HITACHI
Inspire the Next

Hitachi Application Protector User Guide for SAP®

FASTFIND LINKS

Hitachi Data Systems

MK-91HAP016-00

Contents

Preface

This document guides you through the various operations that you can perform by using Hitachi Application Protector for SAP® (Application Protector).

The preface describes the following topics:

- Intended audience
- Product version
- Related documents
- Document organization
- Document conventions
- Getting help
- Comments

Notice: The use of all Hitachi Data Systems products is governed by the terms of the agreement(s) with Hitachi Data Systems.

Intended audience

This document is intended for customers, application backup administrators, and Hitachi Ltd. partners involved in configuring and using Application Protector. Readers of this document should be familiar with the following concepts:

- Oracle® Database Server administration
- Linux® and Solaris® operating system
- Storage administration
- Backup and recovery concepts
- SAP® BR*Tools

Product version

This document revision applies to Hitachi Application Protector User Guide for SAP® v1.2 release.

Related documents

- *Hitachi Application Protector Quick Install & Configuration Guide for SAP®*, MK-91HAP018
- *Hitachi Application Protector CLI Guide for SAP®*, MK-91HAP024
- *Hitachi Application Protector Troubleshooting Guide for SAP®*, FE-91HAP020

Document revision level

This section provides a history of the revision changes to this document.

Revision	Date	Description
MK-91HAP016-00	July 2014	Initial release

Document organization

The following table provides an overview of the content and organization of this document. Click the chapter title in the first column to refer that chapter. The first page of every chapter contains links to the contents.

Chapter	Description
Chapter 1, Introduction	Provides an introduction and overview of Application Protector. It also provides prerequisite details.
Chapter 2, Setting up Application Protector	This chapter provides the procedure to setup Application Protector.
Chapter 3, Configuring Application Protector	This chapter provides the details to configure storage system and Application Protector Server and Application Protector Client. It also provides you with the details to activate license and import metadata.
Chapter 4, Using Application Protector	This chapter provides the procedure to use Application Protector for creating, listing and deleting snapshots and performing recovery.
Chapter 5, Managing logs	This chapter provides the details to view event logs and operation logs.
Appendix A, Appendix	The appendix provides the details of snapshot limit for supported storage and HAPRO sync details.
Glossary	Defines the acronyms and special terms used in this document.
Index	Provides a detailed and linked list of topics in this document.

Document conventions

The document uses the following symbols to draw attention to the specific information.

Symbol	Meaning	Description
	Note	Notes emphasize or supplement important points of the main text.
	WARNING	Warnings indicate that failure to take a specified action could result in loss of data or serious damage to the hardware.

The document uses the following conventions for the support matrix.

Convention	Description
√	Features fully functional and available in Hitachi Application Protector User Guide for SAP® v1.2 release.
x	Features not functional and not available in Hitachi Application Protector User Guide for SAP® v1.2 release.
Not Supported	Features not supported by Hitachi Application Protector v1.2 release.
-	Not applicable

The document uses the following typographic conventions.

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click **OK**.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: copy source-file target-file. **Note**: Angled brackets (< >) are also used to indicate variables.
`screen/code`	Indicates text that is displayed on screen or entered by the user. Example: `# pairdisplay -g oradb`
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: # pairdisplay -g <group> Note: Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.
| vertical bar	Indicates that you have a choice between two or more options or arguments. Examples: [a | b] indicates that you can choose a, b, or nothing. { a | b } indicates that you must choose either a or b.
underline	Indicates the default value. Example: [a | b]

Getting help

If you need to call the Hitachi Data Systems Support Center, make sure you provide as much information about the problem as possible, including:

- The circumstances surrounding the error or failure.
- The content of any error message(s) displayed on the host system(s).

The Hitachi Data Systems customer support staff is available 24 hours a day, seven days a week. If you need technical support, log on to the Hitachi Data Systems Portal for contact information at https://hdssupport.hds.com.

Comments

Your comments and suggestions to improve this document are greatly appreciated. Please send us your comments on this document to doc.comments@hds.com. Include the document title, number, and revision, and refer to specific section(s) and paragraph(s) whenever possible.

Thank you! (All comments become the property of Hitachi Data Systems.)

1

Introduction

Hitachi Application Protector for SAP® (Application Protector) is a snapshot-based backup and recovery software. It is based on the client-server architecture. Application Protector Server is installed on the server having Oracle Database on a non-Automatic Storage Management (ASM) setup in the SAP® (SAP) environment. The Application Protector Client can be installed on the same machine as that of Application Protector Server or on other machine.

This chapter describes the following topics:

Application Protector overview

Application Protector facilitates creation of snapshots of the Oracle Database in SAP environment. You can recover the database from the snapshot. Application Protector uses the following approach:

1. Install and activate the Application Protector license, as applicable.
2. Register the supported storage arrays.
3. Configure the Application Protector Server and Client.
4. Create snapshots and recover database from the snapshots. In addition, you can restore database using a snapshot.
5. View progress and logs of the operations.

Application Protector supports the following.

- Register supported storage arrays.
- Set policy to configure snapshot retention count at server level.
- Create ShadowImage® (SI), Hitachi Thin Image (HTI), and TreeClone snapshots at volume level.
- List, delete, mount, and unmount snapshots.
- Recover and restore database from the snapshot at volume level.
- Native Device-Mapper Multipath environment for Red Hat® Enterprise Linux® (RHEL) and SUSE® Linux Enterprise Server (SLES) operating system.
- Protect databases hosted on the Logical Volume Manager (LVM) devices for SLES operating system. For Solaris platform, the database is hosted on HNAS exports.

Application Protector operations

Application Protector integrates itself with SAP® BR*Tools using BACKINT interface to support end-to-end snapshot based backup and recovery operations. It also provides a command line utility to perform miscellaneous tasks such as configuration, registering the license key, and snapshot management tasks. Refer the following for details:

❒ Using the Application Protector CLI

❒ Integrating with SAP® BR*Tools

Using the Application Protector CLI

You can perform the following using the Application Protector CLI.

- Configuration:
  - Storage configuration
  - Application Protector Server configuration
  - Application Protector Client configuration

  For details about Application Protector configuration, see Configuring Application Protector.
- License management:
  - Generate license request
  - Activate and list Application Protector license

  For details about Application Protector licensing, see Licensing Application Protector.
- Logs and operations:
  - List Application Protector logs
  - List Application Protector operations
  - List events

  For details about Application Protector logs and operations, see Managing logs.
- Application Protector tools:
  - HAPRO dump
  - HAPRO sync

  For details about Application Protector utilities, see HAPRO dump.
- Snapshot management operations:
  - List snapshot
  - Delete snapshot
  - Mount snapshot
  - Unmount snapshot
  - Recover snapshot
  - Restore snapshot

  For details about Application Protector snapshot management operations, see Using Application Protector.

Integrating with SAP® BR*Tools

Application Protector integrates with SAP® BR*Tools using the BACKINT interface. This helps in providing end-to-end support for backup and recovery tasks initiated using the following SAP® BR*Tools utilities:

- `BRBACKUP`: Create snapshot-based backup of the online Oracle Database.

  For details about creating a snapshot, see Creating a snapshot.

- `BRRESTORE`: Restore the database as per given criteria. For details about restoring a database using a snapshot, see Restoring a snapshot.

- `BRRECOVER`: Recover the database as per given criteria. Application Protector supports complete and point-in-time (PIT) recovery.

  For details about recovering a database using a snapshot, see Recovering database using a snapshot.

The SAP tools perform the snapshot management tasks. The `BRBACKUP`, `BRRESTORE`, and `BRRECOVER` utilities communicate with Application Protector through the Application Protector BACKINT interface. For a backup, restore, and recover, BR*Tools calls the Application Protector BACKINT interface and performs the required operation.

NOTE: Installation and related prerequisites are described in the *Hitachi Application Protector Quick Install & Configuration Guide for SAP®* document.

