HITACHI
DATA SYSTEMS

Hitachi HiCommand® Backup Services Manager

NetBackup Policy Auditing Module

November 2006

Version 6.0

Doc ID: MK-95APT012-01

TABLE OF CONTENTS

1. Introduction

HiCommand Backup Services Manager provides an add-on module called "HiCommand Backup Services Manager - NetBackup Policy Auditing". This module provides a set of reports that show the audit trail of changes made to NetBackup Policies, over a selected time period. These reports can be used to determine what changes were made to NetBackup policies, and when the changes were made.

This feature is an add-on and a separate licensed module within the HBSM Suite of products. You can see if this feature is enabled for your HBSM Portal by logging into the Portal Web-Interface and then clicking on Help → About HBSM. In the "About" Box you can click on "Product License Details" to see the list of licensed modules. For information regarding the procurement and licensing of any HBSM product or module, please contact your nearest sales office.

NetBackup Policy Auditing captures the changes made to your underlying NetBackup policies by using database triggers on the NetBackup policy tables within the HBSM database. The database triggers are enabled by default in the base product offering. The NetBackup Policy Auditing Module provides a set of reports to "unlock" and present the data from the policy auditing tables.

If you have a question about the reports, please contact the HDS Technical Support Center which will be happy to assist you:

Technical Support Center Contact Information

Phone:	
Nth & Latin America	1-800-348-4357
Europe	+(44)-175-361-8000
Asia Pacific (call USA GCC)	+(1) 858-547-4765 (or +1 408 871-9848)
Email:	support@hds.com

2. Reports Overview

There are four reports delivered as part of the HBSM – NetBackup Policy Auditing Module. The following is a brief summary of these reports. For a detailed explanation, please refer to the Report Detail section later in this document.

2.1 NetBackup Policy Audit Summary Report

This report provides a one-line summary of the changes made to a NetBackup Policy for the selected reporting period. The summary includes the date/time of the change, the name of the associated master server, the name of the policy, and a brief description of the change.

2.2 NetBackup Policy Audit Detail Report

This report provides a detailed explanation of all of the changes made to any policy for the selected report scope and time period. A detailed description of each change made to a NetBackup policy is displayed on a single line and grouped per policy and master server. The following policy attributes are displayed in this report:

- The creation of a new policy
- Changes to the core policy attributes include such attributes as multi-streaming, keywords, cross-mount points, default storage unit, default volume pool, etc.
- Add, change, delete of policy include and exclude directives

- Add, change, delete of policy clients
- Add, change, delete of policy schedules including retention periods, frequency, schedule type (calendar Vs frequency), number of copies, etc.

2.3 NetBackup Policy Audit Client Detail Report

This report provides a detailed description of the list of changes to client membership in any policy based on the report scope and selection criteria. For each NetBackup Policy, this report will display a list of the added and removed clients grouped by date, master server, and policy name.

2.4 NetBackup Policy Audit File Detail Report

This report provides a detailed description and list of changes made to the file directives for any policy based on the report scope and selection criteria. A single line is displayed in this report for each addition, deletion, or change made to a policy directive. The data is grouped and displayed by date, master server, and NetBackup Policy name.

3. Report Customization

The reports within HBSM and the NetBackup Policy Auditing Module are highly customizable. A user can very easily customize the selection criteria of each of the reports and can also customize the format of the resulting report data.

To customize both the report selection criteria and the format of the resulting generated report, a user would edit the report file that is included with the HBSM Product. The following table describes the location of the HBSM – NetBackup Policy Auditing Reports:

Portal Operating System	Location of NetBackup Policy Auditing Reports
Microsoft Windows	%APTARE_HOME%\database\custom_reports\samples\nbu\policy_audit
UNIX	$APTARE_HOME/database/custom_reports/samples/nbu/policy_audit

Note: It is strongly recommended that you do not edit and make changes to the reports under the "samples" directory. These reports will be written over with subsequent upgrades of your product. If you wish to edit and make changes to a report, you should first copy it to the *custom_reports* directory and make your changes there.

