

SAP SUPPORT

backup, restore and disaster

recovery

SAP-SOP-CSL-008

Document Control

|  |  |
| --- | --- |
| Document Version: | Version 1.0 |
| Document Date: | 24th November, 2021 |
| Procedure Implementation Date: | 24th November, 2021 |
| Document Author(s): | Alejandro Sánchez León |
| Document Classification: | **Client Solutions Internal Use Only** |
| Document Distribution: | SAP Support Team |
| Prior Version History: | Version 1.0 Alejandro Sánchez León |
|  |
|  |
|  |
|  |
| Comments: |  |
| Reviewers | Andreu Mendoza Gilabert |
|  |
|  |
| Approvers | Andreu Mendoza Gilabert |
|  |
|  |

CONTENTS

Contents

[1. Purpose 6](#_Toc88667636)

[2. Responsibility 6](#_Toc88667637)

[3. Policy 6](#_Toc88667638)

[3.1 Backups to local disks 7](#_Toc88667639)

[3.2 Backups to external location 7](#_Toc88667640)

[3.3 Customer special policy 7](#_Toc88667641)

[4. Policy Implementation 7](#_Toc88667642)

[5. VIRTUAL MACHINE BACKUP 8](#_Toc88667643)

[5.1 AZURE Snapshots 8](#_Toc88667644)

[5.1.1 Scheduling VM Snapshots 8](#_Toc88667645)

[5.1.2 Checking VM Snapshots 10](#_Toc88667646)

[5.1.3 Restoring from VM Snapshot 12](#_Toc88667647)

[5.2 AWS Snapshots 13](#_Toc88667648)

[5.2.1 Scheduling VM Snapshots 13](#_Toc88667649)

[5.2.2 Checking VM Snapshots 17](#_Toc88667650)

[5.2.3 Restoring from VM Snapshots 17](#_Toc88667651)

[5.3 VMWARE 17](#_Toc88667652)

[5.3.1 Scheduling VM Snapshots 17](#_Toc88667653)

[5.3.2 Checking VM Snapshots 17](#_Toc88667654)

[5.3.3 Restoring from VM Snapshots 17](#_Toc88667655)

[6. OPERATING SYSTEM BACKUP 18](#_Toc88667656)

[7. DATABASE BACKUP 18](#_Toc88667657)

[7.1 HANA 18](#_Toc88667658)

[7.1.1 Scheduling Backups to disk 18](#_Toc88667659)

[7.1.2 Checking backups to disk 24](#_Toc88667660)

[7.1.3 Restoring database from disk 25](#_Toc88667661)

[7.2 SYBASE ASE 26](#_Toc88667662)

[7.2.1 Scheduling backups to disk 26](#_Toc88667663)

[7.2.2 Checking backups to disk 30](#_Toc88667664)

[7.2.3 Restoring database from disk 30](#_Toc88667665)

[7.3 ORACLE 32](#_Toc88667666)

[7.3.1 Scheduling backups to disk 32](#_Toc88667667)

[7.3.2 Checking backups to disk 34](#_Toc88667668)

[7.3.3 Restoring database from disk 35](#_Toc88667669)

[7.4 SQL SERVER 37](#_Toc88667670)

[7.4.1 Scheduling backups to disk 37](#_Toc88667671)

[7.4.2 Checking backups to disk 37](#_Toc88667672)

[7.4.3 Restoring database from disk 37](#_Toc88667673)

[7.5 MAX DB 37](#_Toc88667674)

[7.5.1 Scheduling backups to disk 37](#_Toc88667675)

[7.5.2 Checking backups to disk 37](#_Toc88667676)

[7.5.3 Restoring database from disk 37](#_Toc88667677)

[7.6 DB2 37](#_Toc88667678)

[7.6.1 Scheduling backups to disk 37](#_Toc88667679)

[7.6.2 Checking backups to disk 37](#_Toc88667680)

[7.6.3 Restoring database from disk 37](#_Toc88667681)

[7.7 SQLANYWHERE 38](#_Toc88667682)

[7.7.1 Scheduling backups to disk 38](#_Toc88667683)

[7.7.2 Checking backups to disk 38](#_Toc88667684)

[7.7.3 Restoring database from disk 38](#_Toc88667685)

[8. BACKUP TO VAULT 39](#_Toc88667686)

[8.1 Azure 39](#_Toc88667687)

[8.1.1 Pre-requisites in Azure 39](#_Toc88667688)

[8.1.2 Pre-requisites in the Operating System 41](#_Toc88667689)

[8.1.3 OS Script to save backup files to Azure 41](#_Toc88667690)

[8.1.4 Checking backups to Cloud 42](#_Toc88667691)

[8.1.5 Restore files from Cloud 44](#_Toc88667692)

[8.2 AWS 45](#_Toc88667693)

[8.2.1 Pre-requisites in AWS 45](#_Toc88667694)

[8.2.2 Pre-requisites in Operating System 46](#_Toc88667695)

[8.2.3 OS Script to save backups to AWS 46](#_Toc88667696)

[8.2.4 Checking backups to Cloud 48](#_Toc88667697)

[8.2.5 Restore files from Cloud 48](#_Toc88667698)

# Purpose

The purpose of the document is detailing the policies for database backups and their restoration procedures.