Supported database server

Application Protector supports the following versions of Oracle Database on the supported operating system.

Table 1-1: Supported Oracle Database versions

Operating system	32 bit	64 bit	Oracle database version
SLES 11 SP3	√	√	Oracle 11g Release 2 (11.2.0.3 and 11.2.0.4) (non-ASM)
	√	√	
RHEL 6.3	√	√	Oracle 11g Release 2 (11.2.0.3 and 11.2.0.4) (non-ASM)
• Solaris 10 u11 • Solaris 11	√	√	Oracle 11g Release 2 (11.2.0.3 and 11.2.0.4) (non-ASM)

For details about configuring the Oracle Database with LVM and multipath devices, see the *Hitachi Application Protector Quick Install & Configuration Guide for SAP®.*

Supported storage arrays

Application Protector supports the following storage arrays.

Table 1-2: Supported storage configurations

Storage	Snapshot type	Protocol	SLES 11 SP3	RHEL 6.3	Solaris 10u11 and Solaris 11
VSP (RAID 700)	Full copy and HTI snapshots	FC	√	√	X
		iSCSI	X	X	X
HUS (DF850)	Full copy and HTI snapshots	FC	X	√	X
		iSCSI	X	√	X
HNAS (3090)	TreeClone snapshots	NFS v3	√	√	√

Firmware version for storage sub-system

Application Protector supports the following firmware versions.

Table 1-3: Firmware version

Storage subsystem	Microcode/Firmware version
VSP RAID 700	70-06-04-00/00
HUS DF850	0915/B-S
HNAS 3090	NAS Platform (M1SEKW0933273)

For details about storage prerequisites, see the Storage Prerequisites section in the *Hitachi Application Protector Quick Install & Configuration Guide for SAP®.*

Application Protector prerequisites

This section provides the details of Application Protector system requirements and Application Protector Server and Client prerequisites. You must confirm that the installation prerequisites in this section are met before you install Application Protector. The requirements apply for remote and local installations.

NOTE: You must create the following directories in `ORACLE_HOME` before installing the Application Protector SAP build:

- sapbackup
- sapreorg
- sapcheck
- saparch

System requirements

The following table provides the Application Protector minimum system requirements.

Table 1-4: System requirements

Item	Description
System memory	4GB+
Free disk space required for installation	100MB (minimum)
Operating system	Any one for the following supported operating system: • SLES 11 SP3 (32-bit and 64-bit) • RHEL 6.3 (32-bit and 64-bit) • Solaris 10 Update 10 and Solaris 11 (x86)
Networking	Gigabit Ethernet recommended
Application software	SAP Module ECC version 6.0 BR*Tools version 7.20 patch level 18 or higher
	For SLES platform: Oracle® Database 11g Release 2 (11.2.0.3 and 11.2.0.4) (non-ASM)
	For RHEL platform: Oracle® Database 11g Release2 (11.2.0.3 and 11.2.0.4) (non-ASM)
	For Solaris platform: Oracle® Database 11g Release2 (11.2.0.3 and 11.2.0.4) (non-ASM)

For details about Application Protector prerequisites, see the Application Protector Prerequisites section in the *Hitachi Application Protector Quick Install & Configuration Guide for SAP®.*

2

Setting up Application Protector

This chapter guides you through the quick pointers for installing Application Protector Server and Client. You can install Application Protector Server and Client on same machine or different machines on the same network.

This chapter describes the following topics:

Installing Application Protector

Install the Application Protector Server and Client using the installer. The installer is in the form of a shell script file. Application Protector is a 32-bit application that can be installed on both 32-bit and 64-bit systems.

For details about storage and Application Protector Server and Client prerequisites, see:

- Supported storage arrays
- Application Protector prerequisites

Install the Application Protector Server by using the following command:

```
./HAPROSetup_Server_x86_SLES.sh -t <Block (VSP/HUS)/HNAS>*[1]
install

./HAPROSetup_Server_x86_RHEL.sh -t <Block (VSP/HUS)/HNAS*>
install

./HAPRO-SAP-Server-v1.2.0.3-Solaris-11-x86.sh install
```

Install the Application Protector Client by using the following command:

```
./<HAPRO Client>.sh install
```

For details about <HAPRO Server> and <HAPRO Client> installers for supported operating system, see *Hitachi Application Protector Quick Install & Configuration Guide for SAP®*.

Installation path

This section provides the details of Application Protector installation path.

Table 2-1: Default installation paths

Details	Path
Server installation	/opt/Hitachi/HAPRO/server
Client installation	/opt/Hitachi/HAPRO/client

Configuring Application Protector for Oracle SID

Post successful installation, Application Protector Server deploys the BACKINT adapter for BR*Tools to facilitate backups. The **HAPRO-SAP Configuration Wizard** is automatically invoked upon successful installation to configure the executable path for an Oracle user.

You can configure the executable path later by executing the following command:

```
$ <HAPRO-Server-Install-Path>/util/
HAPRO_SAP_Configuration_wizard.sh configuresid
```

1.“*” indicates: Provide “HNAS” for HNAS storage, else provide “Block (VSP/HUS)” for other storages.

```
$ <HAPRO-Server-Install-Path>/util/
HAPRO_SAP_Configuration_wizard.sh configureuser
```

Removing the Application Protector Server

You can remove the Application Protector Server by using one of the following commands.

```
./HAPROSetup_Server_x86_SLES.sh -t <Block (VSP/HUS)/HNAS>
uninstall
```

```
./HAPROSetup_Server_x86_RHEL.sh -t <Block (VSP/HUS)/HNAS>
uninstall
```

```
./HAPRO-SAP-Server-<v1.2.0.x>-Solaris-<10/11>-x86.sh
uninstall
```

```
./<HAPRO Server>.sh uninstall --complete
```

```
./<HAPRO Server>.sh uninstall -s
```

WARNING! The `--complete` option removes the Application Protector metadata cache and temporary files associated with Application Protector.

Removing the Application Protector Client

You can remove the Application Protector Client by using the following command.

```
./<HAPRO Client>.sh uninstall
```

3

Configuring Application Protector

Application Protector for SAP is a client-server licensed product that provides snapshot-based backup and recovery for Oracle Database in SAP environment. This chapter guides you to activate the Application Protector license. It also describes the details of the settings that you must perform prior to using Application Protector for snapshot management activities.

This chapter includes the following:

Configuring Application Protector

After installing Application Protector Server and Client, perform the following prior to performing the snapshot management operations:

1. Configure the BR*Tools executable path for SID. For details, see Configuring Application Protector for Oracle SID.
2. Activate the Application Protector license for the supported storage and application. For details, see Licensing Application Protector.
3. Register the supported storage. For details, see

   Configuring the storage subsystem.
4. Configure Application Protector Server and Client, as required. For details, see Configuring the Application Protector Server and Client.

Licensing Application Protector

After installing Application Protector, register a valid license key on the server.

The following is applicable for an Application Protector license key:

- The Application Protector license is node-locked. A license is generated for a given server and you can install it on that server only.
- The license is a perpetual license.

  For example, license keys purchased and installed for version 1.0 continues to function for all 1.x releases. Upgrading to 2.x requires an updated license key.

NOTE: You must generate and activate the Application Protector license for SLES and RHEL setups.

To install and activate the production license

1. Create a capability license request based on information provided while purchasing the product license from HDS.
2. Provide the Activation ID for the supported storage.
3. Install the license response file reverted by the HDSLicensing@hds.com team as a part of production license activation.

This section describes the following:

- ❒ Generating the Application Protector license
- ❒ Activating the Application Protector license
- ❒ Listing the Application Protector license

Generating the Application Protector license

The license request is server specific. You must generate a license request for the specified server using the Application Protector CLI. Send this license request to the HDS licensing team. The HDS licensing team sends the license response file. Use the response file to activate the license.

