Symantec NetBackup™ Network Ports Reference Guide

Release 7.6

Symantec™

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 7.6

Legal Notice

This Symantec product may contain third party software for which Symantec 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. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

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 Symantec Corporation 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. SYMANTEC CORPORATION 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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. 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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

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:

www.symantec.com/business/support/

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:

www.symantec.com/business/support/

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:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

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 6.0 to 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.

Chapter 2

NetBackup Ports

This chapter includes the following topics:

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

Service	Port	Description
VERITAS_PBX	1556	Symantec Private Branch Exchange Service
VNETD	13724	NetBackup Network service
VRTS-AT-PORT	2821	VxSS Authentication Service (vxatd) *
VRTS-AUTH-PORT	4032	VxSS Authorization Service (vxazd) *

* 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

Source	Destination	Service	Port
Master server	EMM server	VERITAS_PBX	1556
Master server	Media server	VERITAS_PBX	1556

Table 2-2 NetBackup master server ports *(continued)*

Source	Destination	Service	Port
Master server	Media server	VNETD	13724 *
Master server	Client	VERITAS_PBX	1556
Master server	Client	VNETD	13724 **
Master server	NetBackup Administration Console	VERITAS_PBX	1556
Master server	Java server	VERITAS_PBX	1556
Master server	Netware	VNETD	13724
Master server	Netware	BPCD	13782
Master server	VxSS	VRTS-AT-PORT	2821
Master server	VxSS	VRTS-AUTH-PORT	4032

* 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

Source	Destination	Service	Port
Media server	Master server	VERITAS_PBX	1556
Media server	Master server	VNETD	13724 *
Media server	EMM server	VERITAS_PBX	1556
Media server	Media server	VERITAS_PBX	1556
Media server	Media server	VNETD	13724 *
Media server	Client	VERITAS_PBX	1556

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

Source	Destination	Service	Port
Media server	Client	VNETD	13724 * *
Media server	PureDisk server	Storage Pool Authority (SPA)	443
Media server	PureDisk server	Content Router (spoold)	10082
Media server	VxSS server	VRTS-AT-PORT	2821
Media server	MSDP server	Deduplication 10102 Manager (spad)	10102
Media server	MSDP server	Deduplication Engine (spoold)	10082
Media server	VxSS server	VRTS-AUTH-PORT	4032
Media server	Netware client	VNETD	13724
Media server	Netware client	BPCD	13782

* 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

Source	Destination	Service	Port
Client	Master server	VERITAS_PBX	1556
Client	Master server	VNETD	13724 *
Client	Media server	VERITAS_PBX	1556
Client	Media server	VNETD	13724 * *
Client	MSDP server	Deduplication Manager (`spad`)	10102
Client	MSDP server	Deduplication Engine (`spoold`)	10082
Client	PureDisk server	Storage Pool Authority (SPA)	443
Client	PureDisk server	Content Router (spoold)	10082
Client	VxSS server	VRTS-AT-PORT	2821

* Only needed for pre- 7.0.1 clients.

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

Novell NetWare ports

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

Table 2-5 Novell Netware ports

Source	Destination	Service	Port
NetWare	Master	BPRD	13720
NetWare	Master	VNETD	13724
NetWare	Media	VNETD	13724

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

Source	Destination	Service	Port
Windows Administration Console	Master server	VERITAS_PBX	1556
Windows Administration Console	Master server	VNETD	13724
Windows Administration Console	EMM server	VERITAS_PBX	1556
Windows Administration Console	Media server	VERITAS_PBX	1556
Windows Administration Console	Media server	VNETD	13724
Windows Administration Console	VxSS server	VRTS-AT-PORT	2821

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

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

Table 2-7 Java Server ports *(continued)*

Source	Destination	Service	Port
Java server	Media server	VERITAS_PBX	1556
Java server	Media server	VNETD	13724
Java server	VxSS server	VRTS-AT-PORT	2821

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 2-8 Java Console ports

Source	Destination	Service	Port
Java Console	Master server	VERITAS_PBX	1556
Java Console	Master server	VNETD	13724
Java Console	Java Server	VERITAS_PBX	1556
Java Console	Java Server	VNETD	13724

NDMP server ports

The port requirements to backup and restore an NDMP server are as follows:

- TCP port 10000 must be open from the media server (DMA) to the NDMP filer (tape or disk) for all types of NDMP operations; local, remote, and 3-way.
- The NetBackup SERVER_PORT_WINDOW must be open inbound from the filer to the media server for remote NDMP. It must also be open for efficient catalog file (TIR data) movement during local or 3-way NDMP.

