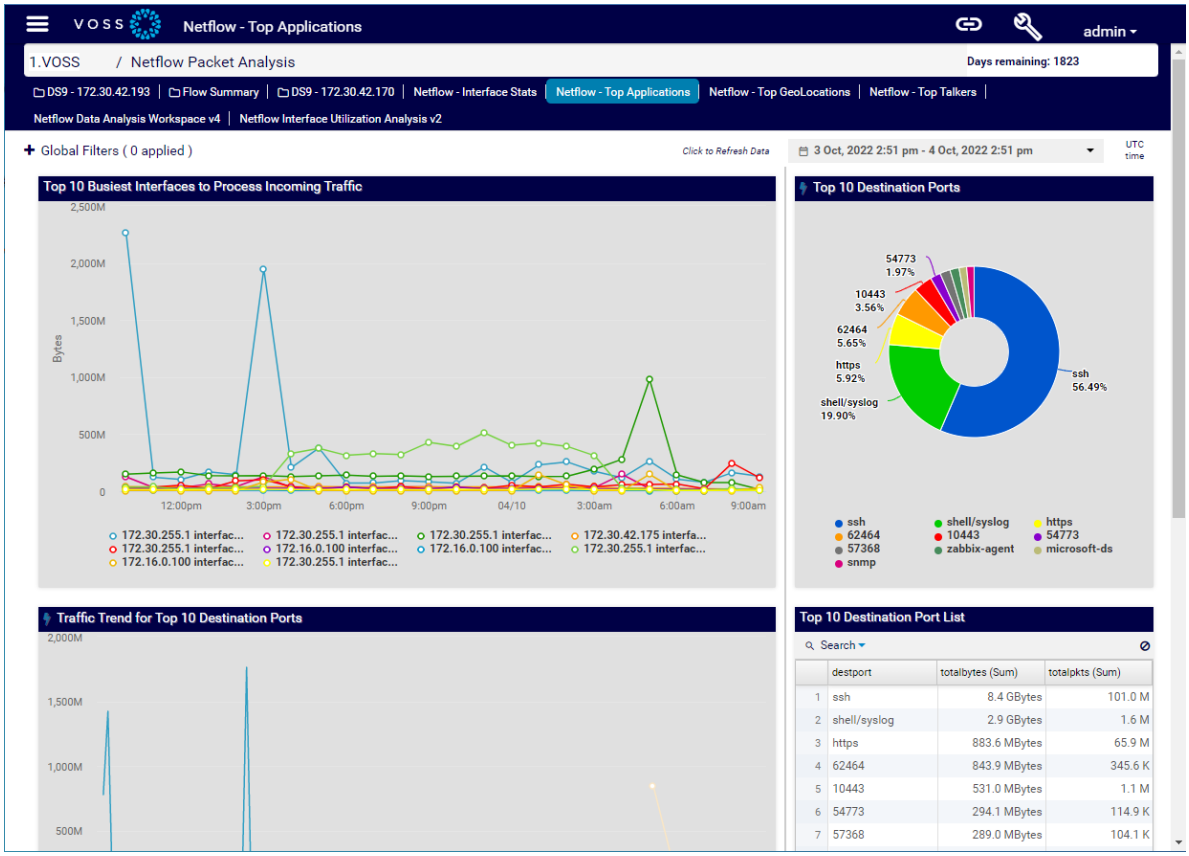
   If the log in page displays, this validates that the system is reachable and the Apache service is running.
2. Log in to the system using admin credentials.

   Successful authentication indicates that the system processes are running, and serving its GUI via Apache.



3. View the default Dashboard.

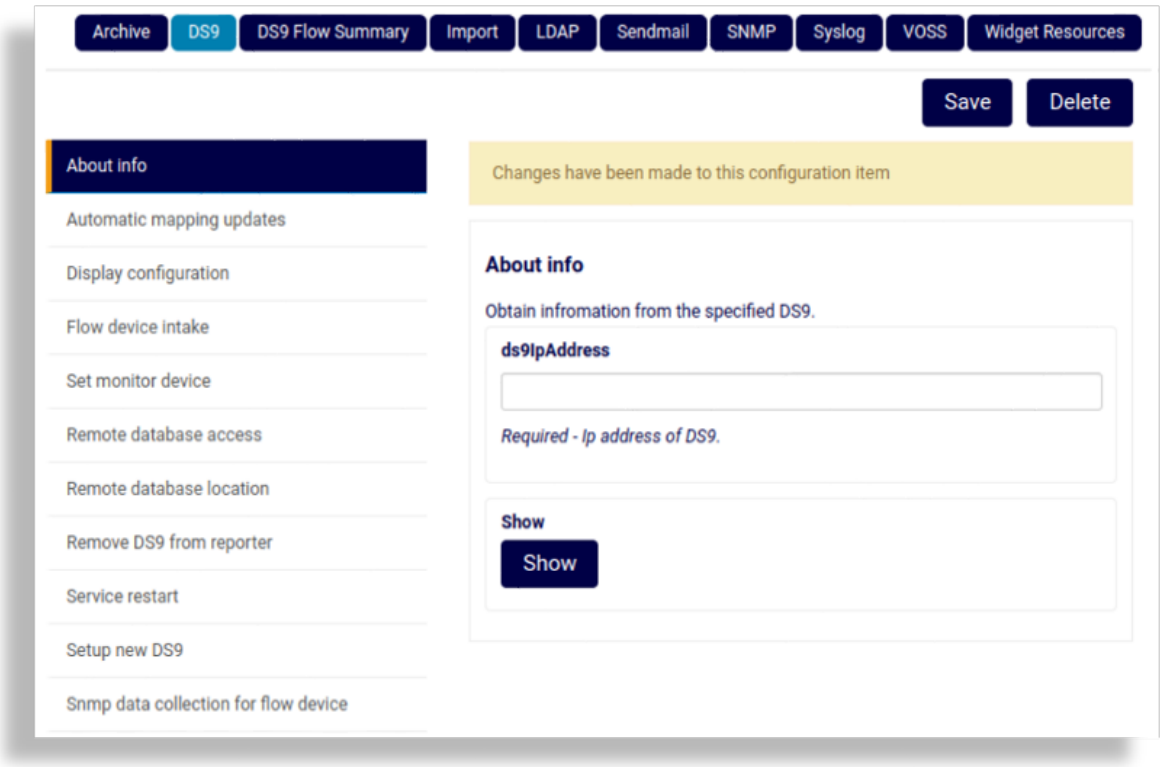
Data displayed in the dashboard validates GUI function and connectivity to the DS9 Collector system from the Dashboard system.



12. Configure DS9 on the Dashboard system

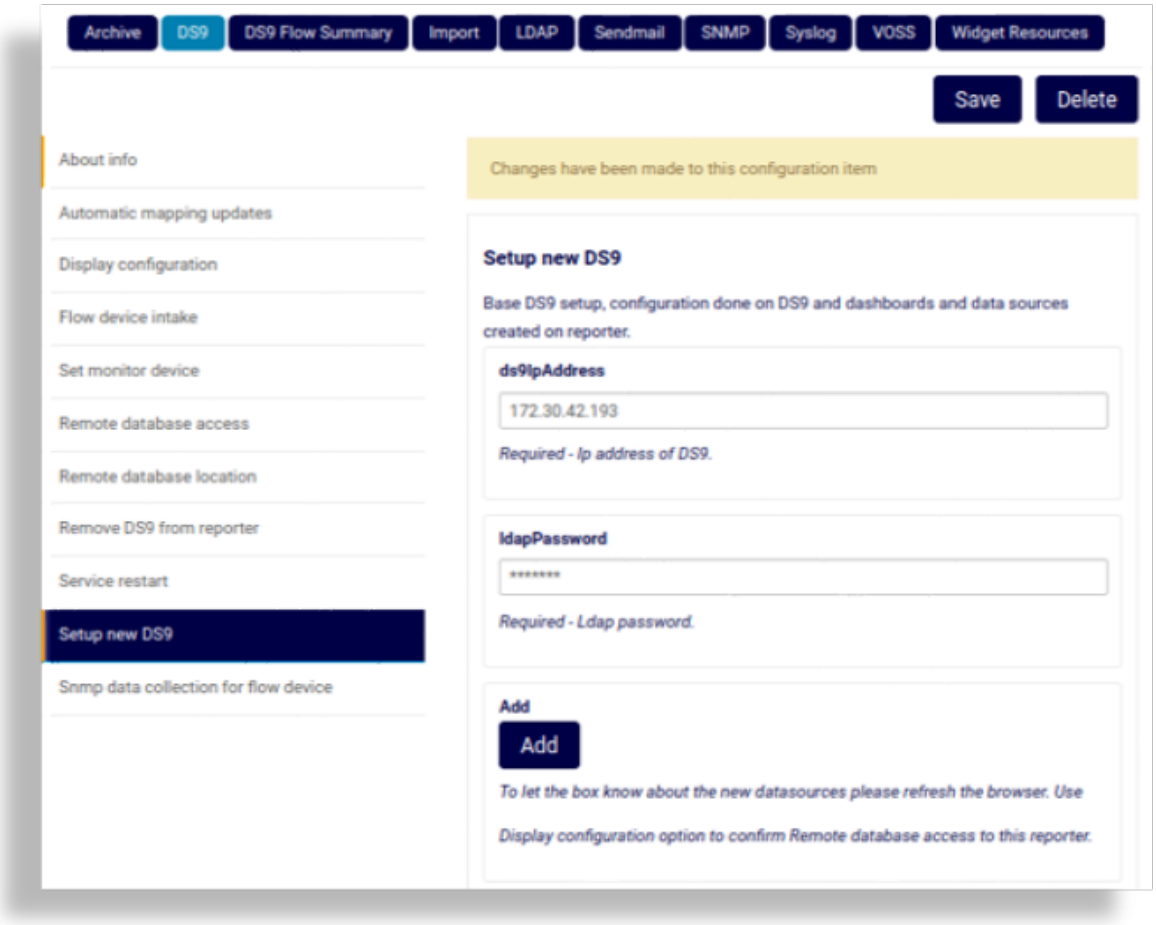
This procedure configures flow devices and SNMP to completes the setup between Insights Dashboard and DS9.

