Hitachi HiCommand® Backup Services Manager

Discovery Administrators Guide for VERITAS NetBackup

November 2006

Version 6.0

DOC ID: MK-95APT009-04

Table of Contents

1. Introduction

This document provides Systems Administrators with information on the Hitachi HiCommand® Backup Services Manager Discovery module.

The Discovery module allows HBSM to discover servers and devices in your enterprise as well as collect physical characteristics (e.g. capacity, usage, free space) of disk based storage units within the backup environment. This information is then accessed through various reports in the HBSM Portal application.

The Discovery module included in the base HBSM product probes NetBackup Media Servers for the physical characteristics of their disk based storage units. The full Discovery functionality which discovers and reports on unprotected clients and data sets by probing for devices in your enterprise is available as an add-on module. If you have not purchased this add-on module, some of the functionality described in this document will not apply to your installed application. Please contact your Hitachi Data Systems representative if you want to learn more about how to license the add-on HBSM Discovery module.

2. Discovery Overview

HBSM Discovery provides a solution to the age-old problem of identifying what data within your organization is not being protected. Customers IT infrastructure, applications, and servers are rapidly changing. Servers often drop off the “backup radar” and the awareness of “When was my last successful backup?” for any given server, application, or business unit is simply not available from the native underlying backup & recovery products.

The following fundamental questions are going un-answered within enterprise storage management environments:

- Where is my data protected? (for example, disk-to-disk, disk-to-tape, or disk-to-disk-to-tape)
- What is the extent and coverage of my data protection?
- Are all my clients and applications protected?
- Is every dataset on every client and every application protected?

HBSM Discovery will help IT managers answer these questions and quickly illuminate risk and exposure within the corporate IT backup and recovery environment.

HBSM Discovery will discover hosts or servers on a corporate network and compare those hosts with the policies of the underlying backup & recovery software. The first goal is to identify “orphan clients” that are not being protected. Discovery can further probe and determine the file-systems or drives of the hosts/servers and compare and contrast these file-systems to the equivalent policies within the underlying backup & recovery software.

3. Discovery Features

3.1. Manage Discovery Policies

HBSM Discovery is a policy based module that allows Administrators to create “Discovery Policies”. A Discovery Policy is a set of rules that allows an Administrator to tune and configure the following parameters for the discovery engine:

Discovery Type	
New Server Discovery	Discover servers or hosts on a network
Media Server File Systems:	Probe NetBackup Media Servers and obtain the file-system information including the name, used, and available disk-space
NetBackup Server File Systems:	Probe the existing NetBackup Clients and determine the current file systems or drives.

IP Range or hostnames to include or exclude in the discovery process. e.g. 172.16.1.1-120

Date/Time window that the discovery engine should perform its discovery and system probing

