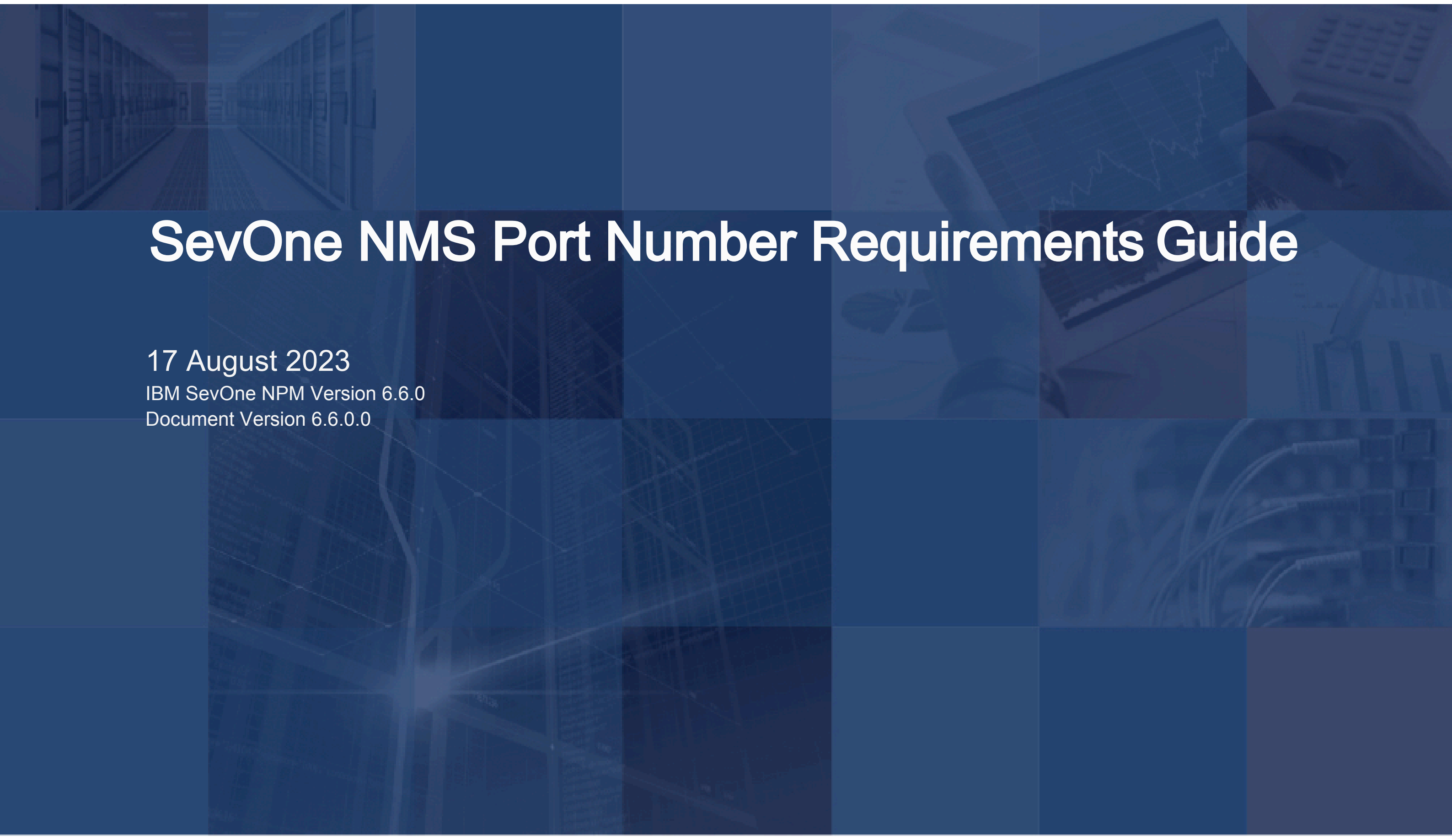

SevOne NMS Port Number Requirements Guide

17 August 2023

IBM SevOne NPM Version 6.6.0

Document Version 6.6.0.0

Table of Contents

SevOne Documentation

All documentation is available from the IBM SevOne Support customer portal.