The `HAPRO` client executable is copied to the `/opt/Hitachi/HAPRO/client/bin` directory. You can run the `hapro` command from anywhere in the console.

To generate a license request

- Execute the `hapro admin generatelicenserequest` command and provide the following mandatory parameters.

Table 3-1: Mandatory parameters to generate license

Parameter	Value/details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.
First Name	First name. Maximum 64 characters are supported.
Last Name	Last name. Maximum 64 characters are supported.
Activation ID	Activation ID provided to you with the product.
Email ID	Valid email ID. Maximum 32 characters are supported.
Company Name	Company name. Maximum 32 characters are supported.
Site ID	Company site ID. Maximum 64 characters are supported.
Address	Company address. Maximum 256 characters are supported.
Country	Country. Maximum 64 characters are supported.
License request file	Provide the license request file with the path.

For more details about generating license parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Syntax for SLES and RHEL operating system

```
hapro admin generatelicenserequest
```

Sample command

```
hapro admin generatelicenserequest -a saporacle -s <Hostname/
IP of Application Protector Server/ FQDN> -u <user> -P
<Password> -E <email@hds.com> -f <first name> -L <last name>
-i <activation ID> -C <company> -c <country> -x /
<Response_SAP_HUS_LastOctetOfIP.xml>
```

Activating the Application Protector license

Application Protector is available with the following license types:

- Trial License (30 days)
- Production License (unlimited)

You must activate the trial license or the production license on the specified server using Application Protector CLI.

After 30 days, the trial license expires and you cannot use the Application Protector features. You must activate the production license to use Application Protector further.

To activate the license

- Execute the `hapro admin activatelicense` command and provide the following mandatory parameters.

Table 3-2: Mandatory parameters to activate license

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.
Trial license/Production license response file	Provide the response file name with the path for production license. For trial license, just provide the parameter.

For more details about activating license parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Syntax for SLES and RHEL operating system

```
hapro admin activatelicense
```

Sample command to activate trial license

```
hapro admin activatelicense -s <Hostname/ IP of Application
Protector Server/ FQDN> -a saporacle -t -u <user> -P
<Password>
```

Listing the Application Protector license

You can perform the snapshot management operations for the activated production license only. All the licenses installed on the specified server are listed.

To list the license

- Execute the `hapro admin listlicense` command and provide the following mandatory parameters.

Table 3-3: Mandatory parameters to list license

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.

For more details about listing license parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Syntax for SLES and RHEL operating system

```
hapro admin listlicense
```

Sample command

```
hapro admin listlicense -s <Hostname/ IP of Application
Protector Server/ FQDN> -a saporacle -u <user> -P <password>
-l
```

Configuring the storage subsystem

Application Protector uses the storage array definitions while integrating with the storage that is hosting the databases. On registration, Application Protector maintains a list of storage arrays for various activities.

Application Protector supports HUS-DF850, VSP-RAID700, and HNAS 3090 Hitachi storage arrays. You can register, change, unregister, modify, and list the registered storage arrays. This section provides the details to register, modify, list, and unregister the storage arrays.

Registering the storage array

You must register the storage subsystem with the storage array details. The storage registration is a one time activity. After authenticating the account for the first time, the logged on information is saved in the system, and the account automatically authenticates when you launch the application next time.

Prerequisites to register the storage array

- Activate the license for the supported storage array and application.

For details about registering supported Hitachi storages, see the following:

Registering the VSP storage

VSP storage is supported for RHEL and SLES platform only. You must configure CCI for the VSP storages. For details about configuring CCI for VSP storage, see *Hitachi Application Protector Quick Install & Configuration Guide for SAP*®.

To register the VSP storage

- Execute the `hapro server registerstoragearray` command and provide the following mandatory parameters.

Table 3-4: Mandatory parameters to register a VSP storage

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.
Storage type	This parameter specifies the type of the storage array. Supported values are `hus`, `hnas`, and `vsp`.
Storage array IP(s)	Storage subsystem IP addresses of the storage controller separated by a comma for the -I | --ip parameter. Provide the Device manager location.Specify the location where the device manager port is configured. By default, the port number of HDvM is 2001.
Serial number	Valid serial number of the VSP storage.
RAIDCOM instance number	RAIDCOM instance number. A positive number. Specify the instance defined in the HORCM Manager.
Storage array admin credentials	Valid storage array admin credentials.

You must provide the following mandatory parameters for registering the VSP storage array. For more details about registering storage parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

Syntax

```
hapro {server} registerstoragearray
```

Sample command for VSP

```
hapro server registerstoragearray -s <Hostname / FQDN / IP
of HAPRO server> -a saporacle -T <vsp> -I <storage array
IP> -r <VSP serial number> -o <RAIDCOM instance number> -
N <storage array admin user> -Z <storage array admin
password> -p <storage pool name>
```

Registering the HUS storage

HUS storage is supported on RHEL platform only.

To register the HUS storage

- Execute the `hapro server registerstoragearray` command and provide the following mandatory parameters.

Table 3-5: Mandatory parameters to register a HUS storage

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.
Storage type	This parameter specifies the type of the storage array. Supported values are `hus`, `hnas`, and `vsp`.
Storage array IP(s)	Storage subsystem IP addresses of the storage controller separated by a comma for the -I | --ip parameter. Provide the IP of the storage array.

You must provide the following mandatory parameters for registering the VSP storage array. For more details about registering storage parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

Syntax

```
hapro {server} registerstoragearray
```

Sample command for HUS storage

```
hapro server registerstoragearray -s <Hostname / FQDN / IP
of HAPRO server> -u <user> -P <password> -a saporacle -T
hus -I <storage array IP(s)>
```

Registering the HNAS storage

HNAS storage is supported for RHEL, SLES, and Solaris platforms.

To register the HNAS storage

- Execute the `hapro server registerstoragearray` command and provide the following mandatory parameters.

Table 3-6: Mandatory parameters to register HNAS storage

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.
Storage array IP(s)	Storage subsystem IP addresses of the storage controller separated by a comma for the -I | --ip parameter. Provide the IP of the storage array.
Storage type	This parameter specifies the type of the storage array. Supported values are `hus`, `hnas`, and `vsp`.

You must provide the following mandatory parameters for registering the VSP storage array. For more details about registering storage parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

Syntax

```
hapro {server} registerstoragearray
```

Sample command for HNAS storage

```
hapro server registerstoragearray -s <Hostname / FQDN / IP
of HAPRO server> -u <user> -P <password> -a saporacle -T
hnas -I <storage array IP(s)>
```

Modifying the storage array details

For HNAS and HUS storages:

You can modify all parameters except storage type.

For VSP:

- Serial number
- RAIDCOM instance number
- Storage pool number
- Description
- Storage username and password

Prerequisites to modify the storage array details

1. Activate the license for the supported storage array and application.
2. Register the supported storage array.
3. List the registered storage arrays to get the storage ID.

NOTE: You cannot change the storage type.

To modify the storage array details

- Execute the `hapro server modifystoragearray` command and provide the following mandatory parameters.

Table 3-7: Mandatory parameters to modify storage details

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.
Storage array ID	Valid storage array ID.
Storage array admin credentials	Valid storage array admin credentials. Mandatory for VSP.

You must provide the following mandatory parameters for changing the storage array details. For more details about changing storage parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

Syntax

```
hapro {server} modifystoragearray
```

Sample command for HUS storage

```
hapro server modifystoragearray -s <Hostname, IP of
Application Protector Server, FQDN> -a saporacle -u <user>
-P <password> -i <storage array ID>
```

Sample command for VSP storage

```
hapro server modifystoragearray -s <Hostname/FQDN/IP of
HAPRO server> -a saporacle -i <storage array ID> -I
<storage array IP> -r <serial number> -o <RAIDCOM instance
number> -N <storage array admin user> -Z <storage array
admin password> -p <storage pool name> -u <user> -P
<password>
```

Sample command for HNAS storage

```
hapro server modifystoragearray -s <Hostname/FQDN/IP of
HAPRO server> -a saporacle -i <storage array ID> -I
<storage array IP> -u <user> -P <password>
```

Unregistering the storage array

You cannot unregister a storage array if snapshots are present in the selected storage array.