DataDomain OpenStorage ports

The following ports must be open to use a DataDomain OST storage server.

- The TCP ports for 2049 (`nfs`), 111 (`portmapper`), and 2052 (`mountd`) must be open from the media server to the target storage server.

- The UDP port 111 (`portmapper`) must be open from the media server to the target storage server.
- The TCP port 2051 (`replication`) must also be open from the media server to the storage server for optimized duplication.

NetBackup Granular Restore Technology (GRT) ports

The following ports must be open to use the GRT feature of NetBackup.

- TCP port 111 (`portmapper`) needs to be open from the client to the media server.
- TCP port 7394 (`nbfsd`) needs to be open from the client to the media server.

Network and Port address translation

NetBackup does not currently support the use of Network Address Translation (NAT) or the Port Address Translation (PAT).

For additional details see, the technote TECH15006.

Chapter 3

Other Network Ports

This chapter includes the following topics:

NetBackup deduplication ports

The following table shows the ports that are used for NetBackup deduplication that includes Media Server Deduplication (MSDP), 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

Port	Usage
10082	This is the NetBackup Deduplication Engine (`spoold`) port that is used by both MSDP and PDDO. Open this port between: ▪ The deduplication client and the storage servers. ▪ The MSDP or the PDDO server and the storage servers.
10102	This is the NetBackup Deduplication Manager (`spad`) port that is used by MSDP. Open this port between: ▪ The deduplication client and the MSDP servers. ▪ The MSDP server and any Additional servers that handle finger printing.
443	This is the Storage Pool Authority (SPA) Web services port that is used by PDDO. Open this port between: ▪ The deduplication client and the PureDisk storage servers. ▪ The PDDO server and the PureDisk storage servers.

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.

