

NetBackup™ Network Ports Reference Guide

Release 11.0

NetBackup™ Network Ports Reference Guide

Last updated: 2025-03-11

Legal Notice

Copyright © 2025 Cohesity, Inc. All rights reserved.

Cohesity, Veritas, the Cohesity Logo, Veritas Logo, Veritas Alta, Cohesity Alta, and NetBackup are trademarks or registered trademarks of Cohesity, Inc. 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 Cohesity 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 Cohesity 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 Cohesity, Inc. 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. Cohesity, Inc. 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 Cohesity 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.

Cohesity, Inc.
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 Cohesity 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 Cohesity 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 Cohesity community site:

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

Cohesity Services and Operations Readiness Tools (SORT)

Cohesity 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 primary server ports	7
	NetBackup media server ports	8
	NetBackup client ports	9
	NetBackup WORM storage server network ports	10
	NetBackup Snapshot Manager ports	11
	NetBackup web UI ports	12
	Java Console ports	13
	D-NAS ports	13
	NDMP server ports	14
	DataDomain OpenStorage ports	14
	NetBackup Granular Restore Technology (GRT) ports	14
	Network and port address translation	14
	Configuring ports for the NetBackup legacy Web Services	15
Chapter 3	Other Network Ports	18
	NetBackup deduplication ports	18
	NetBackup malware detection ports	19
	NetBackup VMware ports	20
	Port usage for the NetBackup vSphere Web Client Plug-in	20
	Nutanix AHV cluster ports	21
	Required ports for different arrays	21
	Port requirements for Kubernetes operator deployment	23
	NetBackup CloudStore Service Container (nbcssc) port	24
Index	26

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 primary server ports](#)
- [NetBackup media server ports](#)
- [NetBackup client ports](#)
- [NetBackup WORM storage server network ports](#)
- [NetBackup Snapshot Manager ports](#)
- [NetBackup web UI ports](#)
- [Java Console ports](#)
- [D-NAS 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.

Cohesity 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	Cohesity Private Branch Exchange Service
VNETD	13724	NetBackup Network service

NetBackup primary server ports

The primary server must be able to communicate with the media servers and clients.

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

Table 2-2 NetBackup primary server ports

Source	Destination	Service	Port
Primary server	Media server	VERITAS_PBX	1556
Primary server	Media server	VNETD	13724 ¹
Primary server	Client	VERITAS_PBX	1556
Primary server	Client	VNETD	13724 ₁
Primary server	Media server	NBSSC	5637 ²

1 - It applies while you use the Resilient Network feature or when NetBackup 8.0 or earlier primary 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 primary 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 primary 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	Primary server	VERITAS_PBX	1556
Media server	Primary 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	Primary server	NBWMC	5637 ¹
Media server	MSDP server	NFS	TCP 2049 ²
Media server	MSDP server	Portmapper	TCP/UDP 111 ²
Media server	MSDP server	Mountd	TCP 20048 ²
Media server	MSDP server	Webserver	443 ³
Media server	MSDP server	SMB/CIFS	TCP 445 ²

Table 2-3 NetBackup media server ports (*continued*)

Source	Destination	Service	Port
MSDP server	Cloud storage	<ul style="list-style-type: none"> ■ AWS-compatible services ■ Azure 	443

- * 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.
- ¹ 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 primary server fails if the older media servers use a different port.
- Must be opened from the media server to the target storage server (client).
- ³ Must be opened from the media server to the primary server.

NetBackup client ports

The client requires access to the primary 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	Primary server	VERITAS_PBX	1556
Client	Primary 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.

** Required while you use the Resilient Network feature.

NetBackup WORM storage server network ports

This topic provides the list of NetBackup ports that the WORM storage server requires to communicate with the NetBackup primary server, media server, and clients.