Note too that the reports will throw an Oracle error 60026 (similar to the following) if they are run on a system where the Policy Auditing license has not been activated:

```
ERROR at line 1:
ORA-60026: Message 60026 not found;  product=RDBMS; facility=ORA
ORA-06512: at "PORTAL.NBU_AUDIT_PKG", line 113
ORA-06512: at line 113
```

3.1 Customizing The Report Selection Criteria

There are several parameters that can be customized as the input or selection criteria parameters for your report. This section will describe in detail the purpose and how to customize each parameter.

The first step is to make sure you are working with a local copy of the report and NOT the version that is resident under the *samples* folder hierarchy. The following table should be used to determine the name of the source report file you are looking to customize and the resulting default output report file that will be created.

Report Name	Source File Name	Default Report Output File
NetBackup Policy Audit Summary Report	list_policy_audit.sql	policy_audit.txt
NetBackup Policy Audit Detail Report	list_policy_audit_detail.sql	policy_audit_detail.txt
NetBackup Policy Audit Client Detail Report	list_policy_client_audit.sql	policy_client_audit.txt
NetBackup Policy Audit File Detail Report	list_policy_file_audit.sql	policy_file_audit.txt

Using your favorite text file editor, open one of the **Source Report Files.** Locate a statement block similar to the following within the source file:

```
nbu_audit_pkg.listPoliciesWithChanges(
    dateRange,
    serverGroupID,
    cascade,
    clientList,
    serverList,
    policyRegExpr,
    :cur);
```

This statement block is where the report calls an HBSM method that does most of the processing behind each report. Each method will accept six input parameters and one output parameter. The following is a detailed explanation of each input and output parameter:

3.1.1 dateRange

The dateRange parameter is an HBSM object that allows you to pass many different types of date range parameters to the method. For example, you might want to report on the “last 14-days” and have the underlying HBSM method figure out the true timeframe. If you look for a statement block just above the method that look’s something like this:

```
dateRange       dateRangeType := dateRangeType(
    timePeriod    => report_package.REPORT_PERIOD_LAST_10_DAYS,
    startTime     => NULL,
    finishTime    => NULL,
    startDate     => NULL,
    finishDate    => NULL,
    timezoneName  => NULL,
    useFinishTime => util.IS_TRUE);
```

This is the definition of the dateRange variable for your report. For a detailed explanation on how to customize the dateRange variable, please refer to **Appendix A: Customizing Your Report Date/Time Period** at the end of this document.

3.1.2 serverGroupID

This is the numeric ID of a server group within the Portal. This report will look in the immediate contents of this server group, or cascade the server group hierarchy (depending on the setting of the "cascade" parameter) looking for master servers and their associated NetBackup Policies

3.1.3 cascade

This parameter tells the report to cascade the server group hierarchy (util.IS_TRUE) or only look in the immediate server group specified by serverGroupID (util.IS_FALSE).

3.1.4 clientList

If this parameter is set, it overrides the serverGroupID and cascade parameters and looks for a set of NetBackup policies that contained one or more of the clients in the clientList parameter. The client simply had to be a member of the policy during the interval of the report time period (as specified by the dateRange parameter).

The clientList parameter is a special data type called a numberListType. This is a list of numeric ID's. The ID's are the ID's of a list of clients. You can determine the ID of any client or server by using the Tools → Search feature within the HBSM Web Interface:

Search Criteria | Search Results

Name	Server ID	IP Address	Last Backup	Backups this Month	GBytes this Month	Manage
afghanistan	305730	157.204.47.184	Jul 12, 2006 12:00:08am	12	294.00	everest
albania	305796	157.204.47.70	Jul 12, 2006 12:00:22am	12	2.00	everest
algeri	305797	157.204.47.106	Jul 12, 2006 12:01:02am	12	3.00	everest
andorra	305805	157.204.7.68	Jul 12, 2006 01:56:39am	12	133.00	everest
angol	305856	157.204.47.196	Jul 12, 2006 12:03:49am	21	916.00	everest
antarctic	305871	157.204.47.16	Jul 11, 2006 11:02:32pm	12	75.00	everest
antigua	305790	157.204.47.197	Jul 12, 2006 01:07:19am	12	383.00	everest
argentina	305920	157.204.7.150		0	0.00	
armenia	305793	157.204.7.151	Jul 12, 2006 12:05:17am	12	4.00	everest
artic	305774	157.204.7.63	Jul 12, 2006 12:20:16am	12	115.00	everest
atlantic	305740	157.204.47.82	Jul 11, 2006 11:32:21pm	12	120.00	everest
australia	305746	157.204.7.46	Jul 11, 2006 11:26:16pm	12	207.00	everest
austria	305843	157.204.7.23		0	0.00	
azerbaijan	305766	157.204.7.117	Jul 12, 2006 12:05:00am	12	6.00	everest
Total Servers: 14			Totals	153	2,258.00	