IN NO EVENT SHALL IBM, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF IBM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND IBM DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

1 About

SevOne peers communicate with each other to maintain a consistent environment. Each peer needs the following ports open between each other.

Encryption

Most ports use TLS as the **encryption** technology which can be negotiated based on the client and server configuration. Same is true for SSH. For some ports, the exact encryption method cannot be guaranteed. For example, SSL port 443 is based on the client's browser.

Terminology usage...

In this guide if there is,

- [any reference to *master*] OR
- [[if a CLI command contains *master*] AND/OR
- [its output contains *master*]],
  it means *leader*.

And, if there is any reference to *slave*, it means *follower*.

2 Peer Port Assignments

2.1 Minimum Ports Required for NMS Cluster Operation

The minimum port requirement is a list of ports required by PAS and/or Between Peers.

> ⓘ The port configured for communication with the WMI proxy must be opened in the firewall.

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
ICMP (*)	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers	Interpeer Monitoring ICMP from and to devices and Interpeer Monitoring
TCP 22 (*)	Y	SSH-based encryption - can be configured by an **admin** user.	-> PAS -> DNC -> HSA <-> Between Peers -> iDRAC -> Data Insight	SSH Access - remote login Required for SevOne Data Insight to update or Install Data Insight Reporting API (DIRA)
TCP 43	N	n/a	Any peer for out-going connections, two-way traffic	Used for Autonomous System (AS) name resolution in FlowFalcon reports. (*Optional*) This port is used only when user needs to resolve AS numbers to names.
TCP 80	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers -> Data Insight	HTTP, SOAP API, and AJAX Calls - End User Terminal UI port for Data Insight - Can be configured using environment variables. Data Insight uses port 80 to redirect any HTTP (80) requests to HTTPS (443)
TCP 389	N	n/a	PAS ->	LDAP (Clear text) Server port (not used for secure configurations)
TCP 443 (*)	Y	TLS-based encryption - can be configured by an **admin** user.	-> PAS -> DNC -> HSA <-> Between Peers	For Livemaps in REST API, the Cluster Leader and Peer use HTTPS on port 443. If the connection is unavailable, it falls back and uses HTTP on port 80.
TCP 443 (for AWS)	Y	TLS-based encryption.	-> AWS	For monitoring AWS services.
TCP 636	Y	TLS-based encryption.	PAS ->	LDAP (SSL) Server port
TCP 873	N	n/a	<-> Between Peers	RSYNC - Interpeer

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
TCP 3306 (*)	Y	TLS-based encryption.	<-> Between Peers	MySQL - Interpeer
TCP 3307 (*)	Y	TLS-based encryption.	<-> Between Peers	MySQL2 - Interpeer
TCP 4443	N	n/a	Local within one appliance	Alerting - Interpeer ⚠ • Port is open only to local (127.0.0.1) connections. • Only used internally and not across peers.
TCP 5050	N	n/a	Local within one appliance	SevOne-masterslaved - Interpeer ⚠ • Port is open only to local (127.0.0.1) connections. • Only used internally and not across peers.
TCP 5051	N	n/a	-> Export Destination	Raw Data Export - SevOne Raw Data Feed (optional for customer streaming data)
TCP 5162	N	n/a	<-> Between Peers	Read data stored in JSON format, from SevOne Data Insight to SevOne NMS (Cluster Leader)
TCP 8080	N	n/a	<-> Between Peers	REST API version 1.x (SevOne version 5.6.0)
TCP 8082	N	n/a	-> PAS	SevOne Data Bus status page (optional / configured) on by default
TCP 8123	n/a	n/a	<-> Between Peers	Squid (5.7.2), Polipo (5.7.1), Interpeer Proxy VMware vCenter
TCP 8443	Y	TLS-based encryption - can be configured by an **admin** user.	-> PAS	Secure port for SevOne Data Bus status page (optional / configured) off by default
TCP 9092 (*)	Y	TLS-based encryption.	<-> Between Peers	Apache Kafka

