VOSS Insights
Analytics Install Guide

Release 25.3

December 04, 2025

Legal Information

DOCUMENT ID: 20251204055234

Contents

1. What's New

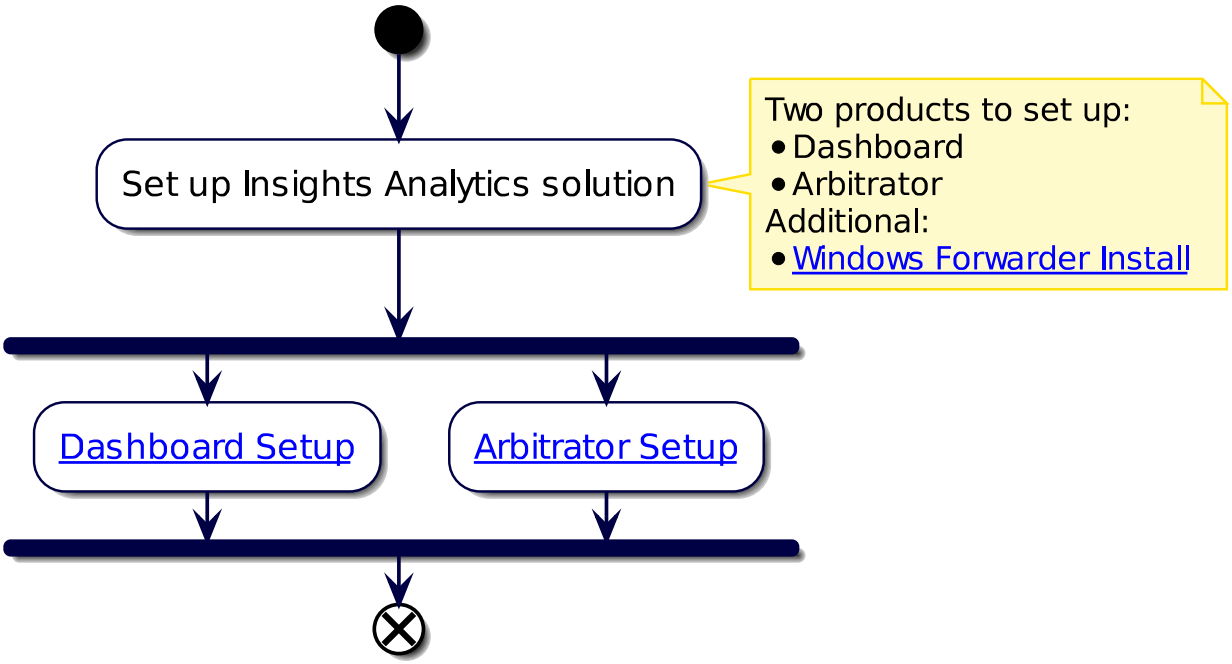
1.1. Analytics Install Guide: Release 25.3

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

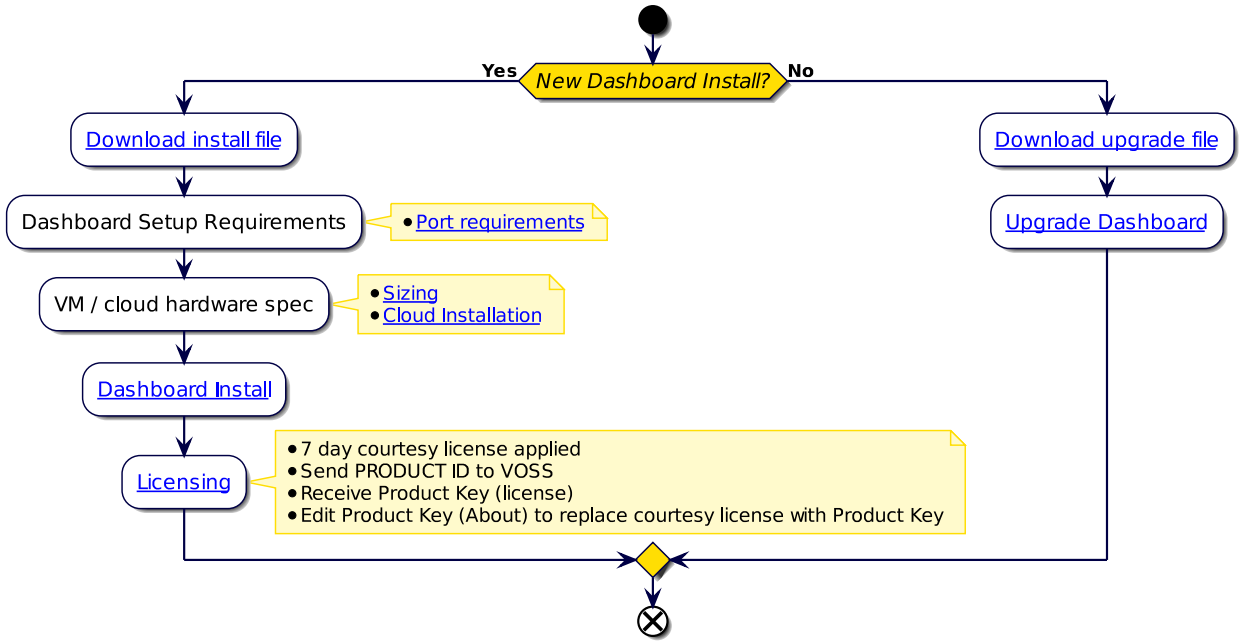
  Added details on the new virtual machine platform support in Automate: Hyper-V and Nutanix

2. Insights Analytics Quickstart

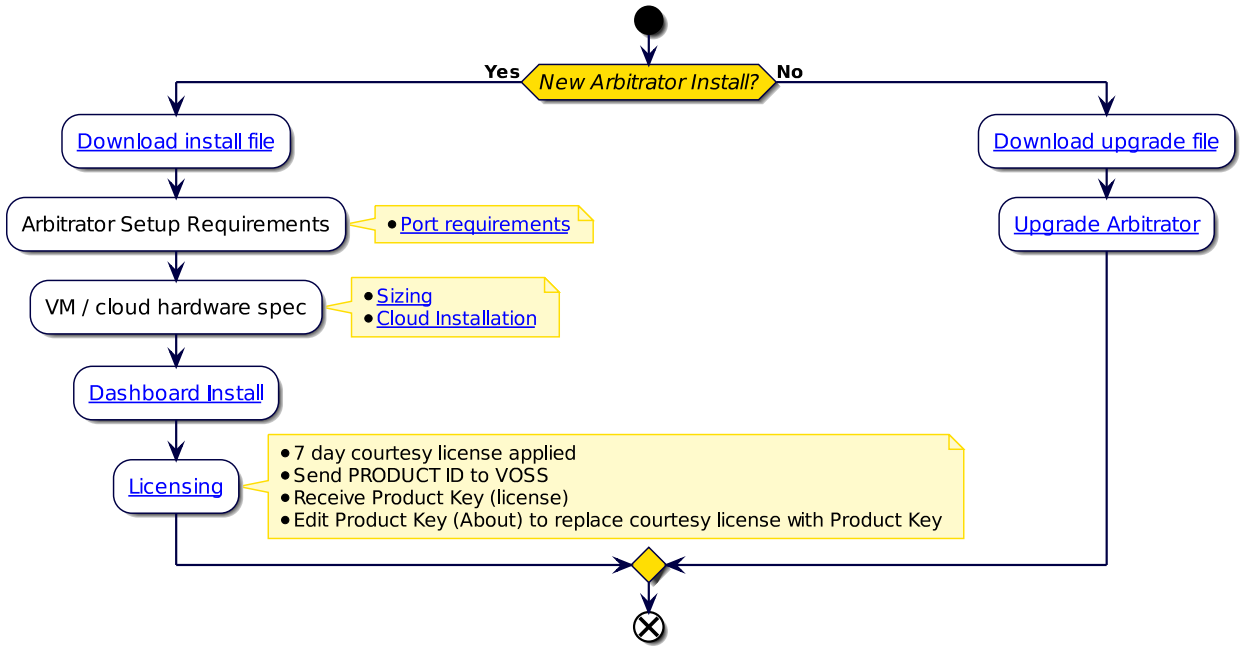
2.1. Insights Analytics Setup Overview



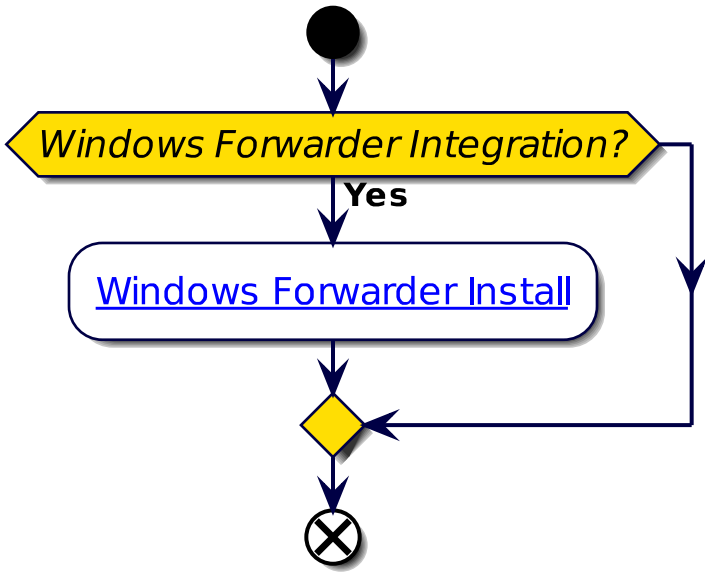
2.2. Dashboard Setup



2.3. Arbitrator Setup



2.4. Dashboard Integrations



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:
  1. Log in on the VOSS Customer Portal
  2. Go to **Downloads > VOSS Insights > Insights Dashboard > <release number> > Upgrade**.
  3. Download the `.lxsp` upgrade file.
  4. Verify that the original `.sha256` checksums on the download site server match.

     system checksum media/<lxsp_file>

     `Checksum: <SHA256>`

4. Virtualization and hypervisor platforms

4.1. 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

4.2. VMWare Esxi 8

4.2.1. 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.

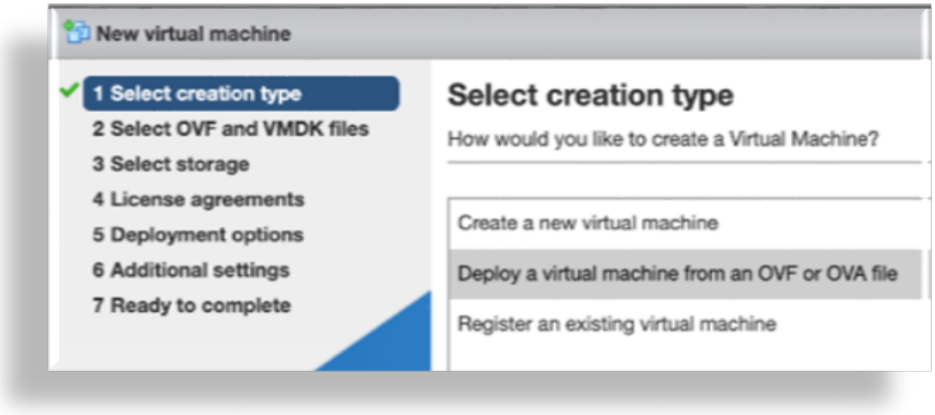
Download OVA

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.

4.3. 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.