1. Log in on the Dashboard GUI as admin.
2. Go to **admin > Configuration**, and on the **Configuration Settings** page, select **DS9**.



3. Select **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.

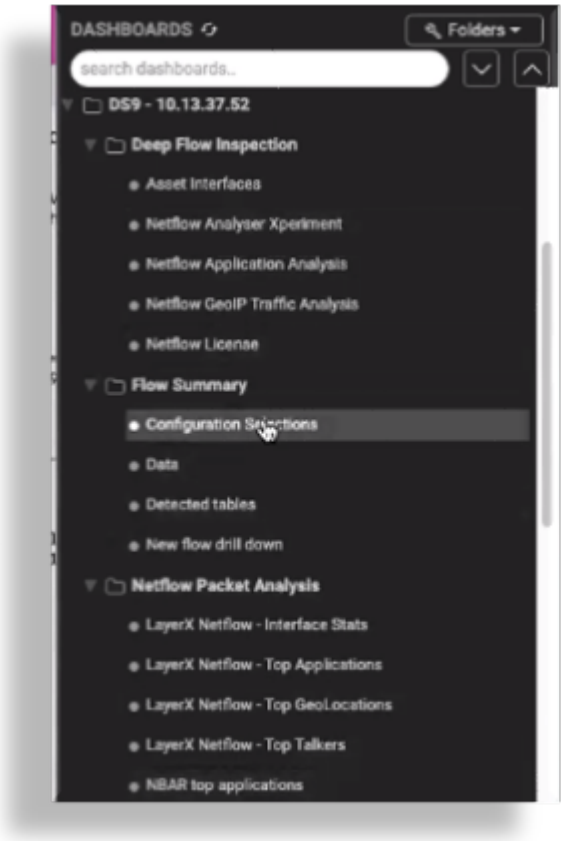


4. Refresh the Dashboard browser page and from the menu, select **Data Sources**.

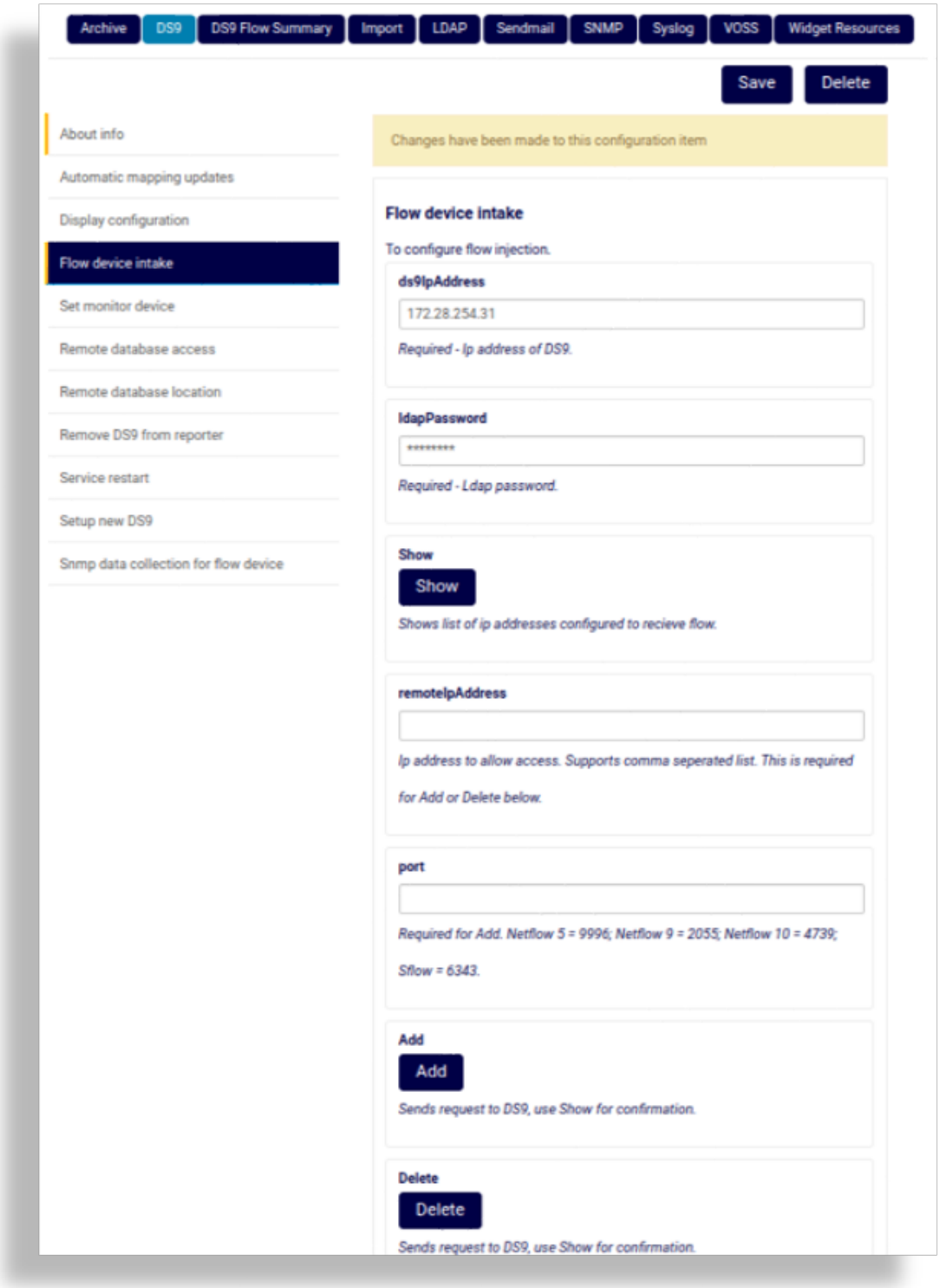
   The new entries for the IP address are listed as `DS9 SNMP...`, `DS9 SUMMARY...` `DS9 TOPN...` entries.

5. Under the **DASHBOARDS** menu, view the new **DS9 - <IP>** dashboard menu. The image shows an example.

Note: At this stage, the sub-menus are still empty.



6. Set up the DS9 to receive netflow from the source devices sending to the DS9:
    - Go to **admin > Configuration**.
    - On the **Configuration Settings** page, select the **DS9** tab.
    - Select **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. Select **Snmp data collection for flow device**.

   Provide NetFlow source device interface utilization statistics, which are gathered using SNMP data collection.

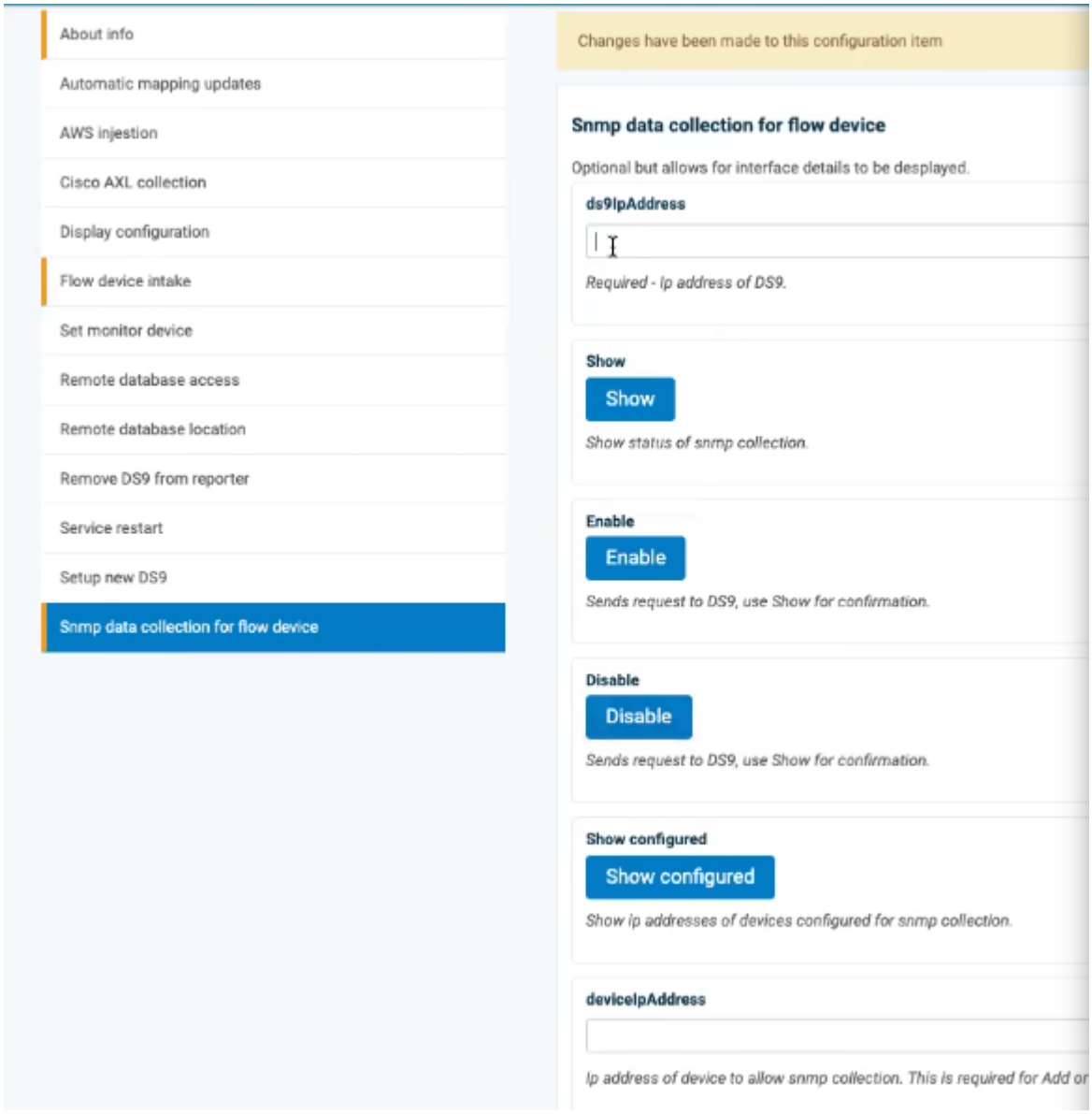
8. Fill out data relevant for your SNMP version configuration preferences.