# Responsibility

The execution of this procedure is a responsibility of the Client Solutions SAP Support Team.

# Policy

We must consider following scenarios:

* Backup to disk
* Backup to External Location

And the following backup targets:

* Virtual Machine (VM)
* Database Data Backup
* Database Logs Backup

Also, the policy differs depending on the following landscape elements:

* SAP Development systems
* SAP Quality systems (User Acceptance Test systems)
* SAP Production systems

In the case of Quality systems, those are refreshed from a Production backup at least, twice in a year. We would perform database data backups to disk, only in the case that their disks have space enough. Logs are usually truncated so, no backup of them will be available.

Development systems are a bit more critical than Quality systems (especially during blueprint and initial implementation of the solution), and for those, we will perform database data backups to disk. Logs can be active if there is disk space enough, otherwise, truncated.

In this document we will focus on the **policies that apply to Production systems**, which are the business-critical ones.

## Backups to local disks

Backups to local disks are always limited by the available space. When a new Server is deployed, following policy must be considered to size the disks to be able to contain required backup sets.

|  |  |  |  |
| --- | --- | --- | --- |
| **Backup Target** | **Periodicity** | **Number of sets** | **Retention time** |
| **VM** | Weekly | 3 | 2 weeks |
| **Database Data** | Daily | 3 | 2 days |
| **Database Logs** | Every 15 minutes | 3 | 2 days |

## Backups to external location

Usually, Production data and logs are being saved to an external location. When the customer is accountable and responsible for such an operation, no further backup policies apply to CS SAP Support Team.

When Client Solutions is responsible for such an operation because the servers are hosted by us in CIX or Cloud (Azure, AWS) then, the following policy applies.

|  |  |  |  |
| --- | --- | --- | --- |
| **Backup Target** | **Periodicity** | **Number of sets** | **Retention time** |
| **VM** | Weekly | 1 | 7 days |
| **Database Data** | Daily | 8 | 7 days |
| **Database Logs** | Every 15 minutes | 768 | 7 days |

## Customer special policy

Policies described in previous sections will be applied by default to any new customer. When a special policy is required by a customer, a specific Official Support Procedure will be added to the repository.

# Policy Implementation

While policy definitions are global, the implementation of such policies depend on the Database Engine, Operating System, SAP Stack type and Cloud Environment (when applicable).

Client Solution is working with the following Database Engines for SAP applications:

* HANA
* ASE (Sybase)
* Oracle
* MS SQL
* DB2
* MaxDB
* SQLAnywere

And the following Operating Systems:

* Windows Server (several versions, from 2008 R2 to Datacenter 2019 and any new version to come).
* Linux (mainly, SUSE SLES12, SLES15 and any new version to come).

And the following SAP stacks:

* ABAP Stack: mainly ERP software, including S/4 for HANA
* JAVA Stack: mainly PI software, including MII.
* Other: as Content Server, Business Objects, Master Data Management, Trex, etc.

In each implementation, we can potentially find mixed Operating Systems (by example, Windows for Application Servers and Linux for Database Servers), mixed Database Engines (by example, HANA for ERP, ASE for Content Server, MaxDB for Business Objects) and mixed Stacks (by example, ABAP for S/4, JAVA for PI and other for Business Objects).

We are going to develop below the following topics:

* Scheduling Backups to disk
* Checking Backups to disk
* Scheduling Backups to Cloud
* Checking Backups to Cloud
* Restore from Disk
* Restore from Cloud

And we will specify the procedure for each Database Engine and scenario.

# VIRTUAL MACHINE BACKUP

## AZURE Snapshots

### Scheduling VM Snapshots

While disk backups are being saved under a Blob Container belonging to an Azure Storage Account, the Virtual Machine Snapshots are being saved to a Recovery Services Vault. So, the first step is to create a Recovery Services Vault where to save the VM Snapshots.

To create one Vault by VM makes eventual recovery tasks easier. An example:

Graphical user interface, text, application

Description automatically generated

The Recovery Service Vault can be created when scheduling the VM Snapshot.

* Log in the Azure Portal, for the customer you want to schedule the snapshots.
* Select Virtual Machines.

Graphical user interface, application, Teams

Description automatically generated

* Click on any production VM you want to backup and select *backup* under *Operation*, on the left panel.

Graphical user interface, text, application

Description automatically generated

* Select Recovery Services vault = create new. Enter a valid name for the new Vault, assign the Resource Group to which the VM belongs to (accept default one) and, push the *Edit this policy* to setup a valid backup policy.