Figure 1: Server ID column display on the Search Results Report

Using the above example, if we wanted to generate a policy audit report for changes made to the two clients called "algeri" and "antartic", you would use the following variable definition for clientList:

```
clientList   numberListType := numberListType(305797, 305871);
```

3.1.5 serverList

If this parameter is set, it overrides the serverGroupID and cascade parameters and looks for a set of NetBackup policies that were associated with one or more of the master servers in the serverList parameter.

If the serverList parameter is set, it will override any values set in both the serverGroupID and clientList parameters.

3.1.6 policyRegExpr

This parameter is optional but if set, allows the user to filter and display only policies that match a character string regular expression. This parameter works in conjunction with all the other parameters to filter and report on only NetBackup policies that match the regular expression.

Note: The regular expressions are case insensitive

The following table shows examples or possible regular expressions that can be used in this parameter:

Example policyRegExpr parameter	Definition
A*	Filter and display all policies that start with the letter "A"
A*B*	Filter and display all policies that start with the letter "A" AND have the letter "B" in their name
A?B*	Filter and display all policies that start with the letter "A" and have the letter "B" in the third character position

3.2 Customize The Location Of The Resulting Report

Hitachi Data Systems provides the user with the source code for each of the NetBackup Policy Auditing Reports. A user is invited to modify these files and place the resulting report output file in a different directory/filename/suffix from the default location provided with the sample report.

To modify the default destination of your report files, you should execute the following:

Locate the file called "custom_report_vars.sql" in the directory $APTARE_HOME/database/custom_reports. Edit this file and change the parameter called REPDIRECTORY at the end of the file. All of the custom reports include and use this file for their global report variables. You can change the destination of all of your reports by simply changing this parameter. See the *Automated Reports Configuration Guid*e included on the Portal Software Installation CD for more details.

3.3 Customizing The Report Format

In addition to customizing the selection criteria for any of the reports, a user can modify and customize the output format or the report. Hitachi Data Systems ships the source code for each report and customers are invited to modify this source code to meet their unique report formatting requirements.

The only limitation is that the report can only be saved in an ASCII text format. This does include formats such as plain text, HTML, CSV file, etc. If you wish to save the report in PDF, we recommend purchasing a third-party PDF writing package and integrating this with the report source file proved by Hitachi Data Systems.

4. Report Detail

The section will provide a detailed review and look at each of the four reports that are provided by the HBSM – NetBackup Policy Auditing Module. For each report, we display examples of the report

4.1 NetBackup Policy Audit Summary Report

This report provides a one-line summary of the changes made to a NetBackup Policy for the selected reporting period. The summary includes the date/time of the change, the name of the associated master server, the name of the policy, and a brief description of the change.

The following is a sample NetBackup Policy Audit Summary Report

```
          N E T B A C K U P    P O L I C Y    A U D I T     R E P O R T
          Completed From 15-Jan-2006 12:00:00am - 21-Jan-2006 11:59:59pm
                    Sorted By Master Server Name, Change Date


DATE                MASTER SERVER    POLICY NAME                POLICY CHANGE
----                -------------    -----------                -------------
21-JAN-06 14:46:03  masterA          unix_systems               New policy created
21-JAN-06 14:46:03  masterA          Windows-NT-Systems         New policy created
21-JAN-06 14:46:03  masterB          SQL-Databases              New policy created
21-JAN-06 14:46:03  masterB          Oracle-Databases           New policy created
21-JAN-06 14:46:03  masterC          Windows-Systems            New policy created
```

4.2 NetBackup Policy Audit Detail Report

This report provides a detailed explanation of all of the changes made to any policy for the selected report scope and time period. A detailed description of each change made to a NetBackup policy is displayed on a single line and grouped per policy and master server. The following policy attributes are displayed in this report:

- The creation of a new policy
- Changes to the core policy attributes include such attributes as multi-streaming, keywords, cross-mount points, default storage unit, default volume pool, etc.
- Add, change, delete of policy include and exclude directives
- Add, change, delete of policy clients
- Add, change, delete of policy schedules including retention periods, frequency, schedule type (calendar Vs frequency), number of copies, etc.