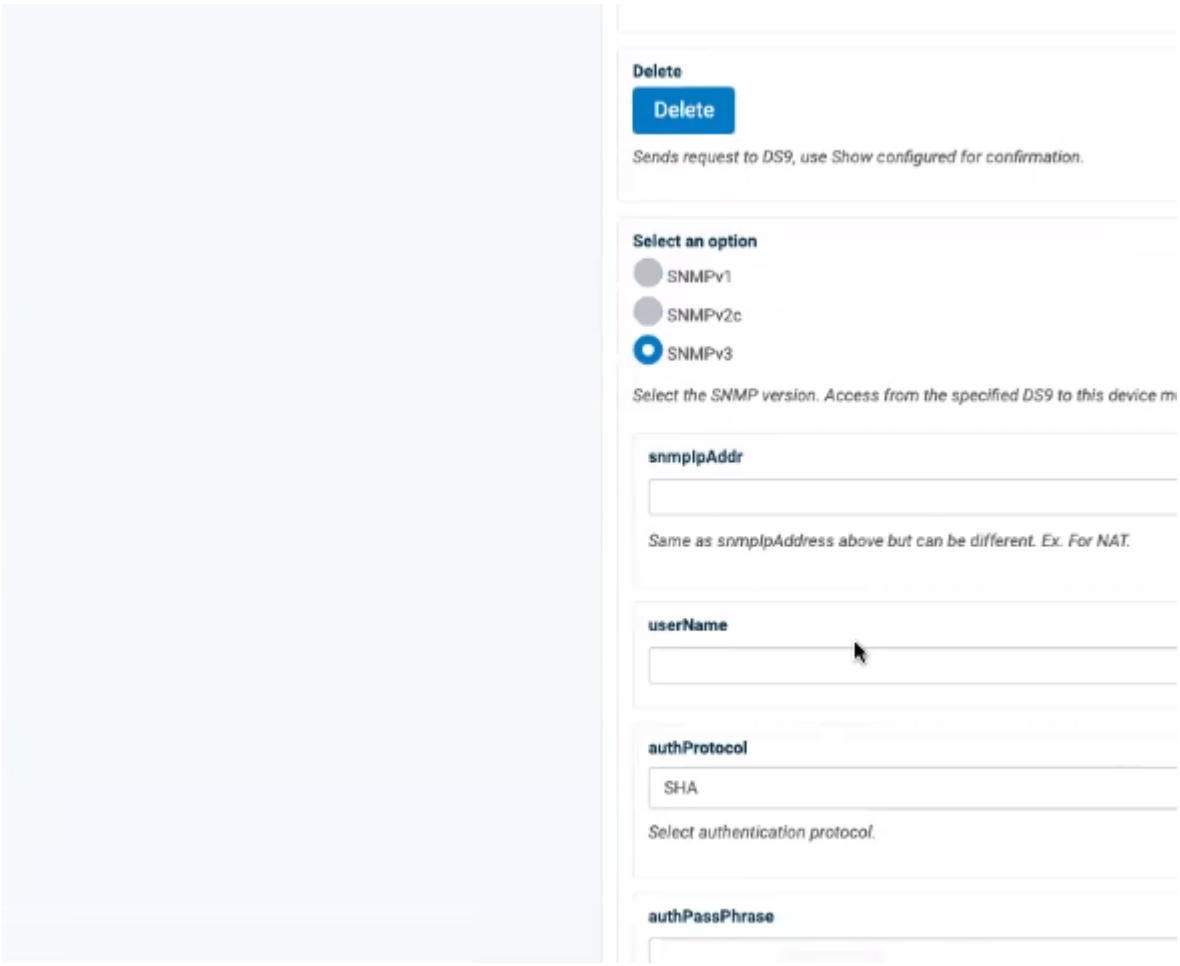
You will repeat this step for each of the flow sources set up to send flow to the DS9.

- 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.

9. Click **Add**.

   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.





13. Dashboard server Netflow data rendering check

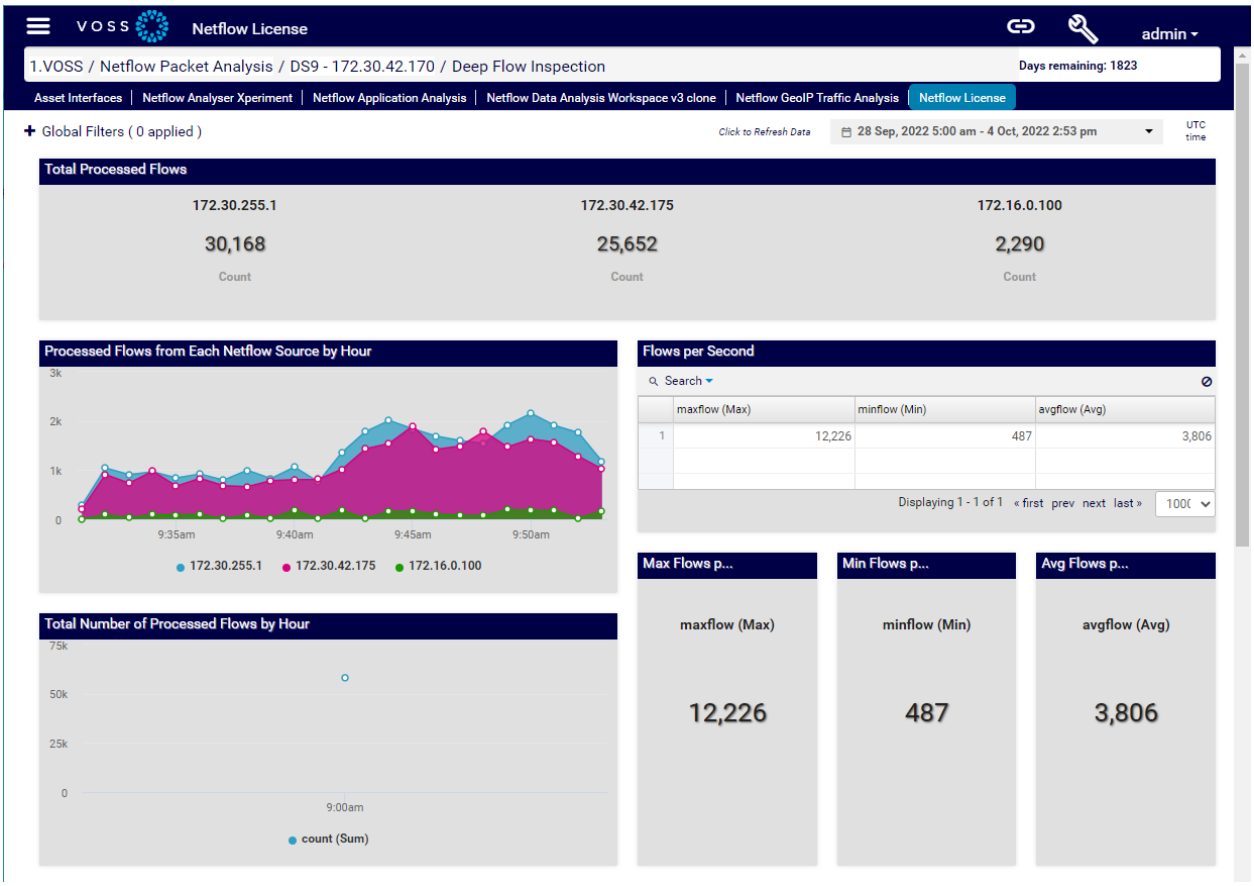
1. In a browser, connect to the Dashboard GUI, using a URL with the following format:

   https://<IP address>

2. Log in to the system using admin credentials.
3. In the **Deep Flow Inspection** folder, select the **Netflow License** dashboard.
4. Set the time frame for the data to be viewed, to the 1 hour time frame.

   If you're able to see data rendered in the tables and graphs in the Netflow License dashboard, system connectivity to the DS9 Collector databases is validated, as well as DS9 Netflow data ingestion.

   If you're able to see data displaying in any dashboard in the Netflow Packet Analysis and Deep Flow Inspection folders on the Dashboard application, then both systems are functioning properly.



14. Virtualization and hypervisor platforms

14.1. Supported virtualization and hypervisor platforms

This section provides details on VM creation in supported virtualization platforms.

