

NetBackup™ Network Ports Reference Guide

Release 10.1.1

VERITAS™

NetBackup™ Network Ports Reference Guide

Last updated: 2022-12-19

Legal Notice

Copyright © 2022 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Veritas Technologies LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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	5
	TCP ports used by NetBackup	5
	Compatibility with back-level hosts	5
Chapter 2	NetBackup Ports	6
	NetBackup default ports	6
	NetBackup master server ports	7
	NetBackup media server ports	8
	NetBackup client ports	8
	Web UI ports	9
	Java Console ports	9
	NDMP server ports	10
	DataDomain OpenStorage ports	10
	NetBackup Granular Restore Technology (GRT) ports	10
	Network and port address translation	10
	Configuring ports for the NetBackup legacy Web Services	11
Chapter 3	Other Network Ports	14
	NetBackup deduplication ports	14
	NetBackup 5200 and 5220 appliance ports (for firewall between master and media server)	15
	NetBackup VMware ports	17
	Port usage for the NetBackup vSphere Web Client Plug-in	17
	Nutanix AHV cluster ports	18
	Port requirements for Kubernetes operator deployment	19
	NetBackup CloudStore Service Container (nbcssc) port	19
Index		21

About the NetBackup network ports

This chapter includes the following topics:

- [TCP ports used by NetBackup](#)
- [Compatibility with back-level hosts](#)

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.

NetBackup Ports

This chapter includes the following topics:

- [NetBackup default ports](#)
- [NetBackup master server ports](#)
- [NetBackup media server ports](#)
- [NetBackup client ports](#)
- [Web UI ports](#)
- [Java Console ports](#)
- [NDMP server ports](#)
- [DataDomain OpenStorage ports](#)
- [NetBackup Granular Restore Technology \(GRT\) ports](#)
- [Network and port address translation](#)
- [Configuring ports for the NetBackup legacy Web Services](#)

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	MSPD server	Deduplication 10102 Manager (spad)	10102
Media server	MSPD 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 (<i>spad</i>)	10102
Client	MSDP server	Deduplication Engine (<i>spoold</i>)	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 (`nbfspd`) 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 primary 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/opensv/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 primary 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/opensv/wmc/bin/install/configurePorts
```

Note: NetBackup Web Services on the primary 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 primary 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 primary 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/opensv/netbackup/var/global/wsl/portfile
```

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

Other Network Ports

This chapter includes the following topics:

- [NetBackup deduplication ports](#)
- [NetBackup 5200 and 5220 appliance ports \(for firewall between master and media server\)](#)
- [NetBackup VMware ports](#)
- [Port usage for the NetBackup vSphere Web Client Plug-in](#)
- [Nutanix AHV cluster ports](#)
- [Port requirements for Kubernetes operator deployment](#)
- [NetBackup CloudStore Service Container \(nbcssc\) port](#)

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.

NetBackup 5200 and 5220 appliance ports (for firewall between master and media server)**Table 3-1** NetBackup deduplication port usage

Port	Usage
10082	This is the NetBackup Deduplication Engine (<i>spsold</i>) port that is used by MSDP. Open this port between: <ul style="list-style-type: none"> ■ The deduplication client and the storage servers. ■ The MSDP and the storage servers.
10102	This is the NetBackup Deduplication Manager (<i>spsad</i>) port that is used by MSDP. Open this port between: <ul style="list-style-type: none"> ■ 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.

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 3-2 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

NetBackup 5200 and 5220 appliance ports (for firewall between master and media server)**Table 3-2** Inbound ports (*continued*)

Source	Destination	Port	Service	Description
Web browser	Appliance	443	https	In-band management GUI
Web browser	Appliance IPMI	80	http	Out-of-band mgmt (ISM+ or RM*)
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 3-3 Outbound ports

Source	Destination	Port	Service	Description
Appliance	Call Home server	443	https	Call Home notifications to Veritas

Table 3-3 Outbound ports (*continued*)

Source	Destination	Port	Service	Description
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 3-4](#) shows the standard ports to be used in a NetBackup vSphere Web Client Plug-in environment.

