Acronis

acronis.com

Cyber Protection service

Protecting SAP HANA

White Paper

REVISION: 5/12/2023

Table of contents

Copyright statement

Acronis patented technologies

Technologies, used in this product, are covered and protected by one or more U.S. Patent Numbers: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; and patent pending applications.

Introduction

SAP HANA is a relational database management system designed to store data in memory. In certain scenarios, this architecture offers significant advantages over traditional databases that rely on a disk storage mechanism. However, this same in-memory design creates additional challenges when protecting servers running SAP HANA because the data located in the memory is not normally copied as part of regular backup.

This document describes the solution for creating consistent disk-level backups of servers running SAP HANA, in a simple, straightforward manner that does not require any SAP HANA knowledge or expertise. The solution allows you to recover SAP HANA servers to bare metal, same or different hardware, migrate them from a physical machine to a virtual machine and vice versa – something that is not offered by traditional and legacy database backup solutions.

SAP HANA backup basics

Although the SAP HANA data resides in the memory, this database uses persistent storage like any other database, to be able to survive across power cycles. This persistent data is split into two areas: the data area and the log area.

Data is automatically saved to the data area at regular intervals (savepoints) and all changes are captured in the redo log entries. As with other databases, an entry is placed in the log after every committed database transaction.

After a sudden power failure, SAP HANA can be restarted like a traditional database: it loads the last savepoint and replays the redo logs from that point up to the last committed transaction.

However, this system does not protect the data from disk storage failures and logical errors. Backups are required to protect against disk failures or to return a database to an earlier point in time.

SAP HANA backup methods

SAP HANA offers three backup methods:

- Backup to the file system
- Backup via the Backint API provided by SAP
- Backup using snapshots

Backup to the file system

This method creates a backup of the data and logs in a folder on the file system, for example, in an NFS folder. A backup can be triggered manually as an action in the SAP HANA Studio, through SQL commands, or scheduled by using the DBA Cockpit.

This is an easy way to obtain a copy of the data, but it requires additional storage and time to create the copy, and it impacts the network load and performance.

Backups via Backint API

This method is similar to backups made to the file system, but the data and logs are redirected through the API to a third-party backup server or storage solution.

As with the previous method, Backint creates a copy of the database only and not of the underlying system. This means that a recovery of the entire server would require a long multi-step process or a standby server.

The Cyber Protection service does not yet offer integration with the Backint API.

Backup using snapshots

This method makes use of a data snapshot preparation mechanism built-in to SAP HANA, which works in conjunction with an external tool (like a storage snapshot or a Cyber Protection service snapshot) that creates a snapshot of the entire data area.

The Cyber Protection service uses the SAP HANA snapshot preparation mechanism to create disk-level, application-consistent backups of the entire SAP HANA server. This solution provides the following advantages:

- Bare-metal recovery to the same or dissimilar hardware, with support for LVM
- Physical-to-virtual and virtual-to-physical conversion
- Almost-instant restore by running a VMware ESXi virtual machine from a SAP HANA server backup

The snapshot solution overview

- The Cyber Protection service provides the tested and verified pre- and post-data capture scripts that handle the intricacies of preparing the internal SAP HANA snapshot and closing the snapshot correctly.
- These scripts are included in a protection plan that backs up the entire SAP HANA server.
- Every time this protection plan runs, the pre-data capture script calls on SAP HANA to prepare the internal snapshot that leaves the database in a ready and consistent state on the disk. This sets the stage for the Cyber Protection service's own snapshot to capture this state.
- The Cyber Protection service takes the disk snapshot.
- The post-data capture script releases the SAP HANA snapshot.

  Preparing, taking, and releasing the snapshot are nearly instantaneous. The database remains operational throughout this time.
- The Cyber Protection creates a backup of the entire machine, including the SAP data area, frozen in time at the moment of snapshot creation.

This backup can be used to recover the entire server, converted to a virtual machine, or mounted to a file system as a volume. Every time, the SAP HANA data inside the backup will be consistent.

Supported SAP HANA versions

HANA 2.0 SPS 03 installed in RHEL 7.6 running on a physical machine or VMware ESXi virtual machine.

Because SAP HANA does not support recovery of multitenant database containers by using storage snapshots, this solution supports SAP HANA containers with only one tenant database.

Backing up physical servers

Prerequisites

- The SAP HANA backup functionality requires the Advanced Backup pack.
- Agent for Linux must be installed on the server running SAP HANA and registered in the Cyber Protection service.

Note
To download the installation file, sign in to the Cyber Protection service and click the account icon in the top-right corner > Downloads.
To install the agent, proceed as described in the "Installing the software" section of the user documentation.

Installing the scripts

- Download the file https://dl.managed-protection.com/u/SAPHANA/SAP-HANA-modules.tar
- Unpack the file: `tar -xvf SAP-HANA-modules.tar`
- Give the executable permissions to the setup script: `sudo chmod 777 setup.sh`
- Run the setup script `setup.sh`

Configuring access to the databases

1. Change the directory:

   ```
   cd /usr/lib/Acronis/SAPHANA/bash/
   ```

2. Specify the access credentials by using the commands described below.
   The user whose credentials you specify must have the Backup Admin and Catalog Read privileges on the respective instance.
   - To add credentials by specifying a user name and password

     ```
     sudo ./config.sh ADD -i <instance_number> -d <database> -u <user> -p <password>
     ```

     The credentials that you provide are stored at /var/lib/Acronis/SAPHANA/Config/config.yaml and are only accessible by the root user. The password is encoded in base64 and not encrypted.
   - To add a user from a secure user store

     ```
     sudo ./config.sh ADD -i <instance_number> -d <database> -U <key>
     ```

   - To remove credentials for a specific database

     ```
     ./config.sh REMOVE -i <instance_number> -d <database>
     ```

- To view the list of added credentials

  ```
  sudo ./config.sh LIST
  ```

- To view credentials for a specific database

  ```
  sudo ./config.sh GET -i <instance_number> -d <database>
  ```