- The steps for each supported platform are to be followed during the installation process - see: *Deploy and VM installation*.
- Installation hardware requirements:
  - Dashboard reporting VM sizing specifications in the Analytics Install Guide.
  - Arbitrator Correlation Consolidation VM Sizing Specifications in the Arbitrator Install Guide.
  - Arbitrator Correlation Consolidation VM Sizing Specifications in the Arbitrator Install Guide.
  - DS-9 Netflow VM sizing specifications in the DS9 for Netflow Install Guide.
- Supported platforms:
  - *VMWare Esxi 8*
  - *Hyper-V*
  - *Nutanix*
- Supported platform version support:
  - Compatibility Matrix

14.2. VMWare Esxi 8

14.2.1. Requirements

Installation hardware requirements by solution:

- Dashboard reporting VM sizing specifications in the Analytics Install Guide.
- Arbitrator Correlation Consolidation VM Sizing Specifications in the Arbitrator Install Guide.
- Arbitrator Correlation Consolidation VM Sizing Specifications in the Arbitrator Install Guide.
- DS-9 Netflow VM sizing specifications in the DS9 for Netflow Install Guide.

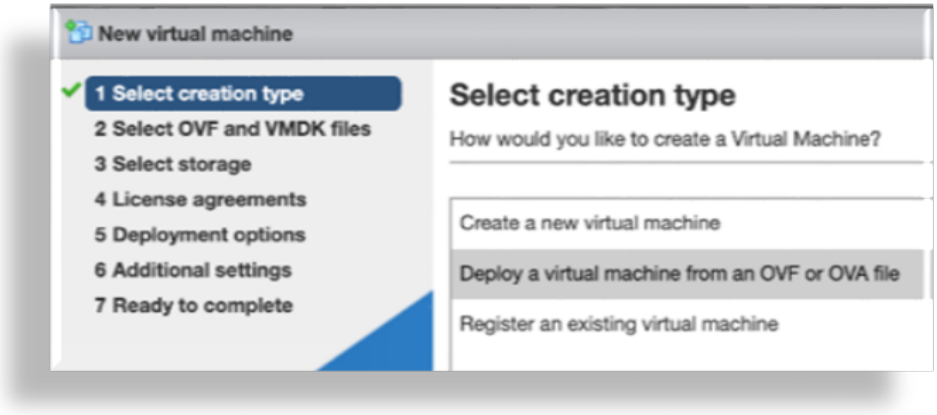
Download OVA

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

Deploy the OVA

To deploy the OVA:

1. Select the downloaded OVA file, and choose a VM name.



2. On the **Select storage** menu, configure storage settings based on the recommended hardware specifications for the required configuration.

   See the *VM Specification and Requirements* for your system.

3. Configure the network mappings based on the recommended hardware specifications for the required configuration.

   See the *VM Specification and Requirements* for your system.

14.3. Hyper-V

Installation hardware requirements by solution:

- Dashboard reporting VM sizing specifications in the Analytics Install Guide.
- Arbitrator Correlation Consolidation VM Sizing Specifications in the Arbitrator Install Guide.
- Arbitrator Correlation Consolidation VM Sizing Specifications in the Arbitrator Install Guide.
- DS-9 Netflow VM sizing specifications in the DS9 for Netflow Install Guide.

14.3.1. Download the install file

Download for your solution and release from the **New Installation** folder on the client portal.

- `insights-<deployment>-hyper-v-<version>.zip`

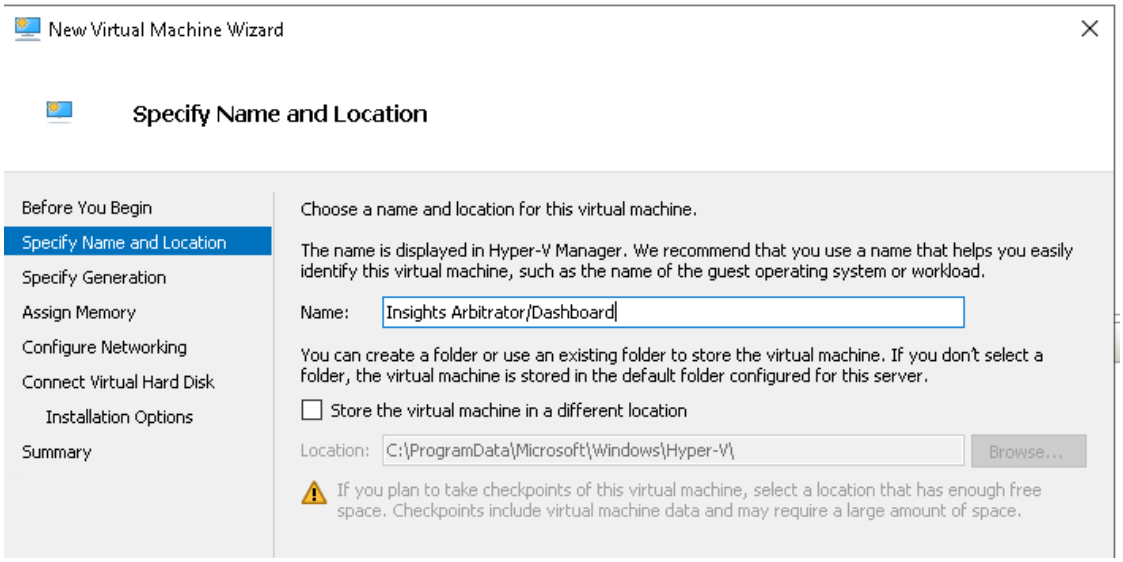
containing the `.vhd` file

14.3.2. Prepare the OS Disk

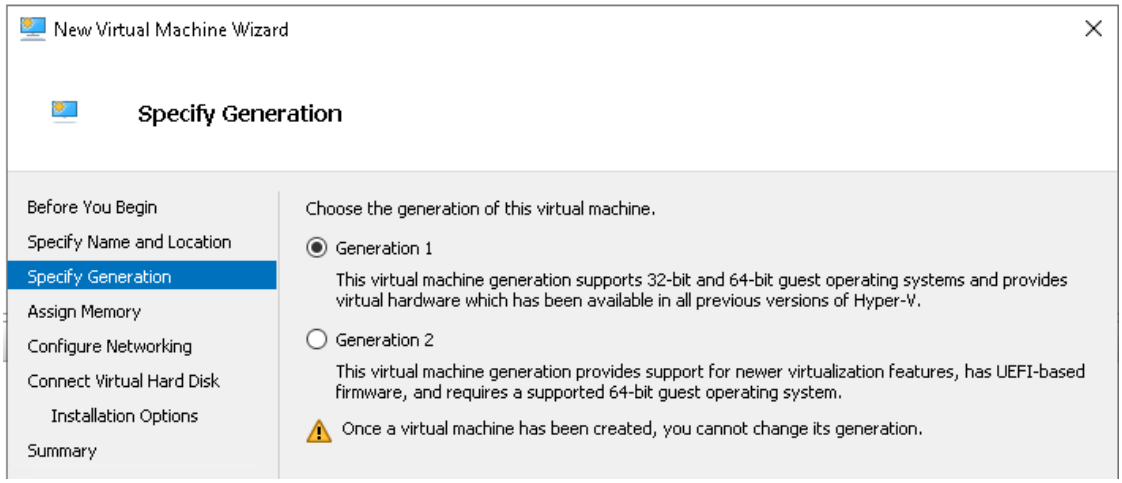
- Copy the `.vhd` to the Hyper-V Settings/Virtual Hard Disks location of your choice.
- Rename it to your own requirements.

14.3.3. Create the VM

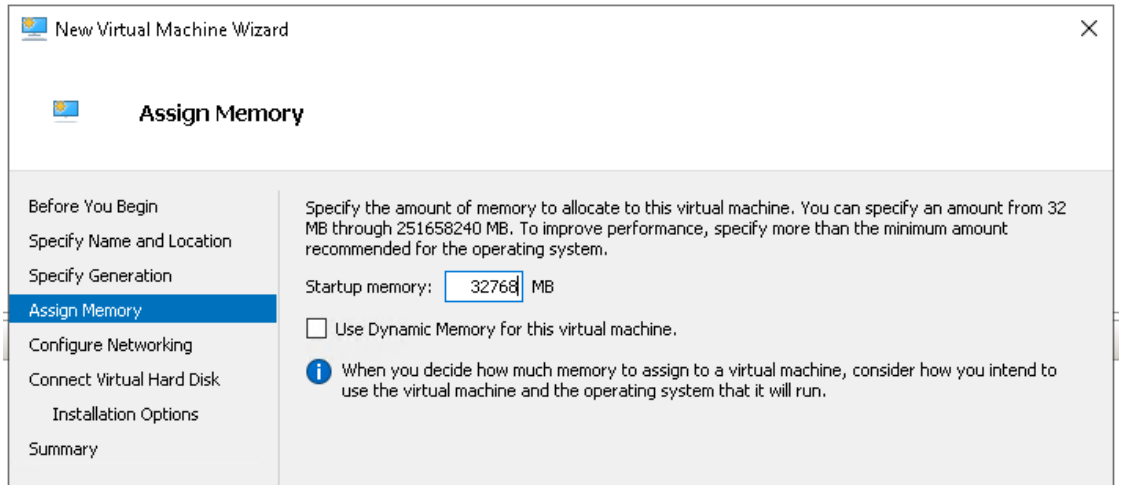
1. In Hyper-V Manager, go to **New > Virtual Machine**.
2. **Specify Name and Location**: Assign a suitable name to the VM.