Prerequisites to unregister the storage array

1. Activate the license for the supported storage array and application.
2. Register the supported storage array.
3. List the registered storage arrays to get the storage ID.

To unregister the storage array

- Execute the `hapro server unregisterstoragearray` command and provide the following mandatory parameters.

Table 3-8: Mandatory parameters to unregister storage array details

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.
Storage type	Supported storage array, VSP.
Storage array ID	Valid storage array ID.

You must provide the following mandatory parameters for unregistering the VSP storage array. For more details about unregistering storage parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

Syntax

```
hapro {server} unregisterstoragearray
```

Sample command for HUS array

```
hapro server unregisterstoragearray -s <Hostname/IP of
Application Protector Server/ FQDN> -u <user> -P <password> -
a saporacle -i <storage array ID>
```

Sample command for VSP array

```
hapro server unregisterstoragearray -s <Hostname/FQDN/IP
of HAPRO server> -u <user> -P <password> -a saporacle -i
<storage array ID>
```

Listing the storage arrays

You can list the registered storage arrays.

Prerequisites to list the storage arrays

1. Activate the license for the supported storage array and application.
2. Register the supported storage array.

To list the storage array

- Execute the `hapro server liststoragearray` command and provide the following mandatory parameters.

Table 3-9: Mandatory parameters to list storage array

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.

NOTE:

- To view the complete data for a particular column, use the `Enable long listing` flag in the command.
- The fields that are not provided by the user, are marked with "-" in the output.

For more details about listing the storage parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

Syntax

```
hapro {server} liststoragearray
```

Sample command

```
hapro server liststoragearray -s <Hostname / FQDN / IP of
HAPRO server> -u <user> -P <password> -a saporacle
```

Sample command for long listing

```
hapro server liststoragearray -s <Hostname / FQDN / IP of
HAPRO server> -u <user> -P <password> -a saporacle -l
```

Configuring the Application Protector Server and Client

The Application Protector Client interface allows you to configure the server to use Application Protector effectively. The following section describes the configurable parameters in Application Protector.

Configurable Application Protector Server parameters

The configurable parameters for Application Protector Server are:

- Configuring the log level
- Configuring the metadata directory
- Configuring the log directory path
- Configuring the snapshot retention count
- Configuring the metadata backup path

You can reset the configurable parameters to the default values by using the `resetconfig` option.

You can set the configuration of Application Protector Server and Client for the specified application.

NOTE: The commands and actions are available depending on the application (`-a|--app`) you select.

Prerequisites to set the configuration

- Activate the license for the supported storage array and application.

To set the server and client configuration

- Execute the `hapro admin setconfig` command and provide the following mandatory parameters

Table 3-10: Mandatory parameters to configure Application Protector Server

Parameter	Value/Details
Application	Application type, `saporacle`
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>
User credentials	Valid username and password
Configuration parameter	Configuration parameter as required. • `haprometadir` • `haprologdir` • `haprosnapshotretentioncount` • `metadatabackuppath` • `mounttoolpath`[1] • `haprologlevel` • `clientloglevel` • `datetimeformat`
Configuration value	Configuration value as required. • `haprologlevel: fatal/error/warn/info/dbg1;` • `clientloglevel: fatal/error/warn/info/debug/trace; datetimeformat: iso/system`

1.This parameter is not applicable for Application Protector for SAP.

For more details about setting configuration parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

Syntax

```
hapro {admin} setconfig
```

Sample command

```
hapro admin setconfig -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -p
haprologlevel -g error
```

For details about the default configuration values, see

Configuration parameter default values.

NOTE: For Solaris operating system, if the Application Protector Server does not respond to the Client request in 30 minutes, then the operation fails and an error displays.

Configuring the log level

The operation logs are generated depending on the log level you have set. If you set the log level to say fatal, then on successful completion of the operation, no operation logs are generated.

You can set the following level of log entries in Application Protector logs.

- **fatal**: Logs fatal cases such as update that leads to inconsistent state.
- **error**: Logs only errors encountered by Application Protector.
- **warn**: Logs errors and warnings encountered by Application Protector.
- **info**: Logs information messages such as output of a particular operation.
- **dbg1**: Logs all messages including tracing types.

To configure the log level

Syntax

```
hapro {admin} setconfig
```

Sample command

```
hapro admin setconfig -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -p
haprologlevel -g error
```

Configuring the metadata directory

The Application Protector metadata is stored in a directory. If you change the metadata directory location to a valid path, all the contents of the previous metadata directory are moved to the new location.

The Application Protector metadata cache is saved in the `/opt/Hitachi/HAPRO/server/metadata/filecache` directory.

NOTE: It is recommended to backup the Application Protector metadata frequently.

WARNING! You should not change the metadata directory path when the operations are in progress.

To configure the metadata directory

Syntax

```
hapro {admin} setconfig
```

Sample command

```
hapro admin setconfig -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -p
haprometadir -g '<hapro metadata directory>'
```

Configuring the log directory path

You can configure the log directory path to save the logs generated by Application Protector.

To configure the log directory path

Syntax

```
hapro {admin} setconfig
```

Sample command

```
hapro admin setconfig -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -p haprologdir
-g '<hapro log directory>'
```

NOTE: You should not change the log directory path when the operations are in progress.

Configuring the snapshot retention count

The snapshot retention count allows you to set the snapshot limit for space efficient snapshots at server level. The snapshot retention count is server based and applies to all the databases on the server.

- Snapshots created beyond the specified count limit are rotated based on timestamp during the creation of snapshots.
- Application Protector first checks the snapshot retention count set in the configuration and then checks the maximum supported storage limit for the storage.

  For details, see Snapshot limit for supported storage.
- If you set the snapshot retention count to zero, then on creating new snapshots beyond the maximum storage limit, the snapshot retention is disabled.
- The maximum acceptable value for retention is 1024.

To configure the snapshot retention count

Syntax

```
hapro {admin} setconfig
```

Sample command

```
hapro admin setconfig -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -p
haprosnapshotretentioncount -g '<count>'
```

Configuring the metadata backup path

Application Protector stores the snapshot metadata on the user configured directory.

- You can configure the metadata backup path to a local directory, remote UNC path, or to the shared LUN path.
- The snapshot metadata is backed up after creating a snapshot. If Application Protector is unable to create a backup of the metadata, then the snapshot is created but an error is logged. You can list the error details in the operation logs.
- After snapshot deletion, the backed up metadata of the corresponding deleted snapshot is deleted.
- You can import the metadata on a host. For details, see Importing metadata.

NOTE: If you change the metadata backup path, you need to copy the existing data manually to the new location.

To configure the metadata backup path

Syntax

```
hapro {admin} setconfig
```

Sample command

```
hapro admin setconfig -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -p
metadatabackuppath -g '<valid path>'
```

NOTE: By default, the path is `/opt/Hitachi/HAPRO/server/`.

Importing metadata

You can import the Application Protector snapshot metadata by restoring the metadata from the backup path.

If you have backed up the metadata on a shared LUN, then you must have read-write access on the shared LUN to import the metadata. Import metadata does not verify and check the XML contents.

To import metadata

Syntax

```
hapro {admin} importmetadata
```

Sample command

```
hapro admin importmetadata -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -b <Import
metadata from this location>
```

Configurable Application Protector Client parameters

The configurable parameters for Application Protector Client are:

- Configuring the Application Protector Client log level
- Setting the date-time format

Configuring the Application Protector Client log level

You can set the following level of log entries in the Application Protector Client log files.