Graphical user interface, text, application, email

Description automatically generated

Assign a meaningful policy name. Setup frequency to Weekly. Choose the day and time where the snapshot will be done (better to choose a day and time with no activity). Retain instant recovery snapshots for 5 days is mandatory for Weekly backups. Set the Retention of weekly backup point as per agreed policy. Push the Ok button, once done.

* Enable backup, pushing the button of same name in previous screen.

### Checking VM Snapshots

* Once in the Azure Portal, select All Resources

Graphical user interface, application

Description automatically generated

* Filter by type and choose the vault corresponding to the VM you wanted to check.

Graphical user interface, text, application, email

Description automatically generated

* Choose *Backup Items* under section *Protected Items* on left panel.

Graphical user interface, text, application

Description automatically generated

Under BACKUP MANAGEMENT TYPE / Azure Virtual Machine, we can see the number of VMs that are being backed up in this Vault.

* Push on the *Azure Virtual Machine.*

Graphical user interface, application

Description automatically generated

Now, we can see how many backups are stored in the Vault and, what was the execution status of them, as well as the recovery point in time.

* Same Information can be seen in section *Monitoring* / *Backup Jobs*. Just use the *Filter* to select a range of dates for which you wanted to monitor jobs results.

Graphical user interface, table

Description automatically generated

### Restoring from VM Snapshot

In the previous section we have seen how to check which VM Snapshots are available. Once we have found the wanted one, we can restore such a Snapshot to any existing VM.

Please, be aware that to restore a VM Snapshot completely overwrites all VM disks with the selected snapshot.

* Enter the snapshot detailed info and select *Restore VM*:

Text

Description automatically generated with medium confidence

Then, follow the steps proposed by the Azure’s Wizard.

* If you wanted to recover just a disk unit, folder, or file, please select *File Recovery* instead.

Graphical user interface, text, application, email

Description automatically generated

And follow the steps proposed by the Azure’s Wizard.

## AWS Snapshots

### Scheduling VM Snapshots

* Open *AWS Backup* service (https://console.aws.amazon.com/backup)
* Select *Backup Vaults* on left panel

Graphical user interface, text, application, website

Description automatically generated

* Use an existing vault or create a new one

Graphical user interface, application

Description automatically generated

* Select *Backup Plans* on left panel, to create a new plan.

Graphical user interface, text, application

Description automatically generated

* Create the backup plan

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

* Select the already created backup plan and push the *Add Resources* button.

A screenshot of a computer

Description automatically generated

* Add resources (those production VMs you wanted to backup)

Graphical user interface, text, application, email

Description automatically generated

Be sure to select resource type *EC2* and then, choose wanted VMs from the *Instance* IDs drop-down list. Their IDs will be transferred below.

Graphical user interface, text, application

Description automatically generated

* Finally, push the *Assign resources* button.

Graphical user interface, text, application, email, website

Description automatically generated

### Checking VM Snapshots

* Log to the AWS Backup console (see 5.2.1) and select *Jobs* on the left panel.

Graphical user interface, application

Description automatically generated

* Choose the period for which you want to check already executed backup jobs
* Select one job and go to details to check its execution details

### Restoring from VM Snapshots

* Search for the *Backup Job* as described in 5.2.2 and go to details.
* In *Actions* you can start a *Restore Job*. Please carefully follow the *AWS wizard* instructions and warnings.

## VMWARE

### Scheduling VM Snapshots

### Checking VM Snapshots

### Restoring from VM Snapshots

# OPERATING SYSTEM BACKUP

The Operating System backup is integrated in the Virtual Machine Backups procedure, since the VM Snapshot includes the Operating System disk.

When needed, ad-hoc backups of the relevant /usr/sap directories can be taken to disk.

# DATABASE BACKUP

## HANA

#### Scheduling Backups to disk

HANA 2.0 Database Engine is a multi-tenant engine, which can hold more than one database. SYSTEMDB database is the administrative database that holds information about any other tenant and, it should be backup together with the tenant databases.

HANA Cockpit is a HANA simplified database that contains information about other systems / Hana databases. It can be accessed with the URL generated during the installation process.

#### Prerequisites

Before we can start backing up any HANA database with HANA Cockpit, pre-requisites are:

* HANA Cockpit must be already installed in the server or environment to manage.
* The URL to access HANA Cockpit must be known
* The administrative user for HANA Cockpit (usually COCKPIT\_ADMIN) must have been defined in the relevant databases.
* The password for such an user must be known (please, see Keeper records).

#### Step 1 – log in HANA Cockpit

Open your preferred Internet browser, enter the URL for the relevant HANA Cockpit installation. You will land on some page as the following one:

Graphical user interface, application

Description automatically generated

#### Step 2 – Open hana-cockpit

After pushing the button “hana-cockpit” you will be able to manage the already defined Hana systems. By example:

Graphical user interface, application

Description automatically generated

#### Step 3 – Open the Resource Directory

The combination of a system and a Hana database, it is being called a *Resource*. In the above picture, we can see that 9 resources were registered in the *Resource Directory* tile. Push *Resource Directory* tile to manage registered databases.

