HITACHI
Inspire the Next

Hitachi Application Protector Quick Install & Configuration Guide for SAP®

FastFind Links

Hitachi Data Systems

MK-91HAP018-00

Contents

Preface

This document guides you with the details to install Hitachi Application Protector (Application Protector) for SAP® on Linux® and Solaris® platform.

The preface describes the following topics:

- Intended audience
- Product version
- Document revision level
- 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 installing, configuring, and using Application Protector. Readers of this document should be familiar with the following concepts:

- Oracle® Database 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 v1.2 release.

Document revision level

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

Revision	Date	Description
MK-91HAP018-00	July 2014	Initial release

Related documents

- *Hitachi Application Protector CLI Guide for SAP®,* MK-91HAP024
- *Hitachi Application Protector User Guide for SAP®,* MK-91HAP016
- *Hitachi Application Protector Troubleshooting Guide for SAP®,* FE-91HAP020

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 title	Description
Chapter 1, Introduction	This chapter provides an introduction, supported databases and storage subsystems, database server configuration, and prerequisites of Application Protector.
Chapter 2, Installing Application Protector	This chapter provides the details of installing and removing Application Protector Server and Client.
Chapter 3, Configuring Application Protector	This chapter provides information about mandatory configuration (first time) after installing Application Protector.
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 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]

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 for v1.2 release.
x	Features not functional or are not available in Hitachi Application Protector for v1.2 release.
Not Supported	Features not supported by Hitachi Application Protector for v1.2 release.

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 (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 or a remote server on the same network or accessible to the Application Protector Server.

This chapter describes the following topics:

Application Protector overview

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

- Register the supported storage arrays.
- Create ShadowImage® (SI), Tree Clone, and Hitachi Thin Image (HTI) snapshots at volume level.
- Create, list, mount, unmount, and delete snapshots.
- Recover and restore database from the snapshot at volume level.
- Set policy to configure snapshot retention count at server level.
- Native Device-Mapper Multipath environment for Red Hat® Enterprise Linux® (RHEL) and SUSE® Linux Enterprise Server (SLES) platform.
- Protect databases hosted on the logical volume manager (LVM2) devices for SLES platform.

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)

Configuring Oracle Database

This section provides details to configure Oracle Database for various setups:

- Configuring non-ASM Oracle Database with LVM devices
- Configuring non-ASM Oracle Database with multipath devices

Configuring non-ASM Oracle Database with LVM devices

This section provides the mandatory details required while configuring non-ASM Oracle Database with the LVM devices for RHEL and SLES platforms.

1. Create physical volumes (PVs) using any of the following type of devices:
   a. SCSI Block Device. For example: `/dev/sdx`.
   b. SCSI Block Device Partition. For example: `/dev/sdx1`.

NOTE: The physical device and multipath device can have only one partition.

   c. Multipath device or partition. For details, see Configuring non-ASM Oracle Database with multipath devices.
2. A PV must be a part of a single volume group (VG) only.
3. Create only one logical volume (LV) for each VG.
4. The LV must not have any partitions (the ext3 filesystem must be created directly on the LV).
5. The DATA, REDO, and ARCHIVE files must reside on different LVs. For example, DATA on LV1 and VG1 and REDO on LV2 and VG2.

Configuring non-ASM Oracle Database with multipath devices

For RHEL platform, when configuring the non-ASM Oracle Database with multipath devices, the following variations of multipath device configurations are supported:

1. A multipath device is mounted using any of the following representations:
   a. WWID of the multipath device. For example: '`/dev/mapper/<wwid>`'.
   b. Friendly name for a multipath device, obtained by making an entry in the multipath configuration file (`/etc/multipath.conf`). For example: '`/dev/mapper/mpatha`'.
   c. Alias defined for a multipath device by making of an entry in the multipath configuration file (`/etc/multipath.conf`). For example: '`/dev/mapper/AliasName`').
2. A single partition created on a multipath device is mounted using any of the following representations:
   a. WWID of the multipath device partition. For example: '`/dev/mapper/<wwid>_part1`'.

b. Friendly name for the multipath device partition, obtained by making an entry in the multipath configuration file (`/etc/multipath.conf`). For example: '`/dev/mapper/mpatha_part1`'.

c. Alias defined for the multipath device partition by making an entry in the multipath configuration file (`/etc/multipath.conf`). For example: '`/dev/mapper/AliasName_part1`'.