- **Fatal**: Logs fatal cases such as update that leads to inconsistent state.
- **Error**: Logs only errors encountered by Application Protector.
- **Warning**: Logs errors and warnings encountered by Application Protector.
- **Information**: Logs errors, warnings, and information types encountered by Application Protector.
- **Trace**: Logs all including tracing types.
- **Debug**: Logs debug information.

The default client log level is `info`.

To configure the log level

Syntax

```
hapro {admin} setconfig
```

Sample command

```
hapro admin setconfig -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -p
clientloglevel -g error
```

Setting the date-time format

You can set the date-time format for the Application Protector Client. The value of this field impacts on various operations such as schedule, snapshot and log listing, and recover snapshot. You can provide either ISO or system format.

To set the date-time format

Syntax

```
hapro {admin} setconfig
```

Sample command

```
hapro admin setconfig -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -p datetimeformat
-g '<date-time format>'
```

Listing the Application Protector configuration

You can list the configuration of Application Protector Server and Client for the specified application.

Prerequisites to list the configuration

- Activate the license for the supported storage array and application.

To list the server and client configuration

- Execute the `hapro admin listconfig` command and provide the following mandatory parameters.

Table 3-11: Mandatory parameters to list configuration

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN/ Valid port number (optional)>.
User credentials	Valid username and password.

NOTE:

- To view the complete data for a particular column, use the `Enable long listing` flag in the command.
- The fields that are not provided by the user, are marked with "-" in the output.

Syntax

```
hapro {admin} listconfig
```

Sample command

```
hapro admin listconfig -s <Hostname / FQDN / IP of HAPRO server> -u <user> -P <password> -a saporacle
```

Sample command for long listing

```
hapro server liststoragearray -s <Hostname / FQDN / IP of HAPRO server> -u <user> -P <password> -a saporacle -l
```

For more details about parameters and details, see *Hitachi Application Protector CLI Guide for SAP®.*

Resetting the Application Protector configuration

You can reset the configuration of the server and client to the default values for the specified server.

Prerequisites to reset the configuration

- Activate the license for the supported storage array and application.

To reset the server and client configuration

- Execute the `hapro admin resetconfig` command and provide the following mandatory parameters.

Table 3-12: Mandatory parameters to reset the configuration

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.
Configuration parameter	Configuration parameter as required. • `haprometadir` • `haprologdir` • `haprosnapshotretentioncount` • `metadatabackuppath` • `mounttoolpath`[1] • `haprologlevel` • `clientloglevel` • `datetimeformat`

1.This parameter is not applicable for Application Protector SAP.

For details about the default configuration values, see

Configuration parameter default values.

Syntax

```
hapro {admin} resetconfig
```

Sample command

```
hapro admin resetconfig -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -u <user> -P <password> -
a saporacle -p haprologlevel
```

For more details about the parameter and details, see *Hitachi Application Protector CLI Guide for SAP®.*

Configuration parameter default values

Table 3-13: Default configuration values

Parameter	Description	Default values
haprologdir	Specifies the directory where logs are saved.	/opt/Hitachi/HAPRO/server/logs/
haprologlevel	Specifies the log levels for logging of information.	Info
haprometadir	Specifies the metadata folder path.	/opt/Hitachi/HAPRO/server/
haprosnapshotretentioncount	Specifies the snapshot rotation count.	1024[1]
metadatabackuppath	Specifies the directory where the snapshot matadata is saved.	/opt/Hitachi/HAPRO/server
mounttoolpath	Specifies the mount tool path to the path where patch set is installed.	NULL
clientloglevel	Specifies the log level for logging client logs.	Info[2]
datetimeformat	Specifies the date-time format for Application Protector Client.	iso

1. The snapshot retention limit for HUS are: HTI (1024), SI (7), for VSP are: HTI (1024) and SI (3), and HNAS TreeClone (1024).
2. Client log level are: fatal, error, warn, info, debug, and trace.

4

Using Application Protector

Application Protector protects the Oracle Databases in SAP environment by using the BR*Tools interface and Application Protector CLI. You can backup and recover the Oracle Database in SAP environment using Hitachi's snapshot technology.

This chapter includes the following key topics.

Introducing snapshot management using Application Protector

Application Protector protects the Oracle Database in SAP environment that are mounted on the VSP, HNAS, and HUS LUNs. You can backup the database by creating snapshots and restoring the database by using the snapshot. You can perform the following tasks.

1. Create snapshots of the online databases using `BRBACKUP`.
2. List, mount, unmount, and delete snapshots using the Application Protector CLI.
3. Recover the database from the snapshot using `BRRECOVER`. Point-in-time (PIT) and complete recovery are supported.
4. Restore the database from the snapshot using `BRRESTORE`.

Snapshot types

This section provides the details regarding how to use Application Protector with the SAP® BR*Tools utilities to protect the Oracle Database in SAP environment.

- You can create ShadowImage (SI), Hitachi ThinImage (HTI), and TreeClone type of snapshots. For SI type of snapshots, you must create a pair relationship of P-VOL and S-VOL prior to creating a snapshot. If the requested P-VOL is in pair relationship with more than one S-VOL:

  The pair selection logic is based on the priority between the available pairs. The highest priority goes to any pair in the PAIR state, if no such pair is found, then the oldest SPLIT pair is selected.
- Application Protector takes (HTI, SI, and TreeClone) snapshot of the data files, control files, and archive logs. The archive logs and control files must be in a volume from the same supported storage array (HNAS, HUS or VSP).

NOTE: Application Protector does not support snapshot of volume created on mixed storages such as a volume1 from HUS and volume2 from VSP.

NOTE: By default, TreeClone snapshot is created.

Creating a snapshot

Application Protector takes backup of the online Oracle Database in SAP environment using BR*Tools.

This section describes the command options for BRBACKUP. If you start BRBACKUP without command options, the values in the init<SID>.sap profile file are used.

If you use BRBACKUP with the command options, these override the corresponding values in the profile file. For more details about using the options, see SAP Help Portal.

NOTE: The profile file is at $oracle home/dbs/init<SID>.sap. You can customize the profile file as required to take backup.

Prerequisites to create a snapshot

1. Activate the license for the supported storage array and application.
2. Register supported storage.
3. Set the appropriate parameters in the init<SID>.sap profile file.

To create a snapshot

1. Provide the following supported parameters.

Table 4-1: Supported parameters for BRBACKUP

Parameter	Value/Details
mode	all: Application Protector backs up the data files and redo logs (with log switch).
	full: Application Protector backs up the data files, redo logs, and archive logs.
device	Backup device type (Application Protector supports util_vol_online only).
type	online: Online backup (with Oracle backup mode). Snapshot of the input files is taken as BRTools sends the DatFiles as input files when backup type is volume_online.
	online_cons: Consistent online backup (with Oracle backup mode and control file).
	file: If backup type is file, snapshot of the DatFiles is taken and MetFiles are copied. $ORACLE_HOME is used to differentiate. In this case, BRTools sends DatFiles and MetFiles as input files when backup type is file.
	If BI_CALL is LAST, all input files (MetFiles) are copied. BRTools sends only metadata files as input files in LAST call of BRBACKUP.
verify	Verifies the backup after the files have been backed up. use_dbv: Performs a database backup followed by a check of the Oracle block structure with the DBVERIFY tool and then restores the control file.
User credentials	Valid database admin user credentials.

NOTE: The Datfiles are the database files (data files and archive files). MetFiles are the files inside $ORACLE_HOME (parameter files, spfiles, and log files).

2. Execute the `BRBACKUP` utility in BR*Tools. Set the required options, else the `init<SID>.sap` profile file values are used.
3. Provide inputs as required in the console. The operation progress appears on the console.

   You can view the logs in the `$ORACLE_HOME/sapbackup` directory.

   Syntax

   ```
   brbackup
   ```

   Sample command

   ```
   brbackup -u <user/password>
   ```

For details about BRBACKUP execution, see SAP Portal.