Graphical user interface, application, table

Description automatically generated

Click on the name of the Database/Database System ID for which you wanted to schedule a backup. By example, DBD@DBD, which means the database DBD in Hana Instance ID DBD.

#### Step 4 – Open Manage Database Backups

Search for the Menu group *Database Administration* and click on *Manage database backups*

Graphical user interface, text, application, email

Description automatically generated

#### Step 5 – Configure Backup

Click on *Configure Backup.*

Graphical user interface, application

Description automatically generated

In this step is where you define the backup policy. You are not scheduling any backup action but, just defining common parameters that apply to every backup made for this database.

Graphical user interface, text, application, email

Description automatically generated

##### Log Settings Section

* Leave *Log Mode* setup as “normal”

##### Log Backup Section

* Define the file destination folder for log backups (Location),
* Define the Time Limit (which is usually 15 minutes for Production Systems).
* The Time Limit parameter will make Hana to backup a log at least after that time expired but, if any log was full before that time, Hana will generate as many logs as needed.

Graphical user interface, text, application, email

Description automatically generated

##### Data Backup Settings Section

* Be sure that the Data Backup Scheduler is Active (Enable Data Backup Scheduler = Yes)
* Assign user SYSTEM.
* Enter the destination folder to store the data backups (Location).

##### Retention Policy Section

* Enable the Retention Policy Scheduler (Yes).
* Assign user SYSTEM as the database user.
* Delete Backup Generations Automatically (Yes).
* Options for Backup Deletion = Remove from backup catalog and delete physically from file system.
* The value for *Retain Backup Generations Younger Than* is the number of copies that you want to keep less one.
* Leave Minimum No. of Retained Backup Generations equal to 1.
* Start Daily Automatic Deletion (UTC). This fixes the hour when the existing backups are being checked for their age and, when the system will delete “old” backups.
* Please, remember to save any change to the Backup Configuration, to make the change effective.
* Note: this step is not required if the Backup Configuration already exists and no change in policy is needed.

#### Step 6 – Schedule backups

If Step 5 was executed then, go back (button “<”). Otherwise push the *Go to Schedules* button.

If there are scheduled backups already in place, you will see them as follows:

Graphical user interface, text, application

Description automatically generated

Please, select the period (1 month in this example) to have an overall look of the days when the database will be backup. Selecting any icon will provide an overview of the task. You can see full details clicking on “More Details”.

Once in more details, if you wanted to delete current schedule, you can do it pushing the *Delete* link button.

To add a new schedule, just click on the day you want the schedule to start.

##### Step 1

Graphical user interface, application

Description automatically generated

In case that you wanted to execute just a single backup, choose *Schedule a Single Backup*. In case that you wanted to schedule a periodic backup, choose *Schedule a Series of Backups.*

The schedule is being defined in several steps. Push the Step N button to continue with the next step, after entering required information.

##### Step 2

* Schedule Name: enter a meaningful description for that backup schedule

##### Step 3

* Backup Type: usually, Complete.
* Backup Prefix: usually, the default value is ok
* Backup Destination: please, define the destination folder where backups will be saved
* Comment: you could enter same information as the Schedule Name

##### Step 4

* Recurrence Pattern: usually, for daily backups you select Weekly

##### Step 5

* Time Zone: UTC. Please, select UTC always, because the *Retention Tool* start of execution time is always expressed in UTC. In that way you will be able to see if some backup or retention tool overlaps in time.
* Create backups at: Enter the starting time (always ended with AM or PM).
* Create backups on: Select the days the backup should run. Usually, all of them.
* Activate Schedule on: enter the first day the first backup must be executed.

##### Review

Last step is to review/modify the already entered information.

If you are ok with the schedule, push the *Save Schedule* at bottom-right hand.

### Checking backups to disk

For this, we will use HANA Studio so, a pre-requisite is that you have HANA Studio installed in your PC and you have already setup the connection to the required database.

* Open HANA Studio
* Select the database connection for which you wanted to check the backup status. Please, select the connection corresponding the database SYSTEMDB of that system.
* Dropdown the list under the connection and double click on the folder called Backup
* A window will be opened on the right panel.
* Go to tab called Backup Catalog

Graphical user interface, application

Description automatically generated

* In Database you can choose the SYSTEMDB database or the Tenant Database.
* Backups in disk can be seen in the list at left hand of the right panel.
* Detailed files corresponding to the currently selected backup can be seen at right hand, as well as their physical location.
* The status of every backup job can be easily check under the column Status. When green, the backup was successful.

### Restoring database from disk

The easiest and safest way to do a restore is to use the HANA Studio tool.

Right-click over the database you want to recover and select Backup and Recovery and then, Recover Tenant Database to recover the real business data or Recover System Database to fix any issue with the system control database.

Graphical user interface, application

Description automatically generatedThen, enter the <sid>adm user for that SAP Instance and its password and let the wizard to guide you with the rest of the recovery process.