WARNING! Mounting the PVs as physical devices with the multipath daemon service in the running state and blacklisting the devices by adding an entry in the multipath configuration file (`/etc/multipath.conf`), will result in failure to mount snapshots. To use physical device names (example: '`/dev/sdx`'), stop the multipath daemon service.

NOTE: DATA, REDO, and ARCHIVE files for non-ASM Oracle Database must be stored on devices of the same configuration. For example, if DATA files are stored on a multipath device with one partition, then ARCHIVE and REDO files must also be stored on multipath devices with one partition each.

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)	Tree Clone 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)

Storage prerequisites

This section provides the details of the storage prerequisites you must set to use Application Protector. For details about supported storage prerequisites, see the following.

- ❒ VSP storage prerequisites
- ❒ HUS storage prerequisites
- ❒ Application Protector prerequisites

VSP storage prerequisites

Set the following storage prerequisites to use Application Protector for VSP storage.

- Configure the RAID Manager (HORCM instance) prior to the Application Protector server configuration and storage registration. For details about CCI configuration, see

  Installing and configuring the command control interface.
- Create a staging hostgroup with the name, `HITACHI-HAPRO-HG` on the VSP storage to stage the V-VOLs created by Application Protector. It is recommended that no hosts are added to this host group.

NOTE:

- World Wide Name (WWN)s belonging to any of the host machines using Application Protector must not be a part of this host group.
- In a multipath setup, the P-VOL on which the SAP database is hosted should have at least one partition.
- The verbosity of the multipath daemon should not be changed by editing the multipath configuration file (`/etc/multipath.conf`). User the default value (2).

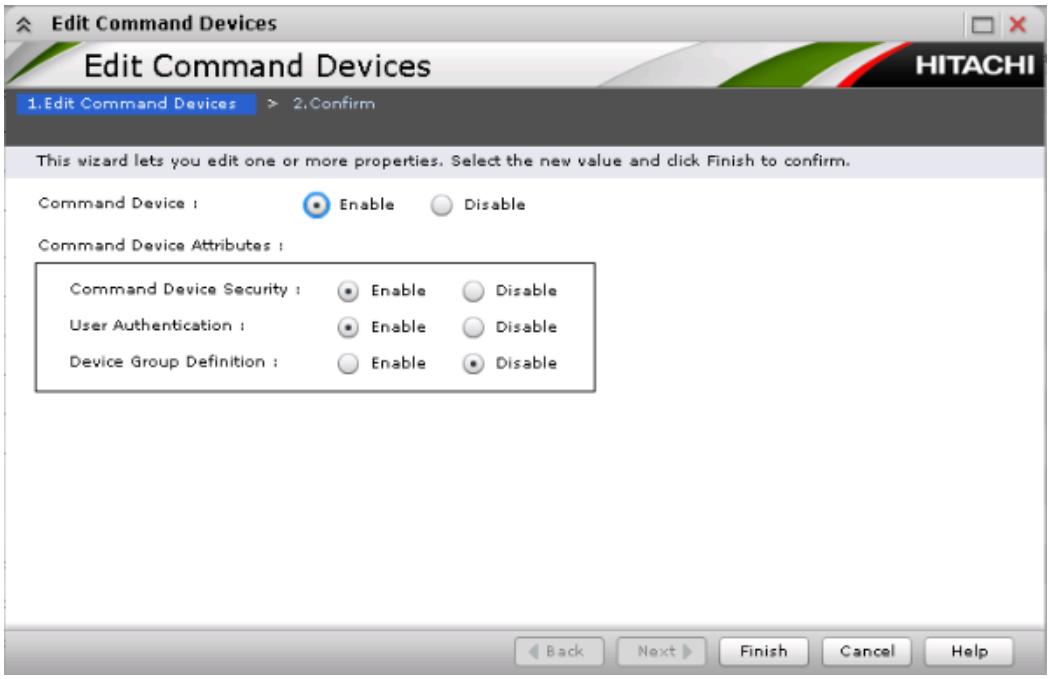
Installing and configuring the command control interface