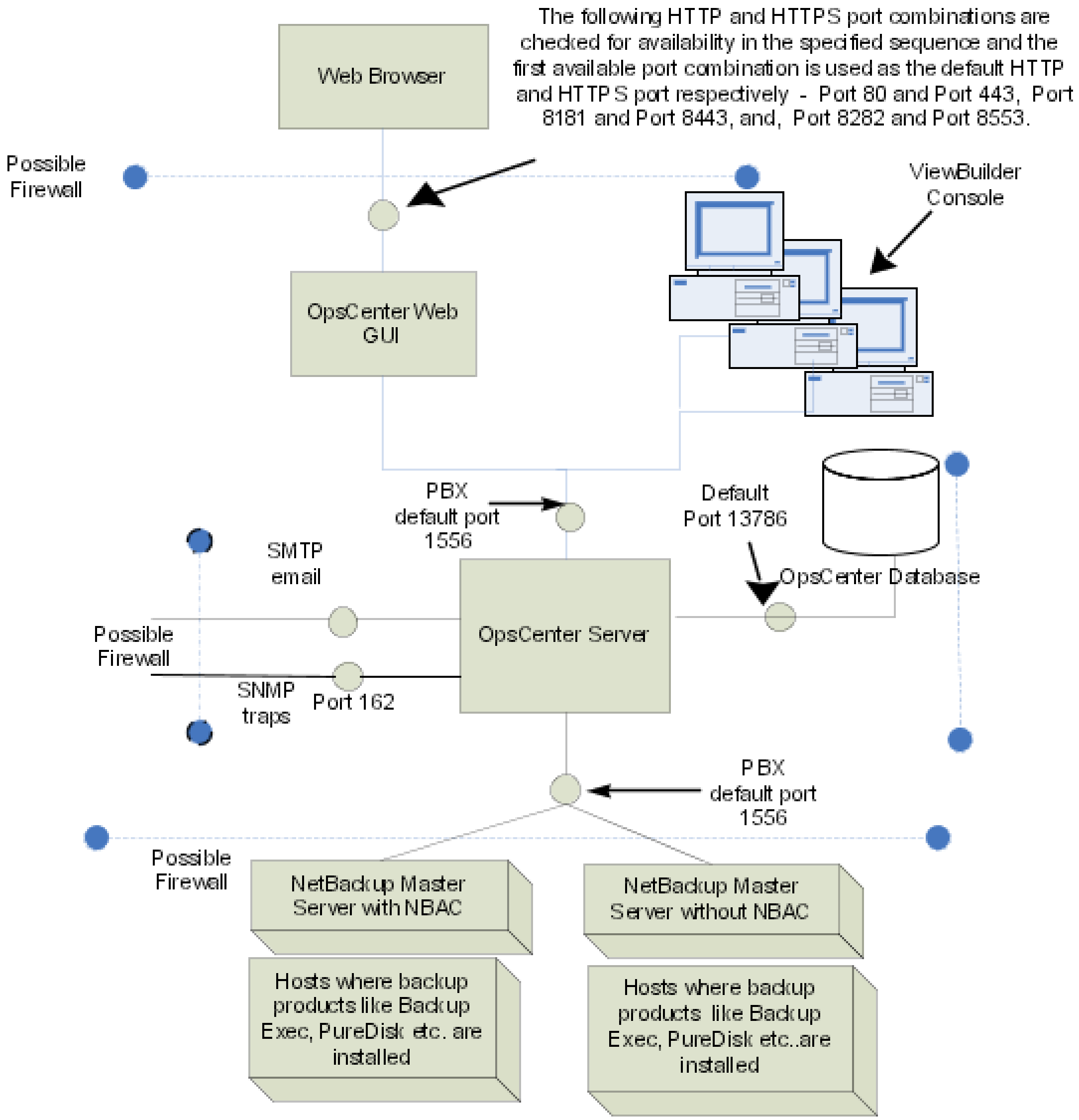
Note: If using Auto Image Replication (AIR) for optimized duplication, TCP ports 1556, 10082, and either 10102 (MSDP) or 443 (PDDO) must be open between the NetBackup domains.

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:

Figure 3-1 NetBackup OpsCenter components


The following HTTP and HTTPS port combinations are checked for availability in the specified sequence and the first available port combination is used as the default HTTP and HTTPS port respectively - Port 80 and Port 443, Port 8181 and Port 8443, and, Port 8282 and Port 8553.
Web Browser
Possible Firewall
ViewBuilder Console
OpsCenter Web GUI
PBX default port 1556
Default Port 13786
OpsCenter Database
SMTP email
Possible Firewall
OpsCenter Server
SNMP traps
Port 162
PBX default port 1556
Possible Firewall
NetBackup Master Server with NBAC
NetBackup Master Server without NBAC
Hosts where backup products like Backup Exec, PureDisk etc. are installed
Hosts where backup products like Backup Exec, PureDisk etc..are installed

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

Source Host	Destination Host	Port Number	Usage (Process Name)	Port Configuration
Symantec OpsCenter Server	Mail Server	25	SMTP	Allow from source to destination.
Symantec OpsCenter Server	SNMP Server	162	SNMP trap	Allow from source to destination.
Symantec OpsCenter Server	NetBackup Master Server(s)	1556	PBX (pbx_exchange)	Allow between source and destination (bi-directional). PBX port number configuration is supported.
Symantec OpsCenter Client	Symantec OpsCenter Server	1556	PBX (pbx_exchange)	Allow between source and destination. Some hardened servers and firewall configurations may block this port. PBX port number configuration is not supported.