Customizable rules to identify and categorize servers

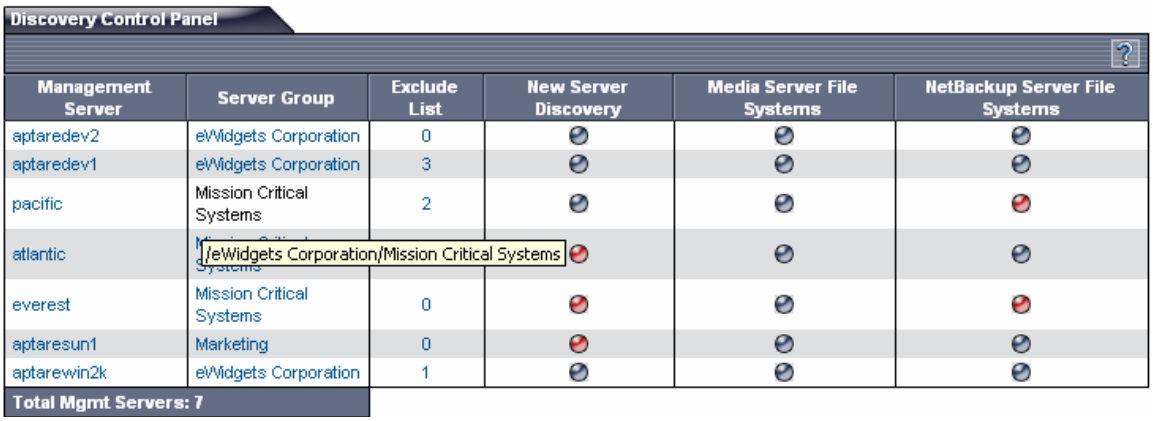

Figure 1: Main discovery control panel selection list

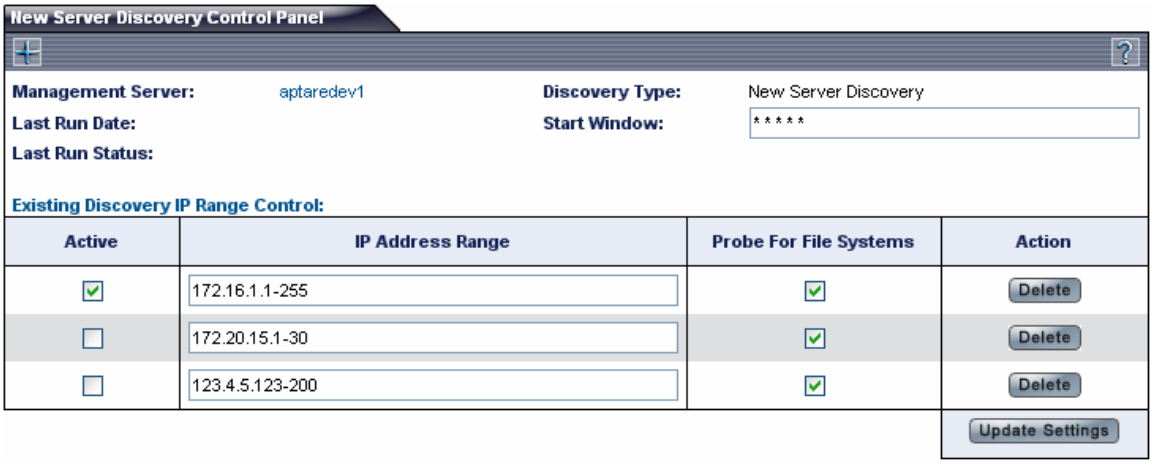

Figure 2: Discovery control panel for a single policy

3.2. Client Protection Summary Report Designer

Once the discovery policies have been set and the discovery engine has probed the network looking for orphan clients and unprotected datasets, an Administrator can then launch the

Client Protection Report Designer. (Note: This report designer is only available if you have installed the add-on Discovery module).

The Client Protection Report Designer provides the ability to customize and personalize a Client Protection Dashboard that will identify exposure and threats to an enterprise data protection environment.

The Designer will allow the user to customize the following parameters:

- Report period
    - This is used to determine the last Full successful (and attempted) backup for the scope of clients
- Report scope
    - Global
    - By server group
    - By list of individually selected clients
    - By discovery server
- Protection status
    - Show all clients independent of their protection status (default)
    - Show Protected Clients – i.e. clients that are part of an active policy that have had a successful full-backup within the reporting period
    - Show just those clients that have had a full backup within the reporting period but are not currently part of an active policy
    - Show Unprotected clients – i.e. clients that have not had a full backup within the reporting period

3.3. Client Protection Summary Report

The Client Protection Report provides a single pane-of-glass view of the protection status for the selected list of clients or servers. This is a tabular report with the following columns:

- Client hostname
    - User can view a summary or “by device” view for any client
- Backup product (currently only VERITAS NetBackup is detected)
- Device (for example, C:\, /export, /, etc.)
- Active Coverage
    - Partial - the device or client is partially protected
    - None - the device or client does not have any active policies providing coverage
    - Full - the device or client is completely protected
    - Unknown - the device does not appear to be running any backup software and is likely an orphan with no data protection
- Summary protection status
    - Date/time of last successful Full backup
    - Date/time of last Full backup attempt
    - List of NetBackup policies that are active and include this device/client

- Exclusion check-box to allow the user to filter a row from any subsequent run of this report