Graphical user interface

Description automatically generated with low confidence

## SYBASE ASE

### Scheduling backups to disk

#### Preparing automatic logs dump

To ensure recoverability of the server, follow instructions as per SAP note **1585981 - SYB: Ensuring Recoverability for SAP ASE**.

* Connect to database <DBSID>

isql -Usapsa -P<password> -X -w 255 -S<DBSID>

* Use master db:

Use master

Go

* Change required DB options. Following DB options must be set up to allow log archiving:

| **Option** | **Value** |
| --- | --- |
| ‘trunc log on chkpt’ | false |
| ‘full logging for all’ | true |
| ‘enforce dump tran sequence’ | true |

Once connected to the DB, use following command to change required option:

sp\_dboption <SID>, [dbname, optname, {true | false}]

**Note: run command checkpoint just after changing the option ‘trunc log on chkpt’.**

Please, be aware that once the option “trunc log on chkpt” is set to “false” then, when the log is full, if no dump is done, the DB will stop any further update attempt and the system will look as “hanged”.

Therefore, it is very important to do these changes at same time of rest of changes that ensure the automatic log dump.

To check current values for a certain database sp\_helpdb <SID> can be used:

Table

Description automatically generated

* Set ASE parameter 'tape retention in days' to a value that is larger than your backup cycle.

Once connected to the master database, use following command to view (without value) or change (with a value) any parameter.

*Sp\_configure <SID>,<parameter>, <value>*

**Very important: to make this value permanent, the configuration file must be updated (/sybase/<SID>/ASE/install/DB<SID>.cfg) as well.**

* Create a File System Folder to hold the log archive separately (easier to handle).

By example, create a folder called LOG under your backup directory.

Text, table

Description automatically generated with medium confidence

Be sure permissions, user and group are at least the same as the upper folder.

Table

Description automatically generated

In the above example, we are planning to dump the log archives to folder /SAP\_backup/LOG.

To separate these dumps (backups) from the ones corresponding to the DataBase, allows a better control of logs, for specific procedures and, helps to clearly identify which DB backups are really kept in the disk.

* In this step we will create two separate dump configurations (i.e. backup configurations) to dump (backup) the DB and its logs separately.

By example, we could distinguish both like this:

<SID>\_DB (by example IEP\_DB)

<SID>\_LOG (by example IEP\_LOG)

To create a dump configuration (backup configuration) you must be using master database and then, execute command:

*sp\_config\_dump @config\_name='<SID>', @stripe\_dir = '<destination\_folder>' , @compression = '101' , @verify = 'header'*

Where SID is the Database Identifier (by example, IEP) and destination\_folder is the folder that will hold the backups for defined configuration.

By example:

Graphical user interface, application, table, Excel

Description automatically generated

After that, we will have two dump configurations (backup configurations) to run the dump (backup) command, mentioning the right one for each case.

* Setup log thresholds

Set up a threshold action for transaction log, as described in note [1801984](https://launchpad.support.sap.com/#/notes/1801984) or in this link: <https://blogs.sap.com/2015/08/05/sybase-automatic-transaction-log-backupdump/>

The idea here is to create a mechanism that automatically dumps the current log file when reaching certain size, to avoid the database engine to stop (because of full log condition). This solution works together with the scheduled log dump and, it is automatically triggered.

We could use just this one instead of the scheduled one. The drawback is that if there were not transactions enough to surpass the threshold, no log could be archived.

**Note: ITSM incident 8000018068 can be of help, also.**

#### Schedule backups to disk

* Log in any SAP Server that has a connection to the database already setup.
* Execute transaction DB13 to schedule the jobs.

To back up the DB, we can use the already created configuration (<SID>\_DB) files. The file names will follow a standard convention as: *<database>\_<timestamp>.dmp*

We need to schedule SQL Scripts as in this example:

*--SAP DBA Planning Calendar: SQL Script*

*print( SELECT "starting job execution at " || str\_replace(convert(VARCHAR(20),getdate(),23),"T","") )*

*dump transaction IEP using config = 'IEP\_LOG'*

*print( SELECT "job execution finished at " || str\_replace(convert(VARCHAR(20),getdate(),23),"T","") )*

So, the commands for both cases should look like this:

Dump database <SID> using config=<SID\_DB>

Dump transaction <SID> using config=<SID\_LOG>

Where <SID> is the DB Id, <SID\_DB> is the dump configuration for the Database (if needed) and <SID\_LOG> is the dump configuration for the Logs.

Please, be aware that all databases must be backup (master, model, saptools, sybmgmtdb, etc), following same approach.

### Checking backups to disk

You can use SAP transaction DB13 to check the execution of the scheduled backups. Those backups that went successful can be seen highlighted in green colour, those still not executed in grey colour and those that had errors in red colour.

Graphical user interface

Description automatically generated

### Restoring database from disk

IMPORTANT: Before starting any restoration procedure, the SAP instance must be stopped (refer to Start/Stop Sybase and SAP instances procedures).

