Veritas NetBackup™ Network Ports Reference Guide

Release 9.0

VERITAS™

Veritas NetBackup™ Network Ports Reference Guide

Last updated: 2020-12-07

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

About the NetBackup network ports

This chapter includes the following topics:

TCP ports used by NetBackup

NetBackup primarily uses the TCP protocol to communicate between processes. The processes can run on the same host or on different hosts. This distributed client-server architecture requires that the destination TCP ports specific to the NetBackup processes be open through any firewalls within the networking infrastructure.

Firewalls may also be configured to filter connections based on the source port. NetBackup typically uses non-reserved source ports for outbound connections.

The sections that follow describe the TCP ports used by NetBackup in the default configuration. The network layers on the hosts and the networking devices between the hosts must be configured to allow these connections. NetBackup requires the proper connections to be configured or it cannot operate.

Compatibility with back-level hosts

- Use the operating system commands (`netstat`, `pfiles`, `lsof`, `process monitor`) to make sure that the expected processes are running and listening for connections.
- The `bptestbpcd` command resides only on NetBackup servers.

Chapter 2

NetBackup Ports

This chapter includes the following topics:

NetBackup default ports

NetBackup primarily uses the ports as destination ports when connecting to the various services.

See Table 2-1 on page 7.

Veritas has registered these ports with Internet Assigned Number Authority (IANA) and they are not to be used by any other applications.

A few features and services of NetBackup require additional ports to be open. Those requirements are detailed in later sections.

By default, NetBackup uses ports from the ephemeral range for the source port. Those ports are selected randomly from the range provided by the operating system.

Note: Configuring the **Connect Options** and other settings may change how source and destination ports are selected. These settings and other non-default configurations, are not discussed here. For details, see the NetBackup Administrator's Guides, volume 1 and volume 2.

The following table lists the ports required by NetBackup to connect to various services.

Table 2-1 NetBackup ports

Service	Port	Description
VERITAS_PBX	1556	Veritas Private Branch Exchange Service
VNETD	13724	NetBackup Network service

NetBackup master server ports

The master server must be able to communicate with the media servers, clients, as well as servers where the Java or the Windows Administration Console is running.

The following table lists the minimum ports required by the master server:

Table 2-2 NetBackup master server ports

Source	Destination	Service	Port
Master server	Media server	VERITAS_PBX	1556
Master server	Media server	VNETD	13724[1]
Master server	Client	VERITAS_PBX	1556
Master server	Client	VNETD	13724[1]
Master server	Media server	NBSSC	5637[2]

1 - It applies while you use the Resilient Network feature or when NetBackup 8.0 or earlier master server cannot reach a legacy service via PBX.

2 - This port is used to provide back-level media server support for the media servers that are configured for cloud storage. Only media server versions 7.7.x to 8.1.2 are supported.

Ensure that the older media servers use this port. Communication with the master server fails if the older media servers use a different port.

NetBackup media server ports

The media server must be able to communicate with the master server, and the clients.

The following table lists the ports required by the media server:

Table 2-3 NetBackup media server ports

Source	Destination	Service	Port
Media server	Master server	VERITAS_PBX	1556
Media server	Master server	VNETD	13724 **
Media server	Media server	VERITAS_PBX	1556
Media server	Media server	VNETD	13724 **
Media server	Client	VERITAS_PBX	1556
Media server	Client	VNETD	13724 **
Media server	MSDP server	Deduplication 10102 Manager (spad)	10102
Media server	MSDP server	Deduplication Engine (spoold)	10082
Media server	Master server	NBWMC	5637+

** It applies while you use the Resilient Network feature or when a NetBackup 8.0 or earlier media server cannot reach a legacy service via PBX.

+ This port is used to provide back-level media server support for the media servers that are configured for cloud storage. Only media server versions 7.7.x to 8.1.2 are supported.

Ensure that the older media servers use this port. Communication with the master server fails if the older media servers use a different port.

NetBackup client ports

The client requires access to the master server to initiate user and client-initiated operations such as application backups for Oracle and SQL Server.

When using the client-side deduplication, the client must also be able to communicate with the MSDP media servers.

The following table lists the ports required by the client:

Table 2-4 NetBackup client ports

Source	Destination	Service	Port
Client	Master server	VERITAS_PBX	1556
Client	Master server	VNETD	13724 *
Client	Media server	VERITAS_PBX	1556
Client	Media server	VNETD	13724 * *
Client	MSDP server	Deduplication Manager (`spad`)	10102
Client	MSDP server	Deduplication Engine (`spoold`)	10082

* It applies while you use the Resilient Network feature or when a NetBackup 8.0 or earlier client cannot reach a legacy service via PBX.