Coverage Report: eWidgets Corporation >> Mar 15, 2005 11:03:57AM - Mar 28, 2005 11:03:57AM

Client Server	Backup Product	Device	Active Coverage	Protection Status	Last Successful Backup	Last Attempted Backup	Covering Policies	Exclude
aptaredev1	Netbackup	System Summary	Partial		Mar 28, 2005 02:50:14am	Mar 28, 2005 02:50:14am	Production_SourceSafe, Production_aptaredev1, Production_aptaredev1, SIMPLE_TEST, SourceSafe, Long_Job, Production_UNIX_Homes, Daily_Backup_Linux_Servers	☐
		/var	Partial		Mar 28, 2005 02:50:14am	Mar 28, 2005 02:50:14am	Daily_Backup_Linux_Servers	
		/opt	Partial		Mar 25, 2005 01:17:58pm	Mar 25, 2005 01:17:58pm	Production_SourceSafe, Production_aptaredev1, Production_aptaredev1, SourceSafe, Long_Job	
		/mnt/cdrom	None					
		/usr	None					
		/home	Full		Mar 25, 2005 01:17:57pm	Mar 25, 2005 01:17:57pm	SIMPLE_TEST, Production_UNIX_Homes	
		/	Full					
		/data	None					
aptaresqa	Netbackup	System Summary	None					☑
		/	None					

Update Settings

Figure 2: Client Protection Summary

4. Discovery Setup process

To setup your system to support Discovery you must:

1. Ensure the license for the add-on Discovery Module has been activated if you want to access the additional discovery features beyond the Media Discovery component. You can run the license utilities in the /opt/aptare/utils directory to view the status of your current license or install your updated license with Discovery enabled.
2. Create discovery policies for your NetBackup Master servers for each of the Discovery types you wish to enable:
   2.1. Select the Discovery icon under Administration, Control Panels in the Global Navigator to display the list of Master Servers.
   2.2. Click the control for the Master Server and Discovery type for which you wish to set up a policy. This will take you to the corresponding Discovery Policy panel.
   2.3. Enable and update the policy settings to activate the discovery policy.
3. Enable SNMP on your Media Servers and any other servers in your environment that you wish to capture file system level information on. Appendix A contains some helpful information on SNMP configuration.
4. Enable the HBSM Agents discovery processes by editing the Agent configuration file on the NetBackup Master Servers as follows:
   4.1. Locate the HBSM Agent configuration file crontab.properties on each of your master servers. The default location for this file is /opt/aptare/mbs/conf
   4.2. Ensure the file contains the following two lines. Note: these lines may already be present but commented out via the "#" character. In this case simply remove the "#" character and save the file.

```
40|com.aptare.mbs.Discoverer.DeviceDiscoverer
35|com.aptare.mbs.Discoverer.BPCDiscoverer
```

5. Each of the discovery processes will then run based on their configured window. Once they have all run, you should be able to run the Client Protection Summary report and view the status of clients that have been probed. The Client Protection Summary report may not contain any data if the discovery processes have not all run. You can check the last run status in the Discovery control panels.

NOTE: The help for each of the control panels provides further detailed information on how to setup and administer the policies for each of the discovery types.

5. Disk Storage Unit Discovery

5.1. Disk Based Reports

The Disk Based Reports provide information on the disk storage units within the NetBackup sub-system and include for example throughput, usage and content reporting. The Media Discovery module enables an enhanced level of reporting by probing the storage units for physical characteristics to incorporate in the reports.

It's important to note that the HBSM Portal disk based reports will still run if the Media Discovery module has not been enabled, however the physical attributes of the storage units in the various reports will not be displayed or will be displayed as "Unknown"

5.2. Media Discovery Module

The Media Discovery Module runs within the HBSM Agent on the NetBackup Master Server and at configurable intervals (every 20 minutes by default) issues SNMP probes to the Media Servers in the backup environment, captures the physical attributes of the Media Servers, and sends the information back to the Portal for insertion into the HBSM database.