This section provides the details to install and configure the command control interface (CCI).

Configuring the command device

Use the Hitachi Storage Navigator to configure the Command Device (CMD). Refer the following screenshot to set the CMD attributes.

Figure 1-1: Configure command device



NOTE: In the preceding figure, **Enable** the User Authentication.

Configuring the command control interface

The CCI HORCM instance must be configured on the host server. Brief instructions for configuring the CCI on a Linux server follows.

For detailed instructions, see the *Hitachi Command Control Interface Installation and Configuration Guide*.

Configuring CCI on a Linux server

1. Confirm the CCI version:

   ```
   # raidqry -h
   Model : RAID-Manager/Linux
   Ver&Rev: 01-29-03/06
   ```

2. In the `/etc` folder, create or link to an instance configuration file for a subsystem. The configuration file must be named as `horcm<instance number>.conf`. For example, the configuration file `/etc/horcm0.conf` is for the instance 0.
3. Edit the configuration file as follows:

   ```
   HORCM_CMD
   #dev_name
   ```

```
/dev/sdf #VSP 66033
/dev/sde #VSP 66034
```

4. Start an instance by executing horcmstart.sh <horcm instance number>:

```
>horcmstart.sh 0
confirm the instance working:
#raidcom get command_status -I0 –s 66033 -login <uid>
<password>

 HANDLE   SSB1    SSB2    ERR_CNT  Serial#    Description
 00c9     -       -       0        66033      -

#raidcom get command_status -I0 –s 66034 -login <uid>
<password>

 HANDLE   SSB1    SSB2    ERR_CNT  Serial#    Description
 00c4     -       -       0        66034      -
```

For more details about command line options, see the following guide.

http://www.hds.com/assets/pdf/cci-user-and-reference-guide.pdf

HUS storage prerequisites

Set the following storage prerequisites to use Application Protector for HUS storage on RHEL setup.

1. Enable the iSCSI target security on the port on which Application Protector server is connected. The iSCSI host initiator name of the machine hosting the Application Protector server must be a part of the iSCSI target that contains the P-VOLs hosting the Oracle database.
2. To create Full Copy (ShadowImage) snapshots using Application Protector, create a pair relationship of P-VOL and S-VOL prior to creating a snapshot.

Application Protector prerequisites

This section provides the details of Application Protector system requirements, Application Protector Server and Client prerequisites.

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. For more details about the prerequisites, see

Application Protector Server prerequisites.

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 11 and Solaris 11 (x86)
Networking	Gigabit Ethernet recommended
Application software	SAP® ECC 6.0 (ERP) BR*Tools version 7.20 patch level 18 or higher
	For SLES setup: Oracle® Database 11g Release 2 (11.2.0.3 and 11.2.0.4) (non-ASM)
	For RHEL setup: Oracle® Database 11g Release2 (11.2.0.3 and 11.2.0.4) (non-ASM)
	For Solaris setup: Oracle® Database 11g Release2 (11.2.0.3 and 11.2.0.4) (non-ASM)

Application Protector Server prerequisites

After you have installed and configured Oracle Database, install Application Protector Server. For details about Application Protector Server prerequisites for supported operating system, see the following.

- Application Protector Server for SLES platform
- Application Protector Server for RHEL platform
- Application Protector Server for Solaris platform

Application Protector Server for SLES platform

The following table provides the Application Protector Server prerequisites for SLES platform.