4.3.1. 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`

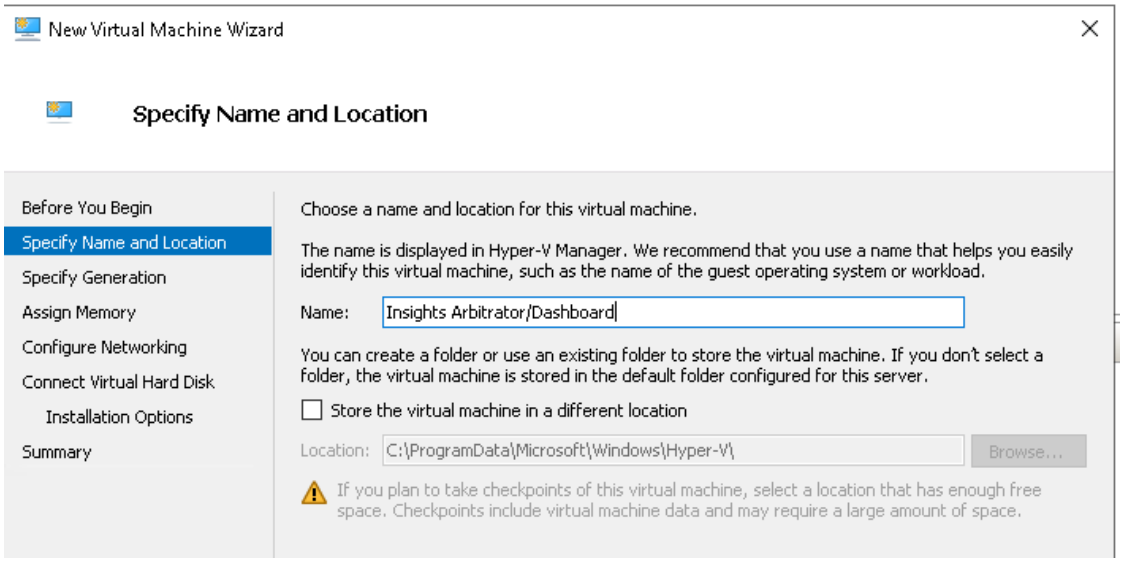
containing the `.vhd` file

4.3.2. Prepare the OS Disk

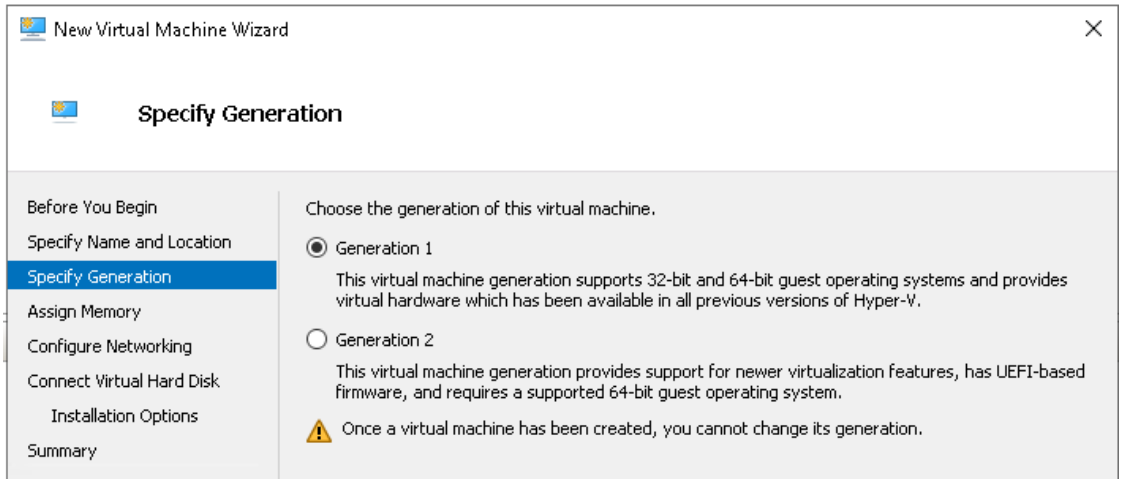
- Copy the `.vhd` to the Hyper-V Settings/Virtual Hard Disks location of your choice.
- Rename it to your own requirements.

4.3.3. Create the VM

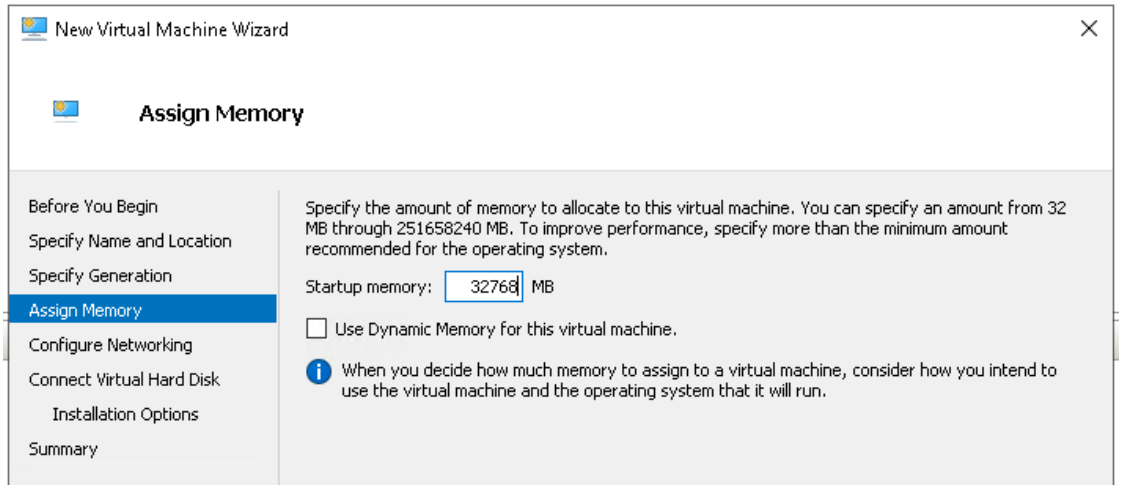
1. In Hyper-V Manager, go to **New > Virtual Machine**.
2. **Specify Name and Location**: Assign a suitable name to the VM.



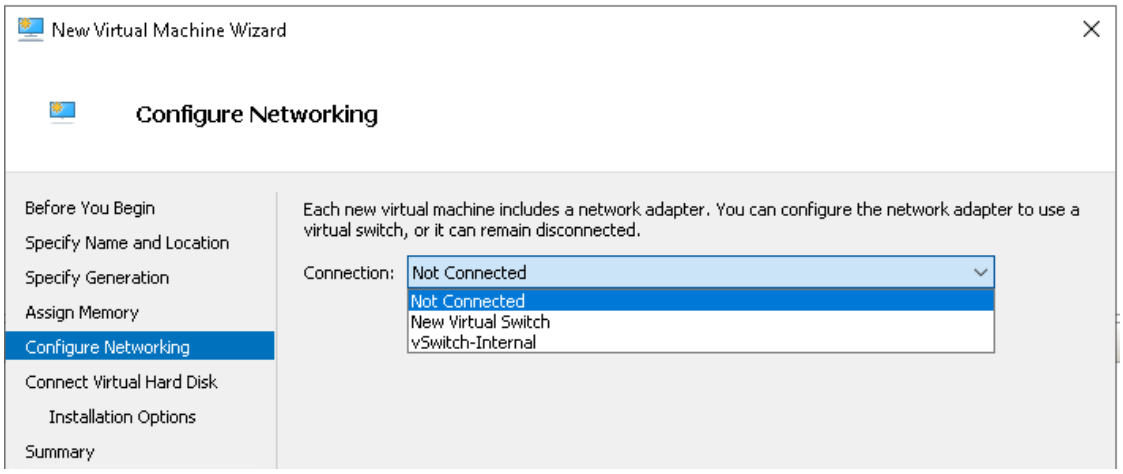
3. **Specify Generation:** Select Generation 1



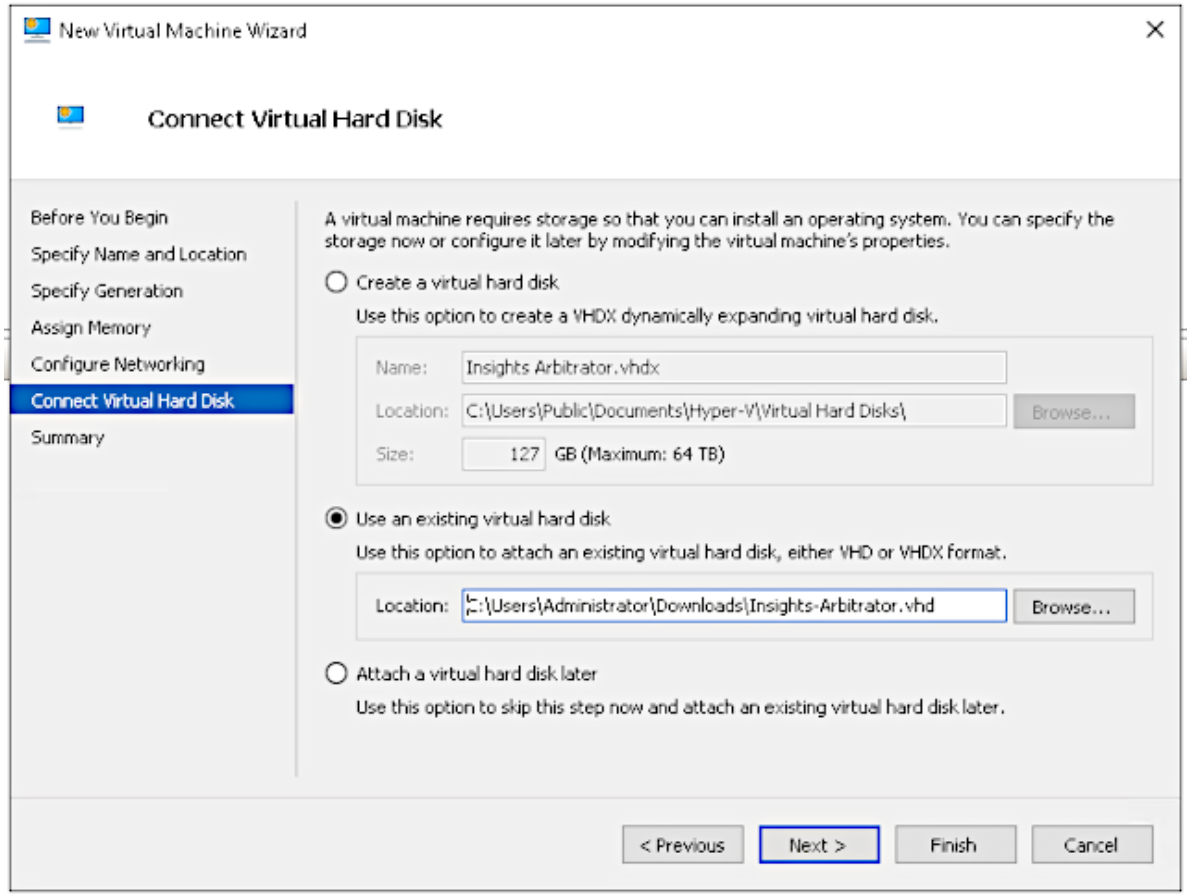
4. **Assign Memory:** Set the Startup memory according to the documentation



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



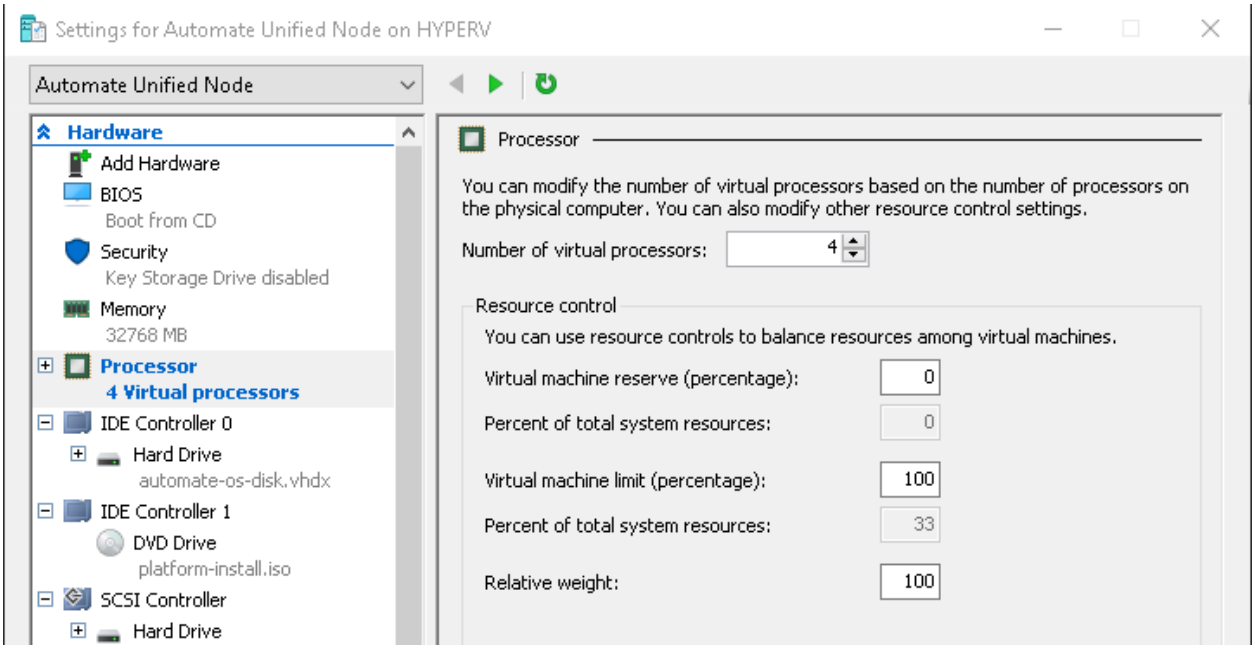
- Click **Finish**.