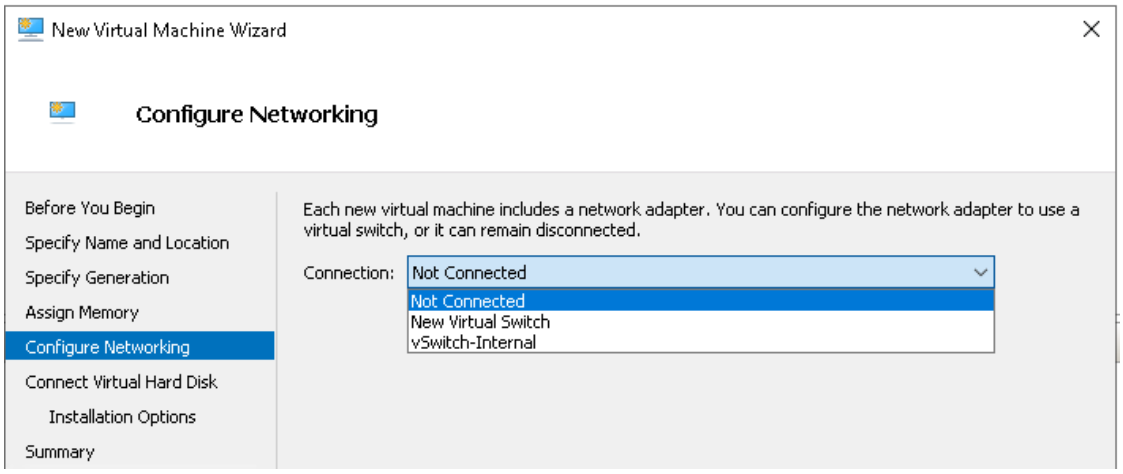
3. **Specify Generation:** Select Generation 1



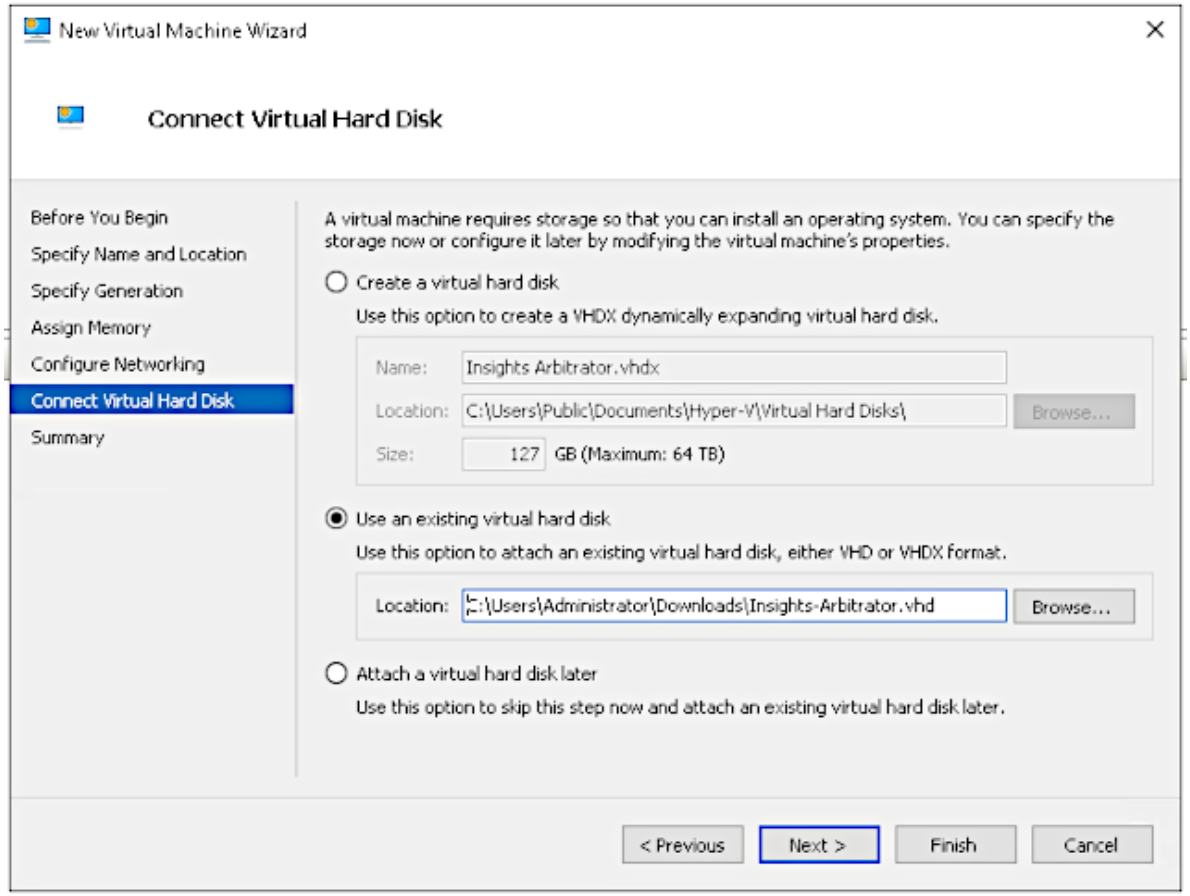
4. **Assign Memory:** Set the Startup memory according to the documentation



5. **Configure Networking:** Select the required Virtual Switch



6. **Connect Virtual Hard Disk:**
   - Select **Use an existing virtual hard disk** and select the `.vhd` file



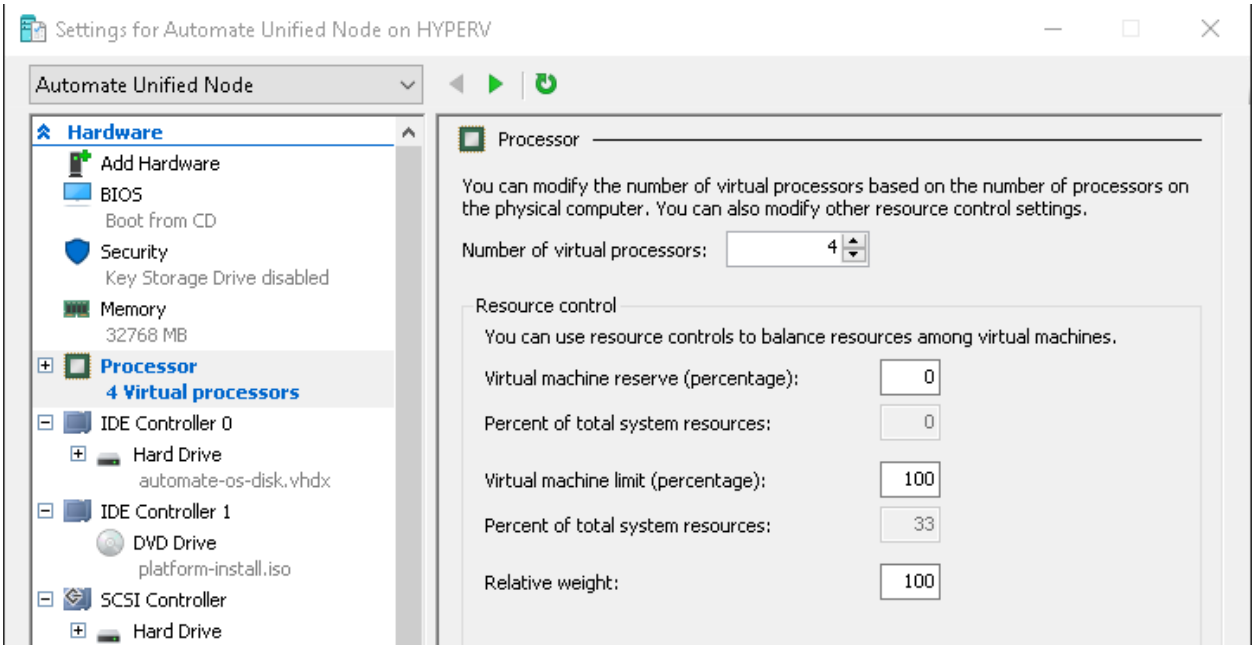
- Click **Finish**.

14.3.4. Configure the VM

Right-click the VM in the list **> Settings**

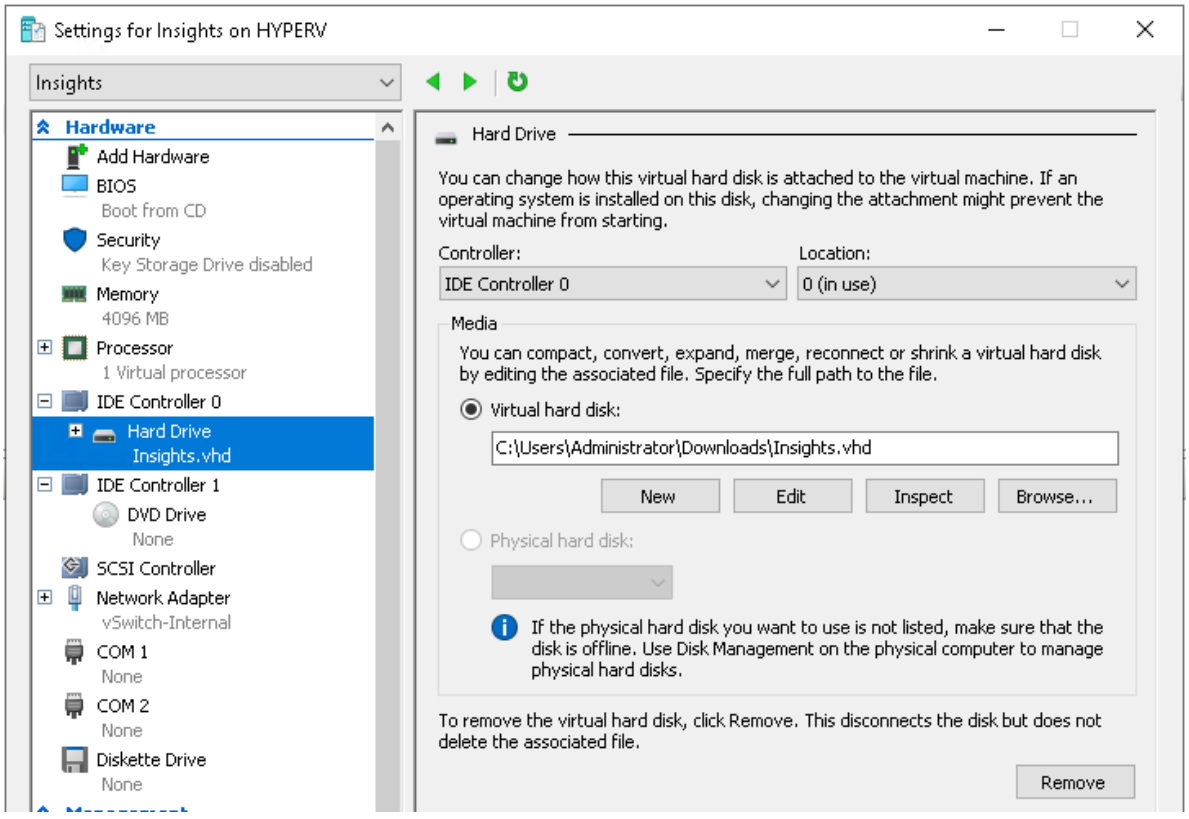
Configure the total processors

Select **Processor** in the left pane. Set the **Number of virtual processors** according to the sizing specifications in the documentation.