Table 1-5: Application Protector Server prerequisites

Software version	Package/RPM	Details
SLES 11 SP3	-	32/64-bit operating system supported
SAP® ECC 6.0 (ERP) with Oracle® Database 11gR2 (11.2.0.3 and 11.2.0.4)	-	Oracle database on non-ASM configuration is supported.
SBLIM SFCB	sblim-sfcb 32 bit[1]	For both 32/64-bit operating system. For 64-bit, comment out the following line: `preload_pam_misc_soin "/etc/init.d/sfcb”`
Parted	parted-2.3-10.38.16	Shipped with the operating system install media and used to detect partitions on the device.
CCI RAID-Manager/Linux version 01-29-03/06	-	Storage prerequisite

1. On installing sblim-sfcb 32-bit manually, you must install the cim-schema. Application Protector user must be in the sfcb user group.

```
# usermod -A sfcb <HAPRO-user>
```

NOTE: Install and configure Oracle database in SAP environment prior to SAP® BR*Tools GUI or CLI execution.

Application Protector Server for RHEL platform

The following table provides the Application Protector Server prerequisites for RHEL platform.

Table 1-6: Application Protector Server prerequisites

Software version	Package/RPM	Details
RHEL 6.3	-	32/64-bit operating system supported.
OpenSSL 0.9.8e	-	Required for secure communication with the client.
SAP® ECC 6.0 (ERP) with Oracle® 11gR2 version 11.2.0.3/4	-	Supported Oracle Database.
Open Pegasus	tog-pegasus	Install 32-bit RPM in 64-bit operating system that is shipped with the system install media.[1]
Parted 2.1	parted 2.1	Shipped with the operating system install media and used to detect partitions on the device.
CCI RAID-Manager/Linux version 01-29-03/06	-	For VSP only.

1. Do not install 64-bit RPM.

After you install and configure Oracle Database, install the prerequisites mentioned in Table 1-6, and perform the following tasks prior to installing the Application Protector Server.

1. HAPRO user must be in the Pegasus user group:

   `usermode -aG pegasus <HAPRO-user>`

2. Create a pair relationship of S-VOL and P-VOL prior to creating snapshot for the VSP or HUS full copy type of snapshots. You must add this S-VOL to the staging host group. Best practice suggests to add it to the `HITACHI-HAPRO-HG` host group that does not contain any host WWNs. After creating a new pair, split the pair to avoid revert failure.
3. Download the DMTF schema 2.9.0 from

   http://dmtf.org/standards/cim/cim_schema_v29/CIM_V2.9.0Final-MOFs.zip.
4. Install `libcurl-7.19.7-26.el6_2.4.i686.rpm`.
5. Install `OpenSSL - 0.9.8e`.
6. Install the following:
   - For RHEL 6.3, install `parted-2.3-10.38.16`
   - For RHEL 5.7, install `parted-1.8.1-28.el5`
7. Install and configure Oracle Database in SAP environment prior to SAP® BR*Tools GUI or CLI execution.

Application Protector Server for Solaris platform

The following table provides the Application Protector Server prerequisites for Solaris platform.

Table 1-7: Application Protector Server prerequisites

Software version	Package/RPM	Details
• Solaris 10 Update 11 • Solaris 11 (x86)	-	32/64-bit operating system supported.
SAP® ECC 6.0 (ERP) with Oracle® Database 11gR2 (11.2.0.3 and 11.2.0.4)	-	Non-ASM configuration Oracle database is supported.

NOTE: On Application Protector Server installation, the root user is added to the `hapro` user group. To add more users, add them to the `hapro` user group to perform Application Protector operations.

Application Protector Client prerequisites

This section provides the details prerequisites required prior to installing the Application Protector Client. For details about Application Protector Client prerequisites for supported operating system, see the following.

- Application Protector Client for SLES platform
- Application Protector Client for RHEL platform
- Application Protector Client for Solaris platform

Application Protector Client for SLES platform

Perform the following tasks prior to installing the Application Protector Client.