4.3.4. Configure the VM

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

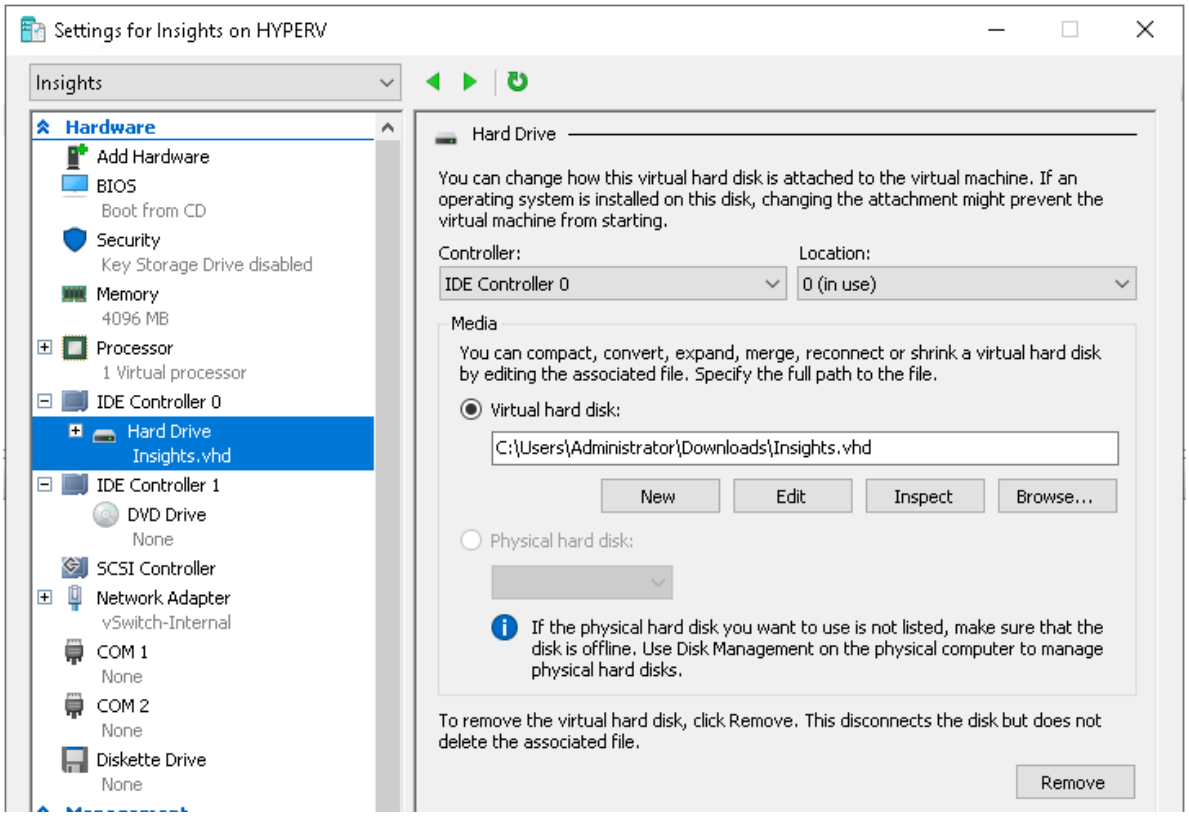
Configure the total processors

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

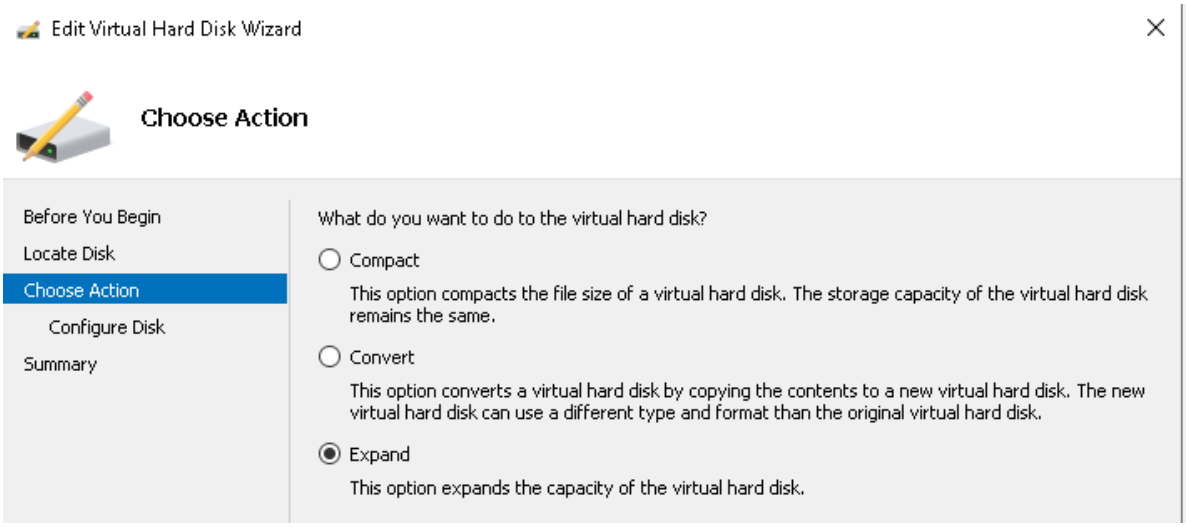


Resize the OS Disk and Data Disk (DS9 only)

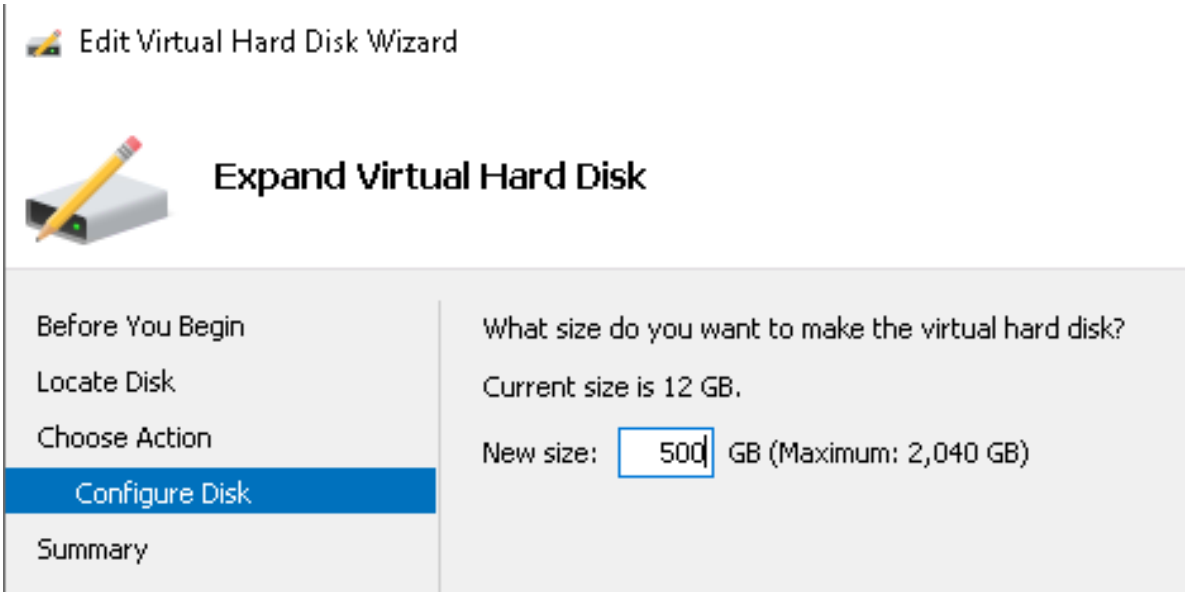
1. Under **IDE Controller 0** in the left pane, select the **Hard Drive**, **Edit**



2. Select **Choose Action > Expand**



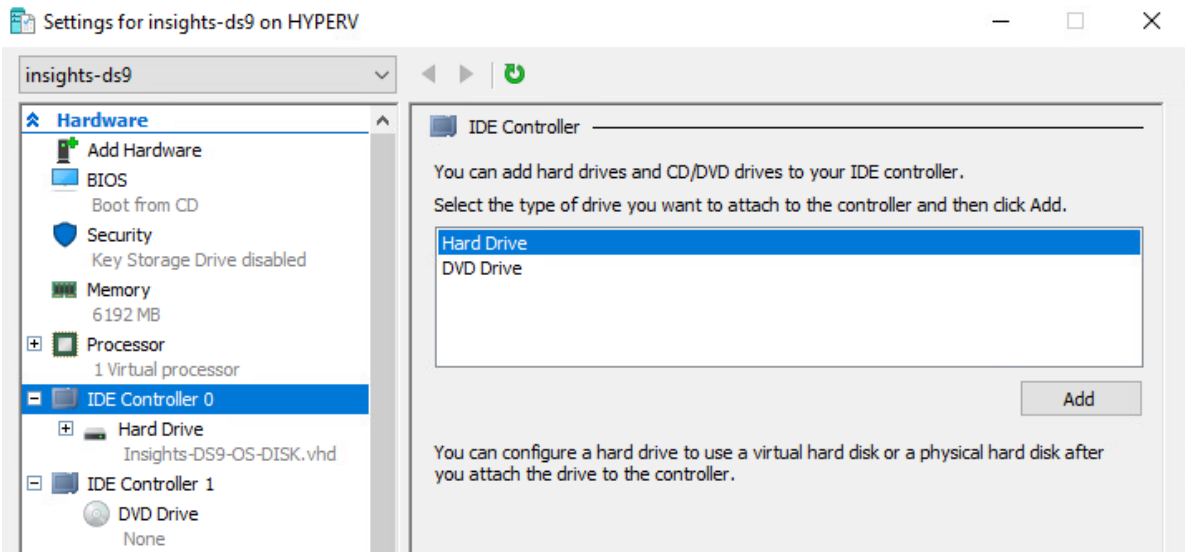
3. **Configure Disk**: Set the size according to the sizing specifications in the documentation.