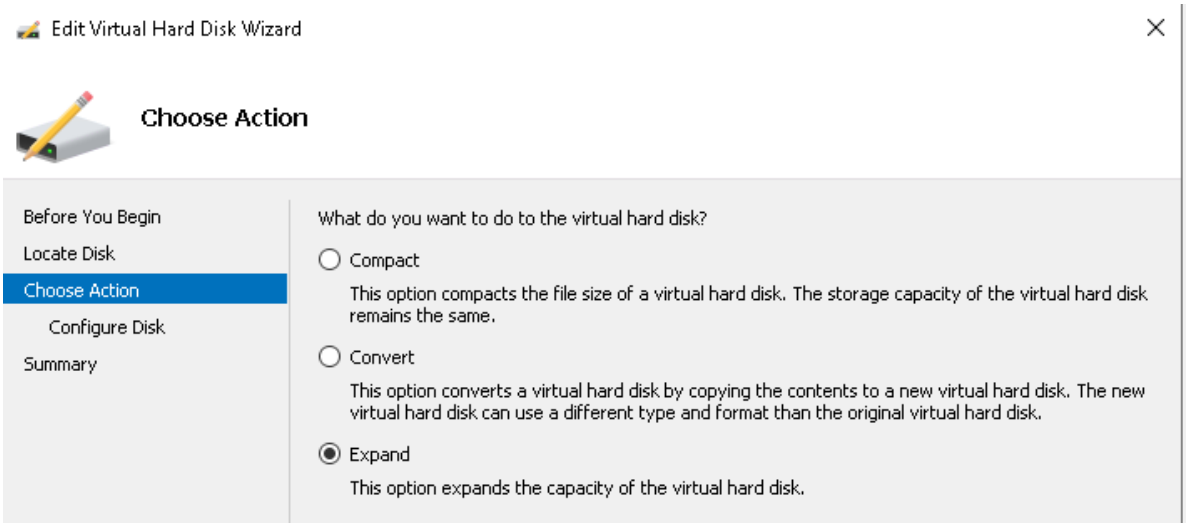


Resize the OS Disk and Data Disk (DS9 only)

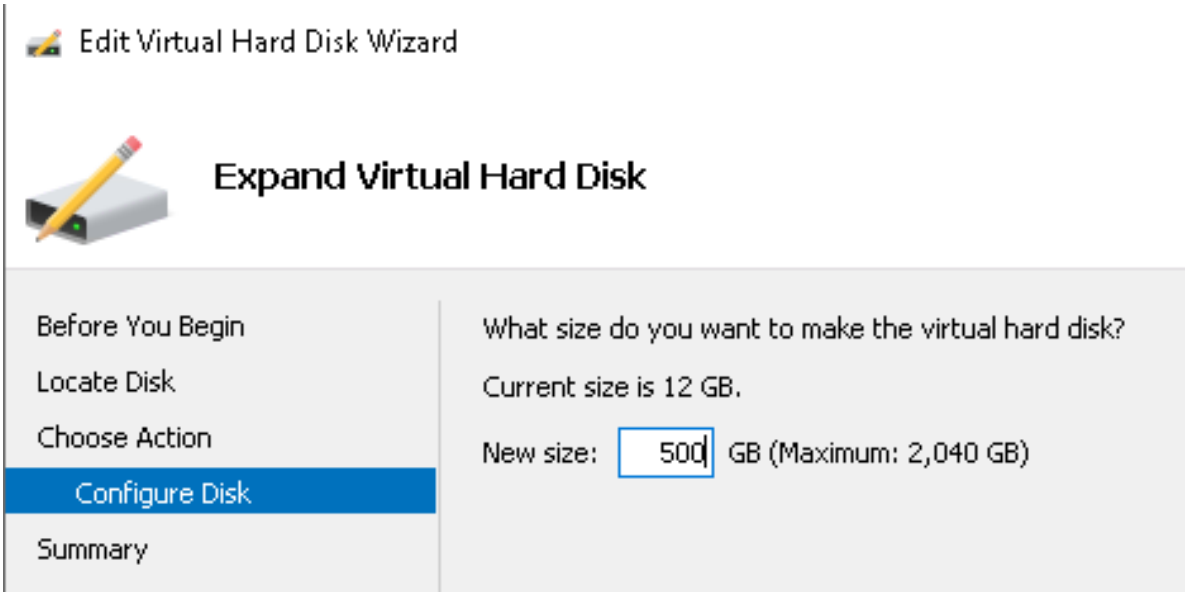
1. Under **IDE Controller 0** in the left pane, select the **Hard Drive**, **Edit**



2. Select **Choose Action > Expand**



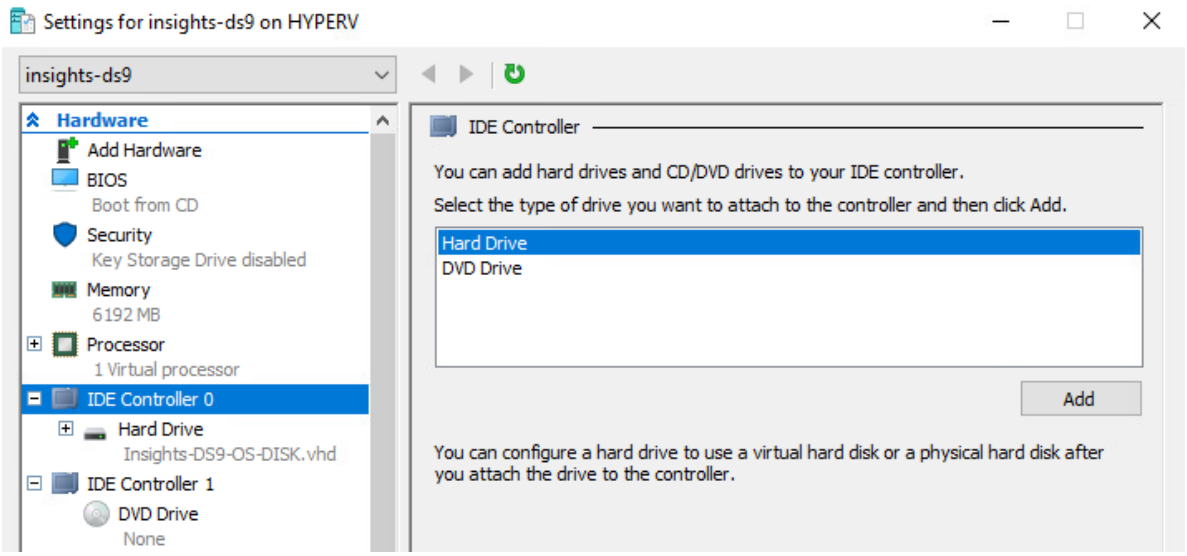
3. **Configure Disk**: Set the size according to the sizing specifications in the documentation.

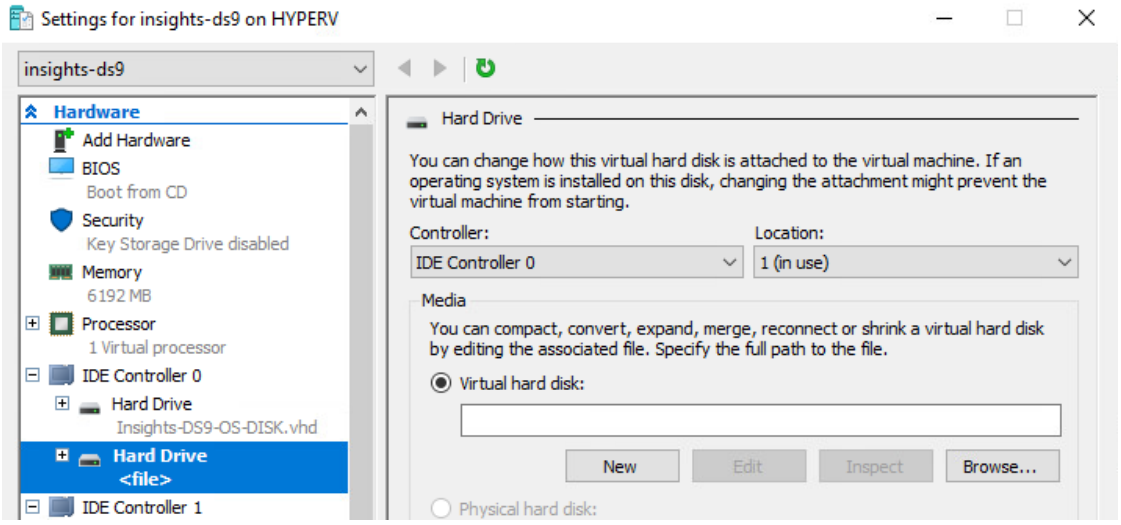


4. Click **Finish**.

Expand the Data disk if you are deploying DS9

1. Select **IDE Controller 0** in the left pane: **Hard Drive > Add**
2. Click **Browse** and select the `insights-ds9-data-disk.vhd`
3. Expand the disk as per above steps and documentation





14.3.5. Connect and start the Virtual Machine

Right-click the VM, **Connect** and click **Start**.