Table 1-8: Application Protector Client prerequisites

Software version	Package/RPM	Details
SLES 11 SP3	-	32-bit and 64-bit operating system supported
Oracle Java JRE 1.6+	JRE 1.6	For 32/64-bit operating system
SBLIM CIM Client	sblim-cim-client2	For 32-bit and 64-bit operating system
Log4j	log4j	For 32-bit and 64-bit operating system

Application Protector Client for RHEL platform

Perform the following tasks prior to installing the Application Protector Client.

Table 1-9: Application Protector Client prerequisites

Software version	Package/RPM	Details
RHEL 6.3	-	32-bit and 64-bit operating system supported
Oracle Java JRE 1.6+	JRE 1.6	For 32/64-bit operating system
SBLIM CIM Client	sblim-cim-client	For 32-bit and 64-bit operating system
Log4j	log4j	For 32-bit and 64-bit operating system

Application Protector Client for Solaris platform

Perform the following tasks prior to installing the Application Protector Client.

Table 1-10: Application Protector Client prerequisites

Software version	Package/RPM	Details
• Solaris 10 Update 11 • Solaris 11 (x86)	-	32/64-bit operating system
Log4j	CSWlog4j	For 32-bit and 64-bit operating system
Oracle Java JRE 1.6+	JRE 1.6	For 32/64-bit operating system

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.

2

Installing Application Protector

This chapter guides you through the installation and removal of the Application Protector Server and Client.

This chapter describes the following topics:

- Installing the Application Protector Server
- Installing the Application Protector Client
- Removing the Application Protector Server
- Removing the Application Protector Client

Installing the Application Protector Server

The Application Protector Server self-extracting installer is distributed in shell script (.sh) file format. Application Protector is a 32-bit application that is installed on both 32-bit and 64-bit systems.

You must accept the end user license agreement and then perform actions based on the command and option provided.

NOTE:

- Make sure **/var/tmp** directory has more than 1GB of free space.
- It is preferred that the `ORACLE_HOME` and `ORACLE_SID` environment variables are set prior to Application Protector installation. This will enable post-configuration wizard to detect the default values for SID and database-backup user.

The following table provides the details of the supported platform and installers.

Table 2-1: Supported platform and installers

Platform	Application Protector Server	Application Protector Client
Solaris	HAPRO-SAP-Server-<v1.2.0.x>-Solaris-<10/11>-x86.sh	HAPRO-Client-<v1.2.0.x>-Solaris-<10/11>-x86.sh
RHEL	HAPROSetup_Server_x86_RHEL.sh	HAPROSetup_Client_noarch_RHEL.sh
SLES	HAPROSetup_Server_x86_SLES.sh	HAPROSetup_Client_noarch_SLES.sh

To install and configure the Application Protector Server

1. Extract the installer as follows.

   tar –xzvf HAPROInstaller.tar

2. The **HAPROInstaller** directory contains the **<HAPRO Server[1]>.sh** installer script. Use the following commands to install the Application Protector Server for the supported platforms.

   ./HAPROSetup_Server_x86_SLES.sh -t <Block (VSP/HUS)/ HNAS>*[2] install

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

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

3. Accept **End User License Agreement (EULA)** to proceed with the installation.
4. On successful installation, to configure Application Protector for SID, enter **y**; else to configure the path later; enter **n**. To configure the path later, see Configure HAPRO-SAP for Oracle SID.
5. Provide the Oracle database SID.

1. <HAPRO Server> refers to the Application Protector Server installer for supported platform.
2. "*" indicates: Provide "HNAS" for HNAS storage, else provide "Block (VSP/HUS)" for other storages.

6. Provide the executable path of the BR*Tools utilities for SID. SID is now configured to use the **HAPRO-SAP** `BACKINT` interface.

On installing the Application Protector Server successfully, the executable files are copied to the /**opt/Hitachi/HAPRO/server/bin** directory.