3. Specify the SAP HANA installation path:

   ```
   sudo ./config.sh SET_INSTALL_PATH --install_path <path>
   ```

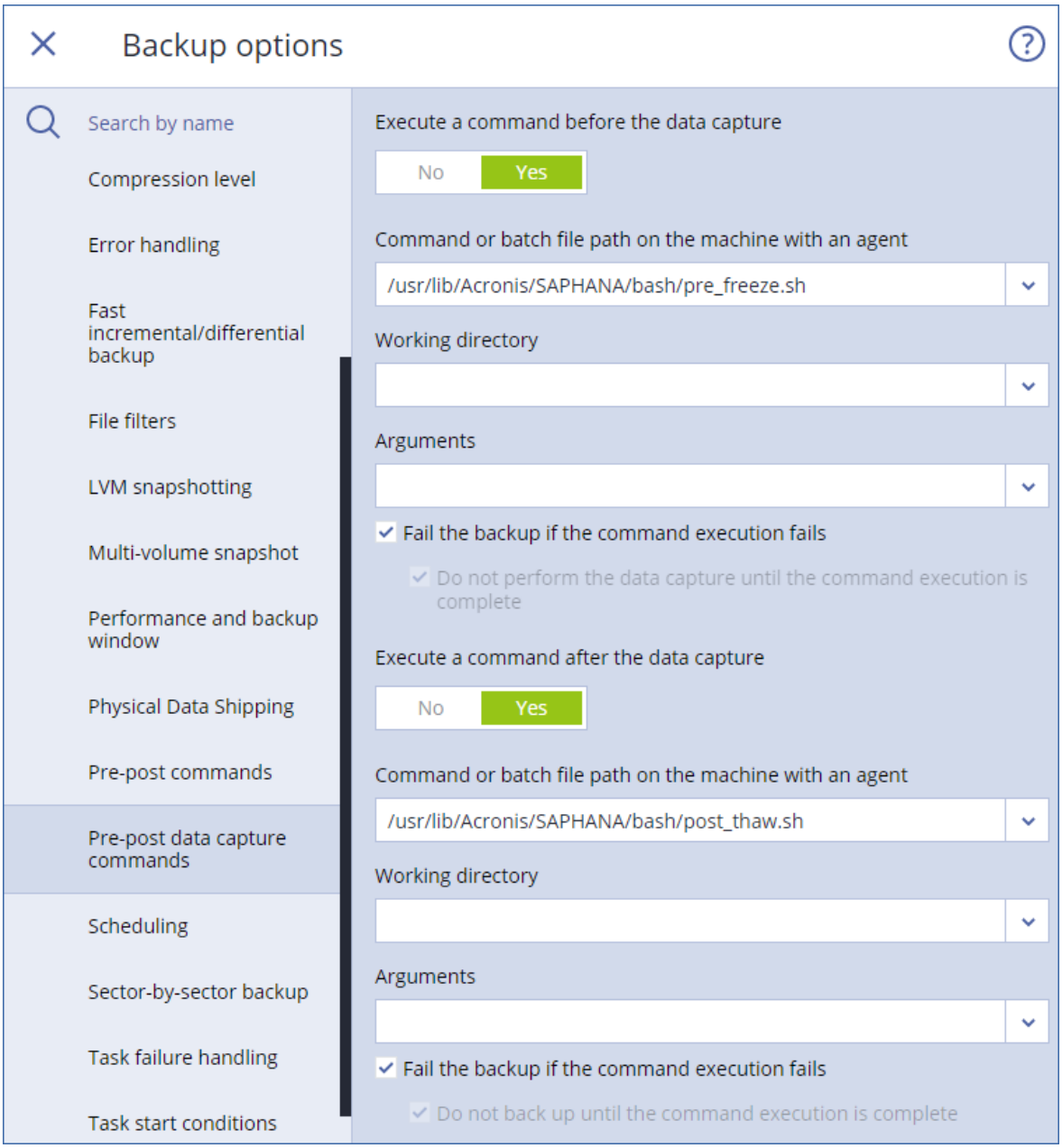
   Here, `<path>` is the path to the `sapservices` file that SAP HANA uses to keep track of where the databases are installed. The default path is /usr/sap.

Creating a protection plan

Create a protection plan for the entire SAP HANA server according to your server protection requirements, as described in the "Backup" section of the user documentation.

When creating the plan:

1. In **Backup options**, select the **Pre-post data capture commands** option.
2. Enable the **Execute a command before the data capture** switch.
3. In the **Command or batch file path on the machine with an agent** field, enter the pre-data capture script path: /usr/lib/Acronis/SAPHANA/bash/pre_freeze.sh
4. Enable the **Execute a command after the data capture** switch.
5. In the **Command or batch file path on the machine with an agent** field, enter the post-data capture script path:
   - /usr/lib/Acronis/SAPHANA/bash/post_thaw.sh – if you do not want to truncate logs
   - /usr/lib/Acronis/SAPHANA/bash/post_thaw_with_truncate_logs.sh – if you want to truncate the logs after each backup. This modified script will delete redo logs after successfully closing the snapshot.



6. Select the **Multi-volume snapshot** option and make sure it is enabled.
7. Click **Done**.
8. Specify other settings of the protection plan as appropriate, and then click **Create**.

The protection plan will be created and applied to your SAP HANA server. The backups created by this plan will contain a consistent database while making use of the powerful functionality that the Cyber Protection service provides for all disk-level backups.

Backing up virtual servers

Prerequisites

- The SAP HANA backup functionality requires the Advanced Backup pack.
- The VMware ESXi virtual machine running SAP HANA must have VMware tools installed.
- Agent for VMware must be installed in VMware vSphere or on a Windows machine, and registered in the Cyber Protection service.

Note
To download the installation file, sign in to the Cyber Protection service and click the account icon in the top-right corner > Downloads.
To install the agent, proceed as described in the "Installing the software" section of the user documentation.

Further steps

Log in to the guest system and perform the "Installing the scripts" and "Configuring access to the databases" procedures described in "Backing up physical servers".

Create a protection plan for the entire SAP HANA server according to your server protection requirements, as described in the "Backup" section of the user documentation. For virtual machines, you do not need to specify pre- and post-data capture commands. The scripts will be called automatically by VMware Tools every time a quiesced snapshot is required. However, make sure that the **Multi-volume snapshot** option is enabled.

To enable or disable log truncation, edit the file /usr/sbin/post-thaw-script. By default, this script calls /usr/lib/Acronis/SAPHANA/bash/post_thaw.sh, which means that the logs are not truncated. To enable the truncation, change the `/usr/lib/Acronis/SAPHANA/bash/post_thaw.sh` string to `/usr/lib/Acronis/SAPHANA/bash/post_thaw_with_truncate_logs.sh`.

Recovering an entire server

Recover the physical or virtual server as described in the "Recovering a machine" section of the user documentation.