14.4. Nutanix

Installation hardware requirements by solution:

- Dashboard reporting VM sizing specifications in the Analytics Install Guide.
- Arbitrator Correlation Consolidation VM Sizing Specifications in the Arbitrator Install Guide.
- Arbitrator Correlation Consolidation VM Sizing Specifications in the Arbitrator Install Guide.
- DS-9 Netflow VM sizing specifications in the DS9 for Netflow Install Guide.

14.4.1. Download the install file

Download the install file for your release from the **New Installation** folder on the client portal.

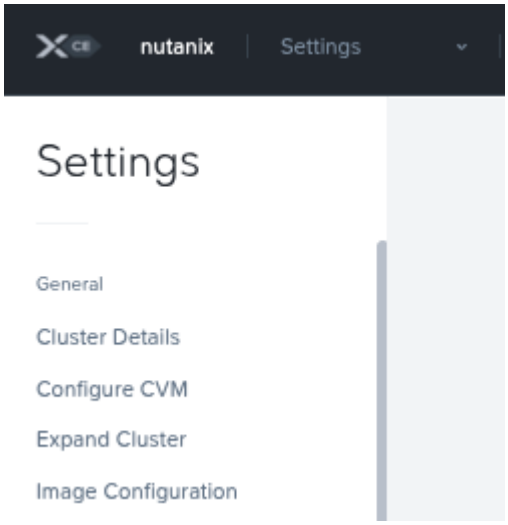
- `insights-<deployment>-<version>-nutanix.zip`

File contents supplied are the OS Disk in raw format - pre-installed.

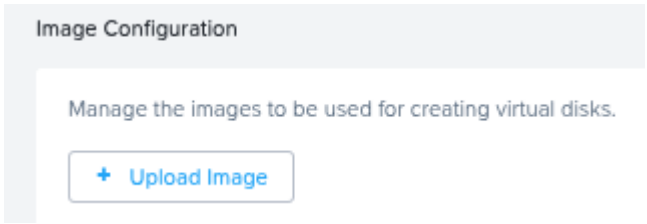
- `insights-<deployment>-<version>-nutanix.raw`

14.4.2. Upload the OS Disk and Data Disk (DS9 Only)

1. Select **Settings** from the drop down menu top left, then **Image Configuration**.



2. Click **Upload Image**

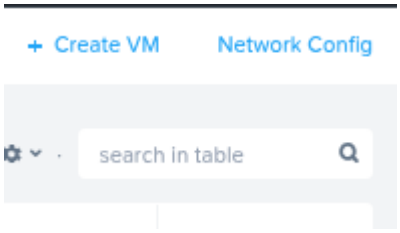


3. File in:

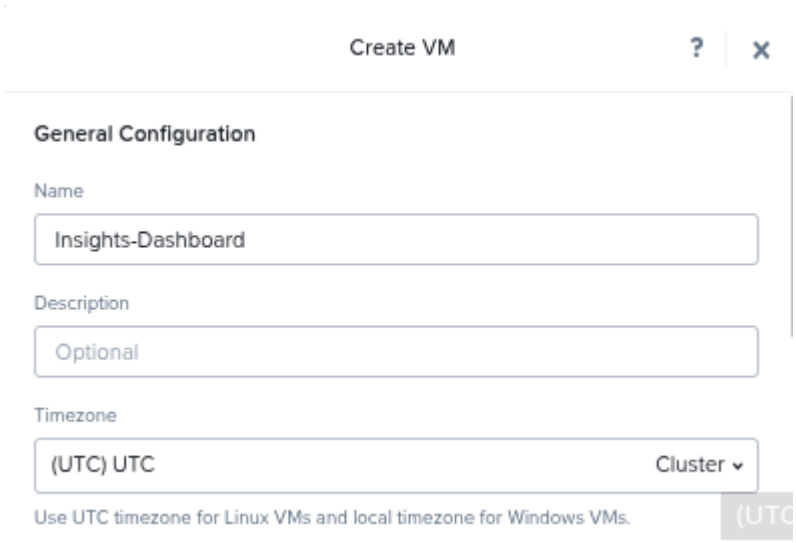
- **Name**: Name the image accordingly - e.g. `insights-dashboard-nutanix.raw`
- **Image Type**: `Disk`
- **Storage Container**: Select the required Storage Container
- **Image Source**: Either `URL` or `Upload a file`
- View the tasks to see the progress of the image creation

14.4.3. Create the VM

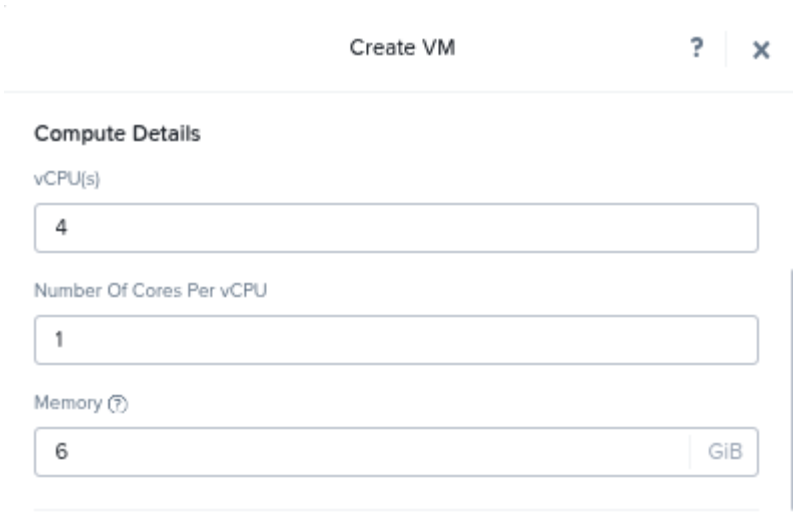
1. Select **VM** from the drop down menu top left, then the **Table** tab.
2. Click **Create VM** at the top right



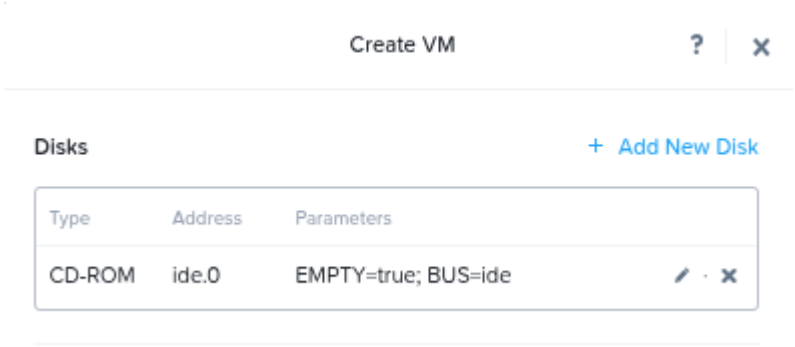
3. Give the VM a name



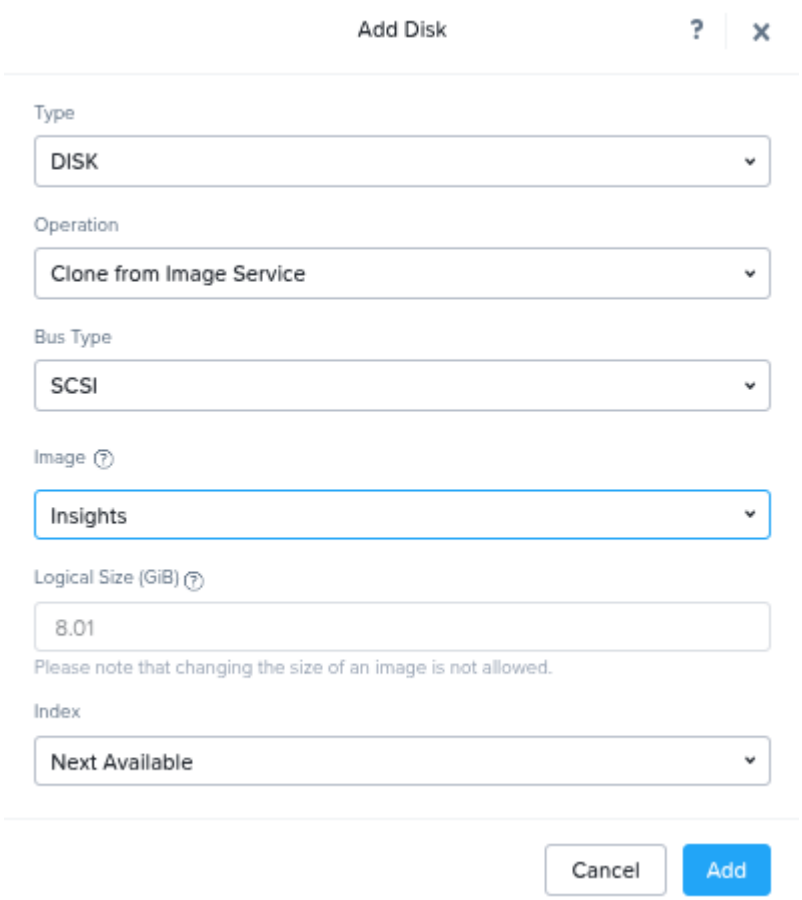
4. Set the CPU and RAM according to the documentation.