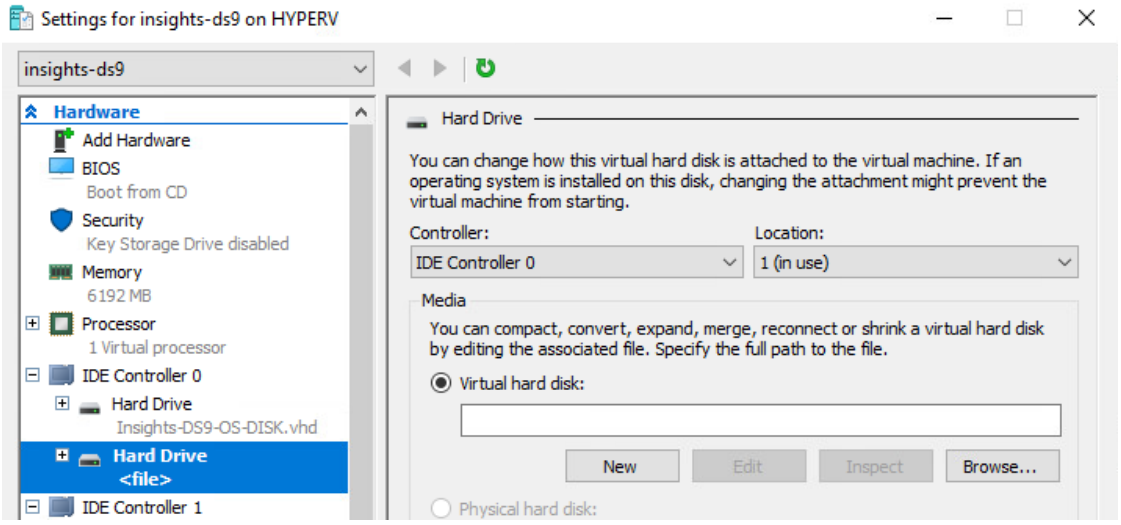


4. Click **Finish**.

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





4.3.5. Connect and start the Virtual Machine

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

4.4. 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.

4.4.1. Download the install file

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

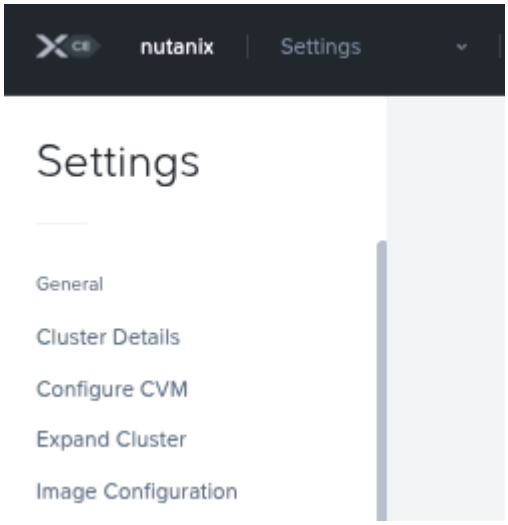
- `insights-<deployment>-<version>-nutanix.zip`

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

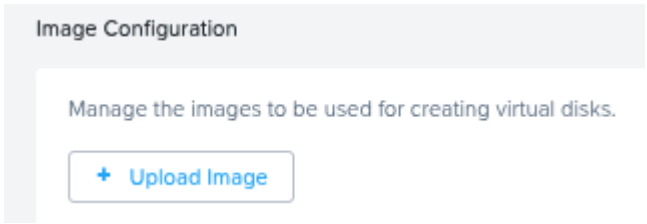
- `insights-<deployment>-<version>-nutanix.raw`

4.4.2. 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**

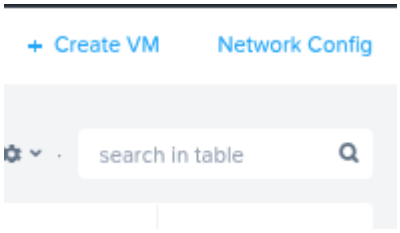


3. File in:

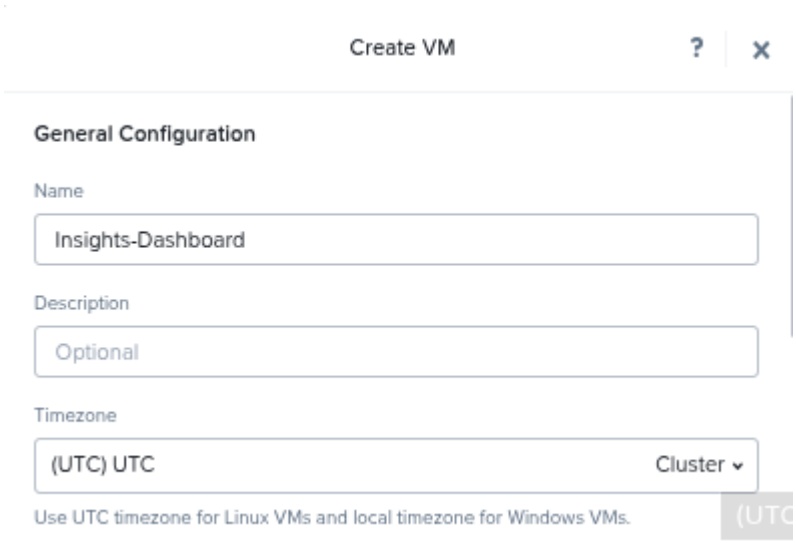
- **Name**: Name the image accordingly - e.g. `insights-dashboard-nutanix.raw`
- **Image Type**: `Disk`
- **Storage Container**: Select the required Storage Container
- **Image Source**: Either `URL` or `Upload a file`
- View the tasks to see the progress of the image creation

4.4.3. Create the VM

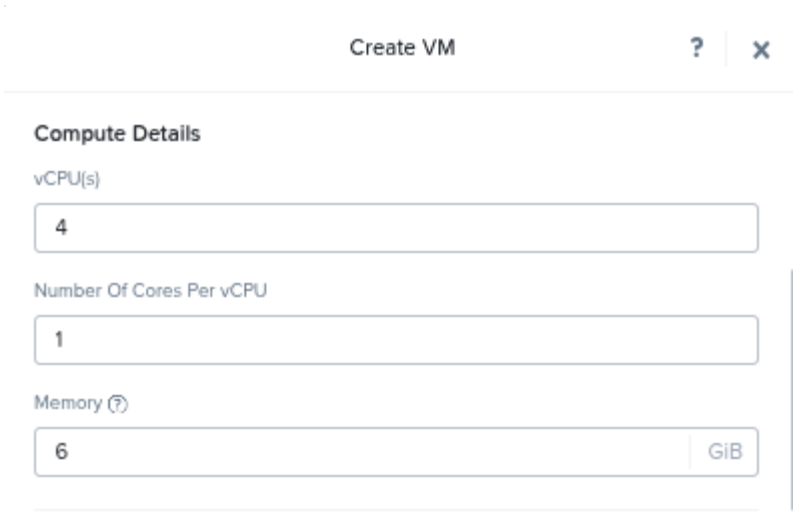
1. Select **VM** from the drop down menu top left, then the **Table** tab.
2. Click **Create VM** at the top right



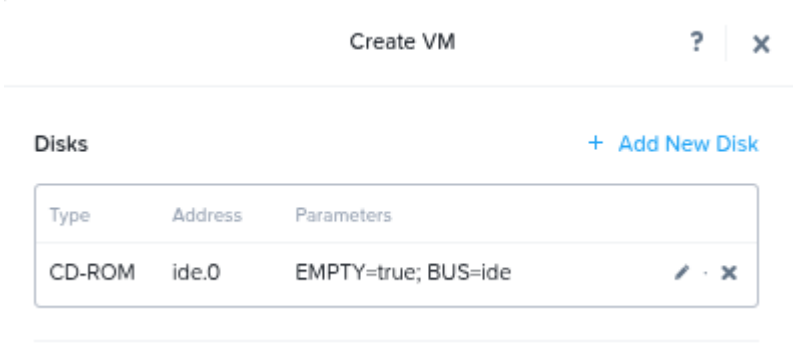
3. Give the VM a name



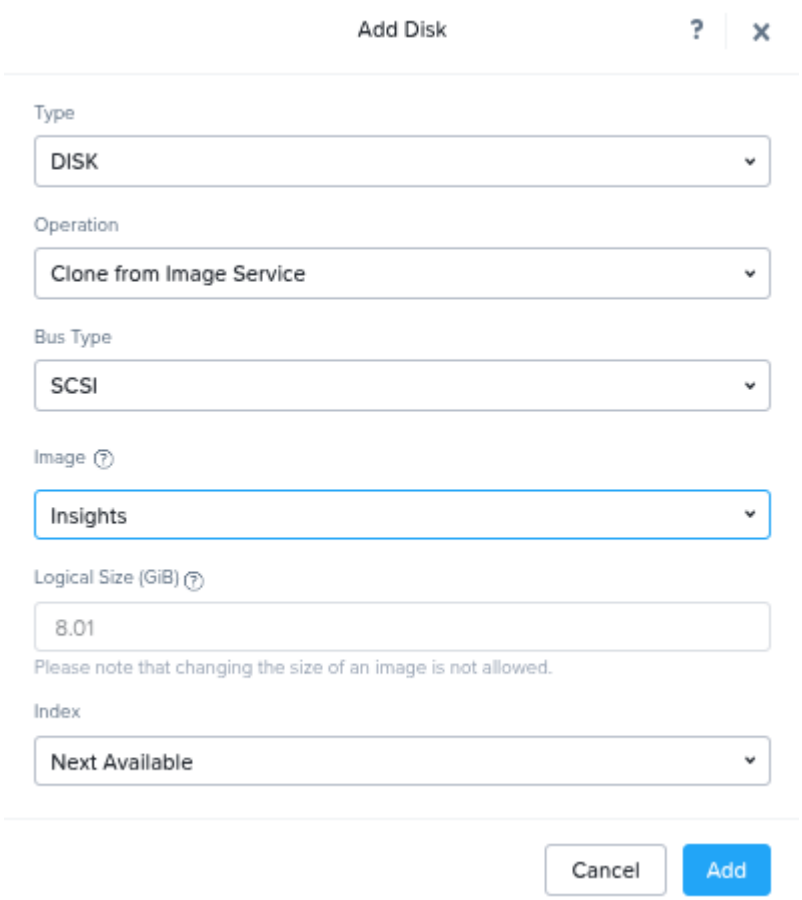
4. Set the CPU and RAM according to the documentation.



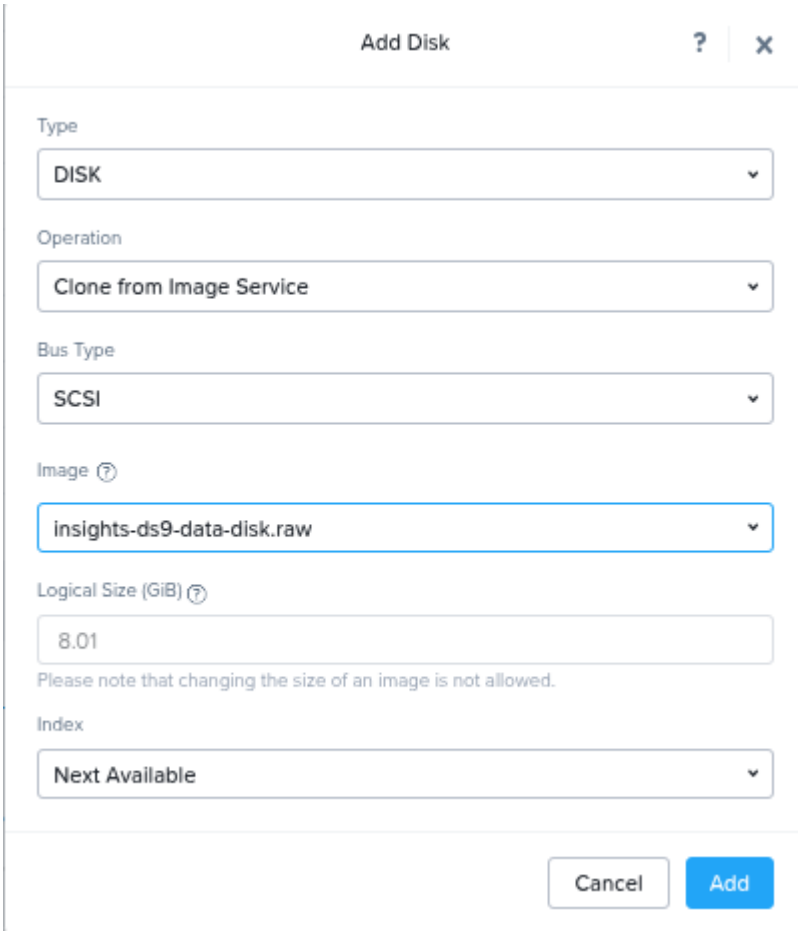
5. Add the OS Disk



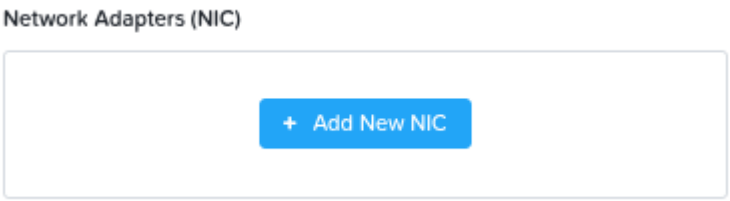
- **Type**: `Disk`
- **Operation**: `Clone from Image Service`
- **Bus Type**: `SCSI`
- **Image**: Select the image / raw disk uploaded in previous step
- Click **Add**