Configure HAPRO-SAP for Oracle SID

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

Syntax

```
HAPRO_SAP_configuration_wizard.sh <configuresid |
configureuser | unconfigure>
```

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

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

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

Application Protector Server installer syntax

The following table provides the command and parameter details of the Application Protector Server installer.

Syntax

./<HAPRO Server>.sh <command> <parameter>

Table 2-2: Command and parameter description

Command	Parameter[1]	Description
• ./HAPROSetup_Server_x86_SLES.sh -t <Block (VSP/HUS)/HNAS> install • ./HAPROSetup_Server_x86_RHEL.sh -t <Block (VSP/HUS)/HNAS> install • ./HAPRO-SAP-Server-<v1.2.0.x>-Solaris-<10/11>-x86.sh install	`--accept_eula| -e`	Installs the Application Protector Server without user confirmation.
	`--help| -h`	Displays the help.
• ./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	`--silent| -s`	Uninstall without user confirmation.
	`--complete| -c`	Removes Application Protector Server and removes metadata and all logs.
	`--help| -h`	Displays the help.
• ./HAPROSetup_Server_x86_SLES.sh version • ./HAPROSetup_Server_x86_RHEL.sh version • ./HAPRO-SAP-Server_<v1.2.0.x>-Solaris-<10/11>-x86.sh version	Not required	Displays version of the installed Application Protector Server.
• ./HAPROSetup_Server_x86_SLES.sh help • ./HAPROSetup_Server_x86_RHEL.sh help • ./HAPRO-SAP-Server_<v1.2.0.x>-Solaris-<10/11>-x86.sh help	Not required	Prints help.
• ./HAPROSetup_Server_x86_SLES.sh update • ./HAPROSetup_Server_x86_RHEL.sh update • ./HAPRO-SAP-Server_<v1.2.0.x>-Solaris-<10/11>-x86.sh update	Not required	Updates to newer version or newer release.

1.Application Protector Server installer parameters are optional.

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

Application Protector Server installer help

```
./HAPRO-SAP-Server-v1.2.0.2-Solaris-10-x86.sh help

usage: HAPRO-SAP-Server-v1.2.0.24-Solaris-10-x86.sh
[COMMAND] [OPTION]

COMMAND: install: Install HAPRO Server.

    usage: HAPRO-SAP-Server-v1.2.0.24-Solaris-10-x86.sh
install [OPTION]

    OPTIONs:-

        -h|--help: Display install help.

        -e|--accept_eula: Auto-accept the End User License
Agreement.

COMMAND: uninstall: Uninstall HAPRO Server.

    usage: HAPRO-SAP-Server-v1.2.0.24-Solaris-10-x86.sh
uninstall [OPTION]

    OPTIONs:-

        -h|--help: Display uninstall help.

        -s|--silent: Do not ask for confirmation.

        -c|--complete: Remove metadata and logs.

COMMAND: update: Update/Repair HAPRO Server.

    usage: HAPRO-SAP-Server-v1.2.0.24-Solaris-10-x86.sh
update [OPTION]

    OPTIONs:-

        -h|--help: Display update help.

COMMAND: version: Display installed HAPRO Server version.

    usage: HAPRO-SAP-Server-v1.2.0.24-Solaris-10-x86.sh
version [OPTION]

    OPTIONs:-

        -h|--help: Display version help.

COMMAND: help: Display this help.
```

Installing the Application Protector Client

The Application Protector Client self-extracting installer is distributed in shell script (.sh) file format. You need to accept the end user license agreement and then perform actions based on the command and option provided.

NOTE: Make sure the **/var/tmp** directory has more than 1GB of free space.

