Veritas NetBackup™ Network Ports Reference Guide

Release 8.1

VERITAS™

Veritas NetBackup™ Network Ports Reference Guide

Document version: 8.1

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

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

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/

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

NetBackup 8.1 and later versions use a minimum set of TCP ports, primarily `VERITAS_PBX` (1556) and `VNETD` (13724) ports.

When connecting to legacy daemons on remote hosts, NetBackup 8.1 and newer servers first attempt to connect to `VERITAS_PBX`. If unsuccessful, the connection is retried to `VNETD`.

If connections are being made to an unexpected destination port, it is likely that a problem in networking, operating systems, or applications is preventing consistent connections to the default ports. To fix the problem, check the following:

- Use the operating system commands (`netstat`, `pfiles`, `lsof`, `process monitor`) to make sure that the expected processes are running and listening for connections.
- Use the `bpclntcmd`, `bptestbpcd` and `bptestnetconn` commands to check connectivity to NetBackup hosts of any version.
  The `bptestbpcd` command resides only on NetBackup servers.
  The `bpclntcmd` and the `bptestnetconn` commands reside on both NetBackup servers and clients.
  The `bpclntcmd -pn` can be used to check connectivity from a client to the master server.

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 8.

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 non-reserved 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 Administration 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, EMM server, VxSS server, 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	Client	VERITAS_PBX	1556
Master server	Client	VNETD	13724 [1]
Master server	Java server	VERITAS_PBX	1556
Master server	Netware	VNETD	13724
Master server	Netware	BPCD	13782

1 - Required as a fall-back option when a legacy service cannot be reached via PBX and is also required when using the Resilient Network feature.

NetBackup media server ports

The media server must be able to communicate with the master server, the EMM 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 Manager (spad)	10102 10102
Media server	MSDP server	Deduplication Engine (spoold)	10082
Media server	Netware client	VNETD	13724
Media server	Netware client	BPCD	13782

* Required as a fall-back option when a legacy service cannot be reached via PBX.

** Required as a fall-back option when a legacy service cannot be reached via PBX and is also required when using the Resilient Network feature.

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

* Required as a fall-back option when a legacy service cannot be reached via PBX and is also required when using the Resilient Network feature.

** Required when using Resilient Network feature.

Java server ports

The Java server is the process running on the master server when you connect using the Java Administration Console. The Java server must be able to communicate with all of the core NetBackup components. The following table lists the ports required for the Java server:

Table 2-5 Java Server ports

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

Java Console ports

The Java Console uses the Java Server for further communication; it requires the following ports:

Table 2-6 Java Console ports

Source	Destination	Service	Port
Java Console	Master server	VERITAS_PBX	1556
Java Console	Master server	VNETD	13724
Java Console	Java Server	VERITAS_PBX	1556
Java Console	Java 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 does not currently support the use of Network Address Translation (NAT) or the Port Address Translation (PAT).

For additional details see, the technote TECH15006.

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.

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.

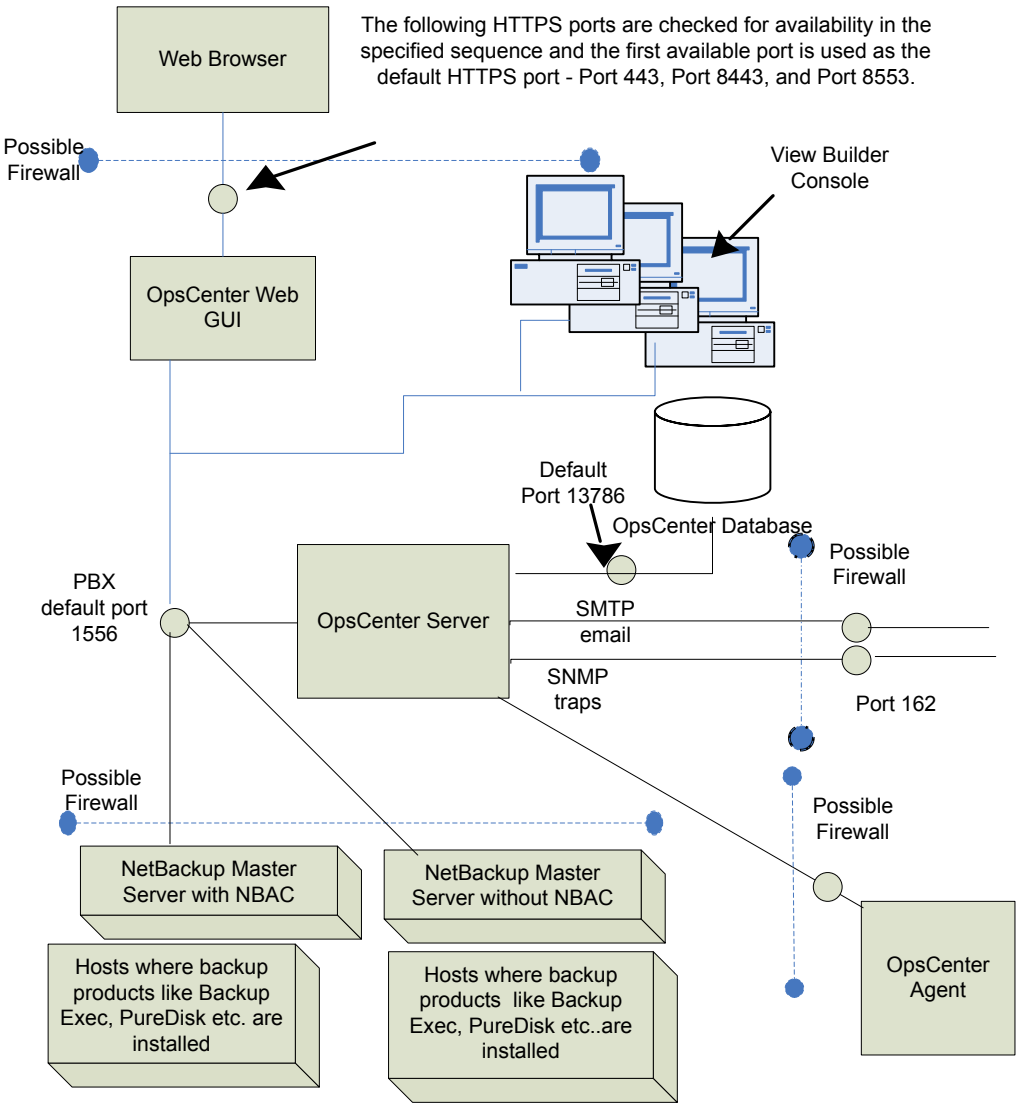
Ports 10082 and 10102 (MSDP) must also be open between the media server and any storage servers that perform optimized duplications.

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 15.

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 (`opsatd`)	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)

The CloudStore Service Container (nbcssc)is a web-based service container that runs on the media server that is configured for cloud storage. This container hosts different services such as the configuration service, the throttling service, and the metering data collector service. NetBackup OpsCenter uses the metering data for monitoring and reporting.

The default port number for the NetBackup CloudStore Service Container (`nbcssc`) service is 5637.

The CloudStore Service Container configuration file resides in the following directories:

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

The following is an example that shows the default value:

```
[NBCSSC]

CSSC_PORT=5637
```

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

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

Index