

Introduction

This document provides a summary of the features and benefits of the APTARE StorageConsole Discovery Module. This module is an add-on software component to the baseline APTARE StorageConsole Enterprise Server product.

APTARE StorageConsole 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)
- Where is the latest version of my data and how quickly can I recover from each source
- Are my current backup environment policies meeting my recovery point objective (RPO) and recovery time objective (RTO) goals or service level objectives?
- 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?

APTARE StorageConsole Discovery is an evolutionary technology that will help IT managers answer these questions and quickly illuminate risk and exposure within the corporate IT backup and recovery environments.

APTARE StorageConsole 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.

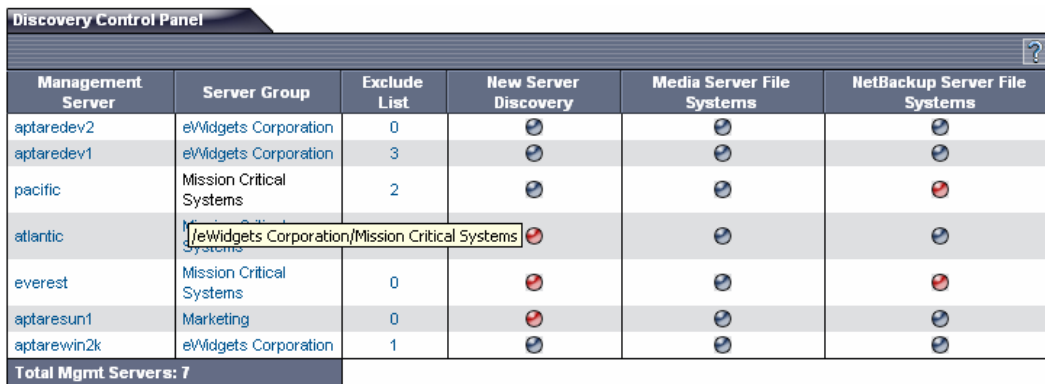
Administrators will finally have an accurate tool that allows them to visualize the protection status of their IT infrastructures and make pro-active decisions to improve their overall data protection prior to the unnerving event of attempting to recover a server or data that was never backed up.

Description of Features

Manage Discovery Policies

APTARE StorageConsole Discovery is a policy based module that allows Administrators within APTARE StorageConsole 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:

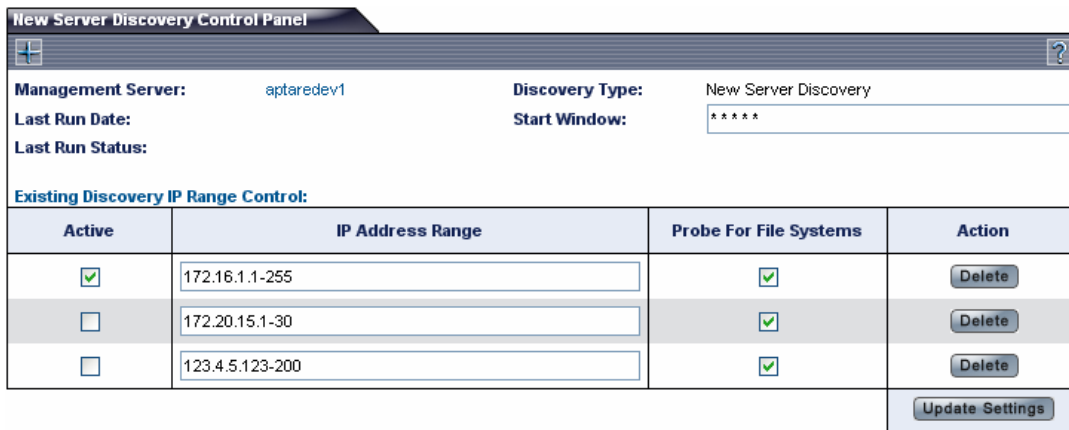
- Type of discovery:
 - Discover servers or hosts on a network
 - Probe Media servers and obtain the file-system information including the name, used, and available disk-space
 - Probe the existing NetBackup clients and determine the current file-systems or drives
- Range of IP addresses or hostnames to include or exclude in the discovery process
 - Range examples: 172.16.1.0-255, APTAREprod*
- Date/Time window that the discovery engine should perform its discovery and system probing
- Customizable rules to identify and categorize servers



