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/
Chapter 1  About the NetBackup network ports ................................. 5
TCP ports used by NetBackup .......................................................... 5
Compatibility with back-level hosts ............................................... 5

Chapter 2  NetBackup Ports ................................................................. 7
NetBackup default ports .................................................................. 7
NetBackup master server ports ......................................................... 8
NetBackup media server ports .......................................................... 9
NetBackup client ports .................................................................... 9
Java server ports .......................................................................... 10
Java Console ports ....................................................................... 10
NDMP server ports ....................................................................... 11
DataDomain OpenStorage ports ...................................................... 11
NetBackup Granular Restore Technology (GRT) ports ......................... 11
Network and Port address translation ............................................... 12

Chapter 3  Other Network Ports .......................................................... 13
NetBackup deduplication ports ........................................................ 13
About communication ports and firewall considerations in OpsCenter
Communication ports used by key OpsCenter components .......... 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 .................... 19
NetBackup CloudStore Service Container (nbcssc) ...................... 20

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

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.
NetBackup Ports

This chapter includes the following topics:

- NetBackup default ports
- NetBackup master server ports
- NetBackup media server ports
- NetBackup client ports
- Java server ports
- Java Console ports
- NDMP server ports
- DataDomain OpenStorage ports
- NetBackup Granular Restore Technology (GRT) ports
- Network and Port address translation

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>
<thead>
<tr>
<th>Table 2-1</th>
<th>NetBackup ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service</strong></td>
<td><strong>Port</strong></td>
</tr>
<tr>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>VNETD</td>
<td>13724</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Table 2-2</th>
<th>NetBackup master server ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>Master server</td>
<td>Media server</td>
</tr>
<tr>
<td>Master server</td>
<td>Client</td>
</tr>
<tr>
<td>Master server</td>
<td>Client</td>
</tr>
<tr>
<td>Master server</td>
<td>Java server</td>
</tr>
<tr>
<td>Master server</td>
<td>Netware</td>
</tr>
<tr>
<td>Master server</td>
<td>Netware</td>
</tr>
</tbody>
</table>

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>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media server</td>
<td>Master server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Media server</td>
<td>Master server</td>
<td>VNETD</td>
<td>13724*</td>
</tr>
<tr>
<td>Media server</td>
<td>Media server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Media server</td>
<td>Media server</td>
<td>VNETD</td>
<td>13724*</td>
</tr>
<tr>
<td>Media server</td>
<td>Client</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Media server</td>
<td>Client</td>
<td>VNETD</td>
<td>13724*</td>
</tr>
<tr>
<td>Media server</td>
<td>MSDP server</td>
<td>Deduplication 10102 Manager (spad)</td>
<td>10102</td>
</tr>
<tr>
<td>Media server</td>
<td>MSDP server</td>
<td>Deduplication Engine (spoold)</td>
<td>10082</td>
</tr>
<tr>
<td>Media server</td>
<td>Netware client</td>
<td>VNETD</td>
<td>13724</td>
</tr>
<tr>
<td>Media server</td>
<td>Netware client</td>
<td>BPCD</td>
<td>13782</td>
</tr>
</tbody>
</table>

* 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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Master server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Client</td>
<td>Master server</td>
<td>VNETD</td>
<td>13724 *</td>
</tr>
<tr>
<td>Client</td>
<td>Media server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Client</td>
<td>Media server</td>
<td>VNETD</td>
<td>13724 **</td>
</tr>
<tr>
<td>Client</td>
<td>MSDP server</td>
<td>Deduplication Manager (spad)</td>
<td>10102</td>
</tr>
<tr>
<td>Client</td>
<td>MSDP server</td>
<td>Deduplication Engine (spoold)</td>
<td>10082</td>
</tr>
</tbody>
</table>

* 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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java server</td>
<td>Master server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Java server</td>
<td>Master server</td>
<td>VNETD</td>
<td>13724</td>
</tr>
<tr>
<td>Java server</td>
<td>Media server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Java server</td>
<td>Media server</td>
<td>VNETD</td>
<td>13724</td>
</tr>
</tbody>
</table>

Java Console ports

The Java Console uses the Java Server for further communication; it requires the following ports:
### Table 2-6 Java Console ports

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Console</td>
<td>Master server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Java Console</td>
<td>Master server</td>
<td>VNETD</td>
<td>13724</td>
</tr>
<tr>
<td>Java Console</td>
<td>Java Server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Java Console</td>
<td>Java Server</td>
<td>VNETD</td>
<td>13724</td>
</tr>
</tbody>
</table>

### 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.
Other Network Ports

This chapter includes the following topics:

- NetBackup deduplication ports
- About communication ports and firewall considerations in OpsCenter
- 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
- NetBackup CloudStore Service Container (nbcssc)