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
TCP, UDP 9094	N	n/a	-> Cluster Leader & HSA <-> Peers	Prometheus Clustering: For Alertmanager high availability clustering ⚠ Peers connect to the Cluster Leader's port 9094 to report alerts and outages as part of Prometheus. This port must be open to other peers in the cluster.
TCP 9443	Y	TLS-based encryption	Web Browser <-> Cluster Leader	Port is **required** for Self Service Upgrades. ⚠ For Self Service Upgrades, the Graphical User Interface installer binds the Cluster Leader to TCP 9443 and runs a service (that the user connects to) through the browser using HTTPS. If the Graphical User Interface installer is required, this port must be exposed.
TCP 9999	N	n/a	-> PAS	SevOne Data Bus to provide host IP address and port number for JMX server (for debug) configurable, off by default
TCP 60005	Y	TLS-based encryption.	<-> Between Peers	Reserved - Interpeer ⚠ Not used post-5.3.x.
TCP 60007 (*)	Y	ZMQ Curve-based encryption.	<-> Between Peers	SevOne-requestd Reserved - Interpeer
TCP 60008	n/a	n/a	<-> Between Peers	Reserved - Interpeer ⚠ Not used post-5.3.x
TCP 60009	n/a	n/a	<-> Between Peers	Reserved - Interpeer ⚠ Not used post-5.3.x

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
UDP 123	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers	NTP Interpeer Time Sync NTP - Interpeer and to NTP time source
UDP 161	N	n/a	PAS -> DNC -> HSA -> <-> Between Peers	SNMP Interpeer Monitoring SNMP - to Devices and Interpeer
UDP 162	N	n/a	-> PAS -> HSA <-> Between Peers	SNMP Trap Interpeer Monitoring and from Devices (optional)
UDP, TCP 514 (**)	N	n/a	PAS -> <-> Between Peers	Syslog
UDP 6831	N	n/a	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6831 is a **compact-thrift** protocol.
UDP 6832	N	n/a	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6832 is a **binary-thrift** protocol.
HTTP 16686 (***)	N	n/a	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port HTTP 16636 is to serve the frontend.

(*) denotes that these ports are a must and absolutely required.
(**) denotes that Syslog is configurable.
(***) denotes that it is recommended to open the port when using Graphical User Interface from the web browser.

2.2 Additional Ports for Hot Standby Appliance (HSA) Deployment

The list below is for additional ports required for Hot Standby Appliance.

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
ICMP (*)	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers	Interpeer Monitoring ICMP from and to devices and Interpeer Monitoring

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
TCP 22 (*)	Y	SSH-based encryption - can be configured by an **admin** user.	-> PAS -> DNC -> HSA <-> Between Peers -> iDRAC	SSH Access - remote login
TCP 25	N	n/a	PAS -> HSA ->	SMTP - to Mail server
TCP 80	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers -> Data Insight	HTTP, SOAP API, and AJAX Calls - End User Terminal UI port for Data Insight - Can be configured using environment variables. Data Insight uses port 80 to redirect any HTTP (80) requests to HTTPS (443)
TCP 443 (*)	Y	TLS-based encryption - can be configured by an **admin** user.	-> PAS -> DNC -> HSA <-> Between Peers -> iDRAC -> Data Insight	HTTPS - End User Terminal UI port for Data Insight - Can be configured using environment variables. Data Insight uses port 80 to redirect any HTTP (80) requests to HTTPS (443)
UDP 123	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers	NTP Interpeer Time Sync NTP - Interpeer and to NTP time source
UDP 161	N	n/a	PAS -> DNC -> HSA -> <-> Between Peers	SNMP Interpeer Monitoring SNMP - to Devices and Interpeer
UDP 162	N	n/a	-> PAS -> HSA <-> Between Peers	SNMP Trap Interpeer Monitoring and from Devices (optional)
UDP, TCP 53	N	n/a	-> PAS -> DNC -> HSA	DNS

(*) denotes that these ports are a must and absolutely required.