Table 3-4 Ports used in NetBackup and the vSphere Web Client Plug-in environment

Source	Port number	Destination
Browser	9443	vSphere Web Client

Table 3-4 Ports used in NetBackup and the vSphere Web Client Plug-in environment (*continued*)

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

Nutanix AHV cluster ports

The following table shows the ports that are used between the NetBackup hosts and the Nutanix AHV cluster hosts. If firewalls exist between the various hosts, you must open the required ports.

Table 3-5 Ports that must be open in a Nutanix AHV cluster environment

Source	Port number	Destination
Backup host	TCP port 111 (port mapper)	Nutanix AHV cluster
Backup host	TCP port 2049 (NFS)	Nutanix AHV cluster
Backup host	TCP port 9440	Nutanix AHV cluster
Backup host	TCP port 9440	Nutanix AHV Prism Central server
Nutanix AHV cluster	TCP port 111 (port mapper)	Backup host
Nutanix AHV cluster	TCP port 2049 (NFS)	Backup host
*bi-directional	iSCSI over TCP 860, 3260	*bi-directional
*bi-directional	iSCSI over TCP 3205	*bi-directional

*Ports must be open bi-directional between AHV access host and AHV cluster. Port 9440 is open only inbound to the AHV cluster from the AHV access host.

Port requirements for Kubernetes operator deployment

Following table shows the port requirements for the Kubernetes operator deployment. If firewall exist between the various hosts, you must open the required communication ports.

Table 3-6 Ports that must be open in a NetBackup Kubernetes cluster environment

Source	Port number	Destination
Primary server	TCP port 443	Kubernetes cluster
Media server	TCP port 443 (new in NetBackup 10.0).	Kubernetes cluster

Note: Review the Kubernetes configuration to ensure that the Kubernetes API server port has not been changed from 443 to a non-default port; often 6443 or 8443.

Kubernetes cluster	TCP port 443 (applicable in NetBackup version 9.1, but not in version 10.0 or later).	Primary server
--------------------	---	----------------

Note: NetBackup Kubernetes Operator (KOps) and datamover pods have additional requirements (new in NetBackup 10.0).

Kubernetes cluster	TCP port 1556 outbound	Primary server
Kubernetes cluster	TCP port 1556 outbound	Media server
Kubernetes cluster	TCP port 13724 bi-directional if using Resilient Network.	Primary and media server

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.

Table 3-7 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	<p>Allow communication between master server and all media servers that are configured for cloud storage.</p> <p>This port is used to provide back-level media server support. Only media server versions 7.7.x to 8.1.2 are supported.</p> <p>Ensure that the older media servers use this port. Communication with the master server fails if the older media servers use a different port.</p>
5637	Master server	Media server 7.7.x to 8.1.2 only	NBCSSC	<p>Allow communication between master server and all media servers that are configured for cloud storage.</p> <p>This port is used to provide back-level media server support. Only media server versions 7.7.x to 8.1.2 are supported.</p> <p>Ensure that the older media servers use this port. Communication with the master server fails if the older media servers use a different port.</p>

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/opensv/netbackup/db/cloud`
- **Windows:** `install_pathVeritas\NetBackup\db\cloud`

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

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

Index

Symbols

5200 and 5220 appliance 15

C

Client ports 8

CloudStore Service Container (nbcssc) port 19

D

DataDomain ports 10

Deduplication 14

G

GRT ports 10

J

Java console ports 9

M

Master server ports 7

Media server ports 8

N

NAT and PAT 10

NDMP server ports 10

NetBackup CloudStore Service Container (nbcssc)
port 19

NetBackup ports 6

P

port numbers

CloudStore Service Container (nbcssc) 19

T

TCP ports 5

V

VERITAS_PBX

VNETD 5

VMware ports 17

vSphere Web Client Plug-in ports 17

W

web UI ports 9