6. Add the Data Disk (DS9 Only)



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



4.4.4. 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

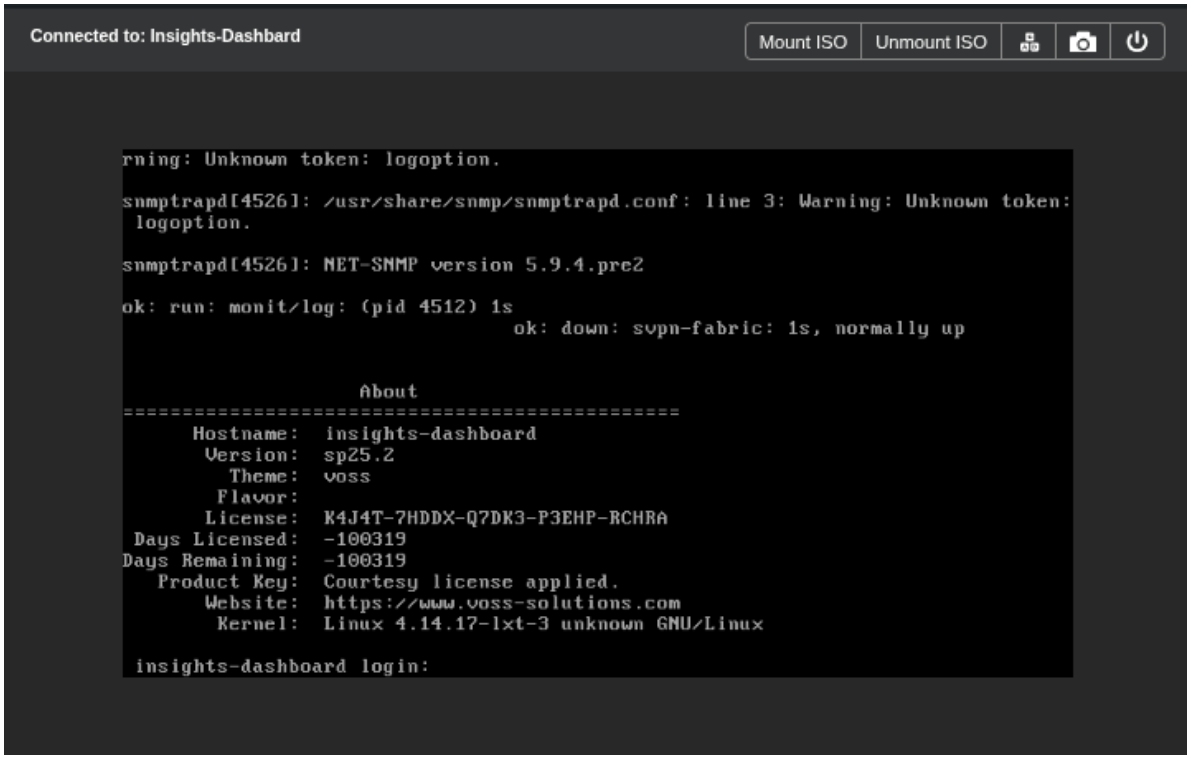
- Select **VM** from the drop down list top left
- From **Table**: Select the VM

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**.

4.4.5. 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**



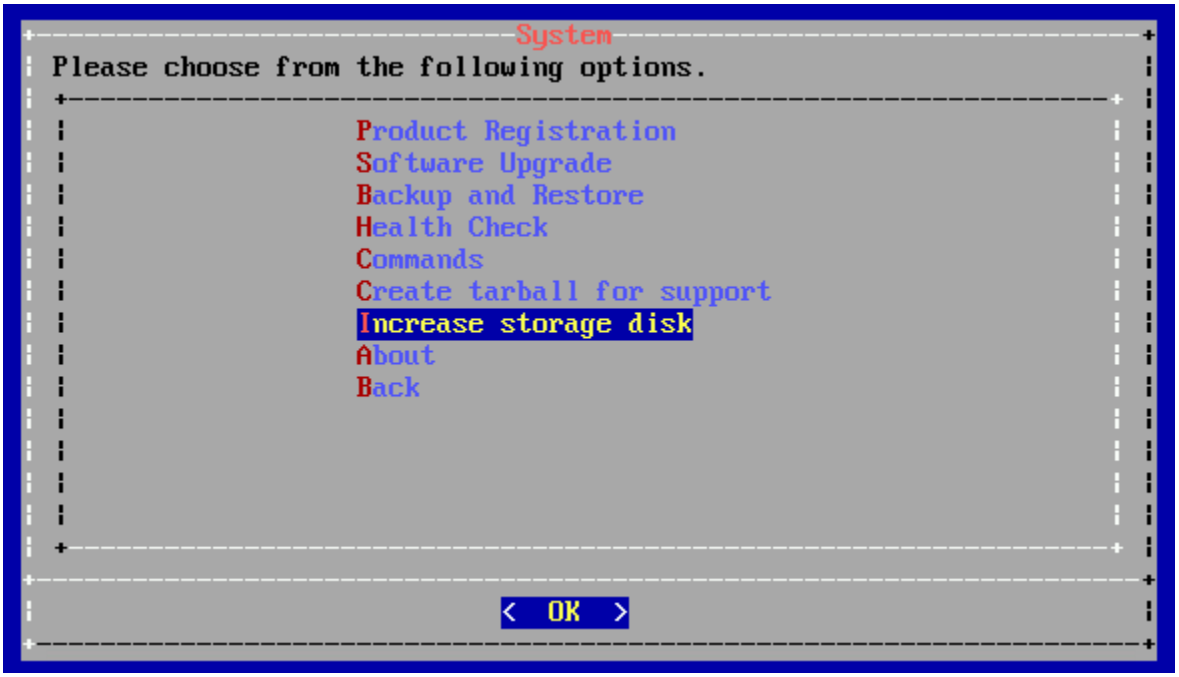
3. Log in via the `admin` account

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

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

4.4.7. Update the Data Disk Size (DS9)

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



5. VM Specification and Requirements

5.1. 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.

5.2. Cloud installation

The VM 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

6. Ports

6.1. Ports, protocols, and access rights

6.1.1. Overview

This topic details the ports, protocols, and access rights (including login and permissions) required for Insights to interact with assets and to monitor and collect analytics data. The topic has the following sections:

- *Ports*
- *Permissions*

6.1.2. Ports

Source: UC assets/devices

The table describes the destinations, protocols, and ports for various UC assets/devices sources required for Insights to interact with assets and to monitor and collect analytics data:

Source	Destination	Protocol	Port
UC Assets/Devices			
Cisco UC / CUBE (Syslog, CDR/CMR)	Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	TCP/UDP	22, 514
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Cisco UC / CUBE (AXL, SNMP query, and SSH)	TCP/UDP	22, 161, 162, 443, 8443
Cisco UCCE (CVP, Finesse, CUIC, VVB, PG/HDS/Roggr/Logger) (SNMP traps)	VOSS Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	TCP/UDP	161, 162
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Cisco UCCE (CVP, Finesse, CUIC, VVB, PG/HDS/Roggr/Logger) (read-only SNMP query)	TCP/UDP	161, 162
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Cisco UCCE (Finesse) (read-only API query)	HTTPS	8443, 443
Cisco Analog Gateways (SNMP trap)	Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	UDP	161, 162
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Microsoft Teams	HTTPS, Graph API	443
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Cisco WebEx Calling DI	HTTPS, AXL API & RIS API	443
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	AudioCodes Mediant Session Border Controllers (SNMP query, API)	TCP/UDP	161, 162, 443
AudioCodes Mediant Session Border Controllers (SNMP traps)	Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	UDP	161, 162

Source: Other applications

The table describes the destinations, protocols, and ports for various other applications (non-UC assets/devices sources) required for Insights to interact with assets and to monitor and collect analytics data:

Source	Destination	Protocol	Port
Other Applications			
Insights Dashboard Server (Cloud)	Microsoft Active Directory LDAP Server	LDAPS	TCP 636
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Microsoft Active Directory LDAP Server	LDAPS	TCP 636
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	Mail Server (SMTPS)	SSL/TLS	TCP 465/587
Insights Arbitration servers (on-premises in Equinix DC EU, APAC, AMER)	ServiceNow	HTTPS	TCP 443

6.1.3. Permissions

The table describes applications and their access rights (including login and permissions) required for Insights to interact with assets and to monitor and collect analytics data.

Application	Permissions
Cisco UC / CUBE / Cisco WebEx DI	Configure the appropriate Cisco UC device: • To forward SNMP trap to the local Insights Arbitration servers • Syslog settings to direct log messages • Forward CDR to the local VOSS Insights Arbitration servers • Create SNMPv2 or SNMPv3 connection string • System user with read-only access and Standard AXL API Access role
Cisco UCCE	Create a system user on UCCE Finesse to enable Insights to execute Finesse API. The role that is applied to the system user should include: • “Read Only Agent Data” • “Read Only Queue Data” privileges
Cisco Analog Gateways	Forward SNMP trap to the local Insights Arbitration servers
AudioCode Mediant eSBC	Configure the appropriate eSBC device: • To forward SNMP traps to the local Insights Arbitration servers • Create SNMPv2 or SNMPv3 connection string • Syslog settings to direct log messages • Read-only System user with API access for system monitoring

Application	Permissions
Microsoft Teams	The following credential info is required: a. Application (client) ID b. Directory (tenant) ID c. Client secret Value The following permissions need to be granted for the application: • AuditLog.Read.All • CallRecord-PstnCalls.Read.All • CallRecords.Read.All • Device.Read.All • DeviceManagementApps.Read.All • DeviceManagementConfiguration.Read.All • DeviceManagementRBAC.Read.All • DeviceManagementServiceConfig.Read.All • Directory.Read.All • Group.Read.All • GroupMember.Read.All • Organization.Read.All • OrgSettings-Microsoft365Install.Read.All • OnlineMeetings.Read.All • Reports.Read.All • ServiceHealth.Read.All • ServiceMessage.Read.All • Team.ReadBasic.All • TeamsActivity.Read.All • TeamSettings.Read.All • TeamworkAppSettings.Read.All • TeamworkDevice.Read.All • TeamworkTag.Read.All • User.Read.All • User.ReadBasic.All • VirtualEvent.Read.All

Application	Permissions
SMTP server	A dedicated service account to be utilized by Insights with the following minimum necessary permissions to: • Send Email • Relay Access (if applicable) • Send As/On Behalf Of (optional but recommended for improved security) • Create a user group that the mail can be sent to.
ServiceNow	A dedicated service account with a role like: `rest_service` **Note:** These are the minimum permissions required. Additional permissions may be required based on specific use case.