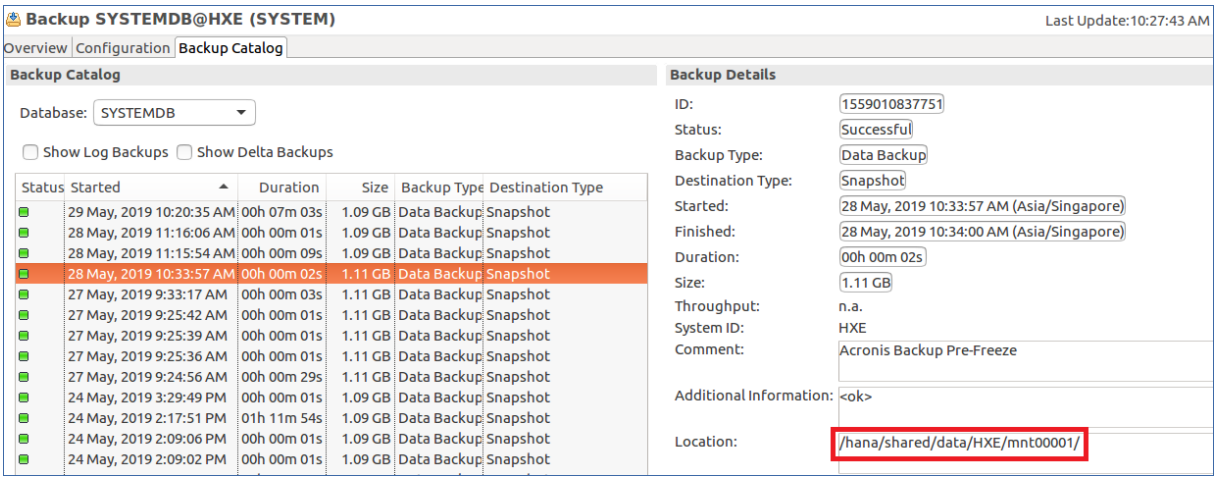
If you want to run a VMware ESXi virtual machine from a backup, proceed as described in the "Running a virtual machine from a backup (Instant Restore)" section of the user documentation.

Recovering a database by using SAP HANA Studio

If there is no need to recover the entire server, you can revert a database to a snapshot by using the native SAP HANA tools. Below are the examples of database recovery from HANA snapshots created during the pre-data capture commands execution.

These snapshots can be identified by the comment "Acronis Backup Pre-Freeze" in the backup details, for example, in the SAP HANA backup catalog.

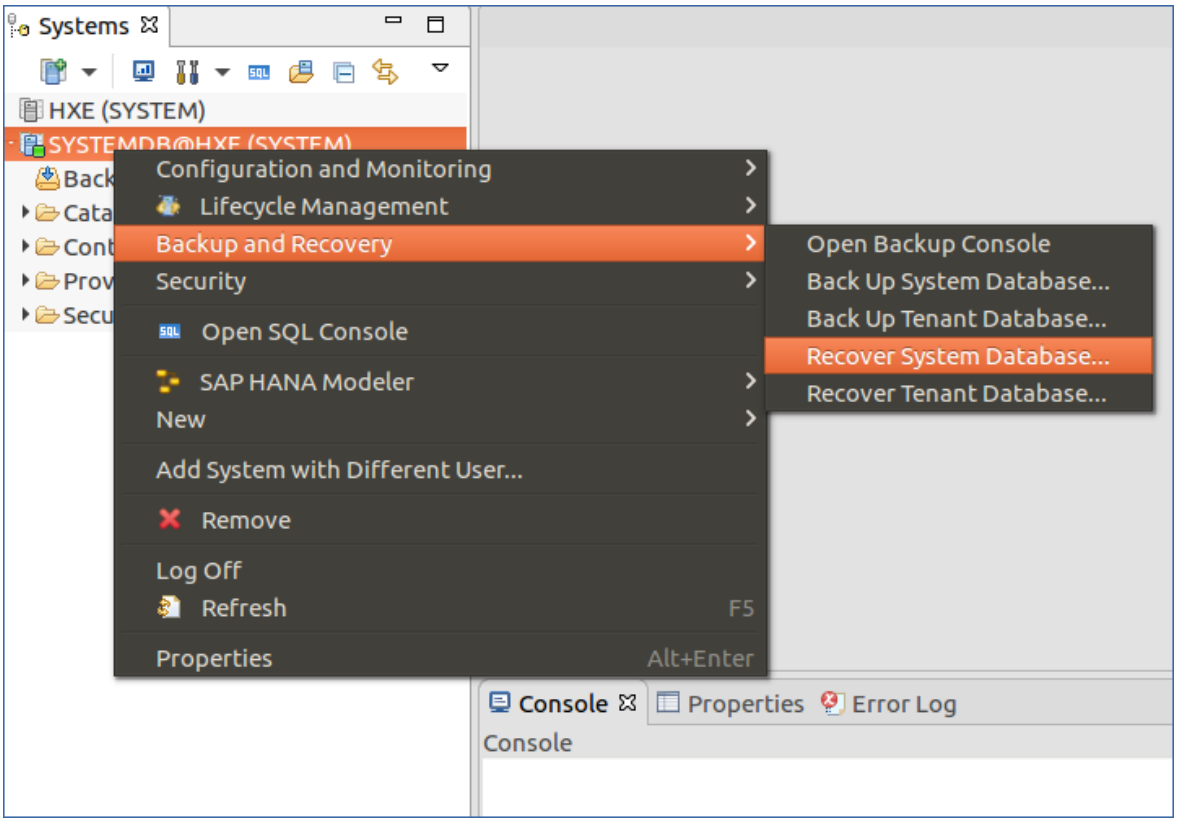
Prior to starting a recovery, make a note of the folder where the snapshots are located:



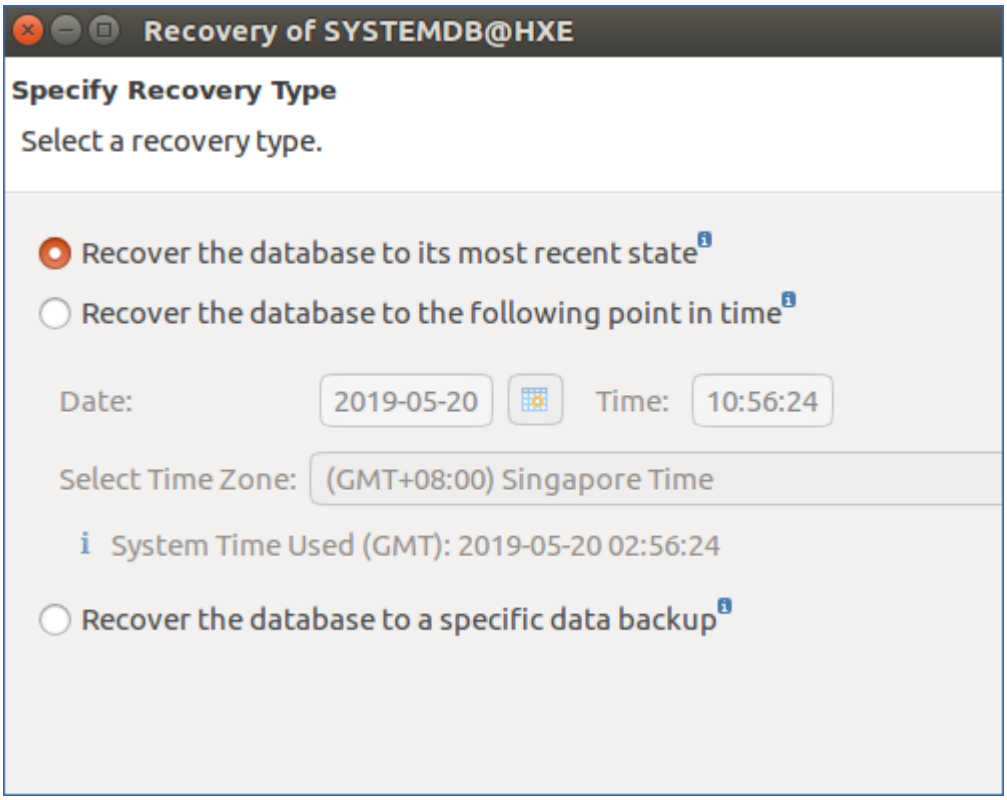
During a recovery, we will first recover the folder containing a snapshot, and then revert the databases to this snapshot by using SAP HANA Studio.