2.3 Required Ports for NMS Data Collection

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
UDP 161	N	n/a	PAS -> DNC -> HSA -> <-> Between Peers	SNMP Interpeer Monitoring SNMP - to Devices and Interpeer
UDP 162	N	n/a	-> PAS -> HSA <-> Between Peers	SNMP Trap Interpeer Monitoring and from Devices (optional)

2.4 Required Ports for Remote Management

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
TCP 22 (*)	Y	SSH-based encryption - can be configured by an **admin** user.	-> PAS -> DNC -> HSA <-> Between Peers -> iDRAC	SSH Access - remote login
TCP 443 (*)	Y	TLS-based encryption - can be configured by an **admin** user.	-> PAS -> DNC -> HSA <-> Between Peers -> iDRAC -> Data Insight	HTTPS - End User Terminal UI port for Data Insight - Can be configured using environment variables. Data Insight uses port 80 to redirect any HTTP (80) requests to HTTPS (443) **prometheus** - for main data collection service (only runs on the Cluster Leader and its HSA) - uses port 80 (for HTTP protocol) and 443 (for HTTPS protocol). **alertmanager** - for main alerting service (only runs on the Cluster Leader and its HSA) - uses port 80 (for HTTP protocol) and 443 (for HTTPS protocol).
UDP, TCP 5900	Y	128-bit SSL encryption. For additional details, please refer to https://www.dell.com/support/article/en-us/sln306877/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip?lang=en#ports	-> iDRAC	iDRAC Virtual console Keyboard and Mouse connection

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
UDP, TCP 5901	Y	128-bit SSL encryption. For additional details, please refer to https://www.dell.com/support/article/en-us/sln306877/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip?lang=en#ports	-> iDRAC	iDRAC Virtual console Video connection

(*) denotes that these ports are a must and absolutely required.

2.5 Other Product Integration

2.5.1 SevOne Data Insight (SDI) Deployment

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
TCP 22 (*)	Y	SSH-based encryption - can be configured by an **admin** user.	-> PAS -> Data Insight	Required for SevOne Data Insight to update or Install Data Insight Reporting API (DIRA)
TCP 80	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers -> Data Insight	HTTP, SOAP API, and AJAX Calls - End User Terminal UI port for Data Insight - Can be configured using environment variables. Data Insight uses port 80 to redirect any HTTP (80) requests to HTTPS (443)
TCP 443 (*)	Y	TLS-based encryption - can be configured by an **admin** user.	-> PAS -> DNC -> HSA <-> Between Peers -> iDRAC -> Data Insight	HTTPS - End User Terminal UI port for Data Insight - Can be configured using environment variables. Data Insight uses port 80 to redirect any HTTP (80) requests to HTTPS (443)
TCP 2379 - 2380 (*)	N	n/a	-> Data Insight	Required only for HA with embedded **etcd** **Source**: K3s server nodes
TCP 3000 (**)	N	n/a	Web Browser <-> Data Insight	Required for the Graphical User Interface Installer

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
TCP 3001 (**)	N	n/a	Web Browser <-> Data Insight	Required for the Graphical User Interface Installer's backend (API)
TCP / UDP 5052	Y	TLS-based encryption - can be configured by an **admin** user.	-> NMS -> Data Insight	⚠ Only applies for SevOne Data Insight versions <= 1.6.0 DSPlugin (Data Insight access for its NMS data source peer)
TCP 6443 (*)	N	n/a	-> Data Insight	Kuberbetes API Server **Source**: K3s agent nodes
TCP 10250 (*)	N	n/a	-> Data Insight	Kubelet metrics **Source**: K3s server and agent nodes
UDP 6831	N	n/a	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6831 is a **compact-thrift** protocol.
UDP 6832	N	n/a	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6832 is a **binary-thrift** protocol.

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
UDP 8472	N	n/a	-> Data Insight	Required only for Flannel VXLAN Source: K3s server and agent nodes The nodes need to be able to reach other nodes over UDP port 8472 when Flannel VXLAN is used. The node should not listen on any other port. K3s uses reverse tunneling such that the nodes make outbound connections to the server and all kubelet traffic runs through that tunnel. However, if you do not use Flannel and provide your own custom CNI, then port 8472 is not needed by K3s. IMPORTANT The VXLAN port on nodes should not be exposed to the world as it opens up your cluster network to be accessed by anyone. Run your nodes behind a firewall/security group that disables access to port 8472.
HTTP 16686 (**)	N	n/a	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port HTTP 16636 is to serve the frontend.