Table 3-2 Communication ports used by key NetBackup OpsCenter components *(continued)*

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

NetBackup 5200 and 5220 appliance ports (for firewall between master and media server)

In addition to the ports used by NetBackup, the 52xx appliances also provide for both in-band and out-of-band management. The out-of-band management is through a separate network connection, the Remote Management Module (RMM), and the Intelligent Platform Management Interface (IPMI). Open these ports through the firewall as appropriate to allow access to the management services from a remote laptop or KVM (keyboard, video monitor, mouse).

The following table describes the ports to open inbound to the NetBackup appliance.

Table 3-3 Inbound ports

Source	Destination	Port	Service	Description
Command line	Appliance	22	ssh	In-band management CLI
Web browser	Appliance	80	http	In-band management GUI
Web browser	Appliance	443	https	In-band management GUI
Web browser	Appliance IPMI	80	http	Out-of-band mgmt (ISM+ or RM*)
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

+ NetBackup Integrated Storage Manager

* Symantec Remote Management – Remote Console

Open these ports outbound from the appliance to allow alerts and notifications to the indicated servers.

Table 3-4 Outbound ports

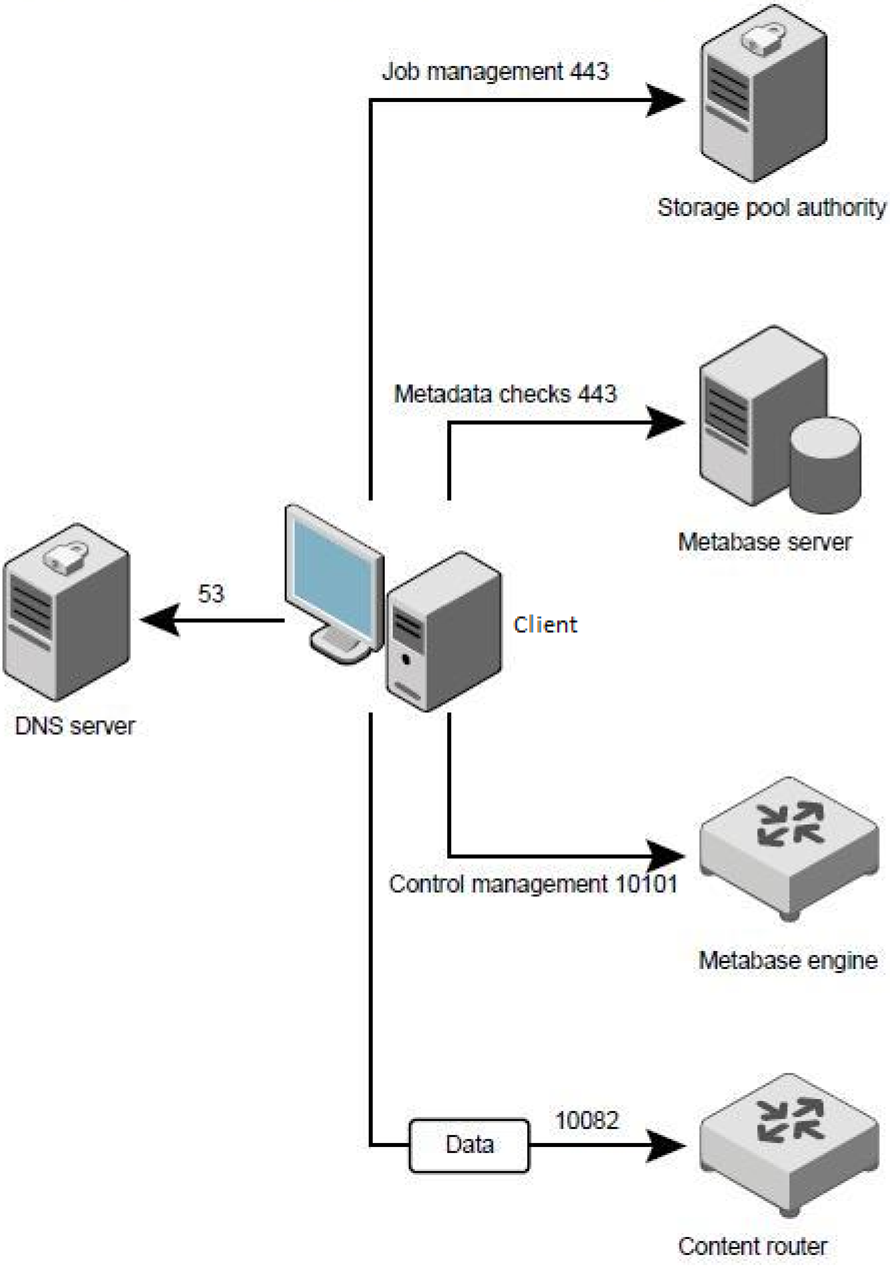
Source	Destination	Port	Service	Description
Appliance	Call Home server	443	https	Call Home notifications to Symantec
Appliance	SNMP Server	162*	SNMP	Outbound traps and alerts
Appliance	SCSP host	443	https	Download SCSP certificates