6.2. Arbitrator and Dashboard system connectivity

This table includes connectivity requirements between Insights Arbitrator, 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	443, 5432, 5000, 60514, 64514, 64515, 65515, 65516, 64005, 64004, 62009, (all TCP)	Intra-system communication and queries - Bi-directional
Arbitrator Server	Arbitrator Server	62002, 62003, 62004, 62005, 62006, 11501,30501, 30503, 40501, 40503 (all TCP)	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

Note: LDAP ports: 389 and 636 for TCP/UDP are not available for the Arbitrator and Dashboard server. If these ports are required for Dashboard server communication, refer to the configuration settings for LDAP in

the **Configuration** chapter the *Dashboard Administration Guide*.

6.3. 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

6.4. MS Teams System Connectivity

Source	Destination	Port / protocol	Notes
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
Arbitrator	Microsoft (https://graph.microsoft.com/v1.0)	443 TCP	The Arbitrator pulls the full call record details directly from Microsoft, using the https://graph.microsoft.com/v1.0 API.

6.5. Netflow and DS9 monitoring system connectivity

6.5.1. 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

6.5.2. 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)

6.5.3. 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	514	Unidirectional	DS9 Dynamic Mapping Updates

6.5.4. 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

6.6. 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

6.7. 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

7. Deploy and Networking Setup

7.1. Deploy and VM installation

7.1.1. Deploy the installation on the VM

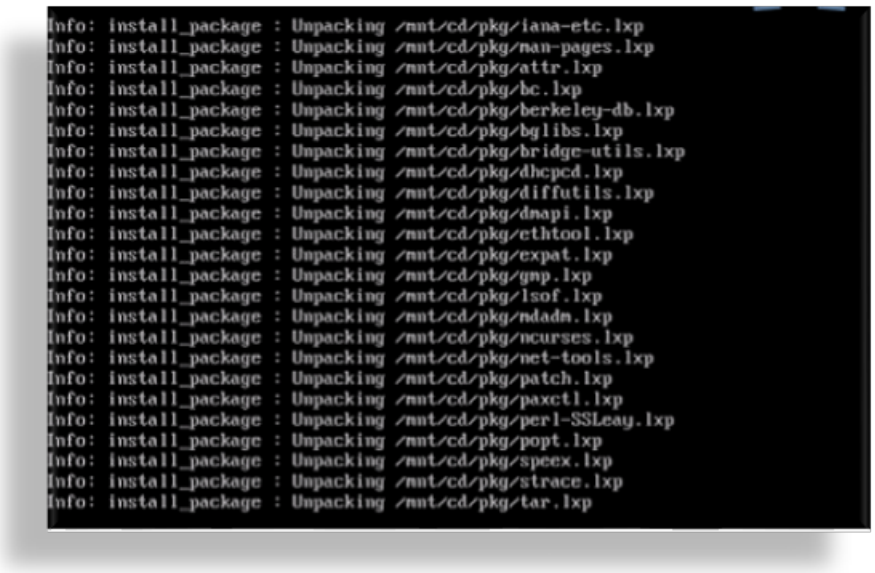
See: *Supported virtualization and hypervisor platforms*

Select virtualization platform:

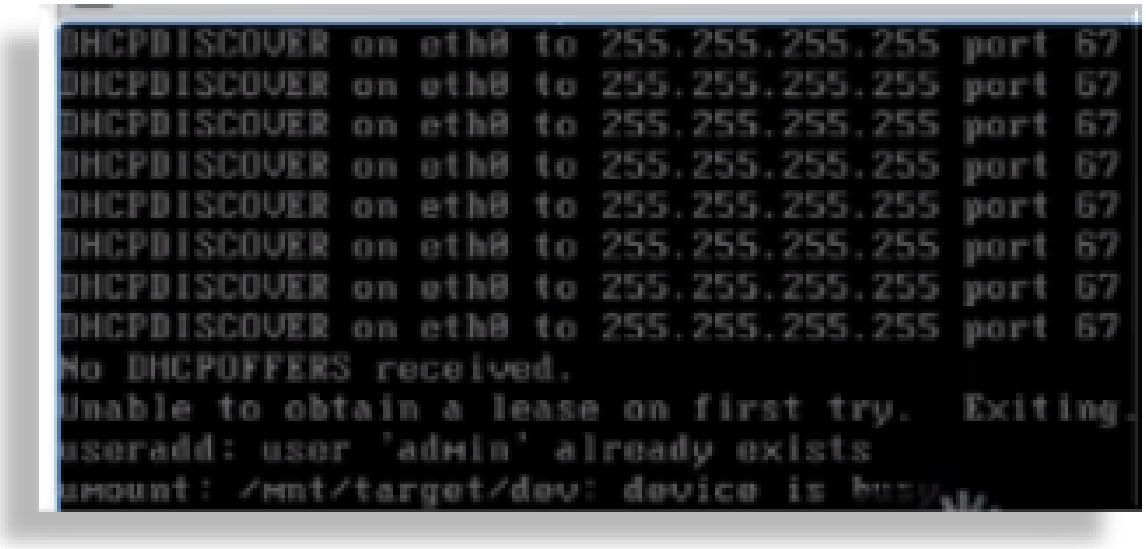
- *VMWare Esxi 8*
- *Hyper-V*
- *Nutanix*