For more details about supported parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

NOTE: You must place the profile file or parameter file on the supported Hitachi storage. In addition, the file should be under the directory tree pointed by the environment variable `ORACLE_HOME`.

Listing the snapshots

You can list all the snapshots created on the specified server by using Application Protector CLI.

NOTE:

- To view the complete details of a particular snapshot, use the `Enable long listing` flag in the command.
- The fields that are not provided by the user, are marked with "-" in the output.

Prerequisites to list the snapshot

- Activate the license for the supported storage array and application.

To list the snapshots

- Execute the `hapro snapshot list` command and provide the following mandatory parameters.

Table 4-2: Mandatory parameters to list snapshot

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
Database name	Valid database name. Lists the snapshots on the provided database only. If the database name is not provided, all the snapshots created on the server are listed.
User credentials	Valid username and password.

For more details about listing snapshot parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Syntax

```
hapro snapshot list
```

Sample command for listing all snapshots

```
hapro snapshot list -s <Hostname/IP of Application
Protector Server/FQDN> -a saporacle -u <user> -P <password>
```

Deleting the snapshots

You can delete snapshots by using Application Protector. The following is applicable while deleting snapshot using Application Protector:

- Unmount the snapshot prior to deleting the snapshot.
- You can delete multiple snapshots.
- Snapshots created using Application Protector must be deleted using Application Protector only.
- When a snapshot is deleted, the metadata backup of the snapshot is deleted.
- The snapshot ID/BID must be exactly 16-character long unique identifier. If supplied value does not meet the format requirement, an error displays.

NOTE: It is recommended that after deleting a snapshot from Application Protector, manually delete the entry from the BR*Tools metadata.

Prerequisites to delete a snapshot(s)

1. Activate the license for the supported storage array and application.
2. Create a snapshot.

To delete a snapshot(s)

- Execute the `hapro snapshot delete` command and provide the following mandatory parameters.

Table 4-3: Mandatory parameters to delete snapshot

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
Snapshot name	Valid snapshot name. Provide the snapshot name to delete a snapshot.
Snapshot set ID	Valid snapshot set ID. Provide either the snapshot name or snapshot set ID.
User credentials	Valid username and password.

For more details about deleting snapshot parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Syntax

```
hapro snapshot delete
```

Sample commands

```
hapro snapshot delete -s <Hostname/IP of Application
Protector Server/FQDN> -a saporacle -u <user> -P <password>
-x <snapshot name>
```

```
hapro snapshot delete -s <Hostname/IP of Application
Protector Server/FQDN> -a saporacle -u <user> -P <password>
-X <snapshot set ID>
```

Mounting the snapshot

This command lets you mount the snapshot at specified path on system. You can mount the snapshots by using the Application Protector CLI.

NOTE: On Linux platform, the Application Protector mount entries are not listed in the `/etc/mtab`. Use the `cat/proc/mounts` command to list the Application Protector mounts.

Prerequisites to mount a snapshot

1. Activate the license for the supported storage array and application.
2. Create a snapshot.

To mount a snapshot

- Execute the `hapro snapshot mount` command and provide the following mandatory parameters.

Table 4-4: Mandatory parameters to mount a snapshot

Parameter	Value/Details
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
Snapshot name	Valid snapshot name. Provide the snapshot name to mount a snapshot.
Snapshot set ID	Valid snapshot set ID. Provide either the snapshot name or snapshot set ID to mount a snapshot.
Mount point	Valid directory path.
User credentials	Valid username and password.

For more details about mounting snapshot parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Syntax

```
hapro snapshot mount
```

Sample command

```
hapro snapshot mount -s <Hostname/IP of Application
Protector Server/FQDN> -a saporacle -u <user> -P <password>
-x <snapshot name> -z <valid directory path>
```

Unmounting the snapshot

This command lets you unmount a mounted snapshot. You can unmount the snapshots by using Application Protector.

Prerequisites to unmount a snapshot

1. Activate the license for the supported storage array and application.
2. Snapshot should be mounted.

To unmount a snapshot

- Execute the `hapro snapshot unmount` command and provide the following mandatory parameters.

Table 4-5: Mandatory parameters to unmount snapshot

Parameter	Value/Details
Application	Application type, `saporacle`
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>
Snapshot name	Valid snapshot name. Provide the snapshot name to unmount a snapshot.
Snapshot set ID	Valid snapshot set ID. Provide either the snapshot name or snapshot set ID to unmount a snapshot.
User credentials	Valid username and password

For more details about unmounting snapshot parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Syntax

```
hapro snapshot unmount
```

Sample command

```
hapro snapshot unmount -s <Hostname/IP of Application
Protector Server/FQDN> -a saporacle -u <user> -P <password>
-x <snapshot name>
```

Recovering database using a snapshot

Application Protector recovers the Oracle Database in SAP environment using the selected snapshots. This section describes the command options for `BRRECOVER`. If you start `BRRECOVER` without command options, the values in the `init<SID>.sap` profile file are used.

If you use `BRRECOVER` with the command options, these override the corresponding values in the profile file.

For more details about using the options, see SAP Help Portal.

You can use the snapshot and archive files to perform complete and PIT recovery.

Complete recovery: Application Protector uses the snapshot and current archive files to perform complete recovery.

PIT recovery: Application Protector uses the snapshot and the logs until the time provided to perform PIT recovery.

NOTE: The profile file is at `$oracle home/dbs/init<SID>.sap`. You can customize the profile file as required to recover the database using the backup.

Performing point-in-time recovery

This section describes the supported command options to use BRRECOVER to perform a database PIT recovery using Application Protector. If you start BRRECOVER without command options, the values in the profile init<SID>.sap are used.

For details about setting profile, see SAP help portal.

Prerequisites to recover a snapshot

1. Activate the license for supported storage array and application.
2. Set the appropriate parameters in the init<SID>.sap profile file.
3. To perform recovery, a snapshot must be present.

To perform PIT recovery

1. Provide the following supported parameters.

Table 4-6: Supported parameters for BRRECOVER

Parameter	Value/details
backup	Backup name from which you need to restore the database. • <log_name>: Restores the database files from the BRBACKUP with the log name entered in <log_name>
device	Backup device type (Application Protector supports util_vol only).
time	PIT to recover the database until the provided time.
type	Recovery type. If you do not provide the recovery type, then by default, complete recovery is performed. For complete recovery, see Performing complete recovery.
User credentials	Valid database admin user credentials.

2. Execute the BRRECOVER function in BR*Tools by providing the PIT in the command line.
3. Provide inputs as required in the console. The operation progress appears in the console.
4. Select the snapshot you need to recover.
5. Check the results in the BRRECOVER logs. The detailed log displays the progress in the console. In addition, you can view the logs in the $Oracle_HOME/dbs/ directory.

   Syntax

   ```
   ./brrecover
   ```

   Sample command

```
./brrecover -u<user> [-p <profile file path>] -t dbpit -pit
<date/time for dbpit recovery> [-m|-pit|-time <yyyy-mo-dd
hh.mi.ss>]
```

For details to perform BRRECOVER, see SAP Help.

For more details about the supported parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Performing complete recovery

This section describes the supported command options to use `BRRECOVER` to perform complete recovery. If you start `BRRECOVER` without command options, the values in the profile `init<SID>.sap` are used.

For details about setting profile, see SAP help portal.

Prerequisites to recover a snapshot

1. Activate the license for supported storage array and application.
2. Set the appropriate parameters in the `init<SID>.sap` profile file.
3. To perform recovery, a snapshot must be present.

To perform complete recovery

1. Provide the following mandatory parameters.

Table 4-7: Mandatory parameters

Parameter	Value/Details for BRRECOVER
backup	Backup name from which you need to restore the database. • <log_name>: Restores the database files from the BRBACKUP with the log name entered in <log_name>
device	Backup device type (Application Protector supports `util_vol` only).
type	Recovery type. If you do not provide the recovery type, then by default, complete recovery is performed.
User credentials	Valid database admin user credentials.