Table 2-5

Source	Destination	Service	Port
Management workstation	WORM storage server	SSH	22 ¹
Primary server	WORM storage server	Web server	443
Media server	WORM storage server	Deduplication Manager (spad)	10102
Media server	WORM storage server	Deduplication Engine (spool)	10082
Client	WORM storage server	Deduplication Manager (spad)	10102 ²
Client	WORM storage server	Deduplication Engine (spool)	10082 ²
Client	WORM storage server	NFS	2049
Client	WORM storage server	Portmapper	TCP/UDP 111
Client	WORM storage server	Mountd	20048
Client	WORM storage server	SMB/CIFS	445
Client	WORM storage server	rpc.statd	TCP/UDP 662
Client	WORM storage server	rpc.mountd	TCP/UDP 892

Table 2-5 (continued)

Source	Destination	Service	Port
WORM storage server	WORM storage server	NetBackup certificate management	10088 ³
WORM storage server	WORM storage server	SPWS	10086 ³
WORM storage server	Primary server	VERITAS_PBX	1556

1 - This port is used to access the deduplication shell for managing the WORM storage server. It is better to only allow access to this port from the management network.

2 - These ports are required when using the Client Direct feature.

3 - These are local host connections.

NetBackup Snapshot Manager ports

The following table lists the ports that are used between NetBackup and NetBackup Snapshot Manager. The required ports must be opened if firewall exists between the ports.

Table 2-6 Ports that must be open in a environment with NetBackup Snapshot Manager

Source	Port	Destination	Description
Primary server	443	Snapshot Manager	To handle API requests. If configured with default port else inbound must be allowed by firewall for custom port.
Media server	443	Snapshot Manager	To handle API requests. If configured with default port else inbound must be allowed by firewall for custom port.
Client	443	Snapshot Manager	To handle API requests. If configured with default port else inbound must be allowed by firewall for custom port.
Snapshot Manager agents	5671	Snapshot Manager	Interaction with Snapshot Manager agents.

Table 2-6 Ports that must be open in a environment with NetBackup Snapshot Manager (*continued*)

Source	Port	Destination	Description
Snapshot Manager	1556	Primary server	Registration with NetBackup primary server.

NetBackup Snapshot Manager for Cloud

Additional ports required for agentless communication with the protected VMs

The following table lists the additional network ports that are required and must be open when NetBackup Snapshot Manager for Cloud is using agentless communication with the protected VMs:

Table 2-7 Additional ports required for agentless communication with the protected VMs

Source	Port	Destination	Description
Snapshot Manager	22	Linux and Windows VM	For agentless connection to Linux/Windows VM (OpenSSH).

Additional ports required for Single File Restore (SFR) from a backup copy

- For Windows: Ports 139 and 445 must be open outbound from the clients (target VMs on which on-host agents are running) to access SMB share from the storage server(s).
- For Linux: Ports 2049 and 111, the standard NFS ports, 2049 and 111 must be open outbound from the clients (target VMs on which on-host agents are running) to access NFS share from the storage server(s).

NetBackup web UI ports

The NetBackup web UI uses the following ports for communication:

Table 2-8 NetBackup web UI ports

Source	Destination	Service	Port
Web browser	Primary server	NBWMC	443
Web browser	Primary server	NBWMC	13731 *

* Use this port only if smart card authentication is configured.

Java Console ports

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

Table 2-9 Java Console ports

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

D-NAS ports

The port requirements for D-NAS backup and restore are as follows:

Table 2-10 D-NAS port requirements

Source	Protocol	Port	Destination	Description
Backup host	TCP	1556	Primary server	PBX
Backup host	TCP	13724	Primary server	VNETD
Backup host	TCP	2049	Array	Required for NFS Access Version 4.
Backup host	TCP	111	Array	Required for NFS Access Versions 2 and 3.
Backup host	TCP	445	Array	SMB
Backup host	TCP	443	Snapshot Manager for Data Center	Default port to handle API requests. If you use a custom port, the firewall must allow the inbound traffic for the custom port.
Snapshot Manager for Data Center	TCP	1556	Primary server	Registration with the NetBackup primary server.

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 (`nbfssd`) 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](#).

NetBackup 8.3 and later versions support media servers in a private network that are connected to the primary server in a public network through a device that performs network address translation (NAT).

The TCP port used by the NetBackup Messaging Broker (`nbmqbroker`) service must be open from the clients to the primary 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 article [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 2-11 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/openv/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 2-11](#) 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 malware detection ports](#)
- [NetBackup VMware ports](#)
- [Port usage for the NetBackup vSphere Web Client Plug-in](#)
- [Nutanix AHV cluster ports](#)
- [Required ports for different arrays](#)
- [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 primary server.