Recovery from the most recent backup

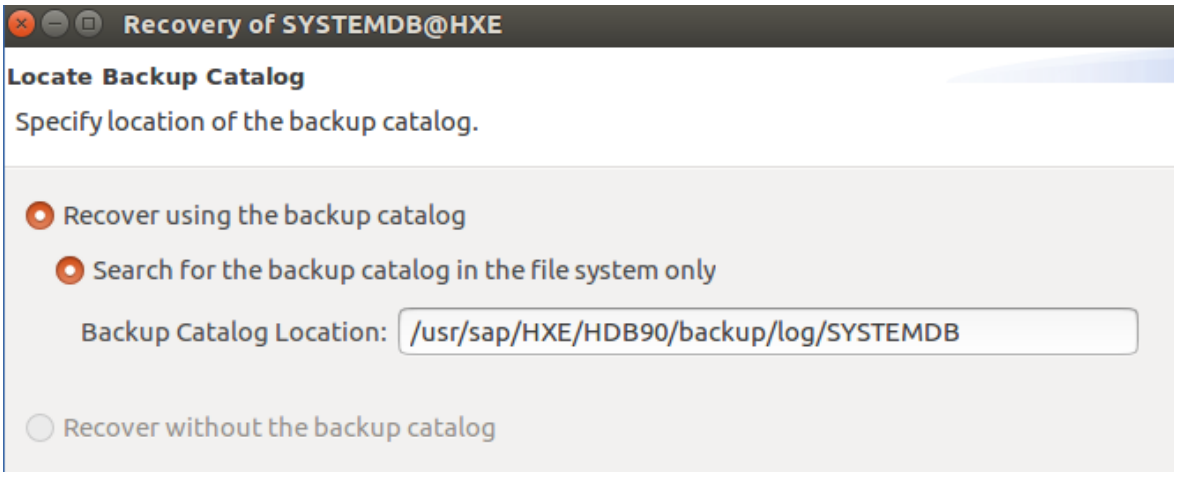
1. Stop the SAP services.
   a. Open the terminal and switch to SAP HANA user: `su <sid>adm`. For example, `su hxeadm`.
   b. Type `HDB stop`.
2. Recover the folder where the snapshots are located from the most recent backup created by the Cyber Protection service. The recovery procedure is described in the "Recovering files by using the web interface" section of the user documentation.
3. Start SAP HANA Studio.
4. Right-click the system database, and then select **Backup and Recovery** > **Recover System Database...**.



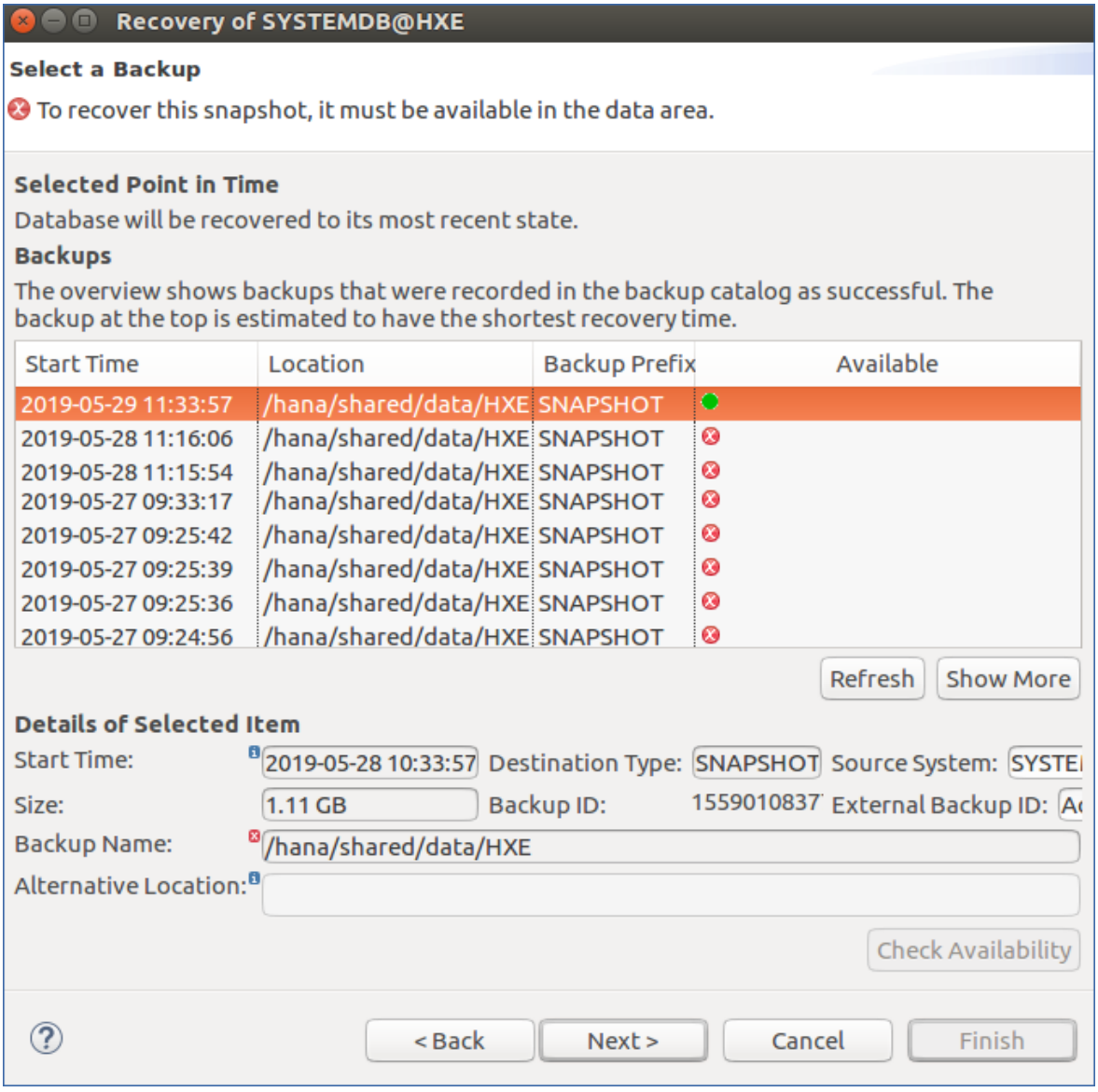
5. Select **Recover the database to its most recent state**.