** Required while you use the Resilient Network feature.

Web UI ports

The NetBackup web UI uses the following ports for communication:

Table 2-5 NetBackup web UI ports

Source	Destination	Service	Port
Web browser	Master server	NBWMC	443

Java Console ports

The Java Console (or NetBackup Administration Console) uses the following ports for communication:

Table 2-6 Java Console ports

Source	Destination	Service	Port
Java Console	Master server	VERITAS_PBX	1556
Java Console	Master server	VNETD	13724

NDMP server ports

The port requirements to backup and restore an NDMP server are as follows:

- TCP port 10000 must be open from the media server (DMA) to the NDMP filer (tape or disk) for all types of NDMP operations; local, remote, and 3-way.
- The NetBackup SERVER_PORT_WINDOW must be open inbound from the filer to the media server for remote NDMP. It must also be open for efficient catalog file (TIR data) movement during local or 3-way NDMP.

DataDomain OpenStorage ports

The following ports must be open to use a DataDomain OST storage server.

- The TCP ports for 2049 (`nfs`), 111 (`portmapper`), and 2052 (`mountd`) must be open from the media server to the target storage server.
- The UDP port 111 (`portmapper`) must be open from the media server to the target storage server.
- The TCP port 2051 (`replication`) must also be open from the media server to the storage server for optimized duplication.

NetBackup Granular Restore Technology (GRT) ports

The following ports must be open to use the GRT feature of NetBackup.

- TCP port 111 (`portmapper`) needs to be open from the client to the media server.
- TCP port 7394 (`nbfsd`) needs to be open from the client to the media server.

Network and port address translation

NetBackup 8.2 and later versions support NetBackup clients in a private network that are connected to NetBackup servers in a public network through a device that

performs network address translation (NAT). Such NetBackup clients are referred to as NAT clients.

For more details on NAT support, refer to the NetBackup Administrator's Guide Volume I.

The TCP port used by the NetBackup Messaging Broker service (`nbmqbroker`) must be open from the clients to the master server. The default port is 13781 unless it is updated with the `configureMQ` command.

Note that the direction of connection initiation between servers and clients is reversed. The TCP port for PBX/1556 must be open from the client to the servers and need not be open from servers to clients.

For additional details see the technote NetBackup support for NAT and PAT.

Configuring ports for the NetBackup legacy Web Services

The NetBackup installation process automatically runs the `configurePorts` script to configure NetBackup legacy Web Services to run on any of the following sets of ports.

Table 2-7 Port sets for NetBackup legacy Web Services

Port set	HTTPS port	Shutdown port
First set	8443	8205
Second set	8553	8305
Third set	8663	8405

Note: The shutdown ports are honored only for local intra-host connections. Therefore, they do not need to be open externally.

The HTTPS port (whichever is in use) should be open inbound to the master server.

If the `configurePorts` script does not find one of the sets free (for example 8443 and 8205), it logs an error to the following file:

Windows:

install_path`\NetBackup\wmc\webserver\logs\nbwmc_configurePorts.log`

UNIX and Linux:

`/usr/openv/wmc/webserver/logs/nbwmc_configurePorts.log`

On UNIX and Linux, the following appears on the NetBackup system console:

```
configurePorts: WmcPortsUpdater failed with exit status <status_code>
```

When this error occurs, use the following procedure on the master server to manually configure the ports. The `configurePorts` command is in the following location:

Windows:

```
install_path\NetBackup\wmc\bin\install\configurePorts
```

UNIX or Linux:

```
/usr/openv/wmc/bin/install/configurePorts
```

Note: NetBackup Web Services on the master server require port 1024 or higher. Do not use a port number that is less than 1024. Ports that are less than 1024 are privileged and cannot be used with the NetBackup Web Services.

To configure ports for the NetBackup Web Services

1. On the master server, enter the following to list the currently configured ports:

   ```
   configurePorts -status
   ```

   Example output:

   ```
   Current Https Port: 8443
   Current Shutdown Port: 8205
   ```

2. Use the `configurePorts` command in the following format to re-configure a port:

   ```
   configurePorts -httpsPort https_port | -shutdownPort shutdown_port
   ```

   You can configure one or two ports at a time. For example, to configure the HTTPS port to 8553:

   ```
   configurePorts -httpsPort 8553
   ```

   Output:

   ```
   Old Https Port: 8443
   New Https Port: 8553
   ```

   Use this command as needed to configure a set of ports for HTTPS and shutdown.