Table 3-1 NetBackup deduplication port usage

Port	Usage
10082	This is the NetBackup Deduplication Engine (<code>spoold</code>) 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 (<code>spad</code>) 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.
10090	This is the Cohesity provision file system (VPFS) port that is used by MSDP. Open this port between: <ul style="list-style-type: none">■ The MSDP engines for NetBackup Flex Scale.■ The MSDP engines for NetBackup Cloud Scale.

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.

Note: For isolated recovery environment, TCP ports 1556, 10082, and 10102 are required to be opened only at the NetBackup source domain.

NetBackup malware detection ports

A scan host is a host machine that has the required malware tool configured. Once it is integrated with NetBackup, NetBackup initiates scanning on the scan host. The scan host must have a share type configured, that is, an NFS or SMB client. Malware scanner ports must be open for NFS or SMB exports to be accessible.

For more information on the requirements for scan host, refer to the 'Prerequisites for a scan host' section of *NetBackup Security and Encryption Guide*.

For more information on NFS and SMB, see the following:

[Running NFS Behind a Firewall](#)

[What ports need to be open for Samba to communicate with clients?](#)

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 3-2](#) shows the standard ports to be used in a NetBackup vSphere Web Client Plug-in environment.

Table 3-2 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 primary server	primary server
primary server	443	vCenter server
Backup host	443	vCenter server
Backup host	902 (for nbd or nbdssl)	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 3-3 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.

Required ports for different arrays

Depending on the storage device plug-ins configured in your environment, additional network ports must be open for the NetBackup Snapshot Manager for Data Center.

Table 3-4 Ports for different array vendors

Destination	Port	Description
Dell EMC PowerMax or VMax	8443	DELL EMC Unisphere APIs
Dell EMC PowerFlex	443	REST API SDK
Dell EMC PowerScale (Isilon)	9021	REST API SDK
Dell EMC PowerStore	443	Python SDK from Dell EMC: Python-Powerstore (1.4.0)
Dell EMC XtremIO	443	REST API

Table 3-4 Ports for different array vendors (*continued*)

Destination	Port	Description
Unisphere managing the Dell EMC Unity	443	Storops SDK python library
Fujitsu Eternus AF/DX	443	REST API
Fujitsu Eternus AB/HB or proxy server managing the array	443	WSAPI
HPE RMC	443	REST API
HPE XP Configuration Manager REST server	443	REST API
HPE Alletra 9000	443	WSAPI
HPE Alletra 6000	443	REST API
HPE GreenLake for Block Storage	443	WSAPI
Hitachi NAS	8444	REST API
Hitachi SAN	8444	REST API
IBM Storwize SAN V7000	7443	REST API
IBM FlashSystem	7443	REST API
IBM SAN Volume Controller	7443	REST API
InfiniBox SAN	443	InfiniSDK
InfiniBox NAS	443	REST API
Lenovo DM 5000	443	ZAPI or REST API
NetApp FAS	443	ZAPI or REST API
NetApp Cloud Volumes ONTAP (CVO)	443	REST API
Amazon FSx for NetApp ONTAP	443	REST API
NetApp E-Series or proxy server managing the array	8443	WSAPI
Nutanix Files File Server	9440	REST API
Pure Storage FlashArray	443	Pure Storage SDK
Pure Storage FlashBlade	443	Pure Storage SDK

Table 3-4 Ports for different array vendors (*continued*)

Destination	Port	Description
PowerMax eNAS	443	XML API
Qumulo NAS, any management interface	443	REST API

Port requirements for Kubernetes operator deployment

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

Table 3-5 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 3-6 NetBackup CloudStore Service Container (nbcssc) port

Port	Source	Destination	Process	Description
5637	Media server 7.7.x to 8.1.2 only	Primary server	NBWMC	<p>Allow communication between primary 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 primary server fails if the older media servers use a different port.</p>
5637	Primary server	Media server 7.7.x to 8.1.2 only	NBCSSC	<p>Allow communication between primary 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 primary 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/openv/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

C

CloudStore Service Container (nbcssc) port 24

D

DataDomain ports 14

Deduplication 18

G

GRT ports 14

N

NAT and PAT 14

NDMP server ports 14

NetBackup CloudStore Service Container (nbcssc)
port 24

NetBackup ports 6

P

port numbers

CloudStore Service Container (nbcssc) 24

T

TCP ports 5

V

VERITAS_PBX

VNETD 5

VMware ports 20

vSphere Web Client Plug-in ports 20