The following is an example of the NetBackup Policy Detail Report

```
      N E T B A C K U P    P O L I C Y    A U D I T    D E T A I L    R E P O R T
            Completed From 20-Jan-2006 12:00:00am - 29-Jan-2006 11:59:59pm
                Sorted By Master Server Name, Policy Name, Change Date


Master: masterA, Policy: Windows-Servers
   25-JAN-06 08:49:51  Removed client:   Winston
   26-JAN-06 14:41:06  Changed policy:   Changed default storage unit from su01 to su02
```

```
Master: masterB, Policy: Oracle
   25-JAN-06 17:24:34  Added client:     portugal
   25-JAN-06 17:24:34  Added client:     england
   25-JAN-06 17:24:34  Removed client:   luxenburg
   26-JAN-06 14:37:06  Changed policy:   Multipexing set to ON
   26-JAN-06 14:41:06  Changed policy:   Retention period changed from 30 to 60 days

Master: masterB, Policy: Oracle-Full
   25-JAN-06 11:07:37  Added client:     oracle-client07
   25-JAN-06 11:07:37  Added pathname:   /opt/oracle/admin/backup_ora_hot_oracle

Master: masterC, Policy: Oracle-Incr
   26-JAN-06 03:18:47  Added client:     oracle-client21
   26-JAN-06 03:18:47  Added pathname:   /opt/oracle/admin/backup_ora_cold
```

4.3 NetBackup Policy Audit Client Detail Report

This report provides a detailed description of the list of changes to client membership in any policy based on the report scope and selection criteria. For each NetBackup Policy, this report will display a list of the added and removed clients grouped by date, master server, and policy name.

As clients are added and removed from various policies on your master servers, you can track the changes over time.

The following is an example of the NetBackup Policy Audit Client Detail Report:

```
        N E T B A C K U P   P O L I C Y   C L I E N T   A U D I T   R E P O R T
              Completed From 01-Jan-2006 12:00:00am - 07-Jan-2006 11:59:59pm
                     Sorted By Change Date, Master Server, Client

DATE                   MASTER SERVER  POLICY            ADDED CLIENTS    REMOVED CLIENTS
----                   -------------  ------            -------------    ---------------
03-JAN-2006 08:19:17   masterA        UNIX-Filesystems  mag-unix-07
03-JAN-2006 08:19:20   masterA        Test                               mag-unix-03
03-JAN-2006 08:19:20   masterA        Test                               mag-unix-09
04-JAN-2006 04:13:18   masterA        Test              mag_unix_31
04-JAN-2006 14:29:31   masterB        NBU-servers                        nbu-media-01
04-JAN-2006 14:30:13   masterB        Solaris-servers                    mag-sol-02
05-JAN-2006 17:22:32   masterB        Windows-NT                         mag-win-45
05-JAN-2006 17:37:15   masterC        Solaris-clients                    mag-sol-24
```

4.4 NetBackup Policy Audit File Detail Report

This report provides a detailed description and list of changes made to the file directives for any policy based on the report scope and selection criteria. A single line is displayed in this report for each addition, deletion, or change made to a policy directive. The data is grouped and displayed by date, master server, and NetBackup Policy name.

This report is extremely useful to determine what changes were made to the include and exclude directives for your NetBackup policies over any calendar period.

The following is an example of the NetBackup Policy Audit File Detail Report:

N E T B A C K U P P O L I C Y P A T H N A M E A U D I T R E P O R T

Completed From 08-Jan-2006 12:00:00am - 14-Jan-2006 11:59:59pm

Sorted By Change Date, Master Server, Client

DATE	MASTER SERVER	POLICY	PATHNAME CHANGE
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/vol0
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: NEW_STREAM
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/local2
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/local3
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/local1
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/local4
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/local7
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/local9
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/local8
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/local6
08-JAN-06 03:06:45	masterA	netapp-filer	Removed: /vol/vol0
08-JAN-06 03:06:46	masterB	WindowsNT	Removed: ALL_LOCAL_DRIVES

Appendix A: Customizing Your Report Date/Time Period

Many of the reports in HBSM provide you with the capability to pass a parameter of type "dateRangeType" to the main reporting method. In this section we will take a look at this custom HBSM data type and describe in detail on how best to leverage the features of this unique data type.