To install the Application Protector Client

1. Extract the installer as follows.

   tar –xzvf HAPROInstaller.tar

2. The **HAPROInstaller** directory contains the **<HAPRO Client**[1]**>.sh** installer scripts. For Application Protector server and client installer names, see Supported platform and installers. Use the following command to install the Application Protector Client for the supported platform:

   ./HAPROSetup_Client_noarch_SLES.sh install

   ./HAPROSetup_Client_noarch_SLES.sh install

   ./HAPRO-Client-v1.2.0.3-Solaris-11-x86.sh install

3. Accept **End User License Agreement (EULA)** to proceed with the installation.

On successful installation of Application Protector Client, the executable files are copied in the following directories:

- Executable files are copied into the **/opt/Hitachi/HAPRO/client/bin** directory.
- Logs are generated in the **/opt/Hitachi/HAPRO/client/logs** directory.

1. <HAPRO Client> refers to the Application Protector Client installer for the supported platform.

Application Protector Client installer syntax

The following table provides the command and parameter details of the Application Protector Client installer.

Syntax

./HAPROSetup_Client_noarch_SLES.sh <command> <parameter>

Table 2-3: Command and parameter description

Command	Parameter[1]	Description
• ./HAPROSetup_Client_noarch_SLES.sh install • ./HAPROSetup_Client_noarch_RHEL.sh install • ./HAPRO-Client-<v1.2.0.x>-Solaris-<10/11>-x86.sh install	`--accept_eula| -e`	Installs the Application Protector Client without user confirmation.
	`--help| -h`	Displays help.
• ./HAPROSetup_Client_noarch_RHEL.sh uninstall • ./HAPROSetup_Client_noarch_SLES.sh uninstall • ./HAPRO-Client-<v1.2.0.x>-Solaris-<10/11>-x86.sh uninstall	`--silent| -s`	Uninstall without user confirmation.
	`--help| -h`	Shows the Application Protector Client help.
• ./HAPROSetup_Client_noarch_SLES.sh version • ./HAPROSetup_Client_noarch_RHEL.sh version • ./HAPRO-Client-<v1.2.0.x>-Solaris-<10/11>-x86.sh version	Not required	Displays version of the installed Application Protector Client.
• ./HAPROSetup_Client_noarch_SLES.sh help • ./HAPROSetup_Client_noarch_RHEL.sh help • ./HAPRO-Client-<v1.2.0.x>-Solaris-<10/11>-x86.sh help	Not required	Prints help message.
• ./HAPROSetup_Client_noarch_SLES.sh update • ./HAPROSetup_Client_noarch_RHEL.sh update • ./HAPRO-Client-<v1.2.0.x>-Solaris-<10/11>-x86.sh update	Not required	Updates to newer version or repair the corrupt files or directories.

1.Application Protector Client installer parameters are optional.

Application Protector Client installer help

```
./HAPRO-Client-v1.2.0.2-Solaris-10-x86.sh help

usage: HAPRO-Client-v1.2.0.2-Solaris-10-x86.sh [COMMAND]
[OPTION]

COMMAND: install: Install HAPRO Client.

    usage: HAPRO-Client-v1.2.0.2-Solaris-10-x86.sh install
[OPTION]

    OPTIONs:-

        -h|--help: Display install help.

        -e|--accept_eula: Auto-accept the End User License
Agreement.

COMMAND: uninstall: Uninstall HAPRO Client.

   usage: HAPRO-Client-v1.2.0.2-Solaris-10-x86.sh uninstall
[OPTION]

    OPTIONs:-

        -h|--help: Display uninstall help.

        -s|--silent: Do not ask for confirmation.

COMMAND: update: Update/Repair HAPRO Client.

    usage: HAPRO-Client-v1.2.0.2-Solaris-10-x86.sh update
[OPTION]

    OPTIONs:-

        -h|--help: Display update help.

COMMAND: version: Display installed HAPRO Client version.

    usage: HAPRO-Client-v1.2.0.2-Solaris-10-x86.sh version
[OPTION]

    OPTIONs:-

        -h|--help: Display version help.

COMMAND: help: Display this help.
```

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

NOTE: The `-s | --silent` option uninstalls Application Protector without user confirmation, else you are prompted to provide the input to uninstall Application Protector Server.