   See Table 2-7 for a list of the port sets.

3. If the master server is in a clustered environment, do the following:

- Make sure that the same set of ports are free on all the cluster nodes: Do step 1 on each node.
- Reconfigure the ports on each node as required: Do step 2.
- To override the ports that are used across all nodes, enter the following:

  `configurePorts –overrideCluster true`

  This command updates the following file on shared disk:

  Windows:

  `install_path``/NetBackup/var/global/wsl/portfile`

  UNIX or Linux:

  `/usr/openv/netbackup/var/global/wsl/portfile`

  The NetBackup installer for `Web Services` uses this file during installation in a clustered mode.

Chapter 3

Other Network Ports

This chapter includes the following topics:

NetBackup deduplication ports

The following table shows the ports that are used for NetBackup deduplication that includes Media Server Deduplication (MSDP), and optimized deduplication. If firewalls exist between the various deduplication hosts, you must open the required ports.

Deduplication hosts are the media servers, deduplication storage servers, any load balancing servers, and any clients that deduplicate their own data.

Note: MSDP with Client-Direct (client deduplication) and optimized duplication need some ports to be opened.

During Client Direct restores, TCP port 1556 must be open between the NetBackup client and the master server.

Table 3-1 NetBackup deduplication port usage

Port	Usage
10082	This is the NetBackup Deduplication Engine (`spoold`) port that is used by MSDP. Open this port between: ■ The deduplication client and the storage servers. ■ The MSDP and the storage servers.
10102	This is the NetBackup Deduplication Manager (`spad`) port that is used by MSDP. Open this port between: ■ The deduplication client and the MSDP servers. ■ The MSDP server and any Additional servers that handle finger printing.

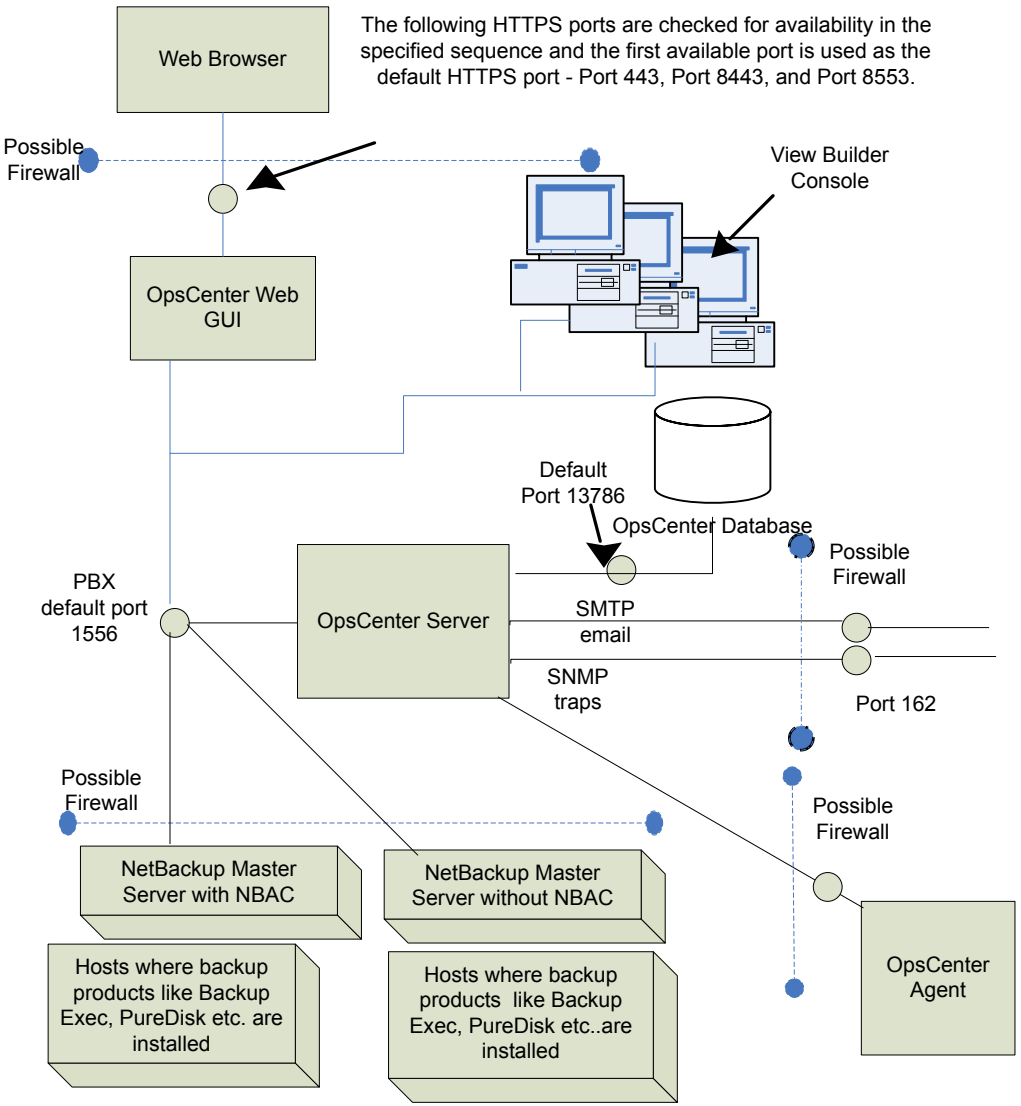
Ports 10082 and 10102 (MSDP) must also be open between the media server and any storage servers that perform optimized duplications.