The dateRangeType is a custom HBSM type parameter in HBSM. It is an object that allows you to pass many different types of date range parameters to the method. For example, you might want to report on the "last 14-days" and have the underlying HBSM method figure out the true timeframe. If you look for a statement block just above the method that look's something like this:

```
dateRange       dateRangeType := dateRangeType(
    timePeriod    => report_package.REPORT_PERIOD_LAST_10_DAYS,
    startTime     => NULL,
    finishTime    => NULL,
    startDate     => NULL,
    finishDate    => NULL,
    timezoneName  => NULL,
    useFinishTime => util.IS_TRUE);
```

The simplest was to use this custom type is to pass a constant in the first parameter and pass NULL for all the other parameters. The first parameter to a dateRangeType object is called "timePeriod". HBSM provides a predefined set list of time periods that you can use in any of your reports.

The following table shows the list of possible timePeriod values

Time Period Constant Values:

- `report_package.REPORT_PERIOD_LAST_12_HOURS`
- `report_package.REPORT_PERIOD_LAST_24_HOURS`
- `report_package.REPORT_PERIOD_LAST_48_HOURS`
- `report_package.REPORT_PERIOD_LAST_72_HOURS`
- `report_package.REPORT_PERIOD_WEEK_TO_DATE`
- `report_package.REPORT_PERIOD_MTH_TO_DATE`
- `report_package.REPORT_PERIOD_QTR_TO_DATE`
- `report_package.REPORT_PERIOD_YEAR_TO_DATE`
- `report_package.REPORT_PERIOD_PREV_WEEK`
- `report_package.REPORT_PERIOD_PREV_MONTH`
- `report_package.REPORT_PERIOD_PREV_YEAR`
- `report_package.REPORT_PERIOD_LAST_7_DAYS`
- `report_package.REPORT_PERIOD_LAST_10_DAYS`
- `report_package.REPORT_PERIOD_LAST_14_DAYS`
- `report_package.REPORT_PERIOD_LAST_21_DAYS`
- `report_package.REPORT_PERIOD_LAST_30_DAYS`

- `report_package.REPORT_PERIOD_LAST_60_DAYS`
- `report_package.REPORT_PERIOD_LAST_120_DAYS`
- `report_package.REPORT_PERIOD_LAST_180_DAYS`
- `report_package.REPORT_PERIOD_LAST_365_DAYS`
- `report_package.REPORT_PERIOD_LAST_YEAR`
- `report_package.REPORT_PERIOD_LAST_3_YEARS`
- `report_package.REPORT_PERIOD_LAST_5_YEARS`
- `report_package.REPORT_PERIOD_LAST_7_YEARS`

If you do not want to use the predefined timePeriod values from the table above, you can provide a specific date/time range by setting the following four parameters within the dateRangeType:

- startTime

  The startTime parameter is a numeric value in the range 0000 – 2359. It represents the hours and seconds since midnight, for example: 2100 would be 9pm

- finishTime

  The finishTime parameter is a numeric value in the range 0000 – 2359. It represents the hours and seconds since midnight, for example: 0600 would be 6am

- startDate

  The startDate parameter is an Oracle DATE type and should only contain the day component. The system will use the startTime to determine the time in minutes and seconds. The following are examples of possible values for the startDate parameter: to_date('01-JAN-2005'), SYSDATE-5.

- finishDate

  The finishDate parameter is an Oracle DATE type and should only contain the day component. The system will use the finishTime to determine the time in minutes and seconds. The following are examples of possible values for the finishDate parameter: to_date('01-JAN-2005'), SYSDATE-5.

NOTE: Oracle has a built-in function called SYSDATE that will return the current date/time. You can use this variable in conjunction with Oracle commands such as TRUNC to build a specific date range. For example, If we wanted to make the startDate equal to the beginning of the current week, we could use the following syntax: startDate => to_date(TRUNC(SYSDATE, 'Day'))

You should refer to Oracle documentation for a complete list of the DATE methods.