2. Execute the `BRRECOVER` function in BR*Tools.
3. Provide inputs as required in the console. The operation progress appears in the console.
4. Select the snapshot you need to recover.
5. Check the results in the `BRRECOVER` logs. The detailed log displays the progress in the console. In addition, you can view the logs in the `$Oracle_HOME/dbs/` directory.

Syntax

```
./brrecover
```

Sample command for complete recovery

```
./brrecover -u<user> [-p <profile file path>]
```

Syntax

```
./brrecover
```

Sample command for database point-in-time recovery

```
./brrecover -u<user> [-p <profile file path>] -t dbpit -pit
<date/time for dbpit recovery> [-m|-pit|-time <yyyy-mo-dd
hh.mi.ss>]
```

For details to perform BRRECOVER, see SAP Help.

For more details about the supported parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

Restoring a snapshot

Application Protector restores the Oracle Database in the SAP environment using a selected snapshot. This section describes the command options for `BRRESTORE`. If you start `BRRESTORE` without command options, the values in the `init<SID>.sap` profile file are used.

If you use `BRRESTORE` with the command options, these override the corresponding values in the profile file.

For more details about using the options, see SAP Help Portal.

NOTE: The profile file is at `$oracle home/dbs/init<SID>.sap`. You can customize the profile file as required to recover the database using the backup.

You can use the snapshot and the log and offline redo files to perform full restore. You can use the snapshot to just restore all tablespaces using the all mode.

Prerequisites to restore a snapshot

1. Activate the license for supported storage array and application.
2. Set the appropriate parameters in the `init<SID>.sap` profile file.
3. To perform restore, a snapshot must be present. Shutdown the database before performing restore.

To perform restore

1. Provide the following mandatory parameters.

Table 4-8: Mandatory parameters

Parameter	Value/Details for BRRESTORE
backup	Snapshot name from which you need to restore the database. • <log_name>: Restores the database files from the BRBACKUP with the log name entered in <log_name>.
device	Backup device type (Application Protector supports `util_vol` only).
restore mode	full: Restores files from the complete backup, including any nondatabase files, directories, control files, online redo log files and offline redo log files.
	all: Restores files in all tablespaces, but not the control files and online redo log files.
User credentials	Valid database admin user credentials.

2. Execute the `BRRESTORE` function in BR*Tools by providing the restore mode in the command line.
3. Provide inputs as required in the console. The operation progress appears in the console.
4. Select the snapshot you need to recover.

5. Check the results in the BRRESTORE logs. The detailed log displays the progress in the console. In addition, you can view the logs in the $Oracle_HOME/dbs/ directory.

   Syntax

   ```
   ./brrestore
   ```

   Sample command

   ```
   ./brrestore -u<user> [-p <profile file path>] -m full
   ```

For details to perform BRRESTORE, see SAP Help.

For more details about the supported parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

After executing BRRESTORE, perform the following.

1. Startup the database, if there are inconsistencies in control files. Copy the correct control file at mentioned location as per the error message.
2. Shutdown database in immediate mode.
3. Startup database.
4. After startup, if following error is displayed:

   ```
   ORA-10873: file 1 needs to be either taken out of backup
   mode or media recovered
   ```

   Execute the following Oracle command for respective datafile, so that the datafile is online:

   ```
   alter database datafile "<datafile with full path>" online
   ```

5. Execute the following Oracle command and specify “AUTO” logs:
   ```
   recover database using backup controlfile until cancel
   ```
6. Execute the following Oracle command:

   ```
   alter database open resetlogs
   ```

7. Database status is now 'Open'.

5

Managing logs

Application Protector generates logs for each operation executed in the server. The logs help in identifying issues when a particular operation fails.

In addition, a common log is generated which logs information about requests of non-snapshotable operations such as listing operations, register service account, and storage in a specific format. The logs include information such as timestamp and details of the operation performed.

This chapter describes the following topics:

Listing the operations

You can view the status and other information of the synchronous and asynchronous operations. You can list the operations by using the Application Protector CLI.

Prerequisites to list the operations

- Activate the license for the supported storage array and application.

To view the operations

- Execute the `hapro admin listoperations` command and provide the following mandatory parameters.

Table 5-1: Mandatory parameters for listing operations

Parameter	Value
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN/ Valid port number (optional)>.
User credentials	Valid username and password.

For more details about listing operations parameters and details, see *Hitachi Application Protector CLI Guide for SAP*®.

Syntax

```
hapro admin listoperations
```

Sample command

```
hapro admin listoperations --server <Hostname / FQDN / IP of HAPRO server> -u <user> -P <password> -a saporacle
```

NOTE:

- To view the complete data for a particular column, use the `Enable long listing` flag in the command.
- The fields that are not provided by the user, are marked with "-" in the output.

Deleting the operations

You can delete the operations by using the Application Protector CLI. You can delete multiple operations.

Prerequisites to delete the operations

1. Activate the license for the supported storage array and application.
2. List the operations to get the operations ID to delete.

To delete the operations

- Execute the `hapro admin deleteoperation` command and provide the following mandatory parameters.

Table 5-2: Mandatory parameters for deleting operations

Parameter	Value
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.
Operation ID(s)	Valid operation ID to delete. Multiple comma separated values are allowed to delete multiple operations.

For more details about deleting operations parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Syntax

```
hapro admin deleteoperation
```

Sample command

```
hapro admin deleteoperation -i <operation
ID1>,<operation ID2> -s <Hostname / FQDN / IP of HAPRO
server> -a saporacle -u <user> -P <password>
```

Listing the operation log details

Application Protector creates separate log file for each operation for which request is submitted to the Application Protector Server. You can view the details of each operation log. Depending on the log level that you have set, you can view the details such as fatal, error, warning logs. For details to configure the server and client log levels, see

Configuring the Application Protector Server and Client.

Prerequisites to list the operation log details

1. Activate the license for the supported storage array and application.
2. List the operations to get the operations ID to list the details.

To list the operation log details

- Execute the `hapro admin listlog` command and provide the following mandatory parameters.

Table 5-3: Mandatory parameters for viewing operation log details

Parameter	Value
Application	Application type, `saporacle`.
Host name	Valid <Hostname/ IP of Application Protector Server/ FQDN>.
User credentials	Valid username and password.

For more details about deleting operations parameters and details, see *Hitachi Application Protector CLI Guide for SAP®*.

Syntax

```
hapro admin listlog
```

Sample command

```
hapro admin listlog -s <Hostname / FQDN / IP of HAPRO
server> -u <user> -P <password> -a saporacle -C 10 -l
```

NOTE:

- To view the complete data for a particular column, use the `Enable long listing` flag in the command.
- The fields that are not provided by the user, are marked with "-" in the output.

Listing the Application Protector logs

This section provides information regarding listing the Application Protector server, client, and operations logs.

Application Protector Server log

Application Protector generates a common server log for logging and synchronization operations. The name of the Application Protector Server log is `HAPROserver.log`.

If the log size exceeds 20MB, then the older log is rotated and renamed to `HAPROserver.log.1` and so on.

By default, the Application Protector Server logs are present in the `/opt/Hitachi/HAPRO/server/logs` directory. To configure the location, see

Configuring the log directory path.

Application Protector Client log

Application Protector generates a common client log for Application Protector client requests. The name of the Application Protector Client log is `HAPROclient.log`.

If the log size exceeds 20MB, then the older log is rotated and renamed to `HAPROclient.log.1` and so on.

The Application Protector Client logs are present in the `/opt/Hitachi/HAPRO/client/logs` directory.

Application Protector operation log

Application Protector creates separate log file in the `OpLog_<unique_id>.log` format for all the Application Protector operations, where `OpLog_<unique_id>` is the operation log ID.

The Application Protector operation logs are present in the `/opt/Hitachi/HAPRO/server/logs` directory.

