Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

support.symantec.com

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

support.symantec.com

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:


Customer service

Customer service information is available at the following URL:


Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

<table>
<thead>
<tr>
<th>Region</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific and Japan</td>
<td><a href="mailto:customercare_apj@symantec.com">customercare_apj@symantec.com</a></td>
</tr>
<tr>
<td>Europe, Middle-East, and Africa</td>
<td><a href="mailto:semea@symantec.com">semea@symantec.com</a></td>
</tr>
<tr>
<td>North America and Latin America</td>
<td><a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a></td>
</tr>
</tbody>
</table>
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 7.0.1 and later versions use a minimum set of TCP ports, primarily VERITAS_PBX (1556).

NetBackup versions 7.0 primarily use the VERITAS_PBX (1556) and VNETD (13724) ports. NetBackup 7.0.1 and newer servers first attempt to connect to VERITAS_PBX.
If unsuccessful, the connection is retried to VNETD. If still unsuccessful, the connection is retried to the daemon or service-specific port.

If connections are being made to an unexpected destination port, it is likely that the Connect Options for the target host are not using the default setting. It is also possible that a problem in networking, operating systems, or applications is preventing consistent connections to the default ports. To fix the problem, check the following:

- When checking Connect Options, review the Client Attributes configuration (bpclient) on the master server, the destination-specific firewall configuration on the source server, and the global Default Connect Options.
- 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 bptestbpcd and bptestnetconn commands to check connectivity to NetBackup hosts of any version.
NetBackup Ports

This chapter includes the following topics:

- NetBackup 7.x default ports
- NetBackup master server ports
- NetBackup media server ports
- NetBackup client ports
- Novell NetWare ports
- Windows Administration Console 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 7.x default ports

NetBackup 7.x primarily uses the ports shown in Table 2-1 as the destination port when connecting to the various services. Symantec 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 7.x Administration Guides*, volumes 1 & 2.

The following table lists the ports required by NetBackup 7.x to connect to various services.

**Table 2-1**  NetBackup 7.x ports

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERITAS_PBX</td>
<td>1556</td>
<td>Symantec Private Branch Exchange Service</td>
</tr>
<tr>
<td>VNETD</td>
<td>13724</td>
<td>NetBackup Network service</td>
</tr>
<tr>
<td>VRTS-AT-PORT</td>
<td>2821</td>
<td>VxSS Authentication Service (vxatd) *</td>
</tr>
<tr>
<td>VRTS-AUTH-PORT</td>
<td>4032</td>
<td>VxSS Authorization Service (vxazd) *</td>
</tr>
</tbody>
</table>

* These services and associated ports are only needed for NetBackup 7.0.1 and previous releases. These processes were replaced in NetBackup 7.1 by nbatd and nbazd, which listen on ports 13783 and 13722, respectively. The new processes are also registered with and reachable through VERITAS_PBX, so it is not necessary to open 13783 and 13722 through the firewall. You only need to open 1556.

**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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master server</td>
<td>EMM server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Master server</td>
<td>Media server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
</tbody>
</table>
Table 2-2  NetBackup master server ports (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master server</td>
<td>Media server</td>
<td>VNETD</td>
<td>13724 *</td>
</tr>
<tr>
<td>Master server</td>
<td>Client</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Master server</td>
<td>Client</td>
<td>VNETD</td>
<td>13724 **</td>
</tr>
<tr>
<td>Master server</td>
<td>NetBackup Administration Console</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Master server</td>
<td>Java server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Master server</td>
<td>Netware</td>
<td>VNETD</td>
<td>13724</td>
</tr>
<tr>
<td>Master server</td>
<td>Netware</td>
<td>BPCD</td>
<td>13782</td>
</tr>
<tr>
<td>Master server</td>
<td>VxSS</td>
<td>VRTS-AT-PORT</td>
<td>2821</td>
</tr>
<tr>
<td>Master server</td>
<td>VxSS</td>
<td>VRTS-AUTH-PORT</td>
<td>4032</td>
</tr>
</tbody>
</table>

* Only needed for pre- 7.0.1 media servers.
** Only needed for pre- 7.0.1 clients.