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Usage</th>
</tr>
</thead>
</table>
| 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 fingerprinting. |

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.
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>
<thead>
<tr>
<th>Source Host</th>
<th>Destination Host</th>
<th>Port Number</th>
<th>Usage (Process Name)</th>
<th>Port Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpsCenter Server</td>
<td>Mail server</td>
<td>25</td>
<td>SMTP</td>
<td>Allow from source to destination.</td>
</tr>
<tr>
<td>OpsCenter Server</td>
<td>SNMP Server</td>
<td>162</td>
<td>SNMP trap recipient</td>
<td>Allow from source to destination.</td>
</tr>
<tr>
<td>OpsCenter Server</td>
<td>NetBackup Master</td>
<td>1556</td>
<td>PBX (pbx_exchange)</td>
<td>Allow between source and destination (bi-directional). PBX port number configuration is not supported.</td>
</tr>
<tr>
<td>OpsCenter Client</td>
<td>OpsCenter Server</td>
<td>1556</td>
<td>PBX (pbx_exchange)</td>
<td>Allow between source and destination. Some hardened servers and firewall configurations may block this port. PBX port number configuration is not supported.</td>
</tr>
<tr>
<td>Web browser</td>
<td>OpsCenter Server</td>
<td>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)</td>
<td>HTTPS</td>
<td>Allow from all hosts on network.</td>
</tr>
</tbody>
</table>
Table 3-2

Communication ports used by key OpsCenter components (continued)

<table>
<thead>
<tr>
<th>Source Host</th>
<th>Destination Host</th>
<th>Port Number</th>
<th>Usage (Process Name)</th>
<th>Port Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpsCenter Server</td>
<td>OpsCenter Server</td>
<td>13786</td>
<td>Sybase database (dbsrv16)</td>
<td>Allow between source and destination. Some hardened servers and firewall configurations may block this port.</td>
</tr>
<tr>
<td>OpsCenter Server</td>
<td>OpsCenter Server</td>
<td>1556</td>
<td>OpsCenter Product Authentication Service (opsatd)</td>
<td>Allow between source and destination in case NBAC is enabled on NetBackup master server.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command line</td>
<td>Appliance</td>
<td>22</td>
<td>ssh</td>
<td>In-band management CLI</td>
</tr>
<tr>
<td>Web browser</td>
<td>Appliance</td>
<td>80</td>
<td>http</td>
<td>In-band management GUI</td>
</tr>
<tr>
<td>Web browser</td>
<td>Appliance</td>
<td>443</td>
<td>https</td>
<td>In-band management GUI</td>
</tr>
<tr>
<td>Web browser</td>
<td>Appliance IPMI</td>
<td>80</td>
<td>http</td>
<td>Out-of-band mgmt (ISM+ or RM*)</td>
</tr>
</tbody>
</table>
### Table 3-3  
Inbound ports (continued)

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

+ NetBackup Integrated Storage Manager


**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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance</td>
<td>Call Home server</td>
<td>443</td>
<td>https</td>
<td>Call Home notifications to Veritas</td>
</tr>
<tr>
<td>Appliance</td>
<td>SNMP Server</td>
<td>162*</td>
<td>SNMP</td>
<td>Outbound traps and alerts</td>
</tr>
<tr>
<td>Appliance</td>
<td>SCSP host</td>
<td>443</td>
<td>https</td>
<td>Download SCSP certificates</td>
</tr>
</tbody>
</table>
* 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

<table>
<thead>
<tr>
<th>Source</th>
<th>Port number</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>9443</td>
<td>vSphere Web Client</td>
</tr>
<tr>
<td>For VM recovery: vCenter server (or vSphere Web Client server if deployed independently)</td>
<td>RESTful interface at port 8443 (https) or as configured on the master server</td>
<td>Master server</td>
</tr>
<tr>
<td>Master server</td>
<td>443</td>
<td>vCenter server</td>
</tr>
<tr>
<td>Backup host</td>
<td>443</td>
<td>vCenter server</td>
</tr>
<tr>
<td>Backup host</td>
<td>902 (for nbd or nbdssl)</td>
<td>ESXi</td>
</tr>
</tbody>
</table>
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
Symbols
5200 and 5220 appliance 17

C
Client ports 9

D
DataDomain ports 11
Deduplication 13

F
firewall considerations 14

G
GRT ports 11

J
Java console ports 10
Java server ports 10

M
Master server ports 8
Media server ports 9

N
NAT and PAT 12
NDMP server ports 11
NetBackup CloudStore Service Container (nbcssc) 20
NetBackup ports 7

P
port numbers
  key OpsCenter components 14

T
TCP ports 5

V
VERITAS_PBX
  VNETD 5
  VMware ports 19
  vSphere Web Client Plug-in ports 19