(*) denotes that these ports are a must and absolutely required.
(**) denotes that it is recommended to open the port when using Graphical User Interface from the web browser.

2.5.2 SevOne Data Bus (SDB) Deployment

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
TCP 8082	N	n/a	-> PAS	SevOne Data Bus status page (optional / configured) on by default
TCP 8443	Y	TLS-based encryption - can be configured by an **admin** user.	-> PAS	Secure port for SevOne Data Bus status page (optional / configured) off by default
TCP 9092 (*)	Y	TLS-based encryption.	<-> Between Peers	Apache Kafka

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
TCP 9443 (**)	Y	TLS-based encryption.	Web Browser <-> Cluster Leader	Port is **required** for Self Service Upgrades. ⚠ For Self Service Upgrades, the Graphical User Interface installer binds the Cluster Leader to TCP 9443 and runs a service (that the user connects to) through the browser using HTTPS. If the Graphical User Interface installer is required, this port must be exposed.
TCP 9999	N	n/a	-> PAS	SevOne Data Bus to provide host IP address and port number for JMX server (for debug) configurable, off by default.

(*) denotes that these ports are a must and absolutely required.
(**) denotes that it is recommended to open the port when using Graphical User Interface from the web browser.

2.5.3 Solutions Deployment

The following table provides port number requirements for Cisco SDN, Enterprise WiFi Monitoring, and SD-WAN (Nokia-Nuage, Versa, and Viptela collectors).

Solution	IP (UDP/TCP)/ICMP	Direction	Purpose
SDN	TCP 80 (HTTP)	-> PAS	The API **config** / **communication** port
	TCP 443 (HTTPS)	-> PAS	The API **config** / **communication** port Required for, • Collection of ACI fabric performance and status data • Collection of site information from a multi-site controller • Transfer of collected ACI fabric data to SevOne NMS PAS for processing and storage
	UDP 6831	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6831 is a **compact-thrift** protocol
	UDP 6832	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6832 is a **binary-thrift** protocol

Solution		IP (UDP/TCP)/ICMP	Direction	Purpose
		HTTP 16686 (*)	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port HTTP 16636 is to serve the frontend
WiFi		TCP 80	-> PAS	PAS REST API **config** / **collection** port
		TCP 443	-> PAS	The API **config** / **communication** port
		TCP 3306	-> PAS	MySQL port
		UDP 6831	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6831 is a **compact-thrift** protocol
		UDP 6832	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6832 is a **binary-thrift** protocol
		HTTP 16686 (*)	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port HTTP 16636 is to serve the frontend
SD-WAN	Nokia-Nuage	TCP 443 (Outbound)	-> PAS	Address: NMS server; for NMS API port
		TCP 5672 (Outbound)	-> VSD (Controller)	Address: Nuage AMQP server; for Nuage message queue bus; required for Messaging Service (ActiveMQ) broker
		TCP 6200 (Outbound)	-> Elasticsearch (Controller)	Address: Nuage Elasticsearch server; for Nuage statistics (*for internal lab only*)
		UDP 6831	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6831 is a **compact-thrift** protocol
		UDP 6832	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6832 is a **binary-thrift** protocol
		TCP 8443 (Outbound)	-> PAS	Address: Nuage VSD server; for Nuage API

Solution		IP (UDP/TCP)/ICMP	Direction	Purpose
	Versa	TCP 9200	-> Elasticsearch (Controller)	Address: Nuage Elasticsearch server; for Nuage statistics
		TCP 9996 (Outbound)	Collector Nodes -> DNC	Address: NMS DNC server; for Flow Augmentor output; required for DNC where the flows are being sent
		HTTP 16686 (*)	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port HTTP 16636 is to serve the frontend
		TCP 443 (Outbound)	-> PAS	Address: NMS server; for NMS API port
		TCP 3000 (*)	Web Browser <-> Collector Leader Node	Required for the Graphical User Interface Installer For Client, config file location is **/etc/sevone-guii/client.yaml**
		TCP 3001 (*)	Web Browser <-> Collector Leader Node	Required for the Graphical User Interface Installer's backend (API) For API, config file location is **/etc/sevone-guii/api.yaml**
		UDP 6831	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6831 is a **compact-thrift** protocol
		UDP 6832	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6832 is a **binary-thrift** protocol
		TCP 9182	-> vDirector	API port number of targeted vDirector
		TCP 9992 (Inbound)	-> Collector Nodes	Flow syslogs from Versa devices
		TCP 9996(Outbound)	Collector Nodes -> DNC	Address: NMS DNC server; for Flow Augmentor output; required for DNC where the flows are being sent
		HTTP 16686 (*)	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port HTTP 16636 is to serve the frontend