If the Media Discovery module is enabled on a Master Server, it will collect information only for the Media Servers associated with that particular Master. If you have several Master Servers in your environment with attached Media Servers and Disk Storage Units, you will need to enable the Media Discovery module on each of these masters.

6. Modifying Discovery System parameters

Many of the default settings for the discovery processes are maintained in the HBSM database and are downloaded to the Agent at run time. From time to time it may be necessary to adjust some of the default settings – for example if your SNMP community string is not "public", or you want to adjust the default timeout values used for the various probes. These settings can be updated by loading a new set of settings from an XML file maintained on the Portal server.

Each server group folder that a master server references (via the <ServerGroupId> parameter in the bnrtriggerconfig.xml file on the master server) has its own set of configuration parameters. Therefore to change the settings for an agent running on a master server, you must first find the value of the ServerGroupId parameter. For the example that follows, we will assume the ServerGroupId value is 100000, and the Portal is installed on a UNIX system. For Windows installations simply replace the forward slashes with backslashes and the ".sh" with ".bat"

On the Portal server, make a copy of and then edit the default discovery settings file

```
cd /opt/aptare/utils

cp DiscoverProperties.xml DiscoverProperties_new.xml

vi DiscoverProperties_new.xml
```

Make the necessary changes (e.g. change "public" to your SNMP community string value)

Save and close the file

Load the new configuration settings into the database for the appropriate ServerGroupId

```
cd /opt/aptare/utils
```

Enter the following as one continuous line:

```
./updDiscoverProperties.sh 100000 ../portalconf/systemlogger.xml
../portalconf/portalproperties.xml DiscoverProperties_new.xml
```

Appendix A: SNMP Configuration Guidelines

NOTE: Hitachi Data Systems provides this information for general guidance and informational purposes only. The Hitachi Data Systems Technical Support Center is not qualified or able to provide Customer Support assistance with the installation, configuration and troubleshooting of SNMP sub-systems on your Servers.

The Simple Network Management Protocol (SNMP) is an Internet standard. SNMP provides a common way to query, monitor, and manage devices connected to IP networks. The protocol is defined in RFC 2571. For more information, see http://www.ietf.org/rfc/rfc2571.txt.

The HBSM Discovery module uses SNMP v2c[1] messaging to query all Media Servers and other servers or devices probed during Discovery for physical attributes of their configured storage units and file systems. The SNMP probe uses UDP and the standard SNMP port 161 by default.

This Appendix provides details on the SNMP probes that are issued as well as information on how to enable and configure SNMP services on your servers to take advantage of this functionality. There are respective sections for the following operating systems:

- Windows
- Redhat Linux 7.3
- Redhat Linux 9.0
- HP-UX 11.00
- Solaris 8/9
- Solaris 10

SNMP Probe Details

The SNMP subsystem must be configured to respond to the following probes to take full advantage of the Discovery functionality:

The first probe issued is for the sysObjectOID (.1.3.6.1.2.1.1.2). This will return an OID that conforms to the enterprise OIDs allocated by the Internet Assigned Numbers Authority (`http://www.iana.org/assignments/enterprise-numbers`). Be aware that this number is returned by the SNMP agent resident on the device and may not be the same as the hardware manufacturer. For example an HP N-class server may return the enterprise OID of 1.3.6.1.4.1.11 or 1.3.6.1.4.1.2021.250.14 depending on whether the SNMP agent is provided by HP or is the open source NET-SNMP package.

The number returned is matched against a lookup table to try and determine the company value of the OID. (Example: IBM or Sun)

[1] This is defined in RFC 1901 at http://www.ietf.org/rfc/rfc1901.txt

Next a probe is made for the sysDescr OID (.1.3.6.1.2.1.1.1). This returns a description of the device or agent. This string is matched against a lookup table to try and determine the system description value. (Example: Windows 2000 or Solaris)

Lastly, if configured, a query is made against the Device and Storage section of the Host Resources Management Information Block (MIB[2]). Specific information retrieved is the file system mount point, storage type, storage description, allocation units, size in storage units, and storage units used.

Before this information is returned, calculations are made to convert the values into kilobytes. Only fixed disk storage units are returned.