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

<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>EMM server</td>
<td>VERITAS_PBX</td>
<td>1556</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>
</tbody>
</table>
### NetBackup media server ports (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media server</td>
<td>Client</td>
<td>VNETD</td>
<td>13724 **</td>
</tr>
<tr>
<td>Media server</td>
<td>PureDisk server</td>
<td>Storage Pool Authority (SPA)</td>
<td>443</td>
</tr>
<tr>
<td>Media server</td>
<td>PureDisk server</td>
<td>Content Router (spoold)</td>
<td>10082</td>
</tr>
<tr>
<td>Media server</td>
<td>VxSS server</td>
<td>VRTS-AT-PORT</td>
<td>2821</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>VxSS server</td>
<td>VRTS-AUTH-PORT</td>
<td>4032</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>

* Only needed for pre-7.0.1 media servers.

** Only needed for pre-7.0.1 clients or 7.5+ resilient clients.

---

### NetBackup client ports

The client requires access to the master server to initiate user and client-initiated operations. The client must also be able to connect to the media servers in the following circumstances:

- If non-default connect options are configured for the client.
- If application backups such as Oracle and SQL are used.
- When using the client-side deduplication, the client must also be able to communicate with the following:
  - MSDP media servers
    All servers in a PureDisk Storage Pool, including the Storage Pool Authority (SPA), and Content Routers (CR).

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>
<tr>
<td>Client</td>
<td>PureDisk server</td>
<td>Storage Pool Authority (SPA)</td>
<td>443</td>
</tr>
<tr>
<td>Client</td>
<td>PureDisk server</td>
<td>Content Router (spoold)</td>
<td>10082</td>
</tr>
<tr>
<td>Client</td>
<td>VxSS server</td>
<td>VRTS-AT-PORT</td>
<td>2821</td>
</tr>
</tbody>
</table>

Novell NetWare ports

The following ports must be open to backup the NetWare servers:

Table 2-5  Novell Netware ports

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetWare</td>
<td>Master</td>
<td>BPRD</td>
<td>13720</td>
</tr>
<tr>
<td>NetWare</td>
<td>Master</td>
<td>VNETD</td>
<td>13724</td>
</tr>
<tr>
<td>NetWare</td>
<td>Media</td>
<td>VNETD</td>
<td>13724</td>
</tr>
</tbody>
</table>

Windows Administration Console ports

To use the Windows Administration console, which is a native Windows application, you must first add the DNS name of the workstation or server to the list of "trusted"
servers in the master server. The following table describes the ports required by the Windows Administration Console:

### Table 2-6  Windows Administration Console ports

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Administration Console</td>
<td>Master server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Windows Administration Console</td>
<td>Master server</td>
<td>VNETD</td>
<td>13724</td>
</tr>
<tr>
<td>Windows Administration Console</td>
<td>EMM server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Windows Administration Console</td>
<td>Media server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
<tr>
<td>Windows Administration Console</td>
<td>Media server</td>
<td>VNETD</td>
<td>13724</td>
</tr>
<tr>
<td>Windows Administration Console</td>
<td>VxSS server</td>
<td>VRTS-AT-PORT</td>
<td>2821</td>
</tr>
</tbody>
</table>

### 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 2-7  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>EMM server</td>
<td>VERITAS_PBX</td>
<td>1556</td>
</tr>
</tbody>
</table>
### Java Server ports (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Java server</td>
<td>VxSS server</td>
<td>VRTS-AT-PORT</td>
<td>2821</td>
</tr>
</tbody>
</table>

### Java Console ports

Many users prefer to use the Java Console instead of the Windows Administration Console. The Java Console uses the Java Server for further communication; it requires only the following 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
- Port and firewall considerations for NetBackup OpsCenter
- NetBackup 5200 and 5220 appliance ports (for firewall between master and media server)
- Port usage for NetBackup PureDisk Release 6.6 and later
- NetBackup VMware ports

NetBackup deduplication ports

The following table shows the ports that are used for NetBackup deduplication that includes Media Server Deduplication (MSDP), PureDisk Deduplication Option (PDDO), 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:** It is not necessary to open these ports if using a simple MSDP configuration where each client passes the backup image directly to only one media server for deduplication. Some examples are, using only MSDP and not PDDO or not using client deduplication, server load balancing, or optimized duplication. In this configuration, there is only normal communication between the media servers and clients using the default ports.
Table 3-1  NetBackup deduplication port usage