Solution		IP (UDP/TCP)/ICMP	Direction	Purpose
		TCP 50001 (Inbound)	-> Collector Nodes	Versa Syslogs from Versa Analytics server (The port on which the collector listens for non-flow syslog data sent by Versa Analytics); required for the log exporter to send UDP data to collector and Syslog data in **kvp** format
	Viptela	TCP 443 (Outbound)	Collector Nodes -> PAS -> vManage	Address: vManage server; for Viptela vManage API Address: NMS server; for NMS API port
		TCP 3000 (*)	Web Browser <-> Collector Leader Node	Required for the Graphical User Interface Installer For Client, config file location is **/etc/sevone-guii/client.yaml**
		TCP 3001 (*)	Web Browser <-> Collector Leader Node	Required for the Graphical User Interface Installer's backend (API) For API, config file location is **/etc/sevone-guii/api.yaml**
		UDP 6831	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6831 is a **compact-thrift** protocol
		UDP 6832	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port UDP 6832 is a **binary-thrift** protocol
		TCP 8443 (Outbound)	-> vManage	Address: vManage server; for Viptela vManage API
		TCP 9995 (Inbound)	-> Collector Nodes	Flow Augmentor input (The port on which Flow Augmentor listens for inbound flows. The port number can range from 9000 - 33000)
		TCP 9996 (Outbound)	Collector Nodes -> DNC	Address: NMS DNC server; for Flow Augmentor output; required for DNC where the flows are being sent
		HTTP 16686 (*)	-> PAS	(Optional) This port is for **Tracing**. This feature is for **Internal Use Only** for the Support Team to use for troubleshooting. Port HTTP 16636 is to serve the frontend

(*) denotes that it is recommended to open the port when using Graphical User Interface from the web browser.

2.5.4 SevOne Distributed Netflow Connector (DNC) Deployment

IP (UDP/TCP)/ICMP	Encrypted	Encryption Type	Direction	Purpose
ICMP (*)	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers	Interpeer Monitoring ICMP from and to devices and Interpeer Monitoring
TCP 22 (*)	Y	SSH-based encryption - can be configured by an **admin** user.	-> PAS -> DNC -> HSA <-> Between Peers -> iDRAC	SSH Access - remote login
TCP 80	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers -> Data Insight	HTTP, SOAP API, and AJAX Calls - End User Terminal UI port for Data Insight - Can be configured using environment variables. Data Insight uses port 80 to redirect any HTTP (80) requests to HTTPS (443)
TCP 443 (*)	Y	TLS-based encryption - can be configured by an **admin** user.	-> PAS -> DNC -> HSA <-> Between Peers -> iDRAC -> Data Insight	HTTPS - End User Terminal UI port for Data Insight - Can be configured using environment variables. Data Insight uses port 80 to redirect any HTTP (80) requests to HTTPS (443)
UDP 123	N	n/a	-> PAS -> DNC -> HSA <-> Between Peers	NTP Interpeer Time Sync NTP - Interpeer and to NTP time source
UDP 161	N	n/a	PAS -> DNC -> HSA -> <-> Between Peers	SNMP Interpeer Monitoring SNMP - to Devices and Interpeer
UDP 6343	N	n/a	-> DNC	sFlow data to DNC (configurable / optional)
UDP 9996	N	n/a	-> DNC	Netflow data (sampled / non-sampled) to DNC (configurable)
UDP, TCP 53	N	n/a	-> PAS -> DNC -> HSA	DNS

(*) denotes that these ports are a must and absolutely required.