The backups and logs SYBASE databases are usually saved to directory /backup/<SID>. Where SID is the SAP System Identifier.

To perform the restore:

• Connect to the server where the database is installed via SSH as syb<SID> user.

• Log on into target database DBSID with the Sybase CLI:

isql -S<DBSID> -Usapsa -P<PASS> -X -e

Where <PASS> is the password for sapsa user

• Once inside, execute:

load database with listonly = LOAD\_SQL, until\_time = go

This command will list everything that needs to be executed to restore the database

specified in the <DB> parameter up to the time <DATE\_TIME>. Example:

load database <SID> with listonly = LOAD\_SQL, until\_time = "oct 24, 2021

02:45:43:866am"

Go

The output will be a list of all the commands to restore de MP1 database to how it

was on October 24th at 02:45 am:

Text

Description automatically generated

Copy the output and paste it directly inside de Sybase CLI.

• Following the output of the command, execute:

online database go

• Start the SAP instance again.

## ORACLE

### Scheduling backups to disk

#### Pre-requisites at Operating System

For SAP environments, there are two profile files that must be maintained before scheduling any Oracle backup. Those can be found under <ORACLEHOME>\database and they have the names init<SID>.ora and init<SID>.sap, where <ORACLEHOME> is the installation directory for Oracle and, where <SID> is the SAP Instance Identifier.

Graphical user interface, text, application, email

Description automatically generated

##### Init<SID>.sap

This is the key file to parametrize how backups and restores will be handled by SAP tools (as *Brtools*).

Text, letter

Description automatically generated

You should carefully understand and review every parameter there, to be sure that the backups triggered by SAP are successful.

Any parameter here is used by *brtools*, which is the standard SAP tool to manage Oracle databases for SAP environments.

#### Scheduling backups in DB13

The standard way to schedule Oracle backups is to use SAP DB13 transaction.

Graphical user interface

Description automatically generated with medium confidence

When scheduling a backup, select the Action *whole database online + redo log backup*, to be sure that both, database, and logs, are being backup.

You will see that the profile corresponds to the OS file already mentioned above in 7.3.1.1.

Function changes the way the backup tool verifies previous backups and creates new ones. The value *-sd* will delete any older backup before creating the new one. Retention periods and, rest of backup policy data is maintained in the profile file, as mentioned in 7.3.1.1.

### Checking backups to disk

For this, same transaction DB13 can be used.

Successful backup tasks will be seen highlighted in green, while failed backup task will be seen highlighted in red. You can click on any task to see further details, like the *job log*:

Graphical user interface, application

Description automatically generated

### Restoring database from disk

The best way to restore an Oracle database from disk is to use the *brtools* command, at OS level.

#### OS Preparation tasks

1. **Be sure that the backup media is ready, available, and readable**.
2. **STOP SAP**
3. **Force 4 times log switching in Oracle (to backup the up to 4 online logs).**
4. **Shutdown Oracle**

Text

Description automatically generated

1. **Delete Oracle’s SAP data files but, leave folders structure**, otherwise, the recovery will fail later, while creating the data files.

Graphical user interface, text, application

Description automatically generated

1. **Save current online logs and online mirror logs**

Graphical user interface, application, Word

Description automatically generated

#### Oracle’s BRTOOLS procedure

At Operating System command line, you should invoke command *brtools* and choose the *Restore and Recovery* option.

Text

Description automatically generated

You can then choose which kind of restore operation do you need. You only need to follow the guided steps that *brtools* provide.

Please, be aware that the default parameters for brtools are taken from file <SID>init.sap, as mentioned in 7.3.1.1.

## SQL SERVER

### Scheduling backups to disk

### Checking backups to disk

### Restoring database from disk

## MAX DB

### Scheduling backups to disk

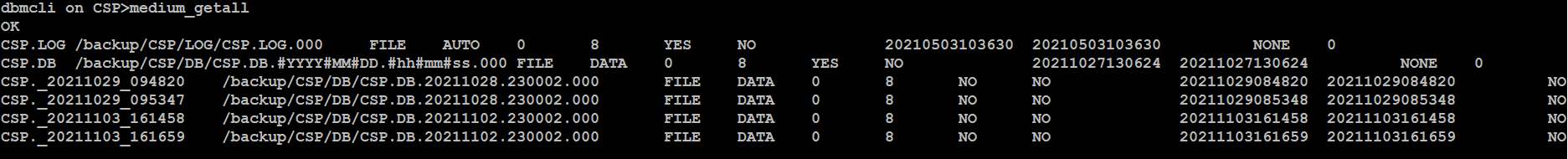
#### Prerequisites

Before proceeding with the MaxDB backups, the prerequisites are:

* Access to the system where the MaxDB is running as root and/or sqd<SID>.
* Access to a system with Database Studio installed and the required Database configured.
* Database *control* and *superdba* user (please, see Keeper records).
* Name and details of the medium, which can be checked following the steps below:
  + Connect to the system via SSH.
  + As sqd<DBSID>, execute:

dbmcli -u control,<PASS> -d <DBSID> medium\_getall

* + The output should look like:



* + From this output, the important values are:
    - 1st column: Medium Name
    - 2nd column: location
    - 4th column: type. It should be DATA

For more information, check [here](https://maxdb.sap.com/doc/7_7/45/0f47b4f1394574e10000000a114a6b/frameset.htm).