<table>
<thead>
<tr>
<th>Port</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>10082</td>
<td>This is the NetBackup Deduplication Engine (spoold) port that is used by both MSDP and PDDO. Open this port between:</td>
</tr>
<tr>
<td></td>
<td>■ The deduplication client and the storage servers.</td>
</tr>
<tr>
<td></td>
<td>■ The MSDP or the PDDO server and the storage servers.</td>
</tr>
<tr>
<td></td>
<td>10102</td>
</tr>
<tr>
<td></td>
<td>■ The deduplication client and the MSDP servers.</td>
</tr>
<tr>
<td></td>
<td>■ The MSDP server and any Additional servers that handle fingerprinting.</td>
</tr>
<tr>
<td></td>
<td>443</td>
</tr>
<tr>
<td></td>
<td>■ The deduplication client and the PureDisk storage servers.</td>
</tr>
<tr>
<td></td>
<td>■ The PDDO server and the PureDisk storage servers.</td>
</tr>
</tbody>
</table>

Ports 10082 and either 10102 (MSDP) or 443 (PDDO) 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 either 10102 (MSDP) or 443 (PDDO) must be open between the NetBackup domains.

Port and firewall considerations for NetBackup OpsCenter

This topic provides information about the communication ports and firewall considerations for NetBackup OpsCenter.

The following image displays the key NetBackup OpsCenter components and how they communicate:
The SMTP recipient ports can be configured from the NetBackup OpsCenter console (using the Settings > Configuration > SMTP Server options). The SNMP trap recipient ports can also be configured from the Symantec OpsCenter console (using the Settings > Recipients > SNMP options).

If these ports are changed, then the appropriate hardware ports must be opened.
The following table describes the communication port usage for NetBackup OpsCenter:

**Table 3-2** Communication ports used by key NetBackup 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>Symantec OpsCenter Server</td>
<td>Mail Server</td>
<td>25</td>
<td>SMTP</td>
<td>Allow from source to destination.</td>
</tr>
<tr>
<td>Symantec OpsCenter Server</td>
<td>SNMP Server</td>
<td>162</td>
<td>SNMP trap</td>
<td>Allow from source to destination.</td>
</tr>
<tr>
<td>Symantec OpsCenter Server</td>
<td>NetBackup Master Server(s)</td>
<td>1556</td>
<td>PBX (pbx_exchange)</td>
<td>Allow between source and destination (bi-directional). PBX port number configuration is supported.</td>
</tr>
<tr>
<td>Symantec OpsCenter Client</td>
<td>Symantec 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>
</tbody>
</table>
Table 3-2 Communication ports used by key NetBackup OpsCenter components (continued)

<table>
<thead>
<tr>
<th>Source Host</th>
<th>Destination Host</th>
<th>Port Number</th>
<th>Port Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web browser</td>
<td>Symantec OpsCenter Server</td>
<td>Port Number</td>
<td>Port Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following HTTP and HTTPS ports are checked for availability in the specified sequence and the first available port combination is used by default:</td>
<td>Allow from all hosts on network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>80 (HTTP) and 443 (HTTPS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>8181 (HTTP) and 8443 (HTTPS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>8282 (HTTP) and 8553 (HTTPS)</td>
</tr>
<tr>
<td>Symantec OpsCenter Server</td>
<td>Symantec OpsCenter Server</td>
<td>13786</td>
<td>Sybase database (dbsrv12)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allow between source and destination.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Some hardened servers and firewall configurations may block this port.</td>
</tr>
<tr>
<td>Symantec OpsCenter Server</td>
<td>Host where Symantec Product Authentication Service (AT) Server is installed</td>
<td>2821</td>
<td>NetBackup Product Authentication Service (vxatd)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></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>
<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>
<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>
</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>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>

* Symantec 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 Symantec</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.

Port usage for NetBackup PureDisk Release 6.6 and later

The following image displays the communication ports between client agents and a storage pool for PureDisk.
Figure 3-2  Communication ports
The following table describes the information about ports required between client agents and their storage pool:

**Table 3-5** PureDisk port usage between client agents and storage pools

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose and notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client agents</td>
<td>Controller</td>
<td>10101</td>
<td>TCP</td>
<td>Registers, authenticates, and controls a metabase engine always hosts a controller service</td>
</tr>
<tr>
<td>Client agents</td>
<td>Content router</td>
<td>10082</td>
<td>TCP</td>
<td>Sends data.</td>
</tr>
<tr>
<td>Client agents</td>
<td>Storage pool authority</td>
<td>443 (HTTPS)</td>
<td>TCP</td>
<td>Checks and updates actions on the client side.</td>
</tr>
<tr>
<td>Client agents</td>
<td>DNS server</td>
<td>53</td>
<td>UDP and TCP</td>
<td>Used when you install PureDisk with FQDNs or hostnames. Not used if you install PureDisk with the IP addresses.</td>
</tr>
</tbody>
</table>

For details about PureDisk, refer to the PureDisk Getting Started Guide.