Windows (NT/2000/XP)

To install the SNMP on Windows 2000/XP, perform the following steps (note that the process is very similar on Windows NT 4):

- Click on **Start | Settings | Control Panel**.
- Double-click on **Add/Remove Programs**.
- Click on **Add/Remove Windows Components**.
- Click on **Management and Monitoring Tools** and click on **Details**.
- Check **Simple Network Management Protocol** and click **OK**.
- Click on **Next** and let the install process complete.
- Double-click on **Administrative Tools** (inside Control Panel).
- Double-click on **Computer Management**.
- Expand the **Services and Applications** tree on the left frame.
- Click on **Services** on the left frame.
- Locate **SNMP Service** on right frame and double-click on it.
- On the **General** tab, select **Automatic** for **Startup Type**.
- On the **Security tab** you can leave the default community name "public" or choose your own (which is more secure). To choose your own, click on **Add**... for accepted community names, leave **Community Rights** as Read-Only and pick a secure Community Name. Click on OK. Remove the "public" entry. You will have to modify the default Discoverer properties configuration file to match this.
- On the security tab in the lower half you can choose which IP addresses are allowed to access the SNMP service. You must at least choose the IP address of the Master Server running the HBSM Agent.
- On the **Agent** tab fill out all edit fields and enable the internet check box to make all SNMP values available.

The following documents might also be helpful with the SNMP setup on Windows:
http://support.microsoft.com/default.aspx?scid=KB;EN-US;q315154&
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/tcpip/part3/tcpch10.asp

[2] as defined in RFC 2790. See http://www.ietf.org/rfc/rfc2790.txt

http://support.microsoft.com/support/kb/articles/Q295/5/87.ASP

http://support.microsoft.com/support/kb/articles/Q237/2/95.ASP

Net-SNMP

Net-SNMP (http://www.net-snmp.org) is an open source implementation of various tools relating to the Simple Network Management Protocol. It provides valuable functionality for the Media Discovery module since it provides an extensible agent for responding to SNMP queries for management information (snmpd). This includes built-in support for a wide range of MIB information modules, specifically the Host Resource MIB.

Net_SNMP is available for many Unix and Unix-like operating systems and also for Microsoft Windows. Note: Functionality can vary depending on the operating system.

See Appendix B for information relating to the setup of Net-SNMP.

Redhat Linux 7.3

Redhat Linux has the ucd-snmp package preinstalled. It is the precursor to net-snmp. It needs to be configured to return the host resource information and to be executed at system startup.

The SNMPD config file is located at /etc/snmp/snmpd.conf. The executable is found at /usr/sbin/snmpd.

Below is an example configuration file showing read-only access to the system and host resource storage portions of the MIB.

```
####
# First, map the community name "public" into a "security name"

#       sec.name  source          community
com2sec notConfigUser  default       public

####
# Second, map the security name into a group name:

#       groupName      securityModel securityName
group   notConfigGroup v1           notConfigUser
group   notConfigGroup v2c          notConfigUser

####
# Third, create a view for us to let the group have rights to:

#       name           incl/excl     subtree         mask(optional)
#view    systemview     included      .1
view     HBSM           included      .iso.org.dod.internet.mgmt.mib-2.system         fe
view     HBSM           included      .iso.org.dod.internet.mgmt.mib-2.host.hrStorage  ff
view     HBSM           included      .iso.org.dod.internet.mgmt.mib-2.host.hrDevice   ff
```

```
# .iso.org.dod.internet.mgmt.mib-2.system = .1.3.6.1.2.1.1
# .iso.org.dod.internet.mgmt.mib-2.host.hrStorage = .1.3.6.1.2.1.25.2
####
# Finally, grant read-only access to the system and storage portions of the MIB2 tree

#       group          context sec.model sec.level prefix read   write  notif
#access  notConfigGroup ""      any       noauth    exact  systemview none none
access  notConfigGroup ""      any       noauth    exact  HBSM none none
```

Redhat Linux 9.0

Redhat Linux has net-snmp package. It needs to be configured to return the host resource information and to be executed at system startup. The sample file above should also work for this version of Redhat Linux.