7.1.2. 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:
```

7.1.3. 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.

7.1.4. 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.

---

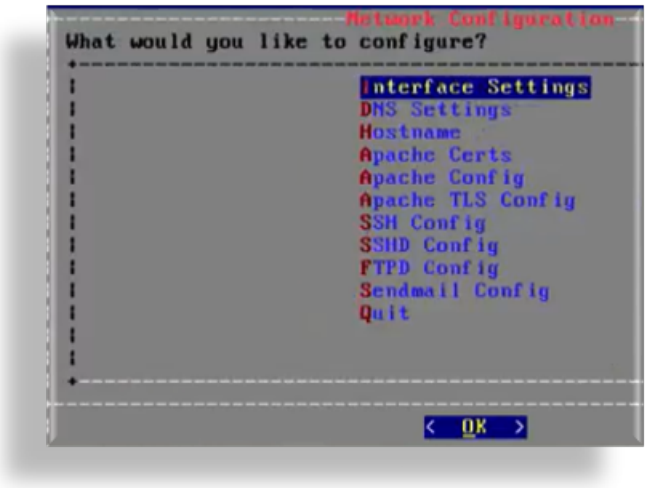
1. On the **Administration** menu, select **Change Passwords**.

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

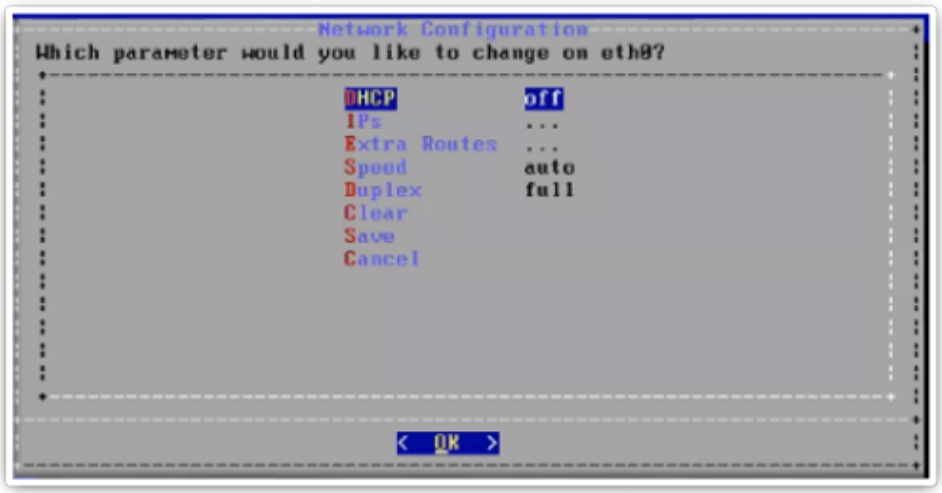
> **Important:** It is strongly recommended that you make a written or digital copy of any system passwords and share the copies with trusted team members or store them in a secure location from where they may be retrieved if needed.

7.1.5. Configure network settings

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

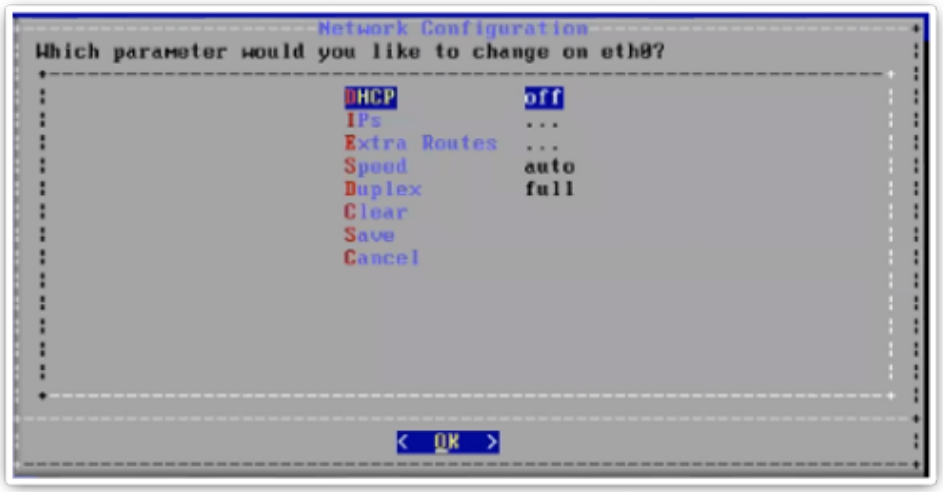


2. Configure interface settings:
   i. Select **Interface Settings**.
   ii. Select the relevant interface.

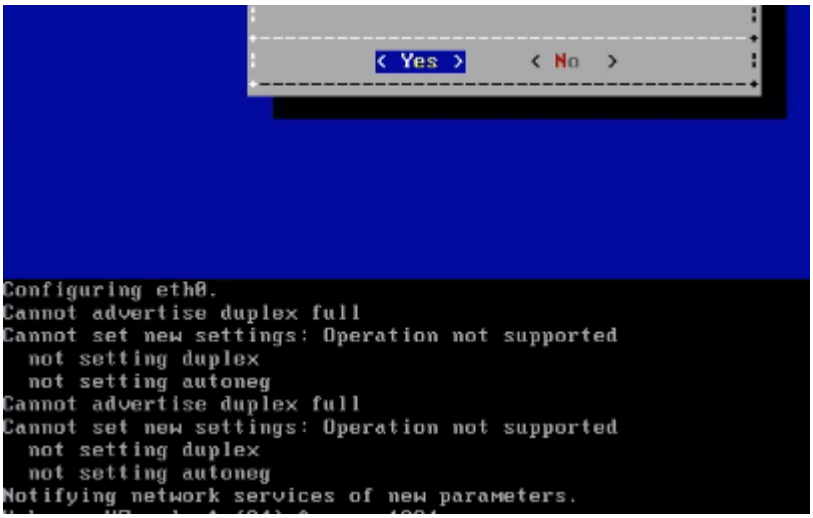


   iii. Select **IPs**. Set the IP address and netmask in the format `nn.nn.nn.nn/24`. Click **OK**.

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



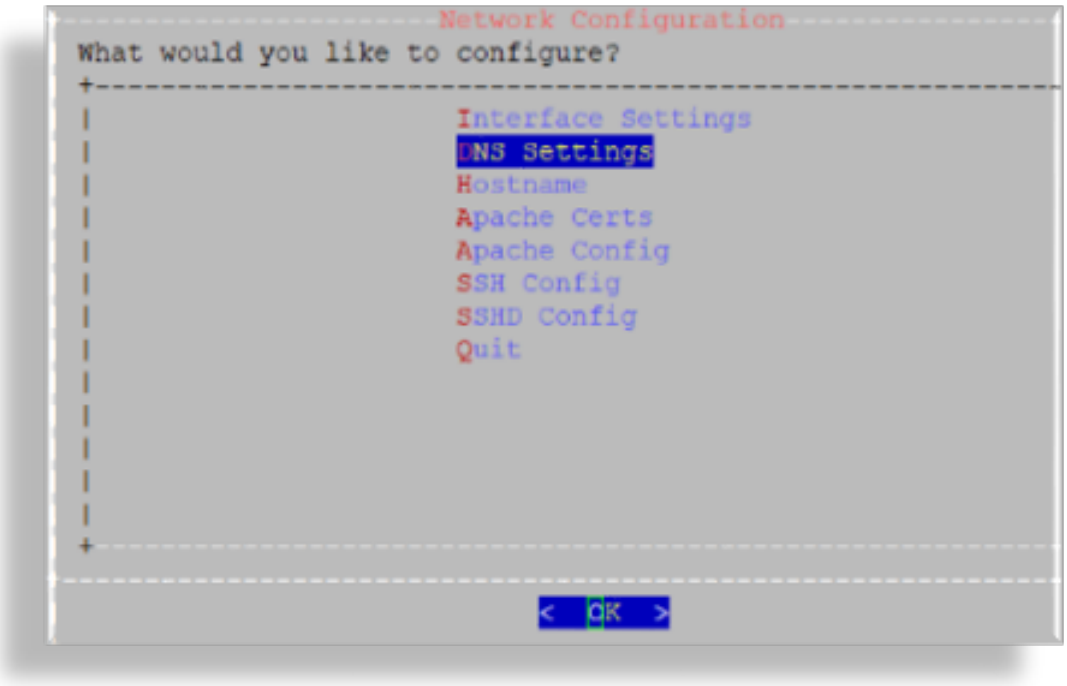
- Use the following format for the entry: *default <gateway IP address>*
- The word *default* is required. For additional route entries use the *<subnet> < gateway>* format. Similar to what would be done on a Linux system at the CLI.



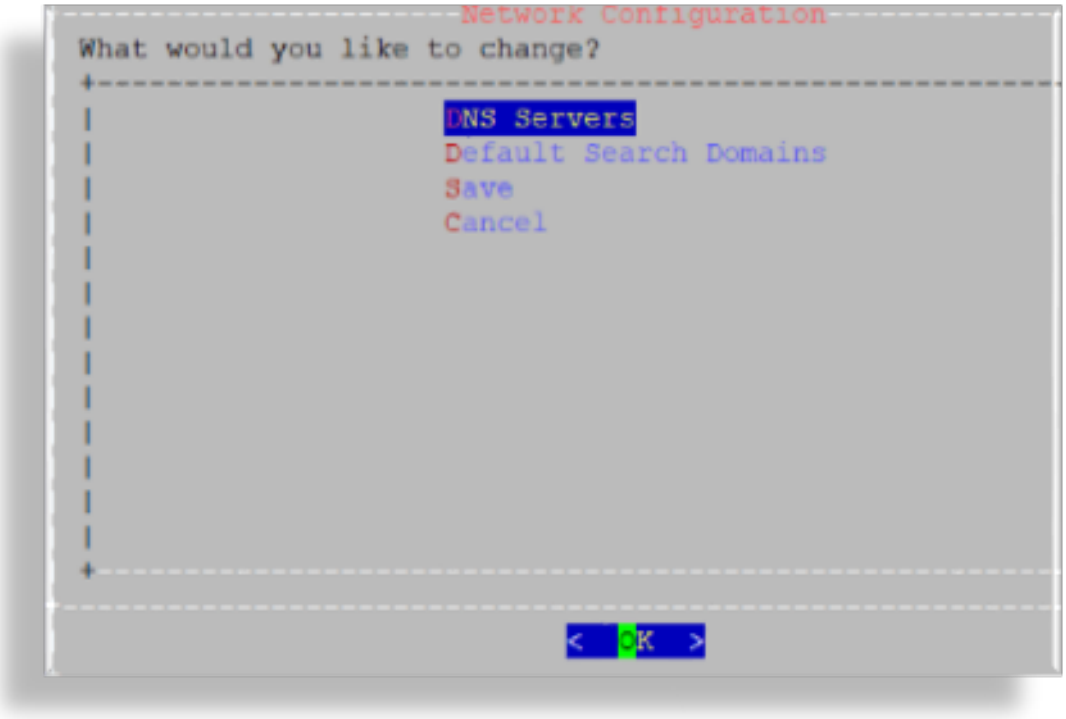
v. Save your changes.

3. Configure DNS settings:

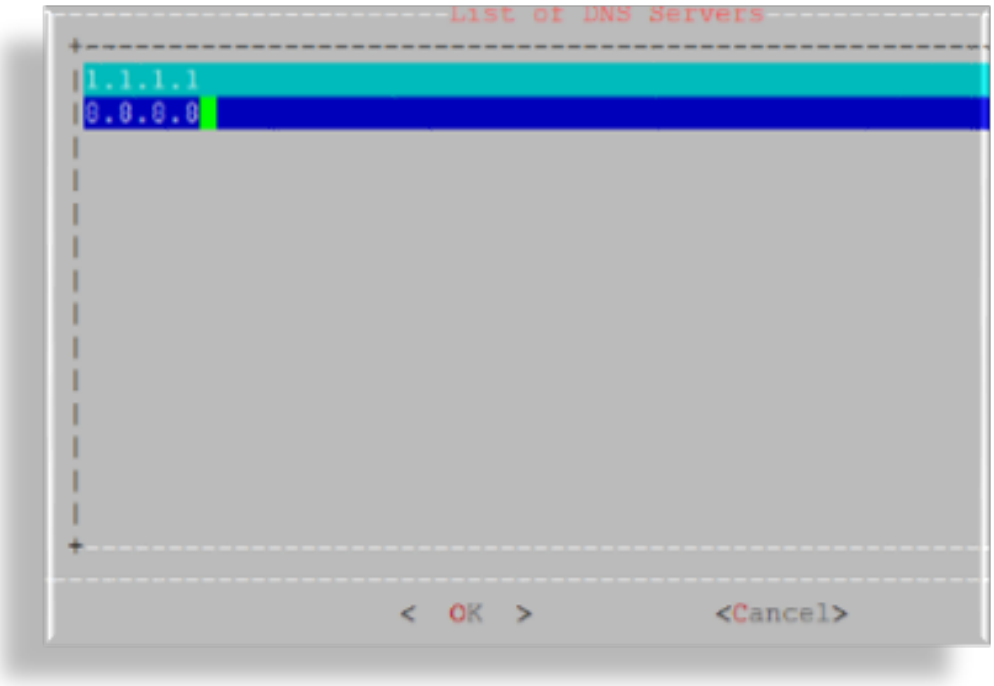
i. Select **DNS Settings**



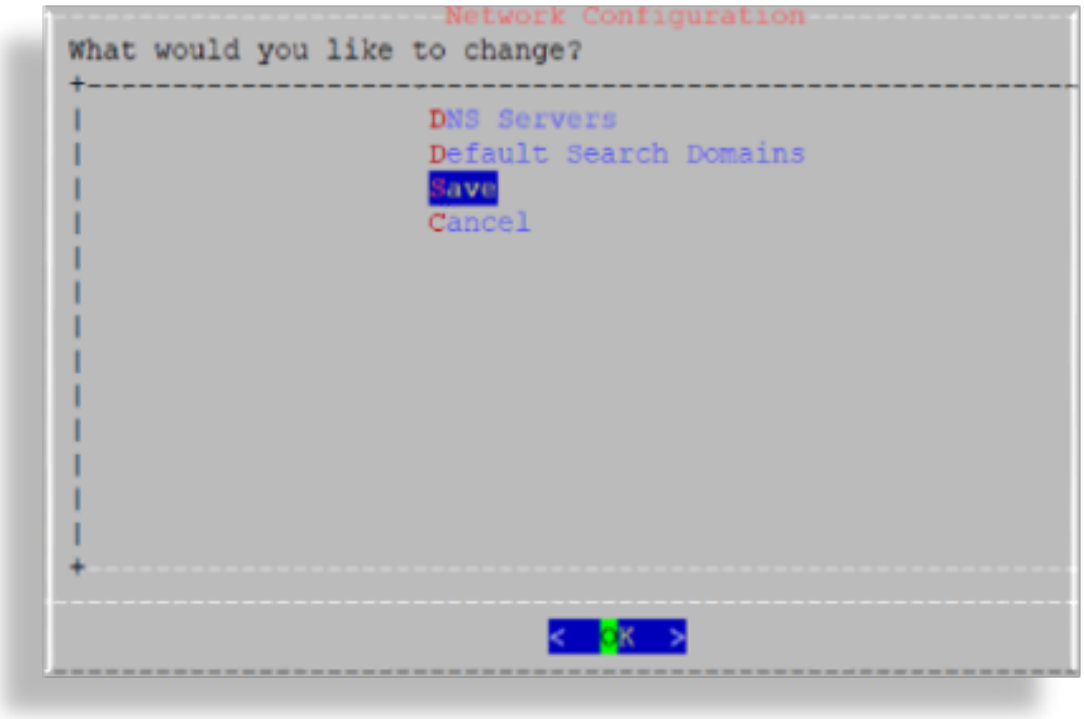
ii. Select **DNS Servers**.



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

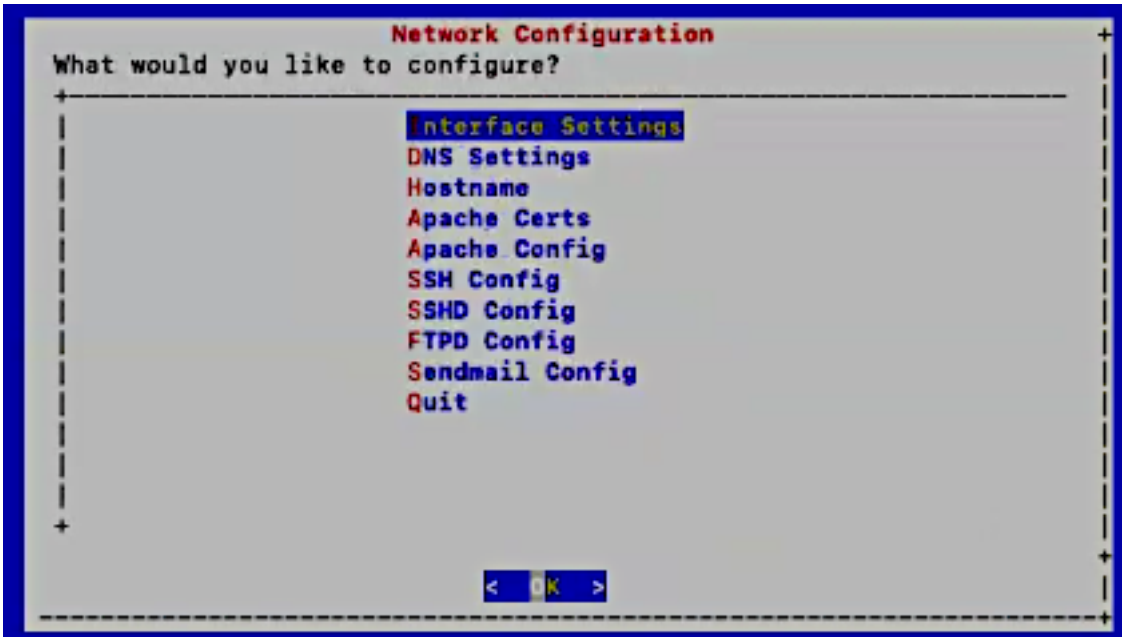


iv. Click **Save**.



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.



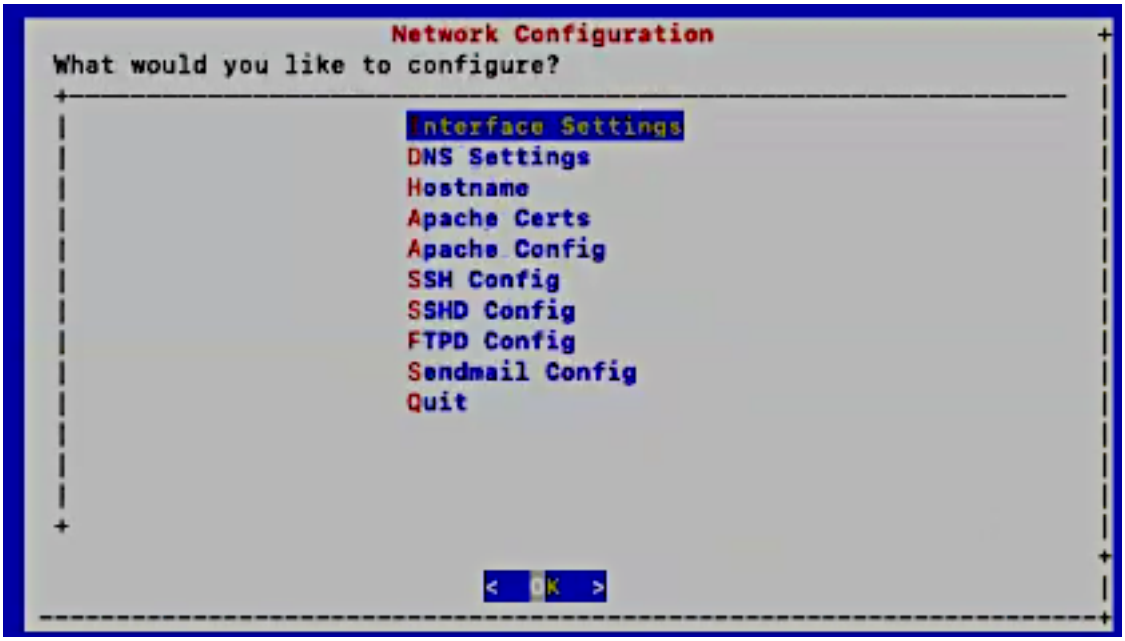
5. Update SSL ciphers.

    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.

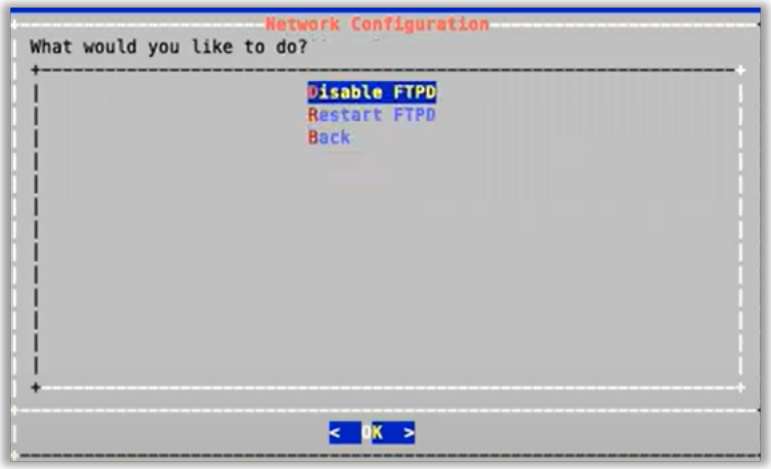
7. Configure SSHD:
   i. Select **SSHD Config**.

   Note:

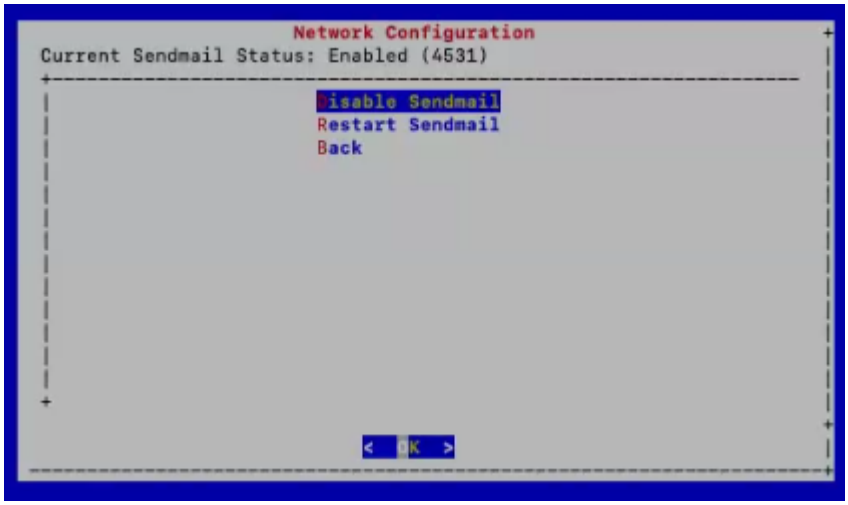
   - Multi-line entries can be added, if required. For example, for CUCM v11.5 support, see: *Configure multi-line CUCM cipher support*.
   - This step is relevant *only* to an Insights Assurance solution and its integration with Cisco UC systems. This step is *not* relevant to the DS9 and Insights NetFlow 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*

7.1.6. 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*

7.1.7. 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.

7.1.8. 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).

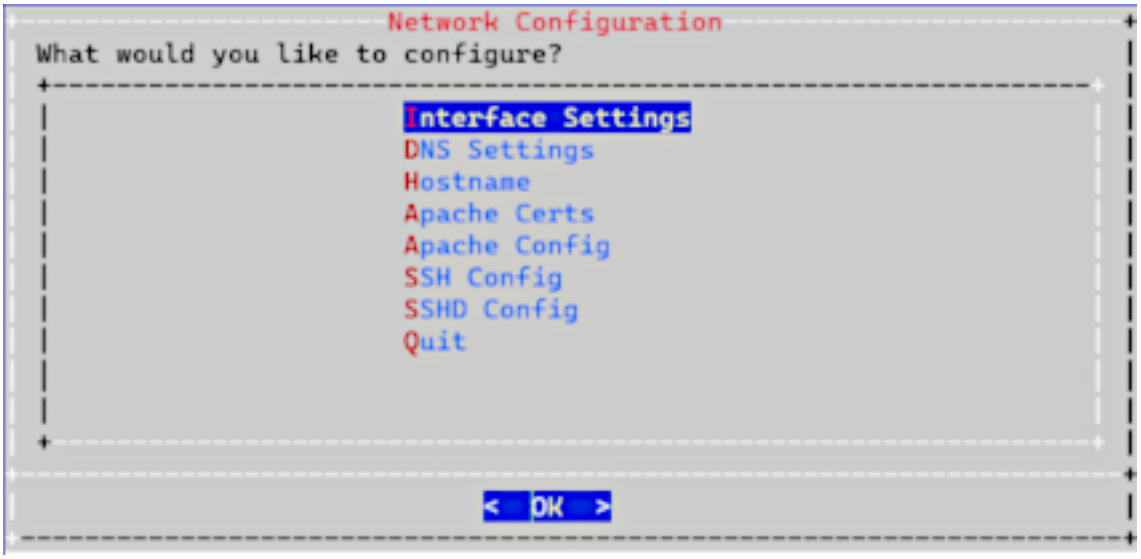
For CUCM v11.5 support:

```
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
```

8. Certificates

8.1. Add or update certificates

Users can now update SSL certificates and SSL keys from the Admin console menu.



Note: If vulnerability testing yields “Weak hashing Algorithm” and “Self-Signed Certificate” issues, these can can be fixed by installing your own SSL certificate.

8.1.1. Add certificates

To add your own certificate, you will need both the certificate and private key.

1. SSH to the system using admin account
2. Select **Network Configuration**
3. Select **Apache Certs**
4. Select **Insert Cert**
5. Paste in customer certificate

   A certificate has the following headers and footers:

```
EXAMPLE:
-----BEGIN CERTIFICATE-----
MAIN SERVER CERTIFICATE
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
INTERMEDIATE CERTIFICATE
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
ROOT CERTIFICATE
-----END CERTIFICATE-----
```

Error checking and solutions:

- `Error 20 at 0 depth lookup:  unable to get local issuer certificate`

  The server certificate needs an intermediate certificate to validate. Add the intermediate certificate after the server certificate.

- `Error 2 at 1 depth lookup:  unable to get issuer certificate`

  The server certificate needs the root certificate to validate. Add the root certificate after the intermediate and or server certificate.

- ```
  Error loading file /etc/apache2/server.crt.tmp
  error:05800088:x509 certificate routines unknown function):
  no certificate or crl found:crypto/x509
  ```

  No certificate; invalid format; or blank.

6. Select **Insert Private Key**.
7. Paste in customer private key.

   A private key has the following header and footer
  ```

```
--BEGIN PRIVATE KEY--
--END PRIVATE KEY--
```

8. Select **Display Cert Details** to view certificate details.
9. Select **Back**, then exit the menu.
10. Refresh the browser. The system should be using the new certificate.

8.1.2. Generate a CSR from an existing certificate

If you want to generate a CSR for the current certificate:

1. SSH to the system using admin account.
2. Select **Network Configuration**.
3. Select **Apache Certs**.
4. Select **Generate Cert**.
5. Press **Enter**. The CSR displays on the screen.
6. Copy and save it.
7. Select **Back**, then exit the menu.
8. Refresh the browser. The system should be using the updated unsigned certificate.

8.1.3. Create new certificates

If you want to generate a new unsigned certificate or to reset a certificate and private key:

1. SSH to the system using admin account
2. Select **Network Configuration**
3. Select **Apache Certs**
4. Select **Generate New Unsigned Cert**
5. When prompted, fill in the information requested.

- For `the number of days the certificate should be valid. (default 365):`, the value should be a positive number from 1 to 3650.

  Publicly Trusted Certificates: For certificates that need to be trusted by web browsers like Chrome, Firefox, or Safari, the maximum validity period is currently 398 days. This is a policy set by the CA/Browser Forum to enhance security by encouraging more frequent certificate renewals and updates.

  Self-Signed Certificates: When you are using OpenSSL to create a certificate for a private network or for testing purposes, you can set a much longer validity period. The tool itself does not prevent you from setting a very high number of days, but you may run into issues with the system's date and time representations (e.g., the Year 2038 problem on 32-bit systems).

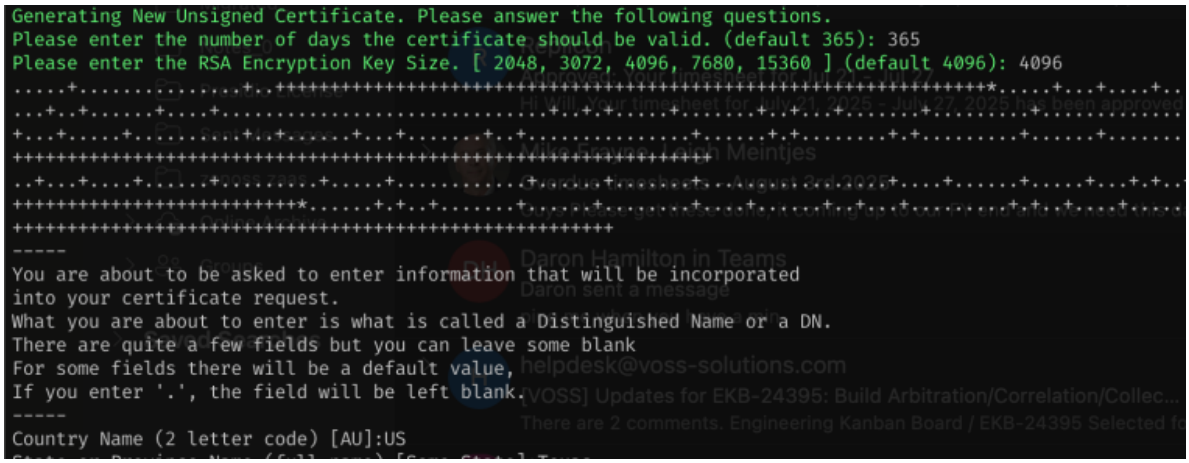
- The default RSA Encryption Key Size is 4096.

  If the check: `Info: Checking modulus of the Certificate and Private Key.` returns with an error: `Error: Certificate and Private Key DO NOT MATCH`, the possible reasons could be:

  – Either wrong certificate uploaded.

  – Private key not uploaded.

  Then generate new unsigned certificate, which will generate a new key and certificate. |




```
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]: Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

6. Select **Back** and exit the menu.
7. Refresh browser. The system should be using the new unsigned certificate.

Index

F