* This port number can be changed within the appliance configuration to match the remote server.

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

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

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

Source	Destination	Port	Protocol	Purpose and notes
Storage pool authority	All PureDisk node services	22 (SSH)	TCP	Facilitates the PureDisk installation, upgrades, and maintenance.
Administrator's host system	Storage pool authority	22 (SSH)	TCP	Performs inquiries.
All PureDisk node services	Storage pool authority	123	TCP and UDP	Synchronizes the time using NTPD service.
All PureDisk node services	Storage pool authority	443 (HTTPS)	TCP	Monitors the communication among all other services.
Administrator's host system	Storage pool authority	443 (HTTPS)	TCP	Connects to the storage pool authority and then to the PureDisk administrative Web UI.

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

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

NetBackup VMware ports

The TCP ports 443 and 902 are required to access the VMware infrastructure.

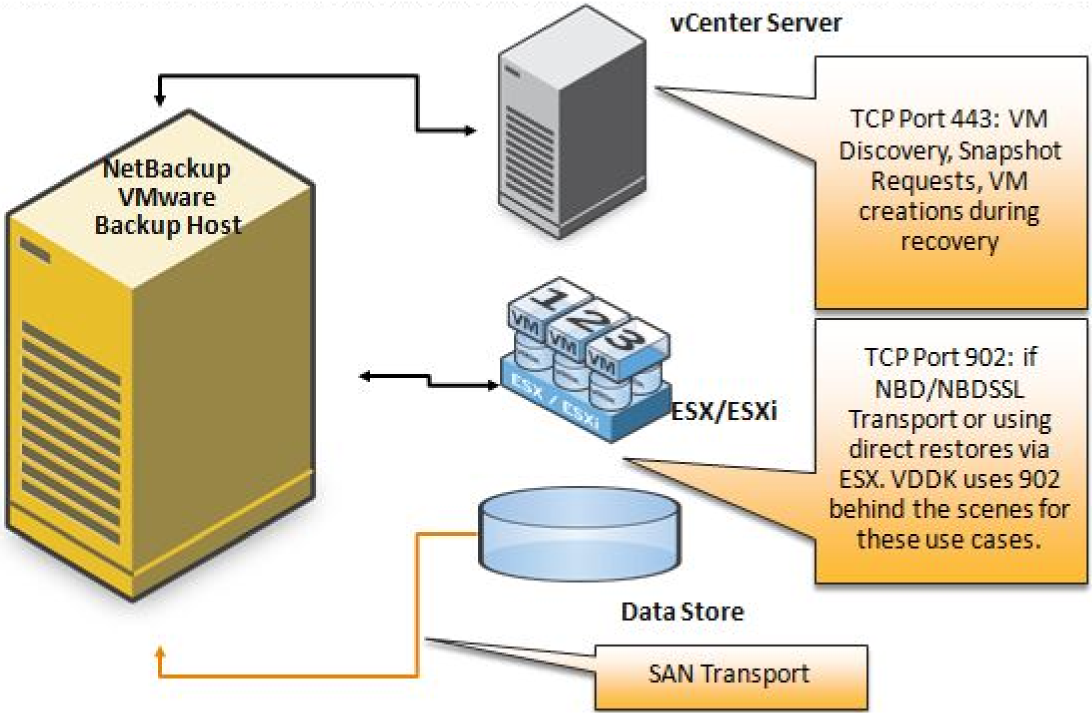
NetBackup must connect to TCP port 443 to access the vCenter server. NetBackup can connect to the vCenter server only through this port for information such as the VM discovery requests, snapshot creation and deletion, and so on.