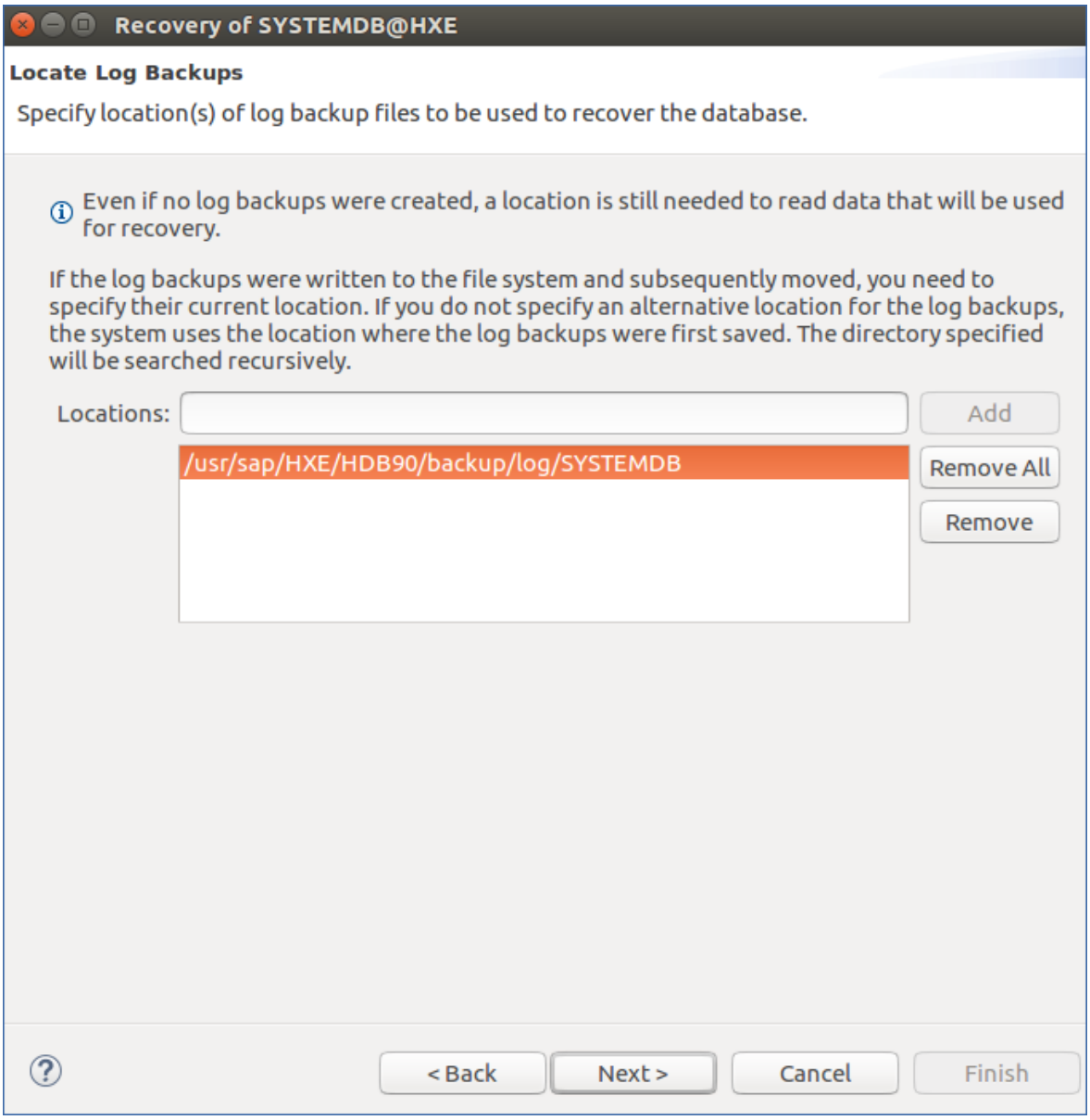
6. Check the backup catalog path and change it if necessary.



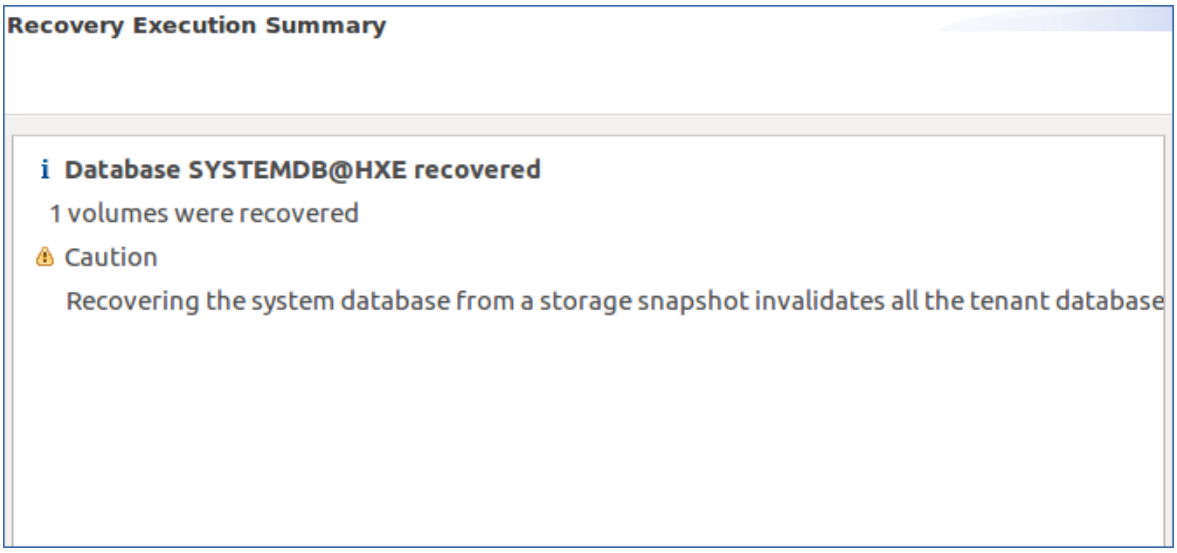
7. The latest snapshot should be available because it was recovered in step 2. Click **Refresh** if it is not.