Note: If using Auto Image Replication (AIR) for optimized duplication, TCP ports 1556, 10082, and 10102 (MSDP) must be open between the NetBackup domains.

About communication ports and firewall considerations in OpsCenter

Figure 3-1 shows the key OpsCenter components and the communication ports that are used.

Figure 3-1 Key OpsCenter components and how they communicate



See "Communication ports used by key OpsCenter components" on page 16.

Communication ports used by key OpsCenter components

The following table shows the default port settings for OpsCenter.

SMTP recipient ports can be configured from the OpsCenter console (using **Settings > Configuration > SMTP Server**). The SNMP trap recipient ports can also be configured from the OpsCenter console (using **Settings > Recipients > SNMP**).

If these ports are changed then the appropriate hardware ports have to be opened.

Table 3-2 lists the communication ports that are used by key OpsCenter components.

Table 3-2 Communication ports used by key OpsCenter components

Source Host	Destination Host	Port Number	Usage (Process Name)	Port Configuration
OpsCenter Server	Mail server	25	SMTP	Allow from source to destination.
OpsCenter Server	SNMP Server	162	SNMP trap recipient	Allow from source to destination.
OpsCenter Server	NetBackup Master Server(s)	1556	PBX (pbx_exchange)	Allow between source and destination (bi-directional). PBX port number configuration is not supported.
OpsCenter Client	OpsCenter Server	1556	PBX (pbx_exchange)	Allow between source and destination. Some hardened servers and firewall configurations may block this port. PBX port number configuration is not supported.
Web browser	OpsCenter Server	The following HTTPS ports are checked for availability in the specified sequence and the first available port is used by default: **1** 443 (HTTPS) **2** 8443 (HTTPS) **3** 8553 (HTTPS)	HTTPS	Allow from all hosts on network.

Table 3-2 Communication ports used by key OpsCenter components *(continued)*

Source Host	Destination Host	Port Number	Usage (Process Name)	Port Configuration
OpsCenter Server	OpsCenter Server	13786	Sybase database (`dbsrv16`)	Allow between source and destination. Some hardened servers and firewall configurations may block this port.
OpsCenter Server	OpsCenter Server	1556	OpsCenter Product Authentication Service (`ops_atd`)	Allow between source and destination in case NBAC is enabled on NetBackup master server.

NetBackup 5200 and 5220 appliance ports (for firewall between master and media server)

In addition to the ports used by NetBackup, the 52xx appliances also provide for both in-band and out-of-band management. The out-of-band management is through a separate network connection, the Remote Management Module (RMM), and the Intelligent Platform Management Interface (IPMI). Open these ports through the firewall as appropriate to allow access to the management services from a remote laptop or KVM (keyboard, video monitor, mouse).

The following table describes the ports to open inbound to the NetBackup appliance.