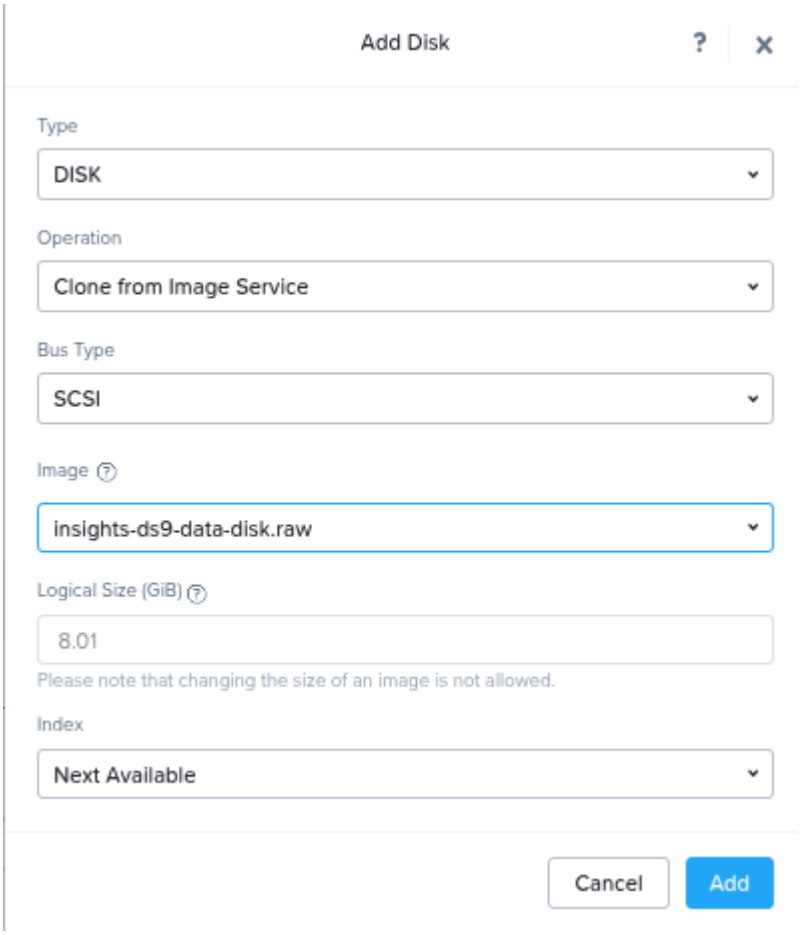
5. Add the OS Disk



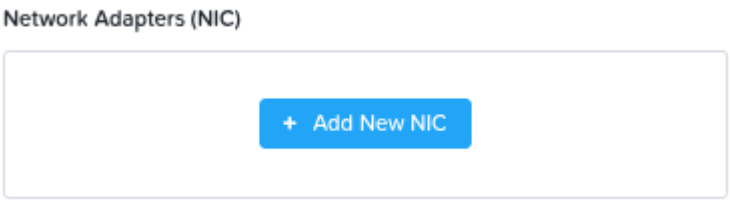
- **Type**: `Disk`
- **Operation**: `Clone from Image Service`
- **Bus Type**: `SCSI`
- **Image**: Select the image / raw disk uploaded in previous step
- Click **Add**



6. Add the Data Disk (DS9 Only)



7. Add the NIC and finally click **Save**



14.4.4. Increase the OS Disk and Data Disk (DS9 Only) size

It is required to resize the disk size according to the hardware specifications in the documentation

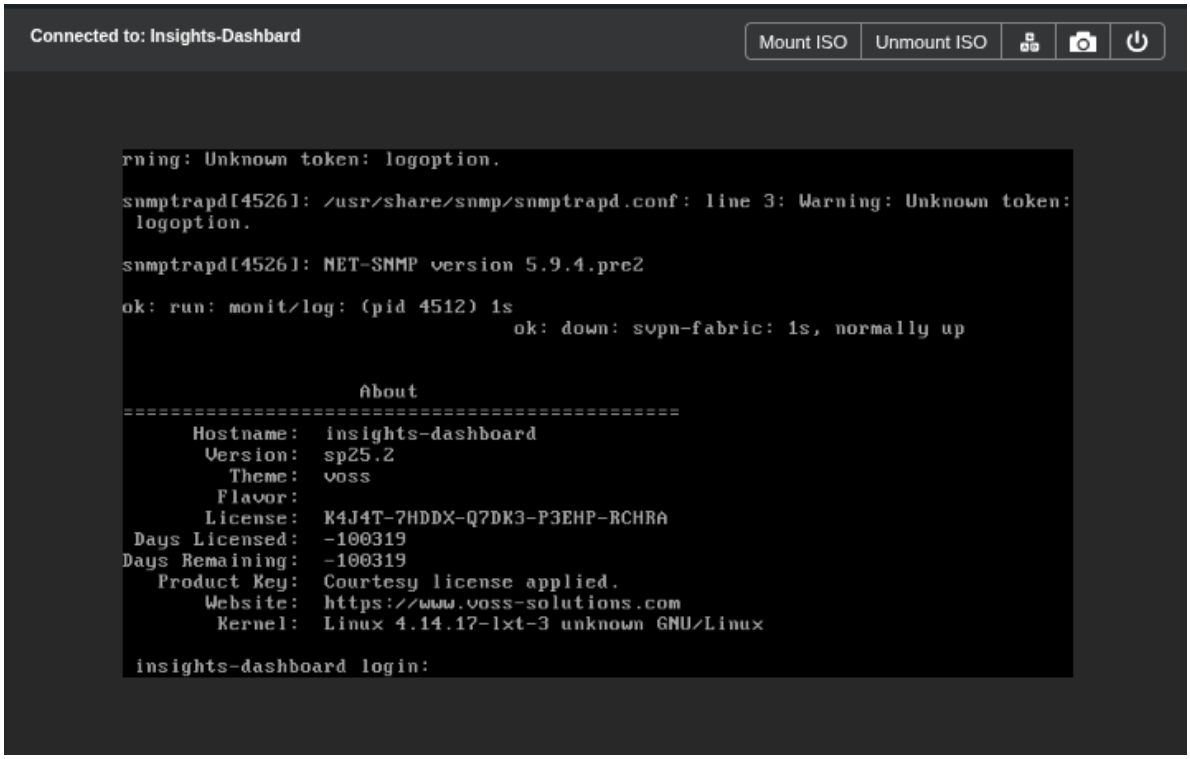
- Select **VM** from the drop down list top left
- From **Table**: Select the VM

Edit the Virtual Disk

1. Click **Update**.
2. Scroll to the **Disks** section.
3. Click the pencil icon to edit the OS Disk.
4. Increase **Logical Size (GiB)** to the new value according to the hardware specifications in the documentation.
5. Click **Update**, then **Save**.

14.4.5. Power the VM on and launch the console

1. Right click the VM **Power On**.
2. Once powered on, right click the VM **Launch Console**



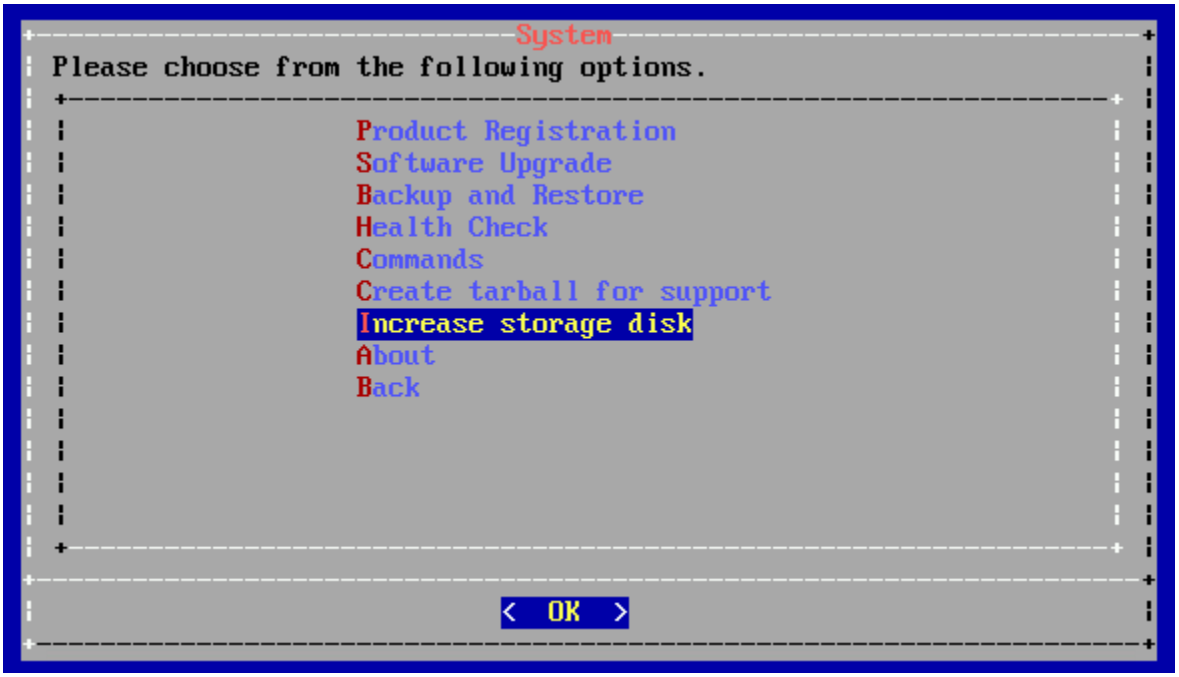
3. Log in via the `admin` account

14.4.6. Update the OS Disk size (Arbitrator and Dashboard)

Scroll to **Resize Disk** and resize it according to the documentation.

14.4.7. Update the Data Disk Size (DS9)

Scroll to **System > Increase Storage Size** and resize according to the documentation



Index

F