The following table describes the information about ports between the storage pool authority node and other services:

**Table 3-6** PureDisk port usage between the storage pool authority node and other services

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose and notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage pool authority</td>
<td>All PureDisk node services</td>
<td>22 (SSH)</td>
<td>TCP</td>
<td>Facilitates the PureDisk installation, upgrades, and maintenance.</td>
</tr>
<tr>
<td>Administrator’s host system</td>
<td>Storage pool authority</td>
<td>22 (SSH)</td>
<td>TCP</td>
<td>Performs inquiries.</td>
</tr>
<tr>
<td>All PureDisk node services</td>
<td>Storage pool authority</td>
<td>123</td>
<td>TCP and UDP</td>
<td>Synchronizes the time using NTPD service.</td>
</tr>
<tr>
<td>All PureDisk node services</td>
<td>Storage pool authority</td>
<td>443 (HTTPS)</td>
<td>TCP</td>
<td>Monitors the communication among all other services.</td>
</tr>
<tr>
<td>Administrator’s host system</td>
<td>Storage pool authority</td>
<td>443 (HTTPS)</td>
<td>TCP</td>
<td>Connects to the storage pool authority and then to the PureDisk administrative Web UI.</td>
</tr>
</tbody>
</table>
Table 3-6  PureDisk port usage between the storage pool authority node and other services (continued)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
<th>Purpose and notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage pool authority</td>
<td>Root broker host</td>
<td>2821</td>
<td>TCP</td>
<td>Authenticates between each node. Authentication from the storage pool authority to the broker.</td>
</tr>
<tr>
<td>All PureDisk nodes</td>
<td>Content router</td>
<td>10082</td>
<td>TCP</td>
<td>Exchanges data.</td>
</tr>
<tr>
<td>Metabase server</td>
<td>Metabase engine</td>
<td>10085</td>
<td>TCP</td>
<td>Processes any queries on data selections. This port should be open only on metabase engine nodes.</td>
</tr>
<tr>
<td>All PureDisk nodes and all clients</td>
<td>Metabase engine</td>
<td>10101</td>
<td>TCP</td>
<td>Controls the client agent software on the clients. Client agents and server agents connect to the storage pool through the controller.</td>
</tr>
<tr>
<td>All PureDisk node services (not shown in figure)</td>
<td>Storage pool authority node</td>
<td>10087</td>
<td>UDP</td>
<td>Facilitates debugging with the debug logging daemon (DLD).</td>
</tr>
<tr>
<td>All PureDisk node services</td>
<td>NetBackup ports</td>
<td></td>
<td></td>
<td>Facilitates any disaster recovery through NetBackup. This communication is bidirectional. Used only when disaster recovery through NetBackup is implemented.</td>
</tr>
<tr>
<td>NetBackup Export Engine gateways</td>
<td>NetBackup</td>
<td></td>
<td></td>
<td>Facilitates any exports to NetBackup. This communication is bidirectional. Used only when the NetBackup export engine is implemented.</td>
</tr>
</tbody>
</table>

NetBackup VMware ports

The TCP ports 443 and 902 are required to access the VMware infrastructure.
NetBackup must connect to TCP port 443 to access the vCenter server. NetBackup can connect to the vCenter server only through this port for information such as the VM discovery requests, snapshot creation and deletion, and so on.

The backup host must also connect to the TCP port 902 on the ESX/ESXi hosts. In specific cases, the backup host must also connect to the TCP port 902 on the ESX/ESXi hosts.

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.

**Figure 3-3** VMware ports

SAN and NBD Transports using a physical VMware backup host
Figure 3-4  VMware ports

TCP Port 443: VM Discovery, Snapshot Requests, VM creations during recovery

TCP Port 902: if HotAdd/NBD/NBDS SSL Transport or using direct restores via ESX. VDDK uses 902 behind the scenes for these use cases.
Symbols
5200 and 5220 appliance 22

C
Client ports 12

D
DataDomain ports 15
Deduplication 17

G
GRT ports 16

J
Java console ports 15
Java server ports 14

M
Master server ports 10
Media server ports 11

N
NAT and PAT 16
NDMP server ports 15
NetBackup ports 9
Novell Netware ports 13

O
OpsCenter 18

P
Ports for Windows Administration Console 13
PureDisk 23

T
TCP ports 7

V
VERITAS_PBX
VNETD 7
VMware ports 26