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:

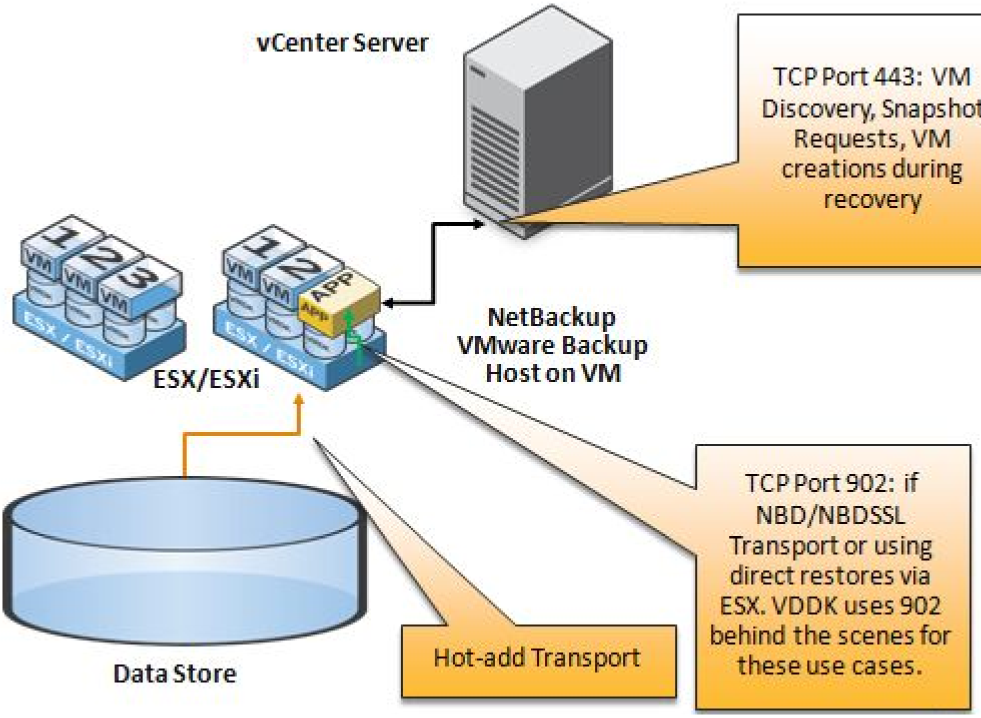
- You use NBD/NBDSSL transport for backups and restore.
- Restores are done through Restore ESX server bypassing the vCenter server.

Figure 3-3 VMware ports


vCenter Server
NetBackup VMware Backup Host
TCP Port 443: VM Discovery, Snapshot Requests, VM creations during recovery
VM
1
2
3
ESX / ESXi
ESX/ESXi
TCP Port 902: if NBD/NBDSSL Transport or using direct restores via ESX. VDDK uses 902 behind the scenes for these use cases.
Data Store
SAN Transport

SAN and NBD Transports using a physical VMware backup host

Figure 3-4 VMware ports


vCenter Server
TCP Port 443: VM Discovery, Snapshot Requests, VM creations during recovery
VM 1
VM 2
VM 3
ESX / ESXi
VM 1
VM 2
APP
APP
ESX / ESXi
ESX/ESXi
NetBackup VMware Backup Host on VM
TCP Port 902: if NBD/NBDSSL Transport or using direct restores via ESX. VDDK uses 902 behind the scenes for these use cases.
Hot-add Transport
Data Store

Index