* + In the image, the Medium Name to use for the backup (or restore) would be “CSP.DB”.

#### Scheduling Data Backups

* Connect to the system where the MaxDB is running as root via SSH.
* To perform a backup, execute:

sudo -u sqd<DBSID> /bin/bash -c ". /home/sqd<DBSID>/.profile ; (echo db\_connect ; echo backup\_start <MEDIUM\_NAME> ) | dbmcli -u control,<PASS> -d <DBSID>"

* To schedule the backups, add the line to the crontab file:

<MINUTE> <HOUR> \* \* \* sqd<DBSID> /bin/bash -c ". /home/sqd<DBSID>/.profile ; (echo db\_connect ; echo backup\_start <MEDIUM\_NAME> ) | dbmcli -u control,<PASS> -d <DBSID>"

* Please note that it may be good to create a script with the “backup command”, since it may be more readable, the password will not be in plain text in the crontab file, and more functionalities can be added (like saving the output of the backup).

#### Scheduling Log Backups

* Connect to the system with Database Studio installed.
* Open Database Studio.
* Enter *superdba* password.
* In the Explorer section, go to World à Local à <CUSTOMER> à Servers à <HOSTNAME> and right click on <DBSID> and select Administration:

Graphical user interface, application, Word

Description automatically generated

* Below the Administration tab, in the Settings section, click on “Automatic Log Backup”:

Text

Description automatically generated

* Select the corresponding medium and configure how often they must be performed:

Graphical user interface, text

Description automatically generated

### Checking backups to disk

#### At OS level

* Connect to the system where the MaxDB is running via SSH.
* List the entries inside the <LOCATION>. They are usually stored in /backup/<DBSID>/DB:

A screen shot of a computer

Description automatically generated with low confidence

To know what <LOCATION> is configured, check the 7.5.1.1 Prerequisites section.

#### Using DB13

If there is an SAP system with the corresponding Database configured, transaction DB13 can be used to check the data and log backups:

* Enter the SAP system and execute DB13.
* Select the corresponding system:
  + Using the dropdown menu in the upper left corner of the screen
  + Or filling the System field below the “DBA Planning Calendar” text

Table

Description automatically generated

* The successful backups are highlighted in green, while those that had errors are in red. Also, double-clicking one of the backups will show the details of the execution and the action parameters.

### Restoring database from disk

Before starting with the restore:

* Stop the SAP instance.
* Check that the folder where the backups are stored contains the file to be used for the restore. To check where they are stored, check 7.5.1.1 Prerequisites.

To perform the recovery:

* Connect to the system with Database Studio installed.
* Open Database Studio
* Enter superdba password.
* In the Explorer section, go to World à Local à <CUSTOMER> à Servers à <HOSTNAME> and right click on <DBSID> and select Administration:

Graphical user interface, application, Word

Description automatically generated

* On the Administration section, on its top bar, click the “Administration Task” button (the one with a tool icon) and select Recovery.

Graphical user interface, text, application

Description automatically generated

* Set the Database in ADMIN mode (remember to have de SAP instance stopped before changing the Database mode).

Graphical user interface, text, application

Description automatically generated

* In the next screen, set how the restore is to be performed:

Graphical user interface, text, application

Description automatically generated

* Please note that the logs will be used if available to restore the database to its most recent version. If the goal is to restore the database as it was a few days earlier, use the “Recover until a specific time” option.
* Press Next until a summary appears. If no warning shows, click Start to perform the recovery. Otherwise, click on resolve:

Graphical user interface

Description automatically generated with medium confidence

* Select create “Temporary medium to use for the recovery” and press OK:

Graphical user interface, text, application, email

Description automatically generated

* Select Start to perform the restore.
* If not automatically restarted, press the green button below the Administration tab once the restore is done:

Graphical user interface, text, application, email

Description automatically generated

* Start the SAP system.

## DB2

### Scheduling backups to disk

### Checking backups to disk

### Restoring database from disk

## SQLANYWHERE

### Scheduling backups to disk

### Checking backups to disk

### Restoring database from disk

# BACKUP TO VAULT

This is only relevant for those system that are saving a copy of the backup files to an external resource in Cloud.

## Azure

### Pre-requisites in Azure

The Cloud environment has been correctly setup and that we have already identified a valid Azure Storage Account and a Blob Container where those backups will be copied.