Listing events

Application Protector supports event logging for the performed operations. The system logs are generated in the `/var/log/messages` directory.

Default log paths

The default log paths for client and server logs is as follows.

Table 5-4: Default log paths

Field	Path
Application Protector Client log directory path	/opt/Hitachi/HAPRO/client/logs
Application Protector Server logs	/opt/Hitachi/HAPRO/server/logs
Event notifications	/var/log/messages

HAPRO dump

Debugging support is provided using the `HAPRO dump` utility. `HAPRO_dump` is a shell script utility, used to gather the Application Protector metadata and logs into a single .tar file.

The format of the file is `HAPRO_dump-<yyyy_mm_dd_HH_mm_ss>.tar`. For example, `HAPRO_dump-2014_05_27_23_59_30.tar.gz`.

Prior to executing `HAPRO_dump`, set the `$Oracle_HOME` path. Execute the script file from the `/opt/Hitachi/HAPRO/server/util` directory.

For more details about using HAPRO dump, see *Hitachi Application Protector CLI Guide for SAP®*.

Appendix

This appendix provides the maximum snapshot limit for supported storages and way to configure the Application Protector metadata on a separate LUN.

This chapter describes the following topics:

- Snapshot limit for supported storage
- Configuring the Application Protector metadata on a separate LUN
- HAPRO sync

Snapshot limit for supported storage

You can create the following number of maximum snapshots for the supported storage arrays.

Table A-1: Snapshot limit

Storage	Snapshot type	Snapshot retention limit
HUS	HTI	1024
	ShadowImage	7
VSP	ShadowImage	3
	HTI	1024
HNAS	TreeClone	1024

Configuring the Application Protector metadata on a separate LUN

It is recommended to create a dedicated storage volume to store the Application Protector metadata. The LUN size depends on the size of database and number of snapshots being handled. The Application Protector metadata stores following:

- Information about snapshot
- Oracle backup metadata
- Application Protector logs
- Scripts registered with Application Protector

Following are the steps to configure storage for the Application Protector metadata:

1. Create a storage volume.
2. Create a posix compliant file system (e.g. ext3) on the storage volume.
3. Mount the volume, which will be used by Application Protector for accessing metadata files.
4. Configure Application Protector metadata path to the newly created path using the Application Protector GUI or Application Protector CLI.

Application Protector will move the existing files to the newly configured path and continue from the new path.

HAPRO sync

The HAPRO_sync utility is used to fix inconsistency caused in the Application Protector metadata, such as snapshot set, snapshot database reference count, and schedule information. This utility works on the Application Protector Server. Execute the utility from `/opt/Hitachi/HAPRO/server/bin`.

Snapshot Set: Fix inconsistencies related to snapshot records in the cache.The `HAPRO_sync -s cache` operation fixes metadata cache snapshots with reference to actual system/storage status of snapshots.

Schedule: Fix inconsistencies related to schedule. Not applicable for Application Protector for SAP.

Snapshot database: Fix inconsistencies in the snapshot database reference counts of snapshot objects.

Replicate: Replicate cache metadata and logs to a user specified path.

Check: Checks if the process related to any Application Protector operation is hung/not in running state. `HAPRO_sync` will change the status of such operations as 'FAILED' (update in operation cache metadata).

NOTE: `HAPRO_sync` synchronizes the Application Protector metadata cache and not the configuration files.

Table A-2: HAPRO sync parameter description

Parameter	Description
`-help|-h`	Displays command line help.
`-ownership|-o`	This option provides Application Protector metadata ownership to the machine running HAPRO_sync.
`-sync|-s {system}`	To sync the system using cache metadata.
`-sync|-s {cache}`	To sync cache metadata using system state.
`-check|-c`	To perform normal HAPRO_sync consistency check. This is the default action taken if no option is given.
`-replicate|-r "<from>[,<to>]"`	To perform replication of metadata, logs, etc from the path provided in `from` to the destination in the `to` parameter. You can use the `replicate` parameter to backup the Application Protector metadata.

For more details about executing HAPRO_sync, see *Hitachi Application Protector CLI Guide for SAP®.*

Glossary

This glossary provides definitions of general storage networking terms as well as specific terms related to the technology that supports your Hitachi Storage System. Click the letter of the glossary section to display that page.

A

Array

A set of hard disks grouped logically together to function as one contiguous storage space.

Application Protector

Hitachi Application Protector

ASM

Automatic Storage Management

B

BRBACKUP

SAP® BR*Tools uses BRBACKUP to create database backups.

BRRECOVER

SAP® BR*Tools uses BRRECOVER to recover the database using the selected snapshot.

BRRESTORE

SAP® BR*Tools uses BRRESTORE to restore the database using the snapshot.

C

CCI

Command control interface

Complete recovery

Complete recovery involves using redo data or incremental backups combined with a backup of database, tablespace, or datafile to update it to the current point-in-time. The recovery is called complete recovery because all redo changes contained in the archived and online logs are overwritten completely. Complete recovery is generally performed after a control file or data file damage.

CLI

Command line interface

D

DM multipath

Device mapper multipath

F

FQDN

Fully qualified domain name

Full copy

Full copy (ShadowImage snapshot) type of snapshots backup complete database and enable restoring the data without referring to any other snapshot copies. A complete copy of the original database is created using full copy snapshot technology that can be replicated to other sites or backed up.

G

Gbps

Gigabit per second.

GUI

Graphical user interface

H

HAPRO

Hitachi Application Protector

HDD

Hard disk drive.

HNAS

Hitachi Network Attached Storage.

HTI

Hitachi ThinImage

HUS

Hitachi Unified Storage. Currently, Application Protector supports the DF 850 array.

I

I/O

Input/output.

Inquire

The Application Protector `BACKINT` adapter uses this command to list the snapshots.

L

LAN

Local Area Network, a computer network that spans a relatively small area, such as a single building or group of buildings.

LU

Logical unit.

LUN

Logical unit number.

LVM

Logical volume manager.

O

Oracle® Database

In this document, refer Oracle Database as Oracle® Database in SAP® environment.

P

PSUS

Pair suspended

P-VOL

A volume that consists of a production volume containing the original data is called the primary volume (P-VOL).

R

RAID

Redundant Array of Independent Disks, a disk array in which part of the physical storage capacity is used to store redundant information about user data stored on the remainder of the storage capacity. The redundant information enables regeneration of user data in the event that one of the array's member disks or the access path to it fails. SNIA.

Recovery

Recovery is the process of copying data from the backup or the snapshot data and then applying logs to roll forward the recovered database up to the point of failure or to any point-in-time. Recovery can be performed on the host that has the current active database and has access to the snapshot volumes.

RHEL

Red Hat® Enterprise Linux®.

S

ShadowImage

ShadowImage (SI) snapshot type of snapshots backup complete database and enable restoring the data without referring to any other snapshot copies. A complete copy of the original database is created using ShadowImage snapshot technology that can be replicated to other sites or backed up.

SCSI

Small Computer System Interface, a parallel interface standard that provides faster data transmission rates than standard serial and parallel ports.

Snapshot

Snapshot is a point-in-time copy of the data of the application database. The data files, control files, and archive log files are backedup while creating a snapshot.

SLES

SUSE® Linux Enterprise Server

S-VOL

Secondary volume contains copies of P-VOL.

T

Target

Devices that receive iSCSI requests that originate from an iSCSI initiator.

V

VSP

Virtual Storage Platform

V-VOL

Virtual volume contains virtual copies on the P-VOL. For HUS storage array, refer the V-VOL as DP-Volume.

Index

T

W

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street, Santa Clara,
California 95050-2629, U.S.A.
www.hds.com

Regional Contact Information

Americas
+1 408 970 1000
info@hds.com

Europe, Middle East, and Africa
+44 (0)1753 618000
info.emea@hds.com

Asia Pacific
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-91HAP016-00