Table 3-3 Inbound ports

Source	Destination	Port	Service	Description
Command line	Appliance	22	ssh	In-band management CLI
Web browser	Appliance	80	http	In-band management GUI
Web browser	Appliance	443	https	In-band management GUI
Web browser	Appliance IPMI	80	http	Out-of-band mgmt (ISM+ or RM*)

Table 3-3 Inbound ports *(continued)*

Source	Destination	Port	Service	Description
Web browser	Appliance IPMI (firmware > 2.13)	443	https	Out-of-band management (ISM+ or RM*)
NetBackup ISM+	5020/5200 Appliance IPMI	5900	KVM	CLI access, ISO & CDROM redirection
NetBackup ISM+	5020/5200 Appliance IPMI	623	KVM	(optional, utilized if open)
Symantec RM*	5220/5x30 Appliance IPMI	7578	RMM	CLI access
Symantec RM*	5220/5x30 Appliance IPMI	5120	RMM	ISO & CD-ROM redirection
Symantec RM*	5220/5x30 Appliance IPMI	5123	RMM	Floppy redirection
Symantec RM*	5220/5x30 Appliance IPMI	7582	RMM	KVM
Symantec RM*	5220/5x30 Appliance IPMI	5124		CDROM
Symantec RM*	5220/5x30 Appliance IPMI	5127		USB or Floppy

+ NetBackup Integrated Storage Manager

* Symantec Remote Management – Remote Console.

Note: Ports 7578, 5120, and 5123 are for the unencrypted mode. Ports 7528, 5124, and 5127 are for the encrypted mode.

Open these ports outbound from the appliance to allow alerts and notifications to the indicated servers.

Table 3-4 Outbound ports

Source	Destination	Port	Service	Description
Appliance	Call Home server	443	https	Call Home notifications to Veritas
Appliance	SNMP Server	162*	SNMP	Outbound traps and alerts
Appliance	SCSP host	443	https	Download SCSP certificates

* This port number can be changed within the appliance configuration to match the remote server.

NetBackup VMware ports

The TCP ports 443 and 902 are required to access the VMware infrastructure, as follows:

443 NetBackup connects to TCP port 443 on the following VMware components:

- On the vCenter server for VM discovery requests, snapshot creation and deletion, vSphere Tag associations, and so on.
- On the vSphere Platform Services Controller (PSC) to discover, back up and restore vSphere Tag associations.
  NetBackup connects to the vSphere Platform Services Controller (PSC) in vSphere 6.0 and later.

902 TCP port 902 is required when:

- You use HotAdd/NBD/NBDSSL transport for backups and restore.
- Restores are done through Restore ESX server bypassing the vCenter server.

Port usage for the NetBackup vSphere Web Client Plug-in

Table 3-5 shows the standard ports to be used in a NetBackup vSphere Web Client Plug-in environment.

Table 3-5 Ports used in NetBackup and the vSphere Web Client Plug-in environment

Source	Port number	Destination
Browser	9443	vSphere Web Client
For VM recovery: vCenter server (or vSphere Web Client server if deployed independently)	`RESTful` interface at port 8443 (https) or as configured on the master server	Master server
Master server	443	vCenter server
Backup host	443	vCenter server
Backup host	902 (for `nbd` or `nbdssl`)	ESXi

NetBackup CloudStore Service Container (nbcssc) port

This is applicable to media server versions 7.7.x to 8.1.2 only.

The CloudStore Service Container (`nbcssc`) is a web-based service container that runs on older media servers that are configured for cloud storage. This container runs the throttling service and the metering data collector service. NetBackup OpsCenter uses the metering data for monitoring and reporting.

Table 3-6 NetBackup CloudStore Service Container (nbcssc) port

Port	Source	Destination	Process	Description
5637	Media server 7.7.x to 8.1.2 only	Master server	NBWMC	Allow communication between master server and all media servers that are configured for cloud storage. This port is used to provide back-level media server support. Only media server versions 7.7.x to 8.1.2 are supported. Ensure that the older media servers use this port. Communication with the master server fails if the older media servers use a different port.
5637	Master server	Media server 7.7.x to 8.1.2 only	NBCSSC	Allow communication between master server and all media servers that are configured for cloud storage. This port is used to provide back-level media server support. Only media server versions 7.7.x to 8.1.2 are supported. Ensure that the older media servers use this port. Communication with the master server fails if the older media servers use a different port.

The port number is defined in the CloudStore Service Container configuration file (`cloudstore.conf`) as follows:

```
CSSC_PORT=5637
```

The configuration file resides in the following directory on the older media servers:

- UNIX: `/usr/openv/netbackup/db/cloud`
- Windows: *`install_path`*`Veritas\NetBackup\db\cloud`

See the *NetBackup Cloud Administrator's Guide* for more details.

http://www.veritas.com/docs/DOC5332

Index