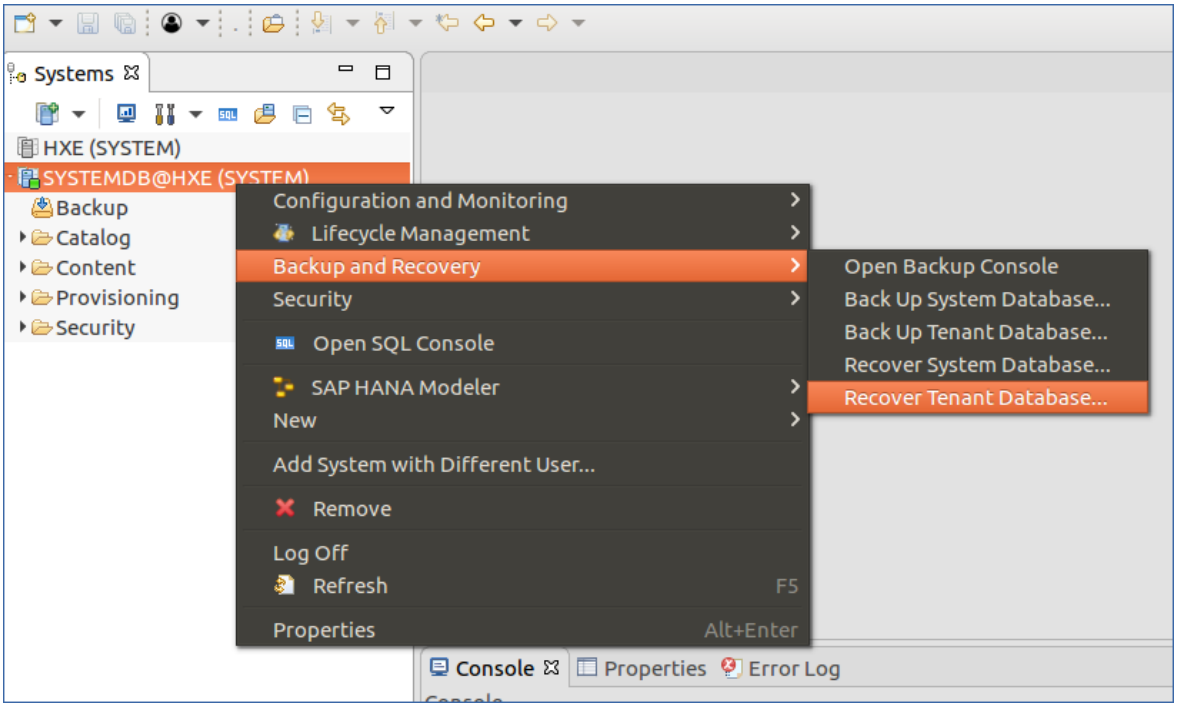
8. Check the log files path and change it if necessary.



9. In the **Other Settings** step, leave the default settings and click **Next**.
10. Review the recovery settings, and then click **Finish**. After a successful recovery, a message about the tenant database is shown.



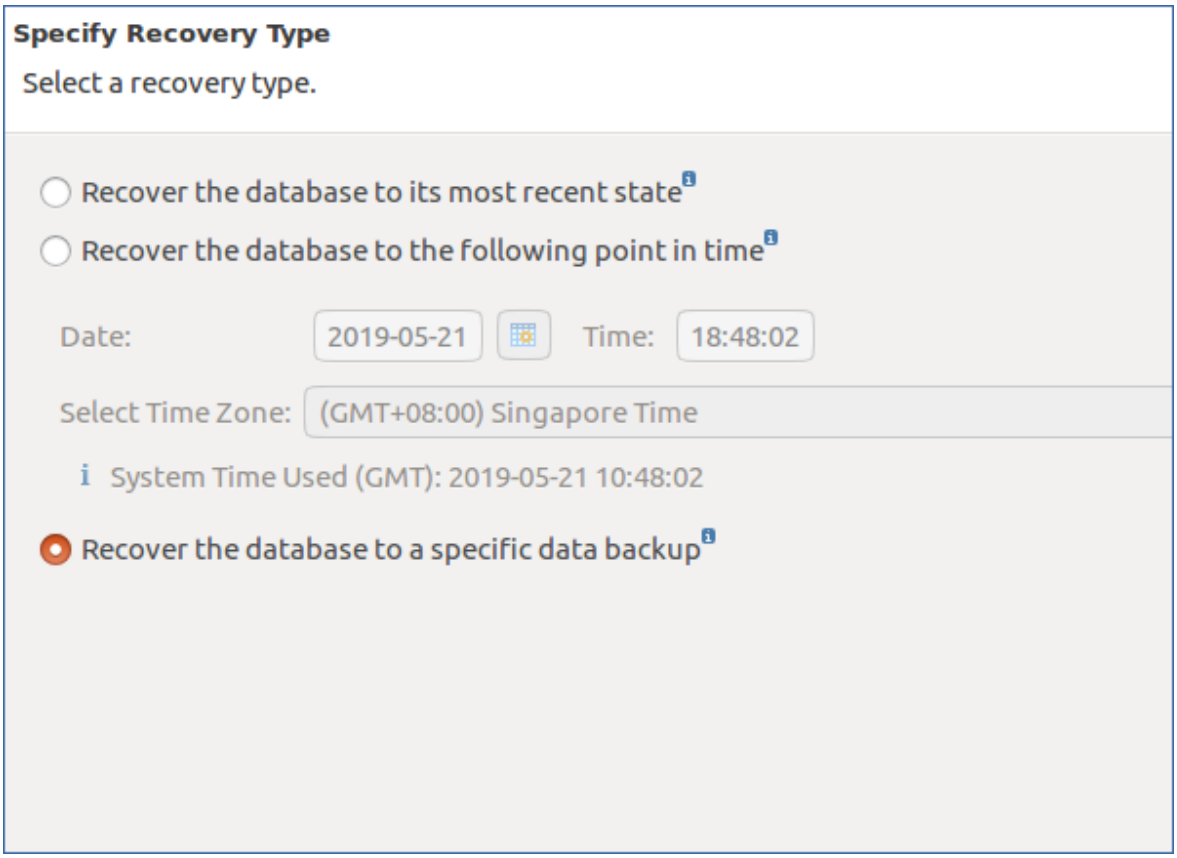
11. Right-click the system database, and then select **Backup and Recovery** > **Recover Tenant Database...**.