Management Server	Server Group	Exclude List	New Server Discovery	Media Server File Systems	NetBackup Server File Systems
aptaredev2	eWidgets Corporation	0			
aptaredev1	eWidgets Corporation	3			
pacific	Mission Critical Systems	2			
atlantic	eWidgets Corporation/Mission Critical Systems				
everest	Mission Critical Systems	0			
aptaresun1	Marketing	0			
aptarewin2k	eWidgets Corporation	1			

Total Mgmt Servers: 7

Figure 1: Main discovery control panel selection list



Management Server:	aptaredev1	Discovery Type:	New Server Discovery
Last Run Date:		Start Window:	*****
Last Run Status:			
Existing Discovery IP Range Control:			
Active	IP Address Range	Probe For File Systems	Action
<input checked="" type="checkbox"/>	172.16.1.1-255	<input checked="" type="checkbox"/>	Delete
<input type="checkbox"/>	172.20.15.1-30	<input checked="" type="checkbox"/>	Delete
<input type="checkbox"/>	123.4.5.123-200	<input checked="" type="checkbox"/>	Delete
Update Settings			

Figure 2: Discovery control panel for a single policy

Discovery 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 Discovery Report Designer.

The Discovery 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 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

Client Protection Dashboard

The Client Protection Dashboard 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 (for example, VERITAS NetBackup)
- 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 backup
- Date/time of last backup attempt
- List of NetBackup policies that are active and include this device/client

- Exclusion check-box ... this will 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	<input type="checkbox"/>
		/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					<input checked="" type="checkbox"/>
		/	None					

[Update Settings](#)

Security

APTARE StorageConsole uses a combination of networking probing mechanisms to obtain its data within a secure corporate network. The following table describes the network protocols, ports, and different probing components of APTARE StorageConsole Discovery:

Discovery Type	Protocol	Network Port
Ping Discovery	ICMP	N/A
SNMP Probe	SNMP	UDP Port 161

The APTARE Discovery application uses SNMP to query an IP connected device for the device description and its attached storage units. The SNMP probe uses UDP, using port 161, the standard SNMP port.

The probe can be configured with the following values in the Discovery properties configuration settings:

SNMPConfig:

- numProbes – (default 16)
- probeTimeout – (default 1000)
- port – (default 161)
- filesysProbe – (default false)
- communityString – (default public)

The first query 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

a 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.

This number is matched against the CompanyLookup sections in the properties configuration.

Next a query 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 compared against a set of matching strings also defined in the properties configuration.

Lastly, if configured, a query is made against the Storage section of the Host Resources Management Information Block (MIB). Specific information retrieved is the storage type, the storage description, the allocation units, the 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.

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 Discovery application uses SNMP v2c messaging to conduct it's queries. This is defined in RFC 1901 at <http://www.ietf.org/rfc/rfc1901.txt>

When querying storage units the Discovery application looks for the Host Resources MIB as defined in RFC 2790. See <http://www.ietf.org/rfc/rfc2790.txt>

Installing SNMP Service

Windows NT/2000/XP

To install the SNMP on Windows 2000/XP, perform the following (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 Discovery 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 machine running APTARE Discovery.
- On the **Agent** tab fill out all edit fields and enable all check boxes to make all SNMP values available.
- The following documents might also be helpful with the SNMP setup on Windows (for more links see below):
<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>
<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. For our needs it includes 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 A 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 APTARE included .iso.org.dod.internet.mgmt.mib-2.system fe
view APTARE included .iso.org.dod.internet.mgmt.mib-2.host.hrStorage 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 APTARE 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. 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 also does not support the Host Resource MIB and so storage unit discovery is not supported. 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>