HP-UX 11.00

Although HP-UX 11.00 has a SNMP agent installed it does not provide access to the Host Resource MIB and so storage unit discovery is not supported. However, the Net-SNMP software package is supported on HP-UX 10.20, 11.00 and 11.11 and binary distributions can be found at http://www.net-snmp.org

Solaris 8-9

The Solstice Enterprise Agent does not support the Host Resource MIB and so storage unit discovery is not supported. However, the Net-SNMP software package is supported on Solaris 5.6, 5.7, 5.8, and 5.9 and binary distributions can be found at http://www.net-snmp.org

Solaris 10

The Solaris System Management Agent (SMA) is a new SNMP agent offering from Sun, based on the Net-SNMP open source implementation version 5.0.9. Further configuration information can be found at http://docs.sun.com/app/docs/doc/817-3000

Appendix B: Net-SNMP installation

If you have downloaded a binary release (binary distributions can be found at http://www.net-snmp.org) then you will have to create a base configuration file. The following is a record of an installation of Net-SNMP 5.2.

User input / responses are in **bold**.

```
# /usr/local/bin/snmpconf -g basic_setup
************************************************
*** Beginning basic system information setup ***
************************************************
Do you want to configure the information returned in the system MIB group
(contact info, etc)? (default = y): no

Do you want to properly set the value of the sysServices.0 OID (if you don't
know, just say no)? (default = y): no
```

```
************************************
*** BEGINNING ACCESS CONTROL SETUP ***
************************************
Do you want to configure the agent's access control? (default = y):
Do you want to allow SNMPv3 read-write user based access (default = y): no
Do you want to allow SNMPv3 read-only user based access (default = y): no
Do you want to allow SNMPv1/v2c read-write community access (default = y): no

Do you want to allow SNMPv1/v2c read-only community access (default = y): yes
Configuring: rocommunity
Description:
  a SNMPv1/SNMPv2c read-only access community name
    arguments:  community [default|hostname|network/bits] [oid]

The community name to add read-only access for: public
The hostname or network address to accept this community name from [RETURN
for all]:
The OID that this community should be restricted to [RETURN for no-
restriction]:

Finished Output: rocommunity  public
Do another rocommunity line? (default = y): no
************************************
*** Beginning trap destination setup ***
************************************
Do you want to configure where and if the agent will send traps? (default =
y): no
************************************
*** Beginning monitoring setup ***
************************************
Do you want to configure the agent's ability to monitor various aspects of
your system? (default = y): no

The following files were created:

  snmpd.conf

These files should be moved to /usr/local/share/snmp if you want them used by
everyone on the system.  In the future, if you add the -i option to the
command line I'll copy them there automatically for you.

Or, if you want them for your personal use only, copy them to
(HOME dir - n/a) .  In the future, if you add the -p option to the command
line I'll copy them there automatically for you.
```

The snmpd executable is located in `/usr/local/sbin/snmpd` and should be started by root.

Troubleshooting Net-SNMP installation

/usr/local/bin/snmpconf requires Perl v5.6 and above. Replace the line:

```
#!/usr/local/bin/perl
```

in /usr/local/bin/snmpconf to reference your perl installation.

If your version of perl is 5.0 or before then you may receive a run time error when executing snmpconf. To correct this, edit the snmpconf file and make the changes below:

```
-          if (! (-d "$opts{'I'}") && ! (mkdir ("$opts{'I'}"))) {
+          if (! (-d "$opts{'I'}") && ! (mkdir ("$opts{'I'}", 0755))) {
            print "\nCould not create $opts{'I'} directory: $!\n";
            print ("File $didfile{$i} left in current directory\n");
          }
@@ -198,7 +198,7 @@
             }
           }
         } elsif ($opts{'p'}) {
-          if (! (-d "$home") && ! (mkdir ("$home"))) {
+          if (! (-d "$home") && ! (mkdir ("$home", 0755))) {
            print "\nCould not create $home directory: $!\n";
            print ("File $didfile{$i} left in current directory\n");
```