WARNING! The `--complete` option removes 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

./<HAPRO Client>.sh uninstall -s

NOTE: The `-s | --silent` option uninstalls Application Protector without user confirmation, else you are prompted to provide the input to uninstall Application Protector Client.

3

Configuring Application Protector

This chapter guides you to activate license for Application Protector. It also provides an overview of the settings that you must perform prior to using Application Protector for snapshot management activities.

This chapter describes the following topics:

- Licensing for Application Protector
- Configuring Application Protector

Licensing for 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: For Solaris operating system, the license is activated on installation. You must generate and activate the Application Protector license for SLES and RHEL setups only.

The Application Protector license must be activated to use the snapshot-based backup and recovery features for the supported storage array and application.

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.

The following command generates a license request for the specified user for the specified server.

To generate the license request

- In the <`/opt/Hitachi/HAPRO/client/bin`> directory, execute the `hapro admin generatelicenserequest` command and provide the following mandatory parameters.

Table 3-1: Mandatory parameters

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.
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.
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 <domain-name.com> -f <first name> -L <last name>
-i <activation ID> -C <company> -c <country> -x /
<Response_SAP_VSP_LastOctetOfIP.xml>
```

Output

```
[I720308D] License request generated successfully.
```

Activating the Application Protector license

Application Protector is available with the following license types:

- Trial License (30 days)
- Production License

You need to 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.

The following command activates the trial license or the production license on the specified server.

To activate the license

- In the </opt/Hitachi/HAPRO/client/bin> directory, execute the `hapro admin activatelicense` command and provide the following mandatory parameters.

Table 3-2: Mandatory parameters

Parameter	Value/details
Application	Application type, `saporacle`.
Server name	Valid <Hostname/ IP of Application Protector Server/ FQDN/ Valid port number (optional)>.
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>
```

Output

```
[I730300D] License activated successfully.
```

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

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

- In the </opt/Hitachi/HAPRO/client/bin> directory, execute the `hapro admin listlicense` command and provide the following mandatory parameters.

Table 3-3: Mandatory parameters

Parameter	Value/details
Application	Application type, `saporacle`.
Server name	Valid <Hostname/ IP of Application Protector Server/ FQDN/ Valid port number (optional)>.
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 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.
2. Activate the Application Protector license for the supported storage and application.
3. Register the supported storage.
4. Configure Application Protector Server and Client, as required.

For configuration details, see *Hitachi Application Protector User Guide for SAP®*.

Glossary

This glossary provides definitions of general storage terms as well as specific terms related to the technology that supports Hitachi Application Protector Quick Install & Configuration Guide for SAP® on Linux®. Click the letter of the glossary section to display that page.

A

API

Application programming interface

Application Protector

Hitachi Application Protector

ASM

Automatic Storage Management

C

CIM

Common information model

CLI

Command line 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.

CSV

Comma separated value

F

Full copy snapshot

Full copy (Shadow image) 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

HTI

Hitachi thin image

I

I/O

Input/output.

L

LU

Logical unit.

LVM

Logical volume manager.

O

OCI

Oracle call interface

P

Point-in-time recovery

Application Protector uses the log files generated by the application server, to replay the log operation to recover the data to the point in time.

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

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®

Restore

Restore is a process of copying a database from a snapshot copy to the original LUN or to a new LUN. On restoring a snapshot, only data files are restored from the snapshot.

RMAN

Oracle Recovery Manager

RPO

Recovery point objective

RTO

Recovery time objective

S

SH

Shell script

SLES

SUSE® Linux Enterprise Server

Snapshot

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

Snapshotable instance

The database instance that resides on a Hitachi supported storage device such as VSP.

S-VOL

Secondary volumes contain copies of the P-VOL.

T

Target

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

V

VSP

Virtual Storage Platform

V-VOL

Virtual volumes contain virtual copies on the P-VOL.

Index

R

S

T

V

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-91HAP018-00