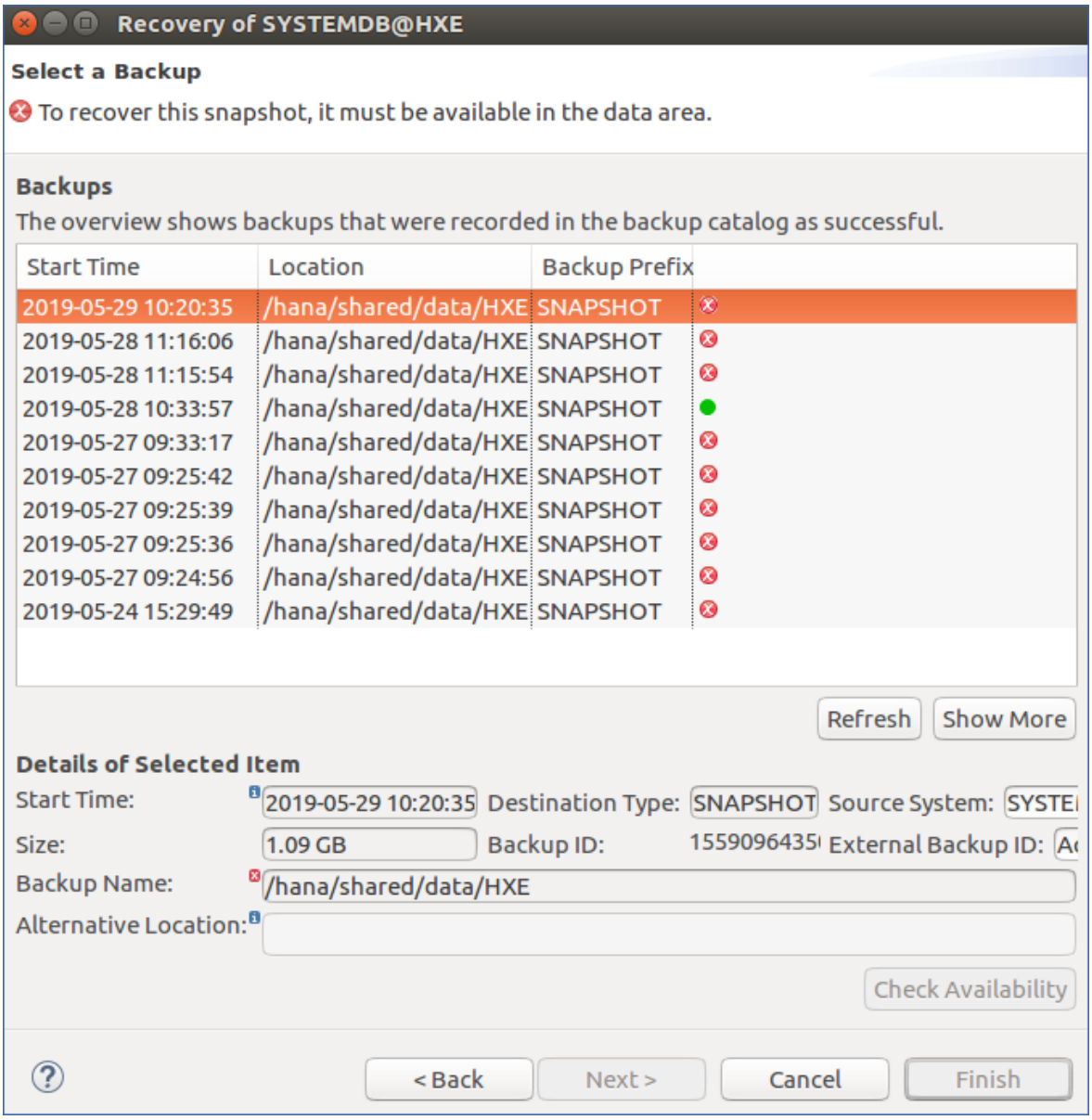
12. Repeat steps 5-10 for the tenant database.
13. After a successful recovery, open the terminal, switch to SAP HANA user, and then type `HDB start`.

Recovery from a specific backup

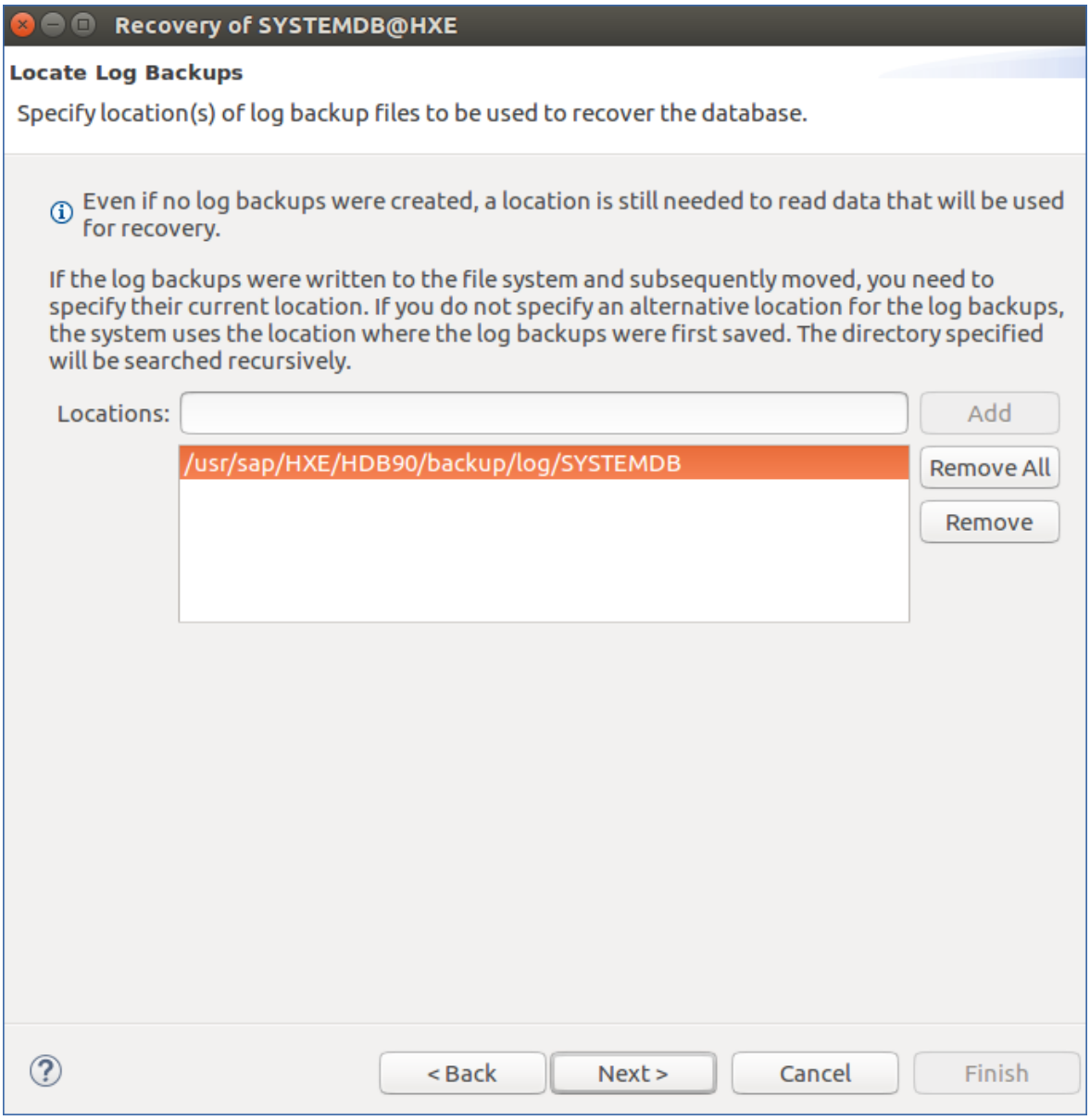
1. Start the SAP HANA studio and log on to the system database.
2. Right-click the system database, and then select **Backup and Recovery** > **Recover System Database...**.
3. Select **Recover the database to a specific data backup**, and then click **Next**.