Graphical user interface, text, application

Description automatically generated

The Storage Keys for the Storage Account have been generated:

Graphical user interface, text, application

Description automatically generated

Storage Account Live Cycle Management implements the retention policy defined (CS Standard or Customer Specific). By example:

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application

Description automatically generated

Table

Description automatically generated

### Pre-requisites in the Operating System

The tool used to backup and recover files to and from Azure Cloud is **AzCopy**, which can be downloaded here: <https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-v10>.

AzCopy must be installed in the server holding the backup data.

### OS Script to save backup files to Azure

A script must be written to upload the backup files from local disk to Azure, by using the command AzCopy.

Also a “watchdog” script must be created which will delete AzCopy logs and any file older than the established retention time.

Those scripts are being scheduled using the command cron (/etc/crontab, for Linux) or the Task Scheduler (for Windows). Here we can see an example of file /etc/crontab in Linux:

Text

Description automatically generated

The script */usr/sap/MP1/script/backup\_MP1\_RMOLD.sh* is the *watchdog* that will delete old files and AzCopy logs once a day (at 00:23h), while the script */usr/sap/MP1/script/backup\_MP1\_ARCHIVE.sh* is the responsible for backing up any new file to Azure, every 15 minutes (this will depend on the agreed backup policies).

Let’s have a look to those *Shell* scripts (Linux). In the case of Windows, we will find similar scripts adapted to *Powershell.*

This is the script backup\_MP1\_RMOLD.sh, which will remove old files and will remove AzCopy logs, once a day.

Text

Description automatically generated

And this is the script backup\_MP1\_ARCHIVE.sh, which will copy any new backup file to the corresponding Azure Blob Container:

Text

Description automatically generated

Note that the storage account, the blob container as well as the Azure SAS Key (masked on the picture, for security reasons) are needed by AzCopy .

### Checking backups to Cloud

We will use the example of Azure for this.

First step is to log in the Azure Portal and selected the wanted Storage Account and Blob Container you want to check. In this example, we are exploring the Blob Container called MP1:

Graphical user interface, text, application, email

Description automatically generated

We can find two folder inside such a container. The first one (DB) is where data backups will be copied and, the second one (LOG) is where the database archive logs will be copied.

This is an partial example of the content of folder DB:

Graphical user interface, table

Description automatically generated with medium confidence

And this, a partial example of the content of folder LOG:

Table

Description automatically generated

### Restore files from Cloud

If the needed backup files are available in the local system, there is no need to restore the backup files from Cloud but, in case that any backup file is missing or damaged in the local system, we can recover the needed backups files from the Cloud Storage Account / Blob Container.

In the Azure Portal, inside the relevant Storage Account / Blob Container and Folder, we can select all those files that we want to copy back to the server and then, we can chose the download option.

Graphical user interface, application

Description automatically generated

For this, you need to access Azure from the target server or, from any other server and, move the files to the target server. This is an example of an script for Windows Powershell to synchronize the local folders from the data available at Azure:

Graphical user interface, application

Description automatically generated

## AWS

### Pre-requisites in AWS

The Cloud environment has been correctly setup and that we have already identified a valid AWS S3 Storage and Bucket where those backups will be copied.

Graphical user interface, application

Description automatically generated

In this example, the bucket is *jjrathigan*. Inside the bucket, a folder for backup must have been created:

Graphical user interface, text, application, email

Description automatically generated

And the corresponding subfolders for each production system.

Graphical user interface, text, application, email

Description automatically generated

In this case, separated folders to backup the HANA database backups were created for system H2P, which belongs to the productive environment S4P.

### Pre-requisites in Operating System

The tool used to copy files from the VM to the AWS S3 bucket/folder is the *AWS CLI (Command Line Interface).* This must have been previously installed, as per link: <https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-started.html>.

### OS Script to save backups to AWS

An OS Script must be created to be able to save the database backup files from the VM’s disk(s) to the S3 bucket/folder in AWS.

The script will be a *Shell* script (in the case of Linux) or a *Powershell* script (in the case of Windows).

This is an example of a shell script:

Table

Description automatically generated

The script must be scheduled to run with the periodicity needed as per implemented backup policy. If the operating system is Linux, we will schedule the command using the file /etc/crontab (for command cron). If the operating system is Windows, we will use the Task Scheduler for the same.

This is an example of a Linux crontab file:

Graphical user interface, text

Description automatically generated

### Checking backups to Cloud

For this go to the Amazon S3 service (<https://s3.console.aws.amazon.com/s3/home?region=eu-west-1&region=eu-west-1>) and select the Bucket and folder that corresponds to the VM backups that you want to check.

Graphical user interface, application, table

Description automatically generated

### Restore files from Cloud

Once you are in the detailed information for any S3 file (please see 8.2.4), you can download it to any wanted location.

Graphical user interface, text, application, email

Description automatically generated

Optionally, you can use the AWS CLI, at the Operating System of the target server to recover more than one file in a single shot. This is an example Shell script to synchronize local disk from data available in AWS.

Table

Description automatically generated