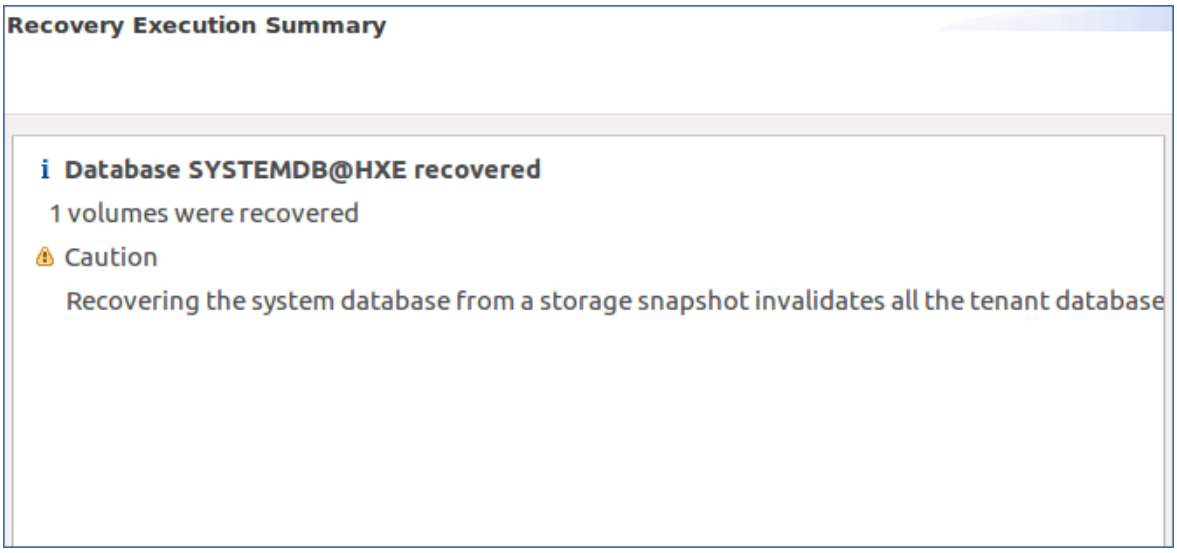
4. Select **Recover using the backup catalog**. Check the backup catalog path and change it if necessary.
5. In the backup catalog, the snapshots are shown as not available. Choose the snapshot to revert the database to and note the snapshot's **Start Time**.
6. Recover the folder where the snapshots are located from the backup created by the Cyber Protection service at the moment corresponding to the **Start Time** value. The recovery procedure is described in the "Recovering files by using the web interface" section of the user documentation.
7. Return to the backup catalog and click **Refresh**. The chosen snapshot is now shown as available. Select this snapshot and click **Next**.



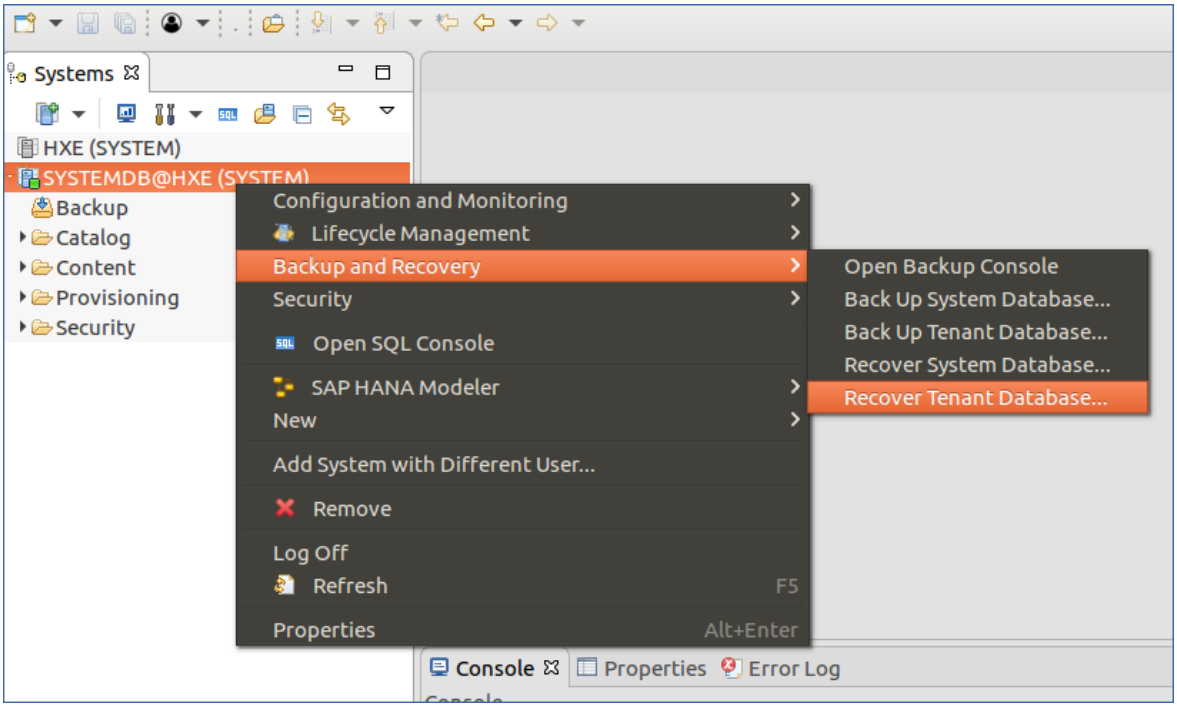
8. Check the log files path and change it if necessary.



9. In the **Other Settings** step, leave the default settings and click **Next**.
10. Review the recovery settings, and then click **Finish**. After a successful recovery, a message about the tenant database is shown.



11. Right-click the system database, and then select **Backup and Recovery** > **Recover Tenant Database...**.



12. Repeat steps 3-4 and 7-10 for the tenant database.
13. After a successful recovery, open the terminal, switch to SAP HANA user, and then type `HDB start`.